BRNO UNIVERSITY OF TECHNOLOGY

FACULTY OF INFORMATION TECHNOLOGY

DEPARTMENT OF INTELLIGENT SYSTEMS

HABILITATION THESIS

FINGERPRINT RECOGNITION TECHNOLOGY: IMAGE QUALITY, SKIN DISEASES AND LIVENESS DETECTION

2008

ING. MARTIN DRAHANSKÝ, PH.D.

Affirmation

This habilitation thesis is the result of my own work. The work has not been submitted either in whole or in part for a degree at any other university. Certain parts of the work have already been published – see please the chapter 7.1.

Dedication

I dedicate this work to my parents and Alex.

Martin Drahanský

Abstract

This thesis deals with three topics in the field of biometric fingerprint recognition. The first topic is devoted to the skin structure and various sensor technologies used for the fingerprint acquirement, namely optical, capacitive, ultrasonic, e-field, electro-optical, pressure, thermal, MEMS (Micro-Electro-Mechanical Systems) and sweep. This is followed by the description of influencing factors which could have an impact on the fingerprint acquirement process. To these factors we count also skin diseases that could be divided into three subcategories, i.e. those attacking the skin color, or papillary line structure, or both of them. Each skin disease is illustrated by a representative example.

The second topic covers the issues of estimation of fingerprint image quality. At the beginning, important error rates and curves for the evaluation of biometric system performance are introduced. In the subsequent text, suitable methods for image quality estimation are discussed (e.g. the methods based on contrast, mean value of grayscale levels, amount of papillary lines, sinusoidal shape of papillary line crosscut, etc.), followed by the methods for image quality enhancement (e.g. Gabor filtering, spatial or frequency domain filtering). At the end of this part, some experimental results related to this topic are presented.

The last topic deals with the liveness detection. At the beginning, some basic risks related to biometric systems are discussed and the need for liveness detection is explained. This is followed by the description of all known methods for the liveness detection which could be suitably used in the fingerprint recognition. At the end again certain experimental results related to this topic are presented.

Keywords

fingerprint, papillary line, sensor, influencing factors, skin, skin disease, image quality, image enhancement, liveness detection

Acknowledgements

First of all, I would like to thank my parents, Alex and friends for their tolerant attitude to my working effort during the elaboration of this habilitation thesis, especially in the last months, when the intensity of work rapidly increased. I would also like to thank my parents for their incessant support during all the years of my studies.

I would like to express my thanks to the head of Department of Intelligent Systems FIT BUT, Doc. Dr. Ing. Petr Hanáček for the proof reading of this thesis and his general support to my work. Further I would like to thank Prof. Ing. Jan M. Honzík, CSc. for his support during the processing of this work. For the cooperation in the field of liveness detection, many thanks belong to my colleague Ing. Dana Lodrová. For the correction of my English text, I would like to thank Ing. Jiří Fojtek, CSc.

At last, I would like to thank the Brno University of Technology, Faculty of Information Technology for its technical support. I would especially mention the research intent MSM0021630528 “Security-Oriented Research in Information Technology” and the project MSMT RP-253 “Promotion of habilitation”.

Contents

1. Introduction 1
1.1 Goals 4
1.2 Organization 5
2. Fingerprint Acquirement and Influencing Factors 7
2.1 Skin Structure 8
2.1.1 Epidermis 9
2.1.2 Dermis 10
2.1.3 Subcutaneous Tissue 11
2.2 Sensor Technologies for Fingerprint Acquirement 11
2.2.1 Inked Fingerprinting 12
2.2.2 Optical Technology 13
2.2.3 Capacitive Technology 16
2.2.4 Ultrasonic Technology 17
2.2.5 E-field Technology 18
2.2.6 Electro-optical Technology 19
2.2.7 Pressure Sensitive Technology 20
2.2.8 Thermal Technology 21
2.2.9 MEMS Technology 21
2.2.10 Touch and Sweep Sensors 23
2.3 Factors Influencing Fingerprint Acquirement 25
2.3.1 Surrounding Environment 25
2.4 Skin Diseases 29
2.4.1 Change of Papillary Line Structure 30
2.4.2 Change of Skin Color 34
2.4.3 Change of Papillary Line Structure and Skin Color 35
2.4.4 Recapitulation 39
3. Quality of Fingerprint Images 40
3.1 Methods for Estimation of Fingerprint Image Quality 46
3.1.1 Image Contrast 46
3.1.2 Mean Value of Grayscale Levels 47
3.1.3 Number of Papillary Lines ("RIP Count") 51
3.1.4 Failure to Acquire (FTA) Rate 52
3.1.5 Sinusoidal Shape of a Papillary Line Crosscut 52

3.1.6 Acquisition Performance Metrics 56
3.1.7 Image Quality as a Predictor of Matcher's Performance 58
3.1.8 Overall Quality Quantification 60
3.1.9 Biometric Sample Quality Scoring 63
3.1.10 Minutiae Quality Scoring 65
3.2 Methods for Image Quality Enhancement 67
3.2.1 Image Filtering Using Gabor Filters 68
3.2.2 Spatial Domain Filtering Algorithm 69
3.2.3 Frequency Domain Filtering Algorithm 70
3.3 Experimental Results 74
3.3.1 Determination of Contrast Ratios 75
3.3.2 Mean Value of Grayscale Levels 77
3.3.3 Number of Papillary Lines 81
3.3.4 FTA Rate 84
3.3.5 Compatibility 84
4. Liveness Detection 86
4.1 Basic Risks and Need for Liveness Testing 86
4.1.1 Susceptibility to Fakes 89
4.1.2 Attacks During Verification/Identification and Human Monitoring 92
4.1.3 Dilemma of Liveness Detection 93
4.2 Liveness Testing in the Fingerprint Recognition Technology 94
4.2.1 Perspiration 95
4.2.2 Spectroscopic Characteristics 97
4.2.3 Ultrasonic Technology 101
4.2.4 Physical Characteristics: Temperature 102
4.2.5 Physical Characteristics: Hot and Cold Stimulus 103
4.2.6 Physical Characteristics: Pressure Stimulus 104
4.2.7 Physical Characteristics: Electrical Properties 106
4.2.8 Physical Characteristics: Bio-Impedance 107
4.2.9 Physical Characteristics: Pulse 109
4.2.10 Physical Characteristics: Blood Oxygenation 115
4.2.11 Other Methods 115
4.3 Practical Experiments from Literature 116
4.3.1 Deceiving of Thermal, Capacitive and Optical Fingerprint Sensors 116
4.3.2 Biasing Current 118
4.3.3 Pulse 118

4.4 My Practical Experiments 119
4.4.1 Production of Fake Fingers 119
4.4.2 Our Experim. on Deceiving of Therm., Cap. and Opt. Fingerprint Sensors 121
4.4.3 Testing of Liveness by Temperature Measurement 122
4.4.4 Conductivity / Resistance 124
4.4.5 Pulse 125
5. Summary 140
6. Glossary 142
7. References 144
7.1 References Related to My Work 144
7.2 Other References 146

List of Tables

Tab. 3.1: Features of Suprema sensor units 75
Tab. 3.2: Region sizes 76
Tab. 3.3: Contrast ratios for all sensors (maximal, minimal and average) 76
Tab. 3.4: Maximal, minimal and average deviation values for mean values of grayscales 79
Tab. 3.5: Average, maximal and minimal numbers of papillary lines 82
Tab. 3.6: Specific fingerprints corresponding to the significant numbers of papillary lines 82
Tab. 3.7: The FTA rates and percentages of fingerprints with a poor quality 84
Tab. 3.8: Evaluation of the interoperability of the sensors 85
Tab. 4.1: Distances of ridges and valleys 126

List of Figures

Fig. 1.1: Different biometric attributes (arranged in accord. with their uniqueness)...........1

Fig. 1.2: Verification vs. identification...........2

Fig. 1.3: Examples of different fingerprints: a) and b) Inked fingerprints; c) Latent fingerprint; d) and e) Live-scan fingerprints...........5

Fig. 1.4: Examples of artificial fingers...........5

Fig. 2.1: An overview of the fingerprint recognition...........7

Fig. 2.2: Skin structure...........8

Fig. 2.3: Inked fingerprinting and manual fingerprint recognition by experts...........12

Fig. 2.4: Example of a Czech dactyloscopic card without personal data...........13

Fig. 2.5: Optical principle of fingerprint scanners...........14

Fig. 2.6: Fingerprint sensor using a) FTIR with a sheet prism; b) optical fibers...........14

Fig. 2.7: Examples of optical scanners (Identix BioTouch® 500; Sagem MorphoSmart Optic 300; BioLink MatchBook 3.5; Mitsumi SEF-A1F1)...........15

Fig. 2.8: Examples of contactless optical scanners (TST BiRD 3; NEC SA701); functionality principle of the contactless optic technology by NanoIdent (below)...........15

Fig. 2.9: Capacitive technology of fingerprint scanning...........16

Fig. 2.10: Examples of capacitive scanners (Veridicom 5th Sense; Suprema SFM3050; Fujitsu MBF200; UPEK TouchStrip™ TCS3-TCD4)...........17

Fig. 2.11: Ultrasonic technology: a) Sensor construction; b) Principle...........17

Fig. 2.12: Examples of ultrasonic scanners (UltraScan; Optel)...........18

Fig. 2.13: The principle of the e-field technology...........18

Fig. 2.14: Examples of e-field scanners (Suprema SFM3000; AuthenTec AES 4000; Validity VFS202)...........19

Fig. 2.15: Electro-optical principle with a CCD-camera...........19

Fig. 2.16: Electro-optical fingerprint sensor principle...........20

Fig. 2.17: Examples of electro-optical scanners (Ethentica; Testech Bio-i CYTE)...........20

Fig. 2.18: Pressure sensitive technology principle...........20

Fig. 2.19: Examples of pressure sensitive scanners (BMF BLP-100; Fidelica FIS-3002) 20

Fig. 2.20: Thermal technology principle...........21

Fig. 2.21: Example of thermal scanner (Atmel® AT77C104B)...........21

Fig. 2.22: The principle of a tactile fingerprint sensor...........22

Fig. 2.23: a) Schematic of the tactile measurement of the fingerprint (left); b) Microscopic images of real micro-beams (right)...........22

Fig. 2.24: Fingerprint sensor with an arrayed micro-heater: a) Device structure; b) Sensing principle...........23

Fig. 2.25: Sweeping sensor principle 24
Fig. 2.26: Examples of sweep scanners (Digital Persona Firefly; AuthenTec AES2810; Idex SmartFinger® IX 10-4) 24
Fig. 2.27: Fingerprints acquired under the influence of various factors 27
Fig. 2.28: Influence of temperature changes to the fingerprint scanning 28
Fig. 2.29: Incontinentia pigmenti on a child hand 29
Fig. 2.30: a) Staphylococcal abscess in a diabetic patient; b) "Music box" spine keratoderma 30
Fig. 2.31: a) Pitted keratolysis; b) Palmar pits; c) Keratolysis exfoliativa 31
Fig. 2.32: Fingertip eczema: a) An early stage; b) A more advanced stage; c) Full inflammation 31
Fig. 2.33: Fingertip eczema: a) Asteatotic eczema; b) Chronic eczema; c) Another form of chronic eczema 32
Fig. 2.34: a) Tripe palms; b) Side view of a pyogenic granuloma 32
Fig. 2.35: a) Verruca vulgaris; b) Pityriasis rubra pilaris 33
Fig. 2.36: a) Blistering distal dactylitis; b) Scleroderma 33
Fig. 2.37: a) Hand-foot-and-mouth disease; b) Hyperlinear palmar creases; c) Plane xanthoma; d) Infective endocarditis 34
Fig. 2.38: a) Tinea of the hand; b) Epidermolytic hyperkeratosis; c) Epidermolysis bullosa simplex; d) Generalized epidermolysis bullosa 35
Fig. 2.39: a) Early irritant hand dermatitis with dryness and chapping; b) Subacute and chronic eczematous inflammation with severe drying and splitting of the fingertips; c) Atopic diathesis 36
Fig. 2.40: a) Numerous tiny vesicles suddenly appeared on these chronically inflamed fingers; b) Irritant dermatitis from chronic handwashing 36
Fig. 2.41: a-c) Different variants of pompholyx; d) Pustular psoriasis 36
Fig. 2.42: a) Hereditary hemorrhagic telangiectasia; b) Purpura fulminans 37
Fig. 2.43: a) Erythema and telangiectasia; b) Scarlet fever 37
Fig. 2.44: a) Norwegian scabies; b) Psoriasis 38
Fig. 2.45: a) Raynauld's phenomenon – acrogangrene; b) Secondary syphilis on palms .38
Fig. 3.1: Diagram of general biometric system 40
Fig. 3.2: Impostor and genuine distributions 42
Fig. 3.3: Receiver Operating Curve (ROC) 43
Fig. 3.4: Minutiae examples (line ending, single bifurcation, double bifurcation, triple bifurcation, point, interval, hook; single whorl, double whorl, through line, crossing, side contact, single bridge, twin bridge) 44
Fig. 3.5: Flowchart results of the minutiae extraction algorithm 45
Fig. 3.6: a) Temporary change of fingerprint image quality; b) Images from the same user with a poor quality 45

Fig. 3.7: Fingerprint compression: a) an uncompressed fingerprint image; b) portion of image compressed using a generic image compression algorithm JPEG; c) portion of image compressed using WSQ 46

Fig. 3.8: Example of a fingerprint histogram 48

Fig. 3.9: Normalized histogram 49

Fig. 3.10: Searching for the mean value *M* 50

Fig. 3.11: a) Type lines; b) Delta configurations; c) Core configurations; d) Number of lines 50

Fig. 3.12: Numbers of horizontal and vertical papillary lines 51

Fig. 3.13: Crosscut of the fingerprint (axis x = pixels, axis y = grayscale values) 53

Fig. 3.14: Application of the sine function to the crosscut of the fingerprint 53

Fig. 3.15: Determination of the thickness of ridges (foreground) 54

Fig. 3.16: Determination of upward and downward sections of the curve 55

Fig. 3.17: Global vs. local pattern 57

Fig. 3.18: Examples of pairs (the left image is original, the right image is an algorithm assessment representation) with a) a good quality and b) poor quality 59

Fig. 3.19: Qualities of different images, legend: *Q*(overall quality, smudginess, dryness) 63

Fig. 3.20: Comparison of worse and better matching samples 64

Fig. 3.21: a) Original fingerprint; b) Ridge skeletons extracted by binarization and thinning algorithm; c) Ridge skeletons extracted by direct gray scale algorithm; d) Enhanced fingerprint image using Gabor filters; e) Ridges extracted by direct gray scale algorithm after Gabor filter based fingerprint image enhancement 66

Fig. 3.22: Examples of fingerprint regions: a) Well-defined region; b) Recoverable region; c) Unrecoverable region 68

Fig. 3.23: Gabor filters in spatial domain with eight different orientations 69

Fig. 3.24: The flowchart of the spatial domain fingerprint enhancement algorithm 70

Fig. 3.25: a) + c) Blocks of a fingerprint model with different frequencies; b) + d) DCT coefficients related to figures a) and c), respectively 71

Fig. 3.26: Examples of the relationship between ridge orientation in spatial domain and peak-angle in DCT domain, all ridge angles relate to the horizontal axis and DC coefficient is set to zero in order to show a high-frequency spectrum 72

Fig. 3.27: Highly curved ridges in spatial and frequency (DCT) domain. The signal is localized in a widely curved sub-band which can be classified as either the principal region (R_1) or the reflection region (R_2) 74

Fig. 3.28: Suprema scanners (SFM3000, SFM3010, SFM3020, SFM3050) 75

Fig. 3.29: Michelson contrast ratios for all sensors 77

Fig. 3.30: The mean value of grayscale values for the sensor Suprema SFM3000 (average ≅ 43) 78

Fig. 3.31: The mean value of grayscale values for the sensor Suprema SFM3010 (average ≅ 40) 78

Fig. 3.32: The mean value of grayscale values for the sensor Suprema SFM3020 (average ≅ 28) 78

Fig. 3.33: The mean value of grayscale values for the sensor Suprema SFM3050 (average ≅ 21) 78

Fig. 3.34: Histogram of the sensor SFM3050 (only a half of the *x*-axis is used) 81

Fig. 3.35: Numbers of papillary lines for the sensor SFM3000 83

Fig. 3.36: Numbers of papillary lines for the sensor SFM3010 83

Fig. 3.37: Numbers of papillary lines for the sensor SFM3020 83

Fig. 3.38: Numbers of papillary lines for the sensor SFM3050 84

Fig. 4.1: Basic components of a biometric system 86

Fig. 4.2: Artificial fingerprints generated by SFinGe 90

Fig. 4.3: Examples of fake fingers produced by the company Vernet® 92

Fig. 4.4: Example of live fingerprint images acquired some time apart 95

Fig. 4.5: The top pair shows captures of an artificial finger acquired 0 and 5 second apart and the bottom pair shows the same for a cadaver finger 95

Fig. 4.6: Live fingerprint signals (bottom), where the solid line shows initial reading and the dashed line shows the reading after five seconds 96

Fig. 4.7: Ascent of sweat from sweat pores on a fingertip (4× zoomed) 97

Fig. 4.8: Spectrographic properties of different components of living tissue (suitable for detection of spoofing attacks on iris recognition) 98

Fig. 4.9: FTIR and multispectral imager 98

Fig. 4.10: Multispectral imager (MSI) 99

Fig. 4.11: a) Conventional and multispectral ($\lambda_{1...5}$ = 475, 500, 560, 576, 625 nm) fingerprint image; b) Real multispectral image data 100

Fig. 4.12: Multispectral image data can clearly discriminate between a living finger and an ultra-realistic spoof. The graphs on the left side show how similar the spectral content of each image is to that expected for a genuine finger 100

Fig. 4.13: Schematic of ultrasonic pulse/echo principle 101

Fig. 4.14: Index finger with newsprint to demonstrate the finger contamination (from left: contaminated original, ultrasound image, optical image) 102

Fig. 4.15: Thermo-scans of the fingertips acquired using a thermo-camera FLIR 103

Fig. 4.16: Functionality principle of the device measuring hot and cold stimulus 103

Fig. 4.17: Images of the fingertips pressed tightly (left subpart) and slightly (right subpart) to the sensor 104

Fig. 4.18: Functionality principle of device measuring pressure stimulus 105

Fig. 4.19: Two functionality principles of device measuring pressure stimulus 105

Fig. 4.20: A sequence of fingerprint images describing the deformation of a real finger105

Fig. 4.21: A flowchart showing different phases of the approach 106

Fig. 4.22: Three skin surface electrode systems on an underarm. Functions: M – measuring and current carrying, CC – current carrying, PU – signal pick-up 108

Fig. 4.23: Typical impedance spectrum obtained with four equal electrodes attached to the skin of the underarm 108

Fig. 4.24: Light absorption, dispersion and reflection by a fingerprint 109

Fig. 4.25: Detection of saturation of hemoglobin 110

Fig. 4.26: a) (left) Demonstration of heart activity; b) (right) Action potential waveforms and propagation in the human heart [68]: A. Schematic of action potentials, recorded in different regions of the human heart, are displaced in time to reflect the temporal sequence of propagation; B. Schematic of a ventricular action potential labeled as follows: 0=depolarization, 1=early (fast) repolarization, 2=plateau phase, 3=late (slow) phase of repolarization, and 4=after hyperpolarization/return to the resting membrane potential (SA=sino-atrial, AV=atrio-ventricular, RV=right ventricle, LV=left ventricle) 111

Fig. 4.27: ECG diagram example 112

Fig. 4.28: Integrated liveness detection – scanner + optical and laser solution 112

Fig. 4.29: Possible integration of a camera-based measurement system for liveness detection with optical fingerprint sensor (CCD/CMOS camera) 113

Fig. 4.30: a) Region for analysis of fine movements; b) Schematic representation of skin behavior before and after heart expansion 113

Fig. 4.31: Possible integration of laser distance measurement for liveness detection with optical fingerprint sensor (CCD/CMOS camera; aperture approx. 6 mm) 114

Fig. 4.32: Photography of my optical bench for measurement by the above mentioned methods 115

Fig. 4.33: Fingerprints from thermal sensor (from true finger (left) and silicon fake (right)) 116

Fig. 4.34: a) Silicon fake fingerprint scanned by a capacitive sensor, with minutiae found in the image (left); b) Moisturized fake fingerprint scanned by a capacitive sensor; c) Fingerprint of dead person scanned by a capacitive sensor 117

Fig. 4.35: Histograms: left – moisturized fake finger; right – live finger 117

Fig. 4.36: Measurement of fake fingers using different scanner technologies 117

Fig. 4.37: Biasing current in connection with 50 Hz signals 118

Fig. 4.38: Acquired 20 images per second using a capacitive sensor 118

Fig. 4.39: Intentional changes of pressure on the finger and resulting graph 119

Fig. 4.40: Optical recognition of heart pulses 119

Fig. 4.41: Individual steps of fake finger(print) production 120

Fig. 4.42: Fingerprint images (from left to right): a) real finger captured by an optical sensor; b) fingerprint stamp captured by an optical sensor; c) real finger captured by a thermal sensor; d) fingerprint stamp captured by a thermal sensor 121

Fig. 4.43: Images captured by a capacitive sensor (from left to right): a) simple breath; b) stamp; c) stamp and breath; d) real finger 122

Fig. 4.44: Thermo-scan of a finger with 4 measurement points 122

Fig. 4.45: Average temperature values for all users and all fingers 123

Fig. 4.46: Measurement of finger skin resistance (conductance) 124

Fig. 4.47: a) Resulting average resistances for DC low voltage measurement (left); b) Resulting average resistances for AC low voltage measurement (right) 125

Fig. 4.48: Macro lens test frames with zoom factors 4 (upper row) and 10 (lower row) 128

Fig. 4.49: Used optical device installations 128

Fig. 4.50: Screenshot from the detection application of fine movements of papillary lines 129

Fig. 4.51: Applications for manual (left) and automatic (right) distance measurement .. 129

Fig. 4.52: Example of manual distance measurement method (User 1) 130

Fig. 4.53: Results from automatic measurement of distance changes (User 1) 131

Fig. 4.54: Results from automatic measurement of distance changes (User 2) 131

Fig. 4.55: Results from automatic measurement of distance changes (User 3) 132

Fig. 4.56: Analysis of the sequence 3 (yellow) from Fig. 4.54 132

Fig. 4.57: Luminance change leading to a failure in finding of appropriate end points in automatic distance change measurement 133

Fig. 4.58: Principle of triangulation 134

Fig. 4.59: Laser measurement installation for liveness detection 134

Fig. 4.60: Distance measurement curves from the triangulation laser sensor. Abscissa: time; ordinate: voltage reflecting distance changes 135

Fig. 4.61: Example (an oscilloscope screenshot) of the curve representing the heart beat rate 135

Fig. 4.62: Original (left) and normalized and adjusted (right) curve from the oscilloscope 136

Fig. 4.63: Time analysis of the acquired curve from the oscilloscope (1 second/division) 136

Fig. 4.64: Time analysis of the acquired curve from the oscilloscope (2 seconds/division) 137

Fig. 4.65: Analysis of the normalized and adjusted curve from the application 138

1. Introduction

The beginning of massive use of biometric devices dates from the terrorist attacks on the World Trade Center in USA. It has been found out that the physical or behavioral attributes, related to the concrete person, are the best way how to confirm the identity of such person. These attributes are, among others, used in biometric systems to prevent terrorists and suspicious people to enter states, buildings or computer networks / systems. Other use is in forensic applications [89] or monitoring systems.

We divide the biometric systems into two main groups – verification or identification systems [33][60][51][Dra21][Dra12] (Fig. 1.2). *Verification systems* are used for the authorization of a user, i.e. the user claims his/her identity and the biometric system should confirm or reject such claimed identity, whereas the decision whether the user is who he/she claims to be is based on the recognition of a biometric attribute. The second group, *identification systems* are most often used for forensic tasks, i.e. based on the biometric attribute the system should find the identity of the user. The difference is not only in database searches, where verification systems do 1:1 comparison (biometric template with the claimed identity is compared with the actually acquired biometric sample; the result is one matching score [33][30][31][32] leading to the decision accept/reject), on the other hand, identification systems do 1:N comparisons (the actually acquired biometric sample is compared with all biometric templates stored in the database (in total N records); the result is a candidate list [33][30][31][32], including the best "fitting" templates to the actual sample), but also in the field of industrial use, error rates, reliability, time consumption, used features, etc.

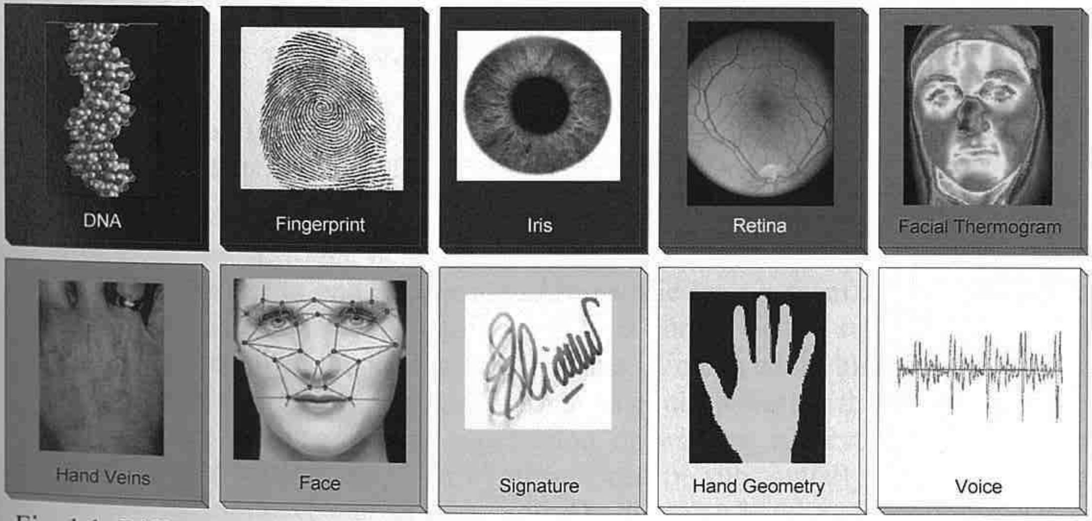
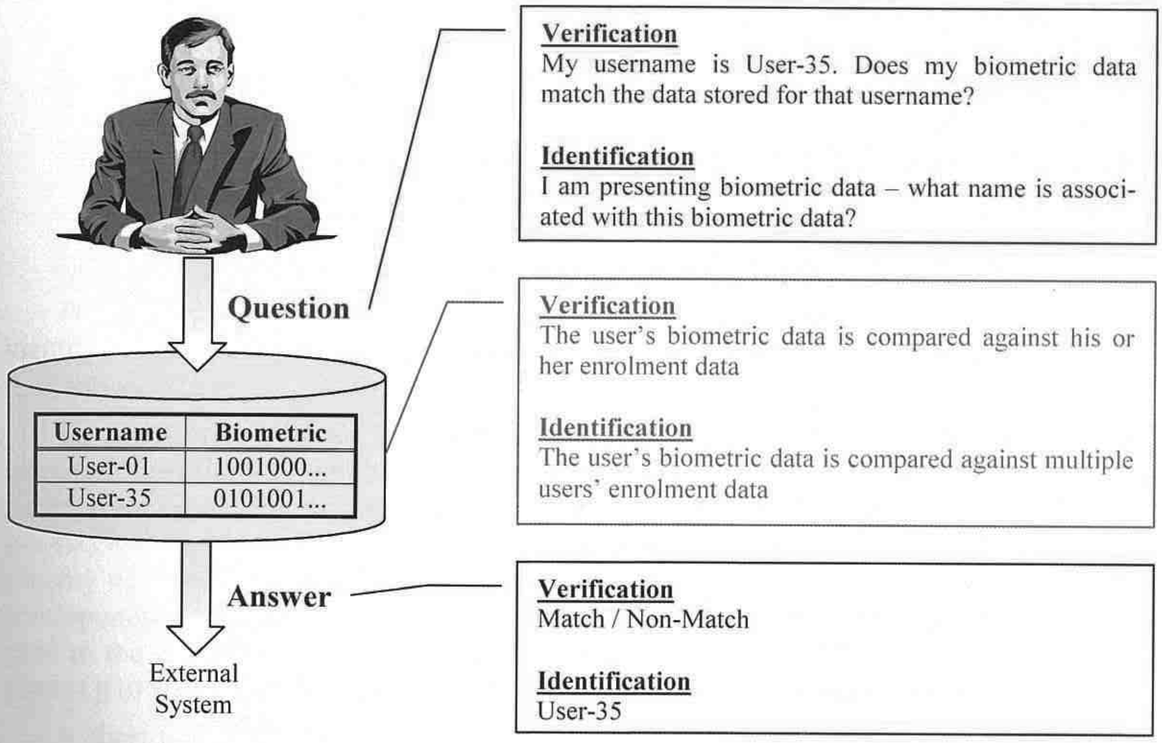


Fig. 1.1: Different biometric attributes (arranged in accord. with their uniqueness) [Dra21].

There are many biometric technologies, which measure some anthropometrical or behavioral attributes of human beings [33][9][69], such as (see Fig. 1.1): *face*, *fingerprint*, *eye iris*, *eye retina*, *DNA* [29], *hand geometry* and *veins*, *finger veins*, *gait*, *signature*, *voice*, *facial thermogram*, *ear shape*, *body odor*, etc. Regrettably, some of them do not have enough entropy [Dra21][Dra18][Dra26][Dra28] to recognize a greater amount of users. Nevertheless there are certain biometric attributes, which have enough entropy, are very reliable and show only little changes during the life of an individual – such as DNA, fingerprint, eye iris, etc. (see background color of the pictures in Fig. 1.1, which corresponds to the entropy, i.e. the ability to recognize respective users).



Username	Biometric
User-01	1001000...
User-35	0101001...

Verification
My username is User-35. Does my biometric data match the data stored for that username?

Identification
I am presenting biometric data – what name is associated with this biometric data?

Verification
The user's biometric data is compared against his or her enrolment data

Identification
The user's biometric data is compared against multiple users' enrolment data

Verification
Match / Non-Match

Identification
User-35

Fig. 1.2: Verification vs. identification [Dra21].

A good question is – why this work is devoted to the fingerprint recognition. There are two big subparts in fingerprint recognition (Fig. 1.2) [Dra23][77]:

- *Access systems* – these are the common systems which are used for the access control to computer, room, network, etc. Here the systems actually do the verification (comparison one to one, i.e. the actual biometric sample from the user is compared only with his template; the user's identity is known before such comparison) and therefore are called the verification systems. We can count biometric travel documents in this category. The access systems could differ by their use, i.e. whether the systems are used under supervision or without supervision. If the system works under supervision, then its misuse can be substantially reduced and therefore its performance can be improved. On the other hand, no supervision leads to the possible use of fake fingers to cheat the system, misuse/damage of the system and deterioration of performance and reliability. The functionality is simple – a user presents his identity to the system (e.g. by ID card, USB token, PIN, etc.) and puts his finger to the scanner. His finger is scanned and respective biometric sample is then compared with the stored biometric template under the user's identity. If the comparison is successful, the user's identity is either accepted or rejected.

- *Forensic systems* – this is that part of biometric systems, where the comparison of one to many is realized, i.e. the user's identity is unknown and the system performs the search in the whole database and compares all relevant templates with the actual biometric sample. Such systems are called dactyloscopic systems (identification systems only in the case of fingerprints). These systems are often used in the criminal practice, e.g. in finding of an offender leaving his fingerprint at the crime scene. The functionality works as follows: the fingerprint is obtained either from the crime scene (often latent fingerprints) or from a user with unknown identity (e.g. dead body), features are extracted and the biometric sample is then compared with all biometric templates stored in the database. In the end, a candidate list is presented, with those candidates who have very similar fingerprints with the given fingerprint. The real identity may not be in the list, however if yes, then the starting candidates should correspond to the real identity of the offender.

The fingerprints are used for the authorization or determination of the claimed user's identity. This function of biometric systems could be found in security systems as an authorization part.

The difference between the verification and identification systems lies in time consumption (passing through the whole database is a time-critical operation), in storage capacity (one biometric template vs. thousands or millions of biometric templates), art of use (access vs. identity determination) and reliability (access systems confirm the user's identity with some probability; identification systems offer the candidate list with the best corresponding templates). In various situations, there are various requirements with regard to the error rates (i.e. FAR (*False Acceptance Rate*) / FRR (*False Rejection Rate*) [Dra31][104]), what influences the setting of a threshold and implementation.

A short history of fingerprint recognition is presented in the following text. The first known use of fingerprinting was in 9th century in China, where merchants applied their fingerprints to documents authenticating a record of debt [119]. In 14th century Persia government officials used their fingerprints in the same way as we use signatures today [119]. Here is the list of significant dates from the history of fingerprints [119]:

- 1684: *Nehemiah Grew* published the first paper on the ridge structure of skin of fingers and palms. In 1685, *Govard Bidloo* and *Marcello Malpighi* published books on anatomy which also illustrated the ridge structure of fingers.
- 1788: *Johann Christoph Andreas Mayer* recognized that fingerprints are unique to each individual.
- 1823: *Jan Evangelista Purkyně*, a professor of anatomy at the University of Breslau, published his thesis discussing nine fingerprint patterns, but he did not mention the use of fingerprints to identify persons.
- 1853: *Georg von Meissner* studied friction ridges.
- 1858: *Sir William James Herschel* initiated fingerprinting in India.
- 1880: *Dr. Henry Faulds* published his first paper on the subject in the scientific journal Nature in 1880. Returning to the UK in 1886, he offered the concept to the Metropolitan Police in London but it was dismissed.

- 1892: *Sir Francis Galton* published a detailed statistical model of fingerprint analysis and identification and encouraged its use in forensic science in his book "Finger Prints".
- 1892: *Juan Vucetich*, an Argentine police officer who had been studying Galton pattern types for a year, made the first criminal fingerprint identification. He successfully proved Francisca Rojas guilty of murder after showing that the bloody fingerprint found at the crime scene was hers, and could only be hers.
- 1897: The world's first Fingerprint Bureau opened in Calcutta, India, after the Council of the Governor General approved a committee report (on June 12th, 1897) that fingerprints should be used for classification of criminal records.
- 1901: The first United Kingdom Fingerprint Bureau was founded in Scotland Yard. The Henry Classification System, devised by Sir Edward Richard Henry with the help of Haque and Bose was accepted in England and Wales.
- 1902: *Dr. Henry P. DeForrest* used fingerprinting in the New York Civil Service.
- 1906: New York City Police Department Deputy Commissioner *Joseph A. Faurot* introduced fingerprinting of criminals to the United States.

As you can see, the fingerprint recognition has a far-reaching history and is today accepted as a reliable person verification and/or identification method. Nevertheless, there are some parts in fingerprint recognition technology, which haven't been studied well till today – and these parts represent the fields of study and goals of this work.

1.1 Goals

This habilitation thesis is focused on a single biometric attribute – a fingerprint. The biometric systems intended for the processing and recognition of fingerprints are well known and are described in detail in the literature, e.g. [52][59][14][49]. However, there are some topics in this field of fingerprint recognition, which are not explored well at the moment or are often neglected. Three of these topics are the main themes of this habilitation thesis – *skin diseases*, *estimation of the fingerprint's quality* and *detection of liveness*.

The theme of *skin diseases* belongs to the group of influencing factors to fingerprint acquirement and image quality. The users suffering from a skin disease often cannot be enrolled into the fingerprint recognition system and therefore could not use such system in the future. This fact is often neglected – almost always only the error rates and reliability of biometric systems are discussed, but nobody thinks of disadvantaged users. Skin diseases don't only change the color of the fingertip, but in the worst case attack the papillary lines and the epidermal layer of the skin and therefore destroy the papillary lines structure. If the epidermal layer is irrecoverably destroyed, then the papillary lines will never be restored and the user can not use such fingerprint recognition system for the whole rest of his life.

The *quality of a fingerprint* is very important, because samples with low quality lead to worse error rates [33][30][31] and could cause false rejection of a genuine user or false acceptance of an offender. The determination of the quality score is not simple – there are many metrics, but the results differ from the quality estimation done by a dactyloscopic expert. The criterion of image quality is applicable especially in dactyloscopic systems [49] – see the variations among different images of fingerprints in Fig. 1.3.

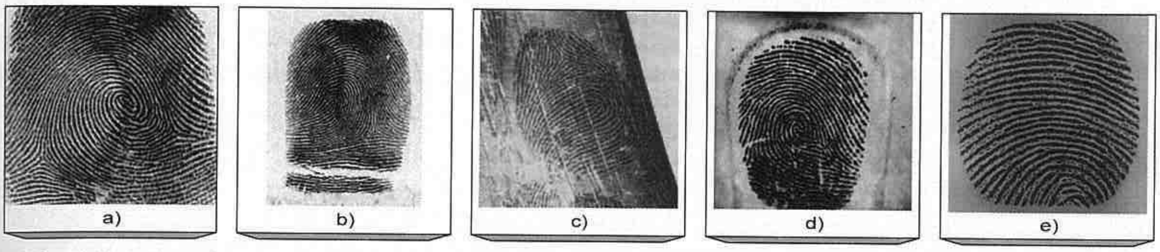


Fig. 1.3: Examples of different fingerprints [Dra21]: a) and b) Inked fingerprints; c) Latent fingerprint; d) and e) Live-scan fingerprints.

The *detection of liveness* is crucial in the contemporary fingerprint recognition systems, as the ability of attackers to make an artificial finger(print) (see Fig. 1.4) and to cheat the biometric system is very high. There is no need of very expensive or inaccessible materials or tools; commonly available things are sufficient and the most fingerprint scanning technologies could be misused. It is very simple to generate an artificial fingerprint [72][Dra02], which has nearly all the same minutiae (or very similar) as the fingerprint of a genuine user being misused.

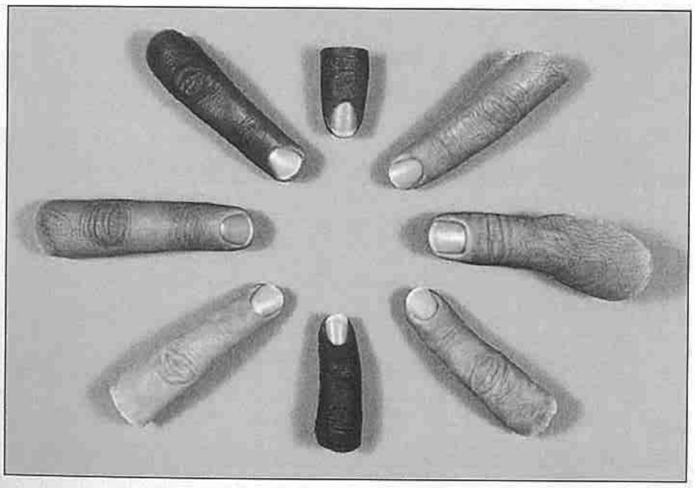


Fig. 1.4: Examples of artificial fingers [108].

1.2 Organization

This work is organized as follows: the chapter 2 describes fingerprint acquirement technologies, i.e. the functionality of fingerprint scanners and impact of factors which can influence the scanning process. One important part of this chapter are skin diseases, which very often represent a neglected factor, however these lead to the rejection of users who have some problems with their skin.

The chapter 3 deals with the estimation of quality of fingerprint images. The first part of this chapter describes known methods for the fingerprint quality estimation. The second part is devoted to the method which is suitable for quality estimation based on papillary lines, i.e. which is recommendable for dactyloscopic systems. At the end, there are shown some experiments and results of selected methods used in tests.

The chapter 4 describes all known methods for the detection of liveness of fingers. In this chapter, there are also described two new and patented methods for detection of liveness. At the end of this chapter, there are shown some experiments and achieved results.

The final chapters contain the summary, glossary (abbreviations) and references.

2. Fingerprint Acquirement and Influencing Factors

This chapter deals with the acquirement of fingerprints and circumstances which influence their quality. The acquirement process is limited only to fingerprint recognition systems, because the whole work is devoted only to the fingerprint related topics.

The fingerprint recognition consists of five main steps (see Fig. 2.1) [59][6][33] [Dra20]:

- *Fingerprint acquirement* – the fingerprint is scanned using a sensor (for sensor technologies see chapter 2.2), i.e. the physical human biometric attribute is digitized and transferred to the computer.
- *Image enhancement* – this step is very important for further processing, because the quality of the fingerprint image could be enhanced here [37]. There are several methods used for image quality enhancement – edge filters, filtering in frequency spectrum (after Fast Fourier Transform), Gabor filter, etc.
- *Thresholding* – the image is normally acquired with 256 gray levels, but we need a binary representation. Using various thresholding schemes (e.g. adaptive thresholding or regional average thresholding), it is possible to separate papillary lines (ridges) from background (valleys).
- *Thinning* or *Skeletization* – the papillary lines from the previous step have varying thickness. To make the algorithm for minutiae extraction as simple as possible, we prefer the thickness of all papillary lines in all parts having only one pixel.
- *Minutiae extraction* – this algorithm detects and extracts all minutiae found in the fingerprint. We distinguish between minutiae in verification systems (here are generally used 2 minutiae – ridge ending and bifurcation [Dra21]) and identification (dactyloscopic) systems [89], where many special minutiae are used.

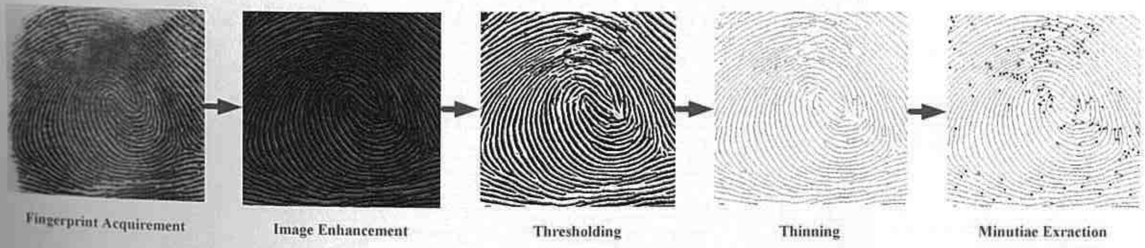


Fig. 2.1: An overview of the fingerprint recognition.

The fingerprint recognition technology is well accepted in our society [71]. Fingerprints could be used not only for the known user verification / identification tasks, but also e.g. for cryptographic key generation [Dra21][Dra22][Dra24][Dra27][Dra29][25][96] [67][19], computerized patient record [55] or for use with credit cards [66][34] etc.

2.1 Skin Structure

In the process of fingerprint image acquirement, the skin structure on the fingertip is scanned. Therefore we should know basics of our skin structure to understand better why for example skin diseases might have an influence on the acquirement process.

Skin is a remarkable organ of the body, which is able to perform various vital functions. It can mould to different shapes, stretch and harden, but can also feel a delicate touch, pain, pressure, hot and cold (see chapter 4.2.5), and is an effective communicator between the outside environment and the brain.

Skin makes up to 12-15% of an adult's body weight. Each square centimeter has 6 million cells, 5,000 sensory points, 100 sweat glands and 15 sebaceous glands. It consists of three layers (see Fig. 2.2) [110]: *epidermis* (the outer layer), *dermis* ("true skin") and *subcutaneous* (fat) layer.

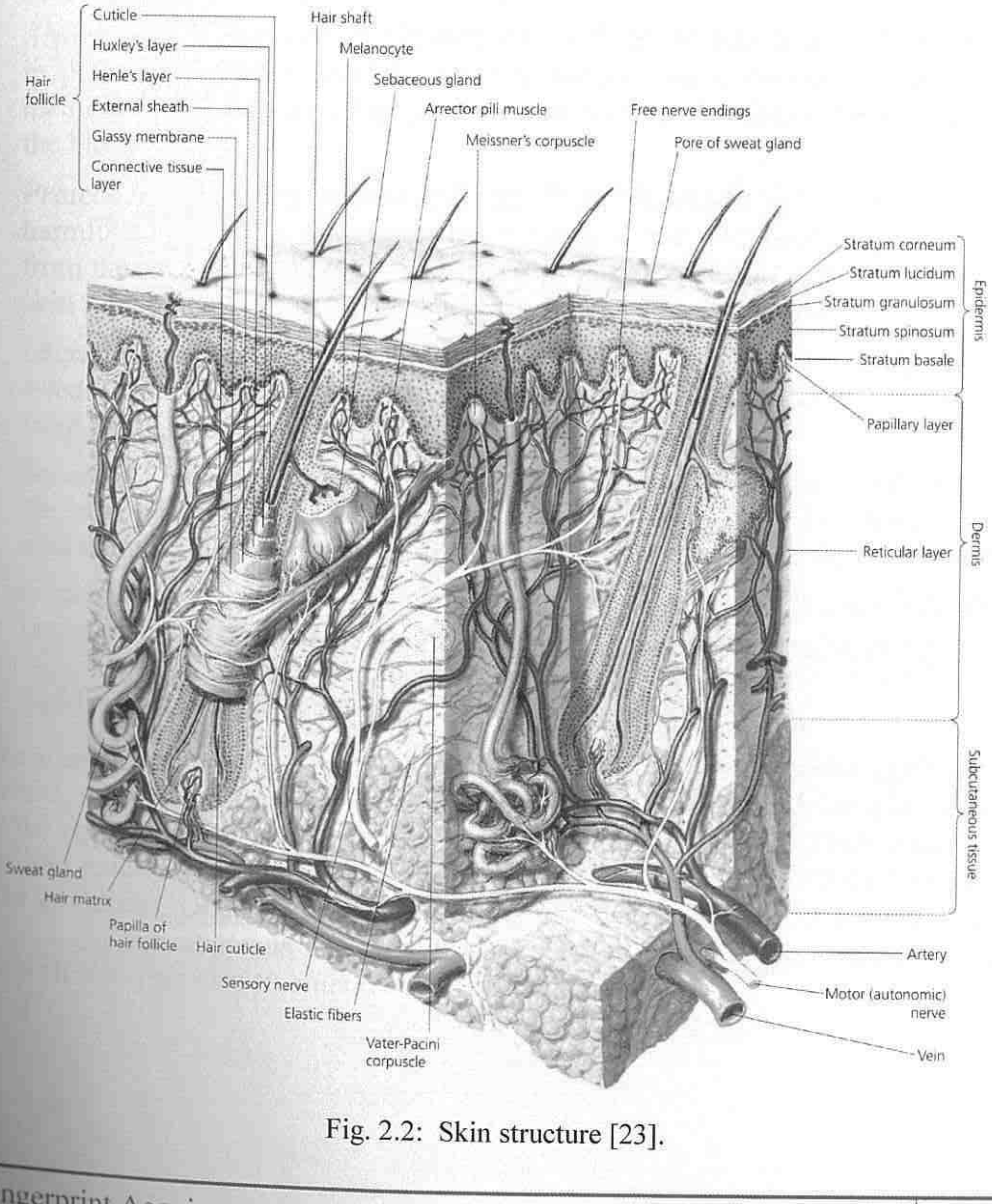


Fig. 2.2: Skin structure [23].

Skin is constantly being regenerated. A skin cell starts its life at the lower layer of the skin (the basal layer of the dermis), which is supplied with blood vessels and nerve endings. The cell migrates upward for about two weeks until it reaches the bottom portion of the epidermis, which is the outermost skin layer – the papillary lines are placed here. The epidermis is not supplied with blood vessels, but has nerve endings. For another 2 weeks, the cell undergoes a series of changes in the epidermis, gradually flattening out and moving toward the surface. Then it dies and is shed.

There are six skin functions [110]:

- *Sensation* – the nerve endings in the skin identify touch, heat, cold, pain and light pressure.
- *Heat regulation* – the skin helps to regulate the body temperature by sweating to cool the body down when it overheats and by shivering creating "goose bumps" when it is cold. Shivering closes the pores. The tiny hair that stands on end traps warm air and thus helps keep the body warm.
- *Absorption* – absorption of ultraviolet rays from the sun helps to form vitamin D in the body, which is vital for bone formation. Some creams, essential oils and medicines (e.g. anti-smoking patches) can also be absorbed through the skin into the blood stream.
- *Protection* – the skin protects the body from ultraviolet light – too much of it is harmful to the body – by producing a pigment called melanin. It also protects us from the invasion of bacteria and germs by forming an acid mantle (formed by the skin sebum and sweat). This barrier also prevents moisture loss.
- *Excretion* – waste products and toxins are eliminated from the body through the sweat glands. It is a very important function which helps to keep the body "clean" from the inside.
- *Secretion* – sebum and sweat are secreted onto the skin surface. The sebum keeps the skin lubricated and soft, and the sweat combines with the sebum to form an acid mantle which creates the right pH-balance for the skin to fight off infection.

Very interesting information about the building of skin structures (papillary lines) and finger formation could be found in [45].

2.1.1 Epidermis

The main function of the *epidermis* [110] is to form a tough barrier against the outside world, while the dermis is a soft, thick cushion of connective tissue that lies directly below the epidermis and largely determines the way our skin looks. Both layers keep repairing and renewing themselves throughout our life, but the dermis does it more slowly than the epidermis. Under the dermis there is a layer of fat cells, which is known as adipose tissue (or subcutaneous fat layer). It provides insulation and protective padding for the body. It also provides an emergency energy supply.

The epidermis consists of five layers [110]:

- *Basal layer* (*stratum germinativum*) – this is the bottom layer of the skin. The cells of this layer are constantly being reproduced, since they contain a nucleus, or seed. As the cells reproduce, the layers get constantly pushed up into the next layer.
- *The prickle cell layer* (*stratum spinosum*) – called this way because the cells have spines which prevent bacteria entering the cells and moisture being lost. These cells also have a nucleus and therefore reproduce.
- *Granular layer* (*stratum granulosum*) – the prickle cells lose their spines and become flatter. The nucleus dies, and a protein called keratin is formed. This protein prevents moisture loss and can be found in skin, nails and hair.
- *Clear layer* (*stratum lucidum*) – this layer is for cushioning and protection and can be found only on the palms of the hands and soles of the feet.
- *Horny* (*cornified*) *layer* (*stratum corneum*) – the cells here are dead and ready to be shed (by desquamation). This process speeds up as we age.

2.1.2 Dermis

The *dermis* [110] is the layer responsible for the skin's structural integrity, elasticity and resilience [110]. Wrinkles develop in the dermis. Therefore, an anti-wrinkle treatment has a chance to succeed only if it can reach the dermis. Typical collagen and elastin creams, for example, never reach the dermis because collagen and elastin molecules are too large to penetrate the epidermis. The curvatures of papillary lines are formed in the dermis layer, which are then projected to the epidermis layer as real papillary lines.

The dermis is the middle layer [110] of the skin located between the epidermis and subcutaneous tissue. It is the thickest of the skin layers and comprises a tight, sturdy mesh of collagen and elastin fibers. Both collagen and elastin are critically important skin proteins: collagen is responsible for the structural support and elastin for the resilience of the skin. The key type of cells in the dermis is fibroblasts, which synthesize collagen, elastin and other structural molecules. The proper function of fibroblasts is highly important for overall skin health. The dermis also contains capillaries (tiny blood vessels) and lymph nodes which produce immune cells. Blood capillaries are responsible for bringing oxygen and nutrients to the skin and removing carbon dioxide and products of cell metabolism. Lymph nodes are engaged in protecting the skin from invading microorganisms. Finally, the dermis contains sebaceous glands, sweat glands, hair follicles and a small number of nerve and muscle cells. Sebaceous glands, based around hair follicles, produce sebum, an oily protective substance that lubricates the skin and hair and provides protection by forming an acid mantle when mixed with sweat. When sebaceous glands produce too little sebum, as it is common at older people, the skin becomes excessively dry and more prone to wrinkling; this could be problematic in fingerprint recognition.

The dermis is thicker than the epidermis, but has fewer cells. It consists mainly of the connective tissue which is made up of fibers of the proteins collagen and elastin and a non-fibrous gelatin-like material called ground substance or extracellular matrix.

2.1.3 Subcutaneous Tissue

Subcutaneous tissue [110] is the deepest layer of the skin located under the dermis and consisting mainly of fat cells. It acts as a shock absorber and heat insulator, protecting underlying tissues from cold and trauma. The loss of subcutaneous tissue in later years, leads to facial sag and makes wrinkles more visible. To counteract it, a cosmetic procedure where fat is taken from elsewhere in the body and injected into facial areas, is common these days. From the point of view of fingerprint recognition, this layer is not very important.

2.2 Sensor Technologies for Fingerprint Acquirement

Before we can process the fingerprint image further we need to obtain a digitalized fingerprint [84][13]. The traditional (dactyloscopic) method uses the ink to get the fingerprint onto a piece of paper. This piece of paper is then scanned using a common (office) scanner. Nowadays, this method is used only in the case when an old paper-based database is being digitalized, a fingerprint is found on a crime-scene or in law enforcement AFIS systems. Otherwise modern live fingerprint readers are used. They do not require the ink anymore; they use different physical effects to acquire the image of a finger.

First of all, we should characterize a digital fingerprint image by the following main parameters [85]:

- *Resolution*. The minimum resolution for FBI-compliant sensors is 500 dots per inch (DPI), and this is also met by many commercial devices. The sensor resolutions lie in the range from 250 DPI to 1,000 DPI.
- *Area*. The larger the area, the more ridges and valleys are captured, and the more distinct the pattern becomes. The minimum area size required by FBI specifications is 1×1 square inches. Many sensors today have an area much smaller than that, thus making it impossible for the entire print to be captured. A small area keeps the cost and size down, but does also lead to unnecessary false rejections. The sensor areas used in contemporary systems start by approx. 0.7×0.7 cm and end by approx. 10×6 cm (for rolled fingerprints or for multi-finger scanning).
- *Dynamic range* (or *depth*). The number of bits used to encode the intensity value of each pixel. A grayscale is used and the FBI standard for pixel bit depth is 8 bits. Some sensors capture however only 2 or 3 bits of information.
- *Geometric accuracy*. Can be defined as the maximum geometric distortion introduced by the acquisition device, and is expressed as a percentage with respect to x and y directions.
- *Image quality* (see chapter 3). Difficult to measure, especially since it is hard to decouple it from the intrinsic finger quality or status.

All the characteristics mentioned above work together to set the accuracy of the system. Some of them could be improved by an enhancement algorithm (e.g. image quality).

While the first generation scanners used optical techniques [85], a variety of sensing techniques are used today and almost all of them belong to one of the three families [85][70]: *optical*, *solid-state*, and *other* (e.g. ultrasound). There is another category yet, fingerprint acquisition via inking [70][49][27], which is the traditional mode of criminal fingerprint capture. It is evident that this is inappropriate for fingerprint verification due to the inconvenience involved with ink, the need for subsequent digitization, and perhaps the stigma of this type of capture. The type of image acquisition for fingerprint verification is also called "live-scan fingerprint capture".

The main technologies used today are optical and solid-state sensors (mainly capacitive sensors). Solid-state sensors are now gaining great popularity because of their compact size, which facilitates in embedding them into laptop computers, cellular phones, smart cards, etc.

It should be considered for which type of scanning the sensor is used. We have to distinguish among three main types of fingerprint scanning purposes:

- *Access systems*: the finger is scanned on a classical scanner or a sweep scanner, where only one finger is scanned in a time.
- *Systems for visa applicants*: there are scanned four fingers simultaneously.
- *Dactyloscopic systems*: each finger is scanned in addition as a rolled fingerprint.

Nevertheless to the above categorization to only three categories, we will define all fingerprint scanning technologies as separate methods, because they do use special physical effects to obtain the impression of a finger. To the known technologies belong [Dra25] [47][80][103][113]: *optical*, *capacitive*, *ultrasound*, *e-field*, *electro-optical*, *pressure sensitive*, *thermal* and *MEMS* (Micro-Electro-Mechanical Systems). At the beginning of the sensor technologies description, it should not be neglected the old method of getting an inked fingerprint – see subchapter 2.2.1.

2.2.1 Inked Fingerprinting

This technique is the first used method for taking of fingerprints. The fingertip is put in touch with a black ink and then pressed to the paper, to leave the impression on the paper (Fig. 2.3 left) [89][74]. This method has been used for the acquirement of fingerprints from a person onto the dactyloscopic card [111] (Fig. 2.4) which has been used for manual fingerprint recognition (Fig. 2.3 right) or comparison with a fingerprint from a crime-scene. However, this obsolete method has been displaced with a new one – using an electronic fingerprint scanner to acquire the fingerprint in a digitalized form and then to process it automatically in a computer (so called AFIS).

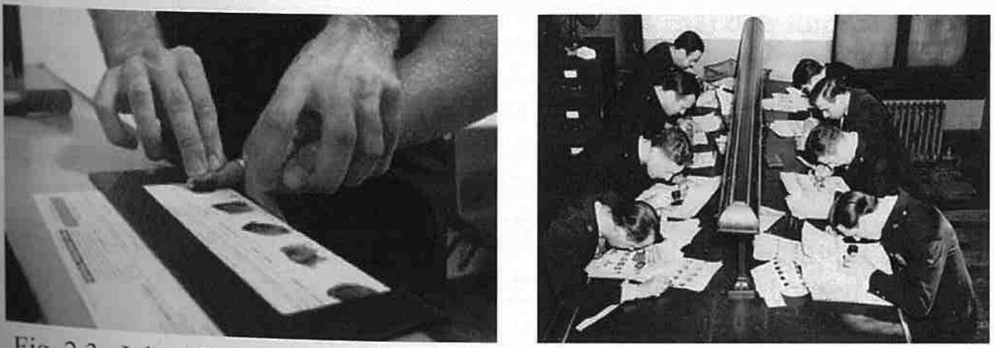


Fig. 2.3: Inked fingerprinting and manual fingerprint recognition by experts [109].

The process of getting an inked fingerprint for dactyloscopic (criminal forensics) recognition is however a little bit different from the classical fingerprint acquirement known from the common access systems. This difference could be observed in Fig. 2.4 – in the two upper rows, there are rolled fingerprints (the finger is laid on one side and rolled to the opposite side), whereas in the lower part of the dactyloscopic card, there are only "picked" or "laid" fingerprints, i.e. the finger is only laid to the paper surface, instead of rolling. The rolling process achieves greater area of the finger (including fingerprint's core and delta point [Dra21]), nevertheless, the papillary lines are often blurred what leads to worse image quality, because there could be an important minutia point in the place, where the blur is occurred.

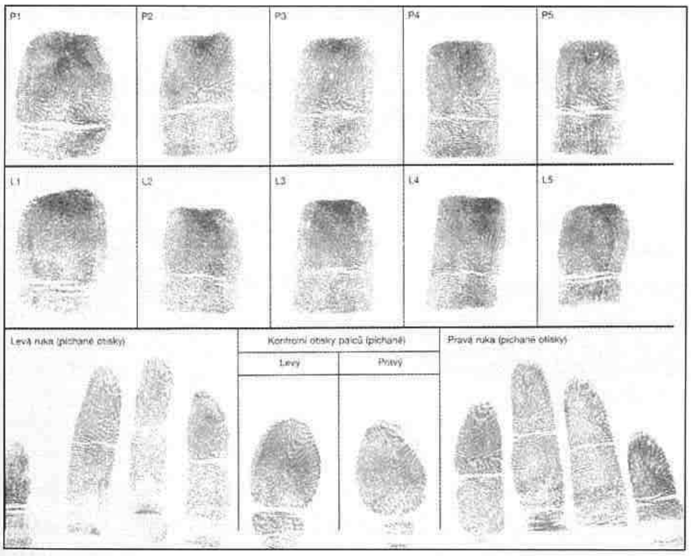

P1
P2
P3
P4
P5
L1
L2
L3
L4
L5
Levá ruka (pichané otisky)
Kontrolní otisky palců (pichané)
Levý
Pravý
Pravá ruka (pichané otisky)

Fig. 2.4: Example of a Czech dactyloscopic card without personal data.

2.2.2 Optical Technology

Optical fingerprint capture devices have the longest history dating back to the 1970s [70]. The optical technology is based on the *Frustrated Total Internal Reflection* (FTIR) principle. When you place your finger on an FTIR-based optical sensor (Fig. 2.5), the ridges will be in contact with the protective glass (or prism) surface, while the valleys (papillary lines) will remain at a distance. One side of the protective glass is illuminated through a diffuse light (a bank of light-emitting diodes (LED) or a film planar light). The light is reflected at the ridges and randomly scattered (absorbed) at the valleys. The lack of reflection from the ridges makes it possible to acquire an image of the fingerprint. In the early days' FTIR sensors, a CCD camera was used to acquire the fingerprint image. Today, the FTIR sensors have shrunk considerably in size and cost with the help of the new CMOS technology [85].

Innovations in optical devices have been made recently, primarily in an effort to reduce the size of these devices. Whereas an optical sensor was housed in a box about 15×8×15 cm still in the mid-1990s, smaller devices have recently appeared, with sizes in the order of 8×2×2 cm [70]. However, it is difficult to make a small enough FTIR device suitable to embed into a PDA or a mobile phone, etc.

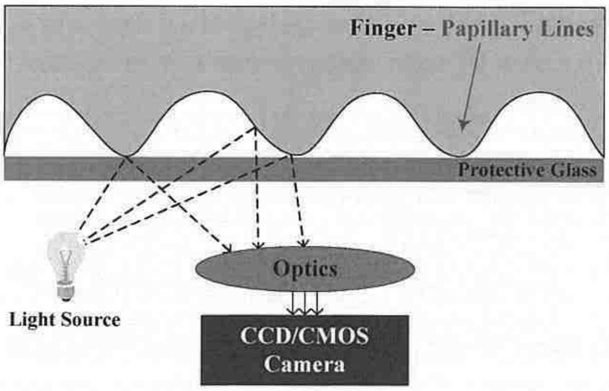


Fig. 2.5: Optical principle of fingerprint scanners [Dra20].

In the optical technology, there are two further possibilities how to construct an optical sensor: *FTIR with a sheet prism* and *optical fibers* (Fig. 2.6).

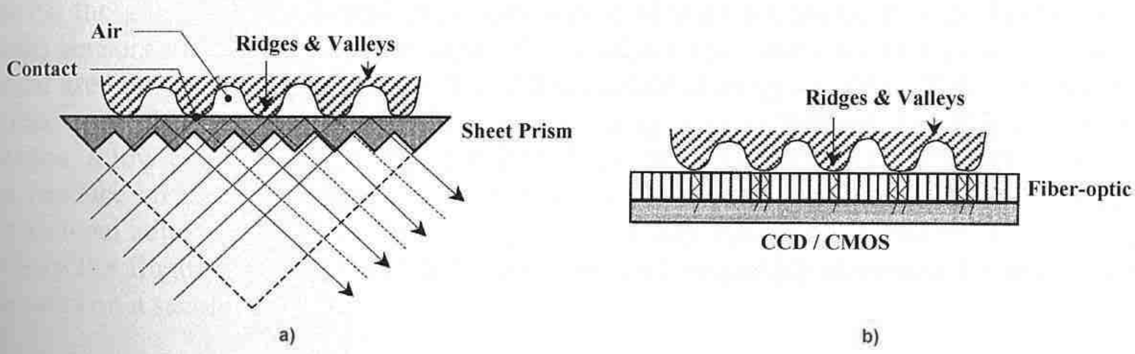


Fig. 2.6: Fingerprint sensor using a) FTIR with a sheet prism; b) optical fibers [85].

FTIR with a sheet prism (Fig. 2.6a) [85] sensor uses a sheet prism made of a number of "primlets" adjacent to each other, instead of a single large prism. With the advantage of size reduction, the quality of the acquired images is however lower than traditional FTIR techniques using glass prisms.

Optical fibers (Fig. 2.6b) [85] technique uses a fiber-optic plate instead of a prism and lens. The finger is in direct contact with the upper side of the plate, while the lower side of the plate is tightly coupled with a CCD or CMOS camera, which receives the light conveyed through the glass fibers. Since the CCD/CMOS camera is in direct contact with the plate (without any intermediate lens as in the FTIR techniques), its size has to cover the whole sensing area. High costs will thus be the downside of producing large area sensors with this technique.

The advantages [85] with optical sensors include withstanding temperature fluctuations (to some degree), a fairly low cost, resolutions up to 500 DPI, better image quality, and the possibility of larger sensing areas. Since FTIR devices sense a three-dimensional surface, it is difficult to fool them with a photograph or image of a fingerprint [85]. The resistance against electrostatic shock is up to ca 18 kV [Dra25].

The disadvantages [85] of optical sensors are their size and problems with latent prints. Cuts, abrasions, calluses, and other damage, as well as dirt, grease and other contamination, can also be a problem with optical scanners [85]. Latent prints are however still a problem [85]. The average power consumption is ca 50 mA.

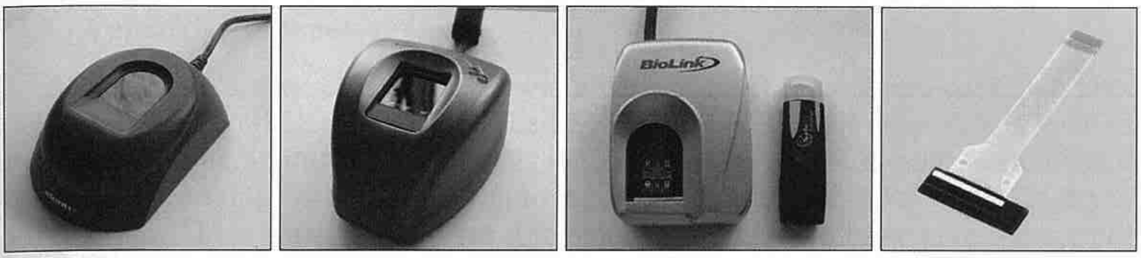


Fig. 2.7: Examples of optical scanners (Identix BioTouch® 500; Sagem MorphoSmart Optic 300; BioLink MatchBook 3.5; Mitsumi SEF-A1F1).

A functionality that has not been available before solid-state sensors is locally adjustable, software-controlled, automatic gain control (AGC) [70]. For the most optical devices, the gain can be adjusted only manually to change the image quality. Some solid-state sensors, however, offer the capability to adjust the sensitivity of a pixel or row or local area automatically to provide the added control of image quality. AGC can be combined with feedback to produce high quality images over different conditions. For instance, a low-contrast image (e.g. dry finger) can be sensed and the sensitivity increased to produce an image of higher contrast on a second capture. With the capability to perform local adjustment, a low-contrast region in the fingerprint image can be detected (e.g. where the finger is pressed with little pressure) and sensitivity increased for those pixel sensors on a second capture.

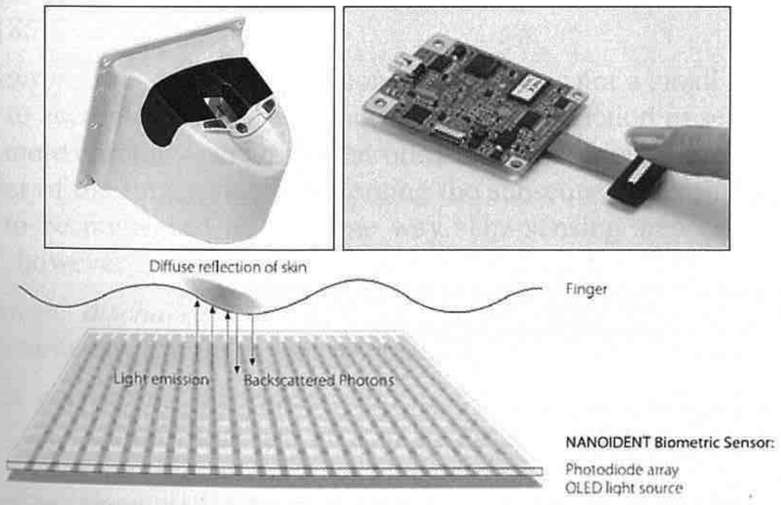


Fig. 2.8: Examples of contactless optical scanners (TST BiRD 3; NEC SA701); functionality principle of the contactless optic technology by NanoIdent (below).

There is a subcategory of the optical technology – *contactless optical scanning*. Contactless readers are based on the optical technology, but in a quite different way than optic readers. The reader unlike conventional fingerprint recognition methods does not require a direct contact between the sensor and the skin surface. The light reflected by the finger is captured by a CMOS sensor which generates the finger image. It is similar to a primitive photographic technique. Some typical contactless sensors are shown in Fig. 2.8, including the characterization of the principle.

2.2.3 Capacitive Technology

A capacitive sensor consists of a two-dimensional array of micro-capacitor plates embedded in a chip [85], see Fig. 2.9. The finger skin works as the other side of each micro-capacitor plate. In this way, variations in electrical charge will appear due to distance variations from a ridge in the fingerprint to the sensor and from a valley in the fingerprint to the sensor. These small capacitance differences are then used to acquire a fingerprint image.

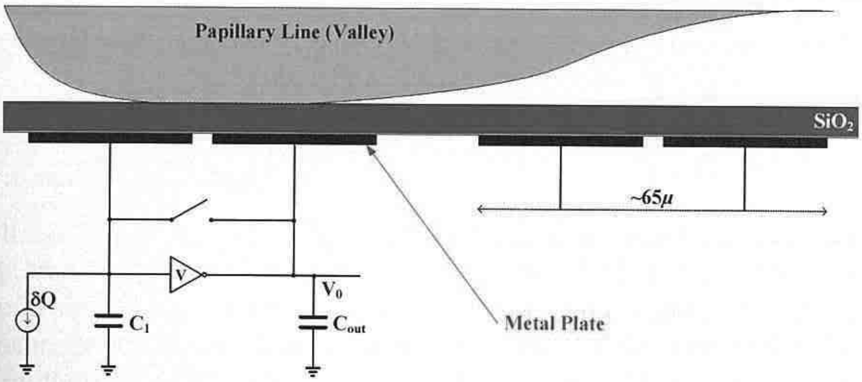


Fig. 2.9: Capacitive technology of fingerprint scanning [Dra20].

Even though being widely used nowadays, capacitive sensors do have a number of disadvantages [85]:

- *Small sensor area*: It can be questioned whether or not a small image scan area is enough to accurately identify an individual. The reduction in sensor size does also require more carefully performed enrollments. A poor enrollment may not capture the center of the fingerprint, thus forcing the subsequent identification/verification fingers to be misplaced in the same way. The sensing area can of course be increased; however it results in a higher cost.
- *Electrostatic discharge* (ESD): Electrostatic discharges from the fingertip can generate large electric fields that could severely damage the device.
- *Chemical corrosion*: The silicon chip needs to be protected from chemical substances (e.g. sodium) that are present in fingerprint perspiration. Protecting the surface with a too thick coating will increase the distance between the pixels and the finger too much and make it more difficult to distinguish between a ridge and a valley. Therefore, the coating must be as thin as possible, yet not too thin, or otherwise it will not resist to mechanical abrasion.

Capacitive sensors have been designed to capture the fingerprint via electrical measurements [70]. Capacitive devices incorporate a sensing surface composed of the array of about 100,000 conductive plates with a dielectric surface. When the user places a finger on this surface, the skin constitutes the other side of the array of capacitors. The rate of voltage at a capacitor decreases with the distance between plates, in this case the distance to a ridge (closer) or a valley (farther).

The resistance against electrostatic shock is up to ca 10 kV [Dra25] and the power consumption lies in the range from 10 to 15 mA [Dra25].

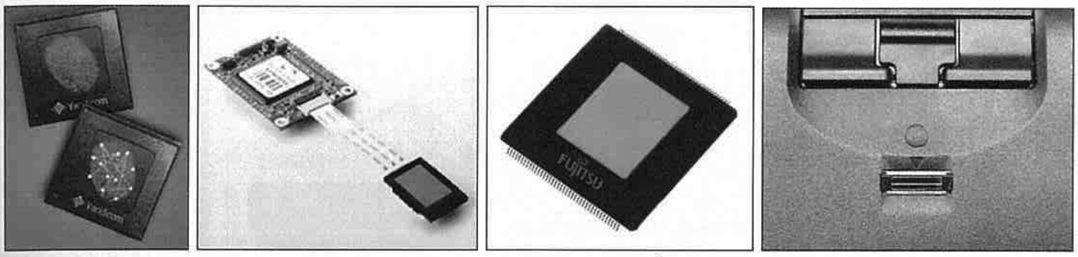


Fig. 2.10: Examples of capacitive scanners (Veridicom 5th Sense; Suprema SFM3050; Fujitsu MBF200; UPEK TouchStrip™ TCS3-TCD4).

2.2.4 Ultrasonic Technology

In an ultrasonic sensor [85] (Fig. 2.11), a transmitter sends acoustic signals toward the fingertip, and a receiver detects the echo signals which bounce from the fingerprint surface. The difference in acoustic impedance of the skin (ridges) and the air (valleys) is used to measure the distance, thus acquiring an image of the fingerprint. The frequency range used by these sensors varies from 20 kHz to several GHz. The top frequencies are used to get the required resolution and to differentiate fingerprints from each other.

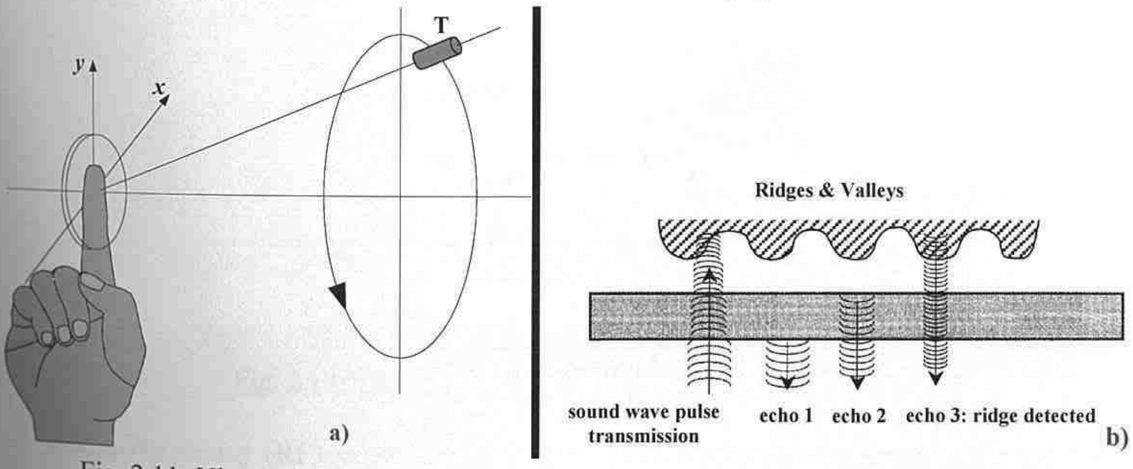


Fig. 2.11: Ultrasonic technology: a) Sensor construction [Dra20]; b) Principle [85].

It has been stated that the improved image quality from ultrasonic sensors results in accuracy rates approximately a factor of 10 better than any other fingerprint sensing technology on the market today [85].

Except of electric fields, ultrasound is one of the few technologies that images the subsurface of the finger skin, thus penetrating dirt, grease, etc., on the sensor surface and finger. The ultrasound technology, though considered perhaps the most accurate of fingerprint technologies, is not yet widely used due to its large size and quite high cost. Moreover, it takes a few seconds to acquire an image.

Nevertheless, there is one strong disadvantage for outdoor use – the technology does not operate properly at low temperatures.

Ultrasonic scanning falls into the contemporary category of fingerprint capture technologies [70]. An ultrasonic beam is scanned across the fingerprint surface much like laser light for optical scanners. In this case, it is the echo signal that is captured at the receiver, which measures range, i.e. ridge depth.

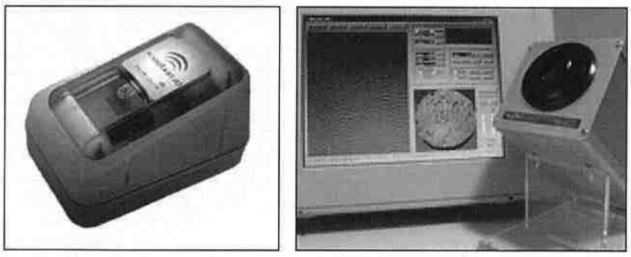


Fig. 2.12: Examples of ultrasonic scanners (UltraScan; Optel).

2.2.5 E-Field Technology

The problems the optical and capacitive sensors have with dry skin conditions, calluses, cuts, etc. is not the case of electric field sensors [85]. These sensors can create a fingerprint image from below the damaged surface layer (Fig. 2.13). The variations of the electric field are measured in the conductive layer, the boundary between the outer layer of damaged skin and the pristine skin.

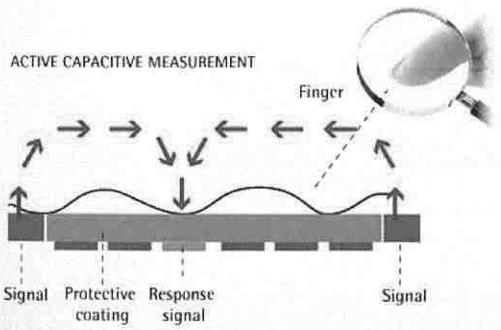


Fig. 2.13: The principle of the e-field technology [109].

Radio-frequency (RF) sensor developed in 1998 creates an electric field from a ring around the sensing area with which an array of pixels can measure variations in the electric field, caused by the ridges and valleys in the finger skin. The e-field is made between the finger and a relevant semiconductor. According to the manufacturer, the variations are detected in the conductive layer of the skin, beneath the skin surface or epidermis. Cells of the scanner technology are working together to receive a quality fingerprint [Dra34].

As a positive aspect of this technology, we can name high-quality images with high resolution. These images are better than images done by capacitive or electro-optical sensors. E-field technology is suitable for most of real applications. These sensors are working correctly even when identifying a person with wet or dry fingers.

The often mentioned disadvantage is its high susceptibility to electrostatic charges of ca 8kV [Dra25]. This sensor could be sensitive on disturbance in his RF modulation but the manufacturers don't provide any further information.

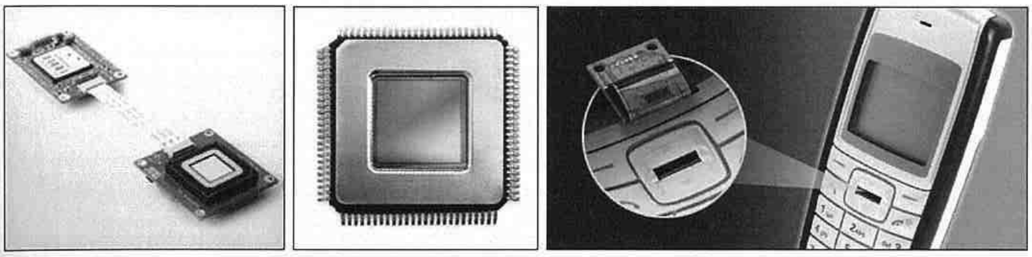


Fig. 2.14: Examples of e-field scanners (Suprema SFM3000; AuthenTec AES 4000; Validity VFS202).

2.2.6 Electro-Optical Technology

This sensor technology consists of four principal layers (Fig. 2.15): an isolation layer, a black coaxial layer, a light-emitting layer (made of polymer material) and a basic layer (permeable for light). When the polymer material is polarized with the proper voltage, it emits light that depends on the potential applied on one side. As the ridges touch the surface, and the valleys not, the potential, and thus also the amount of light, will be different. A photodiode array (embedded in glass) or a CCD/CMOS camera placed under the basic layer receives the light and generates a digital fingerprint pattern.

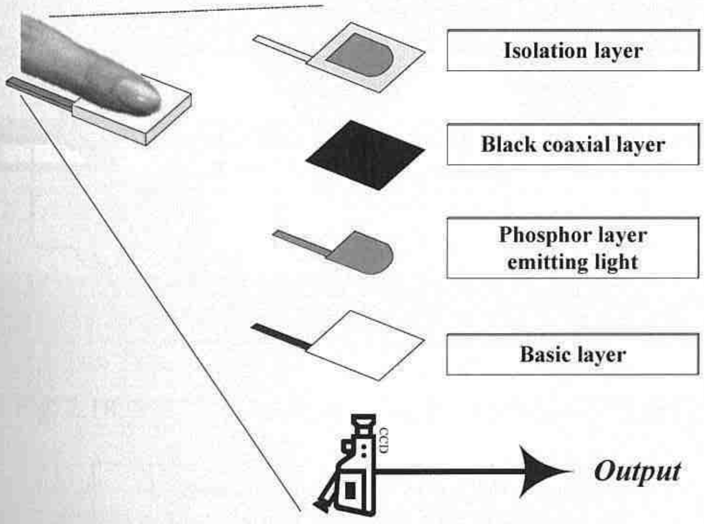


Fig. 2.15: Electro-optical principle with a CCD-camera [Dra20].

Some commercial sensors use a light-emitting polymer material together with ordinary lens and CMOS instead of a photodiode array (Fig. 2.16). Images acquired electro-optically are not comparable in quality with FTIR images [85].

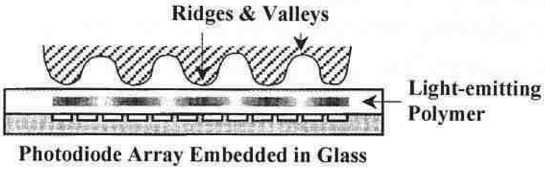


Fig. 2.16: Electro-optical fingerprint sensor principle [85].

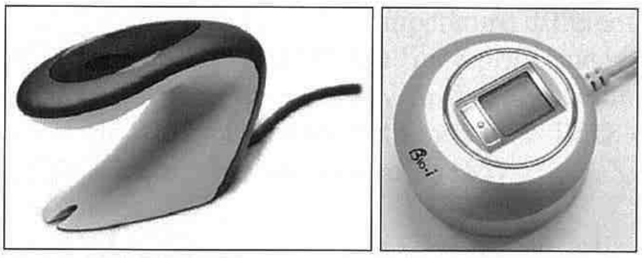


Fig. 2.17: Examples of electro-optical scanners (Ethentica; Testech Bio-i CYTE).

2.2.7 Pressure Sensitive Technology

The sensor surface is made of a non-conductive dielectric material (gel). When pressure is applied by the finger, a small current, dependent on pressure, is generated (this is called a piezoelectric effect) – see Fig. 2.18.

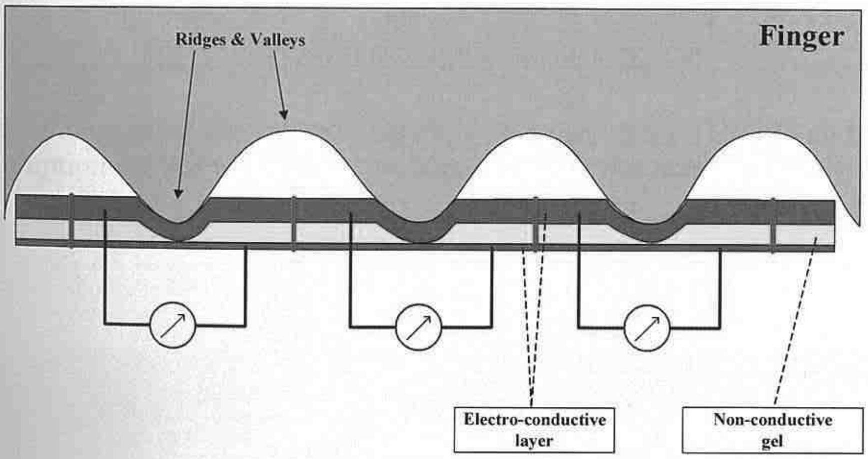


Fig. 2.18: Pressure sensitive technology principle [Dra20].

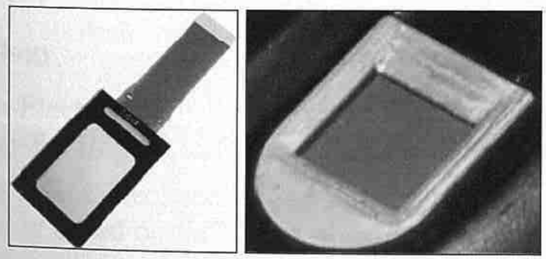


Fig. 2.19: Examples of pressure sensitive scanners (BMF BLP-100; Fidelica FIS-3002).

Valleys and ridges cause different pressure what results in different values of current. One of the disadvantages of this technology is the used material which is often not sensitive enough to detect the differences between ridges and valleys. Additionally, the protective coating blurs the resulting image.

2.2.8 Thermal Technology

Thermal sensors are made of pyro-electric material that generates current based on temperature differentials [85] (Fig. 2.20). The temperature differential between the skin (ridges) and air (in valleys) is used to acquire the fingerprint image. Since thermal equilibrium is reached quickly, it might be necessary to use a sweeping technique when it comes to thermal sensors. Thermal sensors are not sensitive to ESD, nor do they have any problems with a thick (10 to 20 μm) protective coating [85].

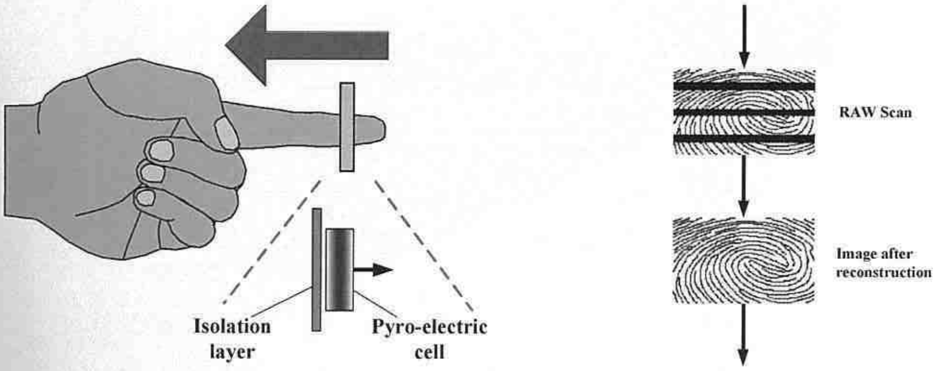


Fig. 2.20: Thermal technology principle [Dra20].

The resistance against electrostatic shock is up to ca 16 kV [Dra25] and the average power consumption for this technology is about 6 mA for one acquirement.

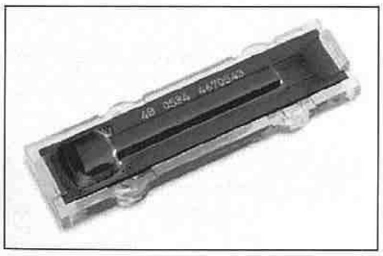


Fig. 2.21: Example of thermal scanner (Atmel® AT77C104B).

2.2.9 MEMS Technology

The MEMS (Micro-Electro-Mechanical Systems) technology is relatively new and the use of this technology for fingerprint sensors dates from the last years [103].

One of the possible MEMS technology subpart is the *tactile measurement* [10][86]. The tactile measurement is based on the use of piezo-resistive micro-beams (cantilevers). There were introduced some improvements to this sensor recently – for details please see [86].

Fig. 2.22 shows a schematic of the tactile sensor. It contains three lines of sensing elements placed besides the electronic parts and bonding pads. The process of fingerprint acquisition with this sensor is presented in Fig. 2.23. First, the user sweeps its finger along the sensor, placed perpendicularly to the direction of the movement. During this step, the ridges and valleys that compose the fingerprint will induce deflections in the different micro-beams of each line of the sensor. The resistance variation of each piezo-resistive gauge is transformed into the voltage variation. A shift register placed on top of each row will switch the signal produced by the micro-beams to a transmission line that feeds the analog amplification chain. After this, the signal is converted to an 8-bit parallel output.

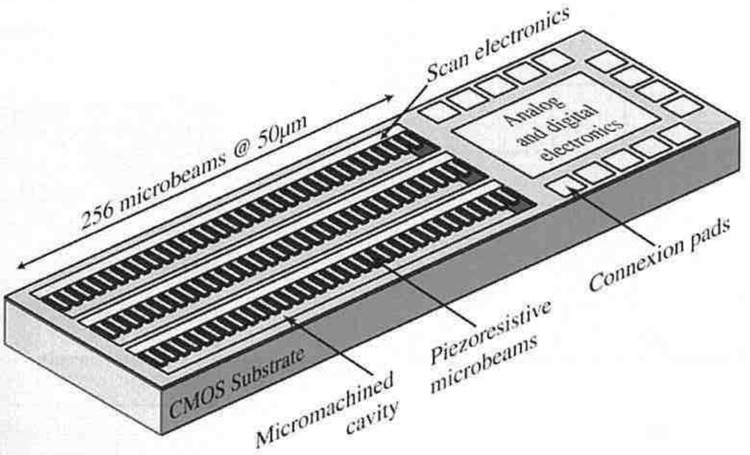


Fig. 2.22: The principle of a tactile fingerprint sensor [10].

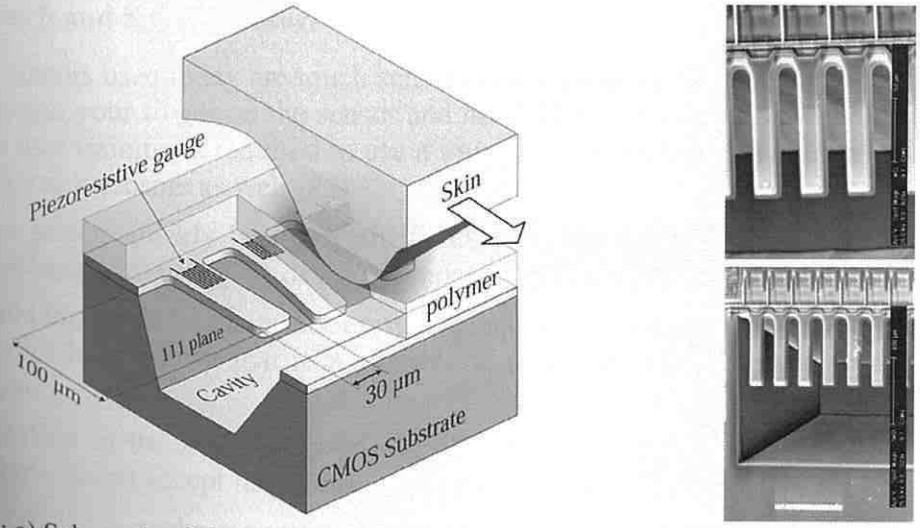
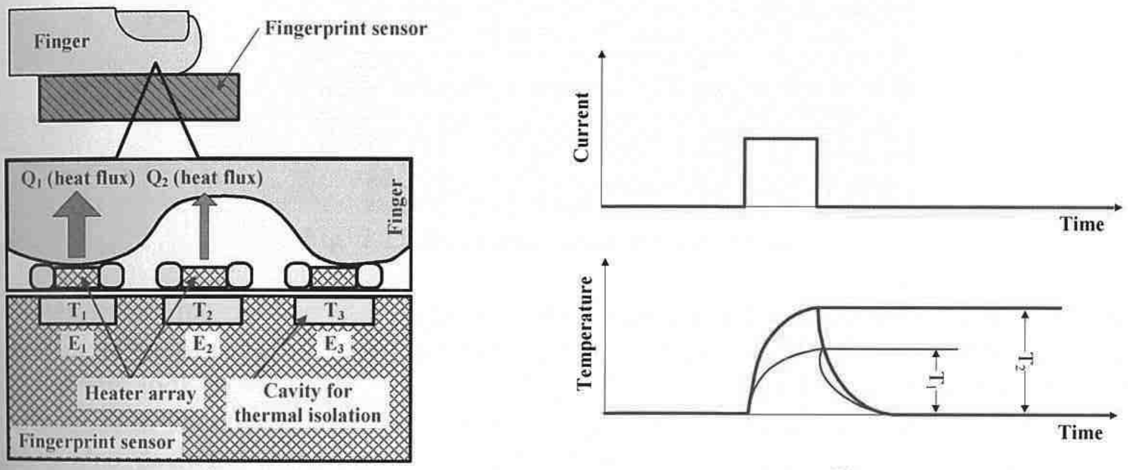


Fig. 2.23: a) Schematic of the tactile measurement of the fingerprint [10] (left); b) Microscopic images of real micro-beams [10] (right).

The structure and working principle of the device using *MEMS arrayed micro-heaters* [24] are schematically shown in Fig. 2.24a. This sensor has an array of micro-heater elements. A cavity is formed under each heater element for enhancing heat insulation between the heater and substrate. When a fingertip is pressed to the device surface, heater element in contact with a ridge of human fingerprint (E_1) shows less temperature rise than that which is facing a recess of fingerprint (E_2), because the finger acts as a heat sink. When a pulsed voltage is applied to each element as shown in Fig. 2.24b, the element E_1 shows less increase in temperature rise than the element E_2 as schematically shown in Fig. 2.24b. The proposed type of sensor has an advantage over the conventional type which has an array of CMOS gates for attachment/detachment sensing and inevitably containing problems such as stray capacitance and charges on a human body.



a) b)

Fig. 2.24: Fingerprint sensor with an arrayed micro-heater [24]: a) Device structure; b) Sensing principle.

2.2.10 Touch and Sweep Sensors

Most sensors used today are touch sensors (area sensors). When using a touch sensor, you simply put your finger on the sensor and hold it for a few seconds without moving it. Very little user training is required to use a touch sensor. However, there are a few drawbacks with touch sensors as well [85]:

- The sensor quickly becomes dirty and must be cleaned. Some users might have problems with using the device, if it does not look clean.
- Problems with latent prints exist. Depending on the type of sensing technique, studies have shown that it is possible to reactivate a latent print on a fingerprint sensor.
- Rotation of the finger may be a problem for recognition. Some matching algorithms do not accept large rotations (e.g. more than 20 degrees) of the finger.
- Necessity to make a compromise between the cost and size of the sensing area. This is especially true for solid-state sensors, where their cost mainly depends on the area of the chip die.

Because of these drawbacks, a new type of sensor was introduced: the sweeping sensor, see Fig. 2.25. Sweeping sensors are as wide as a finger, but only a few pixels high. Therefore, the main advantage of sweeping sensors, especially in silicon sensors, is their reduced cost. The sweeping consists of a vertical movement only. At the end of the swipe or “on-the-fly”, the fingerprint image is reconstructed from all the images earlier acquired.

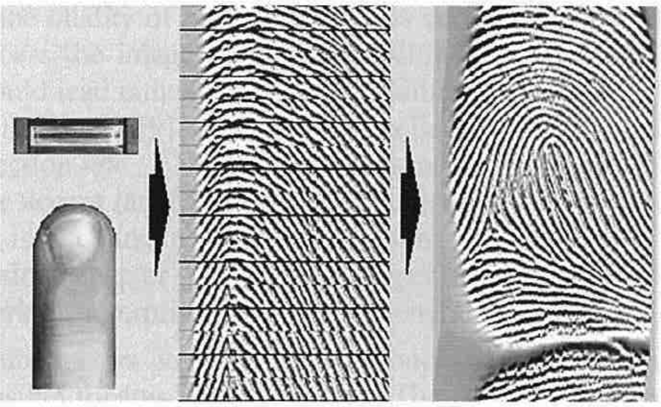


Fig. 2.25: Sweeping sensor principle [109].

The sweeping method was originally introduced in conjunction with thermal sensors, but it is nowadays used in many different types of sensors. Unlike touch sensors, sweeping sensors look clean since each user’s finger “cleans” the sensor during sweeping. No problem with latent prints exists with sweeping sensors, and in most cases, the finger rotation also does not represent a problem. However, sweeping sensors still have some drawbacks, such as [85]:

- Learning time. It takes a number of tries, before a user gets used to sweeping properly (i.e. without sharp speed changes or discontinuity).
- The interface must be able to capture a sufficient number of fingerprint slices to follow the finger sweep speed.
- Reconstructing of the fingerprint image from slices is a time-consuming process which usually produces errors.

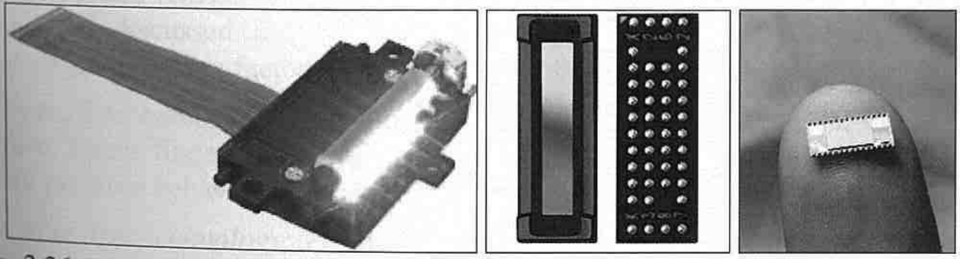


Fig. 2.26: Examples of sweep scanners (Digital Persona Firefly; AuthenTec AES2810; Idex SmartFinger® IX 10-4).

2.3 Factors Influencing Fingerprint Acquirement

The fingerprint acquirement process is crucial for the subsequent processing of the fingerprint image. If the quality of acquired image is very poor, the likelihood that it will be impossible to process the image so that it is followed by a correct decision is quite high; this situation could lead either to increasing failure to acquire (FTA) / failure to enroll (FTE) rates [Dra01][Dra31][9] or to a wrong decision, i.e. false rejection of a genuine user (FRR – false rejection rate / FNMR – false non-match rate) or false acceptation of an impostor (FAR – false accept rate / FMR – false match rate) – for more details, see please [Dra01][Dra31][9]. It is of course possible to determine the quality of a fingerprint image before further processing (chapter 3), but an improper acquirement technology or strong influencing factors during fingerprint acquirement generally results in low quality images.

The following subchapters introduce two groups of possible influencing factors which may be responsible for low quality images. The first group relates to a set of factors coming from the surrounding environment, including the sensor and the user himself. The second group includes skin diseases of palms and fingertips which could make successful enrollment [Dra01][Dra31][9] and subsequent verification or identification [Dra01][Dra31][9] totally impossible.

2.3.1 Surrounding Environment

The environment which surrounds the fingerprint acquirement process plays an important role in the image quality. In fact, this is common for many biometric technologies, e.g. the illumination and background are very strong influencing factors in the face recognition technology. If the intensity of illumination and/or the direction of light always changes, then it is nearly impossible to set adequate parameters for the high quality face acquirement.

In this subchapter, certain known influencing factors for the fingerprint acquirement process coming from the surrounding environment will be introduced. First of all, specific influencing factors related to respective fingerprint acquirement technology will be presented and then discussed. In general, the fingerprint acquirement technologies may have the following influencing factors (for description of these factors – see please below):

- *Optical technology*: surrounding light, electro-magnetic radiation, dirt on the surface, latent fingerprints, dry or moist fingers, physical damage, vibrations, non-cooperative behavior of the user and pressure.
- *Capacitive technology*: electro-magnetic radiation, dirt on the surface, latent fingerprints, dry or moist fingers, physical damage, vibrations, non-cooperative behavior of the user and pressure.
- *Ultrasound technology*: electro-magnetic radiation, vibrations and non-cooperative behavior of the user.
- *E-field technology*: electro-magnetic radiation, dirt on the surface, dry or moist fingers, physical damage, vibrations and non-cooperative behavior of the user.
- *Electro-optical technology*: surrounding light, electro-magnetic radiation, dirt on the surface, physical damage, vibrations, non-cooperative behavior and pressure.

- *Pressure sensitive technology*: electro-magnetic radiation, dirt on the surface, physical damage, vibrations, non-cooperative behavior of the user and pressure.
- *Thermal technology*: electro-magnetic radiation, physical damage, non-cooperative behavior of the user, temperature and pressure.
- *MEMS technology*: electro-magnetic radiation, dirt on the surface, dry or moist fingers, physical damage, vibrations, non-cooperative behavior of the user and pressure.
- *Sweep technology* (in relation to all above mentioned technologies): electro-magnetic radiation, physical damage, non-cooperative behavior of the user and pressure. This is a special case, because only some of the above mentioned technologies are available in a sweep construction, namely thermal, capacitive, MEMS and optical technologies. Such sensor has a perfect property – it is self-cleaning, i.e. no latent fingerprint is left on the surface and a potentially dirty surface is cleaned after the following scan (this could be considered as unhygienic, but the same problem exists with standard sensors).

The above mentioned influencing factors could be summarized as follows: *surrounding light*, *electro-magnetic radiation*, *dirt on the surface*, *latent fingerprints*, *dry or moist fingers*, *physical damage*, *vibrations*, *non-cooperative behavior of the user*, *temperature* and *pressure*.

Surrounding light may influence the scanning process of the optical and electro-optical technology, because it uses a light sensing unit, which is sensitive to the light from the surrounding environment. The sensor area of common optical sensors is similar to an average finger size and therefore the area around the finger, where the light from the environment could come to the sensor camera, is quite small. Nevertheless, if we use the fingerprint scanners which are intended for scanning of more than one finger (e.g. for visa applicants), for rolled fingerprints (dactyloscopic devices) or contactless sensors, the influence of the light from the surrounding environment can be very strong, as the areas, through which such light could enter in the camera, are much bigger as in the previously mentioned case. The influence of the light from the surrounding environment on selected sensors has been tested [Dra34].

Electro-magnetic radiation is a problematic factor for all devices, since not only the sensor itself (its surface) could be influenced, but all other electronic components and cables might be influenced too. It depends on the strength of respective electro-magnetic field, how much all the parts of a scanning device are influenced. For example, it has been shown in [Dra34] that external magnetic field could lead to the situation that the sensor is unable to focus properly and the resulting image is therefore blurred. The cables which connect the device with a main unit (e.g. a computer or a switchboard) are also endangered, especially if there is another wire nearby.

Dirt on the surface is one of the most common factors. It doesn't include only dust or bigger particles but also latent fingerprints which are discussed in the next paragraph. In general, the dirt involves ink, dust, metallic dust, clay, excrements (e.g. at outdoor installation under a tree where birds are often sitting), fat, various liquids and many others. Some dirt can be unintentional but other may be caused by non-satisfied or non-cooperative users, what is hard to prevent. Conductive materials and liquids are very problematic for capacitive and e-field sensor technologies and bigger particles are problematic for almost all technologies, except thermal and sweep technologies. The least affected seems to be the ultrasound technology. Some tests with specific types of dirt (earth dust, metallic dust, wooden dust, fine sand, oil, hairs and ink) are described in [Dra34] (Fig. 2.27).

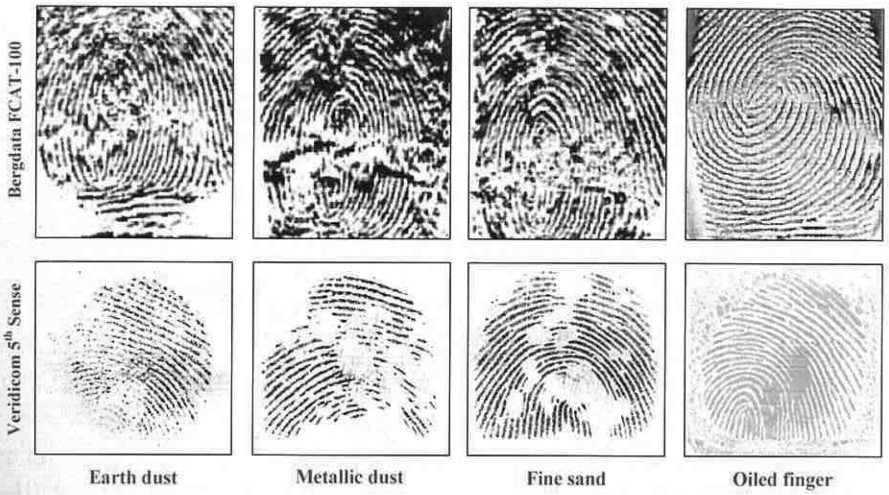


Fig. 2.27: Fingerprints acquired under the influence of various factors [Dra34].

Latent fingerprints [Dra21][Dra31] are a security hazard for a biometric system. At almost all technologies (except sweep sensors), fingers placed or rolled on the scanner surface leave latent fingerprints there; this is in particular the case of users with moist fingers. Such latent fingerprint could be made visible and copied, i.e. an imitation or an artificial finger could be produced and used for deceiving the sensor (see please chapter 4). In fact, it is possible to reactivate a fingerprint by optical, capacitive or e-field technologies. The other technologies are not prone to the reactivation of latent fingerprints.

Dry or *moist fingers* are very typical cases of influencing factors at nearly all fingerprint recognition systems. For example, the measurements of skin resistance (see the experiments in chapter 4 or [Dra06]) have shown that the values of resistance range from several kΩ to MΩ, what means that there is very close connection with the humidity of the skin surface; low values of skin resistance correspond to moist fingers, and vice versa, high values of skin resistance correspond to dry fingers. Technologies sensitive to moist or dry fingers are: optical, capacitive, e-field and partly thermal. Electro-optical, pressure sensitive and especially ultrasound technologies are less influenced. Any of the extremities – excessive dryness or wetness – leads either to indistinct papillary lines (the grayscales of ridges and valleys are quite similar) or overlapping of ridges (become thick and dark).

Physical damage is an extreme case when certain users do not accept biometric technology and do not want to use it. They feel that the best possibility how to take a biometric system out of service is to destroy or damage an input unit – the scanner. It is very difficult to prevent such damaging, because none of these technologies is resistant enough against hard attacks. However, two of them are available in a special robust vandal-resistant design – namely optical and ultrasound technologies, whereas the ultrasound technology is the most resistive against attacks on the functionality.

Vibrations are not harmful for any of the sensor technologies, only some internal components or mechanical parts could be unfastened, what could lead to the situation that the device is out of order. Nevertheless, there is another factor, which is linked to the vibrations – if the device vibrates, then the finger position slightly changes on the scanner surface and the resulting fingerprint image can be blurred. It is therefore not recommendable to use a fingerprint recognition technology in a strongly vibrating environment.

Non-cooperative behavior of the user is typical for those cases when a user tries to play with the system or to find the limits of its functionality (it is not a very dangerous situation) or when a user hates the biometric technology and therefore tries to confuse the device, e.g. by placing his finger wrongly on the scanner surface so that he is not recognized, or when he causes some irreversible changes at the device (this latter behavior leads often to a damaged scanner). These cases also include the use of wrong fingers (which are not enrolled), placement of a correct finger on the sensor under a totally wrong angle (when compared with an enrolled template) or making the finger dirty.

Temperature is a factor which normally has no influence on the scanning process, i.e. small changes of temperature have really zero impact on the fingerprint quality. Only one technology is sensitive to temperature changes – it is the thermal technology. However, if we consider an outdoor usage in winter (e.g. at the Arctic Circle) where the temperatures fall under -40°C or in summer (e.g. in a desert) where the temperatures can raise above +80°C, we have to think about the ability of the technology, i.e. whether some special (automotive or military) components should be used etc. It is known that the ultrasound technology doesn't operate properly at very low temperatures.

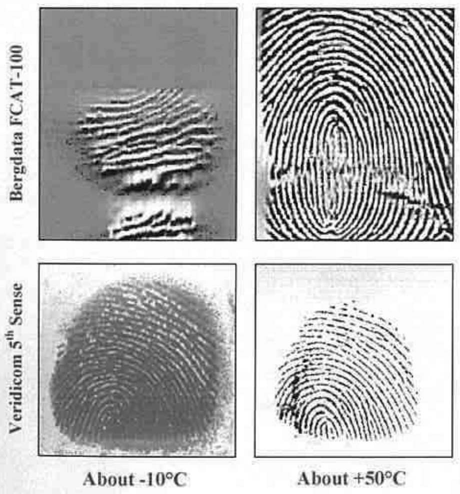


Fig. 2.28: Influence of temperature changes to the fingerprint scanning [Dra34].

The last factor is the *pressure*. The pressure change might be used for the detection of liveness (see chapter 4), however, the pressure change during the scanning process is not good, because the papillary lines can have different thickness in comparison with an enrolled template (the minutiae could be wrong) and any movement during the scanning process can lead to blurred parts in the fingerprint image. Very strong pressure exerted on the finger can cause damage on the scanning device.

2.4 Skin Diseases

Skin diseases represent a very important, but often neglected factor of the fingerprint acquirement. It is impossible to say in general how many people suffer from skin diseases, because there are so many various skin diseases – please refer e.g. to [23][65][121][123][50], but we must admit that such diseases are present in our society. When discussing whether the fingerprint recognition technology is a perfect solution capable to resolve all our security problems, we should always keep in mind those potential users who suffer from some skin disease. What should we do for example with a user who is a respectable person wanting to get a visa to the USA, but who is also suffering from some skin disease which attacked his/her fingertips and is therefore unable to pass successfully through the process of fingerprint acquirement? Should his/her visa application be refused only because his fingers are not acceptable for the required process? Nearly the same question could be put in other fields – e.g. industry. If some industrial company would like to implement an access control system based on fingerprint recognition and some potential users are hard-working operators with their papillary lines on fingertips damaged, abraded or affected by a skin disease (what is quite frequent situation for manual workers), what should we do with them?

The fingerprint recognition systems are usually used only for adults. There is almost no information from appropriate tests with children. Although we know that papillary lines emerge on infant's fingers already in the mother's uterus [112], i.e. we might be able to recognize the fingerprints of infants, the common fingerprint recognition systems are suitable for adults only (due to the area and resolution of fingerprint sensors, etc.).

It should not be forgotten that a skin disease in early childhood could have an influence on the skin in adult years (see an example of incontinentia pigmenti [5] on a small child hand, Fig. 2.29), i.e. there could be some problems with fingerprint acquirement caused by such skin disease in a young age.

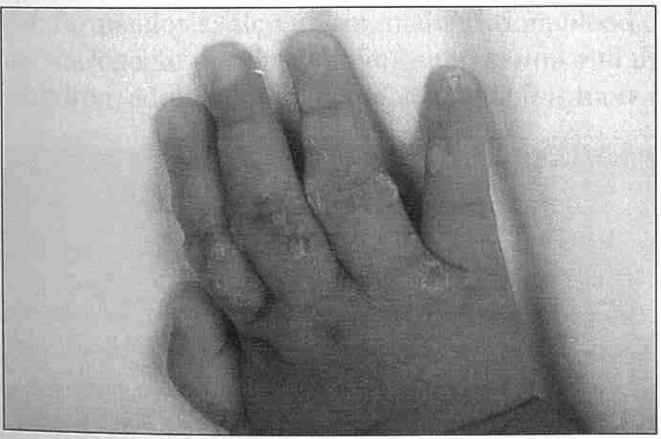


Fig. 2.29: Incontinentia pigmenti on a child hand [5].

In the following text, several skin diseases are introduced, which attack hand palms and fingertips. These are divided into three subcategories: diseases affecting a) only the *papillary line structure*, b) only the *skin color* and c) both *papillary line structure and skin color*.

The subcategory of skin diseases affecting only the skin color are the least dangerous for the quality of the fingerprint image. In fact, only one fingerprint technology can be considered as sensitive to such diseases – the optical technology, but if FTIR-based optical sensors are used, the change of skin color may have no influence on the quality of the resulting images.

The case of the other two subcategories is different. If the structure of papillary lines has changed, it is often impossible to recognize the original curvatures of papillary lines and therefore it is impossible to decide whether the claimed identity is the user's identity. Unfortunately, there are many such skin diseases which attack papillary line structure. Nearly all sensor technologies, namely optical, capacitive, e-field, electro-optical, pressure sensitive and thermal are exposed to such risk. Only one sensor technology is missing here – the ultrasound technology. This technology has an advantage: the ultrasound waves can penetrate under the upper skin layer to the curvatures in epidermis forming the papillary lines structures and therefore it might be possible to reconstruct the real fingerprint image, but only if the disease has not attacked this underlying structure. If yes, there is no chance to get an original papillary lines structure.

The situation after successful recovery of a potential user from such skin diseases is, however, very important for the possible further use of fingerprint recognition devices. If the disease has attacked and destroyed the structure of papillary lines in the epidermis layer of the skin, the papillary lines will not grow in the same form as before (if at all) and therefore such user could be restricted in his/her future life by being excluded from the use of fingerprint recognition systems, though his fingers don't have any symptoms of a skin disease any more.

2.4.1 Change of Papillary Line Structure

A *furuncle* [40] is an acute, round, tender, circumscribed perifollicular staphylococcal abscess that generally ends in central suppuration. Certain systematic disorders may predispose a person to the furunculosis: alcoholism, malnutrition, blood dyscrasias, disorders of neutrophil function, iatrogenic or other immunosuppression and diabetes (Fig. 2.30a). Age of onset [123]: children, adolescents and young adults; it is more common in boys.

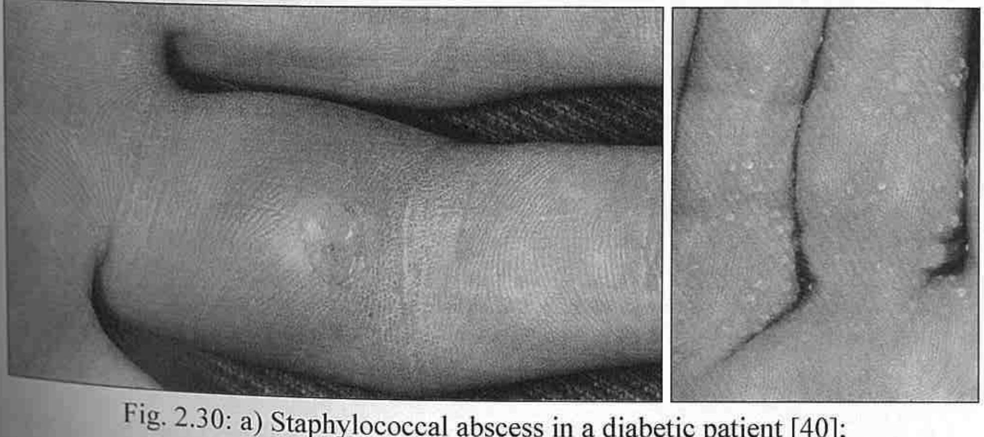


Fig. 2.30: a) Staphylococcal abscess in a diabetic patient [40];
b) "Music box" spine keratoderma [40].

Spiny keratoderma [40] of the palms, known as "music box spines" (Fig. 2.30b) is a distinct variant of the punctate keratosis.

Pitted keratolysis [40][123] is a bacterial infection of the plantar stratum corneum (Fig. 2.31a, Fig. 2.31b). The thick, weight-bearing portions of soles (seldom palms) become confluent, forming furrows. Men with very sweaty feet/palms carrying rubber boots or gloves in hot, humid conditions are most susceptible. No discomfort is produced, though the lesions are often malodorous.

Keratolysis exfoliativa [23] or recurrent focal palmar peeling is a common, chronic, asymptomatic, non-inflammatory, bilateral peeling of the palms of the hands and occasionally soles of the feet (Fig. 2.31c). The eruption is most common during the summer months and is often associated with sweaty palms and soles. Scaling starts simultaneously from several points on the palms or soles with 2 or 3 mm of round scales that appear to have originated from a ruptured vesicle, however, these vesicles are never seen. The scaling continues to peel and extend peripherally, forming larger, roughly circular areas that resemble ringworm, whereas the central area becomes slightly red and tender.

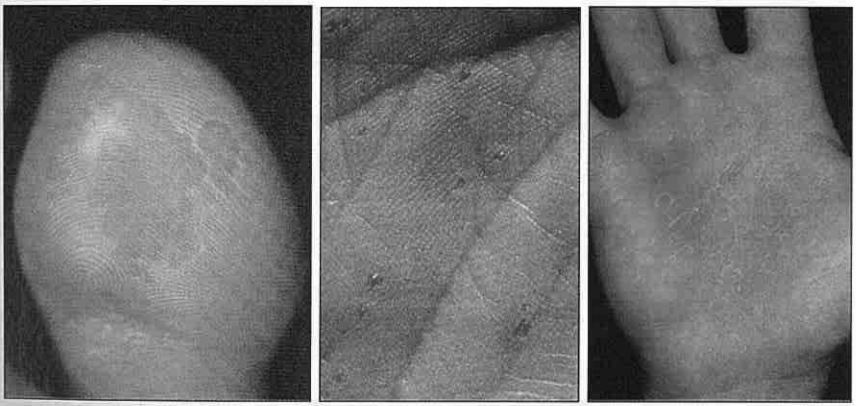


Fig. 2.31: a) Pitted keratolysis [40]; b) Palmar pits [123]; c) Keratolysis exfoliativa [23].

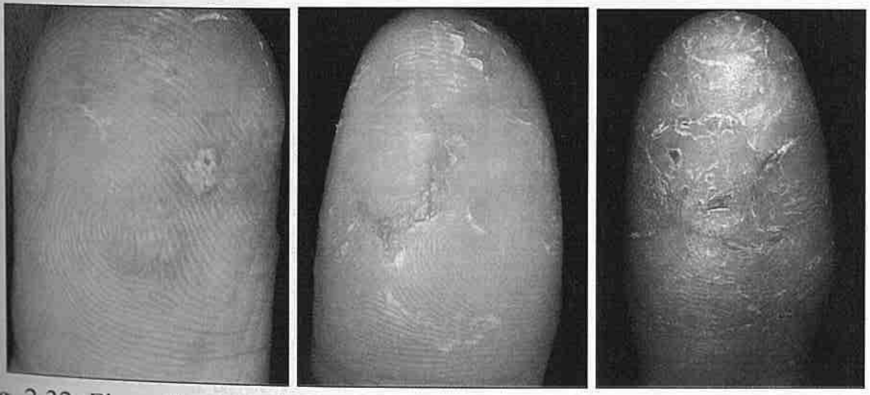


Fig. 2.32: Fingertip eczema [23]: a) An early stage; b) A more advanced stage; c) Full inflammation.

Fingertip eczema [23] is a very dry, chronic form of eczema of the palmar surface of fingertips; it may be the result of an allergic reaction or may occur in children and adults as an isolated phenomenon of unknown cause. One finger or several fingers may be involved. Initially, the skin may be moist and then may become dry, cracked and scaly (see Figures 2.32 and 2.33). The skin peels from the fingertips distally, exposing a very dry, red, cracked, fissured, tender, or painful surface without skin lines. Fingertip eczema may last for months or years and is resistant to treatment.

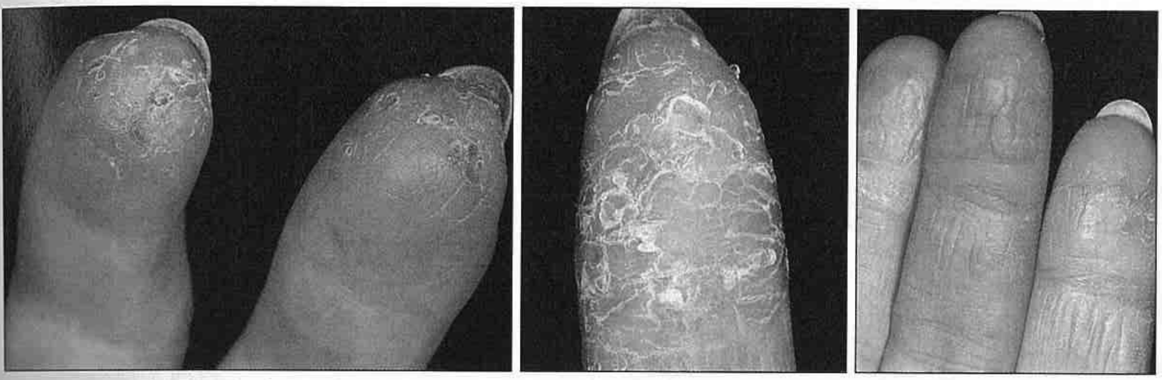


Fig. 2.33: Fingertip eczema [23]: a) Asteatotic eczema; b) Chronic eczema; c) Another form of chronic eczema.

Acanthosis nigricans associated with *malignancy* [40][123] – the "malignant" type of acanthosis nigricans may either precede (18%), accompany (60%), or follow (22%) the onset of the internal cancer. *Tripe palms* [40] (*acanthosis palmaris*) are a type of acanthosis and are characterized by thickened, velvety palms with pronounced dermatoglyphics (Fig. 2.34a). In 40% of these cases, tripe palms are the presenting sign of an undiagnosed malignancy.

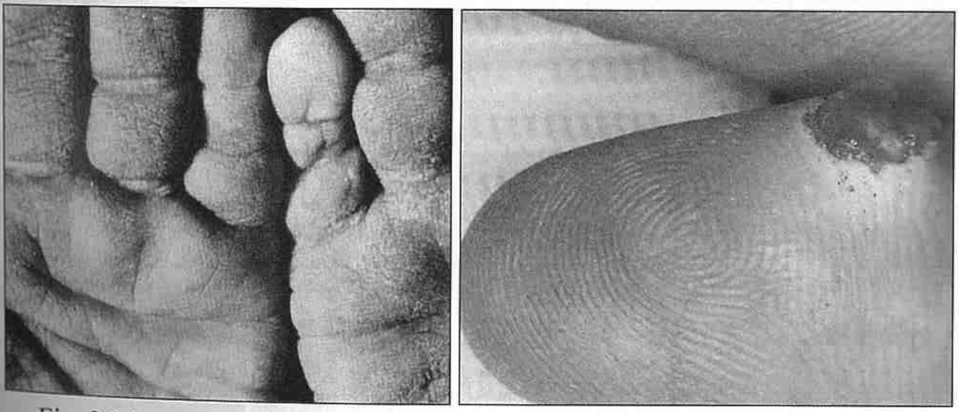


Fig. 2.34: a) Tripe palms [40]; b) Side view of a pyogenic granuloma [23].

Pyogenic granuloma (*lobular capillary hemangioma*) [23] is a benign acquired vascular lesion of the skin and mucous membranes that is common in children and young adults (Fig. 2.34b). It often appears as response to an injury or hormonal factors. Lesions are small (< 1 cm), rapidly growing, yellow-to-bright red, dome-shaped, fragile protrusions that have a glistening, moist-to-scaly surface. They are most commonly seen on the head and neck region and on the extremities, especially the fingers.

Verruca vulgaris [40] – common warts are a significant cause of concern and frustration of certain patients (Fig. 2.35a). Common warts occur largely between the ages of 5 and 20 and only 15% occur after the age of 35. Frequent immersion of hands in water is a risk factor for common warts. Meat handlers (butchers), fish handlers, and other abattoir workers have a high incidence of common warts of the hands. The prevalence reaches 50% in those persons with the direct contact with meat.

Pityriasis rubra pilaris (PRP) [23] is a rare, chronic disease of unknown etiology with a unique combination of features. PRP often has a devastating impact on the lives of patients. PRP can occur at any age, but classic adult PRP begins insidiously, usually in the fifth or sixth decade of life, with a small, indolent, red scaling plaque on the face or upper body. The plaque slowly enlarges over days and weeks, the palms and soles begin to thicken, and bright red-orange follicular papules appear on the dorsal aspects of the proximal phalanges, elbows, knees, and trunk as the disease evolves and progresses into a grotesque generalized eruption (Fig. 2.35b).

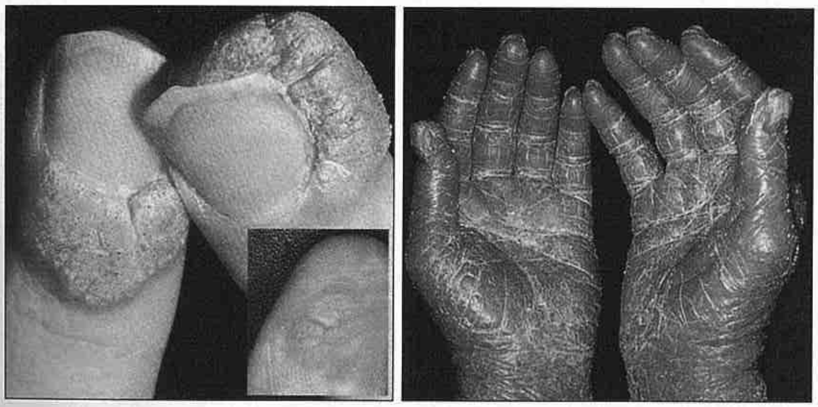


Fig. 2.35: a) Verruca vulgaris [123][40]; b) Pityriasis rubra pilaris [23].

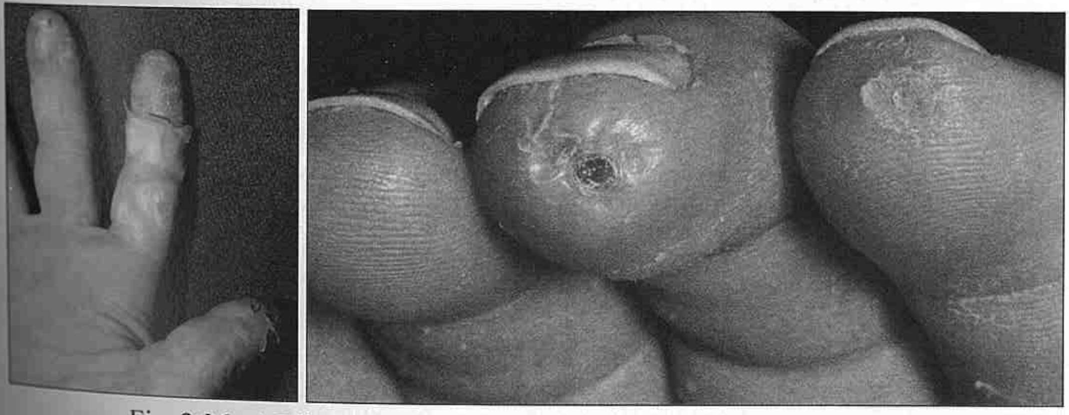


Fig. 2.36: a) Blistering distal dactylitis [121]; b) Scleroderma [123].

Cellulitis [121] is manifested by tender, warm, erythematous plaques with ill-defined borders. Occasionally, linear red macules proximal to the large plaque are seen too. Cellulitis of the fingertips (Fig. 2.36a) often in infants is called *blistering dactylitis* [121] and several fingers may be involved.

Scleroderma [123] is a multisystem disorder characterized by inflammatory, vascular, and sclerotic changes of the skin and various internal organs, especially the lungs, heart, and gastro-tract (Fig. 2.36b).

2.4.2 Change of Skin Color

Hand-Foot-and-Mouth disease (HFMD) [40] is usually a mild illness. It primarily affects children from 2 to 10, but exposed adults may also develop the disease. In 90% of cases oral lesions develop, lesions on the hands and feet are asymptomatic red papules that quickly become small, gray, 3 to 7 mm vesicles surrounded by a red halo. They are often oval, linear, or crescentic and run parallel to the skin (papillary) lines on the fingers and toes (Fig. 2.37a).

Hyperlinear palmar creases [23] (Fig. 2.37b) is very typical for atopic patients. This accentuation may be present in infancy and become more prominent as age and severity of skin inflammation increase. The changes may be initiated by rubbing or scratching. Patients with accentuated skin creases seem to have more extensive inflammation on the body and experience a longer course of disease.

Xanthomas [123] are yellow-brown, pinkish or orange macules, papules, plaques, nodules or infiltrations in tendons. A special art attacking hands is *normolipemic plane xanthoma* [123] (Fig. 2.37c), which consists of diffuse orange-yellow pigmentation and slight elevations of the skin. There is a recognizable border. These lesions can be idiopathic or secondary to leukemia.

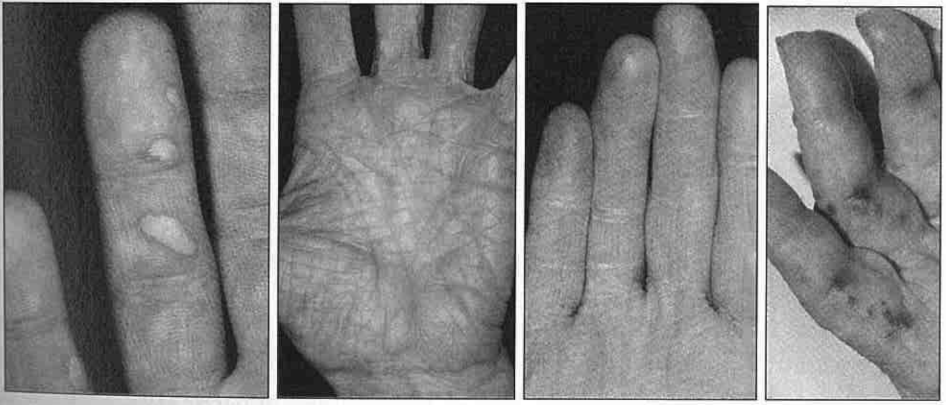


Fig. 2.37: a) Hand-foot-and-mouth disease [40]; b) Hyperlinear palmar creases [23]; c) Plane xanthoma [123]; d) Infective endocarditis [123].

Infective endocarditis, *sepsis* and *septic shock* [123] (Fig. 2.37d) are very serious systematic infections with high associated morbidity and mortality rates. Clinical findings are often acute in onset and relatively nonspecific in nature. Groups of risk [123] are people at the age of 30 to 40, elderly people with valve sclerosis and patients with intravascular prostheses.

Tinea of the hand [23], known as tinea of the dorsal aspect of the hand (*tinea manuum*) (Fig. 2.38a) has all the features of tinea corporis [23]; tinea of the palm has the same appearance as the dry, diffuse, keratotic form of tinea on the soles. The dry keratotic form may be asymptomatic and the patient may be unaware of the infection, attributing the dry, thick, scaly surface to hard physical labor. The usual pattern of infection is involvement of one foot and two hands or of two feet and one hand. Fingernail infection often accompanies infection of the dorsum of the hand or palm.

Epidermolytic hyperkeratosis [121] (Fig. 2.38b), an autosomal dominant disorder, is characterized by extensive scaling at birth, erythroderma, and recurrent episodes of bullae formation. The blisters represent lysis of the epidermal granular layer, and secondary infection with staphylococcus aureus becomes a major difficulty in the neonatal period and during infancy.

Epidermolysis bullosa [121][123] is a term used to describe a group of inherited skin conditions associated with blister formation after mild trauma (Fig. 2.38c). This condition can be associated with defects of many different proteins present at the junction of the dermis and epidermis or within the epidermis or dermis. Generalized epidermolysis bullosa is shown in Fig. 2.38d.

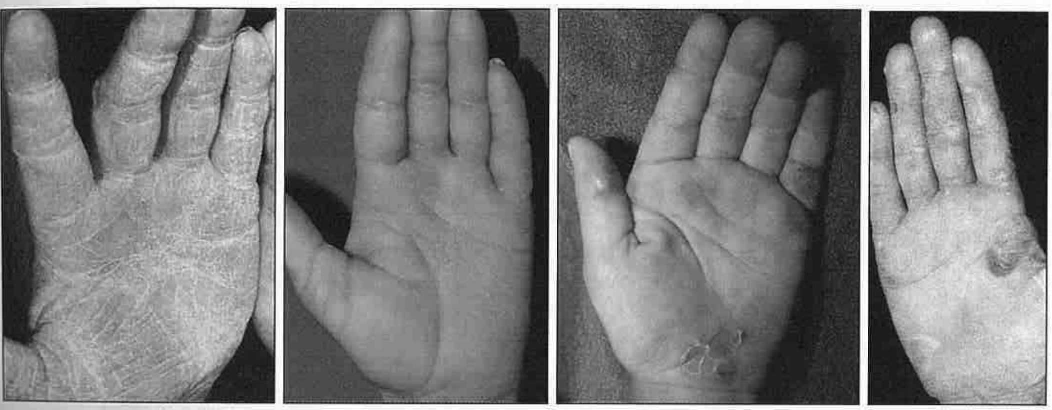


Fig. 2.38: a) Tinea of the hand [23]; b) Epidermolytic hyperkeratosis [121]; c) Epidermolysis bullosa simplex [121]; d) Generalized epidermolysis bullosa [123].

2.4.3 Change of Papillary Line Structure and Skin Color

Hand eczema [23][121] is an inflammation of the hands (Fig. 2.39a, Fig. 2.39b). Hand dermatitis [65] causes discomfort and embarrassment and, because of its location, interferes significantly with normal daily activities. Hand dermatitis is common in industrial occupations: it can threaten job security if inflammation cannot be controlled. *Irritant hand dermatitis* [23][40] (known as *housewive's eczema, dishpan hands* or *detergent hands*) is the most common type of hand inflammation. Some people can withstand long periods of repeated exposure to various chemicals and maintain normal skin (Fig. 2.40a). At the other end of the spectrum, there are those who develop chapping and eczema from simple hand washing (Fig. 2.40b). Patients whose hands are easily irritated may have an atopic diathesis (Fig. 2.39c).

Pompholyx (dyshidrosis) [23] is a distinctive reaction pattern of unknown etiology presenting as symmetric vesicular hand and foot dermatitis (Fig. 2.41a-c). Moderate to severe itching precedes the appearance of vesicles on the palms and sides of the fingers. The palms may be red and wet with perspiration, hence the name dyshidrosis. The vesicles slowly resolve in 3 to 4 weeks and are replaced by 1 to 3 mm rings of scale. Waves of vesiculation may appear indefinitely. *Pustular psoriasis* [102][121] (Fig. 2.41d) of the palms and soles may resemble pompholyx, but the vesicles of psoriasis [102][121] are chronic and the pustules do not evolve and disappear as rapidly as those of pompholyx. The cause of pompholyx is unknown, but there seems to be some relationship to stress.

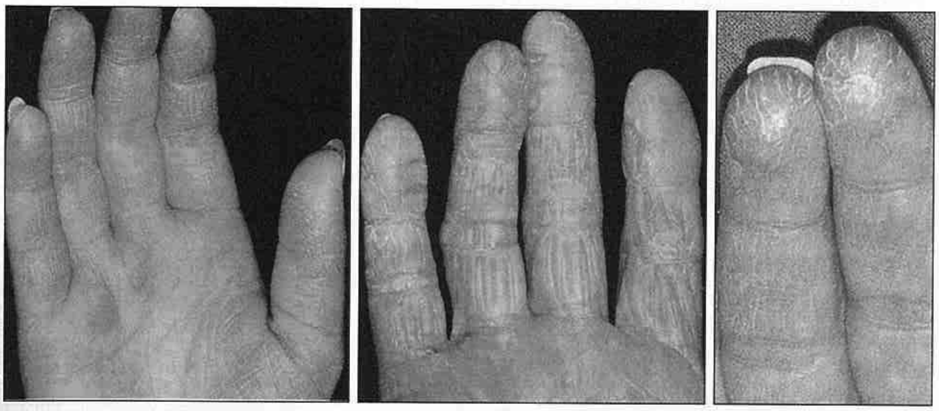


Fig. 2.39: a) Early irritant hand dermatitis with dryness and chapping [23]; b) Subacute and chronic eczematous inflammation with severe drying and splitting of the fingertips [23]; c) Atopic diathesis [65].

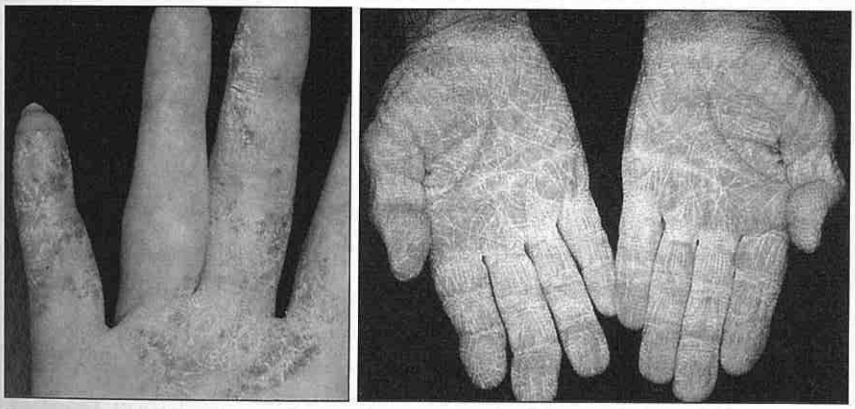


Fig. 2.40: a) Numerous tiny vesicles suddenly appeared on these chronically inflamed fingers [23]; b) Irritant dermatitis from chronic handwashing [40].

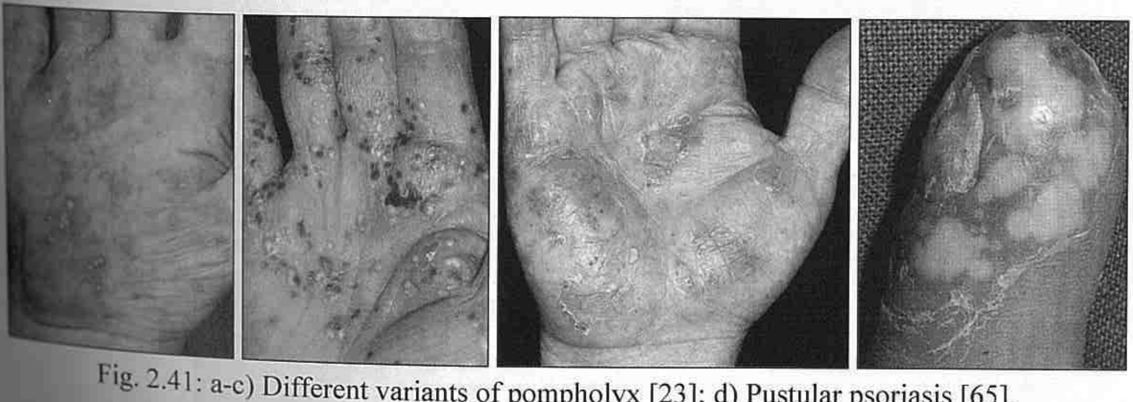


Fig. 2.41: a-c) Different variants of pompholyx [23]; d) Pustular psoriasis [65].

Hereditary hemorrhagic telangiectasia (HHT) [40][123] also known as *Osler-Weber-Rendu disease* [40] is characterized by small tufts of dilated capillaries scattered over the mucous membranes of the skin (Fig. 2.42a). These slightly elevated lesions develop mostly on the lips, tongue, palate, nasal mucosa, ears, palms, fingertips, nailbeds and soles. The telangiectases tend to increase in number in middle age, however, the first appearance on the undersurface of the tongue and floor of the mouth is at puberty.

Purpura fulminans [40] also known as *purpura gangrenosa*, is a severe, rapidly fatal reaction occurring most commonly in children after an infectious illness. The sudden appearance of large ecchymotic areas, especially prominent over the extremities, progressing to acral hemorrhagic skin necrosis is characteristic (Fig. 2.42b).

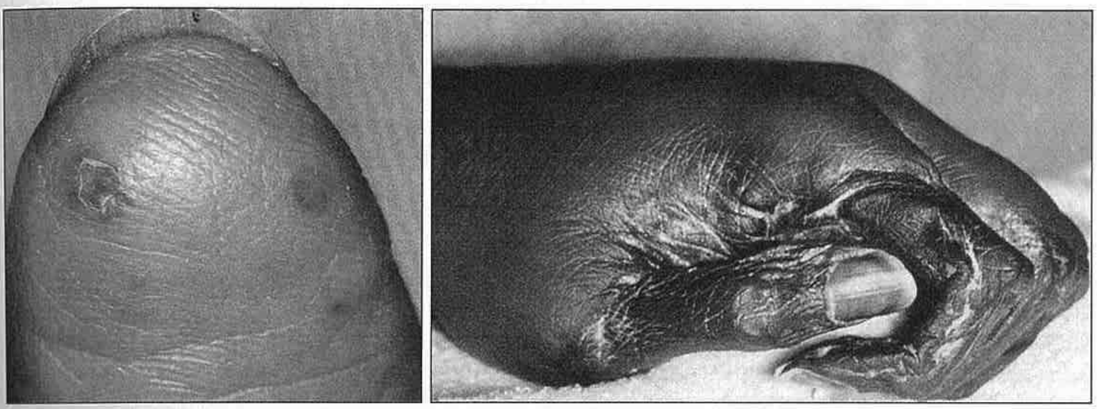


Fig. 2.42: a) Hereditary hemorrhagic telangiectasia [40]; b) Purpura fulminans [40].

Subacute cutaneous lupus erythematosus (SCLE) [23] (Fig. 2.43a) encompasses the clinical spectrum of cutaneous LE between the chronic, destructive discoid LE and the erythema of acute cutaneous LE. The individual lesions of SCLE may last for months. Most patients with SCLE are white females. SCLE may be induced by a variety of drugs, most notably hydrochlorothiazide and calcium channel blockers.

Scarlet fever (*scarlatina*) [23] (Fig. 2.43b) is an endemic, contagious disease produced by a streptococcal, erythrogenic toxin. The infection may originate in the pharynx or skin and is most common in children (aged 1 to 10 years) who lack immunity to the toxin. New waves of scarlet fever are associated with an increase in frequency of streptococcus pyogenes clones.

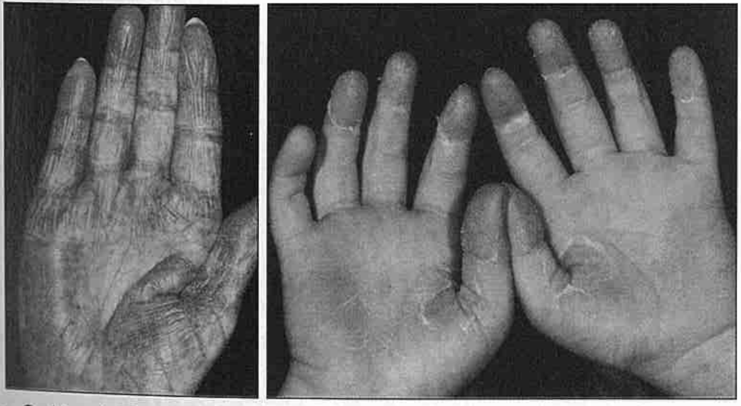


Fig. 2.43: a) Erythema and telangiectasia [23]; b) Scarlet fever [23].

Scabies [121] are pruritic papules on the abdomen, hands, flexural surface of the wrist, elbows, periaxillary skin, genitalia, ankles and feet. Hyperkeratosis and scaling may be particularly prominent on the hands, feet and genitalia. This form of scabies is called *Norwegian scabies* [121] (Fig. 2.44a).

Psoriasis [121][123] (Fig. 2.44b) is thought to be a hereditary disorder that requires an interplay of genetic and environmental factors for full clinical expression. Psoriasis is a clinical diagnosis based on the presence of thick, silvery scales on at least some lesions, the characteristic distribution, nail involvement, and the presence of the isomorphic phenomenon. *Psoriasis vulgaris* [123] is a silvery-white plaque, sharply demarcated, of irregular configuration. On palms and soles the lamellar scales are more adherent than on other parts of the body and only their removal will reveal the reddish inflammatory base.

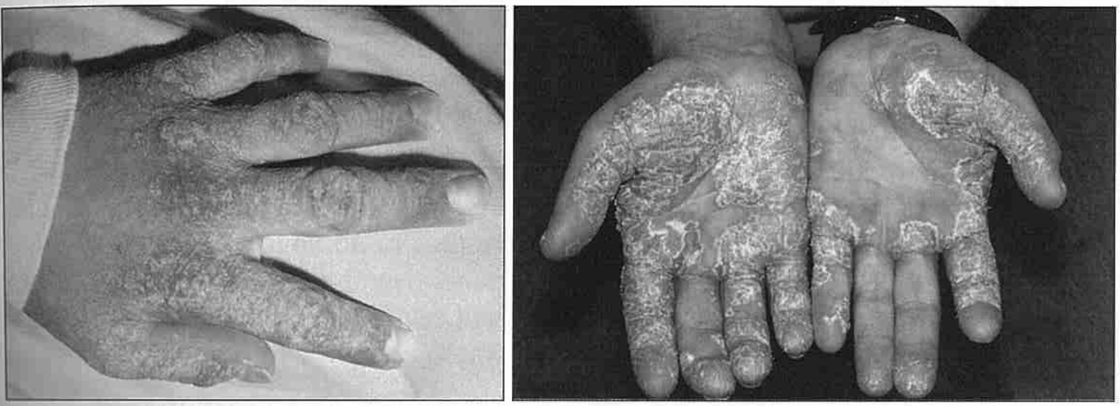


Fig. 2.44: a) Norwegian scabies [121]; b) Psoriasis [121].

Raynaud's disease (*Raynaud's phenomenon* (RP)) [123] is digital ischemia that occurs on exposure to cold and/or as a result of emotional stress (Fig. 2.45a). Afflicted are young adults or women at menopause. RP may occur in persons using vibratory tools, meat cutters, typists and pianists. Precipitating factors are cold, mental stress, certain occupations and smoking.

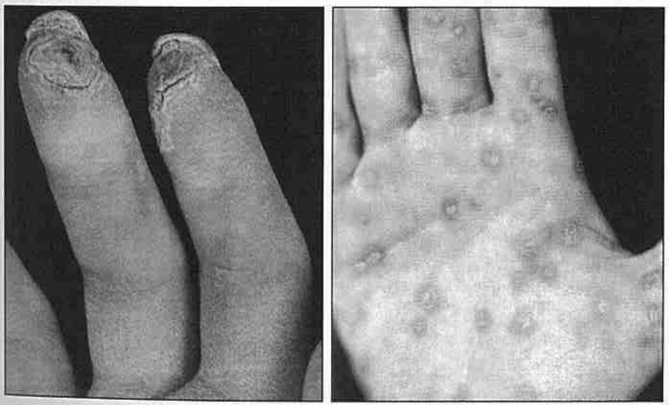


Fig. 2.45: a) Raynauld's phenomenon – acrogangrene [123]; b) Secondary syphilis on palms [123].

Secondary syphilis [123] appears 2 to 6 months after primary infection, 2 to 10 weeks after appearance of the primary chancre, 6 to 8 weeks after healing of chancre. In the Fig. 2.45b is shown the exposure of secondary syphilis – disseminated papulosquamous eruption on palms.

2.4.4 Recapitulation

At the end, we have to discuss the range of influence and importance of the above mentioned skin diseases. It is clear from each subchapter that either the color of the skin or the structure of papillary lines on the fingertip could be influenced. If only the color has changed, some of optical fingerprint scanners might be influenced and so this change is not crucial. On the other hand, the change of skin structure is very significant, because if papillary lines are damaged, it is impossible to find the minutiae and therefore to recognize the person. If we are unable to recognize/enroll a person, then such person cannot use the biometric system based on the fingerprint recognition technology, and therefore the implementing company has a big problem – how to authorize such person, if they don't want to use PINs (*Personal Identification Numbers*) or other authorization methods.

Some of these diseases are only temporary, i.e. after the healing of such disease, the papillary line structure or color is restored and the user is again able to use his/her fingers for the fingerprint recognition in authorization tasks in security systems. However, some diseases leave irrecoverable finger damage restraining a new growth of papillary lines and respective user is then unable to use his/her fingerprints for appropriate recognition tasks in automated fingerprint security systems.

We, as developers and users of biometric systems, need to keep in mind possible problems connected with such users and be prepared for solving them. Each biometric system should include an option for the additional authorization of such users in a different way, because only very small finger damage (e.g. scratch or cut) could lead to the situation when respective user will not be recognized (accepted) by the system, even if he/she has been properly enrolled. One of the possible solutions might be the implementation of a multimodal biometric system [20][13][33].

3. Quality of Fingerprint Images

The quality of an image containing a fingerprint is essential, because the resulting extracted features (biometric template) will strongly depend on the quality of the source signal [97][98][8][53]. There are many factors which can influence the input signal (see chapter 2.3). It is possible to use some methods for quality improvement, although a signal with very poor quality is nearly impossible to enhance [120].

Before we start with the definition of fingerprint image quality, we should briefly introduce the functionality of a biometric system (Fig. 3.1), i.e. its elements important for the following text.

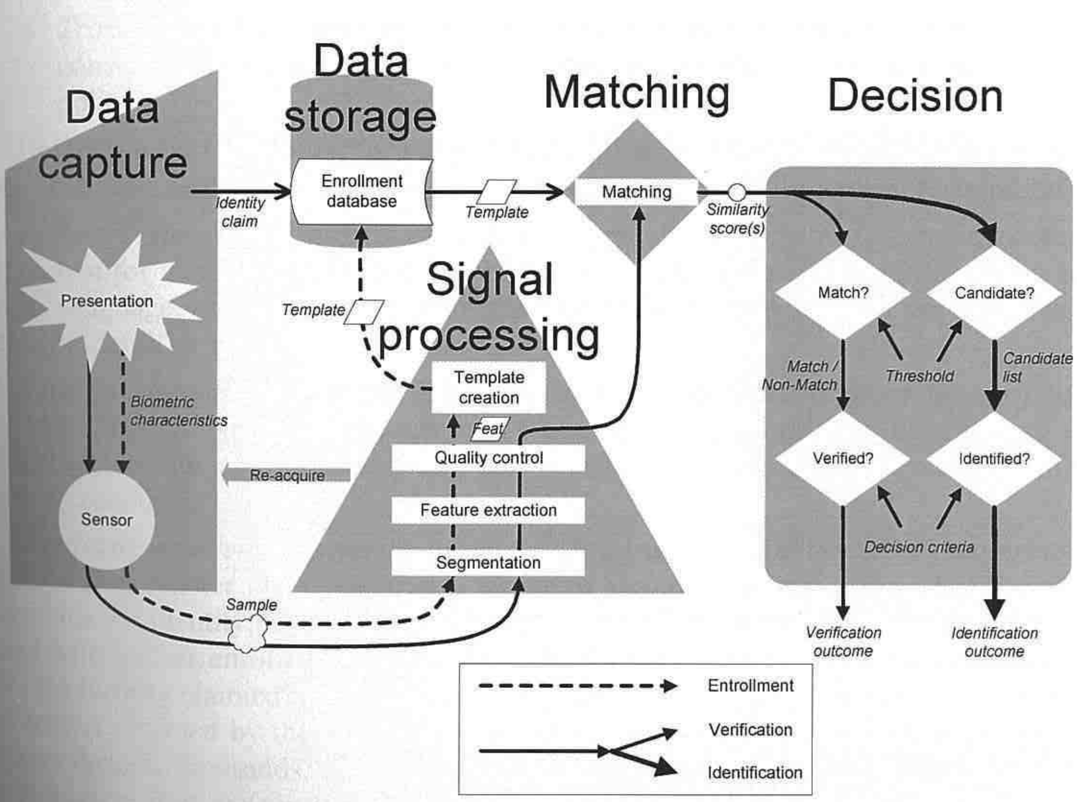


Fig. 3.1: Diagram of general biometric system [30].

A general biometric system consists of the following components [61][Dra14][62][73]; some of them play an important role in the subsequent methods for fingerprint quality estimation:

- *Sample*: A biometric measure provided by the user and captured by the data collection subsystem as an image or signal (e.g. a fingerprint is a sample in our case).
- *Features*: A mathematical representation of the information extracted from the provided sample by the signal processing subsystem that will be used to create enrolment templates or to compare with such templates (e.g. minutiae are features in our case).

- *Template / Model*: A user's stored reference measure based on features extracted from enrolment samples. A reference measure is often a "template" comprising biometric features from an ideal sample provided by the user. More generally, the stored reference will be a "model" representing the potential range of biometric features for that particular user.
- *Matching score*: The degree of similarity between features derived from a provided sample and a stored template, or a measure of how well these features correspond to a user's reference model. A match / non-match decision may be made according to whether this score exceeds a decision threshold.
- *Decision*: The determination of probable validity of a user's claim to his/her identity / non-identity within the system.
- *Transaction*: An attempt by a user to validate a claim of identity or non-identity by consecutively submitting one or more samples, as allowed by the system decision policy.

Before we start to discuss the subject matter of fingerprint recognition, we should define some basic terms and introduce the procedure of common fingerprint recognition.

Authentication is a frequently used term in the field of biometrics, sometimes used as a synonym for verification; in fact, to authenticate a user means, in the information technology language, to let the system know the user's identity regardless of the mode (verification or identification).

Perhaps the most fundamental distinction in the biometrics is between the *verification* and *identification*. Nearly all aspects of the biometrics – performance, benefits and risks of deployment, impact on privacy and cost – differ when passing from one type of this system to another.

Verification systems answer the question, "Am I who I claim to be?" by requiring that a user claims his/her identity before a biometric comparison is performed. After a user claims his/her identity, he or she provides appropriate biometric data which are then compared with his/her enrolled biometric data. Depending on the type of the biometric system, the identity claimed by a user might be a username, a given name, or an ID number; the answer returned by the system is "match" or "non-match". Verification systems can contain dozens, thousands, or millions of biometric records but biometric data provided by respective user are always compared only with his/her own enrolled biometric data. Verification systems are often referred to as 1:1 (one-to-one) biometric systems. The process of providing a username and biometric data is referred to as the authentication.

Identification systems answer the question, "Who am I?" and do not require that a user claims his/her identity before biometric comparisons are performed. The user provides his or her biometric data which are then compared with data from a database of potential users in order to find a match. The answer returned by the system is a specific identity information such as a name or ID number. Identification systems can contain dozens, thousands, or millions of biometric records. Identification systems are often referred to as 1:N (one-to-N or one-to-many) biometric systems, because specific biometric data are compared with multiple (N) records.

Let's assume that a stored biometric sample or template is the pattern $P' = S(B')$ and an acquired sample is the pattern $P = S(B)$. Then, in terms of a testing hypothesis, we have null (invalid) and alternative (valid) hypotheses:

$H_0: \ B = B'$, the claimed identity is correct (3.1)

$H_1: \ B \neq B'$, the claimed identity is incorrect (3.2)

Certain rate of similarity $s = Sim(P, P')$ is often defined and the decision leads to H_0 if $s \geq T_D$ and correspondingly to H_1 if $s < T_D$, where T_D is the decision threshold. The rate of similarity s is also referred to as the matching score. When $P = P'$, s is called a matching score and B and B' are called a matching pair. When $P \neq P'$, s is called a non-matching score and B and B' are called a non-matching pair.

With regard to the expressions (3.1) and (3.2), the decision H_0, when H_1 is true, gives a false acceptance; the decision H_1, when H_0 is true, results in a false rejection. Both *False Acceptance Rate* (FAR – proportion of non-matching pairs resulting in false acceptance) and *False Rejection Rate* (FRR – proportion of matching pairs resulting in false rejection) together characterize the accuracy of a recognition system for a given decision threshold. Any change of the threshold in one direction can reduce FAR with regard to FRR, and vice versa. In the Figure 3.2, FAR corresponds to the area under the density function H_1 on the right side of the threshold and FRR corresponds to the area under the density function H_0 on the left side of the threshold. In a more general framework, we can express these two errors as *False Match Rate* (FMR) and *False Non-Match Rate* (FNMR) [Dra31].

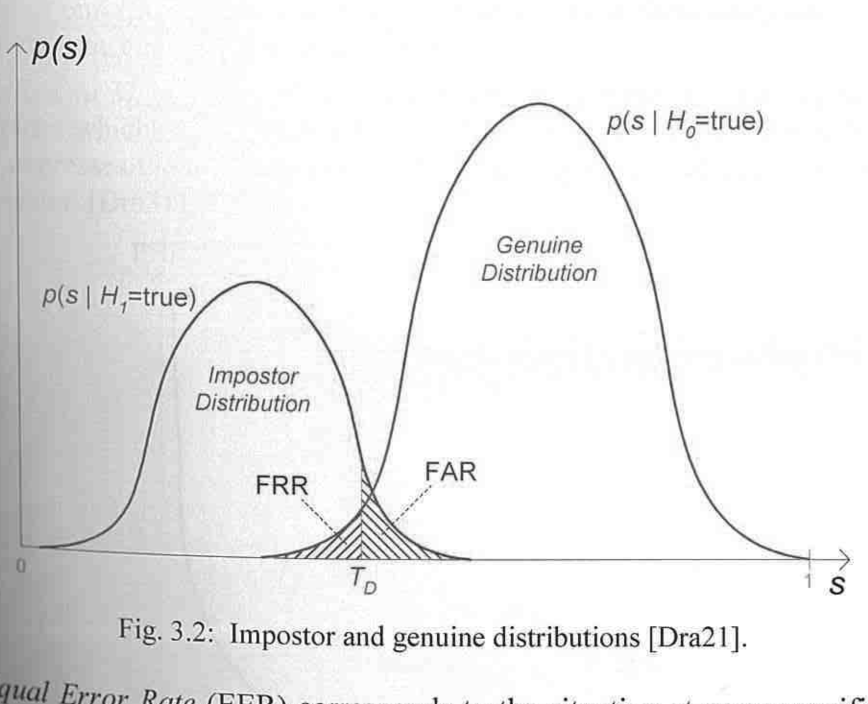


Fig. 3.2: Impostor and genuine distributions [Dra21].

The *Equal Error Rate* (EER) corresponds to the situation at some specific threshold (T_{EER}) when FRR = FAR, i.e. when the areas under the two curves (see Fig. 3.2) are equal.

Rather than showing the error rates in terms of probability densities as in Fig. 3.2, it is desirable to report the accuracy of respective system using a *Receiver Operating Curve* (ROC) [Dra31][Dra21][56]. ROC is related to $T_D \rightarrow$ (FAR, FRR) (Fig. 3.3):

$$ROC(T_D) = \left(FAR(T_D), FRR(T_D)\right) \tag{3.3}$$

Note that in a typical recognition system, all the information contained in the probability distribution functions (PDF) is also contained in ROC. ROC can be directly derived from the probability density functions [Dra21][Dra31] as follows:

$$FAR(T_D) = Prob(s \geq T_D | H_1 = true) = 1 - \int_0^{T_D} p(s \mid H_1 = true)ds \tag{3.4}$$

$$FRR(T_D) = Prob(s < T_D | H_0 = true) = \int_0^{T_D} p(s \mid H_0 = true)ds \tag{3.5}$$

If we let T_D go to zero, then FAR goes to one and FRR goes to zero; if we let T_D go to $T_{\max}$, then FAR goes to zero and FRR goes to one.

The *Failure to Acquire Rate* (FTA) is defined as the expected proportion of transactions for which the system is unable to capture or locate an image or signal of sufficient quality. FTA may depend on adjustable thresholds for image or signal quality [Dra31].

The *Failure To Enroll Rate* (FTE) is the expected proportion of the population for which the system is unable to generate repeatable templates. This will include those users who are unable to provide the required biometric feature or to produce an image of sufficient quality at enrollment, and who cannot reliably match their template in attempts to confirm whether the enrollment is usable [Dra31].

The *Failure to Match Rate* (FTM) determines the percentage share of the input biometric attributes which cannot be compared with some saved template or processed. This failure rate expresses the meaning that the biometric system is unable to do, to some extent, any decision [Dra31].

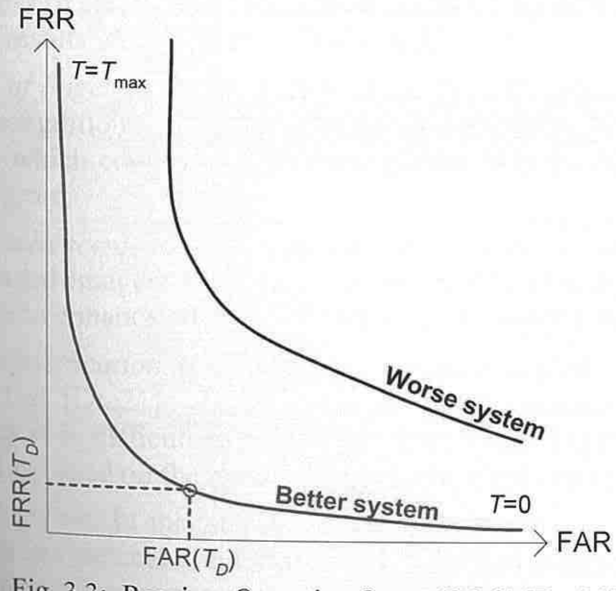


Fig. 3.3: Receiver Operating Curve (ROC) [Dra21].

Although the fingerprint category information and other global pattern configurations such as the number and positions of core and delta points and the ridge count may indicate, to a certain extent, the individuality of fingerprints, the uniqueness of a fingerprint is exclusively determined by the local ridge characteristics and their relationships. Fingerprint matching depends on the comparison of local ridge characteristics and their relationships to determine the individuality of fingerprints. A total of 150 different local ridge characteristics, called *minutia* details, have been identified [14]. These local ridge characteristics are not evenly distributed. Most of them depend heavily on the impression conditions and quality of fingerprints and are rarely observed in fingerprints. The two most prominent ridge characteristics, called minutiae, are a) *ridge ending* and b) *ridge bifurcation*. A ridge ending is defined as the ridge point where a ridge ends abruptly. A ridge bifurcation is defined as the ridge point, where a ridge forks or diverges into branch ridges. Minutiae in fingerprints are usually stable and robust and do not depend, in general, on fingerprint impression conditions. Normally, they can be easily identified. Examples of minutiae are shown in Figure 3.4 [Dra30]. For a given fingerprint, a minutia can be characterized by its type, its *x* and *y* coordinates, and its direction [Dra21].

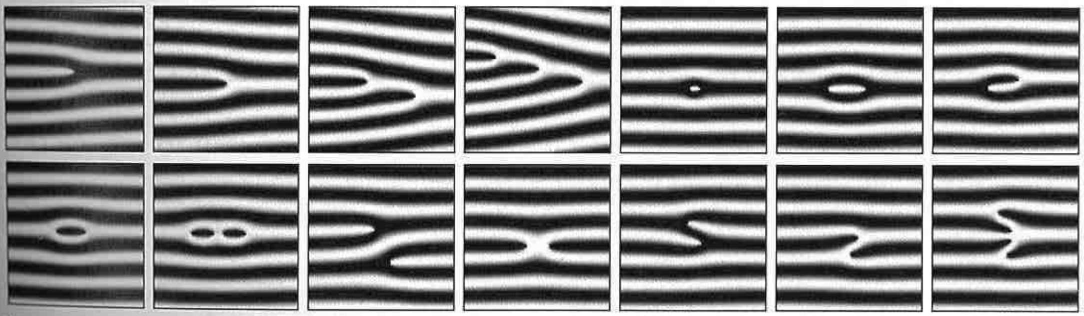


Fig. 3.4: Minutiae examples (line ending, single bifurcation, double bifurcation, triple bifurcation, point, interval, hook; single whorl, double whorl, through line, crossing, side contact, single bridge, twin bridge) [Dra30].

The whole process of fingerprint recognition could be divided into five main steps – see Figure 3.5 (with results of processing) [Dra21][62]:

1) *Acquirement of fingerprint*. The quality of acquired fingerprint is important for the fingerprint recognition. It is recommended to use a fingerprint sensor with a very good quality which could tolerate miscellaneous skin types, dryness or humidity of the finger grain.
2) *Fingerprint enhancement*. This step should enhance the structures of papillary lines in damaged images. However, it is difficult to develop an algorithm which would be able to enhance all types of defects in fingerprint images.
3) *Fingerprint classification*. It relates to the assignment of any fingerprint to the corresponding class [Dra21]. The classification is very demanding process, because in some cases it is difficult to say which class some fingerprint belongs to. The classification is based on the method of analysis of the orientation field [Dra21].
4) *Minutiae extraction*. In this step the structure of papillary lines is examined and the anomalies are detected and extracted as features (minutiae). There are many minutiae points in the structure of papillary lines but only two of them are used for

access systems, namely the ridge ending and ridge bifurcation. All arts of the minutiae points are used for the dactyloscopic system. At the same time, some other algorithms also exist which do not use minutiae points but certain image parts as patterns.

5) *Fingerprints Matching*. The process of matching is based on the comparison of two fingerprints. The first fingerprint is the assumed original of the second one and is usually saved as a template (e.g. on a smart card). During the process, the saved minutiae points in the template and the extracted minutiae points from the newly acquired image are compared. The matching process actually corresponds to the application of pattern comparison algorithm on extracted parts of images.

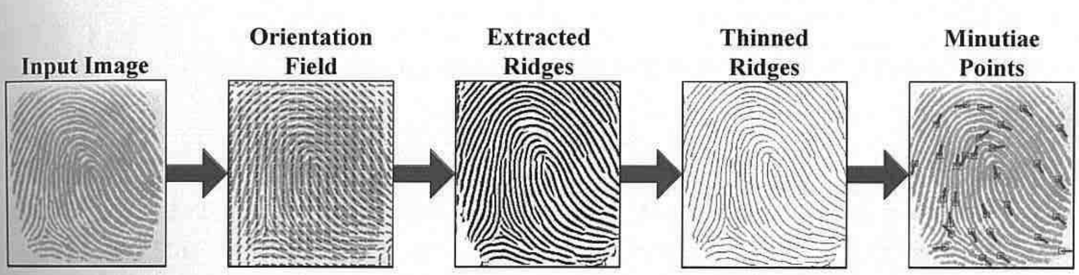


Fig. 3.5: Flowchart results of the minutiae extraction algorithm [Dra21].

At the end of introduction, let us show some examples with a problematic quality. In the Fig. 3.6, there are shown two examples of changed image quality in comparison to the enrolled image (left) and insufficient image quality due to dry skin (right).

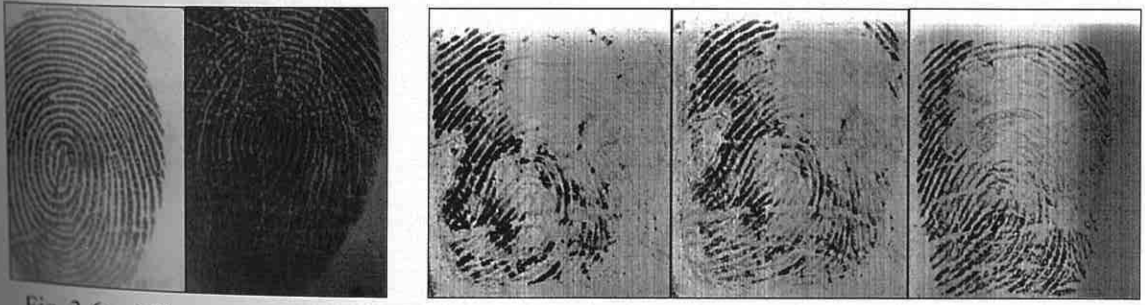


Fig. 3.6: a) Temporary change of fingerprint image quality [35]; b) Images from the same user with a poor quality [35].

Another very crucial factor in fingerprint recognition systems is the data storage. In verification systems, only templates with minutiae (eventually with additional meta-data) are stored, but identification systems (e.g. AFIS) use often fingerprint images, which have to be stored. In this case, the image data compression method plays very important role. There are three possible suitable compression algorithms that are used for the compression of fingerprints at the moment: JPEG, JPEG-2000 and WSQ (Wavelet Scalar Quantization; FBI standard) [15][54]. The more detailed description of the compression method WSQ could be found in [15][54]. An example of images compressed by different methods is shown in Fig. 3.7.

Some parts of the information included in this chapter have been proposed to be included in the drafts of the standards [Dra19] ISO/IEC JTC 1/SC 37/29794-1 (Biometric

Sample Quality – Part 1: Framework) and ISO/IEC JTC 1/SC 37/29794-4 (Biometric Sample Quality – Part 4: Fingerprint Sample Quality Data) in 2007.

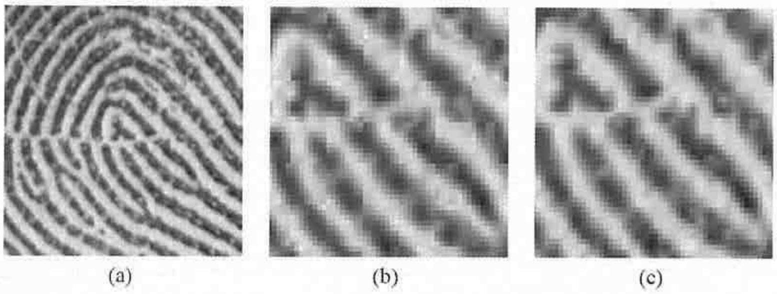


Fig. 3.7: Fingerprint compression [39]: a) an uncompressed fingerprint image; b) portion of image compressed using a generic image compression algorithm JPEG; c) portion of image compressed using WSQ.

In the following subchapters, various methods for fingerprint quality estimation (chapter 3.1) and methods for fingerprint quality enhancement (chapter 3.2) are discussed and at the end some experimental results regarding the methods for previously presented quality estimation (chapter 3.3) are provided. Each subchapter in chapters 3.1 and 3.2 describes a separate method either for the fingerprint image quality estimation or enhancement.

3.1 Methods for Estimation of Fingerprint Image Quality

The exact definition of the quality of a fingerprint image is difficult and nearly impossible. Different types of information are important for various cases – e.g. once it is the contrast, another time the continuality of trajectory of some papillary lines or resulting minutiae quality, etc. In general, it is impossible to formulate one definition covering all cases. But in case of fingerprints, we can find some common properties and, on the basis of such properties, we are able to define some quality requirements.

3.1.1 Image Contrast

The image contrast could be defined in a variety of ways. In the field of fingerprint recognition, two options for the image contrast are available. In these two options, the image contrast is defined as relative local differences in pixel intensities. The definitions are [Dra31][16]:

- Michelson contrast: $C_{Michelson} = \dfrac{(L_{\max} - L_{\min})}{(L_{\max} + L_{\min})}$ (3.6)
- Weber contrast: $C_{Weber} = \dfrac{\Delta L}{L}$ (3.7)

where $L_{\max}$ and $L_{\min}$ in the Michelson contrast are the intensities of the foreground (papillary line) and background (gaps between papillary lines, called valleys), respectively; $L_{\max}$ corresponds to the region with the highest intensity. In the Weber contrast L determines the intensity of the background and ΔL is difference between foreground and background intensities (ridges vs. valleys). The difference of both contrasts is small when small variations of foreground and background intensities are observed, and vice versa, with increasing intensity variations of foreground and background the difference is increasing, too. The complete image contrast could be computed as the mean value of all local intensity differences.

Other possible method is to analyze the intensity differences in specific discrete basic intervals: the difference of intensities *I(i,j)* between the intensity *i* and the intensity *j*, where $i < j$, could be separated from "basic intensities".

In the image with high contrast, nearly all intensity differences are uniformly represented. This is the situation when all pixels show a maximal intensity difference. If the distribution of intensity differences becomes less uniform, the global contrast decreases, too.

It could be said that the degree of similarity with the uniform intensity distribution is a measure for the image contrast determination. If we consider the intensity differences as a vector in a vector space which is separated due to discrete basic intervals, then the image contrast could be specified as a scalar multiplication of the retrieved vector with a base vector in the direction of uniform intensity distribution.

3.1.2 Mean Value of Grayscale Levels

3.1.2.1 Histogram

The meaning of the histogram in this context is the representation of frequencies with a special characteristic, e.g. such histogram makes possible to track the luminosities (gray grades) of image pixels on the horizontal axis.

The horizontal axis is divided into 256 channels depending on the grades of grayscale; the channel with the value 0 corresponds to the lowest luminosity (black) and the channel with the value 255 corresponds to the highest luminosity (white). Other values of the grayscale lie between these two limit values. The histogram is made in such a way that for each image pixel one is added to the sum (or probability distribution function (PDF)) which corresponds to the luminosity of a given pixel. If we go through the whole image, we obtain a luminosity histogram or histogram of gray grades for a specific fingerprint.

We can define the histogram as follows:

$$Hist(r_k) = \frac{n_k}{n},\ k = 0,1,2,\ldots,L-1 \tag{3.8}$$

where $Hist(r_k)$ is the discrete function of the histogram, r_k is the k^{th} gray grade value, n_k is the number of pixels in the channel r_k, L is the number of gray grades and n is the sum of pixels in the image (e.g. 261,144 image pixels for the resolution of 512×512 pixels). The example of such histogram is shown in Fig. 3.8.

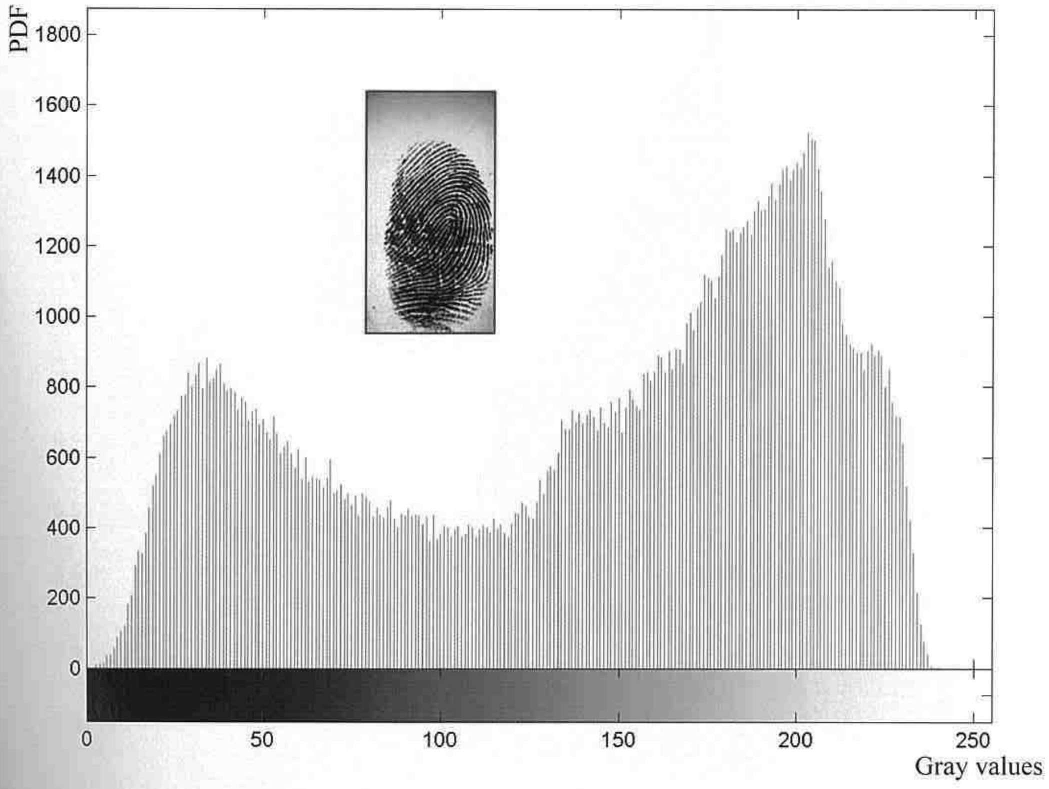


Fig. 3.8: Example of a fingerprint histogram [Dra31].

3.1.2.2 Normalization

For the comparison of histograms of fingerprint images from various sensors, it is crucial to normalize these histograms. It is necessary to find a maximum (on the *y* axis) in the histogram, e.g. the maximum in Fig. 3.8 lies near the gray grade value 200. All other values (or each particular gray grade value) are sorted using this maximum value, i.e. all values will lie in the interval <0,1>. The maximal value is normalized to the new value of 1.0 and all other values are scaled in a corresponding way. The normalized histogram is shown in Fig. 3.9.

3.1.2.3 Mean Value

If we analyze the histogram shown in Fig. 3.9, we can identify two appreciable peaks. The left peak corresponds to the ridges (papillary lines) and the right one to the background (valleys; light background is considered). The papillary lines in fingerprint images are represented usually in dark colors and the valleys (gaps among papillary lines) in light colors; however, an inverse representation is also possible. The presented histogram is nearly an ideal case. Unfortunately, it happens very often that both peaks are not so well recognizable and separable. In general, either one peak is missing or the gray grades are so distributed that a lightly rolling curve spreads across the histogram.

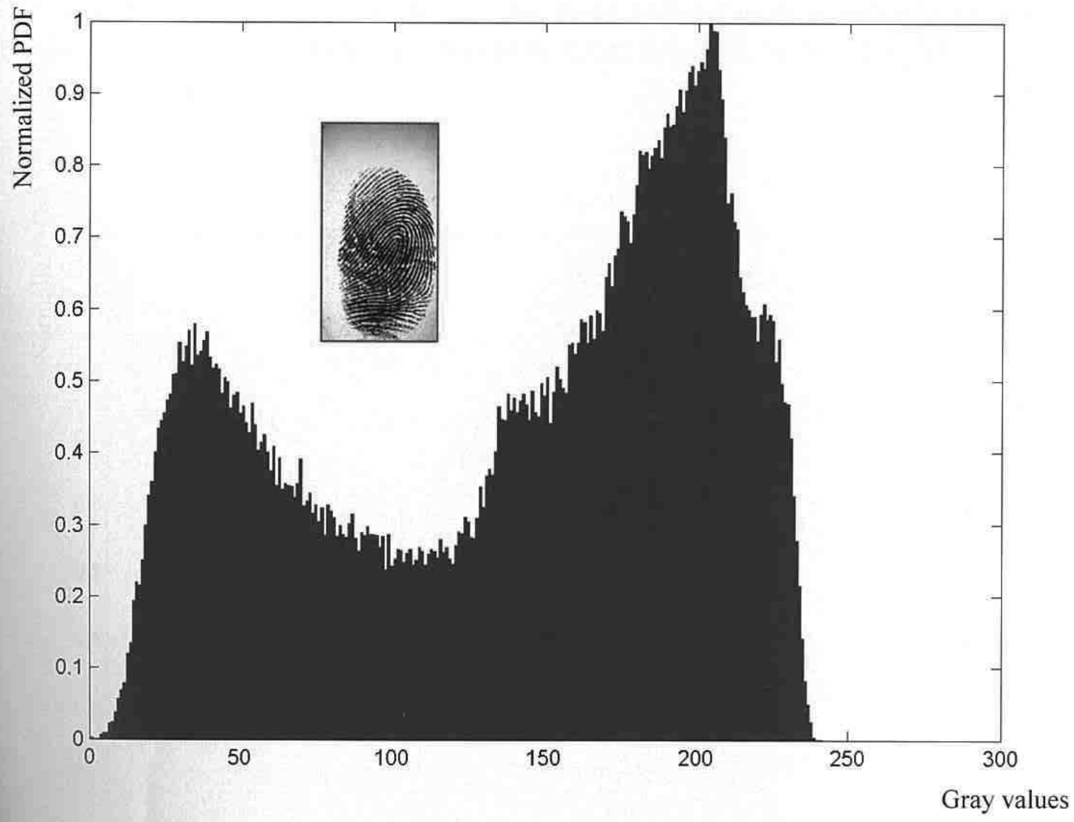


Fig. 3.9: Normalized histogram [Dra31].

In an optimal case, the mean value should be exactly in the middle of the histogram, i.e. at the value 128 (if we consider 256 gray grades). If it is so, it means that the area under the left part S_L of the curve corresponds to the area under the right part S_R of the curve (see Fig. 3.10).

The mean value M represents a quality measure for the distinguishing of papillary lines from the background. The mean value M can lie in the interval <0,255>, because the value represents a gray grade value. This situation is shown in Fig. 3.10. Consequently, the magnitudes of both areas on the left and right sides from the mean value M have to be computed. We denominate these areas as S_L and S_R and then we can write [Dra31]:

$$S_L = \sum_{i=0}^{M-1} h_n(i) \text{ and } S_R = \sum_{i=M}^{255} h_n(i) \tag{3.9}$$

where M is our mean value (at the beginning $M = 128$) and $h_n(i)$ are normalized probability distribution functions for corresponding grades of gray.

If $S_L < S_R$ then the mean value is higher, i.e. moved to the right. In the opposite case ($S_L > S_R$), the mean value is lower (moved to the left). If $S_L \cong S_R$, then the computation of the mean value can be considered as completed.

We should also take notice of the limits of the histogram. Let us denote the beginning of the histogram B_{Dark} and the end B_{Light}. The mean value should obviously lie between B_{Dark} and B_{Light}. We can compute the theoretical mean value M_T as follows [Dra31]:

$$M_T = \frac{B_{Dark} + B_{Light}}{2} \tag{3.10}$$

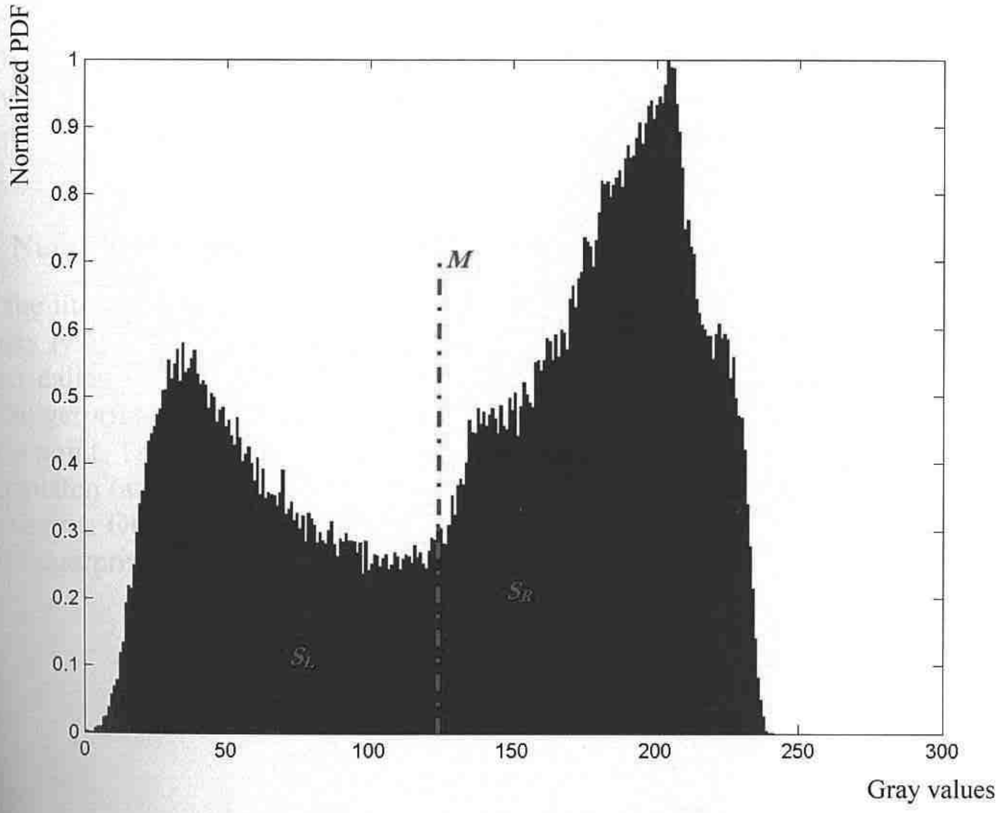


Fig. 3.10: Searching for the mean value M [Dra31].

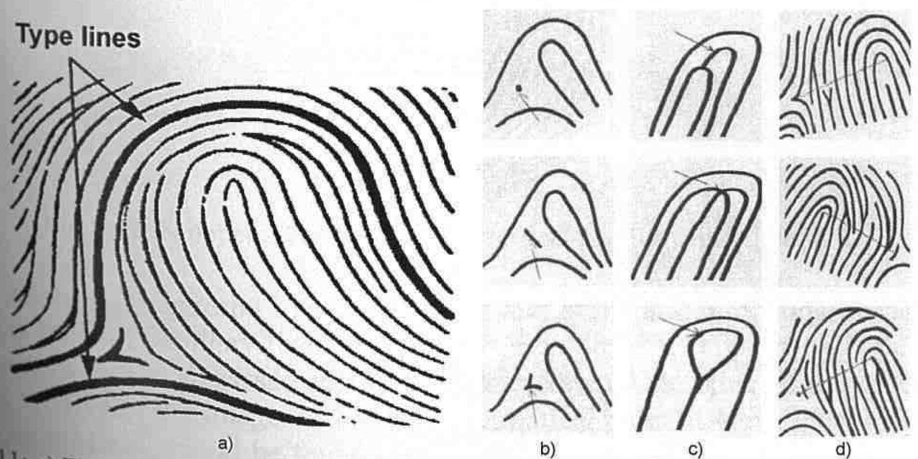


Fig. 3.11: a) Type lines; b) Delta configurations; c) Core configurations; d) Number of lines [Dra31].

Using the real mean value *M,* we are able to compute the deviation *D* from the theoretical value M_T as follows [Dra31]:

$$D = \left|1 - \frac{M_T}{M}\right| \cdot 100\% \tag{3.11}$$

Let us show an example: the histogram starts at the gray grade value $B_{Dark} = 20$ and ends at the value $B_{Light} = 200$. Thus the expected theoretical mean value M_T should lie close to the gray grade value 110. However, the mean value *M* is 140. We can compute the deviation *D* between these two values. The result is $D = 127\%$, i.e. the overrun is 27%, what deviates from the predefined tolerance limit range ±20% (a user-defined range).

3.1.3 Number of Papillary Lines ("RIP Count")

In the literature, the "RIP Count" is used for the computation of the number of papillary lines lying between the fingerprint core and a delta point [Dra31][Dra21], see Fig. 3.11 (so called type lines). This number could be determined in the so called dactyloscopic fingerprints nearly without any problem, because they cover bigger area, including the delta point. The "tip" fingerprints, which are scanned only by putting the finger on the scanner platen (access control), cover smaller area, i.e. the delta point in the fingerprint is often missing. Obviously, it is then impossible to determine the number of papillary lines in such fingerprints as defined in the literature.

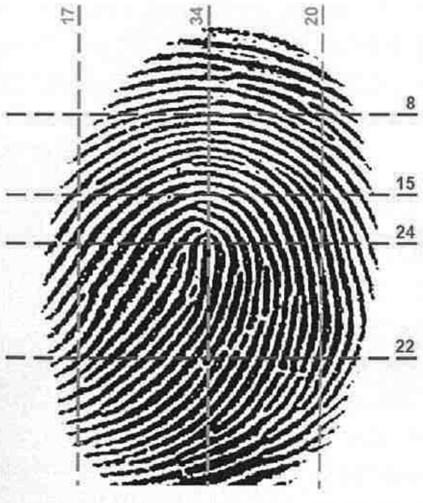


Fig. 3.12: Numbers of horizontal and vertical papillary lines [Dra21].

If we cross the fingerprint image in vertical and horizontal directions, we are able to count the number of papillary lines in each row or column, i.e. how many papillary lines are cut through by the abscissa running from one edge to the other in the given row or column of the fingerprint image. From the mathematical point of view, the maximal number of papillary lines should be found near the core (center) or similarly in homocentric circles where the highest number of such crossings lies near the center of all of them. We are able to determine quite precisely not only the center of the fingerprint [Dra21] but also the quality rate of the sensor.

A larger fingerprint area contains more unique information which can be then exploited for the comparison of fingerprints. The larger the area, the higher number of papillary lines is contained in the fingerprint. It leads to the conclusion that the more papillary lines (in horizontal and vertical directions) we are able to detect, the better results offers the sensor.

One outstanding influence which can affect the count of papillary lines in both directions is either strong blurring (due to a small contrast ratio between papillary lines and background or finger movements during scanning) or merging of two papillary lines together (due to strong pressure or moisture on the finger during scanning). Despite of such influences, the data on the amount of papillary lines are in general stable and reliable.

3.1.4 Failure To Acquire (FTA) Rate

The error rate FTA (*Failure To Acquire*) indicates the percentage of sensor failure occurrences. This error rate is obviously valid for all sensors, not only for fingerprint scanners. The calculation of FTA value could be done as follows [Dra31]:

$$FTA = \frac{N_{Failure}}{N_{Total}} \cdot 100\% \tag{3.12}$$

where $N_{Failure}$ is the number of sensor failures (defects) and N_{Total} is the total amount of all acquirements (both successful and unsuccessful). This factor is usually presented in percents (most frequent case) or as a fraction. The more the result tends to zero, the better is the sensor for fingerprint scanning. And vice versa, the more the result tends to the limit of 100%, the less reliable is the sensor in practice. At higher percentage values, the sensor failures are more frequent, i.e. the user has to put his finger repeatedly to the scanner platen, and this reduces the trust of users to the fingerprint technology.

3.1.5 Sinusoidal Shape of a Papillary Line Crosscut

The fingerprint consists of a copy of papillary lines. In the usual fingerprint image, the ridges have pixels in various grayscale levels. If we make a crosscut (cross-section) through the whole image, preferably through the center of the image (if possible in the fingerprint core), so that we include the maximal amount of papillary lines both in the vertical and horizontal directions, and if we examine this crosscut (sideward) for the amplitude (Fig. 3.13), we can find that the curve of amplitude is similar to a sine function [Dra10][Dra13][Dra15][Dra11]. From this curve of the amount of papillary lines in the fingerprint, we can deduce some very interesting conclusions about the separability of each papillary line from the background, i.e. we can actually assess the suitability of some sensor for fingerprint scanning.

If we have available a crosscut through the fingerprint, then we can compare this crosscut with an ideal (theoretical) sine function curve. The sine function curve represents in fact quite exactly the "right" crosscut through the papillary line – the crossing between ridges and valleys should correspond to the grayscale values plotted on the axis y (see Fig. 3.14), whereas the maximum (sin = 1) should correspond to the black color (ridge = papillary line) and the minimum (sin = –1) should correspond to the white color (valley), or vice versa (in the inverse mode).

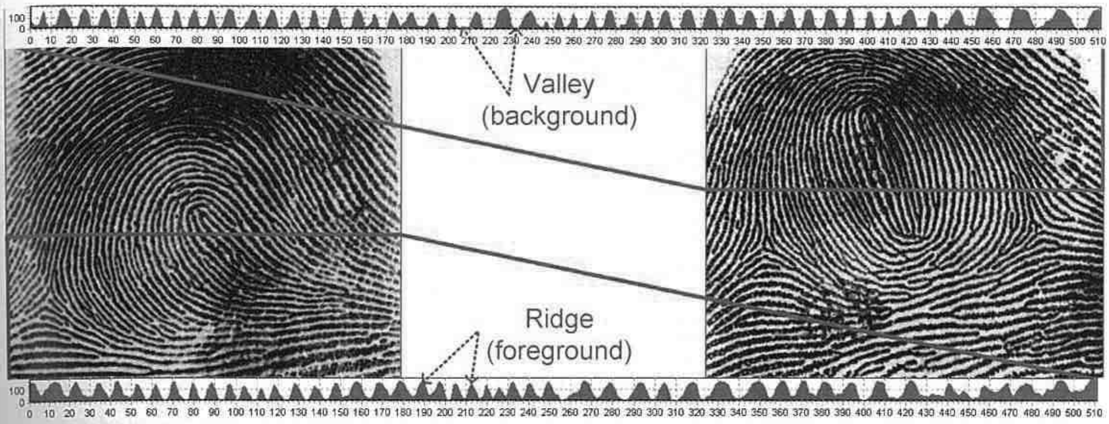


Fig. 3.13: Crosscut of the fingerprint (axis x = pixels, axis y = grayscale values) [Dra10].

The concrete computation should be done as follows. First of all, the crosscut of a fingerprint should be normalized in order to compare it with the sine function curve. The best possibility is to convert it to the range <–1, +1> or <0, 2>. The conversion to the range <0, 2> can be realized by adding the value 1 to the actual function. It is sufficient to extract only one part of the sine function (on the axis x) in the interval $<-\pi/2, 3\pi/2>$ and this part we can apply to the crosscut of the fingerprint – see Fig. 3.14.

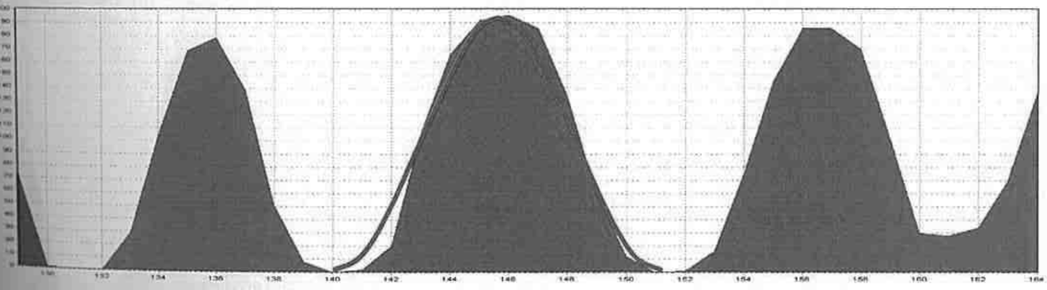


Fig. 3.14: Application of the sine function to the crosscut of the fingerprint [Dra10].

After the right positioning, we are able to measure the deviation (difference/variation of the area) from the "right" theoretical curve. This deviation can be computed as follows [Dra10]:

$$D_D = \left(\frac{A_{FP}}{A_{\sin}} - 1\right) \cdot 100\%, \tag{3.13}$$

where $$A_{FP} = \int_{x_S}^{x_E} f(x)dx, \tag{3.14}$$

and $$A_{\sin} = \int_{x_S}^{x_E} \sin(x)dx \tag{3.15}$$

The value D_D corresponds to the deviation of the papillary line crosscut from the function sine (a negative result signalizes that the curve of the papillary line is lower than the sine function curve; and, on the contrary, a positive result means that the curve of the papillary line is higher than the sine function curve), A_{FP} is the area under the function $f(x)$, i.e. the crosscut of the papillary line, $A_{\sin}$ is the area under the function sine in the interval $<-\pi/2, 3\pi/2>$, the points x_S and x_E denote the beginning and end (on the axis x) of the curve (it results from the function sine that $x_S = -\pi/2$ and $x_E = 3\pi/2$). Some similarity of the papillary line cut is mentioned in the draft of the new standard ISO/IEC SC37 N1954 WD 29794-4, but no tests or deep analyses have been performed yet.

3.1.5.1 Thickness of Papillary Line

It has been defined in the literature [Dra31][14] that the "RIP Count" indicates the number of papillary lines between the center (core) of a fingerprint and the delta point. This number could be easily counted in the so called dactyloscopic fingerprints which are relatively large (with many papillary lines). In the "tip" fingerprints, which result only from the imposition of a finger on the scanner plate, the area is much smaller – it leads often to the situation that the delta point is totally missing in the fingerprint. Hence, the above mentioned computation of the "RIP Count" could not be realized.

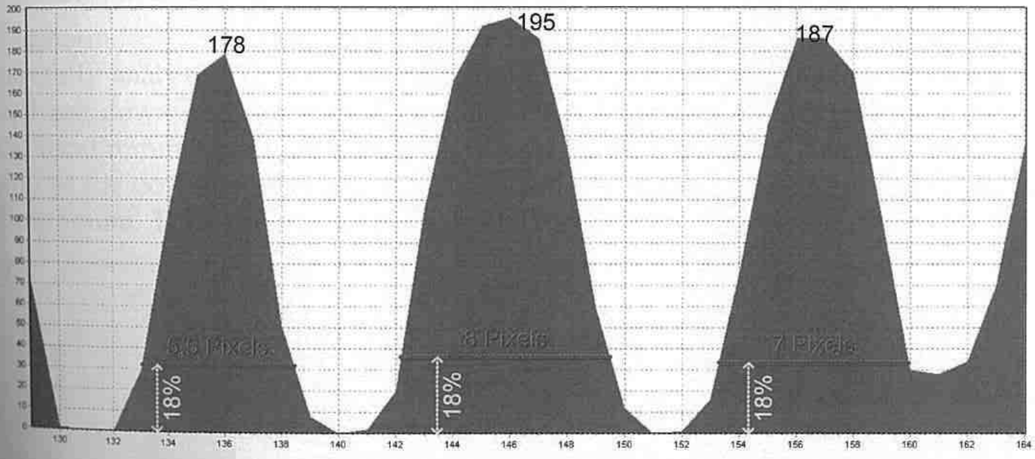


Fig. 3.15: Determination of the thickness of ridges (foreground) [Dra10].

We can deduct some derived criterion from the classical number of papillary lines between the core and delta point – distances among papillary lines and their thicknesses. It can be found in the references [16][Dra21] that the average thickness of a papillary line is 0.33 mm, and the same is true for valleys (gaps) between papillary lines (brief description of ridge / valley width estimation could be found also in [44]). We know the rate of resolution R_{DPI} (DPI) of each sensor. Further, we can count the number of pixels N_{Pix} in the scanned image, which represents a ridge or a valley – for the border calculation, see please [Dra21]. From these two factors, we can calculate the thickness *Th* of the ridge / valley as follows (results are in centimeters, see Fig. 3.15) [Dra10]:

$$Th = \frac{2.54}{R_{DPI}} \cdot N_{Pix} \quad [cm] \tag{3.16}$$

One inch is 2.54 cm, hence the value 2.54 is in the numerator. In relation to the thickness of a papillary line defined in the literature [16][Dra21] as 0.33 mm, we can calculate the deviation D_{Th} of the calculated thickness Th from the above defined value (0.033 is the value of ridge/valley thickness in centimeters) [Dra10]:

$$D_{Th} = \left(\frac{Th}{0.033} - 1 \right) \cdot 100\% \tag{3.17}$$

If $D_{Th} > 0$, then the papillary line obtained from a scanner is displayed thicker as the defined one. And vice versa, if $D_{Th} < 0$, then the papillary line from a sensor is displayed thinner as the defined one. Naturally, we speak only about the graphical representation of papillary line. If $Th \cong 0$, then the scanned papillary line corresponds to the defined one.

On this place, we can extend the analysis – we can test the ability of a sensor to separate a papillary line from the background (valley). It may appear that the contrast difference between the papillary line and the background is too small and the papillary line may be displayed thicker or thinner in comparison with the valley. The thickness should be always approximately 0.33 mm.

3.1.5.2 Steepness of Papillary Line

Furthermore, we can calculate another factor from the crosscut of the fingerprint. If we carefully analyze Fig. 3.15, we can see that we are able to calculate the steepness of upward and downward sections of the curve. The beginning of the upward section is the closest local minimum and the end is the closest local maximum. And vice versa, the beginning of the downward section is the closest local maximum and the end is the closest local minimum. This situation is shown in the Fig. 3.16.

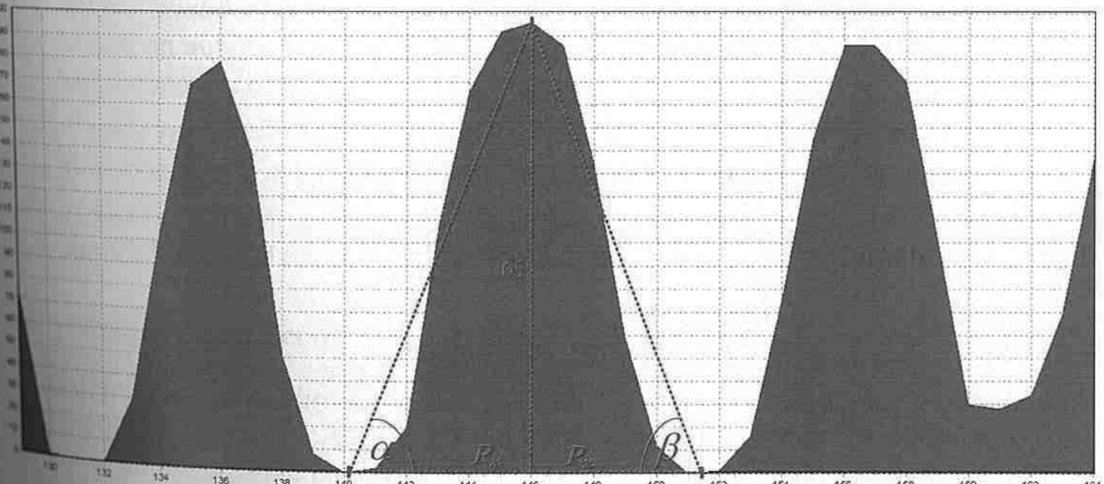


Fig. 3.16: Determination of upward and downward sections of the curve [Dra10].

The values establish the number of points from the beginning of the upward section (point on the left) to the perpendicular in the local maximum (peak), or from the perpendicular in the local maximum to the end of the downward section (point on the right). We can compute two interesting angles from these data [Dra10]:

$$\alpha = \arcsin\left(\frac{P_{x_1}}{\sqrt{P_{x_1} + P_y}} \right) \tag{3.18}$$

$$\beta = \arcsin\left(\frac{P_{x_2}}{\sqrt{P_{x_2} + P_y}}\right) \tag{3.19}$$

Both angles represent the steepness of upward and downward sections. As an ideal case, we can consider an equilateral triangle, i.e. the deviations from these angles could be computed as follows [Dra10]:

$$D_\alpha = \frac{|\alpha - 60°|}{60°} \cdot 100\% \tag{3.20}$$

$$D_\beta = \frac{|\beta - 60°|}{60°} \cdot 100\% \tag{3.21}$$

where D_α is the deviation of the upward angle and D_β is the deviation of the downward angle from the ideal case, i.e. 60°.

At the end it should be mentioned that these metrics for the estimation of quality of papillary lines are strongly influenced by the overall quality of the image. If the image is e.g. strongly compressed, the degree of quality for the papillary line will be different when compared with the case of non-compressed image.

3.1.6 Acquisition Performance Metrics

In the following subsection, there are defined the following three metrics from [125][58], which are linked to the above mentioned metrics:

- *Image quality score* (chapter 3.1.6.1) – is defined as the degree of accuracy at which an automated fingerprint recognition system can extract unique features for subsequent recognition.
- *Usable range* (chapter 3.1.6.2) – is defined as the range of the finger skin condition over which acceptable quality fingerprints can be acquired.
- *Consistency* (chapter 3.1.6.3) – is defined as the rate at which the quality of fingerprint obtained varies with the applied method or with the duration of operation.

3.1.6.1 Image Quality Score

Ideally, an *image quality score* [125] should be defined as the degree of similarity between the image and the actual fingerprint pattern. The fingerprint local structure constitutes the main texture-like pattern of ridges and valleys in a local region. Since a minutia is a local discontinuity, the local structure is a suitable measure for the definition and clarity of a minutia. On the other hand, the valid global structure puts the ridges and valleys into a smooth flow. The flow pattern is characterized by ridges. Thus the global structure is a suitable measure for the definition and clarity of the ridges (Fig. 3.17).

In [125], there are defined the Orientation Certainty Level (OCL) and the Ridge-Valley Structure (RVS) for the estimation of the image quality score. The former is computed using the energy ratio between the tangential and normal direction of the ridge flow, which can be obtained from the ratio of the eigenvalues of the covariance matrix of the image gradient. RVS is computed by the ridge-valley fidelity, measured by the ridge frequency ridge-to-valley ratio and ridge thickness. The number of blocks (S_L) with OCL and RVS exceeding predetermined thresholds will indicate the quality. Another two main measures were also proposed to quantify the global structure [125]. These are the orientation continuity (S_{GO}) and ridge-valley uniformity (S_{GR}). The former is given by the number of foreground blocks in the local structure with uniform ridge-valley structure. The Image Quality Score (QS) is then given by the weighted value of all these measures [125]:

$$QS = (\alpha_1 S_L + \alpha_2 S_{GO} + \alpha_3 S_{GR}) \times \frac{\min(T - T_{BL}, A_{\min})}{A_{\min}} \tag{3.22}$$

where $\alpha_1+\alpha_2+\alpha_3=1$, T is the total number of blocks, T_{BL} is a number of blank blocks and $A_{\min}$ is the predetermined minimum number of blocks for foreground.

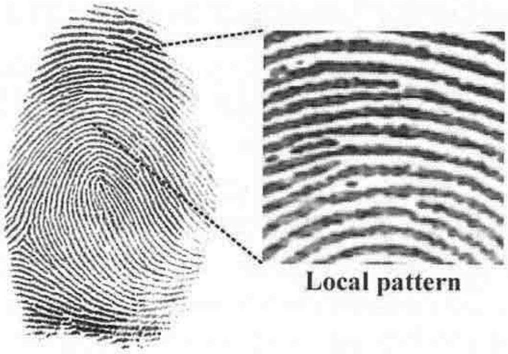


Fig. 3.17: Global vs. local pattern.

3.1.6.2 Usable Range

The *usable range* parameter [125] measures the performance of the sensor across the various finger types due to skin condition, such as wet, normal or dry. However, the accurate determination of the degree of wetness or dryness of a finger is currently difficult. Instead, all fingerprint images are classified into three main classes – normal, dry or wet. The equal weighted average percentage of number of fingerprints achieving a minimum acceptable level of QS in each class will indicate the usable range.

Given M classes of skin type, the usable range (UR) is defined as follows [125]:

$$UR = \frac{\sum_{x=1}^{M} \frac{n_{ax}}{n_{tx}}}{M} \cdot 100 \tag{3.23}$$

where n_{ax} is the number of fingerprints in the class x with $QS \geq T_a$, n_{tx} is the total number of fingerprints in the class x, and T_a is the minimum image quality score for the acceptable fingerprint quality.

3.1.6.3 Consistency

The *consistency metric* C [125] measures the variation of the image quality score measured over time and usage. Effectively, this metric determines the change in the image quality from its initial value after the fingerprint sensor has been used for a fixed time P. We can define [125]:

$$C = \left(1 - \frac{QS_0 - QS_P}{QS_0}\right) \cdot 100 \tag{3.24}$$

where QS_0 is the image quality score at the time 0 and QS_P is the image quality score after the time P.

3.1.7 Image Quality as a Predictor of Matcher's Performance

The following subsection describes another approach from [92] for the computation of image quality, using different metrics. This image quality is then used as a predictor of matcher's performance.

A fingerprint is a pattern of friction ridges on the surface of a fingertip. A good quality fingerprint has distinguishable patterns and features that allow the extraction of features that are useful for subsequent matching of fingerprint pairs. A minutia based automatic fingerprint matching algorithm uses the comparison of local ridge characteristics (minutiae) of two fingerprints (biometric samples) $x_{g(i)}$ and $x_{p(j)}$ and produces a real valued similarity score [92]:

$$s_{ij} = F\left(x_{g(i)}, x_{p(j)}\right) \tag{3.25}$$

where subscript $g(i)$ denotes i^{th} gallery (collection of fingerprint images/templates) and $p(j)$ denotes j^{th} probe and s_{ij} is the similarity (matching) score of the i^{th} gallery matched against the j^{th} probe.

We call similarity scores s_{ii} of a genuine (i.e. the same) person *match scores*, and similarity scores s_{ij}, $i{\neq}j$ of an imposter (i.e. different person) *non-match scores*. For a gallery of size G, with the assumption that there is one and only one biometric sample for each subject enrolled in the system, for each probe image $x_{p(i)}$ there is only one match score s_{ii} and G-1 non-match scores s_{ij}, $i{\neq}j$. Let $s_m(x_i)$ denotes the match score for sample $x_{p(i)}$ and $s_n(x_{ij})$ non-match scores of $x_{p(i)}$ and $x_{g(j)}$, while $i{\neq}j$.

A higher similarity score is considered to indicate a higher likelihood that the samples come from the same individual. Let $M(s_m)$ denotes the cumulative distribution function (CDF) of the match scores, and $N(s_n)$ the CDF of non-match scores. The Detection Error Trade-off characteristic (DET) is a plot of the false non-match rate [92]

$$\text{FNMR} = M(s_m) \tag{3.26}$$

against the false match rate [92]

$$\text{FMR} = 1 - N(s_n) \tag{3.27}$$

for all values of s_m and s_n. The DET, and the equivalent ROC (Receiver Operating Curve), are the most common expressions of performance of a verification system.

We define the *fingerprint image quality* as a predictor of a matcher's performance. Before advancing any further, we need to quantify the matcher's performance. The similarity score is the ultimate expression of expected performance: in conjunction with the underlying match and non-match distributions it yields likelihood for the samples coming from the same person or different people. The match and non-match distributions are results of complex non-linear algorithms and are not usually random but strongly dependent on the internal algorithm and how its parameters are set.

It is common for a match distribution that it is wider than a non-match distribution [92]. It is also quite typical for two distributions that they overlap. The overlapping of match and non-match distributions means that a given sample x_i will match falsely, if its match score $s_m(x_i)$ is lower than some non-match scores $s_n(x_{ij})$, $s_m(x_i) < s_n(x_{ij})$, $i \neq j$. If the quality measure q is to be predictive of matcher performance, good quality fingerprints must be those with high match scores and well separated from the non-match distribution. Similarly, poor quality fingerprints are those with lower match scores, in particular those where their match scores are in the region of overlapping with non-match scores.

Therefore, the *quality measure* q [92] should indicate the degree by which the match distribution $M(s_m)$ is separated from the non-match distribution $N(s_n)$. Specifically, we can define the quality q_i of the biometric sample x_i to predict [92]:

$$o(x_i) = \frac{s_m(x_i) - E\lfloor s_n(x_{ij}) \rfloor}{\sigma(s_n(x_{ij}))}, \ \forall x_i \in \Gamma \vee \Pi \tag{3.28}$$

where Γ is the gallery (collection of fingerprint images/templates), Π is the probe set, $E[]$ is the mathematical expectation, $\sigma()$ is the standard deviation, $s_m(x_i)$ is the match score, and $s_n(x_{ij})$ are the non-match scores of sample x_i, $\forall j$, $i \neq j$. Comparing a probe sample x_i with an internal gallery of G samples, which include one and only one sample from the same subject (person), results in a vector of G scores, s. Only one element of the vector s is the match score of x_i, and the other G-1 elements are its non-match scores. $E[]$ is evaluated by computing the mean of all non-match scores of the probe sample x_i to all G-1 non-matching gallery entries. Likewise, $\sigma()$ is the standard deviation estimated solely from the non-matching elements of s. We call $o(x_i)$ the normalized match score of sample x_i. Basically, we are comparing the subject's biometric sample to the claimed match sample and to other non-matching samples, and adjusting the raw score on the basis of the extra scores.

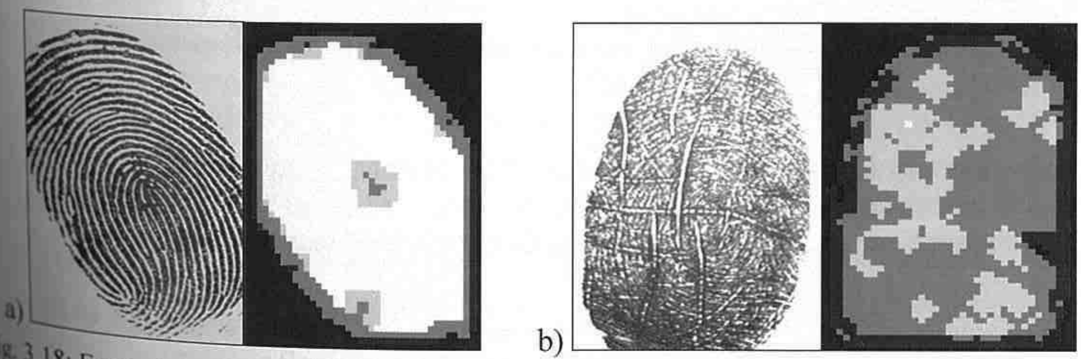


Fig. 3.18: Examples of pairs (the left image is original, the right image is an algorithm assessment representation) with a) a good quality and b) poor quality [92].

For each fingerprint, we define its image quality as the predictor of its normalized match score. Similarity scores as defined by Eq. (3.25), and also normalized match scores as defined by Eq. (3.28), are a function of both probe and gallery samples, but the quality as defined here is a scalar value which is measured for each sample separately. Therefore, the *pair wise quality* q as defined below should predict the recognition performance of the pair (x_Γ, x_Π) [92]:

$$q = \min(q_\Gamma, q_\Pi) \tag{3.29}$$

In an operational setting, if it is ensured that the enrolled samples have a high quality, then a measurement of quality of a subject's biometric sample (probe) can be sufficient to predict its normalized match score.

We measure the (scalar value) quality q_i for a biometric sample x_i, first by computing a feature vector v_i, which contains appropriate signal or image fidelity characteristics of x_i and then finding some (nonlinear) mapping from v_i to $o(x_i)$. Mathematically speaking [92]:

$$v_i = L(x_i) \tag{3.30}$$

$$q_i = \tilde{o}(x_i) = I(v_i) \tag{3.31}$$

The function $L()$ will be realized by computing characteristics and features of x_i that convey information for a matching algorithm. The application of $L()$ to a sample x_i results in an n-dimensional feature vector v_i. For fingerprints, this includes the measured clarity of ridges and valleys, size of image, and number and quality of minutiae. The function $I()$ results from a mapping from the space of feature vectors v to normalized match scores $o()$. Finally, $\tilde{o}(x_i)$ is the predicted value for $o(x_i)$.

3.1.8 Overall Quality Quantification

The precise fingerprint image acquisition up to the minutiae has some peculiar and challenging aspects, many of them caused by contact problems, specifically [124]:

- *Inconsistent contact*: The act of sensing distorts the finger. Determined by the pressure and contact of the finger on the imaging surface (e.g. 2D glass platen), the 3D shape of the finger is mapped onto the 2D surface. Typically, this mapping is uncontrolled and results in different inconsistently mapped regions across impressions.
- *Non-uniform contact*: The ridge structure of a finger would be completely captured, if the ridges of all imaged parts of the finger were in complete optical contact with the glass platen. In practice, due to various reasons, this is not the case.
- *Irreproducible contact*: Manual work, accidents, etc., inflict injuries on the finger, thereby changing the ridge structure of the finger either permanently or semi-permanently. This may introduce additional spurious minutiae or "minutiae-like" features.
- The act of sensing itself *adds noise* to the image. For example, residues leftover from the previous fingerprint capture (so called latent fingerprints).

- A typical *imaging system distorts the image* of the sensed finger due to imperfect imaging conditions.

All these factors contribute to poor samples and feature extraction artifacts during image processing and hence increases false accept/reject rates. Most of the poor quality prints are due to a non-uniform and inconsistent contact. Among the prints with inconsistent contact, the undesirability of the differently distorted impressions (due to application of different pressure on the finger) is very difficult to assess without actually matching the prints and hence is not within the scope of quality assessment. Many quality assessment systems, however, do detect the size of the print area and relative placement/orientation of the finger. These systems can provide a simple feedback to the user about proper placement of the finger to the image acquisition device but cannot quantify the quality of the fingerprint image itself. More sophisticated systems have an explicit method of quantifying the quality of the fingerprint being captured.

The dryness of the finger skin, skin disease, sweat, dirt, and humidity in the air all contribute to a non-uniform and non-ideal contact situation: some parts of the ridges may not come in a complete contact with the platen, and vice versa: regions representing some valleys may come in contact with the glass platen. Non-uniform contact manifests itself in dry prints (too little ridge contact) or smudgy prints (neighboring ridges touching each other obliterating the intervening valleys) or in prints with combinations of such effects. Non-uniform contact may result in "noisy" low contrast images and could lead to many feature extraction artifacts, e.g. spurious minutiae or missing minutiae. For instance, in a dry fingerprint, the ridge is in intermittent contact with the platen, hence dryness of the fingerprint manifests itself in the significant variation of pixel intensities along a dry finger ridge. In extreme situations, there is no particularly dominant direction of a very dry ridge, because too small a fraction is in contact with the platen.

On the other hand, in a smudgy portion of the fingerprint, the neighboring ridges touch each other, thus completely obliterating the intervening valley. As a result, the variation in pixel intensities across the ridge direction is significantly lower than a typical expected variation across an ideal ridge. In extreme situations, the directionality of ridges is obliterated due to a large number of ridges touching each other (this is analogous to image saturation).

For the pattern recognition task of fingerprint representations, prints have been (implicitly or explicitly) modeled as smoothly owing directional textures (ridges) that can be extracted by typical fingerprint feature extraction algorithms. Since the directionality of finger ridges is an essential attribute of its image texture, it was proposed in [124] that this anisotropy can constitute a basis for assessing the *overall quality* of the fingerprint.

Sub-sampling and blocking [124]: For efficiency reasons, the quality analysis uses a sub-sampled image. The analysis samples the image at the rate s in x and y directions. The sub-sampled image is further divided into the square blocks of size B.

Direction and foreground estimation [124]: This step determines whether a given block depicts a portion of a fingerprint and extracts a nominal direction from a foreground block. At each pixel in a given block, a number of pixels is selected along a line segment with the orientation d and pre-specified length l centered around that pixel. A variation in the intensities of the selected pixels is then determined by computing the sum of *intensity differences* $D_d(i,j)$ between the given pixel and the selected pixels [124]:

$$D_d(i,j) = \sum_{(i',j')} \left| f(i,j) - f_d(i',j') \right| \tag{3.32}$$

where d=0, π/n, … π and $f(i,j)$ is the intensity of pixel (i,j) and $f_d(i',j')$ are the intensities of the neighboring pixels (i,j) in the direction d. This indicates the summation of differences between a given pixel of interest, the pixel (i,j), and a number l neighboring pixels in each of the directions. The variation in intensities is computed for n discrete orientations. The orientation at a pixel $\hat{d}$ is the orientation of the line segment for which the intensity variation thus computed is minimal.

Regions of background and portions of impressions having faint residual leftover of earlier captured prints on a dirty input device usually exhibit small intensity variation around their neighborhoods. To determine whether an image pixel belongs to the background, the intensity variation $D(i,j)$ at the pixel (i,j) of interest is subsequently obtained by summing up the differences in the n directions with [124]

$$D(i,j) = \sum\nolimits_d D_d(i,j) \tag{3.33}$$

and when D is smaller than a background threshold τ for each d, the pixel is classified as a background pixel. When more than a fraction of pixels in a block are background pixels, the block is regarded as background block.

Using a connected component analysis, foreground components that are smaller than a certain threshold fraction of the total image area are considered spurious. A print with no legitimate foreground area is of the poorest quality.

Dominant direction: After the foreground blocks are marked, it is determined whether the resulting direction for each block is prominent. The idea is that a block with a prominent direction should exhibit a clear ridge/valley direction that is consistent with most of the pixel directions in the block. The existence of a dominant direction can be assessed by computing a histogram of directions D_d at each pixel in a given block. If the maximum value of the histogram is greater than a prominent threshold, the block is said to have a dominant direction, and is labeled as prominent. Bifurcations of ridges may often result in two dominant directions in a block. Therefore, if two or more directions of the direction histogram are greater than a bifurcation threshold, the corresponding block is labeled as a bifurcation block. A post-processing step removes blocks that are inconsistent with their neighbors. If a "directional" block is surrounded by "non-directional" blocks, it is relabeled as a non-directional block. Similarly, a non-directional block surrounded by neighboring directional blocks is changed to a directional block. Regions of dominant blocks with an area smaller than a threshold number of blocks are discarded.

Quality computation: Since regions (or accordingly minutiae) near the centroid are likely to provide more information for biometric authentication, the overall quality of the fingerprint image is computed from the directional blocks by assigning the relative weight w_i for the foreground block i at the location x_i [124]:

$$w_i = e^{-\frac{\|x_i - x_c\|^2}{2q^2}} \tag{3.34}$$

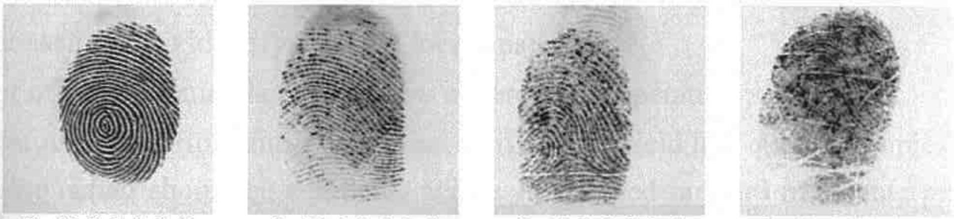
where x_c is the centroid of foreground, and q is a normalization constant.

The **overall quality** ***Q*** of a fingerprint image is obtained by computing the ratio of total weights of directional blocks to the total weights for each of the blocks in the foreground [124]:

$$Q = \frac{\sum_{D} w_i}{\sum_{F} w_i} \tag{3.35}$$

where D is the set of directional blocks and F is the set of foreground blocks. The quality Q is used as a measure of how much reliable directional information is available in a fingerprint image. If the computed Q is smaller than the quality threshold T, the image is considered to be of poor quality.

Dryness and smudginess: Once it is determined that the fingerprint is of a certain poor quality, it is desirable to identify a more specific cause of the low quality. A method for distinguishing smudged poor quality prints from dry poor quality prints is described in [124], based on simple statistical pixel intensity based features. The idea is that for a smudged impression, there are a relatively large number of blocks with a very small contrast. Similarly, for a dry impression, there are a relatively large number of blocks where the contrasts of their neighbors vary significantly (see Fig. 3.19).



Q=(0.9,0.0,0.0) Q=(0.6,0.0,0.4) Q=(0.3,0.0,0.4) Q=(0.1,0.2,0.5)

Fig. 3.19: Qualities of different images [124], legend: Q(overall quality, smudginess, dryness).

3.1.9 Biometric Sample Quality Scoring

As it has been defined in the beginning of this chapter, a sample is a biometric measure, and its quality is very significant for the further algorithmic processing. The biometric sample (i.e. fingerprint in our case) quality takes in consideration [2][38]:

- *Character* (inherent features). It is the description of "inherent" quality of a biometric sample. It includes, e.g. blur, shadows or poor lighting in the image.
- *Fidelity* (accuracy of features). It is the description of "inherent" quality of a biometric sample, too. The fidelity means e.g. a good image of the wrong human body part.
- *Utility* (predicted biometrics performance). If the compared images match better, i.e. they have lower error rates, then the samples are better (Fig. 3.20). The utility depends on the matching algorithm, and does not allow the quantification of "inherent" quality.

In addition to the sample quality, a recommended sample size can be defined. More details to the biometric sample size definition can be found in [18].

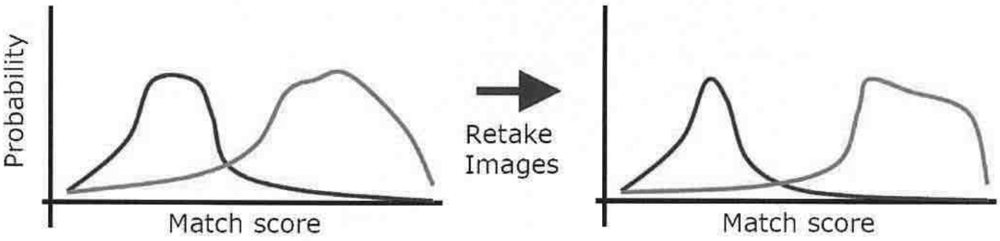


Fig. 3.20: Comparison of worse and better matching samples [2].

The *biometric quality assessment method* (BQAM) [91] derives a numerical quality value from an input biometric sample. The quality value is related to the biometric error rates that are likely to be realized when the sample is matched. Even if this predictive function is imperfect, it is likely to be valuable.

There is a need to summarize quality values computed across all retained samples in an enterprise into a single quality value representing the overall quality of the enterprise. A quality summarization supports monitoring [91]:

- over time (to expose seasonal variation, or trends)
- for each sensor (to identify defective devices)
- at each site (to identify problem locations)
- of officials or attendants (to assess adherence to operating procedures)
- per user basis (to identify users that consistently yield low quality samples).

Quality values should be computed across all retained samples in an enterprise. This can be done online or offline. This will depend on factors such as [91]:

- the computational cost of BQAM execution during enrollment or verification
- whether or not the samples are retained (in the verification, they may not be)
- whether the matching scores or decisions themselves constitute a reportable operational performance measure
- the timescale for production of quality summaries.

Once values have been collected in a central location, these should be aggregated. The provider of a quality assessment algorithm should supply a function to aggregate values into a summary statistic. The quality summary statistics of BQAM should be within the range [0,100]. For verification applications, quality summarization functions should weight the native quality values to reflect the mean expected false non-match rate (FNMR).

A good question is why we worry about low quality biometric samples. The answer is that biometric samples with low quality have less "biometric information". The *biometric information* could be defined as follows [2][1]: the decrease in uncertainty about the identity of a person due to a set of biometric measurements. The *biometric information* is a relative entropy $D(p\|q)$ [2]:

$$D(p\|q) = \int p(x)\log_2 \frac{p(x)}{q(x)} dx \qquad (3.36)$$

where D measures the extra information in p and q, $p(x)$ is the distribution for an individual and $q(x)$ is the distribution for the population. In this case, the following distribution models could be used [2][1]: Gaussian models, PCA features and regularization.

The quality of a biometric measure can be defined as follows [2]:

$$\Delta D(p\|q) = \frac{\frac{1}{N_f}\sum_{i=1}^{N_f}\left(D(p_{f_i}\|q_{f_i}) - D(p_{g_i}\|q_{f_i})\right)^2}{\frac{1}{N_f}\sum_{i=1}^{N_f}\left(D(p_{f_i}\|q_{f_i})\right)^2} \qquad (3.37)$$

where N_f denotes the number of features and f and g denote different "instruments" for the acquirement of biometric samples. $\Delta D(p\|q)$ is the *sample quality difference* between two measurement "instruments" used for the acquirement of the biometric sample.

3.1.10 Minutiae Quality Scoring

The following subsection is based in principle on [11]. The performance of fingerprint verification systems depends very much on the fingerprint image quality. Due to predictable factors such as thin ridges and scars, as well as unpredictable factors such as dry/wet fingers and moving fingers, fingerprint images are sometimes of low quality. This may harm the reliability of fingerprint authentication systems by the extraction of false minutiae.

Minutiae quality scores produced by the Local Ridge Pattern (LRP) algorithm [46] are calculated based on statistical data of the inter-ridge distance around the genuine and false minutiae. Although the LRP algorithm is originally designed for ridge skeletons extracted using the binarization and thinning algorithm, the approximate ridge skeletons called walked map produced by a direct gray scale algorithm [11] may be more desirable in some cases because of its high computational efficiency. This algorithm has been therefore extended [11] by using direct gray scale images as an input and investigating the consistency of ridge information around a minutia in direct gray scale images instead of binarized and thinned images.

From Fig. 3.21b, it could be noticed that ridge skeletons extracted by binarization and thinning are more stable and regular, and thus the ridge information around minutiae is more reliable and suitable for the LRP algorithm. However, the ridge skeletons extracted from direct gray scale images by "walking" along the ridges show significant dithering. The ridge skeletons showed in Fig. 3.21c are relatively less reliable in presenting the real fingerprint ridges.

Considering such a difficulty, a fingerprint image enhancement step for achieving more regular ridges is necessary for improving the ridge skeleton quality in the direct gray scale walked map. An efficient Gabor filtering algorithm has been applied in [11] before the minutiae extraction and minutiae quality evaluation. According to Fig. 3.21e, the ridge skeletons extracted after the image enhancement are even more regular than those from the binarization and thinning algorithm. Therefore, the enhanced direct gray scale images are suitable for performing LRP algorithm to evaluate minutiae quality. Then the minutiae quality scores are calculated on the walked map of the enhanced fingerprint image using the LRP algorithm.

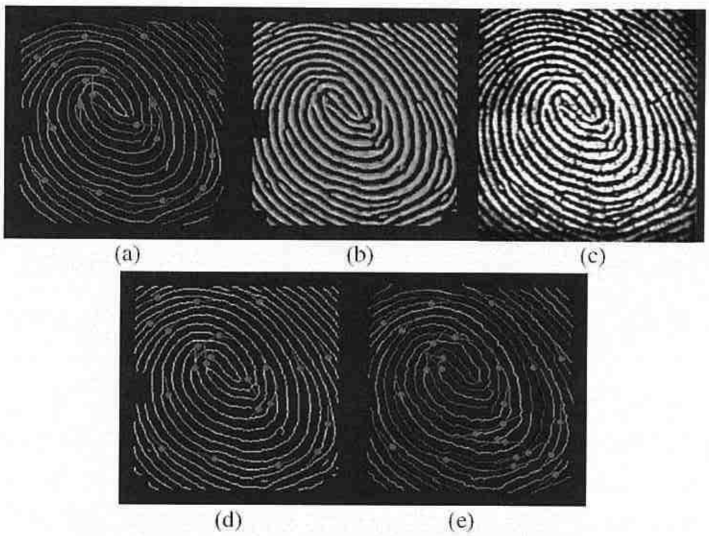


Fig. 3.21: a) Original fingerprint; b) Ridge skeletons extracted by binarization and thinning algorithm; c) Ridge skeletons extracted by direct gray scale algorithm; d) Enhanced fingerprint image using Gabor filters; e) Ridges extracted by direct gray scale algorithm after Gabor filter based fingerprint image enhancement [11].

It was found in [11] that around 30% of the minutiae cannot be assigned with legal quality scores. Parts of these minutiae are located near the edges or core point of the fingerprint images so that inter-ridge parameters cannot be found for a minutiae quality scoring because of the incomplete ridge information or dramatic ridge direction changes. In order to overcome this problem, there has been adopted an image correlation-based approach to address the minutiae quality scoring. The inspiration of this approach comes from the fact that the correlation of fingerprints performs satisfactorily in certain matching tasks.

To achieve the optimum matching of different fingerprint minutiae patterns, some of the algorithms use complicated methods to shift, rotate or even deform the minutiae patterns. Four relatively more straightforward minutiae matching strategies were proposed in [11] and some minutiae quality scores can be embedded into them as follows:

- In *Basic Fingerprint Matcher* (BFM), every minutia from two fingerprints will be stored in two lists accordingly. At each time, a minutia will be selected from each list. These two minutiae are the candidates to form a candidate pair. For the candidate to be matched, preliminarily, they should have a tolerable difference for the following three parameters: distance and orientation of the minutiae with respect to the core point and also the direction of the minutiae [11]. At the same time, both of their quality scores should exceed an acceptable threshold. If any one of them has a quality score lower than the threshold, they will not be regarded as a matched pair. If they satisfy the matching criterion described above, the two minutiae are matched. Then, the matching score of the two fingerprints will be increased by one and both minutiae candidates will be removed from the candidate lists. The whole process continues until one of the lists becomes empty. If more than 80% of total minutiae of two fingerprints are matched, the two fingerprints are said to be matched.

- *Best-Pair-Come-First Fingerprint Matcher (BPM).* This algorithm is basically a variation of BFM. The use of minutiae quality scores in this algorithm is similar to that of BFM. However, unlike the basic matcher, instead of finding a first matched pair, BPM algorithm aims at finding the best matched pair from all possible minutiae pairs. It is based on a belief that first matched minutiae pairs are not always the correct matched pairs. After it first finds a match pair similar to BFM, instead of removing them from the candidate lists, it would continue to match all other possible pairs until the pair with the highest matching score (the best matched pair) for that minutia is found. The matching process will be continued for all other minutiae.
- *Score Filtering Before Fingerprint Matching (SFBM).* Intuitively, high quality minutiae pairs should contribute more to the fingerprint matching score. However, in the previous two matching strategies, low quality minutiae pairs contribute equally to the fingerprint matching score. Furthermore, for low quality minutiae, their parameters may be seriously affected by image noises. Thus, it is expected for fingerprint matching to be more reliable, if some of these uncertainties could be eliminated. Therefore, so as not to match minutiae with uncertain or low quality, minutiae with low quality scores will be removed before matching in SFBM.
- *Minutiae Quality Averaging (MQA).* As mentioned before, around 30% of minutiae cannot be scored using the LRP algorithm. However, such minutiae cannot be simply ignored, as it would cause fingerprint features loss. Besides, some minutiae may have extremely low quality scores due to image noises, which is unfavorable to minutiae quality evaluation. Under the assumption that the minutiae quality within a small fingerprint area should be consistent, the quality scores of minutiae which cannot be scored or have extremely low quality scores can be approximated by averaging the quality scores of their neighboring minutiae.

More details and results to the minutiae quality scoring could be found in [11][46].

3.2 Methods for Image Quality Enhancement

Currently the most widely used and the most accurate automatic fingerprint verification/identification techniques use minutiae-based automatic fingerprint matching algorithms. Reliably extracting minutiae from the input fingerprint images is critical to fingerprint matching. The performance of current minutiae extraction algorithms depends heavily on the quality of input fingerprint images [78]. In an ideal fingerprint image, ridges and valleys alternate and flow in a locally constant direction and minutiae are anomalies of ridges. In practice, due to variations in impression conditions, ridge configurations, skin conditions (dryness, moist finger, aberrant formations in epidermal ridges of fingerprints, postnatal marks, occupational marks, skin diseases), acquisition devices, and non-cooperative attitudes of subjects, etc., a significant percentage of acquired fingerprint images (approximately 10% according to [78]) is of a poor quality. The ridge structures in poor-quality fingerprint images are not always well defined and hence they cannot be always correctly detected. This could result in failures of minutiae extraction algorithms; a significant number of spurious minutiae may be created, a large percentage of genuine minutiae may be undetected, and a significant amount of error in position and orientation may be introduced.

To ensure that the performance of the minutiae extraction algorithms is robust with respect to the quality of input fingerprint images, an *enhancement algorithm*, which can improve the quality of the ridge structures of input fingerprint images, is thus necessary. Generally, for a given fingerprint image, fingerprint regions can be assigned to one of the following three categories (Fig. 3.22) [78]:

- *Well-defined regions*, in which ridges and furrows are clearly visible for a minutia extraction algorithm to operate reliably.
- *Recoverable corrupted regions*, in which ridges and furrows are corrupted by a small amount of creases, smudges, etc. But they can still be correctly recovered by an enhancement algorithm.
- *Unrecoverable corrupted regions*, in which ridges and furrows are corrupted by such a severe amount of noise and distortion that it is impossible to recover them.

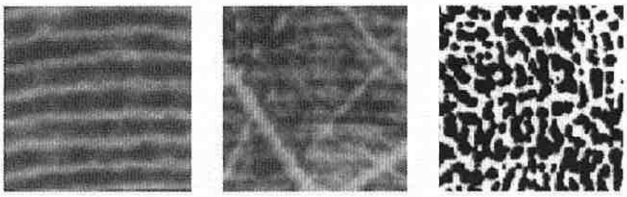


Fig. 3.22: Examples of fingerprint regions [78]: a) Well-defined region; b) Recoverable region; c) Unrecoverable region.

The interoperability among sensors from different vendors, or using different sensing technologies, plays a relevant role. The resulting images from different technologies vary very much in the representation of the grayscale levels, sharpness of valleys and ridges and resolution. Fortunately, it is often possible to compensate these factors to achieve a good interoperability among such sensors, e.g. see [41].

Based on filtering domains, most fingerprint enhancement schemes can be roughly classified using two major approaches [43]: *spatial-domain* and *frequency-domain*. The filtering in a spatial-domain applies a convolution directly to the fingerprint image. On the other hand, the filtering in a frequency-domain needs the Fourier analysis and synthesis. Thus a fingerprint image is transformed, then multiplied by filter coefficients, and in the end inverse-transformed by Fourier coefficients back to an enhanced fingerprint image. In fact, if the employed filters are the same, enhancement results from both domains should be exactly the same according to the signal processing theorem. However, in a practical implementation, these two approaches are different in terms of enhancement quality and computational complexity of algorithms.

In the following subchapters, some important and often used fingerprint enhancement methods will be introduced. Nevertheless, the list of such methods cannot be complete, as the amount of such methods exceeds the scope and possibilities of this thesis.

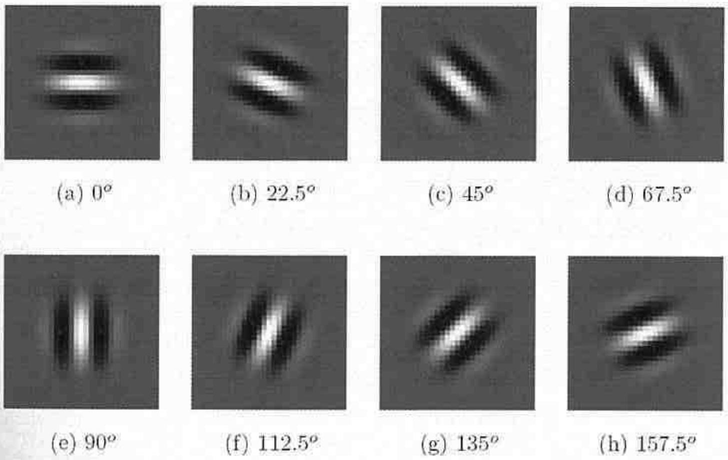
3.2.1 Image Filtering Using Gabor Filters

A 2D Gabor filter [4] can be thought of as a complex plane wave modulated by a 2D Gaussian envelope [81]. These filters optimally capture both the local orientation and frequency information and their development has been initiated by observing the linear response of the receptive field in simple striate cortex cells. By tuning a Gabor filter to a specific frequency and direction, the local frequency and orientation information can be obtained. Thus, they are well suited for extracting the texture information from images. An even symmetric Gabor filter has the following general form in the spatial domain [81]:

$$G_{\theta,f}(x,y) = e^{-\frac{1}{2}\left[\frac{x'^2}{\delta_x^2}+\frac{y'^2}{\delta_y^2}\right]}\cos(2\pi fx') \qquad (3.38)$$

$$\text{and } x' = x\sin\theta + y\cos\theta,\ y' = x\cos\theta - y\sin\theta \qquad (3.39)$$

where f is the frequency of the sinusoidal plane wave at the angle θ with the x-axis, and δ_x and δ_y are the standard deviations of the Gaussian envelope along the x and y axes, respectively.



(a) 0° (b) 22.5° (c) 45° (d) 67.5°

(e) 90° (f) 112.5° (g) 135° (h) 157.5°

Fig. 3.23: Gabor filters in spatial domain with eight different orientations [81].

3.2.2 Spatial Domain Filtering Algorithm

The *spatial domain filtering algorithm* [78] adaptively enhances the clarity of ridge and valley structures using a bank of Gabor filters (see the previous chapter) that are tuned to the local ridge orientation and ridge frequency. The local ridge orientation and ridge frequency are estimated directly from input images in the spatial domain. The main steps of the enhancement algorithm are shown in Fig. 3.24 and are listed below [78]:

- *Normalization.* An input image needs to be normalized so that it has a pre-specified mean and variance. The normalization is a pixel-wise operation, in which an output pixel value depends only on the corresponding input pixel. It does not change the clarity of the ridge and valley structures. The main purpose of normalization is to reduce the variations in gray-level values along ridges and valleys what facilitates the subsequent steps.
- *Local ridge orientation estimation.* The local orientation indicates the major ridge orientation tendency in a local neighborhood. It represents an intrinsic property of a fingerprint image and defines an invariant coordinate for ridges and valleys in a local neighborhood. In neighboring ridges, the local ridge orientation changes

slowly. Therefore, it is usually a specified block-wise property. In addition, there is no difference between a local ridge orientation of 90° and 270°, since the ridges oriented at 90° and the ridges oriented at 270° in a local neighborhood cannot be differentiated from each other.

- *Local ridge frequency estimation.* Local ridge frequency is the frequency of the ridge and valley structures in a local neighborhood along a direction normal to the local ridge orientation. The ridge and valley structures in a local neighborhood, where minutiae or singular points appear, do not form a well-defined sinusoidal-shaped wave. In such situations, the frequency is defined as the average frequency in the neighborhood. The local ridge frequency represents another intrinsic property of a fingerprint image.
- *Estimation of region mask.* The region mask is used to indicate the category of pixels. A pixel could be either a non-ridge-and-valley (unrecoverable) pixel or a ridge-and-valley (recoverable) pixel. A pixel (or a block of pixels) in an input fingerprint image could be either in a recoverable region or in an unrecoverable region. The classification of pixels into recoverable and unrecoverable categories can be performed based on the assessment of the shape of the wave formed by local ridges and valleys.
- *Filtering.* A bank of Gabor filters tuned to the local ridge orientation and ridge frequency is applied to the ridge-and-valley pixels in the normalized input fingerprint image to obtain an enhanced fingerprint image.

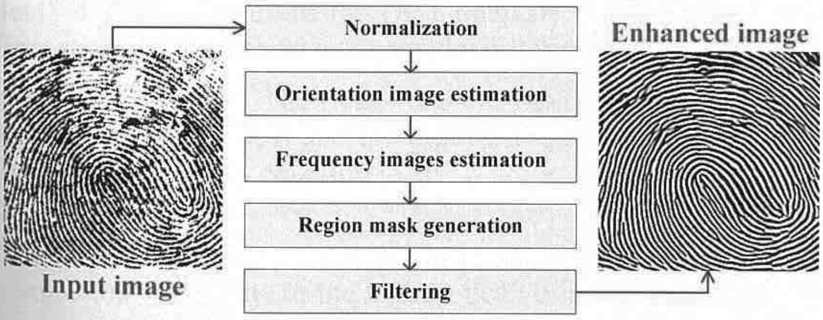


Fig. 3.24: The flowchart of the spatial domain fingerprint enhancement algorithm [37].

3.2.3 Frequency Domain Filtering Algorithm

The fingerprint enhancement approach in a frequency domain introduced in [43] consists of four concatenated processes: discrete cosine transform of sub-blocks of partitioning fingerprint, ridge orientation and frequency parameters estimation, filtering in DCT (Discrete Cosine Transform) domain and inverse discrete cosine transform of sub-blocks. The advantages of the proposed approach are as follows [43]:

- Fingerprint ridges form a natural sinusoid image – its spectrums are packed or localized in a frequency domain. Hence these spectrums can be easily shaped or filtered in this domain. Moreover, a filter can be specially designed in order to handle high curvature ridge area such as singular points. This is a great advantage over the spatial-domain filtering approach.

- When comparing with the discrete Fourier transform, the discrete cosine transform performs better in terms of energy compaction. Moreover, DCT coefficients are real numbers in comparison with complex numbers of discrete Fourier transform (DFT) coefficients. Therefore, we can handle DCT coefficients easier than DFT coefficients. Besides, the fast DCT requires less computational complexity and less memory usage when comparing with the fast Fourier transform (FFT).
- By partitioning a fingerprint into sub-blocks, the proposed approach utilizes the spatially contextual information including the instantaneous frequency and orientation. Intrinsic features such as ridge frequency, ridge orientation, and angular bandwidth can be simply analyzed directly from DCT coefficients.

Conventional fingerprint enhancement schemes, when applied with non-overlapping blocks of partitioning fingerprint, often encounter blocking artifacts such as ridge discontinuities and spurious minutiae [43]. To preserve the ridge continuity and eliminate blocking artifacts, an overlapping block is applied to both DCT decomposition and reconstruction procedures. However, there is no need to apply any smooth spectral window for DCT because the overlapping area is large enough to prevent any blocking effects, corresponding with its energy compaction property.

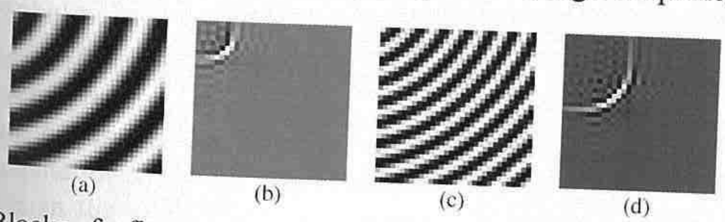
3.2.3.1 Intrinsic Parameter Estimation on DCT Domain

The ridge frequency, ridge orientation, and angular bandwidth can be analyzed from DCT coefficients directly. Therefore the DCT analysis yields an appropriate domain to perform the fingerprint enhancement and provides filtering parameters at the same time.

Ridge frequency estimation: The ridge frequency ρ_0 is simply obtained by measuring a distance between the origin (0,0) and the highest DCT peak of a high frequency spectrum as it suggests the following equation [43]:

$$\rho_0 = \sqrt{u_0^2 + v_0^2} \tag{3.40}$$

where (u_0,v_0) is the coordinate of the highest peak of a high-frequency spectrum.

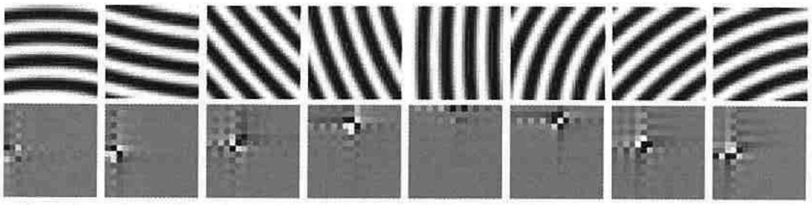


(a) (b) (c) (d)

Fig. 3.25: a) + c) Blocks of a fingerprint model with different frequencies [43]; b) + d) DCT coefficients related to figures a) and c), respectively [43].

Ridge orientation estimation: The dominant orientation of parallel ridges θ is closely related to a peak-angle ϕ in DCT coefficients, where ϕ is measured counterclockwise (if $\phi > 0$) from the horizontal axis to the terminal side of the highest spectrum peak of high frequency (DC spectrum is not included). However, θ and ϕ relationship is not a one-to-one mapping. The ridge orientation, with θ varying in the range of 0 to π, is projected into the peak-angle, with ϕ varying in the range of 0 to $\pi/2$. The relationship between θ_0 or the ridge orientation in spatial domain and ϕ_0 or the peak angle in frequency domain is described by the following equation [43], and presented in some examples in Fig. 3.26.

$$\phi_0 = \tan^{-1}\left(\frac{v_0}{u_0}\right),\ \phi_0 = \left|\frac{\pi}{2} - \theta_0\right|,\ \text{where } 0 \le \theta_0 \le \pi \tag{3.41}$$



$\theta_0=\pi=0$ $\theta_0=7\pi/8$ $\theta_0=3\pi/4$ $\theta_0=5\pi/8$ $\theta_0=\pi/2$ $\theta_0=3\pi/8$ $\theta_0=\pi/4$ $\theta_0=\pi/8$

Fig. 3.26: Examples of the relationship between ridge orientation in spatial domain and peak-angle in DCT domain, all ridge angles relate to the horizontal axis and DC coefficient is set to zero in order to show a high-frequency spectrum [43].

In order to identify the quadrant and avoid the influence of interference, two 2D perpendicular diagonal vectors, V_1 and V_2 [43] are formed, with their size 5×3 pixels and their center at the peak position. The average directional strengths of each vector (S_1,S_2) are then computed by the following equation [43]:

$$S_i = \max_{n=-1,0,1} \frac{\left|\sum_{m=-2}^{2} V_i(u_0+m, v_0+n)\right|}{5},\ \text{where } i=1,2 \tag{3.42}$$

Then the quadrant can be classified and the actual fingerprint ridge orientation can be identified as shown in the subsequent equation [43]:

$$\theta = \begin{cases} \pi/2 - \phi & S_1 \ge S_2 \\ \pi - (\pi/2 - \phi) & otherwise \end{cases} \tag{3.43}$$

Finally, the estimated ridge frequency and orientation of each local region is transformed into a frequency field and an orientation field. Then the Gaussian filter is applied to smooth both global fields in order to reduce noise effect.

Angular bandwidth estimation: In the singularity region, the ridge spectrum is not an impulse but it spreads bandwidth out. Therefore, the desired filter of each block must be adapted depending on its angular bandwidth. This non-coherence factor represents how wide the ridge orientation can be in the block that has more than one dominant orientation. This factor is in the range of 0 to 1, where 1 represents a highly non-coherent or highly curved region and 0 represents a non-oriented region. The *non-coherence factor* can be expressed by the following relation [43]:

$$NC(u_c, v_c) = \frac{\sum_{(i,j)\in W} \left|\sin\left(\theta(u_c, v_c) - \theta(u_i, v_j)\right)\right|}{W \times W} \tag{3.44}$$

where (u_c,v_c) is the center position of the block, (u_i,v_j) are the i^{th} and j^{th} positions of neighboring blocks within $W\times W$, and the angular bandwidth (ϕ_{BW}) can be estimated by the following equation [43]:

$$\phi_{BW}(u_c,v_c) = \sin^{-1}\left(NC(u_c,v_c)\right) \tag{3.45}$$

3.2.3.2 Enhancement Filtering in DCT Domain

In the DCT domain, the filtering process is not simply the same as in the DFT domain [43] which required only the multiplication of coefficients. The Gabor filter is modified in order to cooperate with the DCT domain based on the Cartesian-form representation. The enhancement filtering in the DCT domain can be divided into two arithmetic manipulations, i.e. multiplication and convolution.

Filtering by Multiplication [43]: The enhancement filter can be expressed in terms of the product of separable Gaussian functions what is similar to the frequency-domain filtering technique [43]:

$$F_{fd}(\rho,\phi) = F(\rho,\phi)H_f(\rho)H_d(\phi) \tag{3.46}$$

where $F(\rho,\phi)$ are DCT coefficients in polar-form representation, directly related to DCT coefficients $F(u,v)$ in rectangular-form representation. $F_{fd}(\rho,\phi)$ are DCT coefficients of the filtering output. The $H_f(\rho)$ filter, which performs the ridge frequency filtering in Gaussian shape, is given by [43]:

$$H_f(\rho|\rho_0,\sigma_\rho,Z) = e^{-\frac{(\rho-\rho_0)^2}{2\sigma_\rho^2}}\text{, } \rho_0 = \sqrt{u_0^2+v_0^2}\text{, } \rho_{\min} \le \rho_0 \le \rho_{\max} \tag{3.47}$$

where ρ_0 and σ_ρ are the center of the high-peak frequency group and the filtering bandwidth parameter, respectively. The $\rho_{\min}$ and $\rho_{\max}$ parameters are minimum and maximum cut-off frequency constraints which suppress the effects of lower and higher frequencies such as ink, sweat gland holes or scratches in the fingerprint. Z is a filtering normalization factor depending on the filtering energy result.

The $H_d(\phi)$ filter, which performs the ridge orientation filtering, is given by [43]:

$$H_d(\phi|\phi_0,\sigma_\phi,\phi_{BW}) = \begin{cases} e^{-\frac{(\phi-\phi_0)^2}{2\sigma_\phi^2}} & |\phi-\phi_0| \ge \phi_{BW} \\ 1 & \text{otherwise} \end{cases} \tag{3.48}$$

where ϕ_0 is the peak orientation for the bandpass filter, σ_ϕ is the directional bandwidth parameter, and ϕ_{BW} is the angular bandwidth, given by Eq. (3.45).

Filtering by Convolution [43]: Since θ and π-θ ridge orientation coefficients are projected into the same DCT domain region, both directional coefficients still remain from the previous filtering. In order to truncate inappropriate directional coefficients, two diagonal Gabor filters are exploited by the convolution operation. The finally enhanced DCT coefficients are given by [43]:

$$F_{enh}(u,v) = F_{fd}(u,v) * H_q(u,v) \tag{3.49}$$

where $F_{enh}(u,v)$ are enhanced DCT coefficients in rectangular-form, $F_{fd}(u,v)$ is the previous result of enhanced DCT coefficients in rectangular-form converted from $F_{fd}(\rho,\phi)$ in polar-form. The quadrant correction filter, $H_q(u,v)$, is given by [43]:

$$H_q(u,v) = \begin{cases} \cos\left[\frac{(u+v)\pi}{2}\right] \cdot e^{-\frac{(u+v)^2}{2\sigma_q^2}} & \theta \geq \pi/2 \\ \cos\left[\frac{(u-v)\pi}{2}\right] \cdot e^{-\frac{(u-v)^2}{2\sigma_q^2}} & otherwise \end{cases} \qquad (3.50)$$

where σ_q is the quadratic parameter and $\cos(n\pi/2)$ can attain only one of the three following values: -1, 0 or 1. Indeed, this convolution operation requires less computing because most of bandpass filtered coefficients are truncated to zero from the previous operation. In case of highly curved ridges, the transformed coefficients are projected into widely curved sub-band of the DCT domain as shown in Fig. 3.27.

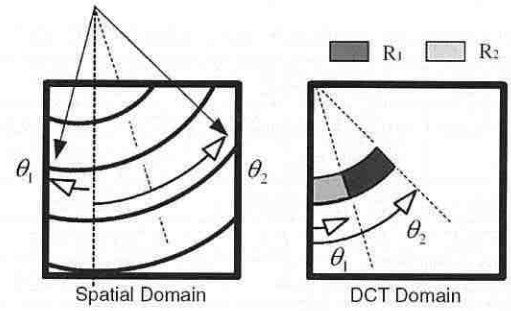


Fig. 3.27: Highly curved ridges in spatial and frequency (DCT) domain. The signal is localized in a widely curved sub-band which can be classified as either the principal region (R_1) or the reflection region (R_2) [43].

From Fig. 3.27, we can approximate the orientation range from θ_1 to θ_2 by a non-coherence factor from Eq. (3.39). The curved sub-band can be classified as one of two regions, either the principal region (R_1) or the reflection region (R_2). The principal region R_1 contains only one diagonal component (45° or 135°) as mentioned before. The 45° or 135° diagonal components correspond to the phase pattern of the oriented ridges in the range of 0° to 90° or 90° to 180°, respectively. The reflection region R_2 is composed of both 45° and 135° diagonal components from the reflection property of DCT coefficients. Then the convolution is applied only in the principal region.

It is then possible to compute a quality index of the fingerprint in the frequency domain [12] which gives us the information about the fingerprint image quality.

3.3 Experimental Results

This chapter contains the introduction of experimental results from the tested devices – the evaluation kit Suprema SFM3000 EVK which was used for the image quality testing – it is a development kit base board which can cooperate with other sensor units listed in the following overview (Fig. 3.28). The evaluation kit including all four sensor units has been lent by the company Digitus[1] and all components have been placed in the biometric laboratory at the Department of Intelligent Systems, FIT BUT[2].

[1] http://www.digitus.cz
[2] http://www.fit.vutbr.cz

At the beginning of this chapter, there is a short description of used devices (Fig. 3.28 and Tab. 3.1) followed by the description of biometric samples collection (corpus collection, i.e. a database of fingerprints) and the achieved results are shown in the end.

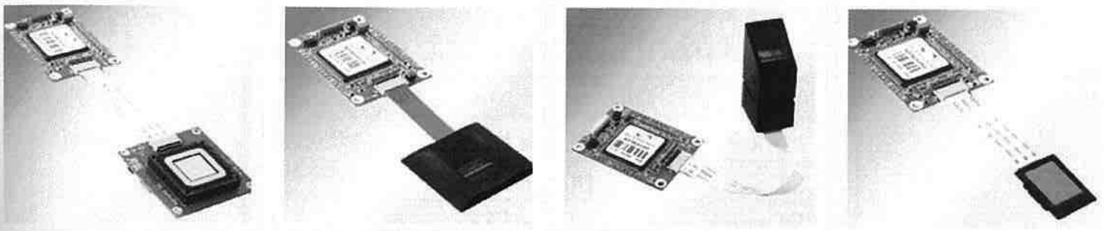


Fig. 3.28: Suprema scanners (SFM3000, SFM3010, SFM3020, SFM3050).

Tab. 3.1: Features of Suprema sensor units.

Model / Features	**SFM3000**	**SFM3010**	**SFM3020**	**SFM3050**
Sensor	FingerLoc AF-S2 by AuthenTec	FingerChip by Atmel®	not known	TouchChip® TCS2 by UPEK
Technology [Dra25]	e-field	thermal, sweep	optical	capacitive
Power supply	3.3 V (DC)	3.3 V (DC)	3.3 V (DC)	3.3 V (DC)
Take-off current	100 – 300 mA	4.5 mA	not known	not known
Resolution [DPI]	250	500	500	500
Sensor size [mm]	13 × 13	11.6 × 0.4	16 × 19	10.4 × 14.4
Module size [W×D×H] [mm]	55 × 40 × 8	55 × 40 × 8	55 × 40 × 8	55 × 40 × 8
Image size [pix.]	128 × 128	360 × 500	272 × 320	256 × 360

The results of fingerprint acquirement have been saved into a database of fingerprints. This database includes the fingerprints from 30 users; each person has provided the fingerprints from both hands and all fingers except of little fingers (these are generally not used in the access system – it often happens that these fingers are placed wrongly on the scanner platen due to their size; a small finger contains a smaller amount of significant information). Each user put all four fingers on both hands 5 times on each sensor. Thus each user provided 160 fingerprints which have been stored in the database. The size of the full database is 4,800 fingerprints (its volume is approximately 650 MB).

All fingerprint images have been visually checked one by one; the criterion for rejection was the fingerprint area smaller than one half of the image (images containing fingerprint on three quarters of the area were preferred). The second factor for rejection was associated with smudged or blurred papillary lines (due to the high perspiration of hands). The number of rejected images for each sensor is shown in Tab. 3.7.

3.3.1 Determination of Contrast Ratios

The Michelson contrast (Eq. (3.6)) was used for the computation of contrast in the images for this metrics. The values of local intensity differences have been computed according to the definition. After averaging them we obtained the global image contrast.

The local intensity differences were determined on specific parts (regions) of the image in a predefined range. What concerns various input sizes, it has been decided to determine the local differences in corresponding sizes of partial regions; their size was set in accordance to the size of the whole image. The exact values are shown in the Tab. 3.2.

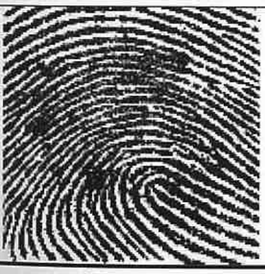
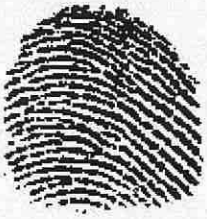
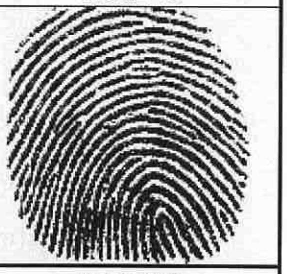
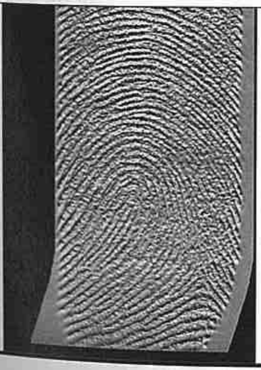
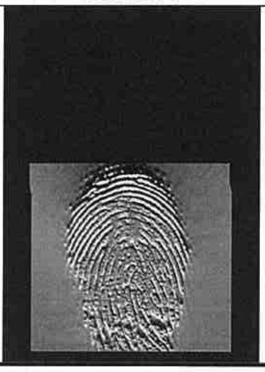
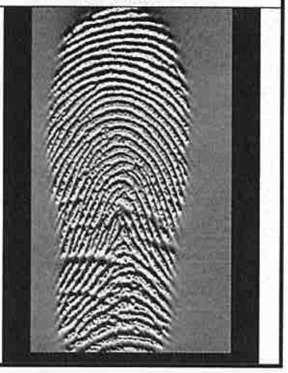
Tab. 3.2: Region sizes [Dra16].

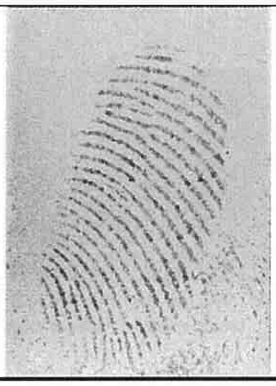
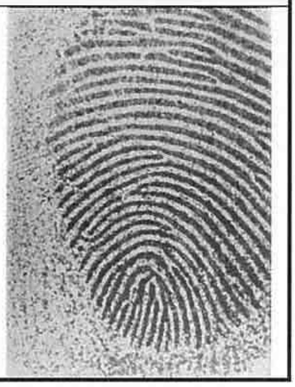
Module	Output resolution	Region size
SFM3000	128 × 128	8 × 4
SFM3010	360 × 500	15 × 12
SFM3020	272 × 320	15 × 12
SFM3050	256 × 360	15 × 12

Generally, it is very difficult to determine the exact contrast values which should be contained in the images. It depends strongly on the quality of the recognition algorithm, which should be able to recognize the images correctly with low contrast ratios. Thus the more contrast the sensor provides, the better is the separation of papillary lines from background and therefore the higher quality is achieved at the input of the recognition algorithm. The maximal value for the contrast is 1.0. The more these sensors can approach this value, the better image output is achieved. The fingerprint quality is closely related to this metric. The bigger finger area is scanned, the higher contrast is reached and therefore the image quality is also better.

The measured values are shown in Tab. 3.3. The enclosed image examples contribute to the visualization of this concept. These images correspond to the individual values for each sensor. The distribution of global contrast ratios for all sensors is shown in Fig. 3.29.

Tab. 3.3: Contrast ratios for all sensors (maximal, minimal and average) [Dra16].

Sensor	Maximal contrast	Minimal contrast	Average contrast
SFM3000	1.00000	0.57617	0.88245
			
SFM3010	0.78748	0.31206	0.60955
			

SFM3020	0.98441	0.50792	0.80456
SFM3050	0.58689	0.26393	0.45023
			

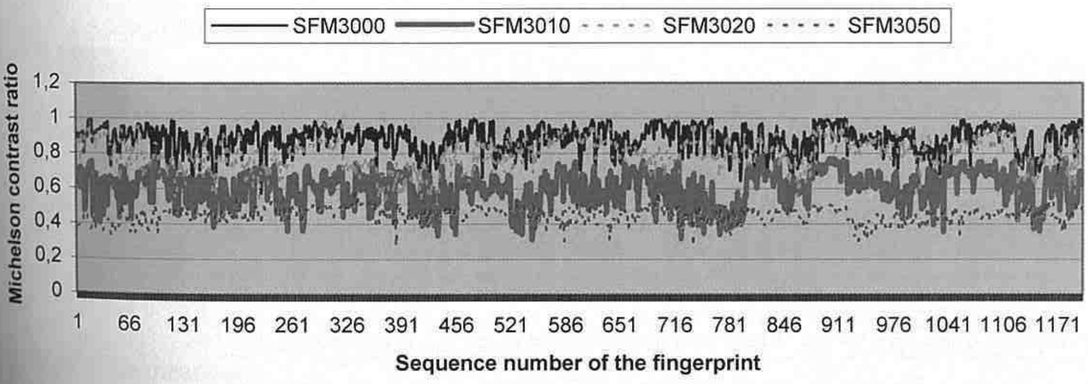


Fig. 3.29: Michelson contrast ratios for all sensors [Dra16][Dra09].

3.3.2 Mean Value of Grayscale Levels

This method expresses the ability of the sensor to distinguish background and papillary lines from each other. Two clearly recognizable peaks can be found normally in the image histogram, which represent the background and papillary lines.

The graphs presenting the complete deviation values in all measured samples are shown in Fig. 3.30 through 3.33 (the blue color corresponds to the mean value of gray grades for each image from respective sensor; the violet color corresponds to the average value).

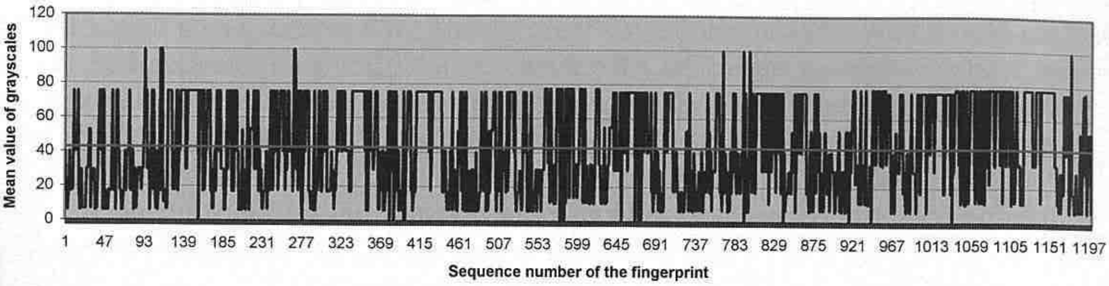


Fig. 3.30: The mean value of grayscale values for the sensor Suprema SFM3000 (average ≅ 43) [Dra16][Dra09].

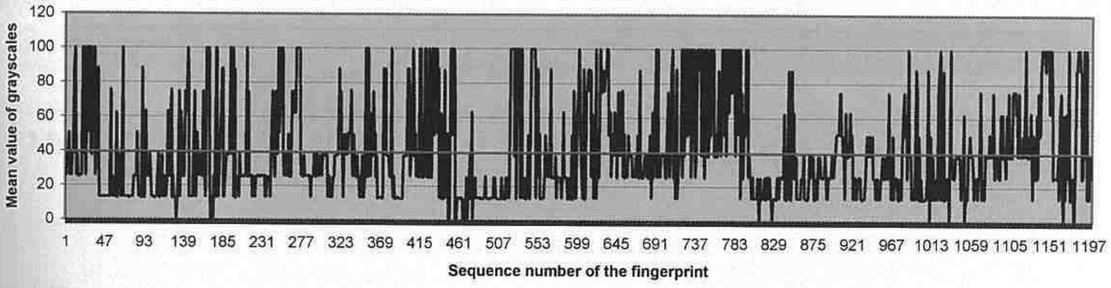


Fig. 3.31: The mean value of grayscale values for the sensor Suprema SFM3010 (average ≅ 40) [Dra16][Dra09].

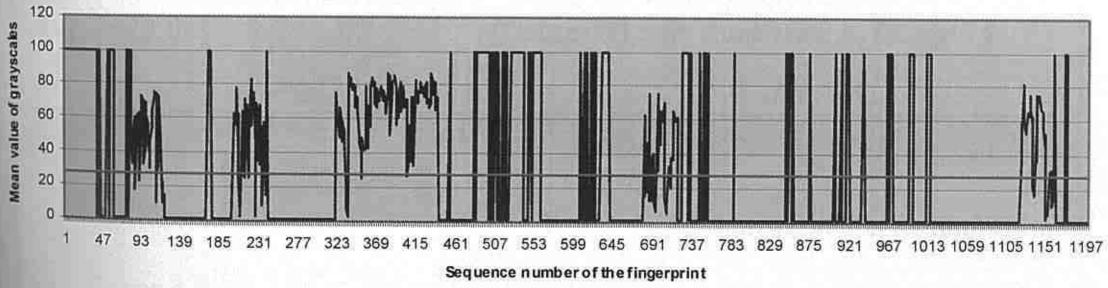


Fig. 3.32: The mean value of grayscale values for the sensor Suprema SFM3020 (average ≅ 28) [Dra16][Dra09].

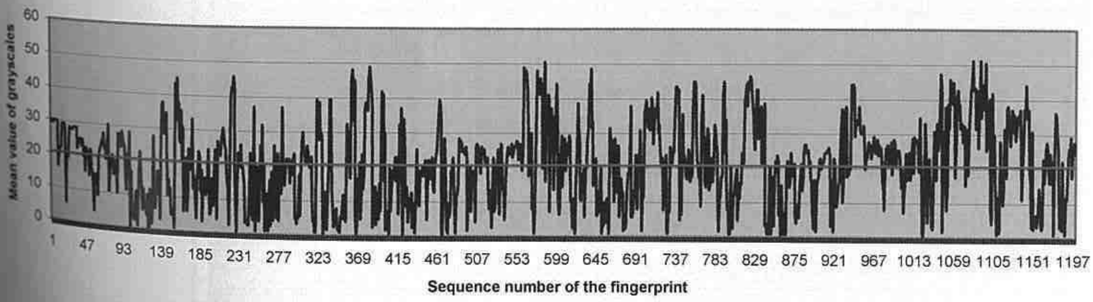
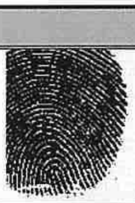
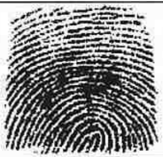
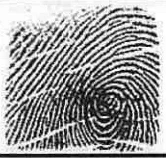
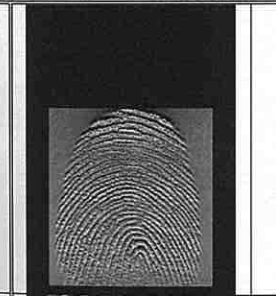
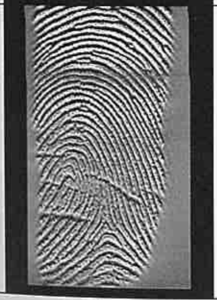
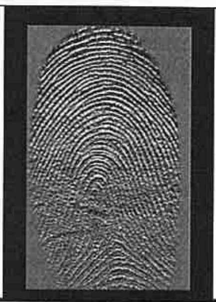
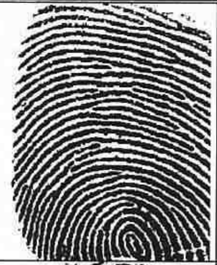
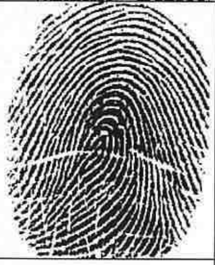
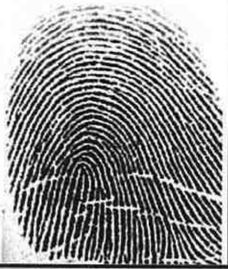
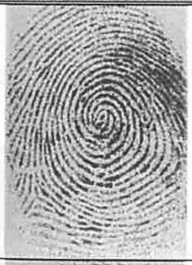
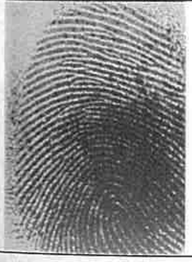


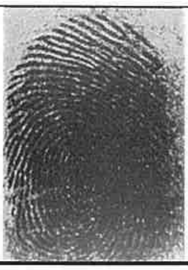
Fig. 3.33: The mean value of grayscale values for the sensor Suprema SFM3050 (average ≅ 21) [Dra16][Dra09].

The real evaluation rank of each sensor may not be clearly visible from the above results. Although some sensors have shown great deviations and therefore would not pass through the tolerance limit of 20% (see chapter 3.1.2.3), their histograms show insufficient resolution. The results come out from a precise histogram analysis where the method does not offer suitable resolution in sparse histograms. These histograms have strong non-uniform distribution but both peaks which determine papillary lines and background are nevertheless visible, whereas other smaller peaks are nearly insignificant. It is therefore very important to interpret the histograms correctly. The fully relevant results have been achieved only with the sensor SFM3050 which provides the outputs with a fully valuable histogram.

Tab. 3.4: Maximal, minimal and average deviation values for mean values of grayscales [Dra16].

Sensor SFM3000			
Max	100.0		user 03, right hand, ring finger, image 02
Min	0.392		user 15, left hand, thumb, image 04
Avg	43.0		user 02, left hand, thumb, image 04
Sensor SFM3010			
Max	100.0		user 01, right hand, index finger, image 01
Min	0.781		user 12, left hand, thumb, image 02

Avg	39.8		user 01, left hand, middle finger, image 05
Sensor SFM3020			
Max	100.0		user 01, right hand, thumb, image 01
Min	0.392		user 02, left hand, middle finger, image 02
Avg	27.7		user 18, left hand, middle finger, image 01
Sensor SFM3050			
Max	51.2		user 28, right hand, index finger, image 01
Min	0.00		user 03, right hand, index finger, image 02

Avg	20.6		user 02, right hand, index finger, image 03

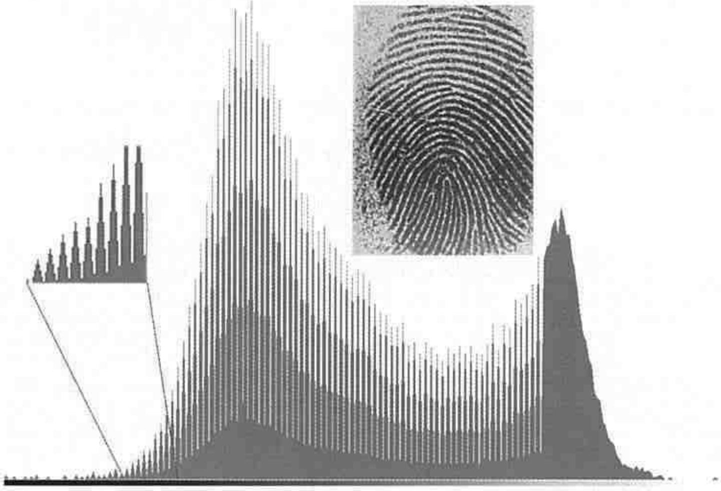


Fig. 3.34: Histogram of the sensor SFM3050 (only a half of the x-axis is used) [Dra16][Dra09].

Some interesting aspects could be seen in the test data from the sensor SFM3050 – the incompleteness of histogram from acquired images – see Fig. 3.34. The basic line imitates the expected curve but when subjected to a detailed analysis, it can be seen that each second value is zero. The effectiveness of the sensor is evidently not influenced by this fact, but the question is why the sensor performs such a strict filtering.

3.3.3 Number of Papillary Lines

This metrics has been slightly modified for fingerprints from biometric access systems (the delta point is often missing here). The term "RIP Count" will not be considered as defined in chapter 3.1.3 but the definition for calculation of the amount of papillary lines in horizontal and vertical directions will be exploited. In general, it can be stated that the higher the density of papillary lines in the image is, the more accurate is the process of recognition – this reflects the relationship to the amount of information in the image (see chapter 3.1.3). The density depends directly on the scanning area of the sensor.

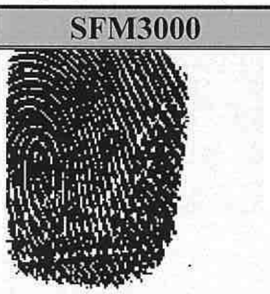
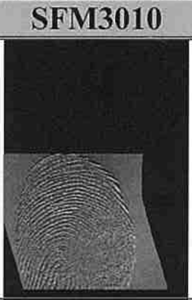
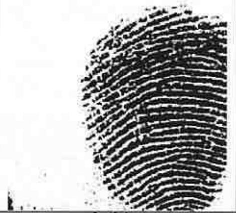
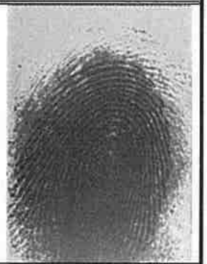
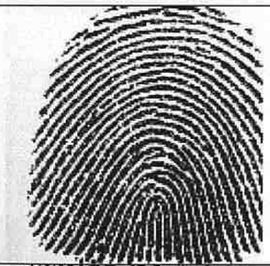
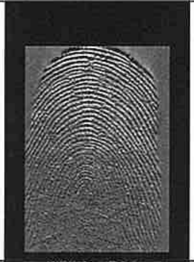
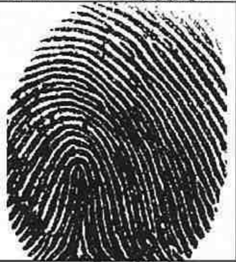
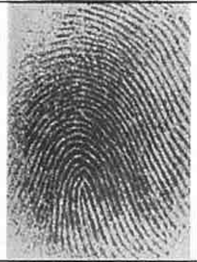
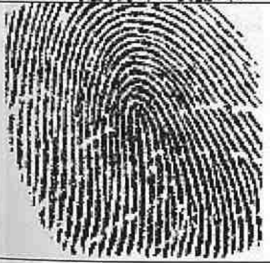
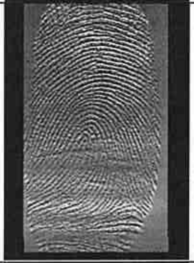
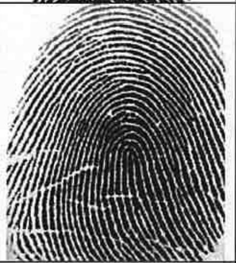
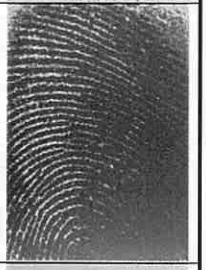
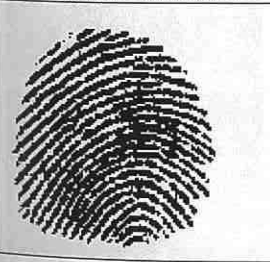
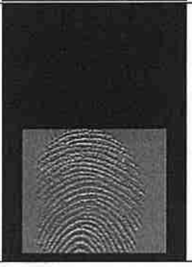
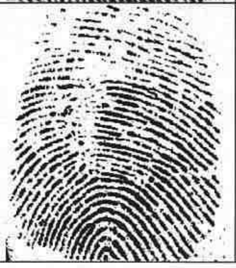
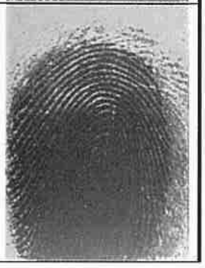
Some external values may not correspond to the real state. Due to a lower quality of certain images, it was not possible to exploit the fully automatic detection of papillary lines – see problems described in chapter 3.1.3. It is necessary to say that the application of a suitable filter would improve this situation but this exceeds the scope and purpose of this test. In addition, the application of such filter would distort the information about real quality of images supplied by the sensor. The measured values of the number of papillary lines in horizontal and vertical directions are summarized in the Tab. 3.5.

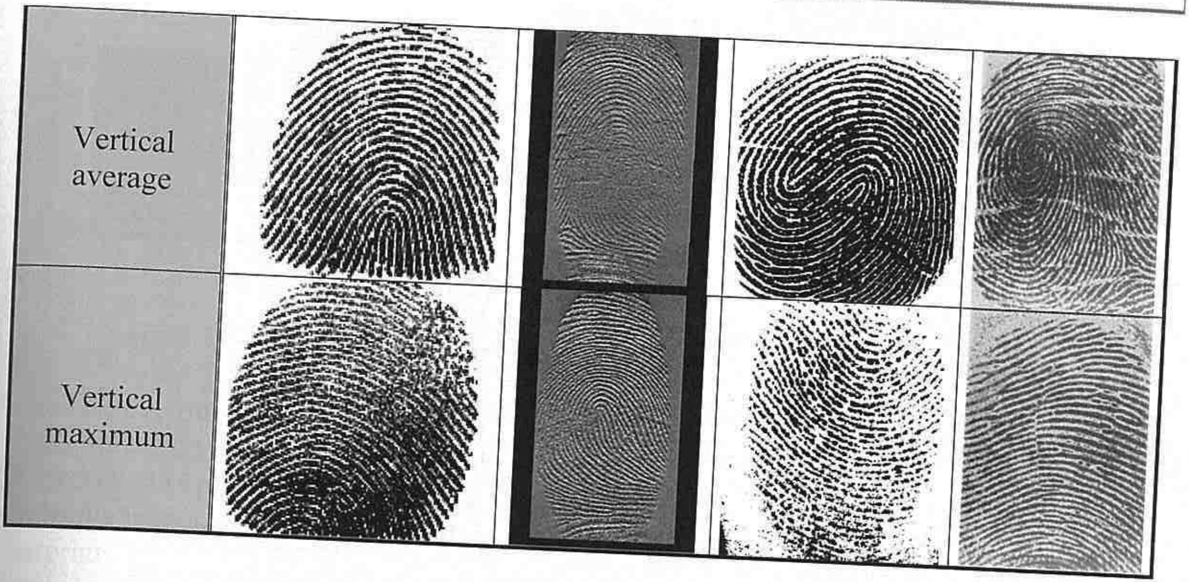
Tab. 3.5: Average, maximal and minimal numbers of papillary lines [Dra16][Dra09].

Sensor	SFM3000	SFM3010	SFM3020	SFM3050
Horizontal minimum	6.00	6.00	9.00	10.00
Horizontal average	12.86	19.30	19.93	21.25
Horizontal maximum	23.00	27.00	30.00	31.00
Vertical minimum	5.00	3.00	11.00	11.00
Vertical average	13.26	33.18	22.79	25.67
Vertical maximum	24.00	51.00	31.00	37.00

Tab. 3.6 depicts specific fingerprints corresponding to the minimal, average and maximal numbers of papillary lines from Tab. 3.5.

Tab. 3.6: Specific fingerprints corresponding to the significant numbers of papillary lines [Dra16].

Sensor	SFM3000	SFM3010	SFM3020	SFM3050
Horizontal minimum				
Horizontal average				
Horizontal maximum				
Vertical minimum				



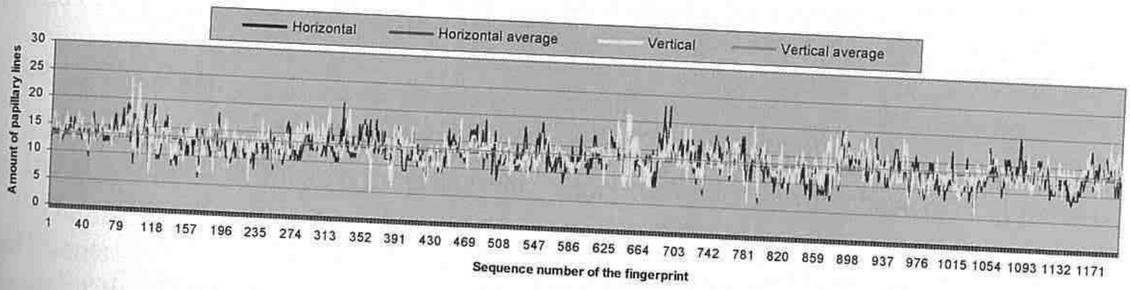


Fig. 3.35: Numbers of papillary lines for the sensor SFM3000 [Dra16][Dra09].

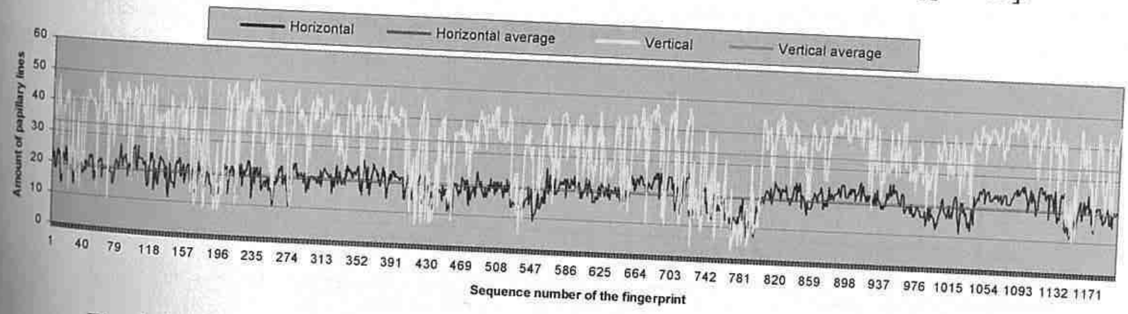


Fig. 3.36: Numbers of papillary lines for the sensor SFM3010 [Dra16][Dra09].

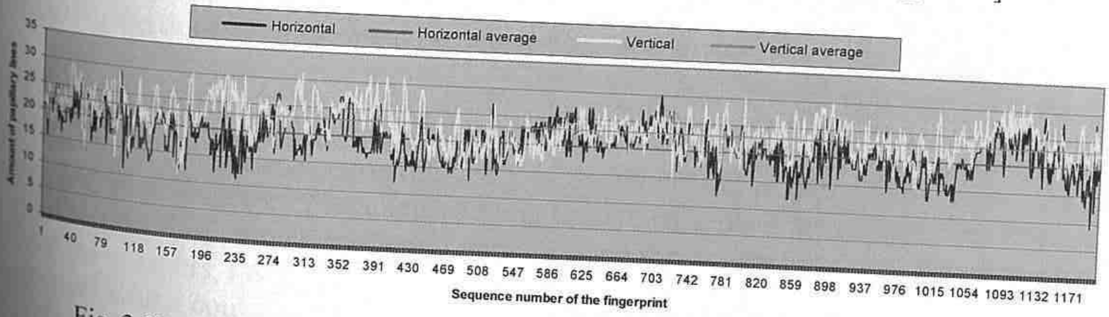


Fig. 3.37: Numbers of papillary lines for the sensor SFM3020 [Dra16][Dra09].

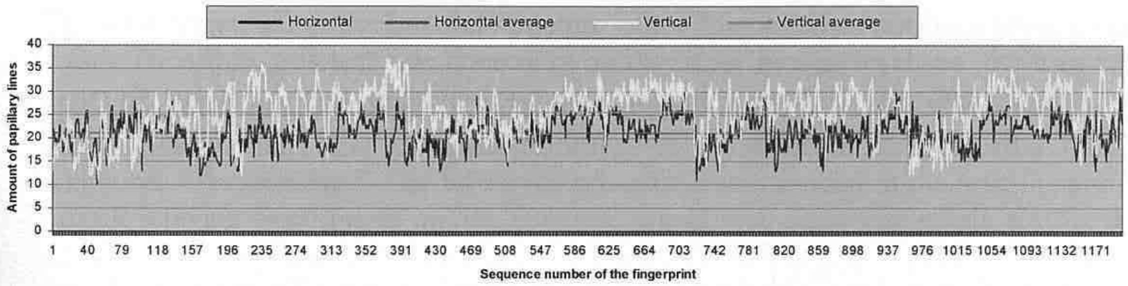


Fig. 3.38: Numbers of papillary lines for the sensor SFM3050 [Dra16][Dra09].

The determination of one concrete value of the number of papillary lines in the defined direction is very specific and this value is sometimes impossible to determine. However, it is possible to compute a long-term average for each sensor. If the actual value from the presented finger differs from such average, it could mean that the provided fingerprint does not have a sufficient quality and therefore a new fingerprint should be acquired once again (see Fig. 3.35 to Fig. 3.38).

3.3.4 FTA Rate

The satisfaction of users is closely associated with the FTA rate, but it depends also on the algorithms for fingerprint processing which follow after the phase of acquirement.

The users, who participated on the creation of the database of fingerprints, recorded the events when the sensor had not responded to scanning and/or had not acquired any image or the image had not contained a fingerprint although the user applied a finger on the scanning area of the sensor. Some of these users recorded strongly biased or damaged fingerprints without feeling any responsibility for such results. All these results have been put together in Tab. 3.7.

Tab. 3.7: The FTA rates and percentages of fingerprints with a poor quality [Dra09].

Sensor / Rate	FTA [%]	Fingerprints with a poor quality [%]
SFM3000	0.595	7.500
SFM3010	2.140	15.120
SFM3020	0.000	5.710
SFM3050	0.120	5.600

The best results have been achieved with the sensor SFM3020, the second best was SFM3050, the third SFM3000 and the worst was SFM3010.

3.3.5 Compatibility

In addition to the comparison of quality of the outputs from individual sensors, the interoperability of fingerprint templates among individual sensors was tested. The base station SFM3000 EVK, which processed and analyzed the fingerprints, was the same for all fingerprint scanners, i.e. the structure of the template was in any case the same. The only parameters which could have been changed were the resolution of the sensor and the way of presentation (contrast, etc.) of the fingerprint.

The information about the internal structure of the template has not been made available to us. Therefore, this test was done only on the experimental level, i.e. the user was registered by one sensor and respective template was transferred to other three sensors.

The test was realized only with three samples – it was sufficient with regard to the result which has been achieved. The following procedure was applied in the test: the enrolment of all relevant fingerprints on one concrete sensor was done first of all; further the scanner module was replaced by another scanner module one by one and it was tested whether the relevant information from the enrolled fingerprint (stored in the template) enables a successful authentication on a specific replaced scanner module currently in use. This procedure was performed for all combinations of sensors and tested users. The results are summarized in Tab. 3.8. The letters have no quality-related meaning; they serve only as a connection to the legend.

Briefly summarized, it was not possible, with a single exception, to make a successful verification on another sensor. This single exception was the combination of sensors SFM3050 (enrolment) and SFM3020 (authentication). With approximately 50% probability, it was finally possible to verify certain samples but only after a maximum effort and multiple repetitions. The conclusion is that the modules do not provide sufficiently reliable compatibility required for the replaceability (interoperability) of individual sensors.

Small remark at the end – nearly all sensors had problems with biased (slightly distorted) images. The deformations emerge after the application of finger on the scanner area and subsequent small movement, what is a quite frequent phenomenon. A very small movement resulted already in so big fingerprint deformation that the sensors were not able to process the fingerprint.

Tab. 3.8: Evaluation of the interoperability of the sensors [Dra09].

		Verification (authentication)			
	Scanner	SFM3000	SFM3010	SFM3020	SFM3050
Enrolment	SFM3000	A	---	---	---
	SFM3010	---	A	---	---
	SFM3020	---	---	B	---
	SFM3050	---	---	C	D

Legend:

A ⇒ Quick and comfortable enrolment and verification, perfect hit rate

B ⇒ More demanding enrolment for the user; possible rotations ±90°; verification practically without problem

C ⇒ Fingers had to be placed in the same position and direction

D ⇒ If the finger is placed in an ideal position and the fingerprint has a good quality, it works; possible rotations ±50°

4. Liveness Detection

The biometric systems using fingerprint recognition technologies have been introduced in the previous two chapters. The functionality of such systems is influenced not only by the used technology, but also by the surrounding environment (including skin diseases). Biased or damaged biometric samples (fingerprint images in our case) could be rejected after revealing their poor quality, or may be enhanced, what leads to the situation that samples, which would be normally rejected, are accepted after the enhancement process. But this process could present also a risk, because the poor quality of a sample could be caused not only by the sensor technology or the environment, but also by using an artificial biometric attribute (imitation of a finger(print)). Such risk is not limited just to the deceptional technique (see chapter 4.1), but if we are not able to recognize whether an acquired biometric sample originates from a genuine living user or an impostor, we would then scan an artificial fake and try to enhance its quality using an enhancement algorithm. After a successful completion of such enhancement, such fake fingerprint would be compared with a template and if a match is found, the user is accepted, notwithstanding the fact that he can be an impostor! Therefore the need of careful liveness detection, i.e. the recognition whether an acquired biometric sample comes from a genuine living user or not, is crucial.

This chapter is organized in a logical manner. First, the basic risks related to a biometric system and reasons for the liveness testing necessity are discussed. Then the basic information on certain measurable human body attributes, suitable for liveness detection, is introduced, together with concrete liveness detection methods applicable for fingerprint recognition systems. At the end, some experimental results achieved in our biometric laboratory are presented.

4.1 Basic Risks and Need for Liveness Testing

To satisfy identification or verification tasks, biometric systems have to withstand various types of attacks. Nevertheless, the convenience and speed are often preferred to the security [48]. However, it is reasonable to seek a compromise between acceptable levels of security and convenience.

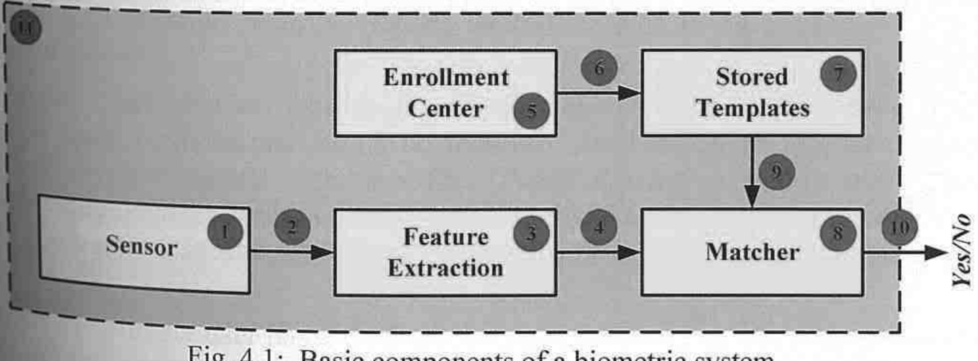


Fig. 4.1: Basic components of a biometric system.

Each component of a biometric system presents a potentially vulnerable part of such system. The typical ways of deceiving a biometric system are as follows (Fig. 4.1) [20][36][3][21]:

1. *Placing fake biometrics on the sensor*. A real biometric representation is placed on the device with the aim to achieve the authentication, but if such representation has been obtained in an unauthorized manner, such as making a fake gummy finger, an iris printout or a face mask, then it is considered as a deceiving activity.
2. *Resubmitting previously stored digitized biometric signals* (*replay attack*). A digitized biometric signal, which has been previously enrolled and stored in the database, is replayed to the system, thus circumventing the acquisition device.
3. *Overriding the feature extraction process*. A pre-selected template is produced in the feature extraction module using a Trojan horse.
4. *Tampering with the biometric feature representation*. During the transmission between the feature extraction and matching modules, a fraudulent feature set replaces the template acquired and processed by the device.
5. *Attacking the enrollment center*. The enrollment module is also vulnerable to spoof attacks such as those described in the previous points 1 to 4.
6. *Attacking the channel between the enrollment center and the database*. During the transmission, a fraudulent template replaces the template produced during the enrollment.
7. *Tampering with stored templates*. A template, previously stored in the database (distributed or not), can be modified and used afterward as corrupted template.
8. *Corrupting the matcher*. A pre-selected score is produced in the matching extraction module using a Trojan horse.
9. *Attacking the channel between the stored templates and the matcher*. During the transmission between the database and the matching module, a fraudulent template replaces the template previously stored.
10. *Overriding the final decision*. The result of the decision module can be modified and then used for the replacement of the output obtained previously.
11. *Attacking the application*. The software application can also be a point of attack and all possible security systems should be used to reduce the vulnerability at this level.

From the above list of possible attacks we can deduce that most security risks or threats are quite common and could be therefore resolved by traditional cryptographic tools (i.e. encryption, digital signatures, PKI (*Public Key Infrastructure*) authentication of communicating devices, access control, hash functions, etc.) or by having vulnerable parts at a secure location, in tamper-resistant enclosure or under constant human supervision [48].

When a legitimate user has already registered his finger in a fingerprint system, there are still several ways how to deceive the system. In order to deceive the fingerprint system, an attacker may put the following objects on the fingerprint scanner [64][3][79]:

- *Registered (enrolled) finger*. The highest risk is that a legitimate user is forced, e.g. by an armed criminal, to put his/her live finger on the scanner under duress. Another risk is that a legitimate user is compelled to fall asleep with a sleeping drug in order to make free use of his/her live finger. There are some deterrent techniques against similar crimes, e.g. to combine the standard fingerprint authentication with another method such as a synchronized use of PINs or identification cards; this can be helpful to deter such crimes.
- *Unregistered finger* (*an impostor's finger*). An attack against authentication systems by an impostor with his/her own biometrics is referred to as a non-effort forgery. Commonly, the accuracy of authentication of fingerprint systems is evaluated by the false rejection rate (FRR) and false acceptance rate (FAR) as mentioned in the previous chapters. FAR is an important indicator for the security against such method (because a not enrolled finger is used for authentication). Moreover, fingerprints are usually categorized into specific classes [14]. If an attacker knows what class the enrolled finger is, then a not enrolled finger with the same class (i.e. similar pattern) can be used for the authentication at the scanner. In this case, however, the probability of acceptance may be different when compared with the ordinary FAR.
- *Severed fingertip of enrolled finger*. A horrible attack may be performed with the finger severed from the hand of a legitimate user. Even if it is the finger severed from the user's half-decomposed corpse, the attacker may use, for criminal purposes, a scientific crime detection technique to clarify (and/or enhance) its fingerprint.
- *Genetic clone of enrolled finger*. In general, it can be stated that identical twins do not have the same fingerprint, and the same would be true for clones [64]. The reason is that fingerprints are not entirely determined genetically but rather by the pattern of nerve growth in the skin. As a result, such pattern is not exactly the same even for identical twins. However, it can be also stated that fingerprints are different in identical twins, but only slightly different. If the genetic clone's fingerprint is similar to the enrolled finger, an attacker may try to deceive fingerprint systems by using it.
- *Artificial clone of enrolled finger*. More likely attacks against fingerprint systems may use an artificial finger. An artificial finger can be produced from a printed fingerprint made by a copy machine or a DTP technique in the same way as forged documents. If an attacker can make then a mold of the enrolled finger by directly modeling it, he can finally also make an artificial finger from a suitable material. He may also make a mold of the enrolled finger by making a 3D model based on its residual fingerprint. However, if an attacker can make an artificial finger which can deceive a fingerprint system, one of the countermeasures against such attack is obviously based on the detection of liveness.
- *Others*. In some fingerprint systems, an error in authentication may be caused by making noise or flashing a light against the fingerprint scanner, or by heating up, cooling down, humidifying, impacting on, or vibrating the scanner outside its environmental tolerances. Some attackers may use such error to deceive the system. This method is well known as a "fault based attack" (e.g. denial of service), and

may be carried out by using one of the above mentioned techniques. Furthermore, a fingerprint image may be made protruding as an embossment on the scanner surface, if we spray some special material on such surface.

Many similar attacks are documented in the literature, including all the above mentioned types. In this chapter, however, we will focus only on finger(print) fakes. One example of the attack on fingerprint technology has been presented in [57]. Hackers in the club-magazine "Die Datenschleuder" (4,000 copies in one edition) have printed a fingerprint of the thumb from the right hand of the German minister of the interior – Dr. Wolfgang Schäuble, and invited readers to make a fake finger(print) of the minister and to try to pretend that their identity is those of the minister. This could be considered as a bad joke, as a fingerprint also serves as a conclusive proof of a person's identity. A hacker has acquired this fingerprint from a glass after some podium discussion. Nevertheless, biometric travel documents (issued in Germany starting from 2007, to be issued in the Czech Republic from 2009), enforced not only by Dr. Schäuble, should be protected just against this situation. The implementation of fingerprints into the travel documents was prescribed by a direction of the European Union in 2004.

It is clear from [64] that the production of a fake finger(print) is very simple (see chapter 4.3.1). Our own experiments have shown that to acquire some images (e.g. from glass, CD, film or even paper) is not very difficult and, in addition, such image could be enhanced and post-processed, what leads to a high-quality fingerprint. The following production process of a fake finger(print) is simple and can be accomplished in several hours. After that, it is possible to claim the identity as an impostor user and common (nearly all) fingerprint recognition systems confirm this false identity supported by such fake finger.

Therefore, the application of liveness detection methods is a very important task, and should be implemented (not only) in all systems with higher security requirements, such as border passport control systems, bank systems, etc. The biometric systems without the liveness detection could be fooled very easily and the consequences might be fatal.

The security of a biometric system should never be based on the fact that biometric measurements are secret, because biometric data can be easily disclosed. Unlike typical cryptographic measures where a standard challenge–response protocol can be used, the security of a biometric system relies on the difficulty of replicating biometric samples [48]. This quality known as the *liveness* ensures that the measured characteristics come from a live human being and are captured at the time of verification. We should realize that any testing of liveness is worthless unless the capture device and communication links are secure. Due to the fact that a biometric system uses physiological or behavioral biometric information, it is impossible to prove formally that a capture device provides only genuine measurements. Consequently, it cannot be proven that a biometric system as a whole is fool-proof [48]. Each solution of this problem has its own advantages and disadvantages; it is more suitable for a certain particular type of the biometric system and environment than for other. Some solutions are software-based; other require a hardware support. Methods which combine both approaches can also be used.

4.1.1 Susceptibility to Fakes

The term "*fake samples*" (e.g. fake finger(print)) [48][64] may be widely used with reference to biometric samples which are used to deceive biometric systems. However, the term "*artificial samples*" (e.g. artificial fingerprint) [48][64] (Fig. 4.2) corresponds to biometric samples which are entirely artificially produced. Mathematically, "artificial samples" represent a subset of "fake samples", because the set "fake samples" may also include modifications of live samples [48][64], e.g. "artificial samples" are fingerprints produced from a mold, but the set "fake samples", contains also injured or otherwise modified live fingers and biometric samples. In addition, the term "*live samples*" [48][64] denotes biometric samples which represent a part of living bodies and the term "*spoofing*" [48][64] denotes the process of defeating a biometric system through the introduction of fake samples.

In the case of either an incorrect liveness testing implementation or a vital quality absent at all, there are two basic risks [48][36]: attacks in the enrollment phase and attacks in the verification phase.

The traditional authentication used during the enrollment process should be stronger than all subsequent verifications, because each of the subsequent verifications depends upon the strength of authentication and the quality of biometric samples acquired during enrollment. However, in many biometric implementations the enrollment process may become a weak link.

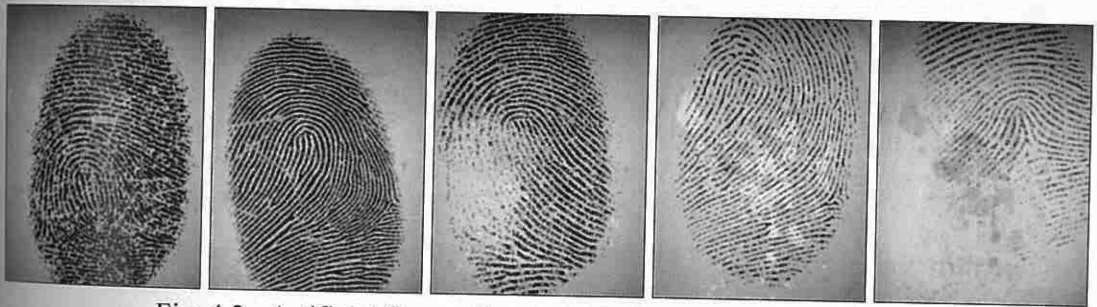


Fig. 4.2: Artificial fingerprints generated by SFinGe [115][114].

Since the enrollment process associates the user's identity with captured biometric samples, adversaries can use two general ways to exploit or misuse the enrollment process and afterwards to defeat a biometric system using the following methods [48]:

- enroll with a false identity
- enroll their identity with a poor master template.

To overcome the former problem, a high level of assurance in the initial authentication process must be guaranteed. Most biometric systems employ a trained enrollment administrator to guard verification of the user's identity based on exogenous identifiers [48]. However, the trained personnel may also be corrupt. In such cases or when a biometric system relies on self-enrollment, a liveness testing should be implemented. It should be maintained that the strength of initial verification is always higher than the strength of subsequent verification, or otherwise adversaries can establish a false relationship between the user identity and biometric samples. As a result, they can use the biometric system as an entrance for dishonest purposes without any problem.

Even though the initial verification process was honestly performed, there still remains a significant risk which could be employed by the attacker. This is a type of risk, when the generated master template would not exactly represent the subject. The master template, this way affected, may be too "quiet" or too "noisy". Both of which would allow an adversary to pose an "*evil twin*" [48] of the individual with the poor template. For example, a "quiet" master template would be created if there were poor lighting conditions during enrollment in the case of a facial recognition system. If a biometric system was allowed to create such master template then an adversary could darken the lighting conditions (e.g. switch off the lamp) during verification to easily impersonate the enrollee. The "noisy" template is similar to the above mentioned, i.e. significant movement of the subject during enrollment could allow someone to pose as an "evil twin" by moving suddenly during verification. In these cases, the template matching algorithm might accept two blurred samples as a match.

Poor templates are closely related with the FTE (*Failure To Enroll*) category, where the user's injury or disability prevents the generation of normal master templates. Also environment modifications (e.g. heat, weather, humidity etc.) during enrollment could pose a random element into templates that adversaries could exploit later. A principal solution against the threats or risks discussed is a suitable quality control during the initial process of biometric sample acquisition (chapter 3.2). If the quality is insufficient, the capture device must repeat the capture of respective biometric sample. If it is possible, the same environmental conditions and also the same type of capture device should be guaranteed to minimize differences between enrollment phase and subsequent verifications. Nevertheless, from our point of view the liveness testing could also pose a partial solution, when e.g. during verification an impostor moves his finger to present a blurred fingerprint and to impersonate the enrollee, but the liveness detection module could not check the pulse and therefore, a biometric system determines the finger as an artificial one and transmits a negative decision.

The implications of this demonstrable susceptibility to spoofing – defeating a biometric system through fake biometric samples (e.g. Fig. 4.3) – include the following [28]:

- Fake finger attacks may be mounted against existing enrollments in order to gain access to a protected facility, computer, or other resource.
- A fake finger may be used for authentication at a given computer or border crossing in order to fraudulently associate an audit trial with an unwitting individual.
- A fake finger may be used to enroll in a biometric system and then be shared across multiple individuals, thereby undermining the entire system.
- An individual may repudiate transactions associated with his account or enrollment – claiming instead that they are the result of attacks – due to the inability of the biometric system to ensure liveness.

Given biometrics' widespread acceptance [28] as a solution for a range of public and private sector applications such as civil identification, network security, border control, and point of sale authentication, the question of liveness detection in leading biometric technologies must be addressed.

The concept of liveness detection can be framed by considering the detection of liveness versus the detection of non-liveness [28]. Biometric systems are comprised of acquisition elements and processing elements. Acquisition elements record, image, or otherwise capture raw data: fingerprints, facial images, photographs, etc. Processing elements scan these raw data for distinctive or identifiable characteristics. The liveness detection may take place at the acquisition stage, such that non-live data are not acquired, or at the processing stage, such that non-live data are not processed. If one places an eraser on an optical fingerprint sensor, an image appears but no feature extraction takes place: the detection is at the processing stage. In most silicon systems, the same eraser would not produce an image, such that detection would take place at the acquisition stage.

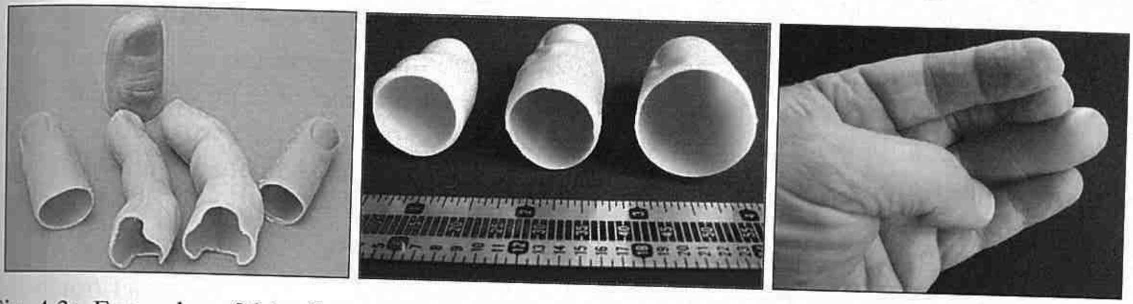


Fig. 4.3: Examples of fake fingers produced by the company Vernet® (however papillary lines are missing here – nevertheless these could be "added").

4.1.2 Attacks During Verification/Identification and Human Monitoring

Let us assume that the enrollment process was properly performed and the user has registered his biometric sample, without which it is pointless to assure the system in the verification/identification phase. In general, three basic attacks are feasible whenever the liveness detection is not well implemented [48][36]:

- *Presenting artificial samples* of the registered user is the most common and most important threat or risk in this category because of the relative easy effort and variety of ways in which such an attack could be realized. Artificial samples could be produced in many ways from many materials, what poses a problem for detection countermeasures. Dishonest acts with artificial samples could be divided into two classes: artificial samples produced with the assistance of the registered user and artificial samples produced without his assistance. The former class mostly provides better quality than the artificial samples from the latter class, but the latter ones are still able to defeat biometric systems.
- A *latent sample reactivation* risk relates to touch fingerprint systems. The rarely used sweep sensors do not have to address this problem, because the method for imaging includes a self-cleaning function during each capture. In addition to the liveness detection, touch fingerprint systems should include a cleaning mechanism after each imaging. Some vendors protect their devices (e.g. Siemens ID Mouse Professional version 4) by implementing latent print reactivation (LPR) algorithms, which are designed to reject any print that is identical to the earlier authenticated one. But depending upon the technology it may be relatively easy for an attacker to insert a small amount of noise to avoid LPR algorithms but still close enough for acceptance. It is worth noting that a biometric system should reveal under no circumstances the information (like a score or threshold) to the user that could be useful for attackers. Additionally, before initiating another transaction, a biometric system should clear

all biometric data from the memory, to ensure its security in a case when the attacker gains control of the system.

- Last but not least, a *severed sample from the registered user* could be presented. This attack consists of severing the user's biometric samples from the registered user or his cadaver. In some cases the user's half-decomposed corpse may be used for such purposes.

To overcome the above mentioned threats or risks, the liveness detection should be implemented. In an environment where a higher level of security is required, a biometric system should be a part of two- or three-factor authentication solution. There are other attacks at the sensor level but they are possible whether or not liveness quality is implemented.

Human monitoring [48] is suitable as an extension to the liveness detection. The supervision is more important during enrollment, where the trained personnel also explain the use of the biometric system to users who usually do not have any previous experience with such kind of biometric system. The supervision during verification is also profitable and could easily notice some kinds of artifacts and tampering with the capture device but, on the other hand, it may be difficult to detect, e.g. an artificial fingerprint pattern molded on a thin laminate and attached over the top of a real fingerprint. We should not forget that human professionals could be forcibly removed, corrupted or distracted, so supervision is not a valid substitution for the liveness testing but is desirable as a supplementary precaution. In an environment where the biometric system relies on the self-enrollment or the self-verification process, the organization should, as well as including the liveness detection, still perform random spot checks or guard the system through video cameras.

4.1.3 Dilemma of Liveness Detection

A biometric system may solve the liveness problem either as a liveness detection, where the system checks that one or more qualities of a biometric sample are coincident with the qualities related to live biometric samples, or as a non-liveness detection, where the process is similar but the qualities related to non-live biometric samples are checked [48].

The liveness testing may take place at the acquisition stage, when non-live data are not acquired, or at the processing stage, when non-live data are not processed. For example, in the case of a fingerprint system with pulse checking, the entire artificial finger would not be acquired, so the detection is at the acquisition stage. On the other hand, when we use fingerprint system with perspiration checking, fingerprint images have to be taken to determine perspiration, so the detection takes place at the processing stage.

Another very important feature for the security and proper working of a biometric system is to assure that the capture of the biometric sample and measurement of liveness occur at the same point in space and time [48]. Otherwise, an attacker may present his live biometrics to pass the liveness testing and then he may deceive the verification process by supplying an artificial sample. The similar situation arises when we consider the matter of space. Last but not least, user acceptance, ease of use and other characteristics have to be considered before taking a decision about liveness testing.

Unlike regular cryptographic systems, where algorithms and methods of operation are well known and security is based only on the key protection, biometric systems are mostly presented and treated as black boxes. Such an industry's closed approach known as security by obscurity [48] has been discussed and two different opinions by different groups are maintained. Manufacturers and vendors claim that regardless of the liveness testing methods used, if the algorithm is known, an attacker may exploit the information to thwart it. But it is well known that the secrecy of methods at best increases the time taken for the completion of an attack, because the reverse engineering may be involved. On the other hand, mostly security and cryptography experts have long called to break through the manufacturers' unwillingness and to open critical functions and methods for inspections, analysis, criticism, and improvement. Today, nearly all liveness testing algorithms are at some point reliant on one or more secrets, which pose a risk in a case of disclosure and are rightly considered as a nearly non-existent capability. Manufacturers and vendors have to realize that any liveness detection methods can be defeated, and the only way to build stronger methods is to open such methods to third-party inspections.

The liveness detection relates to another problem which can be called unrealistic performance claims [48]. Such a problem poses the overstated and sometimes misleading information not only about the liveness testing quality. The biometric industry should head towards rigorous implementation standards and realistic independent inspections to overcome the problems mentioned above.

4.2 Liveness Testing in the Fingerprint Recognition Technology

Securing automated and unsupervised fingerprint recognition systems used for the access control is one of the most critical and most challenging tasks in real world scenarios. Basic threats for a fingerprint recognition system are repudiation, coercion, contamination and circumvention [Dra17][Dra13]. A variety of methods can be used to get an unauthorized access to a system based on the automated fingerprint recognition. If we neglect attacks on the algorithm, data transport and hardware (all these attacks demand good IT knowledge), one of the simplest possibilities is to produce an artificial fingerprint using soft silicon, gummy and plastic material or similar substances [64][93]. The fingerprint of a person enrolled in a database is easy to acquire, even without the user's cooperation. Latent fingerprints on daily-use products or on sensors of the access control system itself may be used as templates.

To discourage potential attackers from presenting a fake finger (i.e. an imitation of the fingertip and the papillary lines) or, even worse, to hurt a person to gain access, the system must be augmented by a liveness detection component [Dra17][Dra13]. To prevent false acceptance we have to recognize if the finger on the plate of the fingerprint sensor (also referred to as fingerprint scanner) is alive or not.

In this section a description of different liveness detection methods is presented and discussed related to the fingerprint recognition system. Speaking in terms of the liveness detection it has to overcome the fact that the outmost layer of the human skin (epidermis) is almost dead material [48] and therefore it has to focus on other characteristics of the finger.

4.2.1 Perspiration

A non-invasive biomedical measurement for determination of the liveness for use in fingerprint scanners was developed by the Biomedical Signal Analysis Laboratory at Clarkson University/West Virginia University[3] [88]. This software-based method processes the information already acquired by a capture device and the principle of this technique is the detection of perspiration as an indication of liveness (see Fig. 4.4).

It is worth noting that the outmost layer of the human skin houses around 600 sweat glands per square inch [88]. These sweat glands diffuse the sweat (a dilute sodium chloride solution) on to the surface of the skin through pores. The position of skin pores does not change over time and their pore-to-pore distance is approximately 0.5 mm over fingertips.

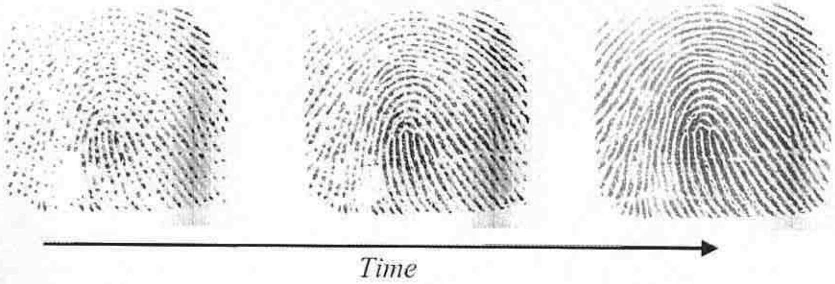


Fig. 4.4: Example of live fingerprint images acquired some time apart [Dra04][88].

The perspiration method is based on a high difference in the dielectric constant and electrical conductivity between the drier lipids that constitute the outer layer of the skin and the moister sweaty areas near the perspiring pores. The dielectric constant of sweat is around 30 times higher than the lipid, so the electrical model of the skin thanks to perspiration can be created.

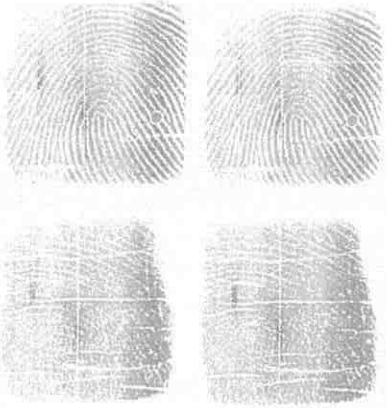


Fig. 4.5: The top pair shows captures of an artificial finger acquired 0 and 5 second apart and the bottom pair shows the same for a cadaver finger [48].

Because the capacitive fingerprint scanner (see chapter 2.2.3) is sensitive to moisture, the above method can profit from this fact to determine a temporal change in moisture

[3] http://people.clarkson.edu/~biosal/

due to perspiration. The algorithm works with two consecutive fingerprint images captured in 5 seconds (Fig. 4.6). The first one typically looks “patchy”, because perspiration in the live finger starts from the pores, either completely covering them or leaving the pore as a dry dot in the center of the sweating source. The second image is more affected by perspiration, because during that time sweat diffuses along the ridges, making the semi-dry regions moister and darker in the image. In Fig. 4.5 we can see that in a cadaver or artificial images such a perspiration process does not occur and therefore scans with the same 5 seconds time separation are nearly identical.

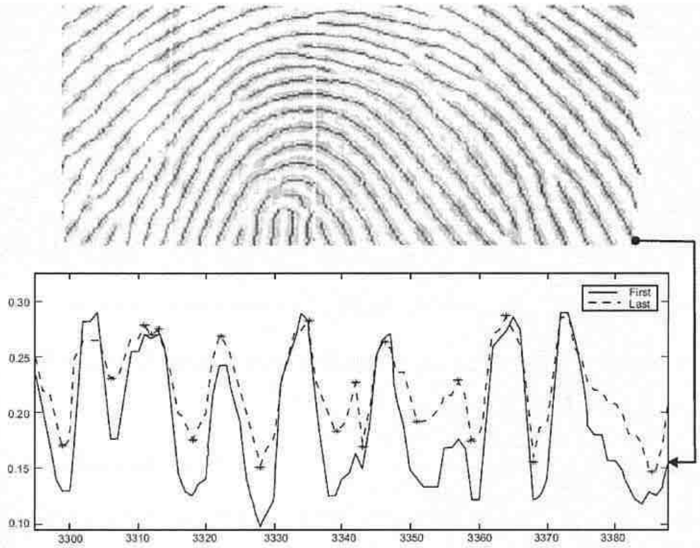


Fig. 4.6: Live fingerprint signals (bottom), where the solid line shows initial reading and the dashed line shows the reading after five seconds [48].

The algorithm develops one static measure and four dynamic measures [48][88]. First the average Fourier transform of the first image’s signal is computed to quantify the energy as a static measure. The following step is the computation of four dynamic measures. Dynamic measures also use the variation of minimums. For live fingerprint signals, the maximums are fairly constant, but the minimums are higher in the second capture as compared with the first. The final classification can be based on each of the individual measures, but in such a case the algorithm reaches higher equal error rates of the liveness testing functionality. However, a much better classification can be made, when the decision is based on a combination of all the above mentioned measures. In that event a Back-Propagation Neural (BPN) network with one static measure and four dynamic measures as input is utilized.

The main advantage of this non-invasive and perspiration-phenomenon-based approach is its purely software implementation. Due to the small size and reasonable price of capacitive sensors they are popular and widely used in portable devices (i.e. mobile phones, laptop and hand-held computers, etc.). In devices of this type the perspiration liveness method, without any additional hardware, could be implemented.

On the other hand, many questions must be addressed and improvements [48] made before putting the perspiration liveness method into practice. Further, the research into perspiration disorders (finger too moist or too dry) and other abnormal skin conditions must be performed. Furthermore, testing against fake samples which try to imitate a real-perspiration phenomenon should be performed. Another subject designed for further investigation and improvements is the algorithm's speed. Is it necessary to put a five second gap between two acquisitions or could the algorithm use more than two captures? The compromise between precision and speed of the perspiration liveness method will need to be addressed.

The sweat creation and ascent from sweat pores during the scanning with 4× zoom factor could be seen in Fig. 4.7.

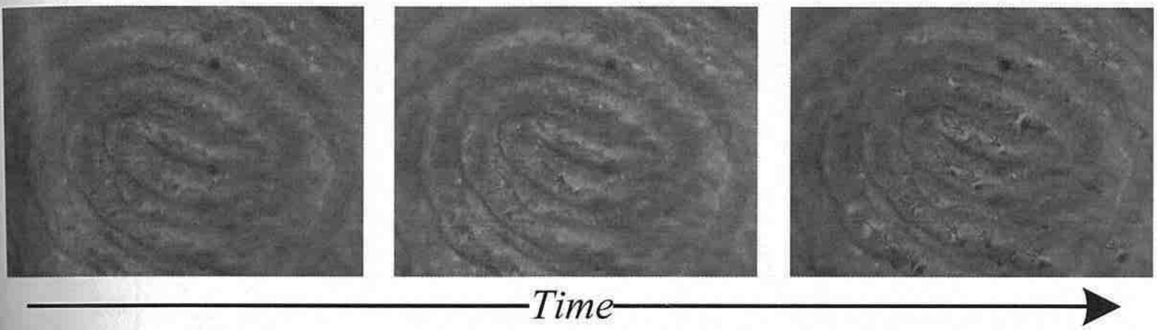


Fig. 4.7: Ascent of sweat from sweat pores on a fingertip (4× zoomed).

4.2.2 Spectroscopic Characteristics

The technology discussed in this section was developed by the Lumidigm[4] company [83][48] from Albuquerque and is based on the optical properties of human skin. This hardware method may be regarded not only as a liveness detection mechanism but also as an individual biometric system with an inherent liveness capability.

As Fig. 2.2 shows, the human skin consists of multiple layers and contains mixtures of chemicals and structures such as sweat glands, hair follicles and others. These characteristics vary in many ways (i.e. pigmentation, thickness of the layers, density of collagen, capillary beds etc.) for each person's skin when compared to any other's skin and additionally these spectral characteristics are also capable of distinguishing live human skin from other "spoof" materials or dismembered human skin. This means that they may be used for biometric and liveness detection purposes [48].

Living human skin has certain unique optical characteristics due to its chemical composition, which predominately affects optical absorbance properties, as well as its multi-layered structure, which has a significant effect on the resulting scattering properties [83][82]. By collecting images generated from different illumination wavelengths passed into the skin, different subsurface skin features may be measured and used to ensure that the material is living human skin. When such a multispectral sensor is combined with a conventional fingerprint reader, the resulting sensing system can provide a high level of certainty that the fingerprint originates from a living finger.

The principle of this technique lies in passing light of different wavelengths through a sample and measuring the light returned, which is affected by the structural and chemical

[4] http://www.lumidigm.com/

properties of the sample. Different wavelengths have to be used to measure the sample satisfactorily, because diverse wavelengths penetrate to different depths into the sample and are differently absorbed and scattered [48]. For example, when we put a flashlight against the tip of a finger only the red wavelengths can be seen on the opposite side of the finger. This is because shorter (mostly blue) wavelengths are absorbed and scattered quickly in the tissue, unlike longer (red and very near infrared) ones, which penetrate deep into the tissue. The measurements can be transformed into a graph (Fig. 4.8) that shows the change in all measured wavelengths after interacting with a sample and is known as a spectrum. Next, the proper analysis of tissue spectra, based on multivariate mathematical methods has to be done to provide correct results.

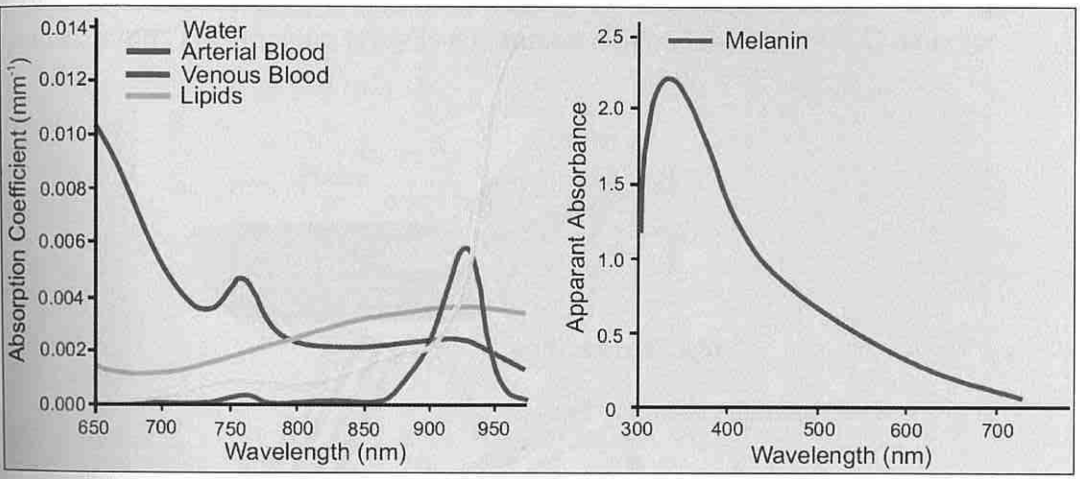


Fig. 4.8: Spectrographic properties of different components of living tissue (suitable for detection of spoofing attacks on iris recognition) [94].

Figure 4.9 shows the layout of an optical fingerprint sensor that combines a conventional frustrated total internal reflection (FTIR) fingerprint reader with a multispectral imager.

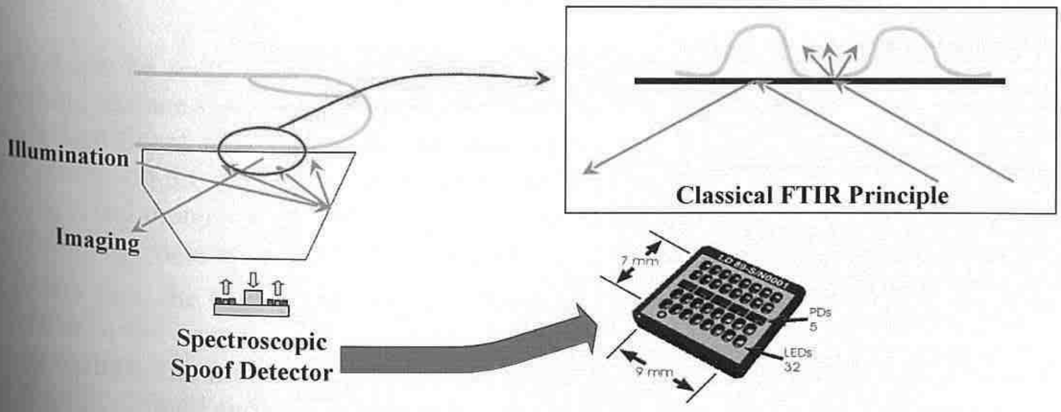


Fig. 4.9: FTIR and multispectral imager [82].

In general, the optical resolution requirements for this application of a multispectral imager are relatively modest [83]. Because of the highly scattering nature of skin, the multispectral imager needs not have a greater resolution than that used for the conventional fingerprint image, typically 250-1,000 pixels per inch. Assuming a nominal one inch sensing surface, a readily available VGA (*Video Graphics Array*; 640×480) or 1.3 megapixels array provides the adequate resolution for most applications.

The key components of a multispectral imager [82][83] suitable for imaging fingers are shown in Fig. 4.10. The light sources are LEDs of various wavelengths spanning the visible and short-wave infrared region. Crossed linear polarizers may be included in the system to reduce the contribution of light that undergoes a simple specular reflection to the image, such as light that is reflected from the surface of the skin. The crossed polarizers ensure that the majority of light seen by the imaging array has passed through a portion of skin and undergone a sufficient number of scattering events to have randomized the polarization. The imaging array is a common silicon CMOS or CCD detector.

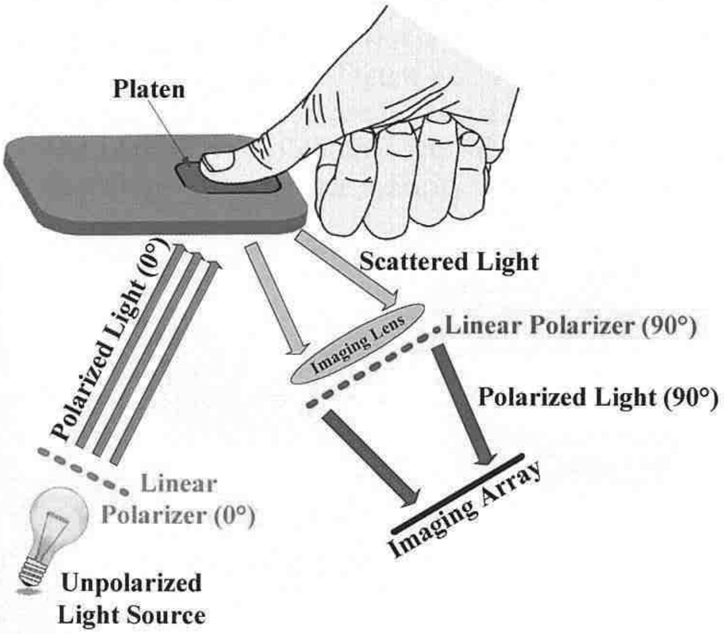


Fig. 4.10: Multispectral imager (MSI); re-drawn from [82].

As it can be seen, both sensors (Fig. 4.9 and Fig. 4.10) can view a finger placed on the sensing surface without interfering with each other. The multispectral imager can thus provide significant new biometric information without requiring any different or additional actions on the part of the user. An example of a conventional fingerprint image and a multispectral image of the same finger is illustrated in Fig. 4.11a, whereas the real multispectral image data are shown in Fig. 4.11b.

In this case, the skin of the subject's finger is relatively dry, causing a noticeable deterioration in the contrast and continuity of the lines in the conventional fingerprint image. In contrast, the multispectral pseudo-color image shows spectral and spatial features that are well defined and consistent with a living finger. In addition, the fingerprint image is observable in the multispectral data, which can be used to further authenticate the conventionally collected fingerprint pattern as well as to augment missing or poorly defined portions of the conventional fingerprint.

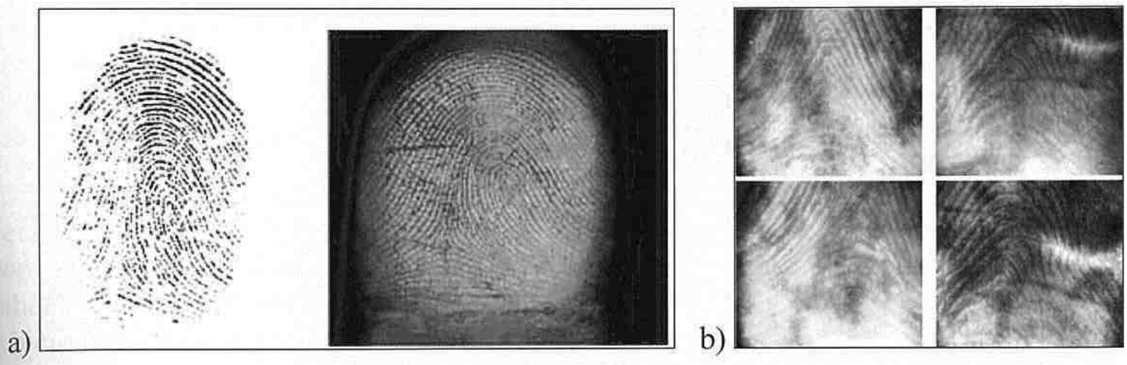


Fig. 4.11: a) Conventional and multispectral ($\lambda_{1...5}$ = 475, 500, 560, 576, 625 nm) fingerprint image [83]; b) Real multispectral image data [82].

A highly realistic artificial finger made by Alatheia Prosthetics [83] was one of a number of different spoof samples used to test a multispectral imager's ability to discriminate between real fingers and spoofs. Figure 4.12 shows the results of a multivariate spectral discrimination performed to compare the consistency of the spectral content of a multispectral image of a real finger with both a second image of a real finger and a prosthetic replica of the same finger. The imager's ability to distinguish between the two sample types is clear.

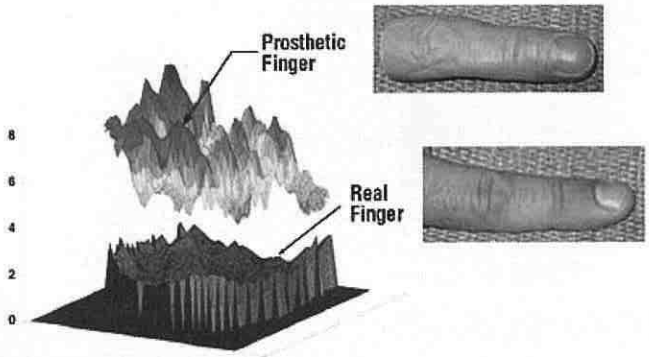


Fig. 4.12: Multispectral image data can clearly discriminate between a living finger and an ultra-realistic spoof. The graphs on the left side show how similar the spectral content of each image is to that expected for a genuine finger [83][94].

As a non-human tissue or "spoof" material has very different optical properties than the complicated human skin, computed spectrum can be used to distinguish living from the other samples (Fig. 4.12). Additionally, excised or amputated samples undergo rapid changes in chemical properties, distribution of fluids and other physiological changes which cause a corresponding modification to the resulting spectrum. And because the spectral signal is based on the characteristics, which are believed invariable over time, this method of liveness testing could work simultaneously with many biometric systems.

This approach can be used as a liveness testing module simultaneously with many types of biometric systems or as an individual biometric system with an inherent liveness testing capability. It is very flexible in terms of scalability, and therefore sensors can be modified to satisfy the application needs. Sensors can be designed to operate on nearly any portion of the skin.

Another approach of the liveness detection using the wavelet analysis in images is presented in [87].

4.2.3 Ultrasonic Technology

In this paragraph, a biometric system using an ultrasonic technology with inherent liveness testing capability will be described. This technique is being developed by the company Optel[5] from Poland and is based on the phenomenon called contact scattering. Another ultrasonic biometric device is offered by the company Ultra-Scan[6] from the USA, which is the second and last vendor of this technology principle in the market at the moment.

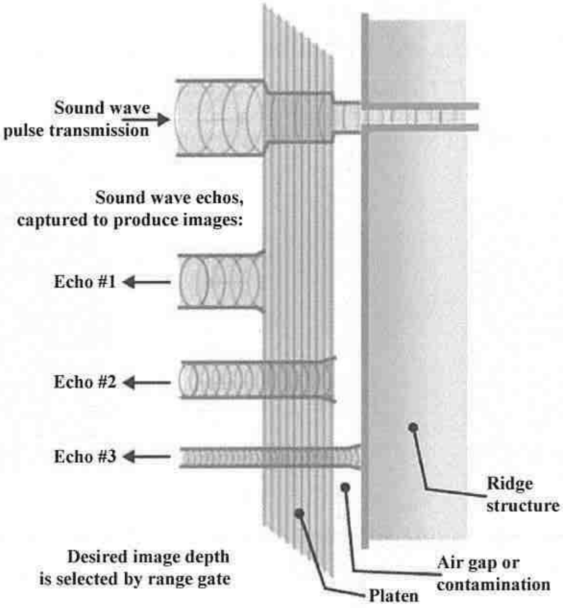

Sound wave pulse transmission
Sound wave echos, captured to produce images:
Echo #1
Echo #2
Echo #3
Desired image depth is selected by range gate
Ridge structure
Air gap or contamination
Platen

Fig. 4.13: Schematic of ultrasonic pulse/echo principle [95].

Standard *ultrasonic methods* [48] use a transmitter, which emits acoustic signals toward the fingerprint, and a receiver, which detects the echo signals affected by the interaction with the fingerprint (Fig. 4.13). A receiver utilizes the fact that the skin (ridges) and the air (valleys) have difference in acoustic impedance; therefore the echo signals are reflected and diffracted differently in the contact area. This approach with inherent liveness testing capability among its foremost principles uses the fact that sound waves are not only reflected and diffracted, but are also subject to some additional scattering and transformation. This phenomenon is called *contact scattering* [48] and it was discovered that this scattering is, to a significant extent, affected by the subsurface structure of the acquired object. Hence, the class corresponding to the live tissue could be modeled and whenever the received acoustic waves are inconsistent with this class, they are rejected. The main problem here is not to obtain clear signals, but to analyze and to make a reconstruction of internal structures from signals which are very difficult to interpret.

[5] http://www.optel.pl
[6] http://www.ultra-scan.com/

The ultrasonic device reached the following conclusions [48][7]:

- As the inner structure of the live skin compared with spoof samples differs, the character and the amplitude of acoustic signals also differ significantly. Hence, it is possible to distinguish between live and artificial fingers.
- There is no need to deal with the problem known as latent print reactivation because the signal level from the latent print is at least 30 dB lower than the signal given by the real finger. Even when the soot or metal powder is used in order to enhance the quality of signal, the previous is true.
- This method is much less sensitive to dirt, grease and water compared with other methods (see Fig. 4.14). In addition, fingers with damaged surface give a relatively clear image, because their inner structure seems to be visible.

Since this approach scans the inner structure of the object, it has the ability to check for pulse by measuring volumetric changes in the blood vessels [7].

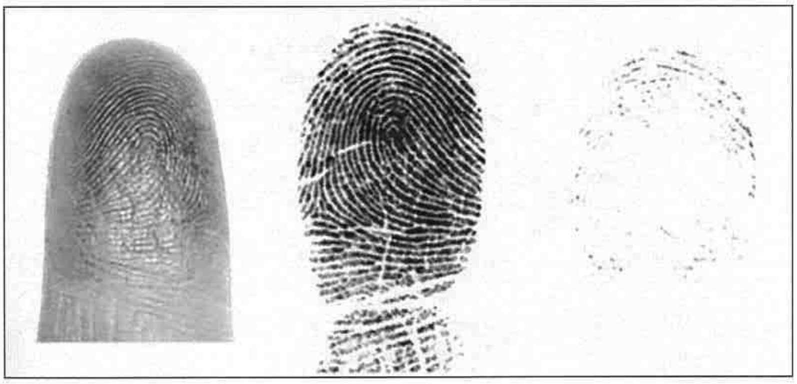


Fig. 4.14: Index finger with newsprint to demonstrate the finger contamination (from left: contaminated original, ultrasound image, optical image) [95].

4.2.4 Physical Characteristics: Temperature

This simple method measures the temperature of the epidermis during a fingerprint acquisition. The temperature of the human epidermis of the finger moves in the range of approximately 25–37°C (see Fig. 4.15). However, this range usually has to be wider to make the system usable under different conditions. In addition, there are many people who have problems with blood circulation, a fact which leads to deviations in the body's temperature and hence to wrong liveness module decision. The only way how to improve such a situation is to make the working range broader again or simply warm the user's finger. The former will increase the likelihood that the system will be deceived while the latter can also be applied to fake samples. In the case where an attacker uses a wafer-thin artificial fingerprint glued on to his finger, this will result in a decrease by a maximum of 2°C [Dra06] compared with an ordinary finger. Since the difference in temperature is small, the wafer-thin sample will comfortably fall within the normal working margin. In consequence, this method is not a serious security measure at all.

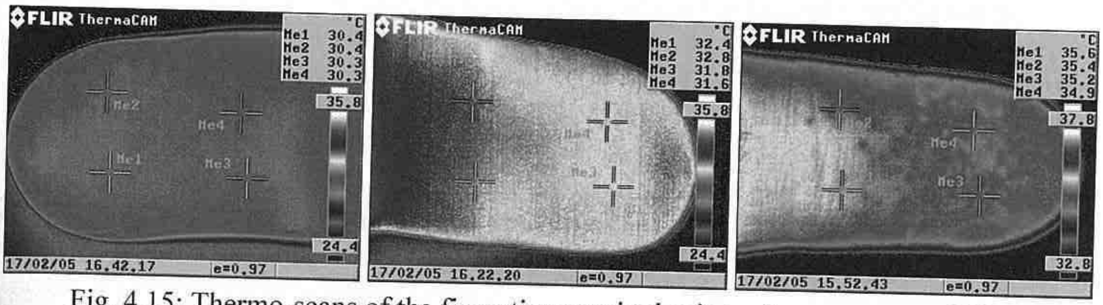


Fig. 4.15: Thermo-scans of the fingertips acquired using a thermo-camera FLIR.

4.2.5 Physical Characteristics: Hot and Cold Stimulus

This technique is based on the fact that the human finger reacts differently to thermal stimuli compared with other artificial, non-living material.

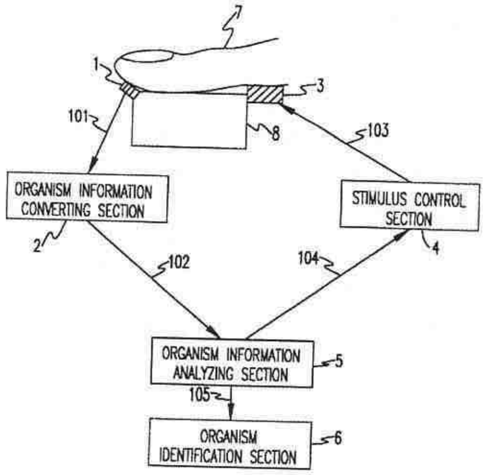

7
1
3
101
8
103
ORGANISM INFORMATION CONVERTING SECTION
2
STIMULUS CONTROL SECTION
4
102
104
ORGANISM INFORMATION ANALYZING SECTION
5
105
ORGANISM IDENTIFICATION SECTION
6

Fig. 4.16: Functionality principle of the device measuring hot and cold stimulus [99].

The designed liveness testing module [48][99] is working as follows (Fig. 4.16). A stimulus-giving section gives a stimulus (it may cover a cool and a hot stimulus) to the finger by a contact plate with which the finger makes contact. Next, typical information could be measured by an organism information-measuring section, which is produced by the live finger in response to the stimulus. Concretely, the amount of the fluctuation for the flow rate of the blood flowing in the peripheral vascular tracts varies according to the stimuli. Hence, as peripheral vascular tracts of the tip of the finger are extended or contracted, the amplitude value of the blood flow is measured and processed by an organism information-measuring section. Under hot stimulus the amplitude of the blood flow increases, while it decreases under cool stimulus. Moreover, according to the autonomic nervous system, the amplitude is delayed a little with respect to the application of the stimulus. Since these facts are typically observed when the live fingers are measured, they could be employed to distinguish live among artificial and dead samples. After the processing phase, such information is transferred to a determining section, where together with the other information related to stimulus (i.e. the time intervals, the strength of stimuli etc.) is evaluated. Finally, a determining section analyses how the amplitude of the blood flow fluctuates in response to the stimulus to make the right decision.

Since the human peripheral nervous system is very sensitive, it is able to react to weak cool and hot stimuli without being noticed by the person whose fingerprint is checked. This fact should also reduce success spoofing ratio. More information about the method discussed here can be found in [99].

4.2.6 Physical Characteristics: Pressure Stimulus

The principle of this method lies in some changes in characteristics of the live skin, which are realized due to pressure applied to the finger [48][101]. Since the structure and the characteristics of artificial and dead samples are different, when compared with a live finger, this phenomenon could not be seen if such samples were used.

The color of the live skin of the finger not under pressure is usually reddish but becomes whitish when pressure is applied to the skin of the finger. It has been shown that the spectral reflectance of the light in the red spectral range (i.e. the light wavelength of approximately 640–770 nm) [101] does not show a substantial difference between the pressed state and the non pressed state. On the other hand, the spectral reflectance of the light in the blue and green spectral range (i.e. the light wavelength of approximately 400–600 nm) [101] in the not pressed state is much smaller than in the pressed state. Hence, for the purposes of the device discussed in this section it is suitable to measure the spectral reflectance in the blue and green spectral range (see Fig. 4.17).

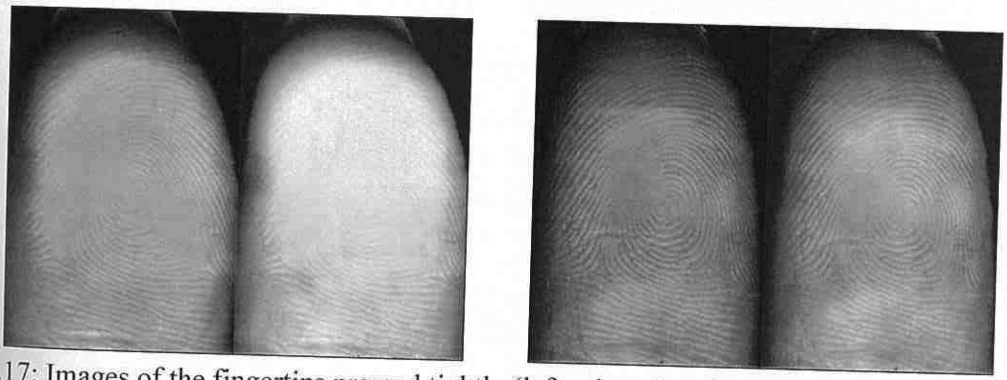


Fig. 4.17: Images of the fingertips pressed tightly (left subpart) and slightly (right subpart) to the sensor [Dra04].

A liveness testing module is proposed in [101] (see Fig. 4.18) and consists of a transparent plate, a light source, a light detection unit and a determining section. Since the light source and the light detection unit are placed under the plate, this plate has to be transparent to enable light to be sent towards the finger and receiving the reflected light. The light source projects a light beam towards the surface of the placed finger. Next, depending on the pressure or non-pressure state, the reflected light is measured by the light detection unit.

Based on such measurements the determining section returns the right decision, i.e. as the finger changes its state from non-pressure to pressure, the color of the skin changes from reddish to whitish, what leads to a change in the spectral reflectance. As a result, the light detection unit can detect that the spectral wavelength of the spectral ranges is increased.

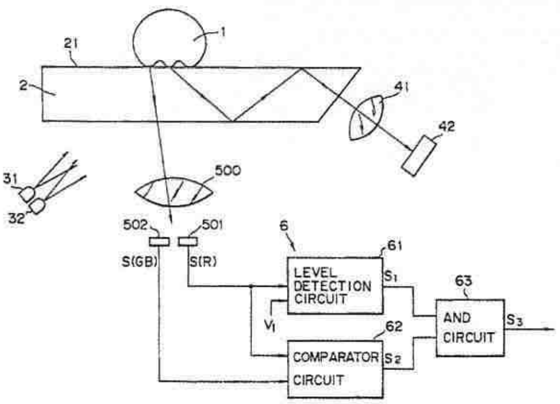


Fig. 4.18: Functionality principle of device measuring pressure stimulus [101].

Another method using pressure based characteristics is discussed in [100] (see Fig. 4.19), but unlike the method described in the previous paragraph, this technique employs the change in fingerprint ridges width. When the fingerprint changes its state from non-pressure to pressure, the fingerprint ridges change, i.e. as the pressure becomes stronger, the fingerprint ridges flatten out, and therefore their change of width could be measured. Only objects which demonstrate the typical change in fingerprint ridge width due to pressure could be determined as live ones.

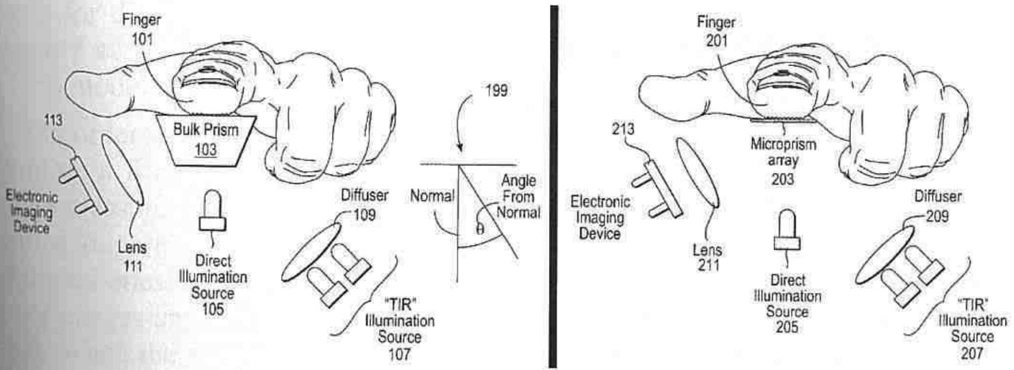

Finger
101
113
Bulk Prism
103
Electronic Imaging Device
Lens
111
Direct Illumination Source
105
Diffuser
109
"TIR" Illumination Source
107
199
Normal
Angle From Normal
θ
Finger
201
213
Microprism array
203
Electronic Imaging Device
Lens
211
Direct Illumination Source
205
Diffuser
209
"TIR" Illumination Source
207

Fig. 4.19: Two functionality principles of device measuring pressure stimulus [100].

A new approach to the fake finger detection based on skin elasticity analysis has been introduced in [42]. When a user puts a finger on the scanner surface, the scanner captures a sequence of fingerprint images at a certain frame rate. The acquired image sequence is used for the fake finger detection. One or more of them (at the end – see Fig. 4.20) can be used for fingerprint authentication.

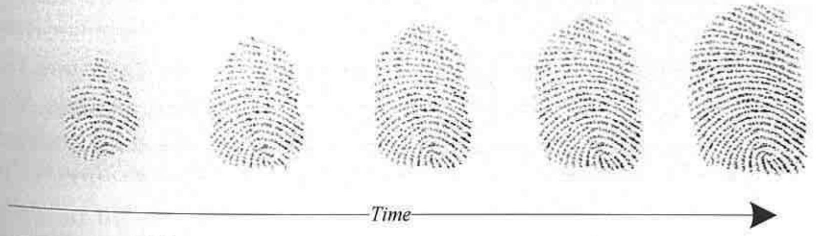


Fig. 4.20: A sequence of fingerprint images describing the deformation of a real finger [42].

For each image sequence, there are computed two features: the *correlation coefficient* of the fingerprint area with an average signal intensity and the *standard deviation* of the fingerprint area extension in *x* and *y* axes. Finally the Fisher linear discriminant is used to determine the final "real" or "fake" results. The flowchart of different phases of the approach from [42] is shown in Fig. 4.21.

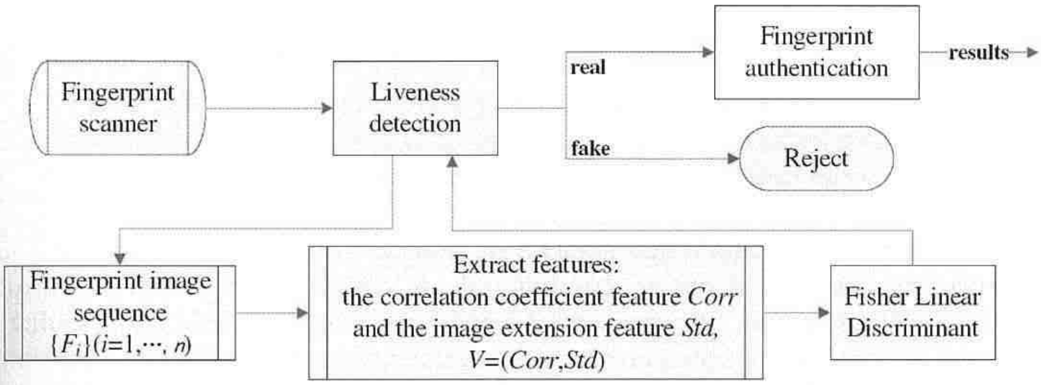

Fingerprint scanner
Liveness detection
real
fake
Fingerprint authentication
results
Reject
Fingerprint image sequence $\{F_i\}(i=1,\cdots,n)$
Extract features: the correlation coefficient feature *Corr* and the image extension feature *Std*, $V=(Corr,Std)$
Fisher Linear Discriminant

Fig. 4.21: A flowchart showing different phases of the approach [42].

It has been shown (e.g. in [126] that fake fingers are generally more rigid than skin and the deformation is lower even if made of highly elastic materials. The elasticity is the basis for discriminating fake fingers from real ones. When a real finger moves on the scanner surface, it produces larger distortion than fake fingers. The Thin Plate Spline (TPS) model is introduced in [126] to describe the finger distortion.

In order to describe the distortions produced by the finger, the user is required to firstly place a finger onto the scanner surface without any superficial tension, then to apply some pressure in four directions: 0°, 90°, 180° and 270° respectively. A sequence of acquired fingerprints is captured for each finger, including the natural fingerprint and the distorted ones. Before the computation of the TPS distortion model, the acquired fingerprint images are enhanced and analyzed to extract relevant features related to skin distortion. When the fingerprint is distorted, its minutiae, as the most popular local features in the fingerprint, have different removal according to their locations. If the minutiae distribute almost symmetrically all over the fingerprint, their displacement can represent the global distortion. More information could be found in [126].

4.2.7 Physical Characteristics: Electrical Properties

Some methods of liveness testing are based on the fact that the live human skin has different electrical properties compared with other materials [48]. The suitable fingerprint recognition system could be extended by an electrode system and an electrical evaluation unit. These sections are the main parts of the liveness testing module where the electrical evaluation unit can evaluate the change in the state in the electrode system. The sensing of the electrical change should take place simultaneously with the recognition of the fingerprint. Therefore, these parts of biometric systems should be designed in such a way that two simultaneous measurements cannot disturb each other. Furthermore, such a system may be able to measure more than one of the fingerprint liveness characteristics related to electrical properties (e.g. conductivity, dielectric constant).

The *conductivity* [48] of the human skin is based on humidity, which is dependent on people's biological characteristics and environmental conditions: some people have dry fingers and others have sweaty ones; also during different seasons, climatic and environmental conditions, humidity differs significantly. As a result, the span of permissible resistance levels has to be big enough to make the system usable. In such a situation it is quite easy for an intruder to fool the system. Moreover, the intruder can use a salt solution of a suitable concentration or put some saliva on the fake finger to imitate the electric properties of the real finger.

The *relative dielectric constant* (RDC) [48] of a specific material reflects the extent to which it concentrates the electrostatic lines of flux. Many advocates claim that the RDC has the ability to distinguish between real and artificial samples. However the RDC is highly dependent on the humidity of the sample, so the same situation as in the case of conductivity arises. To fool this method an attacker can simply use an artificial sample and dip it into a compound of 90% alcohol and 10% water. In [76] we can read that the RDC values of alcohol and water are 24 and 80, respectively, while the RDC of the normal finger is somewhere between these two values. Since the alcohol will evaporate faster than the water, the compound will slowly turn into the water. During evaporation, the RDC of spoof samples will soon be within the acceptance range of the sensor.

We have run a small test series with 10 people, each finger, horizontal and vertical measurement strips, and 5 measurements per finger – conductivity (resistance) measurements – see chapter 4.4.4. The range of values we found was from 20 kΩ to 3 MΩ [Dra06]. A paper copy or an artificial finger made of non skin-like material have higher electrical resistance, but for example, soft silicon (moisturized) shows resistance values close to the range found in our experiments.

4.2.8 Physical Characteristics: Bio-Impedance

Bio-impedance [63][22][17] describes the passive electrical properties of biological materials and serves as an indirect transducing mechanism for physiological events, often in cases where no specific transducer for that event exists. It is an elegantly simple technique that requires only the application of two or more electrodes. The impedance between the electrodes may reflect "seasonal variations in blood flow, cardiac activity, respired volume, bladder, blood and kidney volumes, uterine contractions, nervous activity, the galvanic skin reflex, the volume of blood cells, clotting, blood pressure and salivation."

Impedance Z [22] is a general term related to the ability to oppose AC (*Alternating Current*) flow, expressed as the ratio between an AC sinusoidal voltage and an AC sinusoidal current in an electric circuit. Impedance is a complex quantity because a biomaterial, in addition to opposing current flow, phase-shifts the voltage with respect to the current in the time-domain.

The conductivity of the body is ionic (electrolytic) [22], because of the presence of e.g. Na^+ and Cl^- in the body liquids. The ionic current flow is quite different from the electronic conduction found in metals: the ionic current is accompanied by a substance flow. This transport of substance leads to concentrational changes in the liquid: locally near the electrodes (electrode polarization), and in a closed-tissue volume during prolonged DC (*Direct Current*) current flow.

The body tissue is composed of cells with poorly conducting, thin-cell membranes. Therefore, the tissue has capacitive properties [22]: the higher the frequency, the lower the impedance. The bio-impedance is frequency-dependent, and impedance spectroscopy, hence, gives important information about tissue and membrane structures as well as intra- and extracellular liquid distributions.

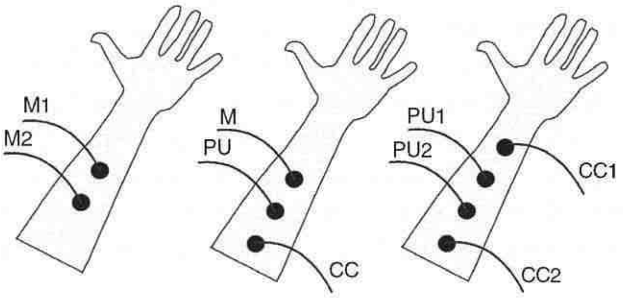


Fig. 4.22: Three skin surface electrode systems on an underarm [22]. Functions: M – measuring and current carrying, CC – current carrying, PU – signal pick-up.

Fig. 4.22 shows three most common electrode systems. With two electrodes, the current carrying electrodes and signal pick-up electrodes are the same. If the electrodes are equal, it is called a bipolar lead, in contrast to a monopolar lead. With 3-(tripolar) or 4-(tetrapolar) electrode systems, separate current carrying and signal pick-up electrodes are used. The impedance is then transfer impedance [22]: the signal is not picked up from the sites of current application.

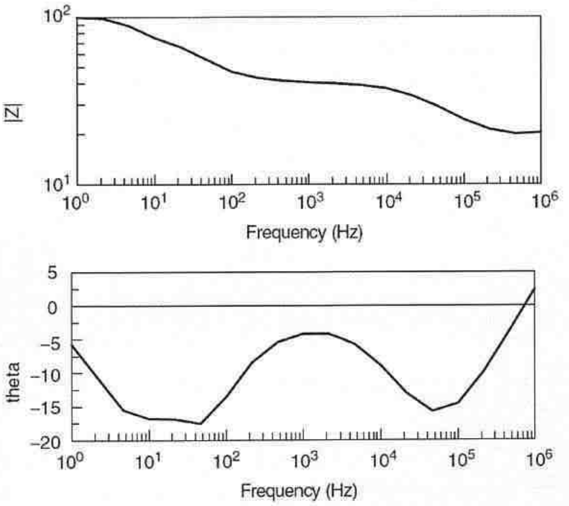


Fig. 4.23: Typical impedance spectrum obtained with four equal electrodes attached to the skin of the underarm [22].

Fig. 4.23 shows a typical transfer impedance spectrum obtained with the 4-electrode system from Fig. 4.22. It shows two dispersions [22]. The transfer impedance is related to, but not solely determined by, the arm segment between the PU electrodes. The spectrum is determined by the sensitivity field of the 4-electrode system as a whole. The larger the spacing between the electrodes, the more the results are determined by deeper tissue volumes. Even if all the electrodes are skin surface electrodes, the spectrum is, in principle, not influenced by skin impedance or electrode polarization impedance.

4.2.9 Physical Characteristics: Pulse

Scanners based on this technique try to detect whether the scanned object exhibits characteristics of the pulse and blood flow consistent with a live human being [48]. It is not very difficult to determine whether the object indicates some kind of pulse and blood flow, but it is very difficult to decide if the acquired characteristics are coincident with a live sample. As a result, it is difficult to create an acceptance range of the sensor, which would lead to small error rates. The main problem is that the pulse of a human user varies from person to person – it depends on the emotional state of the person and also on the physical activities performed before the scanning procedure. In addition, the pulse and blood flow of the attacker's finger may be detected and accepted when a wafer-thin artificial sample is used.

One of the sensors usually detects variation in the levels of the reflected light energy from the scanned object as evidence of the pulse and blood flow [48]. First, the light source illuminates the object and then a photo-detector measures the light energy reflected from the object. Finally, there is the processing instrument (which also controls the light source) which processes the output from the photo-detector. Since there are some ways how to simulate pulse and blood flow characteristics (e.g. by flashing the light or by motion of the scanned object), scanners should have a deception detection unit [48].

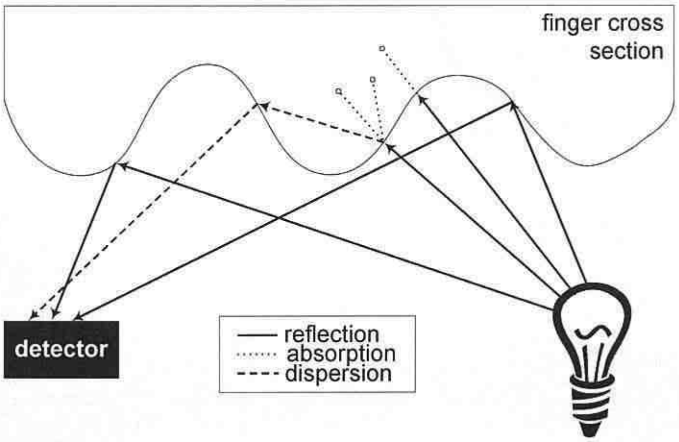


Fig. 4.24: Light absorption, dispersion and reflection by a fingerprint [Dra17].

Our skin is semi-permeable for light, so that movements below the skin (e.g. blood flow) can be visualized. One example of an optical skin property is the *skin reflection* [Dra17][Dra08]. The light illuminating the finger surface is partly reflected and partly absorbed (Fig. 4.24). The light detector acquires the reflected light which has been changed in phase due to dispersion and reflection and thus has a slightly different wavelength compared to the original light source. One can try to link the change in wavelength to the specific characteristics of the skin with respect to light dispersion and reflection to detect whether the light has been scattered and reflected only from the fingerprint skin, or if there is some intermediate layer between the finger skin and the light source or detector.

Another example for optical skin feature is the *saturation of hemoglobin* [Dra17][Dra08], which binds oxygen molecules. When blood comes from the heart, oxygen molecules are bound to the hemoglobin, and vice versa, when blood is flowing back to the heart, it is less saturated by oxygen. The color of oxygenated blood is different from that of non-oxygenated blood. If we use a light source to illuminate the finger skin, we can follow the blood flow based on the detection of oxygenated and non-oxygenated blood, respectively [Dra17][Dra08]. The blood flow exhibits a typical pattern for a live finger, i.e. the analysis of blood flow is well suited for finger liveness detection.

In both above mentioned examples, it is shown that the human skin has special characteristics which can be used for the liveness testing. It can be argued that it is possible to confuse such system, e.g. by using a substance with similar optical characteristics as a human skin, or, in the second example to simulate the blood flow. Even though the argument is correct, obviously the effort to be exerted for these attacks is much higher than for the other physical characteristics presented so far.

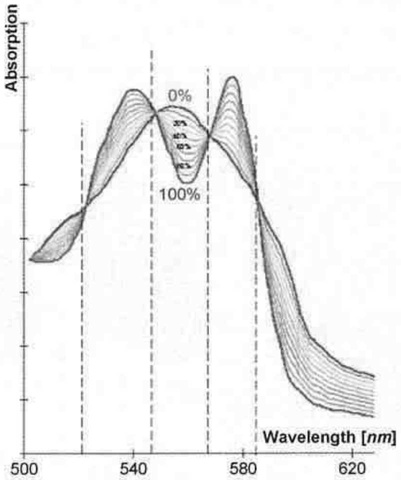


Fig. 4.25: Detection of saturation of hemoglobin [105].

Another solution is proposed in [Dra17][Dra08] based on the analysis of movements of papillary lines of the fingertips and measurements of the distance of the fingertip surface to a laser sensor, respectively. The system is compact enough to be integrated with optical fingerprint sensors.

One advantage of this implementation is that the finger is not required to be in contact with a specific measuring device, and so it can be integrated with standard fingerprint sensors. Moreover, the implementation could be acceptably low. This is of particular importance, as in most cases the liveness detection will be an add-on that augments already existing robust and field-tested fingerprint scanners.

The method presented in [Dra17][Dra08] requires the analysis of at least one heart activity cycle, thus both the camera and the laser measurement method sketched in this section would add an extra time of at least one or two seconds to the overall authorization process interval.

4.2.9.1 Physiological Basics of Heart Activity

Let us introduce some background basics for the following liveness detection based on heart activity measurement.

The function of the right side of the heart is to collect deoxygenated blood from the body and pump it into the lungs so that carbon dioxide can be removed and oxygen regained by diffusion. The left side collects oxygenated blood from the lungs and pumps it out into the body [106][75].

The left ventricle is much stronger (1.3 - 1.5 cm thick) than the right one (0.3 - 0.5 cm thick) as it has to pump blood around the entire body, which involves exerting a considerable force to overcome the vascular pressure. The right ventricle pumps blood to the lungs [106][75].

The function of the heart is to pump blood around the body (see Fig. 4.26a). Every single beat of the heart involves a sequence of events known as the cardiac cycle, which consists of three major stages: atrial systole, ventricular systole and complete cardiac diastole [106]. A more detailed description of heart activity exceeds the scope of this thesis and can be found in anatomy books such as in online medical libraries [106] or [75].

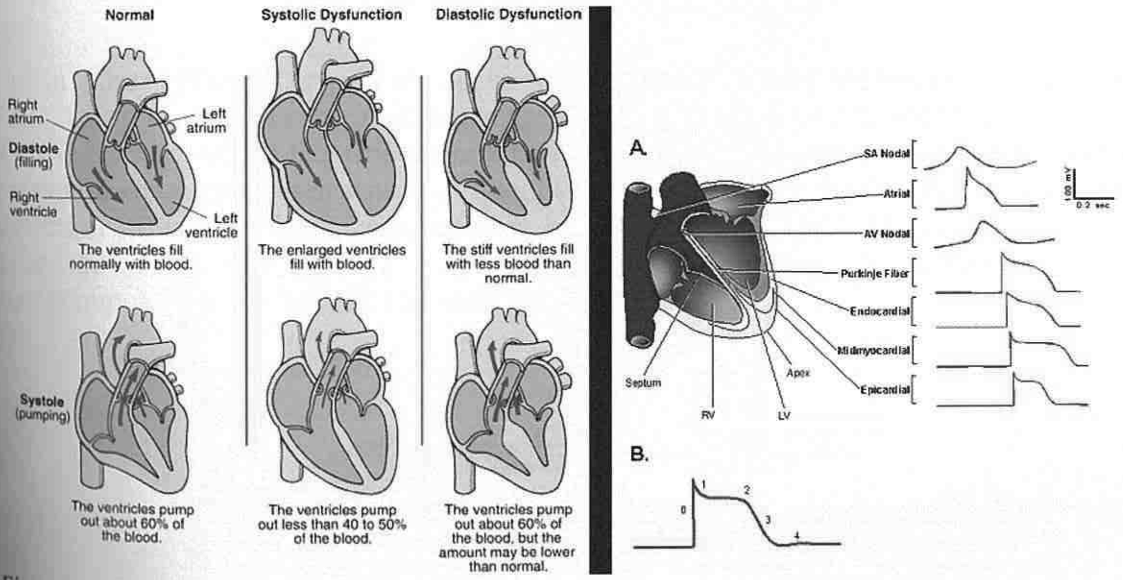

Normal
Systolic Dysfunction
Diastolic Dysfunction
Right atrium
Left atrium
Diastole (filling)
Right ventricle
Left ventricle
The ventricles fill normally with blood.
The enlarged ventricles fill with blood.
The stiff ventricles fill with less blood than normal.
Systole (pumping)
The ventricles pump out about 60% of the blood.
The ventricles pump out less than 40 to 50% of the blood.
The ventricles pump out about 60% of the blood, but the amount may be lower than normal.
A.
SA Nodal
Atrial
AV Nodal
Purkinje Fiber
Endocardial
Midmyocardial
Epicardial
100 mV
0.2 sec
Septum
RV
LV
Apex
B.
0
1
2
3
4

Fig. 4.26: a) (left) Demonstration of heart activity [106]; b) (right) Action potential waveforms and propagation in the human heart [68]: A. Schematic of action potentials, recorded in different regions of the human heart, are displaced in time to reflect the temporal sequence of propagation; B. Schematic of a ventricular action potential labeled as follows: 0=depolarization, 1=early (fast) repolarization, 2=plateau phase, 3=late (slow) phase of repolarization, and 4=after hyperpolarization/return to the resting membrane potential (SA=sino-atrial, AV=atrio-ventricular, RV=right ventricle, LV=left ventricle) [68].

Heart activity measurements are well-known as electrocardiogram (ECG) in medicine [26] (see Fig. 4.26b). An example of a record on ECG-measurement, the ECG-diagram or heart activity diagram, is shown in Fig. 4.27, where *P* denotes an atrial depolarization wave (right atrium is contracting in average time 80 ms, so-called filling phase), *T* is a ventricular repolarization wave (left atrium is dilating), and *U* is a late repolarization wave (late left atrium dilatation) [26][Dra17][Dra08].

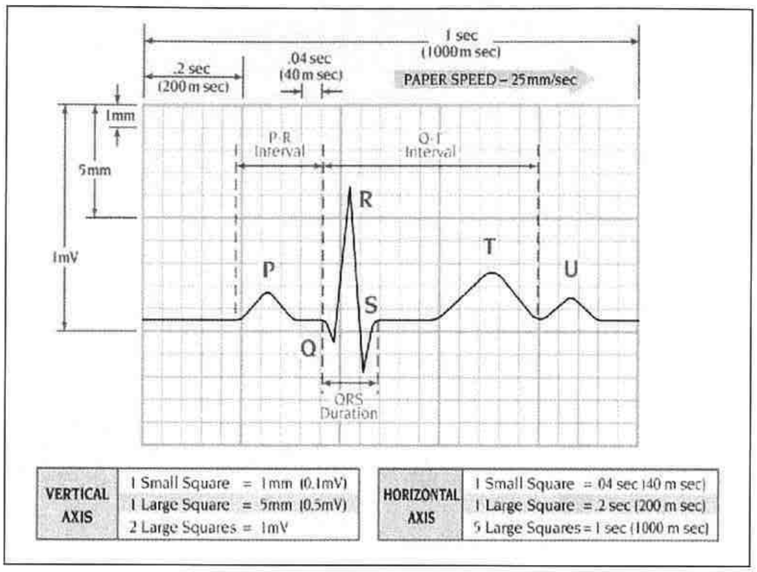


Fig. 4.27: ECG diagram example [107][75].

In [Dra17][Dra08], two approaches for measuring of fine movements of papillary lines, based on optical principles, are suggested (Fig. 4.28). The first solution is based on a close-up view of the fingertip acquired with a CCD camera; the second one is distance measurement with a laser sensor. It should be noted that adding the proposed liveness detection solution (either camera or laser based) to a fingerprint recognition system, as proposed in Fig. 4.29 and Fig. 4.31 may significantly influence the hardware requirements imposed on the complete system.

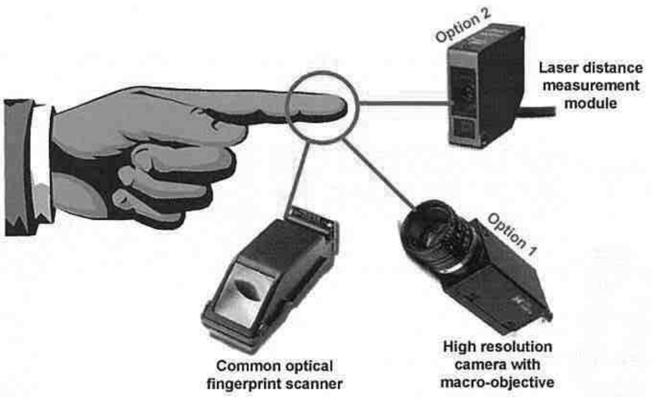

Option 2
Laser distance measurement module
Option 1
Common optical fingerprint scanner
High resolution camera with macro-objective

Fig. 4.28: Integrated liveness detection – scanner + optical and laser solution [Dra33].

4.2.9.2 Camera Solution

The camera solution scheme is outlined in Fig. 4.29. The main idea is that a small aperture (approximately 6 mm) is created in the middle of a glass plate with an alternately functioning mirror below the plate. First, during the fingerprint acquirement phase, the whole fingerprint is stored and the system operates as a classical fingerprint acquisition scanner (mirror permeable) by projecting the fingerprint on the CCD/CMOS camera. Next, in the liveness detection phase, the mirror is made impermeable for light and a part of the fingertip placed on the aperture is mirrored to the right and projected on the CCD/CMOS camera by a macro lens. The latter part of the system is used to acquire a video sequence for the liveness detection analysis.

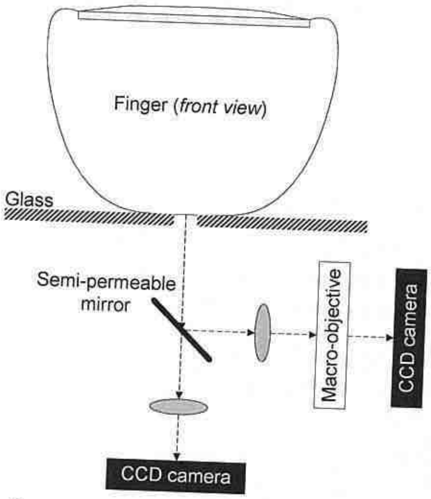


Fig. 4.29: Possible integration of a camera-based measurement system for liveness detection with optical fingerprint sensor (CCD/CMOS camera) [Dra17].

The important aspect in our case is the analysis of the video stream. First of all, the single frames of the video sequence are processed to find unique points (e.g. minutiae), which can be used as reference points to identify that region of the fingerprint which will be further analyzed. In the example shown in Fig. 4.30a, we use two papillary line bifurcations as the reference points. The distances between the reference points and papillary lines within the region defined by the reference points are computed for each image. From the sequence of images we can find the variation of those distances with time (Fig. 4.30b).

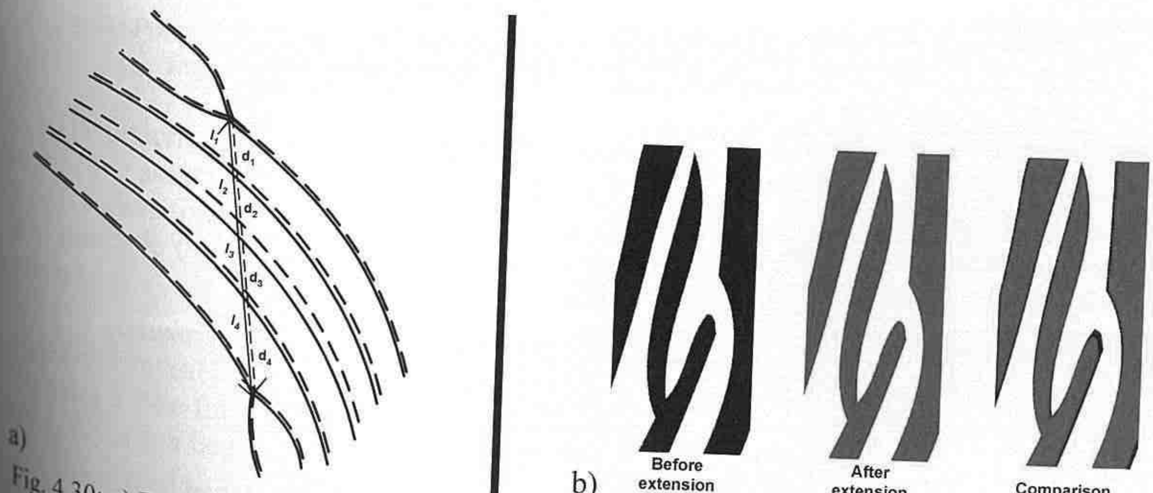


Fig. 4.30: a) Region for analysis of fine movements [Dra17]; b) Schematic representation of skin behavior before and after heart expansion [Dra33].

When the heart delivers blood (into the blood distribution system), each cell supplied with blood (called adenoblast) is expanding. The volume expansion causes the increase of distances between papillary lines [Dra17][Dra08], and vice-versa, the suction of blood back into the heart leads to the contraction of adenoblast cells, i.e. the volume contraction causes the decrease of such distances. In Fig. 4.30a two quadruplets of distances $d_1,\ldots,d_4$ and $l_1,\ldots,l_4$ are shown. The quadruplet l_i belongs to solid (papillary) lines and the quadruplet d_i to the dashed lines. During the volume contraction, we measure the distances l_i, whereas during the volume expansion, we measure the d_i distances.

4.2.9.3 Laser Solution

The second optical method for the liveness testing is based on laser distance measurements [Dra17][Dra08]. Fig. 4.31 outlines the laser distance measurement module, which could be integrated with a standard optical fingerprint sensor. The optical lens system and CCD camera for acquisition of the fingerprint are the same as in Fig. 4.29. However, unlike the solution shown in Fig. 4.29, the laser distance measurement module is placed to the right side of the glass plate, which is L-shaped here. The user places his finger in such a way that it is in contact with the horizontal and the vertical side of the glass plate.

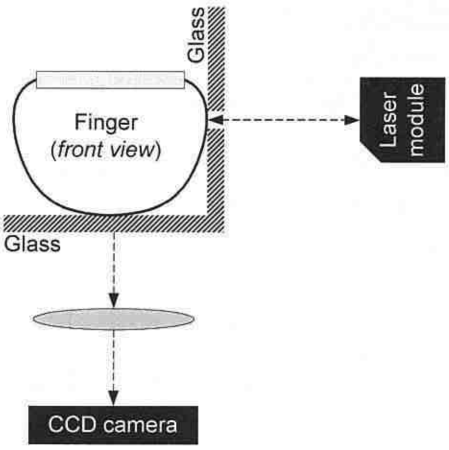


Fig. 4.31: Possible integration of laser distance measurement for liveness detection with optical fingerprint sensor (CCD/CMOS camera; aperture approx. 6 mm) [Dra17].

The underlying physical measurement principle is the same as in the video camera solution. We assume volume changes (expansion and contraction) due to the heart activity, which causes fine movements of the skin. The laser sensor is able, based on the triangulation principle (see chapter 4.4.5.3), to measure very small changes in distance down to several µm.

The comparison of the computed curve and a normalized standard curve (the template) will reveal whether the measurement corresponds to a standard live fingerprint or indicates a fake finger or another attempt of fraud. For example, the comparison between both curves can be realized by the normalization followed by the cross correlation.

The optical bench (designed by me) used for my experiments is shown in Fig. 4.32.

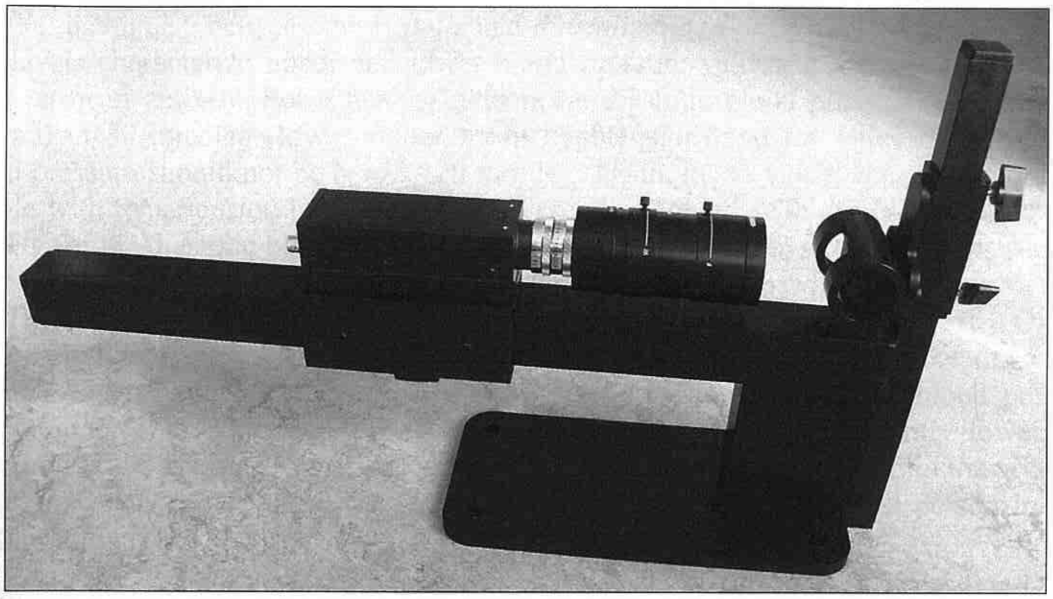


Fig. 4.32: Photography of my optical bench for measurement by the above mentioned methods.

There are other liveness detection methods based on optical principles – see [100] and [101]; some of them have been introduced in chapter 4.2.6. They coincide in principles (both are optical) but differ in monitored physical characteristics.

4.2.10 Physical Characteristics: Blood Oxygenation

Sensors which measure *blood oxygenation* [48] are mainly used in medicine and have also been proposed for use in liveness testing modules. The technology involves two physical principles. First, the absorption of light having two different wavelengths by hemoglobin differs depending on the degree of hemoglobin oxygenation. The sensor for the measurement of this physical characteristic contains two LEDs: one emits visible red light (660 nm) and the other infrared light (940 nm). When passing through the tissue, the emitted light is partially absorbed by blood depending on the concentration of oxygen bound on hemoglobin. Secondly, as the volume of arterial blood changes with each pulse, the light signal obtained by a photo-detector has a pulsatile component which can be exploited for the measurement of pulse rate.

The sensors mentioned above are able to distinguish between artificial (dead) and living samples but, on the other hand, many problems remain. The measured characteristics vary from person to person and the measurement is strongly influenced by dyes and pigments (e.g. nail varnish).

4.2.11 Other Methods

There are some other methods based on the medical science characteristics which have been suggested for liveness testing purposes [48]. Nonetheless, they are mostly inconvenient and bulky. One example can be the measurement of *blood pressure* [Dra17] but this technology requires to perform measurement at two different places on the body, e.g. on both hands.

We distinguish between the *systolic* and *diastolic blood pressure* [116][Dra17]; these two levels characterize upper and lower blood pressure values, respectively, which depend on heart activity. For a healthy person the diastolic blood pressure should not be lower than 80 mm Hg (lower values mean hypotension) and the value of the systolic blood pressure should not be below 120 mm Hg (again, lower values mean hypotension). People with hypertension have higher blood pressure values, with critical thresholds 140 mm Hg for the diastolic blood pressure and 300 mm Hg for the systolic blood pressure. In fact, diastolic and systolic blood pressure values are bound up with the ranges from 80 mm Hg to 140 mm Hg and from 120 mm Hg to 300 mm Hg, respectively [116]. On one hand, blood pressure values outside these normal ranges can indicate a fake fingerprint [Dra17]. On the other hand we can think of configurations, where the blood pressure measurement of a fake fingerprint glued to the finger which significantly lowers the measured blood pressure value, can still give us a measurement value within the accepted range. An attacker with hypertension would be accepted as a registered person in such configuration [Dra17].

4.3 Practical Experiments from Literature

In this subchapter, some practical experiments found in the literature are introduced, together with some results illustrating the field of liveness detection.

4.3.1 Deceiving of Thermal, Capacitive and Optical Fingerprint Sensors

The test in [122] consisted from reading of images and their analysis using the identification software. Silicon fakes and images from a dead person were used as fake fingers. Fig. 4.33 shows the comparison of original and fake silicon finger.

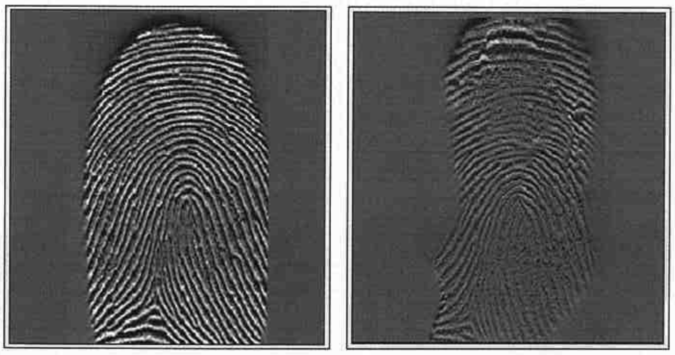


Fig. 4.33: Fingerprints from thermal sensor (from true finger (left) and silicon fake (right)) [122].

Although there are many different functionality principles in the capacitive technology, only some of them were tested in [122]. However, all of them led to the sufficient amount of minutiae – see Fig. 4.34a.

In some cases, it was needed to moisturize the silicon fake to get an acceptable fingerprint (Fig. 4.34b). In other cases, the use of graphite dust on the fake finger led to the success. The moisture or graphite simulated the conductivity of real skin.

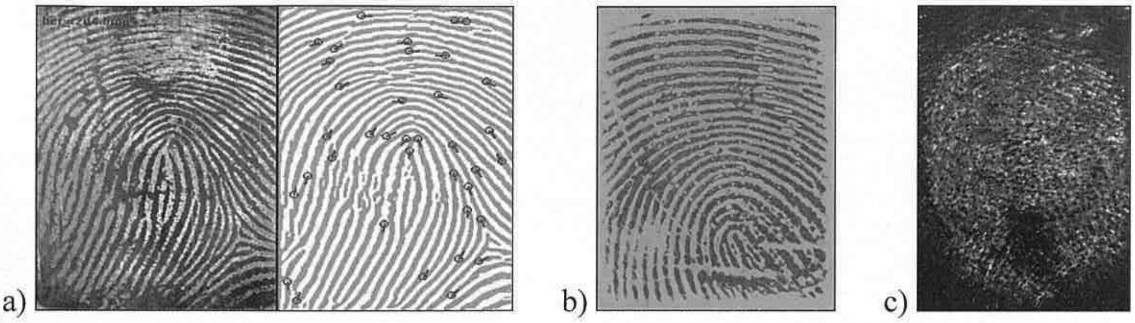


Fig. 4.34: a) Silicon fake fingerprint scanned by a capacitive sensor, with minutiae found in the image (left) [122]; b) Moisturized fake fingerprint scanned by a capacitive sensor [122]; c) Fingerprint of dead person scanned by a capacitive sensor [122].

The histograms of a moisturized fake finger and a real live finger are shown in Fig. 4.35. The dynamics (difference between the maximal peaks of grayscale values) corresponds in quality with the average live fingers.

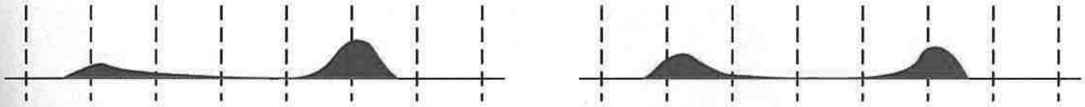


Fig. 4.35: Histograms [122]: left – moisturized fake finger; right – live finger.

It can be observed in Fig. 4.35 that the dynamics between the left and right maximum of both curves is very similar. The histogram of the fake finger resembles the histogram of the dry live finger. Strangely enough, the fake finger offers better quality than the live finger with dry or flat skin structure. The capacitive sensor was tested also with a sample of finger from a dead person [122] – see Fig. 4.34c. The death happened 12 hours before scanning; the body temperature during scanning was 6.5°C. Necessary to say that with such finger it was not possible to adjust the system to accept this "dead" finger for a successful recognition.

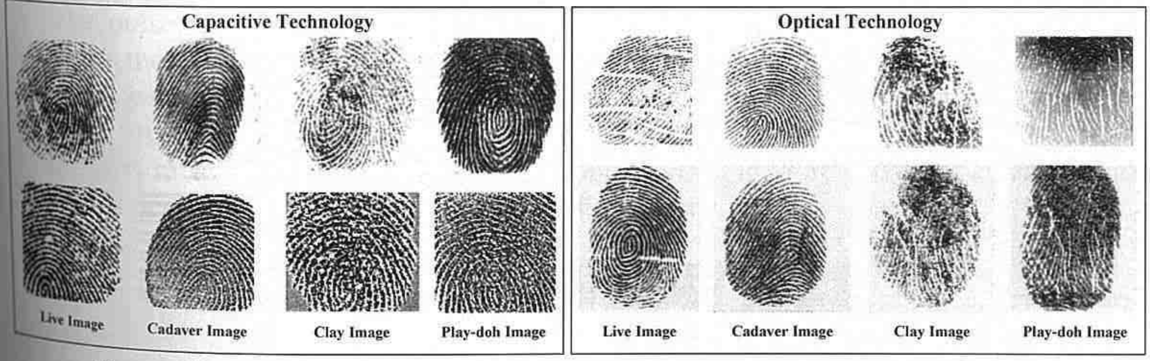


Fig. 4.36: Measurement of fake fingers using different scanner technologies [88].

Some examples of acquired fake fingerprints using capacitive or optical sensor technologies [88] are shown in Fig. 4.36. Other examples can be found in [64].

4.3.2 Biasing Current

It should be mentioned in conjunction with the measurement of conductivity that it is also possible to measure the biasing current on the body which is caused by the electromagnetic field in the environment. The functionality of the body as an antenna has been tested in [122] for signals with 50 Hz – see Fig. 4.37.

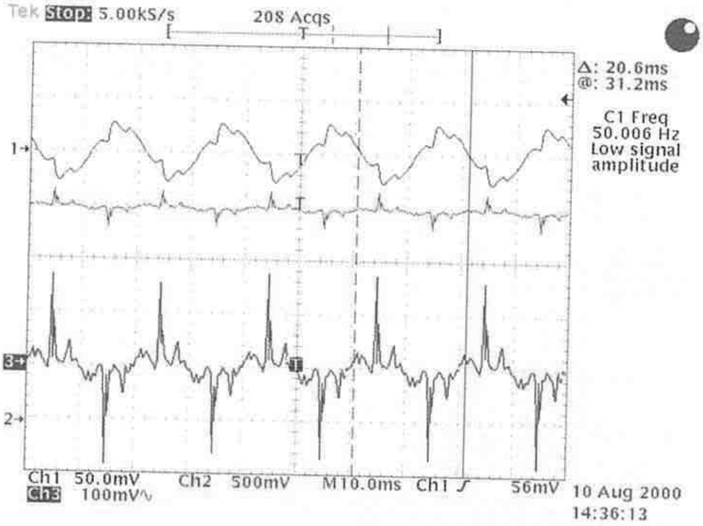


Fig. 4.37: Biasing current in connection with 50 Hz signals [122].

The channel 3 shows the alternation part of the signal [122], i.e. the incorporated portion of the human body. The filtered portion signal (using a bandpass-filter), which represents the biasing value, can be seen in the channel 1. When a fake finger was applied, it was not possible to detect this biasing signal. The problem in implementation would be the dependence on the place of measurement – no tolerance limits are defined.

4.3.3 Pulse

The pulse is a unique characteristic of a living organism. The liveness detection is based on the principle of changing mechanical and optical characteristics of blood in veins and capillaries of the finger. The mechanical changes of the finger resulting from the pulse are reflected in the acquired fingerprints but a sufficient amount of images or image parts must be recorded for practical application. Fig. 4.38 shows an example with 20 images per second acquired using a capacitive sensor.

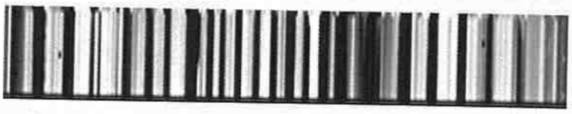


Fig. 4.38: Acquired 20 images per second using a capacitive sensor [122].

Notwithstanding the application of corresponding mathematical methods, no definite proof of pulse (and thus the liveness) was achieved in the example described in [122]. It is very difficult to keep the finger lying quietly on the finger scanner platen. On the other hand, it was possible to simulate the pulse by changing the pressure on the finger during scanning – see Fig. 4.39.

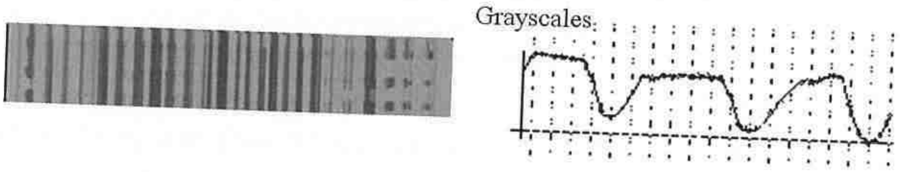


Fig. 4.39: Intentional changes of pressure on the finger and resulting graph [122].

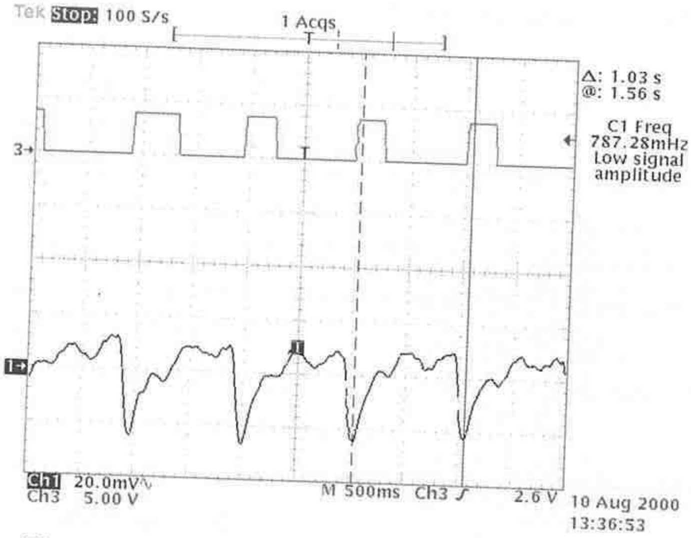


Fig. 4.40: Optical recognition of heart pulses [122].

The human tissue is relatively transparent for infrared light, especially in the range 600 – 1,000 nm. This has been exploited for the optical measurement of heart pulses. The color of blood depends on the saturation of hemoglobin with oxygen. When using suitable wavelength of light from the above mentioned range, we are able to measure the light intensity changes resulting from blood transport due to heart activity [122] – Fig. 4.40.

4.4 My Practical Experiments

In this subchapter, I would like to present some practical experiments in the field of liveness detection which I have performed in our laboratory at the Faculty of Information Technology, Brno University of Technology.

4.4.1 Production of Fake Fingers

The production of a fake finger(print) is described in [117][64] (Fig. 4.41). We have made comparable experiments with similar results, using professional dactyloscopic equipment.

The production of fake finger(print) consists of the following steps [117][64]:

1. *Finding a latent fingerprint (fat residues*). First of all, some suitable fingerprint is needed. It is very simple to find latent fingerprints on various materials. Latent

fingerprints with a good quality can be found especially on glass, slides, CDs/DVDs, shiny paper or door handles.

2. *Making the latent fingerprint visible*. The best way is to use special dactyloscopic equipment (special powders and brushes). Such powder is applied to the latent fingerprint using very soft brush. This powder keeps on the papillary lines.
3. *Making the latent fingerprint permanently visible*. It follows the application of a quick-drying glue (containing cyanoacrylate). Important are here the exhalations from cyanoacrylate, which keep on the papillary lines structures (better than using the dactyloscopic powder).
4. *Result of cyanoacrylate application*. White substance is built on the papillary lines and the latent fingerprint is made visible.
5. *Digitization of the fingerprint*. Such fingerprint is than acquired using a digital camera or a scanner.
6. *Enhancement and processing of the fingerprint*. Because the quality of the acquired fingerprint is often poor, it should be enhanced using special software. Wrong or corrupted papillary lines might be improved in this step.
7. *Application of wood-adhesive*. Special glue for wood is applied to the impression of the fingerprint on the slide.
8. *Coating of the wood-adhesive* on the whole fingerprint impression.
9. *Crusting (curing) of wood-adhesive*.
10. *Cutting off the fake fingerprint*. The size should be adjusted for a human finger.
11. *Finishing the fake fingerprint*.
12. *Taking and using foreign identity*...

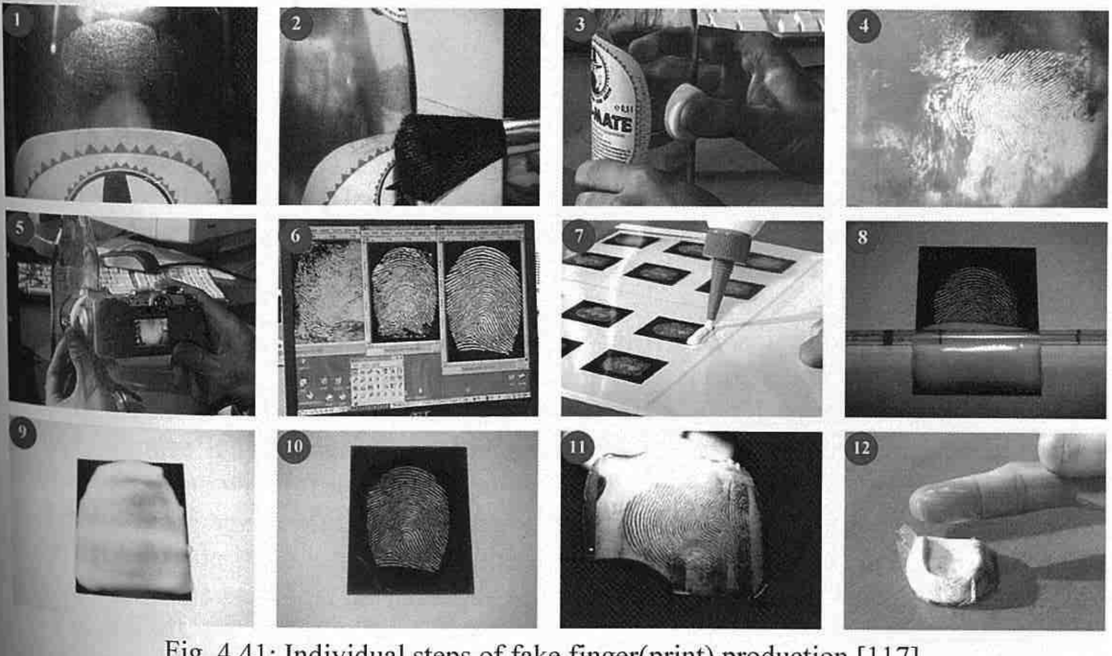


Fig. 4.41: Individual steps of fake finger(print) production [117].

4.4.2 Our Experiments on Deceiving of Thermal, Capacitive and Optical Fingerprint Sensors

We have successfully proven that the deceiving of fingerprint sensors (see chapter 4.3.1) with a stamped fingerprint is possible. A common office stamp set from a stationery shop has been used. The fingerprint stamp was made in two days and it cost 4 €.

We have tried to deceive three most used types (technologies) of fingerprint sensors. Our tests have started with the optical technology (sensor Suprema SFM 3020-OP). We have made several tens of attempts to deceive the sensor in the time period of several weeks and every attempt was successful. An example of the captured fingerprint stamp is shown in Fig. 4.42b and images captured from a real finger are shown for comparison in Fig. 4.42a and 4.42c .

The tests have continued with a thermal technology. At first, we have tried to deceive the sensor Suprema SFM 3010-FC. Unfortunately, this sensor has some protruding stripes for guiding the fingerprint in the right direction which damaged the fingerprint stamp. We have therefore tried another sensor (Bergdata FCAT 100 – thermal technology). Both sensors are based on the Atmel's FingerChip technology (most widespread solution for thermal sensors). They can be fooled easily but it depends on the skills of an intruder because the work with a thermal sensor is generally more difficult than the work with other sensors. An example of the stamp captured by a thermal sensor is in Fig. 4.42d and the real fingerprint captured by the same sensor is in Fig. 4.42c.

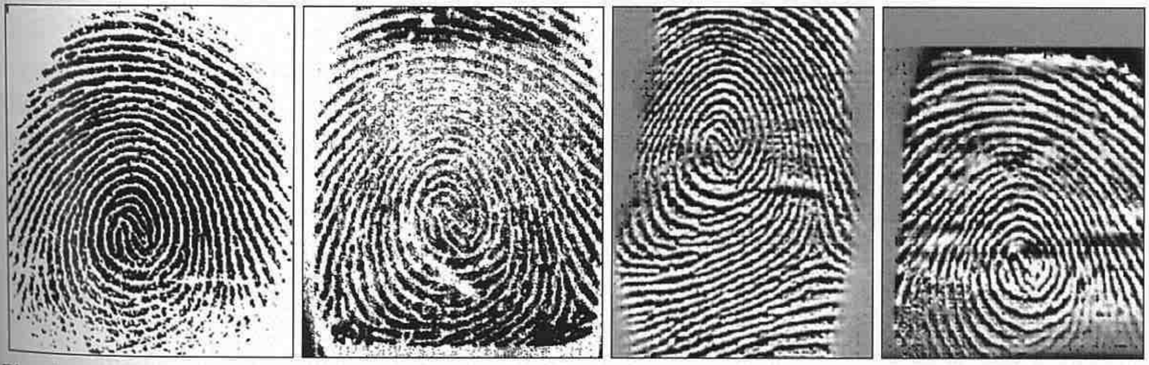


Fig. 4.42: Fingerprint images [Dra33] (from left to right): a) real finger captured by an optical sensor; b) fingerprint stamp captured by an optical sensor; c) real finger captured by a thermal sensor; d) fingerprint stamp captured by a thermal sensor.

The last tests have been done with the capacitive sensor Suprema SFM 3050-TC1. First of all we have tried to reactivate a latent fingerprint using the method of simple breathing on the sensing area [Dra33][Dra05]. However, this method requires some experience because it is difficult to estimate the degree of such breathing. Next we have continued the tests with a fingerprint stamp. The captured image of the stamp is shown in Fig. 4.43b (the image contrast is rather poor). After breathing on the stamp, the conductance of its surface increases and the quality of captured image also increases (see Fig. 4.43c). This image is almost perfect (it is indistinguishable from the image of a real finger – see Fig. 4.43d).

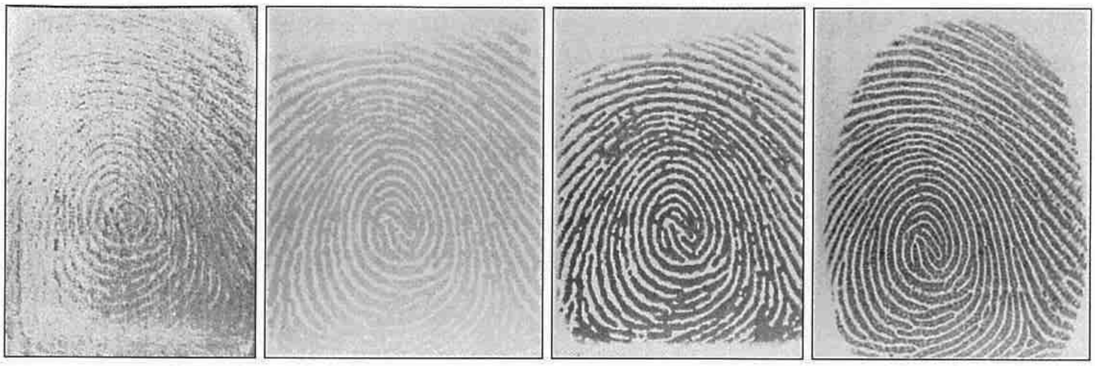


Fig. 4.43: Images captured by a capacitive sensor [Dra33] (from left to right): a) simple breath; b) stamp; c) stamp and breath; d) real finger.

4.4.3 Testing of Liveness by Temperature Measurement

Now we will discuss the temperature measurement test. Using the temperature measurement, it is possible to distinguish between a dead person or fake finger(print) and a living person. The temperature of living human tissue is approximately 37°C [122]. However, an intruder can overcome the problem by warming up the fake finger to the temperature of a live tissue.

The following text describes our own measurements [Dra06]. This simple method of liveness detection measures the temperature of the epidermis during fingerprint acquisition. The temperature of the human finger epidermis is in average in the range of 25-37°C (see chapter 4.2.4) [Dra06]. However, this range usually has to be made wider to make the system operational under different conditions. In addition, there are many people who have certain problems with blood circulation what results in deviations in the body temperature and leads to wrong decisions of the liveness testing module. The only way to improve such a situation is to make the working range even broader or simply warm up the user's finger. The former precaution could increase the likelihood that the system will be deceived while the latter one can also be applied on fake samples. When an attacker uses a wafer-thin artificial fingerprint glued onto his finger, the temperature of such fake sample may decrease only by 2°C compared with a direct application of a true finger [Dra06]. Since the difference in temperature is small, the wafer-thin sample can comfortably fall within the normal working margin and pass a liveness detection test.

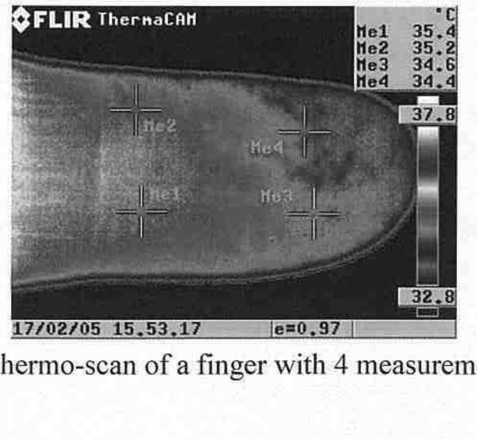


Fig. 4.44: Thermo-scan of a finger with 4 measurement points.

Our further experiments – measurement of human skin temperature – have been made using one thermo-camera FLIR ThermaCAM™ PM545G (see Fig. 4.44). Users from different human races (European, Asiatic and African) participated in this experiment.

The thermo-scan from this thermo-camera has the resolution 320×240 pixels. In this device, it's possible to set five measurement points with direct indication of the temperature in the right upper corner. We used only 4 of them – see Fig. 4.44. They formed a rectangle – one side of rectangle was near the end of the finger and the second one near the phalanx.

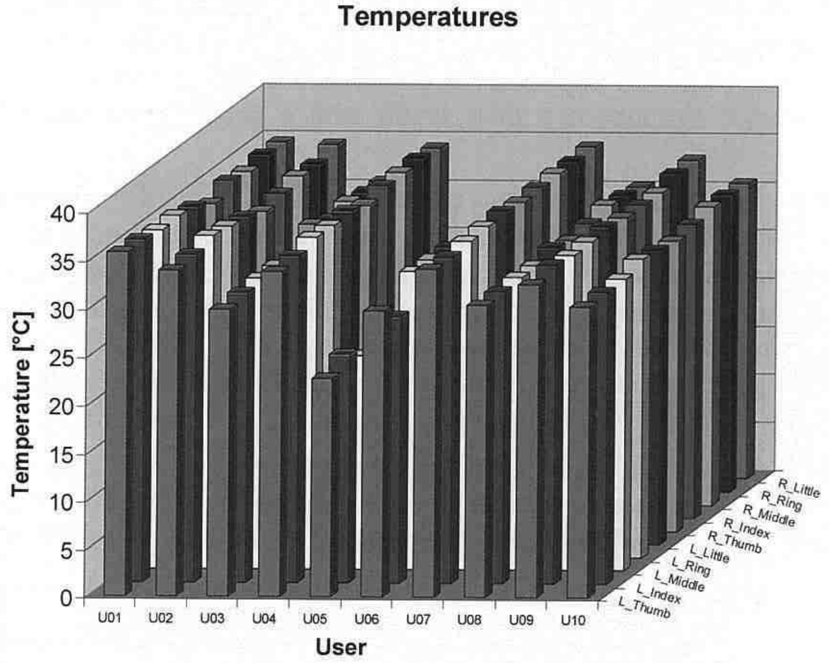


Fig. 4.45: Average temperature values for all users and all fingers [Dra06].

All measurements have been taken at the room temperature and humidity in one day (the reason was to preclude any changes in room temperature and humidity, in addition, the outdoor temperature can influence such measurement). The index of thermal radiation of human skin was set to *e*=0.97. The room temperature was in average 26°C and humidity about 64%. Only ten users participated in the test (these were the same people as in the resistance measurement – see chapter 4.4.4), but it was enough to get the results as indicated below. Each user was scanned only once, all ten fingers and each finger four times.

If you carefully analyze Fig. 4.45, you can see that the variations of skin temperature of respective participants are quite high. The differences in temperature of fingers of the same participant are not so high but distinguishable. Our observation is that the temperature difference between the left and right hand of one participant can be "only" approx. 0.6°C. This value seems to be unimportant, but the difference between live finger and fake finger could be lower. The skin temperature varied between the extreme values 21.5°C and 35.7°C (it should be mentioned that only healthy people (i.e. without fever) participated in our test).

4.4.4 Conductivity / Resistance

The conductivity value of a finger placed between two electrodes could be used as a sign of the living body. However, it is necessary to take in consideration the fact that the magnitude of the conductivity can vary strongly and depends on various factors, e.g. skin thickness, diameter of the finger, humidity of the finger surface and position and wear of surface of both electrodes [122].

In the measurements realized in [122], the values of conductivity of a finger were in the range $2\cdot10^{-6}$ S and $3.3\cdot10^{-7}$ S. The measurements of conductivity on the finger of a dead person gave the value approx. $3.3\cdot10^{-8}$ S. The measurements on the silicon fake finger gave the values close to zero. This option seems to be a very simple method for a check measurement on the live tissue. However, it is also very simple to imitate the conductivity of a real finger using a fake finger with a conductive layer (e.g. of graphite powder).

Some methods of liveness testing are based on the fact that a live human skin has different electrical properties compared with other materials. A suitable fingerprint recognition system could be then adapted by adding an electrode system and an electrical evaluation unit [Dra06]. These are the main parts of the liveness testing module with the electrical evaluation unit which is able to evaluate any change in the state of the electrode system. The detection of such electrical change should take place at the same time with the recognition of the fingerprint to ensure the simultaneity.

We prepared a small experiment with the measurement of finger skin resistance of living people [Dra06]. The scheme and arrangement of measurement point(s) is shown in Fig. 4.46. The following instruments/equipment were used for this experiment:

- *Automatic LCR Meter 4210*, model 1EW-4210, Farnell Instruments, Ltd.
- *Keithley 179-20A TRMS Multimeter*, Keithley Instruments
- *Ohmmeter BS407 Precision Milli/Micro Ohmmeter*, TTI
- *Copper slices*, with the area 18×8 mm, thickness 1 mm, R_S=6,3 mΩ
- *Copper wire*, R_W=8,7 mΩ

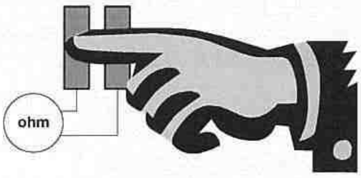


Fig. 4.46: Measurement of finger skin resistance (conductance).

The copper slices were placed vertically and horizontally (both directions of the finger have been measured). We have employed two methods of skin resistance measurement:

- Method 1: direct current (DC), U=4 V (low voltage)
- Method 2: alternating current (AC), U=4 V (low voltage), f=100 Hz

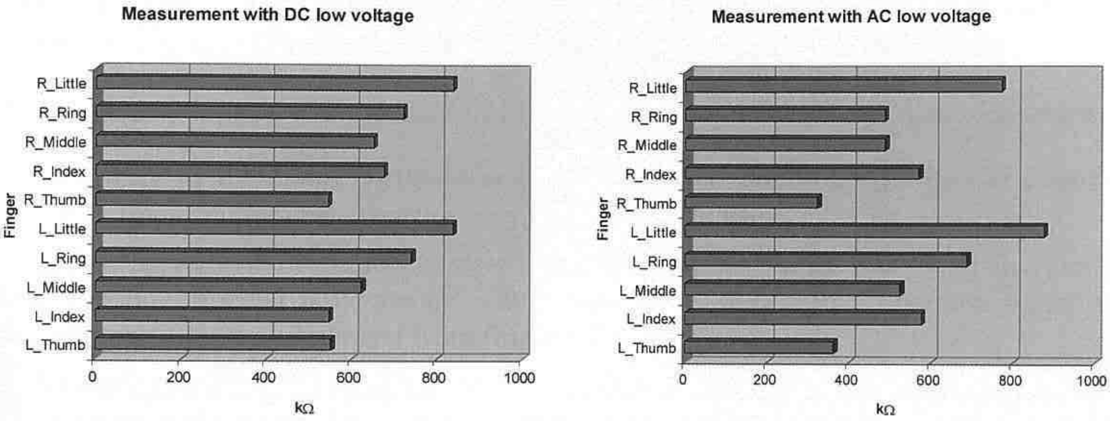


Fig. 4.47: a) Resulting average resistances for DC low voltage measurement [Dra06] (left); b) Resulting average resistances for AC low voltage measurement [Dra06] (right).

Ten users from different human races (European, Asiatic and African) participated in the experiment. Each participant has been scanned only once, all his fingers, and each finger five times. The averaged results of all measurements are shown in Fig. 4.47a and Fig. 4.47b (DC and AC low voltage measurement, respectively). The name of finger and corresponding resistances are outlined in these graphs. Generally, it could be said that the differences among individual fingers are significant, but cannot be somehow generalized (statistically or mathematically described).

After all tests, we have deduced two intervals for changes in skin resistance [Dra06]:

- Method 1, DC: <20 kΩ, 2 MΩ>
- Method 2, AC: <20 kΩ, 1.7 MΩ>

Because the difference is not important, we can confirm that the type of current (AC/DC) plays no role in the measurement. It's clear that the use of DC is more practical, as the most biometric devices are operated with DC. However, when using AC, it would be better to measure the bio-impedance (see chapter 4.2.8).

The main reason for such a broad interval of skin resistance is the finger skin moisture. Some participants had a very dry skin what resulted in high resistance (low conductivity), and vice versa, some had a wet skin what lead to very low resistance (high conductivity).

We have found some interesting additional information [Dra06][Dra07]. The difference between left and right hand of each user is approximately 5 kΩ to 10 kΩ. In the test, there was no difference between the use of copper slices or copper wire. In both cases, the skin resistance was always same. Pros and cons of each copper type should be discussed before the implementation of this method of liveness detection.

4.4.5 Pulse

Short description of pulse measurements has been done in chapter 4.3.3. It has taken approximately 3 seconds to acquire a set of data, i.e. the measurement has taken 3 or more seconds. At least 3 pulse curves had to be measured – for adjustment, because the heart activity of different people varies slightly to marginally (e.g. in combination with some disease).

4.4.5.1 Assumptions for Our Method of Liveness Detection Based on Pulse Measurement

According to the [Dra17], the skin on the finger expands by 13 μm in diameter (6,5 μm in finger radius) between the systole and diastole stage.

The measurement of basic characteristics of papillary lines was done in [Dra32] [Dra21] using a special laser device. The results were plotted in a diagram, where the maximal amplitude was deducted from (Figure 4.61).

According to precise measurements of the ridge and valley distances and proportions [90], the maximal distance between two neighboring papillary lines is 0.7 mm. An analysis tried to answer the question how often the inter-papillary lines occur between papillary lines. The distances between papillary lines and the proportion (width and height) of papillary and inter-papillary lines had been also quantified. All the values are displayed in Tab. 4.1.

It is clear that the inter-papillary ridges are significantly lower than papillary ridges. Therefore, their appearance on the fingerprint image taken by optical sensor depends on the angle of illumination of the finger. With some lower value of this angle, they might be hidden in the shadow of the papillary edge.

The change of width of the finger during pulsation is very small. For the detection of the change of distance between papillary lines, it is enough just to take a cut-out of the fingerprint with one whole papillary line and one beginning edge of the neighboring papillary line. As the method cannot reject a person just for his large fingers or papillary ridge distances, the maximum possible value has been taken into calculations [Dra32]. Therefore, it is considered that the distance for successful measurement is equal to the maximum distance between two papillary lines, i.e. 689.4 μm ≈ 700 μm = 0.7 mm.

Tab. 4.1: Distances of ridges and valleys [Dra32].

Measured distance	Avg. value [μm]	Deviation [μm]	Minimum [μm]	Maximum [μm]
Inter-papillary ridge height	24.9	±10.0	14.9	34.9
Papillary ridge height	59.0	±19.2	39.8	78.2
Inter-papillary ridge width	194.8	±65.1	129.7	259.9
Papillary ridge width	435.5	±57.4	378.1	492.9
Papillary ridges distance (incl. inter-papillary ridge in between)	610.5	±78.9	531.6	689.4
Papillary ridges distance (without inter-papillary ridge)	484.9	±70.6	414.3	555.5

First, we need to realize that the expandability of the papillary lines must be captured at least by one pixel within the scanned image [Dra32]. Therefore, the size of change must be evaluated. We know that the finger changes 13 μm during the pulse in its diameter. The finger is not planar. In fact, mathematically, it is some kind of a deformed cylinder. If you place a finger on a horizontal plate and make a virtual vertical cut, you will receive roughly an ellipse. An ellipse could be simplified to a circle. The circumference of the circle is $o=2\times\pi\times r$, where r is the diameter of the circle. A half of the circumference is $o_h=\pi\times r$. As the top of the skin expands by $\Delta = 6.5$ µm (a half of 13 µm), the circumference is also expanding. The change of circumference (c_c) divided by the amount of papillary lines (N) gives a change per one papillary line (x).

We could estimate the number of papillary lines in this way [Dra32]: We know the sum of distance between two papillary lines and width if the line appears alone. It is $l = 700$ µm = 0.7 mm. The estimation of number of papillary lines could be done in this way. Next, let's consider, that the width of the finger (not a thumb) is 20 mm, what makes 10 mm for its radius r.

$$r = 10{,}000\,\mu m; d = 6.5\,\mu m; l = 700\,\mu m$$

$$o'_h = \pi \times (r + \Delta) = 31{,}436.35\,\mu m \tag{4.1}$$

$$c_c = o'_h - o_h = \pi \times (r + \Delta - r) = \pi \times \Delta = 20.42\,\mu m \tag{4.2}$$

$$N = \frac{o'_h}{l} = 44.78 \tag{4.3}$$

$$x = \frac{c_c}{N} = 0.454\,\mu m \tag{4.4}$$

From the previous calculation (Eq. (4.4)), we have obtained the change of skin expansion (which happens due to the pulsation wave) per one papillary line. The value is 0.454 µm, which is a very small value. In fact, this value, if it should be measured, is so small, that it collides with the wavelength of visible light (0.39 µm – 0.7 µm). This could lead to the problem of blurring during measurements. Another problem rises from the circle of confusion.

None of the lenses produces a precisely sharp image. When you are capturing a small point of light in infinite distance (let's assume a very long distance) with nearly zero diameter, the point displayed on the image plane will have some (even very small) diameter. This diameter is called circle of confusion [Dra32] and the effect (which happens due to this) is called aberration [Dra32]. Usually, the circle of confusion is being estimated as 1/1,000 of focal length of the lens system, or from Zeiss formula as 1/1,730 of the diameter of the chip [Dra32]. Another problem could be with the effect called chromatic aberration [Dra32]. The wavelengths of the white light are in interval from 0.39 µm to 0.7 µm. A chromatic aberration phenomenon occurs when the red parallel rays from the object plane intersects in a different point in the image plane than the blue parallel rays. This problem could be solved either by using a monochromatic light to illuminate the finger or by adding a photo-filter or software processing of the scanned image.

Further computations and estimations of optical distances, focal lengths, etc., could be found in [Dra32].

For a preliminary verification of the liveness detection method proposed in [Dra17][Dra08] (chapter 4.2.9), some practical experiments have been performed with a simplified test setup compared to the proposed integrated liveness detection component in Fig. 4.29 and Fig. 4.31.

4.4.5.2 Liveness Detection – Camera Solution

For the liveness testing based on a camera solution (see chapter 4.2.9.2), I have used for my experiments at the beginning a video camera with macro lens having zoom factors 4 and 10. Some example frames from the video stream are shown in Fig. 4.48. The black spots in the images were caused by dirt in the optical system of macro lens.

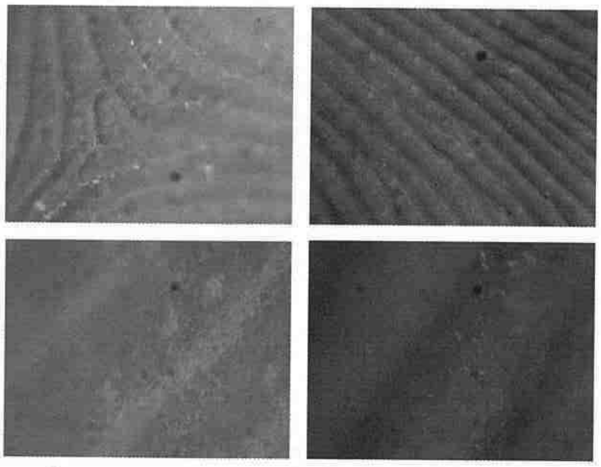


Fig. 4.48: Macro lens test frames with zoom factors 4 (upper row) and 10 (lower row) [Dra17].

In the images with the zoom factor 10 no minutiae or other reference points can be identified, whereas the images with the zoom factor 4 have enough information with respect to reference points. Unfortunately, the zoom factor is not high enough for detecting the fine movements of the papillary lines. From these results, we can conclude that we need a zoom factor of 10, but with a clear optical system of higher quality than the one used in the beginning phase, so that both the fine movements and the minutiae can be identified.

In Fig. 4.49, all used installations are shown (from left: the first prototype for patent submission experiments, the installation for diploma thesis and finally the actual optical bench for measurements at our faculty).

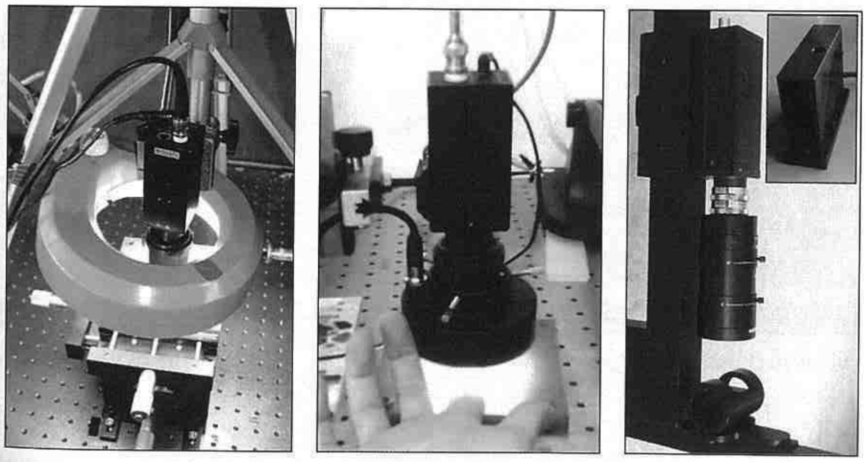
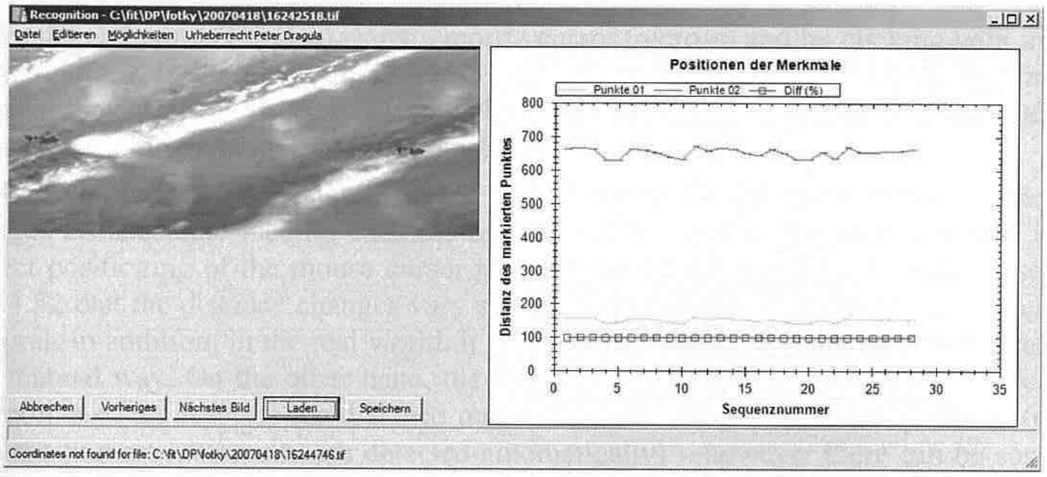


Fig. 4.49: Used optical device installations.

In [Dra03], there are described some experiments using the resulting images (video-sequences) from the first and second installations (Fig. 4.49). One of the results is shown in Fig. 4.50, even when it was not possible (due to the camera resolution and dirt in the optical system) to recognize the fine movements of the papillary lines. However, in [Dra03] and [Dra32], there are published some contemplations and computations (performed under my supervision), which lead to the improvement of the optical measurement installation (see Fig. 4.49 right; the laser unit is shown in the right upper corner).



Coordinates not found for file: C:\fit\DP\fotky\20070418\16244746.tif

Fig. 4.50: Screenshot from the detection application of fine movements of papillary lines [Dra03].

Within the scope of this work, fifteen videos have been acquired (covering 3 users and 5 fingers) with the duration 15 seconds each and zooming 10×. The following equipment has been used for the acquirement:

- Industrial camera Sony XCD-SX910CR (FireWire)
- Macro-objective Computar MLH-10x
- Illumination unit – LED Osram Golden Dragon® LCW W5SM (white)

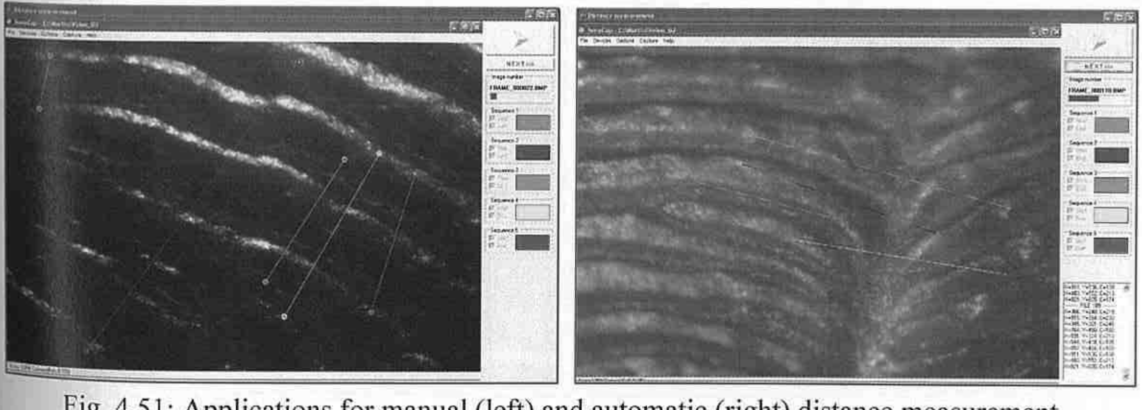


Fig. 4.51: Applications for manual (left) and automatic (right) distance measurement.

From these video sequences, 220 images containing each frame from the whole video file have been extracted. These image files were subjected to an analysis using two applications or procedures (manual and automatic) implemented for this purpose – see Fig.

4.51. The application for the *manual measurement of distance changes* makes possible to set manually the positions of relevant points (areas with the highest luminosity – the analyst had to find such points and to put the mouse cursor on them) in the image with papillary lines extracted from the video sequences. The *automatic application* finds the most sensitive points (pixels with the highest luminosity) in the image and computes automatically the distances in the whole image sequence.

Always 5 distances were used (see Fig. 4.51: colors green, red, cyan, yellow and blue), whereas the end points (circles) have been selected only by manual setting (the user places the end points (circles) using a mouse cursor (a cross) and by clicking with the left mouse button). In the automatic modus, these circles are shown only in the first image, while in the following images only the abscissas are shown – the reason is to be able to control the right positioning of the end points by the user.

It is evident that the manual setting of end points for the measurement of distance changes is inaccurate (see an example on Fig. 4.52) – due to the inaccurateness in the correct positioning of the mouse cursor to the always same position. It could be seen in Fig. 4.52 that the distance changes vary significantly and do not show any periodical behavioral. In addition, in the real world, it is not possible to perform the liveness detection in a manual way. On the other hand, the algorithm in the automatic application puts the end points of an abscissa for distance measurement always to the same position (pixels with the highest luminosity are detected automatically) – however there can be some instability in finding such end points due to the variation of luminosity in the surroundings, what could lead to finding of the neighboring point (a tolerance box of ±5 points has been used).

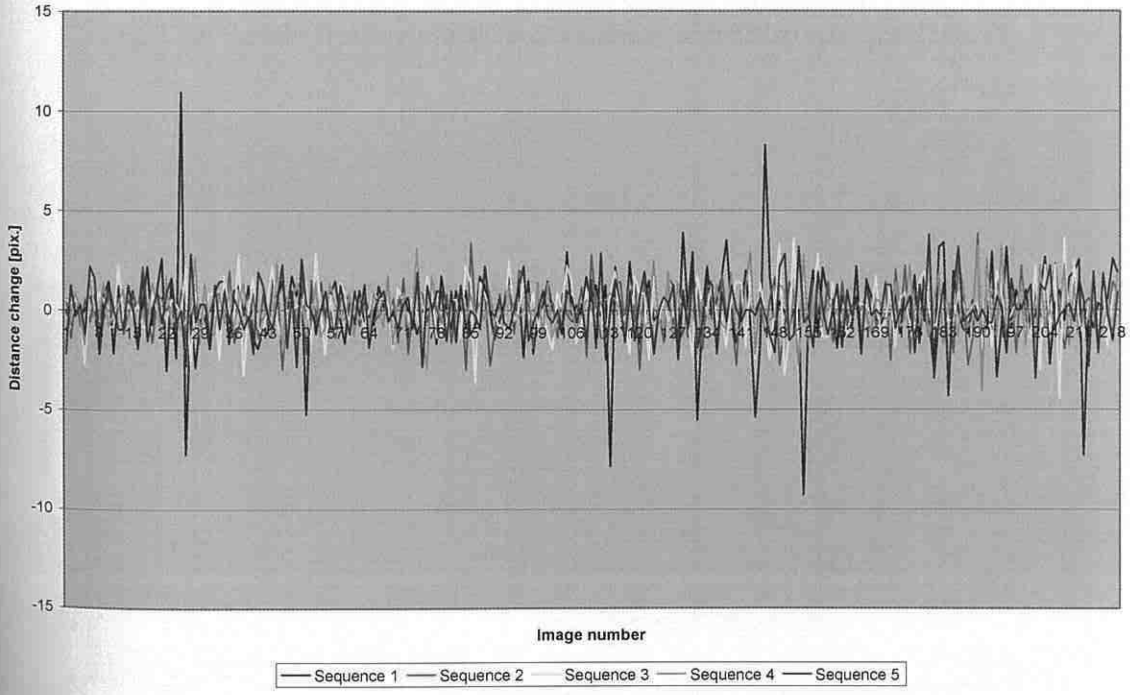


Fig. 4.52: Example of manual distance measurement method (User 1).

In Fig. 4.53 to 4.55, there are three examples of changes in automatic distance measurement modus for all three users in the test. In all graphs, there are distortions caused by changes of illumination during the acquirement process. These illumination changes were caused by hand shaking – different fine shadows were formed on the papillary lines, what lead to the fine changes in illumination. It is necessary either to fix the hand or to use more advanced image filtering.

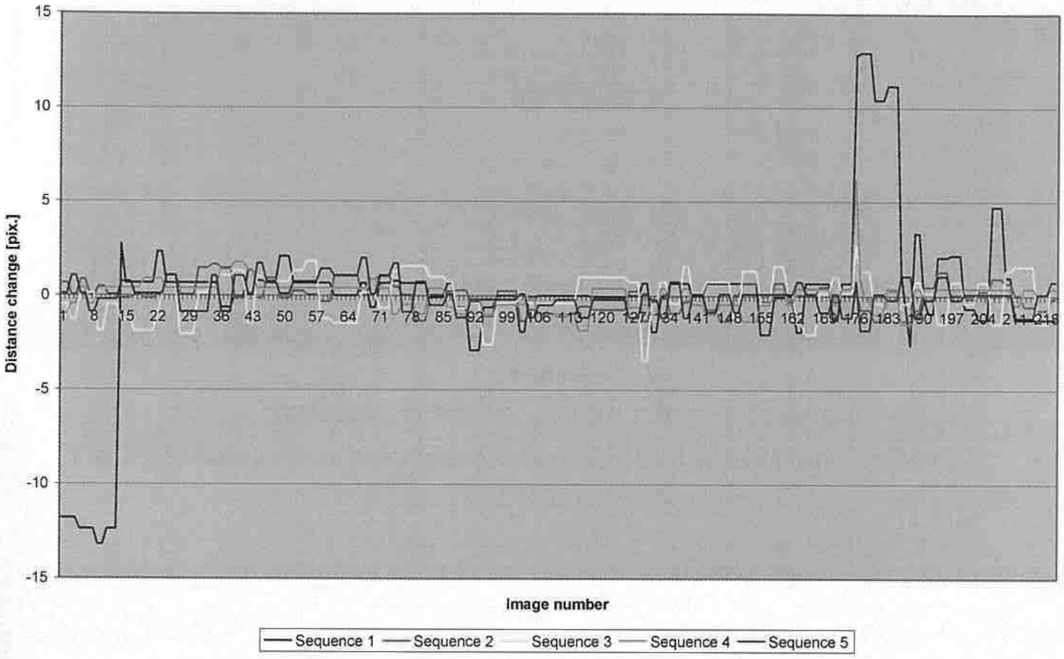


Fig. 4.53: Results from automatic measurement of distance changes (User 1).

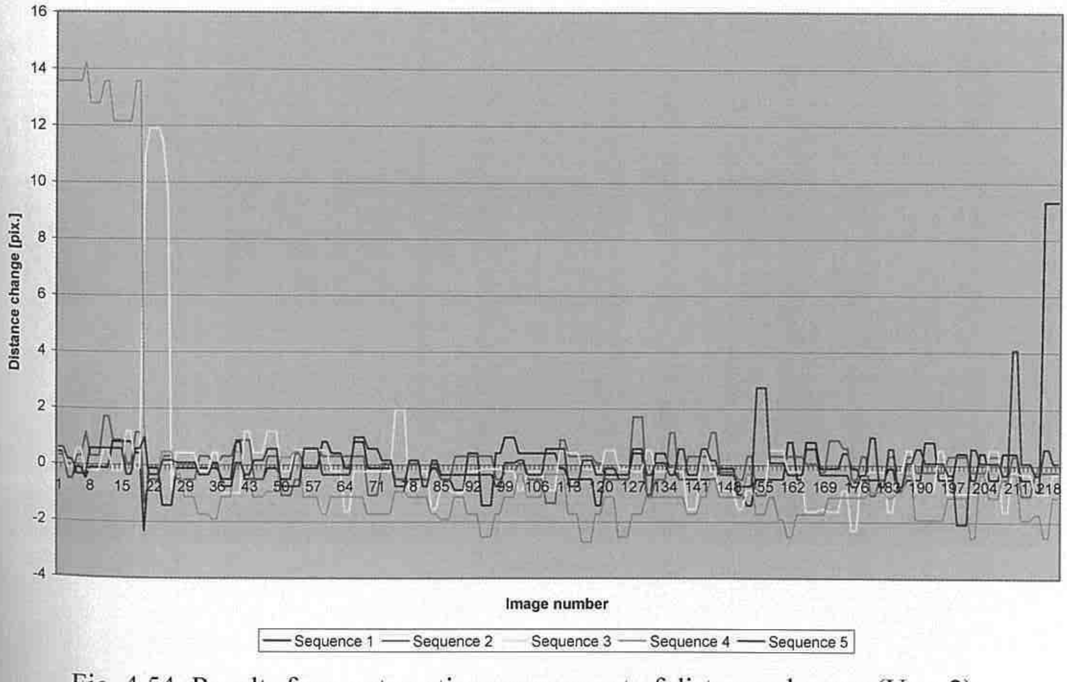


Fig. 4.54: Results from automatic measurement of distance changes (User 2).

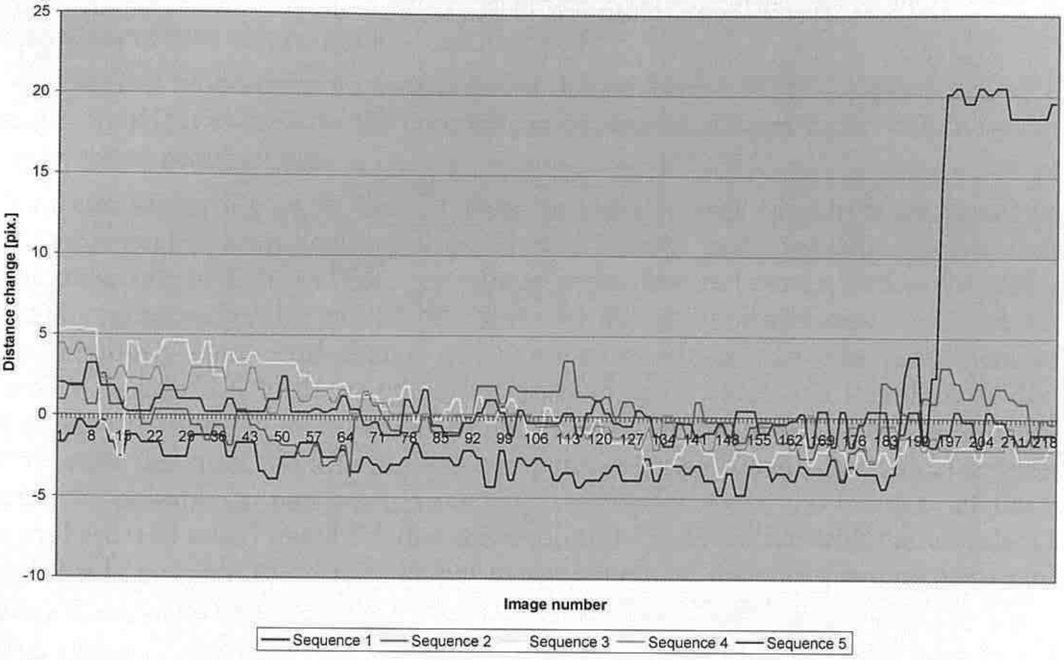


Fig. 4.55: Results from automatic measurement of distance changes (User 3).

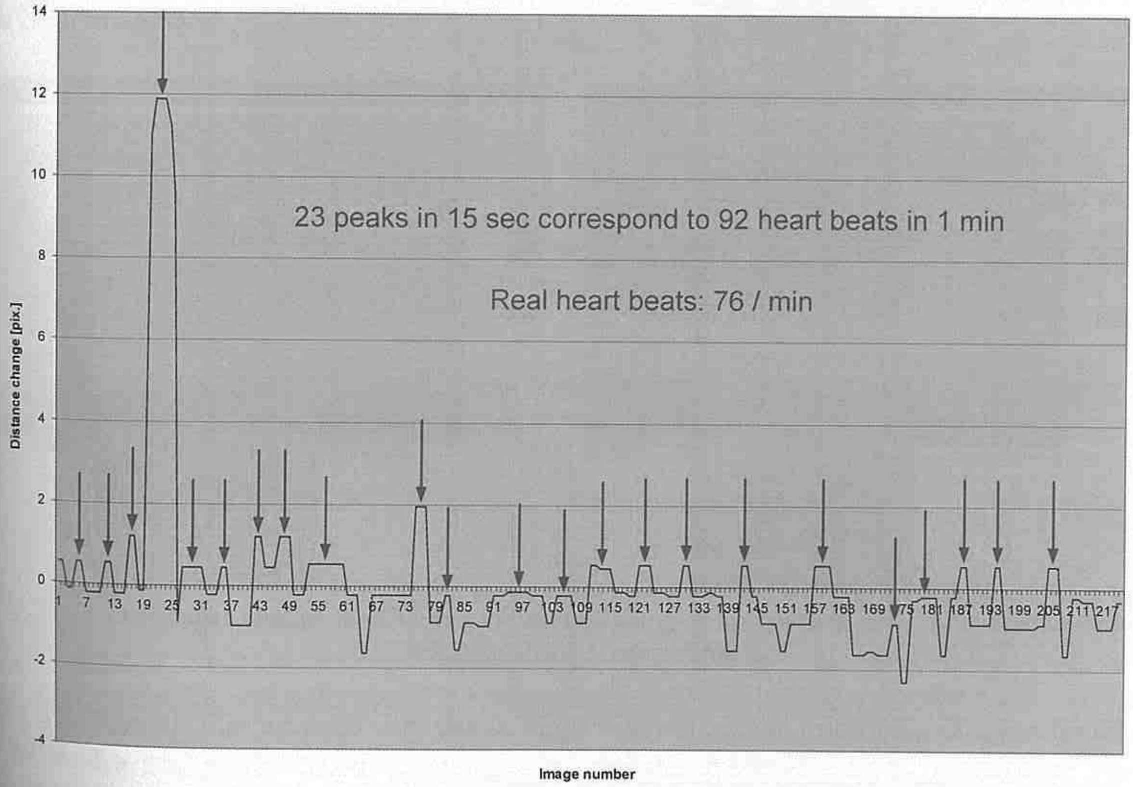


Fig. 4.56: Analysis of the sequence 3 (yellow) from Fig. 4.54.

Although some fine changes appeared in illumination caused by hand shaking, some periodical curve runs can be found – see Fig. 4.56.

The medical blood pressure measurement device Sanitas SBM 04 (produced by Hans Dinslage GmbH) was used for the comparison of measured heart beats with the real ones during all video acquirements.

You can see in Fig. 4.56 that 23 local maximal values (peaks) were found which might correspond to heart beat impulses. These 23 peaks in a 15-second interval indicate that the pulse rate is 92 heart beats per minute, what does not correspond to the real (conventionally measured) value of 76 heart beats per minute. The difference could be caused by the previously mentioned change of illumination, which led to the movement of the previously found pixel to the neighboring pixel in some cases and therefore to the distance change resulting in incorrect peaks. No filtering of the curvature has been used. We can only state that after the filtering and computation of a probable periodical behavioral, it would be possible to make some relevant statements about the liveness of the user. Though there was stated in 4.4.5.1 that the resolution could collide with the wavelength of the light, it is possible to do this optical measurement of distance changes between two papillary lines, because the changes are in some micrometers.

The situation of failure in finding of neighboring point with higher luminance (which is responsible for the distance changes leading to the detection of more peaks in sequence, or in other words, to the detection of higher than the real (conventionally measured) value of the pulse rate) is shown in Fig. 4.57 (magenta and green arrows show to the same place in both images).

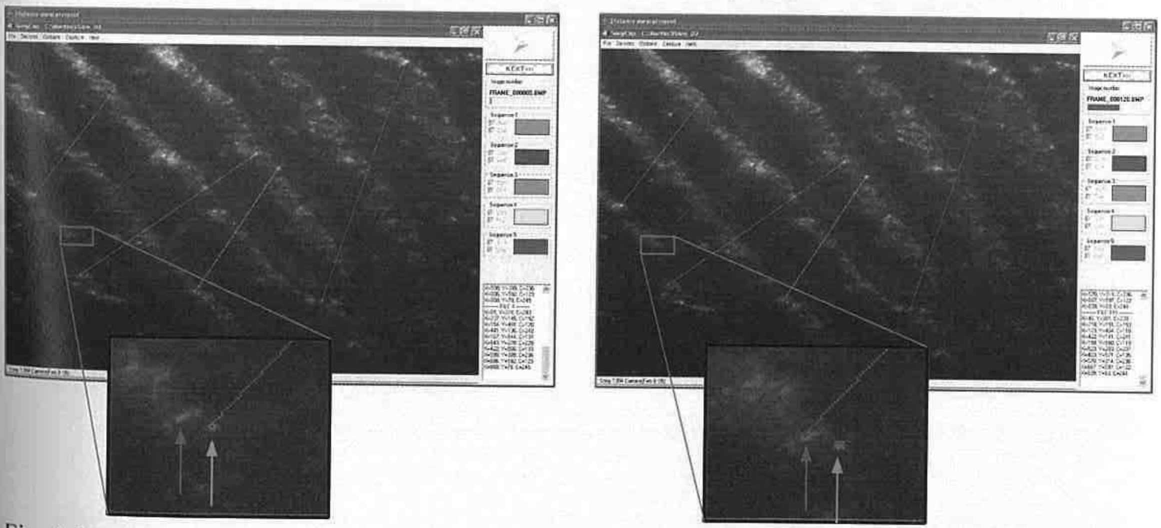


Fig. 4.57: Luminance change leading to a failure in finding of appropriate end points in automatic distance change measurement.

The result is that we need very stable finger fixation, zoom minimally 10× (preferably 12×) and a good illumination unit. In this case it would be possible to detect the fine changes in papillary lines movements caused by the heart activity. This method seems to be reliable, but it needs higher computational performance (capacity) in comparison to the following laser solution.

4.4.5.3 Liveness Detection – Laser Solution

For the second experiment with the liveness detection based on a laser module solution (see chapter 4.2.9.3) we have used a Panasonic LM10 laser connected to an oscilloscope. The LM10 device is well suited for measurements with the accuracy 1 μm and works with the wavelength 685 nm. The measurement principle is based on triangulation; see the sketches in Fig. 4.58: The lighting equipment may be located at *A*, whereas the camera is located at *B*. The leg *AP* and the space coordinates of the object point *P* can be calculated from the angles α and β and the length of the triangle base *AB*. The installation of the laser measurement unit is shown in Fig. 4.59.

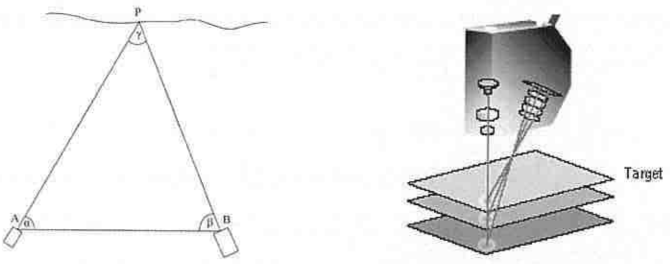


Fig. 4.58: Principle of triangulation [Dra17][118].

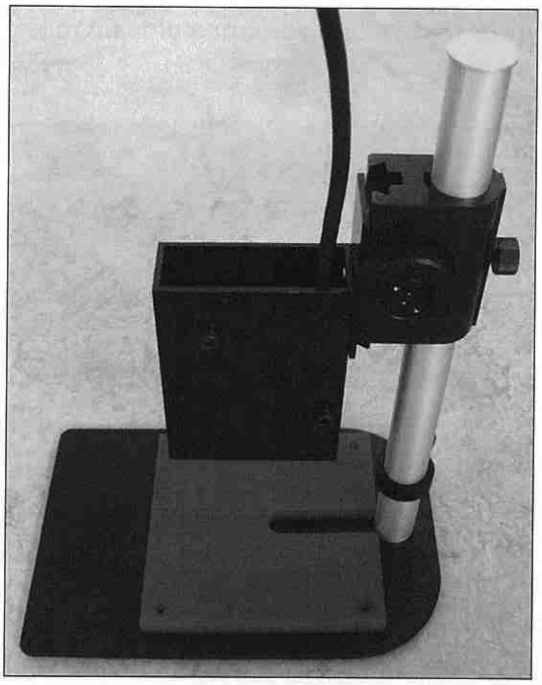


Fig. 4.59: Laser measurement installation for liveness detection.

Fig. 4.60 shows an example plot from our first tests. The curve shows the variation of the distance of a point on the fingertip surface from the laser sensor (vertical axis) with time (horizontal axis). We can see the expected periodic changes of the distance with time caused by the periodic changes of the fingertip volume.

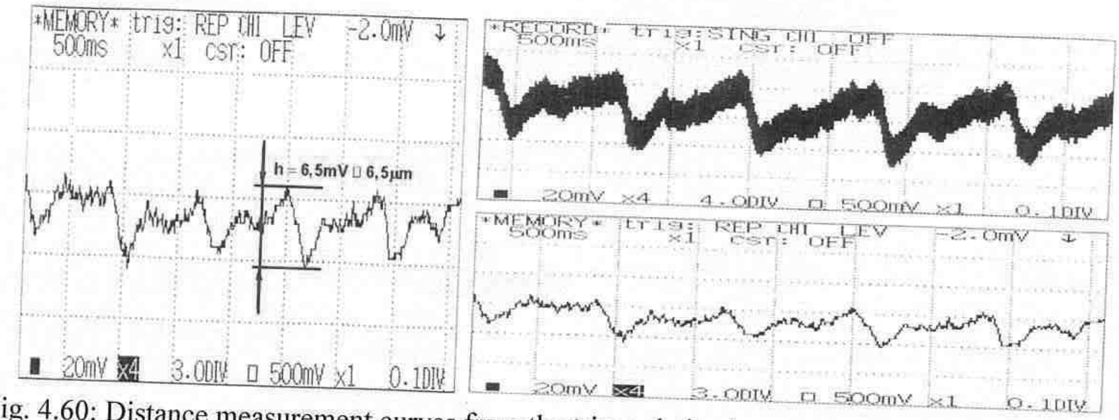
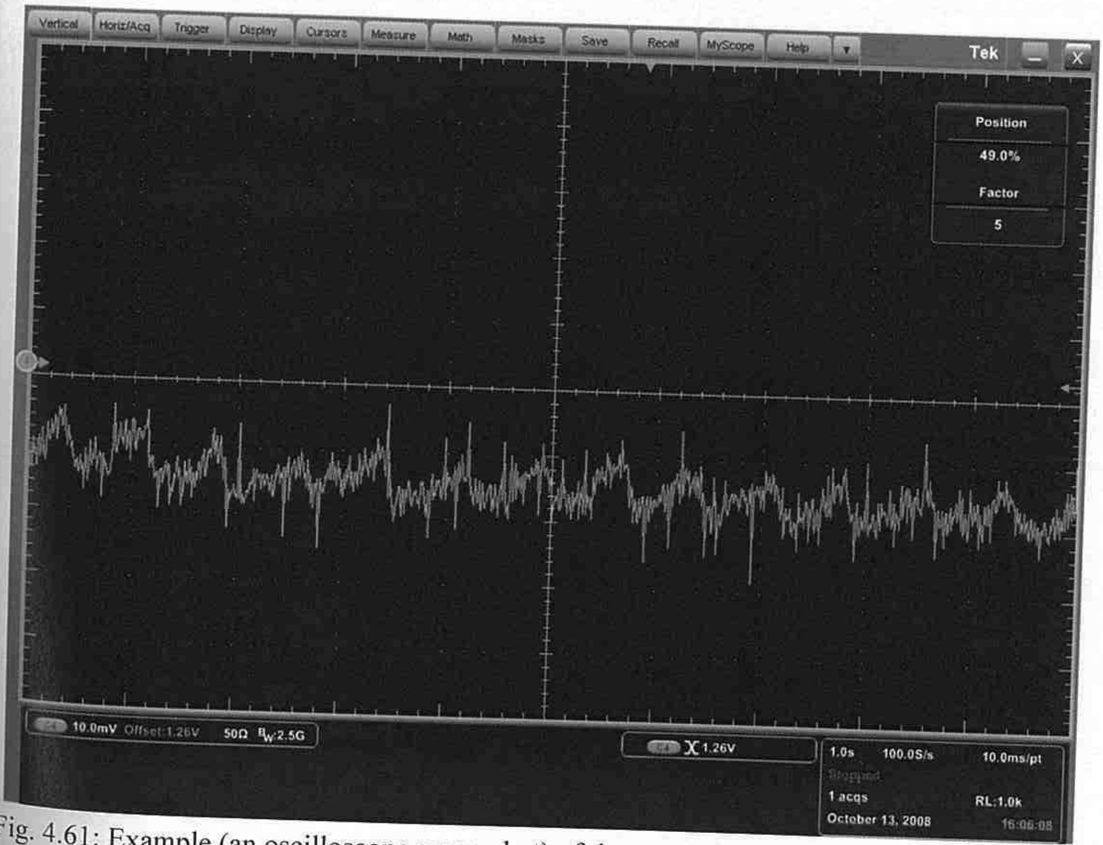


Fig. 4.60: Distance measurement curves from the triangulation laser sensor. Abscissa: time; ordinate: voltage reflecting distance changes [Dra17].

The new curves have been acquired using the following equipment:

- Laser module Panasonic LM10 ANR1250
- Control unit Panasonic LM10 ANR5132 for the laser module
- Oscilloscope Tektronix DPO7254

One example of the acquired curve (screenshot of the oscilloscope) is shown in Fig. 4.61. There is very well recognizable periodical behavioral of the curve – the period corresponds to the heart activity.



Position
49.0%
Factor
5

C4 10.0mV Offset:1.26V 50Ω B_W:2.5G
C4 ⨯ 1.26V
1.0s 100.0S/s 10.0ms/pt
Stopped
1 acqs RL:1.0k
October 13, 2008 16:06:08

Fig. 4.61: Example (an oscilloscope screenshot) of the curve representing the heart beat rate.

Within the scope of this thesis, an application for the computation of normalized and adjusted curve from the oscilloscope diagram was implemented – see the result in Fig. 4.62.

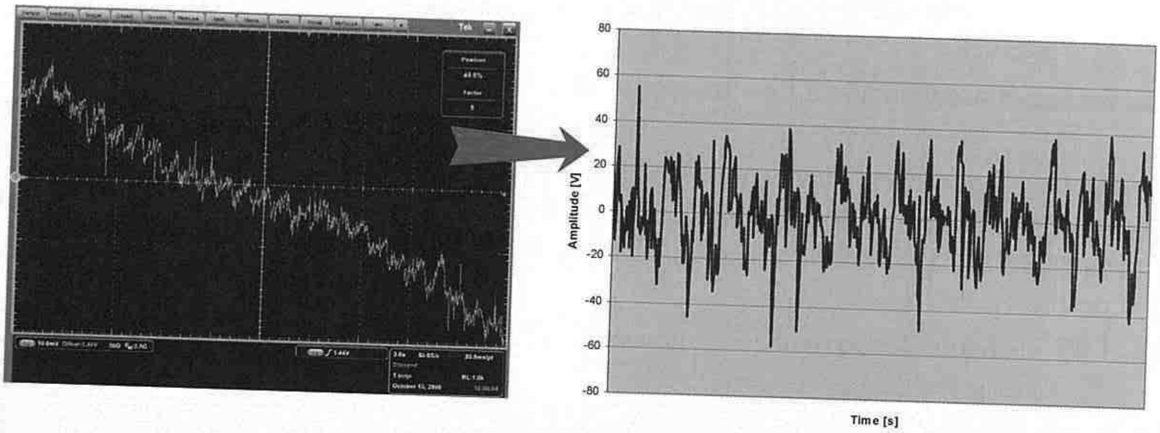
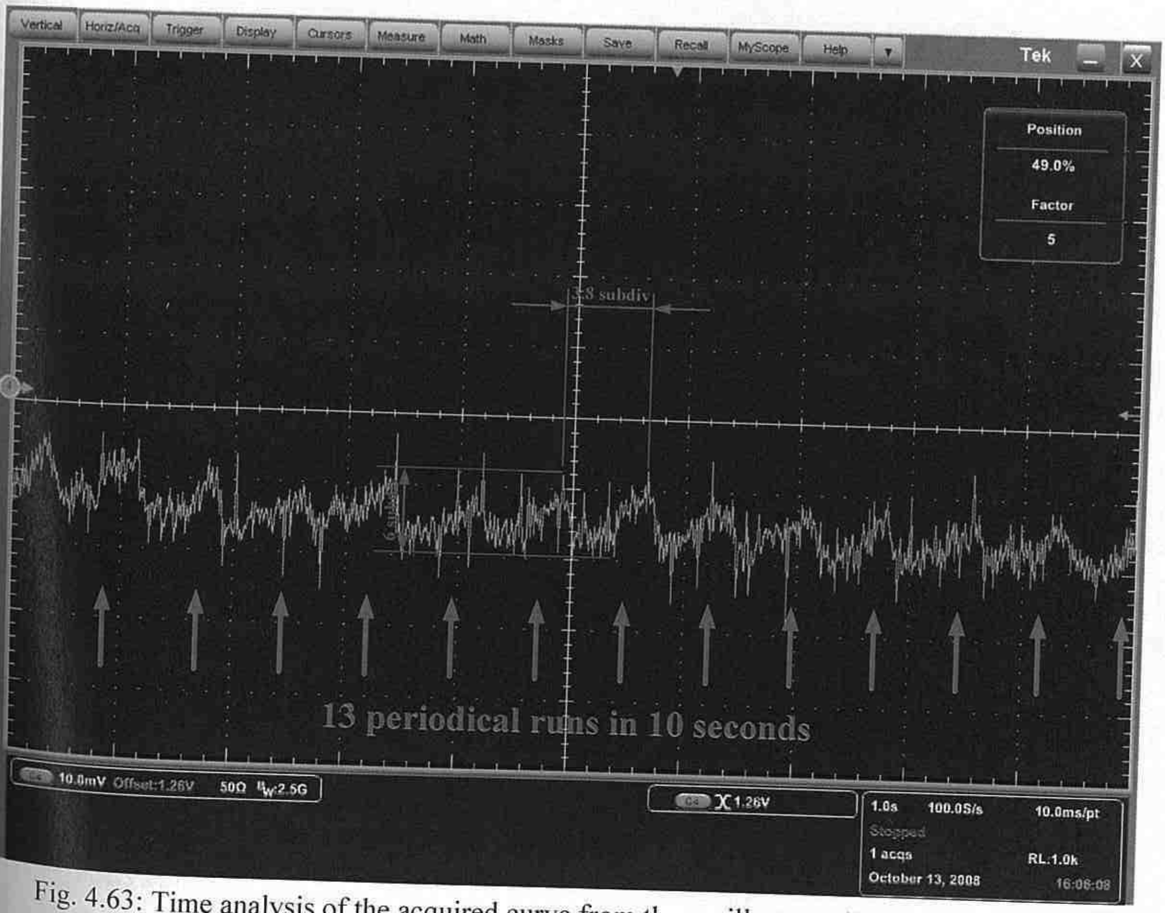


Fig. 4.62: Original (left) and normalized and adjusted (right) curve from the oscilloscope.

It was necessary to set the acquirement modus of the oscilloscope to very low frequencies (50-100 samples/sec), because the heart beat rate corresponds approximately to one beat per second – it is therefore reasonable to use the time interval of 1 or 2 seconds.



Position
49.0%
Factor
5

C4 10.0mV Offset:1.26V 50Ω BW:2.5G
C4 ✗ 1.26V
1.0s 100.0S/s 10.0ms/pt
Stopped
1 acqs RL:1.0k
October 13, 2008 16:06:08

Fig. 4.63: Time analysis of the acquired curve from the oscilloscope (1 second/division).

An analysis of the acquired signals has been performed – see Fig. 4.63 and Fig. 4.64. The curve in Fig. 4.63 has the following attributes:

- Axis *x*: time, 1 second / division.
- Axis *y*: voltage, 10 mV / division.
- Amplitude of one periodical run: 6 subdivisions → 12 mV between the minimum and maximum values.
- Time period of one periodical run: 3.8 subdivisions, what corresponds to 0.76 second per one run; verification: 49.4 (3.8 × 13) subdivisions in 50 subdivisions (10 divisions × 5 subdivisions) → the average value should be 50/13 = 3.85 subdivisions.
- 13 periodical runs (heart beats) in 10 seconds (10 divisions) found → 78 heart beats per 1 minute.
- Real heart beat rate (measured by Sanitas SBM 04): 76 per min. The concordance of computed and conventionally measured values is quite good.

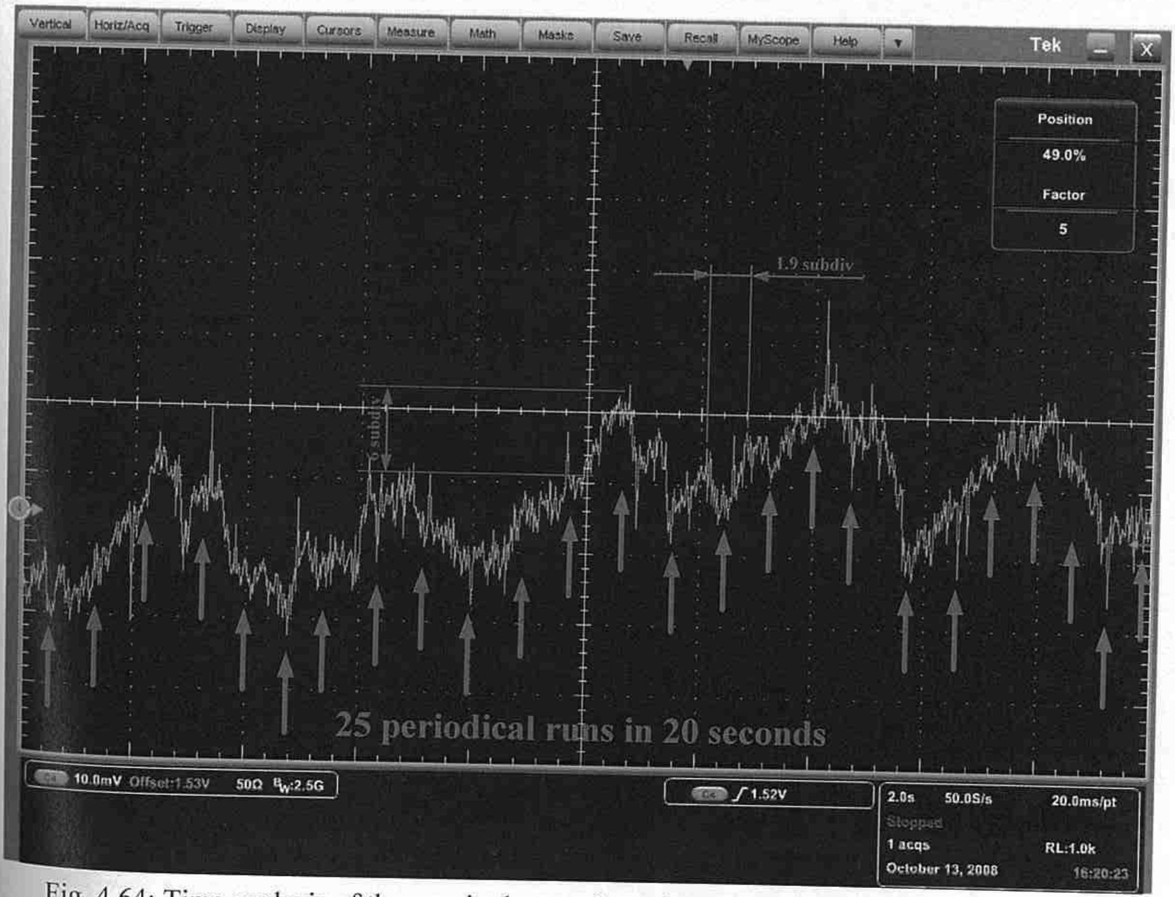


Fig. 4.64: Time analysis of the acquired curve from the oscilloscope (2 seconds/division).

The curve in Fig. 4.64 has the following attributes:

- Axis *x*: time, 2 seconds / division.
- Axis *y*: voltage, 10 mV / division.

- Amplitude of one periodical run: 6 subdivisions → 12 mV between the minimum and maximum values.
- Time period of one periodical run: 1.9 subdivisions, what corresponds to 0.95 second per one run; verification: 47.5 (1.9 × 25) subdivisions in 50 subdivisions (10 divisions × 5 subdivisions) → the average value should be 50/25 = 2 subdivisions.
- 25 periodical runs (heart beats) in 20 seconds (10 divisions) found → 75 heart beats per 1 minute.
- Real heart beat rate (measured by Sanitas SBM 04): 70 per min. The concordance of computed and conventionally measured values is still good.

As we can see from both graph analyses, the deviation of estimated (some periodical runs, especially in Fig. 4.64, are not clearly recognizable) heart beat rates (derived from the oscilloscope graphs) from the real heart beat rate values is not marginal. The real (conventional) measurement of heart beat rate is more accurate, because it takes longer time for measurement.

An example of the analysis of the normalized and adjusted curve from the application is shown in Fig. 4.65. There have been found 18.7 periodical runs in 20 seconds, what corresponds to the 56.1 heart beats in 1 minute. The real (conventionally measured) value was 57 heart beats per minute. The concordance is clearly visible.

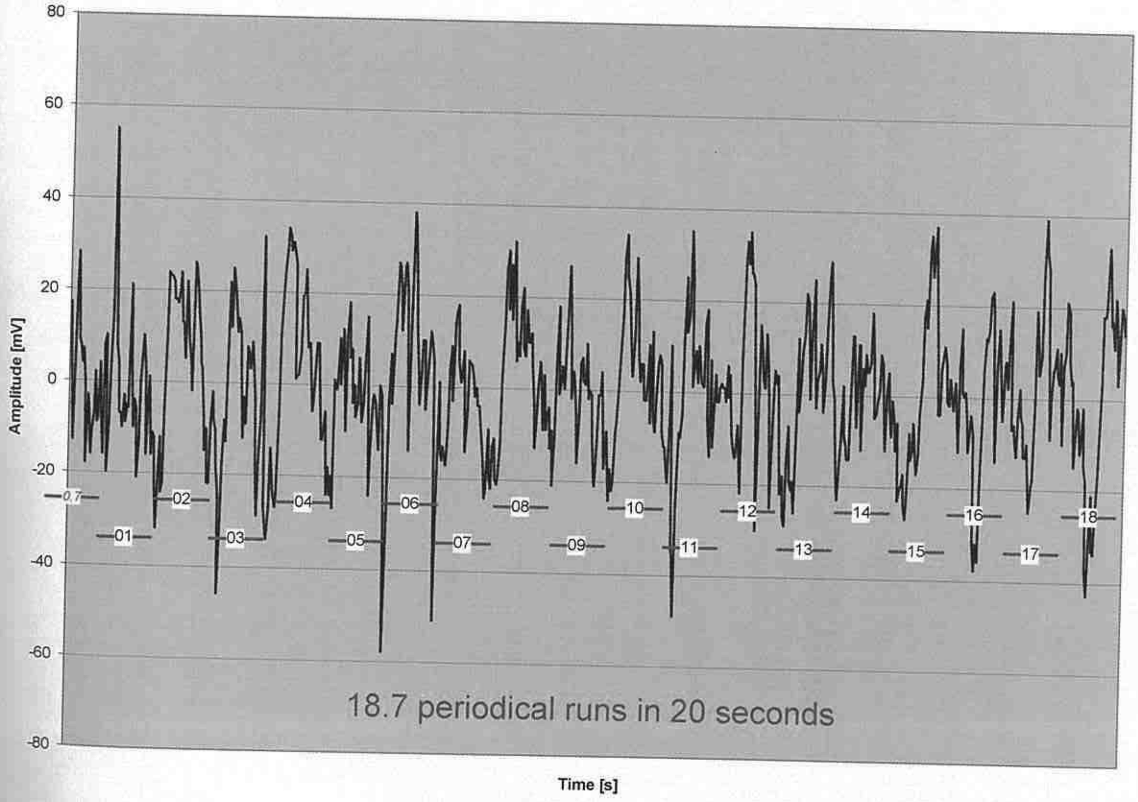


Fig. 4.65: Analysis of the normalized and adjusted curve from the application.

When summarizing the results of method for liveness detection based on the laser measurement principle, we can say that this method is very reliable, quick (several seconds are needed for the detection of a periodical run in the curve) and does not need very much performance from the processor, i.e. it is quite simple for computation. However, the disadvantage of this method lies in an expensive laser module and space requirements – it is not possible to integrate such solution in common, very small fingerprint scanners, with perhaps one exception of optical sensors, as their physical principle of functioning leads to bigger device constructions.

Other very interesting tests related to this topic have been presented in [85]; however, the description of those experiments exceeds the scope of this thesis.

5. Summary

This thesis is devoted to three important topics in the biometrical field of fingerprint recognition. Our fingerprints will be stored in our biometrical travel documents and will be used for our authentication of the data stored in the document on the chip. This idea is very popular and pushed forward at the moment, however, when planning the usage of such systems, we should think of some subparts of such biometrical system which could bring us some troubles.

The first topic (chapter 2) describes one subpart of the fingerprint recognition technology, where some problems could arise. First of all the skin structure is explained to the extent which is relevant to the subsequent chapters. Then it follows the description of the functionality of fingerprint acquirement technologies; some rare technologies are also represented. All fingerprint acquirement technologies could be influenced by various factors from the environment (e.g. surrounding light, electro-magnetic radiation, dirt on the surface, latent fingerprint, dry or moist fingers, etc.), what could lead to the distortion or defects of acquired images – this is discussed in the next subchapter. The main themes of the following subchapter are skin diseases and their influence on the fingerprint acquirement process. The summarization and division of such diseases into three subclasses is one of three main contributions of this thesis to the knowledge of biometrical systems based on fingerprint recognition. Skin diseases are divided into three subclasses – they could change the skin color, skin structure or both. At the end of this chapter, the impacts of skin diseases on the acquirement and recognition process are discussed.

The second topic (chapter 3) is devoted to the assessment of fingerprint image quality. The influencing factors and skin diseases described in the previous chapter can have an impact on the quality of a fingerprint image. This is partly influenced by the user and partly by the surrounding environment. First of all, the biometrical system should evaluate the quality of an image before further processing of the image in the system. For such quality evaluation, we need some well defined metrics. However, it is not simple to define suitable quality metrics for all fingerprint scanner technologies. The reason is that each fingerprint acquirement technology is based on different physical principles and therefore the output images are different. Nevertheless, some of the metrics are applicable to all fingerprint acquirement technologies. These are described in this chapter. In the beginning, some basics in biometric systems, which are relevant for the following explanation of the image quality estimation, are introduced. In particular, the following metrics can be counted among the suitable parameters for quality estimation: image contrast, mean value of grayscale levels, number of papillary lines (this could be used for the computation of the center (not core) of the fingerprint), sinusoidal shape of a papillary line crosscut, biometric sample quality scoring and minutiae quality scoring. If we have had estimated the quality of an image including a fingerprint, we have to decide whether such image can be enhanced or not. If yes, we can select from several practical methods for fingerprint image enhancement, e.g. Gabor filters, spatial domain filtering or frequency domain filtering. At the end of this chapter, some experimental results achieved in our laboratory are presented – four fingerprint acquirement technologies connected with the platform made by Suprema have been used and the quality of the acquired fingerprint images has been tested. The summarization of methods for estimation of fingerprint image quality, the description of one new method for this purpose (subchapter 3.1.5) and implementation of suitable tests represents the second of three main contributions of this thesis to the knowledge of biometrical systems based on fingerprint recognition.

The last topic (chapter 4) is oriented towards the liveness detection in fingerprint recognition systems. At the beginning, certain basic threats, which can be used in an attack on the biometric system, are described in general. One of them is the use of fake finger(print)s. Of course, the security of the biometric system is discussed here too, however, this is rather out of scope of this thesis. This is followed by a detailed introduction to the liveness detection and to all known methods and related principles; these include perspiration, spectroscopic characteristics, ultrasonic principle and many physical characteristics. At the end, several experiments on the liveness detection realized in our laboratory are presented, including the production of fake fingers, deceiving of thermal, capacitive and optical fingerprint scanners, skin temperature and resistance measurements and pulse measurements, using two patented methods [Dra08]. The summarization of methods for liveness detection, the introduction and patenting of two own methods for liveness detection (subchapter 4.2.9) and realization of the tests (subchapter 4.4) represents the third of three main contributions of this thesis to the knowledge of biometrical systems based on fingerprint recognition.

At the end, it could be said that these are my three main contributions to the knowledge of biometrical systems based on fingerprint recognition (all of them accompanied by many presentations at relevant conferences or workshops and publications in specialized journals): 1) summarization of influencing factors to fingerprint recognition and summarization and categorization of skin diseases and their impact to fingerprint recognition; 2) summarization of methods for quality estimation, proposal of one new method for fingerprint image quality estimation and realization of tests in this field; 3) summarization of methods for liveness detection, design of two new (patented) methods for this purpose and realization of related experiments.

6. Glossary

AC	Alternating Current
AFIS	Automated Fingerprint Recognition System
AGC	Automatic Gain Control
BFM	Basic Fingerprint Matcher
BPM	Best-Pair-Come-First Fingerprint Matcher
BPN	Back-Propagation Network
BQAM	Biometric Quality Assessment Method
CCD	Charge Coupled Device
CDF	Cumulative Distribution Function
CMOS	Complementary Metal-Oxide Semiconductor
DC	Direct Current
DCT	Discrete Cosine Transform
DET	Detection Error Trade-off
DFT	Discrete Fourier Transform
DNA	Desoxy-Ribonucleic-Acid
DPI	Dots Per Inch
DTP	Desk Top Publishing
ECG	Electrocardiogram
EER	Equal Error Rate
ESD	Electrostatic Discharge
FAR	False Accept Rate
FBI	Federal Bureau of Investigation
FFT	Fast Fourier Transform
FMR	False Match Rate
FNMR	False Non-Match Rate
FRR	False Rejection Rate
FTA	Failure to Acquire
FTE	Failure to Enroll
FTIR	Frustrated Total Internal Reflection
FTM	Failure to Match
HFMD	Hand-Foot-and-Mouth Disease
HHT	Hereditary Hemorrhagic Telangiectasia
ID	Identification

JPEG	Joint Photographic Expert Group
LED	Light Emitting Diode
LPR	Latent Print Reactivation
LRP	Local Ridge Pattern
MEMS	Micro-Electro-Mechanical Systems
MQA	Minutiae Quality Averaging
MSI	Multispectral Imager
NIST	National Institute of Standards and Technology
OCL	Orientation Certainty Level
PDA	Portable Digital Assistant
PDF	Probability Distribution Function
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PRP	Pityriasis Rubra Pilaris
RDC	Relative Dielectric Constant
RF	Radio Frequency
ROC	Receiver Operating Curve
RP	Raynaud's Phenomenon
RVS	Ridge-Valley Structure
SCLE	Subacute Cutaneous Lupus Erythematosus
SFBM	Score Filtering Before Fingerprint Matching
TPS	Thin-Plate Spline
VGA	Video Graphics Array
VISIT	Visitor and Immigrant Status Indicator Technology
WSQ	Wavelet Scalar Quantization

7. References

7.1 References Related to My Work

[Dra01] Bonfig K. W., Drahanský M.: *Biometrie*, Kreuztal, DE, bQuadrat, 2004, p. 153, ISBN 3-933609-02-X.

[Dra02] Chaloupka, R.: *Generátor otisků prstů (Generator of Fingerprints)*, Diploma Thesis (tutor: Martin Drahanský), FIT BUT, CZ, 2007, p. 51.

[Dra03] Dragula, P.: *Erkennung der feinen Hautbewegungen des Fingers*, Diploma Thesis (tutor: Martin Drahanský), FIT BUT, CZ, 2007, p. 60.

[Dra04] Drahanský M., Lodrová D.: *Liveness Detection for Biometric Systems Based on Papillary Lines*, In: Proceedings of Information Security and Assurance, 2008, Busan, KR, IEEE CS, 2008, pp. 439-444, ISBN 978-0-7695-3126-7.

[Dra05] Drahanský M., Lodrová D.: *Optical Principle for Liveness Detection*, Summer School on Biometrics, Presentation, Alghero, IT, 2008, p. 10.

[Dra06] Drahanský M.: *Experiments with Skin Resistance and Temperature for Liveness Detection*, In: Proceedings of the Fourth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Los Alamitos, US, IEEE CS, 2008, pp. 1075-1079, ISBN 978-0-7695-3278-3.

[Dra07] Drahanský M.: *Biometric Systems – Testing of Image Quality in Fingerprints and Liveness Detection*, Lesson at the Masaryk Univ. Brno, CZ, 2008, p. 34.

[Dra08] Drahanský M., Funk W., Nötzel R.: *Method and Apparatus for Detecting Biometric Features*, International PCT Patent, Pub. No. WO/2007/036370, Pub. Date 05.04.2007, Int. Application No. PCT/EP2006/009533, Int. Filing Date 28.09.2006, http://www.wipo.int/pctdb/en/wo.jsp?wo=2007036370&IA=WO2007036370&DISPLAY=STATUS.

[Dra09] Drahanský, M., Nezhyba, O.: *Testy obrazové kvality snímačů otisků prstů Suprema (Tests of Image Quality of Fingerprint Scanners from Suprema)*, In: Crypto-world, Vol. 9, No. 11, 2007, Prague, CZ, pp. 6-11, ISSN 1801-2140.

[Dra10] Drahanský, M.: *Sinusoidal Shape of a Papillary Line*, In: 2007 ECSIC Symposium on Bio-Inspired Learning, And Intelligent Systems for Security, Los Alamitos, US, IEEE CS, 2007, pp. 19-21, ISBN 0769529194.

[Dra11] Drahanský M., Orság F.: *Testování kvality snímků otisků prstů* (*Testing of Quality in Fingerprint Images*), In: Datakon 2007, Brno, CZ, MUNI, 2007, pp. 161-168, ISBN 978-80-7355-076-9.

[Dra12] Drahanský M.: *Identita v nás ukrytá (detailní rozbor biometrických systémů)* (*Identity Hidden in us (Detailed Analysis of Biometric Systems)*), In: CONNECT!, Vol. 2007, No. 4, Brno, CZ, pp. 24-25, ISSN 1211-3085.

[Dra13] Drahanský M.: *Methods for Quality Determination of Papillary Lines in Fingerprints*, NIST, Gaithersburg, USA, 2007, p. 25.

[Dra14] Drahanský M.: *Přehled biometrických systémů a testování jejich spolehlivosti (An Overview of Biometric Systems and of Testing their Reliability)*, Presentation, Networks Security Congress, Prague, CZ, 2007, p. 37.

[Dra15] Drahanský M.: *Testen der Qualität von Fingerabdruckbildern*, TeleTrusT, Berlin, GE, 2007, p. 28.

[Dra16] Drahanský, M., Orság, F., Malinka, K.: *Závěrečná zpráva – Testování senzorů firmy Suprema (Final Report – Testing of Scanners from Suprema)*, Version 1.4, Brno, CZ, 2006, p. 21.

[Dra17] Drahanský M., Funk W., Nötzel R.: *Liveness Detection based on Fine Movements of the Fingertip Surface*, In: IEEE – The West Point Workshop, West Point, New York, USA, 2006, pp. 42-47, ISBN 1-4244-0130-5.

[Dra18] Drahanský M., Orság F.: *Biometrische kryptographische Schlüssel*, In: DuD – Datenschutz und Datensicherheit, Vol. 2006, No. 8, Wiesbaden, DE, pp. 501-505, ISSN 1614-0702.

[Dra19] Drahanský M., Orság F.: *Směrnice a standardy v biometrii (Directions and Standards in Biometrics)*, In: DSM Data Security Management, Vol. 2006, No. 4, CZ, pp. 26-29, ISSN 1211-8737.

[Dra20] Drahanský, M.: *Biometric Systems*, Course at the Faculty of Information Technology, BUT, http://www.fit.vutbr.cz/study/courses/BIO/.

[Dra21] Drahanský, M.: *Biometric Security Systems – Fingerprint Recognition Technology*, Dissertation Thesis, FIT BUT, CZ, p. 140, 2005, (ISBN 80-214-2969-0).

[Dra22] Drahanský M., Orság F.: *Může biometrie sloužit ke kryptografii? (Can be Biometrics Used for Cryptography?)*, In: Crypto-world, Vol. 7, No. 11, 2005, Prague, CZ, pp. 13-18, ISSN 1801-214.

[Dra23] Drahanský M.: *Biometrische Sicherheitssysteme – Fingerabdrucktechnologie*, Presentation, In: MTK'05, Remagen, DE, 2005, p. 25.

[Dra24] Drahanský M.: *Concept of Biometric Security System*, In: Proceedings of the 11th Conference and Competition STUDENT EEICT 2005, Brno, CZ, FEEC BUT, 2005, pp. 200-204, ISBN 80-214-2890-2.

[Dra25] Drahanský, M., Nötzel, R., Bonfig, K.W.: *Sensoren zur Fingerabdruckerkennung*, SSS2004, Bundle 5, Kreuztal, bQuadrat, GE, pp. 49-60, 2004, ISBN 3-933609-19-4.

[Dra26] Drahanský M., Smolík L.: *Entropic Numbers from the Fingerprint*, The Royal Statistical Society, London, GB, 2004, p. 20.

[Dra27] Drahanský M., Orság F., Zbořil F.V.: *Biometrics in Security Applications*, In: Proceedings of 38th International Conference MOSIS'04, Ostrava, CZ, MARQ, 2004, pp. 201-206, ISBN 80-85988-98-4.

[Dra28] Drahanský M., Orság F.: *Biometric Security Systems: Robustness of the Fingerprint and Speech Technologies*, In: BT 2004 – International Workshop on Biometric Technologies, Calgary, CA, 2004, pp. 99-103.

[Dra29] Drahanský M., Smolík L.: *Biometrické certifikáty* (*Biometric Certificates*), In: DSM Data Security Management, Vol. 8, No. 5, 2004, CZ, pp. 20-22, ISSN 1211-8737.

[Dra30] Drahanský M.: *Fingerabdruckerkennung mittels neuronaler Netze*, Diploma Thesis, FEEC BUT, 2001, p. 120.

[Dra31] *Evaluation of Fingerprint Recognition Technologies - BioFinger*, Public Final Report, version 1.1, Bundesamt für Sicherheit in der Informationstechnik, p. 122, (co-worker on this project: Martin Drahanský), 2004.

[Dra32] Lichvár M.: *Detekce živosti prstu na základě změn papilárních linií* (*Liveness Detection of a Finger Based on Changes of Papillary Lines*), Diploma Thesis (tutor: Martin Drahanský), FIT BUT, 2008, p. 67.

[Dra33] Lodrová D., Drahanský M.: *Methods of Liveness Testing By Fingers*, In: Analysis of Biomedical Signals and Images, Brno, CZ, VUTIUM, 2008, p. 7, ISBN 978-80-214-3612-1, ISSN 1211-412X.

[Dra34] Tuč, D.: *Testing of the Environmental Influences on Fingerprint Sensors*, BSc. Project (tutor: Martin Drahanský), FIT BUT, 2005, p. 63.

7.2 Other References

[1] Adler, A., Dembinsky, T.: *Human vs. Automatic Measurement of Biometric Sample Quality*, School of Information Technology, University of Ottawa, Canada, p. 4, 2006.

[2] Adler, A., Youmaran, R.: *Measuring Biometric Sample Quality by Biometric Information*, NIST Biometric Workshop II, Gaithersburg, USA, p. 10, 2007.

[3] Ambalakat, P.: *Security of Biometric Authentication Systems*, In: 21st Computer Science Seminar, SA1-T1-1, 2005, p. 7.

[4] Bauer, N.: *Handbuch zur Industriellen Bildverarbeitung*, Fraunhofer IRB Verlag, Stuttgart, GE, 2007, p. 513, ISBN 978-3-8167-7386-3.

[5] Benáková, N. (Ed.) a kol.: *Dermatovenerologie, dětstká dermatologie a korektivní dermatologie* (*Dermatovenerology, Pediatric Dermatology and Corrective Dermatology*), Triton, Prague, CZ, 2006, p. 294, ISBN 80-7254-855-7.

[6] Bhanu, B., Tan, X.: *Computational Algorithms for Fingerprint Recognition*, Kluwer Academic Publishers, USA, 2004, p. 188, ISBN 1-4020-7651-7.

[7] Bicz, W.: *The Impossibility of Faking Optel's Ultrasonic Fingerprint Scanners*, Optel, Poland, http://www.optel.pl/article/english/livetest.htm, 2008.

[8] *Biometric Technology Security Evaluation under the Common Criteria*, Version 1.2, Communications Security Establishment, Canadian Common Criteria Evaluation and Certification Scheme, Government of Canada, p. 52, 2001.

[9] Bolle, R.M., Connell, J.H., Pankanti, S., Ratha, N.K., Senior, A.W.: *Guide to Biometrics*, Springer-Verlag, 2004, p. 364, ISBN 0-387-40089-3.

[10] Charlot, B., Parrain, F., Galy, N., Basrour, S., Courtois, B.: *A Sweeping Mode Integrated Fingerprint Sensor With 256 Tactile Microbeams*, In: Journal of Mi-

croelectromechanical Systems, Vol. 13, No. 4, 2004, pp. 636-644, ISSN 1057-7157.

[11] Chen, J., Chan, F., Moon, Y.S.: *Fingerprint Matching with Minutiae Quality Score*, In: Proceedings of ICB 2007, LNCS 4642, Springer-Verlag Berlin Heidelberg, Seoul, Korea, 2007, pp. 663-672, ISBN 978-3-540-74548-8.

[12] Chen, Y., Dass, S., Jain, A.K.: *Fingerprint Quality Indices for Predicting Authentication Performance*, In: Proceedings of AVBPA2005, USA, p. 10, ISBN 3-540-27887-7, 2005.

[13] Chirillo, J., Blaul, S.: *Implementing Biometric Security*, Wiley Publishing, USA, 2003, p. 399, ISBN 0-7645-2502-6.

[14] Collins, C.G.: *Fingerprint Science*, Copperhouse/Atomic Dog Publishing, p. 192, 2001, ISBN 978-0-942-72818-7.

[15] Criminal Justice Information Services Division: *WSQ Gray-Scale Fingerprint Image Compression Specification*, FBI, IAFIS-IC-0110(V3), 1997, p. 56.

[16] Dannamiller, J.L., Stephens, B.R.: *Asymmetries in Contrast Polarity Processing in Young Human Infants*, In: Journal of Vision 2001, pp. 112-125, 2001, ISSN 1534-7362.

[17] *Das BIA-Kompendium* – Data Input GmbH, Body Composition, 3rd Edition, 2007, p. 70, www.data-input.de.

[18] Dass, S.C., Zhu, Y., Jain, A.K.: *Validating a Biometric Authentication System: Sample Size Requirements*, In: IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 28, No. 12, pp. 1902-1913, 2006.

[19] Daugman, J.: *Biometric Decision Landscapes*, University of Cambridge, p. 13, 2001.

[20] Dessimoz, D., Richiardi, J., Champod, C., Drygajlo, A.: *Multimodal Biometrics for Identity Documents*, Research Report, PFS 341-08.05, Version 2.0, Université de Lausanne & École Polytechnique Fédérale de Lausanne, 2006, p. 161.

[21] Galbally, J., Fierrez, J., Ortega-Garcia, J.: *Vulnerabilities in Biometric Systems: Attacks and Recent Advances in Liveness Detection*, Biometrics Recognition Group, Madrid, Spain, 2007, p. 8.

[22] Grimnes, S., Martinsen, Ø.G.: *Bioimpedance*, University of Oslo, Norway, Wiley Encyclopedia of Biomedical Engineering, John Wiley & Sons., Inc., 2006, p. 9.

[23] Habif, T.P.: *Clinical Dermatology*, 4th Edition, Mosby, China, 2004, p. 1004, ISBN 978-0-323-01319-2.

[24] Han, J.S., Kadowaki, T., Sato, K., Shikida, M.: *Thermal Analysis of Fingerprint Sensor Having a Microheater Array*, In: International Symposium on Micromechatronics and Human Science, IEEE, 1999, Japan, pp. 199-205, ISBN 0-7803-5790-6.

[25] Hao, F., Anderson, R., Daugman, J.: *Combining Cryptography with Biometric Effectivity*, Technical Report, University of Cambridge, 2005, p. 17, ISSN 1476-2986.

[26] Honzíková, N., Honzík, P.: *Biologie člověka* (*Human Biology*), The Faculty of Electrical Engineering and Communication, BUT, Brno, CZ, 2003, p. 136.

[27] Hoover, J.E.: *The Science of Fingerprints*, United States Department of Justice, FBI, e-Book 19022, 2006, p. 197, www.gutenberg.org.

[28] IBG: *Liveness Detection in Biometric Systems*, International Biometric Group, www.biometricgroup.com, 2008.

[29] Innes, B.: *DNA und der genetische Fingerabdruck*, Amber Books / Tosa Verlag, Germany, 2007, p. 96, ISBN 978-3-85003-202-5.

[30] ISO/IEC 19795-1, *Information Technology – Biometric Performance Testing and Reporting – Part 1: Principles and Framework*, 2006.

[31] ISO/IEC 19795-2, *Information Technology – Biometric Performance Testing and Reporting – Part 2: Testing Methodologies for Technology and Scenario Evaluation*, 2007.

[32] ISO/IEC 19795-3, *Information Technology – Biometric Performance Testing and Reporting – Part 3: Modality-specific Testing*, 2007.

[33] Jain, A.K., Flynn, P., Ross, A.A.: *Handbook of Biometrics*, Springer-Verlag, 2008, p. 556, ISBN 978-0-387-71040-2.

[34] Jain, A.K., Pankanti, S.: *A Touch of Money*, IEEE Spectrum, 2006, pp. 14-19, www.spectrum.ieee.org.

[35] Jain, A.K., Ross, A., Pankanti, S.: *Biometrics: A Tool for Information Security*, In: IEEE Transactions on Information Forensics and Security, Vol. 1, No. 2, 2006, pp. 125-143, ISSN 1556-6013.

[36] Jain, A.K.: *Biometric System Security*, Presentation, Michigan State University, p. 57, 2005.

[37] Jain, A.K.: *Fingerprint Enhancement*, Presentation, Michigan State University, p. 16, 2005.

[38] Jain, A.K., Uludag, U., Ross, A.: *Biometric Template Selection: A Case Study in Fingerprints*, In: Proceedings of AVBPA2003, LNCS 2688, USA, p. 8, ISBN 3-540-40302-7, 2003.

[39] Jain, A.K., Pankanti, S.: *Automated Fingerprint Identification and Imaging Systems*, In: Advances in Fingerprint Technology, CRC Press, 2001, pp. 275-326.

[40] James, W.D., Berger, T.G., Elston, D.M.: *Andrew's Diseases of the Skin – Clinical Dermatology*, 10th Edition, Saunders Elsevier, Canada, 2006, p. 961, ISBN 0-8089-2351-X.

[41] Jang, J., Elliott, S.J., Kim, H.: *On Improving Interoperability of Fingerprint Recognition Using Resolution Compensation Based on Sensor Evaluation*, In: S.-W. Lee and S.Z. Li (Eds.): ICB 2007, LNCS 4642, 2007, pp. 455-463, Springer-Verlag Berlin Heidelberg, 2007, ISSN 0302-9743.

[42] Jia, J., Cai, L., Zhang, K., Chen, D.: *A New Approach to Fake Finger Detection Based on Skin Elasticity Analysis*, In: S.-W. Lee and S.Z. Li (Eds.): ICB 2007, LNCS 4642, 2007, pp. 309-318, Springer-Verlag Berlin Heidelberg, 2007, ISSN 0302-9743.

[43] Jirachaweng, S., Areekul, V.: *Fingerprint Enhancement Based on Discrete Cosine Transform*, In: Proceedings of ICB 2007, LNCS 4642, Springer-Verlag Berlin Heidelberg, Seoul, Korea, 2007, pp. 96-105, ISBN 978-3-540-74548-8.

[44] Jung, D.W., Park, R.H.: *Robust Fingerprint Identification Based on Hybrid Pattern Recognition Methods*, In: World Scientific (www.worldscientific.com), 2001, p. 26.

[45] Katzenmeier, H.U.: *Formanalytische Untersuchungen über Zusammenhänge zwischen Mustertypen der Fingerbeeren und Form der Fingerendglieder*, Ph.D. Thesis, Justus-Liebig-Universität Gießen, DE, 2002, p. 77.

[46] Kim, D.H.: *Minutiae Quality Scoring and Filtering Using a Neighboring Ridge Structural Analysis on a Thinned Fingerprint Image*, In: Proceedings of AVBPA05, LNCS, Vol. 3546, p. 674. Springer-Verlag – Heidelberg, 2005.

[47] Kletke, I.: *Das digitale Bild des Fingerabdrucks*, VDM Verlag Dr. Müller, Berlin, Germany, 2007, p. 79, ISBN 978-3-8364-0911-7.

[48] Kluz, M.: *Liveness Testing in Biometric Systems*, Master Thesis, Faculty of Informatics, Masaryk University Brno, CZ, 2005, p. 57.

[49] Komarinski, P.: *Automated Fingerprint Identification Systems (AFIS)*, Academic Press, 1st Edition, 2004, p. 312, ISBN 978-01-241-8351-3.

[50] Konkoľová, R.: *Korektivně dermatologické metody* (*Corrective Dermatologic Methods*), Maxdorf – Jessenius, Prague, CZ, 2001, p. 114, ISBN 80-85912-54-6.

[51] Kung, S.Y., Mak, M.W., Lin, S.H.: *Biometric Authentication – A Machine Learning Approach*, Prentice Hall Professional Technical Reference, 2005, p. 461, ISBN 0-131-47824-9.

[52] Lee, H.C., Gaensslen, R.E.: *Advances in Fingerprint Technology*, CRC, 2nd Edition, 2001, p. 456, ISBN 978-08-493-0923-6.

[53] Lee, S.W., Li, S.Z.: *Advances in Biometrics*, In: Proceedings of the International Conference ICB 2007, Seoul, Korea, 2007, p. 868, ISBN 3-540-74548-3.

[54] Lepley, M.A.: *JPEG 2000 and WSQ Image Compression Interoperability*, MITRE Technical Report, Center for Integrated Intelligence Systems, Bedford, USA, 2001, p. 52.

[55] Ling, Q., Bardzimashvili, T.: *Biometrics in Computerized Patient Record*, Presentation, 2005, p. 33.

[56] Liu, H., Wu, T.: *Estimating the Area under a Receiver Operating Characteristic Curve for Repeated Measures Design*, Department of Medicine, School of Medicine & Department of Biostatistics, School of Public Health, UCLA, p. 18, 2003.

[57] LN: *Němečtí hackeři šíří otisk prstu ministra* (*German Hackers Distribute the Minister's Fingerprint*), Lidové noviny, March 31, 2008.

[58] Lorch, H., Morguet, P., Schröder, H.: *Fingerprint Distortion Measurement*, In: BioAW 2004, LNCS 3087, 2004, Springer-Verlag, pp. 111-123.

[59] Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S.: *Handbook of Fingerprint Recognition*, Springer-Verlag, 1st Edition, 2005, p. 348, ISBN 978-03-879-5431-8.

[60] Maltoni, D., Jain, A.K.: *Biometric Authentication*, In: ECCV 2004 International Workshop, BioAW 2004, Prague, CZ, p. 340, ISBN 3-540-22499-8.

[61] Mansfield, A.J., Wayman, J.L.: *Best Practices in Testing and Reporting Performance of Biometric Devices*, NPL Report CMSC 14/02, Centre for Mathematics and Scientific Computing, National Physical Laboratory, p. 36, 2002.

[62] Mansfield, T., Kelly, G., Chandler, D., Kane, J.: *Biometric Product Testing – Final Report*, Issue 1.0, Centre for Mathematics and Scientific Computing, National Physical Laboratory, p. 22, 2001.

[63] Martinsen, Ø.G., Grimnes, S., Haug, E.: *Measuring Depth Depends on Frequency in Electrical Skin Impedance Measurements*, In: Skin Research and Technology No. 5, 1999, pp. 179-181, ISSN 0909-752X.

[64] Matsumoto, T., Matsumoto, H., Yamada, K., Hoshino, S.: *Impact of Artificial "Gummy" Fingers on Fingerprint Systems*, In: Proceedings of SPIE Vol. 4677, Optical Security and Counterfeit Deterrence Techniques IV, 2005, p. 11.

[65] Moll, I.: *Dermatologie*, 6th Edition, Thieme – Dual Reihe, Germany, 2005, p. 592, ISBN 3-13-126686-4.

[66] Murray, L., Park, U.: *Biometrics in Credit Cards: A New Way to Pay*, Presentation, CSE891, 2005, p. 31.

[67] Müller, R.: *Fingerprint Verification with Microprocessor Security Tokens*, Ph.D. Thesis, Technical University Munich, GE, 2001, p. 151.

[68] Nerbonne, J.M.: *Keynote Lecture: Molecular Mechanisms Underlying Heterogeneities in Repolarization*, Japanese Circulation Society, 2008, http://www.j-circ.or.jp/english/sessions/reports/64th-ss/nerbonne-l1.htm.

[69] Nolde, V., Leger, L.: *Biometrische Verfahren*, Fachverlag Deutscher Wirtschaftsdienst, Germany, 2002, p. 477, ISBN 3-87156-464-8.

[70] O'Gorman, L.: *Fingerprint Verification*, In: Jain, A.K., Bolle, A.K., Pankanti, S.: Biometrics: Personal Identification in Networked Society, 1998, p. 23.

[71] Petermann, T., Scherz, C., Sauter, A.: *Biometrie und Ausweisdokumente*, TAB – Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, Arbeitsbericht No. 93, 2003, p. 168.

[72] Project *SFinGe – Synthetic Fingerprint Generator*, biolab.csr.unibo.it, 2008.

[73] *Protection Profile for Biometric Verification Mechanisms*, Version 1.04, Federal Ministry of the Interior, Germany, BSI-PP-0016-2005, 2005, p. 19.

[74] Protivinský, M., Klvaňa, K.: *Základy kriminalistiky (Basics of Criminal Science)*, 2nd Edition, TRIVIS, Armex Publishing, 2007, p. 156, ISBN 978-80-86795-50-8.

[75] Provazník, I., Kozumplík, J.: *Úvod do biomedicínské informatiky* (*Introduction to Biomedical Informatics*), Scriptum, Faculty of Electrical Engineering and Communication, BUT, 2002, p. 36.

[76] Putte, T., Keuning, J.: *Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned*, In: IFIP TC8/WG8.8 4th Working Conference on Smart Card Research and Advanced Applications, Kluwer Academic Publishers, 2000, pp. 289-303.

[77] Rak, R., Matyáš, V., Říha, Z. et. al.: *Biometrie a identita člověka ve forenzních a komerčních aplikacích (Biometrics and Human Identity in Forensic and Commercial Applications)*, Grada Publishing, Prague, CZ, 2008, p. 631, ISBN 978-80-247-2365-5.

[78] Ratha, N., Bolle, R.: *Automatic Fingerprint Recognition Systems*, Springer-Verlag, USA, 2004, p. 458, ISBN 0-387-95593-3.

[79] Roberts, C.: *Biometric Attack – Vectors and Defences*, 2006, p. 25.

[80] Ross, A., Jain. A.K.: *Biometric Sensor Interoperability: A Case Study in Fingerprints*, In: Proceedings of International ECCV Workshop on Biometric Authentication, LNCS 3087, Springer-Verlag, 2004, pp. 134-145.

[81] Ross, A.: *Information Fusion in Fingerprint Authentication*, Ph.D. Thesis, Michigan State University, USA, 2003, p. 187.

[82] Rowe, R.K.: *Spoof Detection*, In: Summer School for Advanced Studies on Biometrics for Secure Authentication, Alghero, Italy, 2008, p. 43.

[83] Rowe, R.K.: *A Multispectral Sensor for Fingerprint Spoof Detection*, www.sensormag.com, January 2005.

[84] Říha, Z., Matyáš, V.: *Biometric Authentication Systems*, Faculty of Informatics, Masaryk University Brno, FIMU-RS-2000-08, 2000, p. 46.

[85] Sandström, M.: *Liveness Detection in Fingerprint Recognition Systems*, Institute for System Technology, Linköpings University, Sweden, ISRN LITH-ISY-EX-3557-2004, Diploma Thesis, 2004, p. 149.

[86] Sató, N., Shigematsu, S., Morimura, H., Yano, M., Kudou, K., Kamei, T., Machida, K.: *Novel Surface Structure and Its Fabrication Process for MEMS Fingerprint Sensor*, In: IEEE Transactions on Electron Devices, 2005, p. 7, ISSN 0018-9383.

[87] Schuckers, S., Abhyankar, A.: *Detecting Liveness in Fingerprint Scanners Using Wavelets: Results of the Test Dataset*, In: BioAW 2004, LNCS 3087, 2004, Springer-Verlag, pp. 100-110.

[88] Schuckers, S., Hornak, L., Norman, T., Derakhshani, R., Parthasaradhi, S.: *Issues for Liveness Detection in Biometrics*, CITeR, West Virginia University, Presentation, 2003, p. 25.

[89] Straus, J.: *Kriminalistická daktyloskopie (Criminalistic Dactyloscopy)*, Kriminalistický ústav Praha Policie ČR, Prague, CZ, 2005, p. 285, ISBN 80-7251-192-0.

[90] Stücker, M., Geil, M., Kyeck, S., Hoffman, K., Röchling, A., Memmel, U., Altmeyer, P.: *Interpapillary Lines – the Variable Part of the Human Fingerprint*, Journal of Forensic Sciences, ASTM International, 2001, p. 5, ISSN 0022-1198.

[91] Tabassi, E., Grother, P.: *Quality Summarization*, NISTIR 7422, National Institute of Standards and Technology, p. 7, 2007.

[92] Tabassi, E., Wilson, C.L., Watson, C.I.: *Fingerprint Image Quality*, NISTIR 7151, National Institute of Standards and Technology, p. 72, 2004.

[93] Tan, B., Lewicke, A., Schuckers, S.: *Novel Methods for Fingerprint Image Analysis Detect Fake Fingers*, SPIE, 10.1117, 2.1200805.1171, p. 3, 2008.

[94] Toth, B.: *Biometric Liveness Detection*, In: Information Security Bulletin, Vol. 10, 2005, pp. 291-297, www.chi-publishing.com.

[95] UltraScan: *The Theory of Live-Scan Fingerprint Imaging (Breaking the Optical Barriers with Ultrasound)*, UltraScan, USA, 2004, p. 8.

[96] Uludag, U.: *Secure Biometric Systems*, Dissertation Thesis, Michigan State University, 2006, p. 171.

[97] *U.S. Government Biometric Verification Mode Protection Profile for Basic Robustness Environments*, Version 1.1, IAD – Information Assurance Directorate, 2007, p. 84.

[98] *U.S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments*, Version 1.1, IAD – Information Assurance Directorate, 2007, p. 140.

[99] *U.S. Patent 6,314,195 – Organism Identifying Method and Device*, November 2001.

[100] *U.S. Patent 6,292,576 – Method and Apparatus for Distinguishing a Human Finger From a Reproduction of a Finger*, September 2001.

[101] *U.S. Patent 5,088,817 – Biological Object Detection Apparatus*, February 1992.

[102] Vlašín, Z., Jedličková, H.: *Praktická dermatologie v obrazech a schématech* (*Practical Dermatology in Illustrations and Schematics*), Vladerma, Brno, CZ, 2001, p. 251, ISBN 80-238-6966-3.

[103] Wasserman, P.D.: *Solid-State Fingerprint Scanners*, Presentation, NIST, 2005, p. 38.

[104] Wayman, J.L.: *National Biometric Test Center – Collected Works 1997-2000*, Version 1.3, San José State University, p. 289, 2000.

[105] Web page LEA Medizintechnik GmbH: http://www.lea.de/deu/txabtisspecd.htm.

[106] Web page: http://www.merck.com/mmhe/sec03/ch025/ch025a.html.

[107] Web page – London Ambulance Service:
http://www.lond.ambulance.freeuk.com/ecg/ECG.htm.

[108] Web page: http://www.karlloren.com/Diabetes/images/finger_high.jpg.

[109] Web page: http://pagesperso-orange.fr/fingerchip.

[110] Web page: http://www.naturalrussia.com/natural/skin/structure.html.

[111] Web page: http://home.att.net/~dermatoglyphics/MalcolmX.jpg.

[112] Web page: http://www.rodina.cz/scripts/detail.asp?id=1966.

[113] Web page: http://www.bromba.com/technole.htm.

[114] Web page – Fingerprint Verification Competition 200*2*, 200*4*, 200*6* (200*x*)
http://bias.csr.unibo.it/fvc200*x*.

[115] Web page: http://biolab.csr.unibo.it/.

[116] Web page: http://www.healthandage.com.

[117] Web page: http://www.ccc.de/biometrie/fingerabdruck_kopieren?.

[118] Web page: http://www.keyence.com/products/vision/laser/lkg.

[119] Web page: http://en.wikipedia.org/wiki/Fingerprint.

[120] Wein, L.W., Baveja, M.: *Using Fingerprint Image Quality to Improve the Identification Performance of the U.S. Visitor and Immigrant Status Indicator Technology Program*, In: Proceedings of the National Academy of Sciences of the United States of America, Vol. 21, No. 21, pp. 7772-7775, ISSN 1091-6490, 2005.

[121] Weston, W.L., Lane, A.T., Morelli, J.G.: *Color Textbook of Pediatric Dermatology*, Mosby Elsevier, China, 2007, p. 446, ISBN 978-03-23049-09-2.

[122] Wolf, M., Viehmann, M.: *Biometrische Sensorik zur Personenidentifikation und Lebenderkennung am Beispiel Fingerabdrucksensoren*, Institut für Maschinen, Antriebe und elektronische Gerätetechnik GmbH Nordhausen (IMG), GE, 2002, p. 10.

[123] Wolff, K., Johnson, R.A., Suurmond, D.: *Color Atlas and Synopsis of Clinical Dermatology*, 5th Edition, McGraw-Hill, USA, 2005, p. 1085, ISBN 0-07-144019-4.

[124] Yao, M.Y.-S., Pankanti, S., Haas, N., Ratha, N., Bolle, R.M.: *Quantifying Quality: A Case Study in Fingerprints*, IBM T.J. Watson Research Center, New York, USA, p. 6, 2002.

[125] Yau, W.Y., Chen, T.P., Morguet, P.: *Benchmarking of Fingerprint Sensors*, In: BioAW 2004, LNCS 3087, Springer-Verlag, 2004, pp. 89-99.

[126] Zhang, Y., Tian, J., Chen, X., Yang, X., Shi, P.: *Fake Finger Detection Based on Thin-Plate Spline Distortion Model*, In: S.-W. Lee and S.Z. Li (Eds.): ICB 2007, LNCS 4642, 2007, Springer-Verlag Berlin Heidelberg, 2007, pp. 742-749, ISSN 0302-9743.