Brno University of Technology
Faculty of Information Technology
Department of Intelligent Systems

Ing. Martin Drahanský

BIOMETRIC SECURITY SYSTEMS
FINGERPRINT RECOGNITION TECHNOLOGY

BIOMETRICKÉ BEZPEČNOSTNÍ SYSTÉMY
TECHNOLOGIE ROZPOZNÁVÁNÍ OTISKŮ PRSTŮ

Short version of Ph.D. Thesis

Study field:	Information Technology
Supervisor:	Doc. Ing. František Zbořil, CSc.
Opponents:	Prof. Ing. Václav Matoušek, CSc.
	Doc. Ing. Václav Jirsík, CSc.
Presentation date:	03.06.2005

Keywords: biometrics, cryptography, verification, authentication, identification, fingerprint, enrollment, matching, classification, orientation field, ridge count, biometric template, biometric key, certificate, entropy, error rate, PIN, password

Klíčová slova: biometrie, kryptografie, verifikace, autentikace, identifikace, otisk prstu, registrace, porovnání, klasifikace, pole orientací, počet papilárních linií, biometrická šablona, biometrický klíč, certifikát, entropie, chybovost, PIN, heslo

The original of the dissertation is available in the library of the Faculty of Information Technology at the Brno University of Technology, Czech Republic.

ISBN 80-214-2969-0
ISSN 1213-4198

CONTENTS

1 INTRODUCTION

Biometric technologies, as we know them today, have been made possible by explosive advances in computing power and have been made necessary by the near universal interconnection of computers around the world. The increased perception of information as near equivalents of money, in conjunction with the opportunities for access provided by the Internet, is a paradigm shift with significant repercussions on authentication. If data is money, then server-based or local hard drives are our new vaults, and information-rich companies will be held responsible for their security. A number of biometric attributes are in use in various applications (Fig. 1.1 [5]).

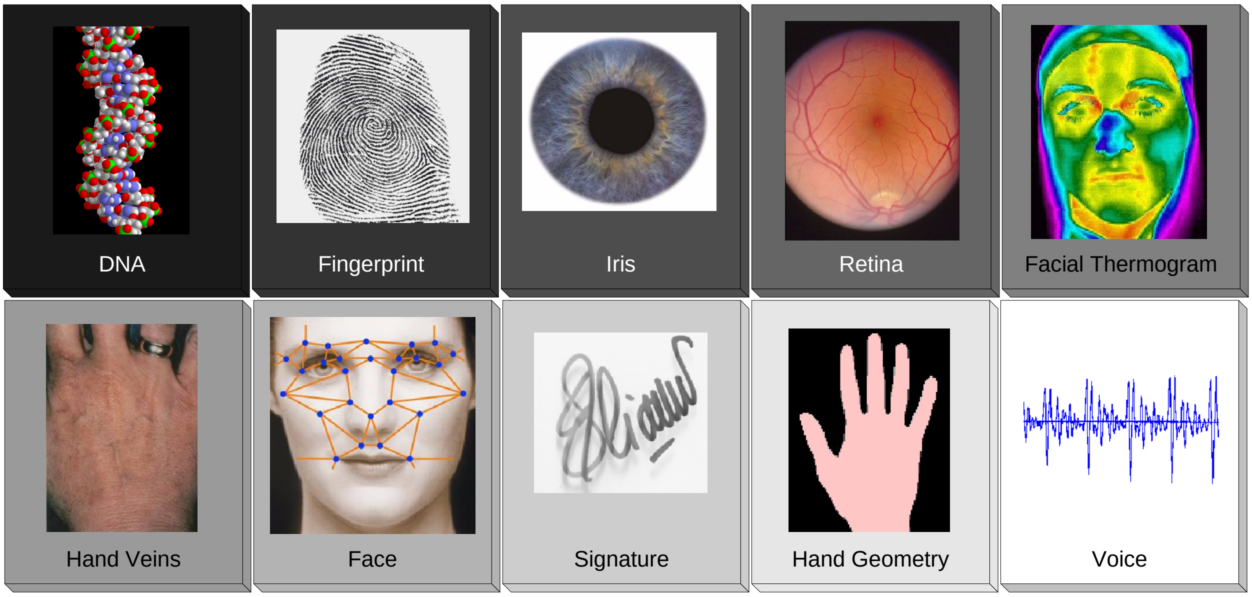

Fig. 1.1: Different biometric attributes (ordered in accordance with their uniqueness)

1.1 Benefits of Biometrics

Three following fundamental techniques are used in authentication mechanisms:

- Something you *know*, which usually refers to passwords and PINs.
- Something you *have*, which usually refers to smart cards or tokens.
- Something you *are*, which refers to biometrics – the measurement of physical characteristics or personal traits.

The most frequently used authentication methods are passwords and PINs. They secure access to personal computers, networks, and applications. Handheld tokens (such as cards and key fobs) have replaced passwords in some higher-security applications. However, passwords, PINs, and tokens or cards have a number of problems that call into question their suitability for modern applications (access to online financial accounts or medical data).

1.2 Key Biometric Terms

Biometrics is the automated use of physiological or behavioral characteristics to determine or verify identity.

Biometric System is essentially a pattern recognition system that recognizes a person by determining the authenticity of a specific physiological or behavioral characteristic possessed by the person. Depending on the application context, a biometric system may be called either a verification or identification system.

Identity is often misunderstood in the context of biometrics, where a distinction must be drawn between an individual and an identity. An individual is a singular, unique entity – colloquially, a person – but an individual can have more than one identity.

Authentication is also frequently used in the biometric field, sometimes as a synonym for verification; actually, in the information technology language, authenticating a user means to let the system know the user's identity regardless of the mode.

Verification systems answer the question, "Am I who I claim to be?" by requiring that a user claim an identity in order for a biometric comparison to be performed. After a user claims an identity, he or she provides biometric data which is then compared against his or her enrolled biometric data. Verification is often referred to as 1:1 (one-to-one). The process of providing a username and biometric data is referred to as authentication.

Identification systems answer the question, "Who am I?" and do not require that a user claim an identity before biometric comparisons take place. The user provides his or her biometric data, which is compared to data from a number of users in order to find a match. The answer returned by the system is an identity. Identification is often referred to as 1:N (one-to-N or one-to-many), because a person's biometric information is compared against multiple (N) records.

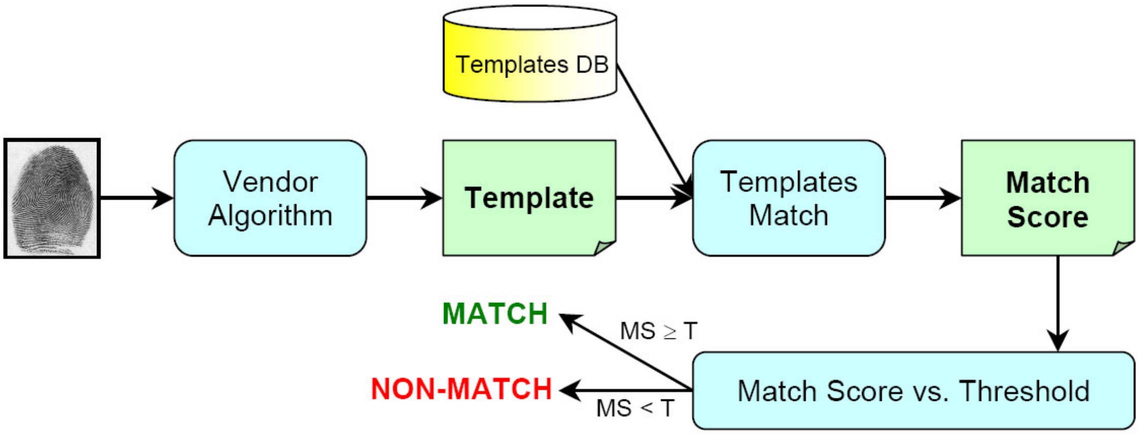

Fig. 1.2: Biometric Matching – Process Flow

Sensor. The sensor is an input device which transfers the real biometric information of the user into the electrical information and then into the digital information. The technologies for fingerprint scanners are briefly described in the Ch. 2.1.1 and [4].

Biometric data. The biometric data users provide, represents an unprocessed image or recording of a characteristic.

Feature extraction. The automated process of locating and encoding distinctive characteristics from biometric data in order to generate a template.

Templates. A template is a small file derived from the distinctive features of a user's biometric data, used to perform biometric matches. Biometric systems store and compare biometric templates, not biometric data.
Biometric Matching. The comparison of biometric templates to determine their degree of similarity or correlation. The matching process results in a match score, which, in most systems, is compared against a threshold. If the match score exceeds the threshold, the result is a match; otherwise, the result is a non-match.

1.3 Error Classification and Performance Evaluation

To assess the performance of a biometric system, it can be analyzed in the framework of testing hypothesis [15]. Let the stored biometric sample or template be pattern $P' = S(B')$ and the acquired one be pattern $P = S(B)$. Then, in terms of testing hypothesis, we have null and alternative hypotheses:

$$H_0 : B = B', \quad \text{the claimed identity is correct} \tag{1.1}$$

$$H_1 : B \neq B', \quad \text{the claimed identity is not correct} \tag{1.2}$$

Certain measure of similarity $s = Sim(P, P')$ is often defined and H_0 is decided if $s \geq T_D$ and H_1 is decided if $s < T_D$, where T_D is a decision threshold. The measure of similarity s is also referred to as the *match score*.
With regard to the expressions (1.1) and (1.2), 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*. The *False Acceptance Rate* (**FAR**) and *False Rejection Rate* (**FRR**) together characterize the accuracy of a recognition system for a given decision threshold. In Fig. 1.3 (left), **FAR** is the area under the H_1 density function to the right of the threshold and **FRR** is the area under the H_0 density function to the left of the threshold. In a more general framework, we can express the two errors as *False Match Rate* (**FMR**) and *False Non-Match Rate* (**FNMR**) [1]. The *Equal Error Rate* (**EER**) corresponds to a point at some threshold ($T_{\mathbf{EER}}$), where **FRR** = **FAR**.
Rather than showing the error rates in terms of probability densities, as in Fig. 1.3 (left), it is desirable to report system accuracy using a *Receiver Operating Curve* (**ROC**) [15, 1]. A **ROC** is a mapping $T_D \rightarrow$ (**FAR**, **FRR**) (Fig. 1.3, right):

$$ROC(T_D) = \left(FAR(T_D), FRR(T_D)\right) \tag{1.3}$$

Note that in a typical recognition system, all the information contained in the probability distribution functions is also contained in the **ROC**. The **ROC** can be directly constructed from the probability density functions as

$$FAR(T_D) = Prob(s \geq T_D \,|\, H_1 = true) = 1 - \int_0^{T_D} p(s \,|\, H_1 = true)ds \tag{1.4}$$

$$FRR(T_D) = Prob(s < T_D \,|\, H_0 = true) = \int_0^{T_D} p(s \,|\, H_0 = true)ds \tag{1.5}$$

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 [1].
The *Failure To Enroll Rate* (**FTE**) is the expected proportion of the population for whom the system is unable to generate repeatable templates. This will include those unable to present the required biometric feature, those unable to produce an image of sufficient quality at enrollment, and those who cannot reliably match their template in attempts to confirm whether the enrollment is usable [1].
The *Failure to Match Rate* (**FTM**) gives the percentage portion of the input biometric attributes, which cannot be compared with some saved template, or be processed [1].

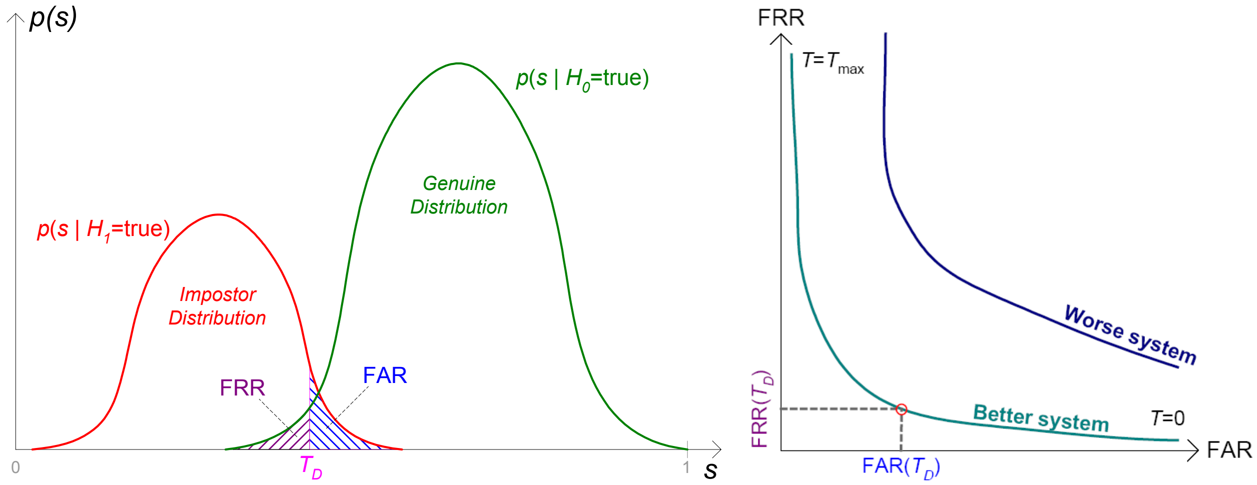

*Fig. 1.3: Impostor and Genuine distributions; Receiver Operating Curve (**ROC**)*

1.4 Goals of this work

There are three main goals which are new and newly published in this work.
The first goal is to estimate and compute the number of possibilities, which the fingerprint minutiae or details offer. This computation is important for an answer to the question, if there is enough information in the fingerprint to generate a key for the cryptographic purposes.
The second goal is to design a biometric security system, which supports the use of cryptography in conjunction with biometrics. This biometric security system should be open for other biometric technologies, such as voice, face or eye recognition, etc.
And the last goal of this work is the description of such fingerprint key generation. A vector should be generated from the fingerprint minutiae that could be considered as a key for symmetrical cryptography which would then protect appropriate confidential and/or secret data of the user.

2 ACTUAL STATE

2.1 Problem Definition

In the context of fingerprint recognition, fingerprints or simply prints are generally used to refer to the impressions of human fingers. Operationally, fingerprint identification can be decomposed into the following three fundamental tasks [6]:

- Fingerprint acquisition,
- Fingerprint classification, and
- Fingerprint matching.

Fingerprints are acquired from fingertips or impressions of the ridges and furrows. Fingerprint classification assigns a fingerprint into a certain category according to its global ridge and furrow configuration. Fingerprint matching determines whether two fingerprints are from the same finger. Fingerprint recognition is one of the most reliable and valid personal recognition methods which has been in use for a long time.

2.1.1 Fingerprint Acquisition

A fingerprint may be either (a) an *inked fingerprint* or (b) a *live-scan fingerprint*. Inked fingerprint is a term which is used to indicate that the fingerprint image is obtained from an impression of the finger on an intermediate media such as paper. The live-scan fingerprint is a collective term for a fingerprint image directly obtained from the finger without any intermediate step like getting an impression on paper. A number of scanning mechanisms can be used to scan ridges and furrows for finger impressions, including [3] (a) *optical frustrated total internal reflection*, (b) *ultrasonic total internal reflection*, (c) *optical total internal reflection of edge-lit holograms*, (d) *thermal scanning* of the temperature differential, (e) *scanning of differential capacitance*, and (f) *non-contact 3D scanning*.

2.1.2 Fingerprint Classification

Global patterns of ridges and furrows in the central region of fingerprints form special configurations, which have a certain amount of intra-class variability. But these variations are sufficiently small, which makes a systematic classification of fingerprints possible. When considering the fingerprint classification, only a portion of a fingerprint, referred to as the *pattern area*, is of interest [6, 7]. The pattern areas of fingerprints can contain two types of singular points: (a) *delta point* and (b) *core point*. The delta point, is defined as the point of ridge at or in front of and nearest to the centre of the divergence of the type lines. The core point is defined as the specific point located on or within the innermost sufficiently curved ridges.

With the above definitions, fingerprint categories can be described as follows:

- A *loop* is that type of fingerprint in which "one or more of the ridges enter on either side, recurve, touch or pass an imaginary line drawn from the delta point to the core point, and terminate or tend to terminate on or toward the same side from which such ridge or ridges entered” [3]. Loops can be further divided into *lunar loop* and *radial loop* subcategories.

- A *whorl* is that type of fingerprint in which “at least two delta points are present with a recurve in front of each” [3]. Whorls can be further divided into four subcategories: (a) *plain whorl*, (b) *central pocket loop*, (c) *double loop*, and (d) *accidental*.
- An *arch* is a special type of fingerprint configuration. Less than 15% of all fingerprints are arches [3]. Arches can be divided into two subcategories: (a) *plain arch* and (b) *tented arch*.

2.1.3 Fingerprint Matching

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 have been identified [6, 8]. 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. For a given fingerprint, a minutia can be characterized by its type, its *x* and *y* coordinates, and its direction (gradient).

Generally, in order to determine that two fingerprints are from the same finger, four factors must be evaluated: (a) correspondence of general pattern configuration, which means that two fingerprints must be of the same pattern configuration, (b) qualitative correspondence which requires that the corresponding minutiae details must be identical, (c) quantitative factor which specifies that at least a certain number (a minimum of 12 according to the forensic guidelines in the U.S.A. and Germany) of corresponding minutiae details must be found, and (d) relationship of minutiae details which specifies that the corresponding minutiae details must be identically interrelated.

2.2 Fingerprint Recognition Algorithms

The whole process of fingerprint recognition could be divided into 5 main steps:

1. *Acquirement of fingerprint*. The quality of acquired fingerprint is important for the fingerprint recognition. The basics were described in the Chapter 2.1.1.
2. *Fingerprint enhancement*. This step should enhance structures of papillary lines in damaged images. See description in the Chapter 2.2.1.
3. *Fingerprint classification*. It relates to the assignment of any fingerprint to the corresponding class [3, 6]. Further description can be found in the Ch. 2.2.2.
4. *Minutiae extraction*. In this step the structure of papillary lines is examined and the anomalies are detected and extracted as features (minutiae), namely the ridge ending and ridge bifurcation. All arts of the minutiae points are used for the dactyloscopic system.

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 the smart card).

2.2.1 Fingerprint Enhancement

Ideally, the ridge structures in a fingerprint image are well-defined. Each ridge is separated by two parallel narrow furrows and minutiae are anomalies in the ridges. When a fingerprint image is disrupted, such well-defined ridge structures are no longer visible. It is possible to develop an enhancement algorithm that can exploit these visual clues to improve the clarity of ridge structure in fingerprint images which in turn will improve the performance of the minutiae extraction algorithm.

2.2.2 Fingerprint Classification

There are two classification systems. The first one is the *Galton Classification System*, which includes only three fingerprint classes [10]. The second one is the *Henry Classification System*, which includes five fingerprint classes (arch / tended arch, right / left loop and whorl) and is used by the most fingerprint recognition systems [10]. Computational steps for classification (using OF) are as follows:

1. *Singular Points*: The *Poincare Index* [8] on the orientation field (OF) is used to determine the number of delta and core points in a fingerprint. A digital closed curve Ψ about 25 pixels long around each pixel is used to compute the *Poincare Index* as defined below:

$$Poincare(i,j) = \frac{1}{2\pi}\sum_{k=0}^{N_\Psi}\Delta(k), \tag{2.1}$$

where

$$\Delta(k) = \begin{cases} \delta(k) & if\,|\delta(k)| < (\pi/2) \\ \pi + \delta(k) & if\,\delta(k) \le (-\pi/2) \\ \pi - \delta(k) & otherwise \end{cases} \tag{2.2}$$

$$\delta(k) = \mathrm{O}'(\Psi_x(i'),\Psi_y(i')) - \mathrm{O}'(\Psi_x(i),\Psi_y(i)) \tag{2.3}$$

$$i' = (i+1) \mod N_\Psi$$

O is the orientation field, $\Psi_x(i)$ and $\Psi_y(i)$ denote coordinates of the i^{th} point on the length of arc of the parameterized closed curve Ψ.

2. *Symmetry*: The feature extraction stage also includes the estimation of position of an axis locally symmetric to the ridge structures at the core, and computation angle between the symmetry axis and the line segment joining core and delta points; average angle difference between the ridge orientation and the orientation of the line segment joining the core and delta points; and the number of ridges crossing the line segment joining core and delta points.
3. *Ridge Structure*: The classifier utilizes not only the information on orientation but also on structure of extracted ridges. This feature summarizes the overall

nature of the ridge flow in the fingerprint. In particular, it classifies each ridge of the fingerprint into three categories:

- Nonrecurring ridges: the ridges which do not curve very much.
- Recurring ridges: ridges which curve approximately by π angle.
- Fully recurring ridges: ridges which curve by more than π angle.

The distribution of fingerprint classes is following [8]: Plain Arch = 25,3%; Tended Arch = 10,9%; Left Loop = 21,6%; Right Loop = 20,4% and Whorl = 21,7%. Approximately 0,1% of fingerprints are unclassifiable – they have a special pattern combination of more classes.

2.2.3 Minutiae Extraction

The purpose of minutiae extraction is to extract representative features, called minutiae, from the input fingerprint images. Minutiae extraction is a trivial task when an ideal thinned ridge map *TR* [6] is available. Following conditions can determine the types of minutiae (see Fig. 2.11):

- If $(TR(i,j) = 1 \ \& \ \sum_{u=-1}^{1}\sum_{v=-1}^{1} TR(i+u, j+v) = 2) \Rightarrow$ the pixel (i,j) is a *r. ending*.
- If $(TR(i,j) = 1 \ \& \ \sum_{u=-1}^{1}\sum_{v=-1}^{1} TR(i+u, j+v) > 3) \Rightarrow$ the pixel (i,j) is a *r. bifurcation*.

For each detected minutiae, the following parameters are recorded: *type*; *x-position*; *y-position* and *orientation* (*gradient*) which is defined as the local ridge orientation of the associated ridge.

2.3 Actual Solutions

2.3.1 Fingerprint Technology

The company *Giesecke & Devrient* developed a system that uses a fingerprint as an instrument for secrecy encryption. The secrecy (a code word) is multiplied by a generation matrix of some redundancy code. Then the fingerprint technology is used to protect this secrecy. As a result, a biometrically enciphered secrecy is generated. By the inverse algorithm, a fingerprint from the same finger is used to decipher the enciphered secrecy. The solution of the company *ITSI* is oriented more to police investigation. This solution uses fingerprints as some art of signature for documents. When a trespasser is caught by the police, a police report is written in the field and a fingerprint of this trespasser is scanned on spot. The fingerprint is attached to the end of the document and the document is sent wireless to the police station. The solution of the company *Gemplus* focuses more to confusion of the attacker than to data protection and therefore will not be described closer. The company *Bioscrypt* introduced the Biometric Encryption system [5], which can protect *N*-bit long key using fingerprint information. This method is based on the image filtering and correlation; it does not use minutiae.

3 STRENGTH OF FINGERPRINT INFORMATION

Although the word "fingerprint" is popularly perceived as a synonym for individuality, the uniqueness of fingerprints is not a proven fact but an empirical observation [11]. The following chapters are concerned with this problem.

3.1 Basics of Entropy and Attack Possibilities

3.1.1 Shannon's Theory

Suppose X and Y are random variables. We denote the probability that X takes on the value x by $p(x)$, and the probability that Y takes on the value y by $p(y)$. The joint probability $p(x,y)$ is the probability that X takes on the value x and Y takes on the value y. The conditional probability $p(x|y)$ denotes the probability that X takes on the value x given that Y takes on the value y. The random variables X and Y are said to be independent if $p(x,y) = p(x) \cdot p(y)$ for $\forall$ possible values $x \in X$ and $y \in Y$.
Joint probability can be related to conditional probability by the formula

$$p(x,y) = p(x \mid y) \cdot p(y) \text{ and } p(x,y) = p(y \mid x) \cdot p(x) \qquad (3.1)$$

From these two expressions, we immediately obtain the following result, which is known as *Bayes'* Theorem [16]:
If $p(y) > 0$, then

$$p(x \mid y) = \frac{p(x) \cdot p(y \mid x)}{p(y)} \qquad (3.2)$$

X and Y are independent variables if and only if $p(x \mid y) = p(x)$ for $\forall\ x, y$.

3.1.2 Entropy

Suppose we have a random variable X which takes on a finite set of values according to a probability distribution $p(X)$. What is the information gained by an event which takes place according to distribution $p(X)$? This quantity is called the *entropy* of X and is denoted by $H(X)$. An event occurring with the probability p might be encoded by a bit string with the length of approximately $\log_2(p)$. Given an arbitrary probability distribution p_1, p_2, ..., p_n for a random variable X, we take the weighted average of the quantities $-\log_2(p_i)$ to be our criterion of information. This motivates the following formal definition: Suppose X is a random variable which takes on a finite set of values according to the probability distribution $p(X)$. Then the entropy of this probability distribution is defined to be the quantity [16]

$$H(X) = -\sum_{i=1}^{n} p_i \cdot \log_2(p_i) \qquad (3.3)$$

If possible values of X are x_i, $1 \le i \le n$, then we have

$$H(X) = -\sum_{i=1}^{n} p(X = x_i) \cdot \log_2(p(X = x_i)) \qquad (3.4)$$

3.1.3 Pseudorandom Bits and Sequences

The security of many cryptographic systems depends upon the generation of unpredictable quantities [12]. Examples can be the secret key in the DES encryption algorithm, the primes p and q in the RSA encryption and digital signatures. In all these cases, the generated quantities must be of sufficient size and "random" in the sense that the probability of any particular value being selected must be sufficiently small to prevent an attacker from gaining advantage through optimizing a search strategy based on such probability.

3.2 Uniqueness of Fingerprints

What do we mean by fingerprint uniqueness? The problem of fingerprint uniqueness can be formulated in many different ways. Two typical formulations are [14]:

- The uniqueness problem may be considered as determining the probability that any two individuals may have sufficiently similar fingerprints in a given target population.
- Given a sample fingerprint, determine the probability of finding a sufficiently similar fingerprint in a target population.

The problem of uniqueness is defined in a study [14] as the probability of a false association: For given two fingerprints from two different fingers, determine the probability that they are "sufficiently" similar.

3.2.1 Fingerprint Uniqueness Model

To estimate the probability of correspondence, the following assumptions should be made [14]:

- Two types of minutiae details are considered: ridge endings and bifurcations.
- A uniform distribution of minutiae in a fingerprint will be assumed.
- Correspondence of a minutiae pair is an independent event and each correspondence is equally important.

The probability of matching q minutiae in both position and direction is expressed by

$$p(M,m,n,q) = \sum_{\rho=q}^{\min(m,n)} \left(\frac{\binom{m}{\rho} \cdot \binom{M-m}{n-\rho}}{\binom{M}{n}} \cdot \binom{\rho}{q} \cdot (l)^q \cdot (1-l)^{\rho-q} \right) \tag{3.5}$$

where n is the number of minutiae in the original file, m is the number of minutiae in the template file, ρ is the number of falling into the similar positions, M=(A/w)/2r_0, A is the area of overlap, w is the ridge period, r_0 is length tolerance in minutiae location, l is the probability of two position-matched minutiae having similar direction and (1-l) is the probability of two position-matched minutiae taking different directions.

3.2.3 Experimental Results

The probabilities of fingerprint correspondence obtained for different values are [14]: e.g. M=104, m=26, n=26, q=26 $\Rightarrow$ $p(FP\ Correspondence)$=5,27·10^{-40}; M=104, m=26, n=26, q=12 $\Rightarrow$ $p(FP\ Correspondence)$=3,87·10^{-9}; M=248, m=46, n=46, q=46 $\Rightarrow$ $p(FP\ Correspondence)$=1,33·10^{-77} and M=70, m=12, n=12, q=12 $\Rightarrow$ $p(FP\ Correspondence)$=1,22·10^{-20}.

3.3 Strength of Information from Fingerprints

Three dactyloscopic axioms have been defined [9]:

- There are no such two people in the world which would have an identical pattern structure of papillary lines.
- The pattern of papillary lines of any person remains relatively stable or unchanged for his or her whole life.
- The papillary lines regenerate with the growth of the skin. The papillary lines cannot be destroyed, only when very deep removal of the skin occurs.

3.3.1 Resolution

Let σ_F is the size of a minutia (average thickness of a papillary line). The average size of minutiae was established on the basis of measurements on real fingers and measurements on fingerprints with known image resolution. Total 315 fingerprints were examined and, in each of them, two representative papillary lines were selected and then measured. The average of all values is σ_F = 0,331625 $mm \cong$ 0,33 mm. So we can take the size σ_F = 0,33 mm as the size of typical papillary line (i.e. minutia).

The size of one pixel in a sensor image can be denoted as σ_S. When we use the resolution of 600 *dpi*, then we have the pixel size σ_S = 0,043 mm. The relation between the minimal resolvable scales σ_F and σ_S is σ_F » σ_S. If the pixel size of the sensor is greater than the size of minutiae, then some pieces of information are lost.

3.3.2 Fingerprint Size

The comparison of fingerprint areas in all three FVC2004[1] databases enables us to say that the average fingerprint area is approximately 10 mm × 15 mm (width × height). Such area size is well accepted by all algorithms and the processing of such fingerprints is quite reliable. The area of 1,0 cm × 1,5 cm can be expressed in terms of σ_F or σ_S. This area is then $31\sigma_F \times 46\sigma_F$ or $233\sigma_S \times 349\sigma_S$.

3.3.3 Minutia and Antiminutia

Let the square $\sigma_F \times \sigma_F$ be called the elementary cell (see Figure 3.1a). During the recognition procedure, only those minutiae are discovered which can be clearly distinguished from the "background signal". In other words, there should be at least a

[1] http://bias.csr.unibo.it/fvc2004/

small area surrounding the minutia *m* (see Figure 3.1b). We call the eight elementary cells *A* around the minutia *m* as the antiminutiae and *A* gets for simplicity the same scale σ_F. The choice of such characteristic resolution σ_F guarantees sufficient invariance against small changes in the fingerprint structure due to aging or other systematic effects.

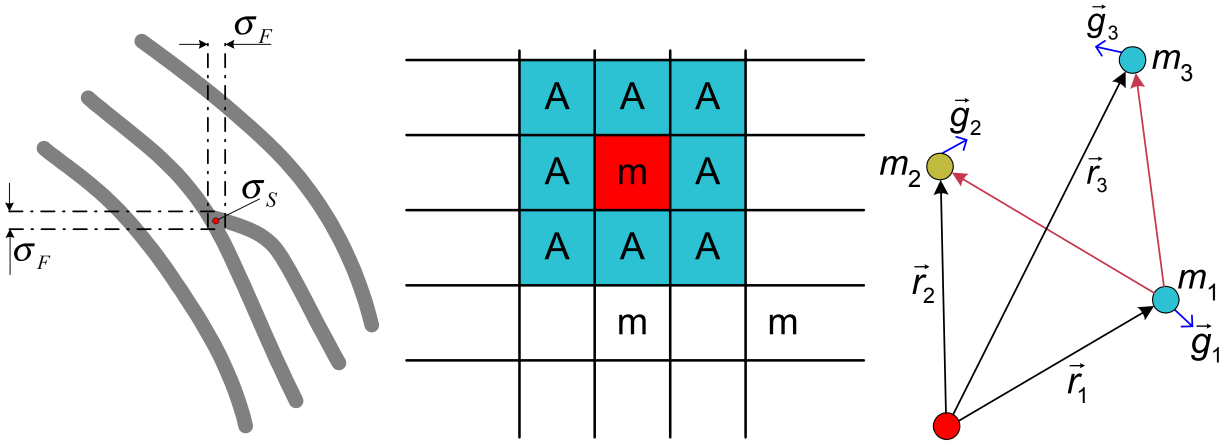

Fig. 3.1: a) Bifurcation in the corresponding biological resolution σ_F and the final reduction to the resolution of the sensor σ_S; b) Definition of minutia (m) and antiminutia (A); c) The information which characterizes the minutiae

If we consider a fingerprint with the typical dimension of 10 *mm* × 15 *mm*, which corresponds to the matrix of $31\sigma_F \times 46\sigma_F$, the maximal number of minutiae is 368. Generally, we can use the following equation for the computation of the number of minutiae:

$$P_M = \left\lfloor \frac{a+1}{2} \right\rfloor \cdot \left\lfloor \frac{b+1}{2} \right\rfloor \tag{3.6}$$

where P_M is the number of minutiae contained in the rectangle of $a \cdot \sigma_F \times b \cdot \sigma_F$ – any fraction of such number should be rounded down.

3.3.4 Strength of Information Contained in Fingerprints

Considering the method of minutiae recognition, the following pieces of information are usually stored with each extracted minutia μ_i [3]: Relative position (*x* and *y* coordinates); Type t_i (ridge ending or ridge bifurcation); Gradient (angle or direction of respective papillary line). We need to encode the position, type and gradient of minutiae (see Fig. 3.1c).

We have available the quantity of *M* minutiae. These are all real minutiae which have been found in the fingerprint. To encode the positions, all *x* and *y* coordinates need to be stored. If we consider the fingerprint rectangle of 10 *mm* × 15 *mm* with the resolution of 600 *dpi*, then we have total 80.500 (230 × 350 pixels) places in this matrix. To encode 80.500 places or positions, we need about 17 bits, which corresponds to the number of all possible, non-redundant, different vectors. The factor for positions is 2^{17}. For *M* minutiae:

$$\left(2^{17}\right)^{M-1} \tag{3.7}$$

In the Eq. (3.7) only M-1 minutiae are used because the reference minutia has already been defined as having the position in the origin of the coordinate system. The encoding of minutiae types is simple. We have only two types – ridge bifurcation and ridge ending. These two minutiae types can be encoded only with a single bit, which results in the factor:

$$2^{M} \tag{3.8}$$

The factor for types uses M minutiae, as the reference minutia has also a type assigned. The last factor to be created is based on the gradients. Here again only M-1 minutiae can be used, as the reference minutia has no direction (it is neutral). In our estimation of factors, we have used the matrix of $5\sigma_F \times 5\sigma_F$ for the computation of the gradient [3]. In this matrix, the gradient can be determined only in 16 possible directions (the angular resolution is therefore 22,5°). The resulting factor for the resolution equal to 22,5° can be computed as follows:

$$16^{M-1} = \left(2^{4}\right)^{M-1} \tag{3.9}$$

For the consequent factors, we should consider the minimal and maximal entropy factors. What concerns the *minimal entropy factor*, we should consider 12 minutiae (recommended by FBI and BKA as the minimum quantity of minutiae). On the basis of this condition, the minimal entropy can be computed [5] as follows:

$$\left(2^{17}\right)^{12-1} \cdot \left(2^{12}\right) \cdot \left(2^{4}\right)^{12-1} = 2^{243} = 1{,}4135 \cdot 10^{73} \tag{3.10}$$

What concerns the *maximal entropy factor*, it is possible to use up to 368 minutiae (see Chapter 3.3.3). Then the maximal entropy factor is [5]:

$$\left(2^{17}\right)^{368-1} \cdot \left(2^{368}\right) \cdot \left(2^{4}\right)^{368-1} = 2^{8075} = 6{,}5647 \cdot 10^{2430} \tag{3.11}$$

What concerns the approximate entropy factor, we can consider approximately 50 minutiae, which can be often found in a fingerprint. This latter quantity of minutiae corresponds to the factor $2^{1079} = 6{,}4768 \cdot 10^{324}$.

3.3.5 Vector Quantization

The topological positioning with this level of resolution can lead to minutiae locating failures. To avoid this art of failures, the quantization of positions is needed. In general, the topological quantization can be expressed as:

$$\sigma_Q = n \cdot \sigma_F \,, \quad n = 1,2,\ldots \tag{3.12}$$

The quantization of resolution reduces the sensitivity of minutiae extraction procedure to systematic and statistical effects.

3.3.6 Key Length

The minimal quantity of 12 minutiae with the minimal entropy factor 2^{243}, i.e. the key length 243 bits (see Eq. (3.10)), is sufficient for symmetric keys as well as for elliptic curves cryptography but not for asymmetric keys. The maximal entropy factor (Eq. (3.11)) is, indeed, suitable for all key lengths and types. If we consider the entropy factor for 50 minutiae, which is 2^{1079}, we arrive at the conclusion that the bit stream with the length of 1079 bits is not suitable for asymmetric cryptography. Further, if we consider the quantization step, then the average key length (for 12 minutiae) is around 144 bits and such length is suitable for both symmetric cryptography and elliptic curves cryptography.

3.3.7 Summary of Fingerprint Information Strength

In the beginning of this chapter, the *Shannon's* theory and basics of the entropy were described. In the following subsection, the description of fingerprint uniqueness, published in [14], was introduced. The Chapter 3.2 shows that (when comparing two fingerprints) the probability of correspondence between these two fingerprints lies in the range of $<5{,}47\cdot10^{-59}; 5{,}86\cdot10^{-7}>$. The more important question is how much information is hidden in the fingerprint and whether this amount of information is sufficient for generation of cryptographic keys. The answer to this question can be found in the Chapter 3.3 where my own computations and results are described. The resulting information entropy lies in the range of $<1{,}41\cdot10^{73}; 6{,}57\cdot10^{2430}>$ (when neglecting the quantization). The result is that a closed 100-bit data stream is sufficient for the generation of cryptographic keys for the symmetric cryptography. Elliptic curves cryptographic keys are also conceivable with this data stream but the generation of the cryptographic key pair is difficult. Furthermore, such bit stream size is not sufficient for general asymmetric cryptography.

The following equation can be considered as a general result for the entropy factor. First of all the quantity of minutiae P_M is computed using Eq. (3.6) and then we receive the following expression for the matrix $a\cdot\sigma_F\times b\cdot\sigma_F$:

$$E = \left(2^{N_B}\right)^{P_M-1} \cdot 2^{P_M} \cdot \left(2^{N_G}\right)^{P_M-1} \tag{3.13}$$

where E is the entropy factor, N_B is the number of bits needed to encode the positions of minutiae in the matrix $a\cdot\sigma_F\times b\cdot\sigma_F$, and N_G is the number of bits to encode the gradients (directions) of minutiae. The number N_G is defined as equal to 4, because we have 16 directions and $16=2^4$. The number N_B needs to be computed each time for the corresponding matrix $a\cdot\sigma_F\times b\cdot\sigma_F$. And the last value P_M is limited to the matrix $a\cdot\sigma_F\times b\cdot\sigma_F$, as well as the value N_B.

Of course, such very high resolution (600 *dpi*) reduces dramatically the potential for correct key generation during the generation phase. In order to achieve a higher process reliability and performance, we introduced a new additional step into the standard recognition procedure that makes the algorithm more robust and resistant against systematic effects. The price for this is the reduction of the maximal available information data size to a limit having the value between approximately 2^{177} and 2^{122} (for 12 minutiae and the quantization factors n=1 and n=5, respectively). Although this number is big, it is still negligible when compared with the amount of data necessary for the generation of an asymmetric key. On the other hand, this number is big enough for the use as a symmetric key and has much higher information entropy then commonly used passwords or PINs.

4 KEY GENERATION

The general concept of the biometric system can be extended. We have introduced a cryptobiometric system using the combination of key generation from the fingerprint and voice [13], and a cryptographic algorithm. Let us call this system the Biometric Security System (only fingerprint technology is considered further).

4.1 Biometric Security System

The Biometric Security System consists of a general biometric system and a general cryptographic system. A new special step, an art of pipe through both systems, has been developed and tested. This connecting step corresponds to the key generation from the fingerprint. The whole Biometric Security System must be divided into two separate concepts. The first one is the Certificate Creation concept, and the second one the Certificate Usage concept.

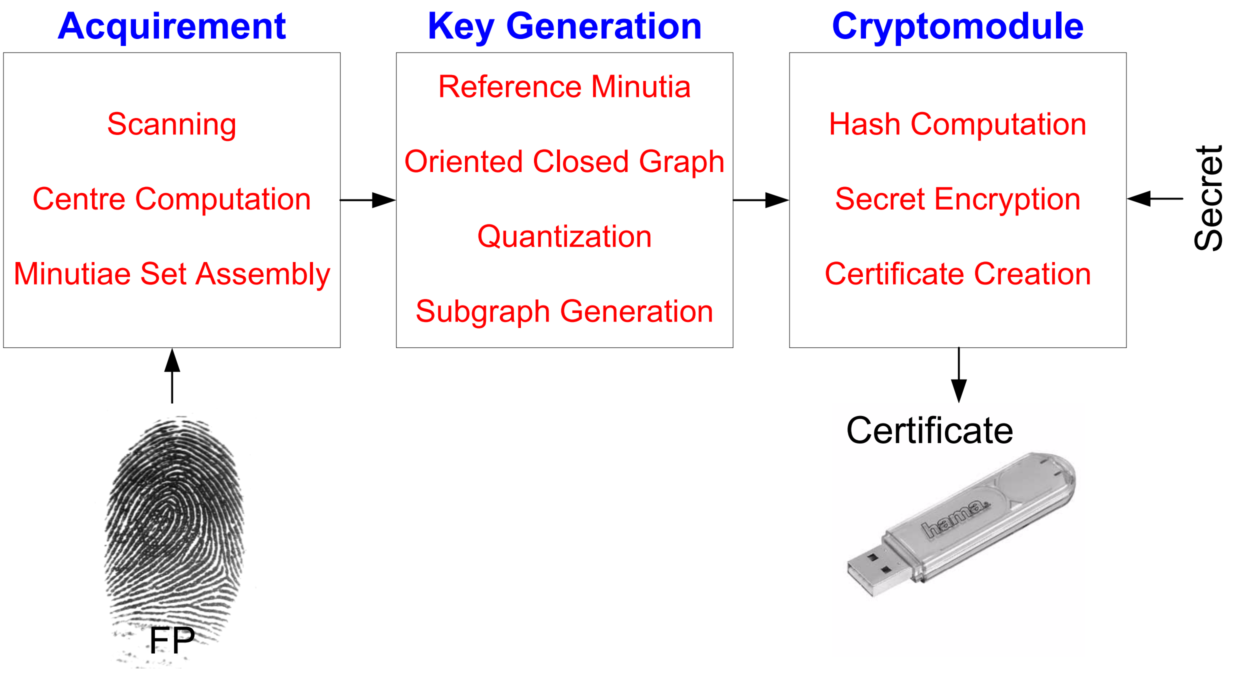

Fig. 4.1: Concept of Certificate Creation for the Biometric Security System

4.2 Certificate Creation Concept

In this concept, the certificate is generated, including appropriate biometric information. The certificate could be based on the X.509 standard, but an own format of the certificate structure can also be used. It is important that this Certificate Creation is done only once. Since this creation is done by an administrator, the certificate does not need to be reloaded and naturally, there is no reason to generate the certificate several times, only if some part of the certificate is to be modified or when the certificate is no more valid. In such cases, a new certificate has to be created. In Fig. 4.1 is shown the scheme for the concept of Certificate Creation.

4.2.1 Acquirement Phase

For the fingerprint acquirement, some sensor has to be used. The output of fingerprint sensor is represented by an image with the resolution of aprox. 500 *dpi* and generally with 256 gray levels. Following steps of image processing are used [3, 6]: image enhancement, thresholding, ridge thinning and minutiae extraction.

In each step (there are five of them in our case) the minutiae of the appropriate fingerprint are stored. Let us call the minutiae μ_i^j, where i is the descriptor of the fingerprint image (i=1,...,5), and j is the number of minutiae n_i found in the appropriate fingerprint (j=1,...,n_i). Each minutia (only ridge ending and ridge bifurcation are considered) has three items (position is regarded as a single item) [3]:

$$\mu_i^j = \left(x_i^j, y_i^j, \phi_i^j, t_i^j\right) \tag{4.1}$$

where x_i^j is the x-position, y_i^j is the y-position, ϕ_i^j is the gradient and t_i^j is the type.

Computation of fingerprint centre

Very important piece of information is the position of the centre of the fingerprint. All three methods for fingerprint centre computation can be described as follows:

- *Method based on the minutiae gravity centre*. This method is based on the position of all the minutiae μ_i^j, more precisely on their x and y coordinates. The Euclidean distances and minimum value of these distances in each fingerprint can be computed by the following expressions [2]:

  $$d_i^j = \frac{1}{n_i - 1} \cdot \sum_{k=\{1\ldots n_i\}\setminus\{j\}} \sqrt{\left|x_i^j - x_i^k\right|^2 + \left|y_i^j - y_i^k\right|^2} \quad \& \quad \delta_i = \min\left(d_i^1, \ldots, d_i^{n_i}\right) \tag{4.2}$$

  The minutia with the minimal distance δ_i has the same coordinates as the centre of the fingerprint with coordinates [C_X;C_Y].
- *Method based on ridge count*. We can consider the papillary lines (from aspects of fingerprint image pattern) as homocentric circles with the origin in the real centre of the fingerprint. We can compute the number of throughpasses in the horizontal and vertical directions. It is clear that the number of circle throughpasses in the centre of all circles is greater than in outlying regions. The following expressions can be used for the computation of vertical ridge counts (in rows) and for the selection of the vertical centre:

  $$RC_{V,All} = \{RC_i \mid i = 0\ldots Height\} \text{ and } RC_V = avg(\max(RC_{V,All})) \tag{4.3}$$

  where *Height* is the number of pixels in the vertical direction (image height) and RC_i is the ridge count for the corresponding row in the image. Similar equations can be used for the horizontal ridge count (in columns). At the end of this computation procedure, we obtain two coordinates RC_V and RC_H, which represent the fingerprint centre [C_X;C_Y], respectively.
- *Method based on the Orientation Field*. The main steps in determining the orientation image using the algorithm based on the least mean square iteration method are as follows [6]:

  1) Divide the input fingerprint image into blocks of size w×w (500 *dpi* ≈ 16).

2) Compute the gradients [6] $\partial_x(i,j)$ and $\partial_y(i,j)$ at each pixel, (i,j); the *Sobel* or more complex *Marr-Hildreth* operator [18] can be used.
3) Estimate the local orientation of each block centered at pixel (i,j) using the following equations [6, 7]:

$$v_x(i,j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} 2\partial_x(u,v)\partial_y(u,v) \tag{4.4}$$

$$v_y(i,j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} (\partial_x^2(u,v) - \partial_y^2(u,v)) \ ; \ \theta(i,j) = \frac{1}{2}\cot\left(\frac{v_y(i,j)}{v_x(i,j)}\right) \tag{4.5}$$

where $\theta(i,j)$ is the least square estimate of the local ridge orientation at the block centered at pixel (i,j).
4) In order to perform the low-pass filtering, the orientation image needs to be converted into a continuous vector field, which is defined as follows [7]:

$$\Phi'_x(i,j) = \sum_{u=-\frac{w_\Phi}{2}}^{\frac{w_\Phi}{2}} \sum_{v=-\frac{w_\Phi}{2}}^{\frac{w_\Phi}{2}} h(u,v)\Phi_x(i-uw, j-vw) \tag{4.6}$$

where h is a 2D low-pass filter with a unit integral and $w_\Phi \times w_\Phi$ specifies the size of the filter. For Φ'_y can be used similar equation, based on Eq. (4.6).
5) Compute the local ridge orientation at (i,j) using

$$\mathrm{O}(i,j) = \frac{1}{2}\cot\left(\frac{\Phi'_y(i,j)}{\Phi'_x(i,j)}\right) \tag{4.7}$$

Let us call the reduced orientation field O_R. The computation of the centre, based on O_R, consists of following steps:

1. Normally, 8 possible directions are used in each block $w \times w$ [3]. These directions are shown in the Fig. 4.2a, and have the following angle values: ①=90°; ②=67,5°; ③=45°; ④=22,5°; ⑤=0°; ⑥=157,5°; ⑦=135°; ⑧=112,5°. This number of directions is necessary for the classification. But for the fingerprint centre computation, the number of directions could be reduced – only 4 directions are sufficient (①, ③, ⑤ and ⑦). Other directions are assigned to these directions.
2. The fingerprint image needs to be divided into four uniform blocks (see Fig. 4.2b). To determine the centre of the fingerprint, it is necessary to compute the centers of gravity for the following orientation field directions: ①, ③, ⑤ and ⑦. Two centre points are computed for each direction, each lying in the opposite block(s). These two points for each direction can be considered as the end points of an abscissa. If we compute the cross-points for the lines of $y_1 + y_5$ and $y_3 + y_7$ then these two points create an abscissa. If we compute the middle of this abscissa, we receive the centre $[C_X;C_Y]$.

Assembly of Minutiae Set

After five repetitions of the minutiae set acquirement, some art of comparison of these sets should be made. Only those minutiae μ_i^j which can be identified in all the sets are allowed to be stored in the result set. The minimal threshold $\mu_{\min}$ for respective number of minutiae needs to be defined. The number of minutiae must not be lower than 12 (12 rule, see Chapter 3.3.4). On the other side, we should consider the maximal number of minutiae in a fingerprint. This number is 368 (see Chapter 3.3.3). Then the condition for minimal and maximal threshold for respective number of minutiae can be formulated as follows (n_μ = final number of minutiae):

$$12 < \mu_{\min} \le 368 \text{ and } n_\mu \ge \mu_{\min} \tag{4.8}$$

After assembly of minutiae set, we obtain resulting final minutiae set:

$$\mu = \left\{ \mu_i \,|\, \mu_i = \left(x_i, y_i, \phi_i, t_i \right),\, i = 1 \ldots n_\mu \right\} \tag{4.9}$$

4.2.2 Key Generation Phase

Determination of Reference Minutia

From the previous steps, we have obtained the minutiae set μ. We need to generate an oriented closed graph [2] and therefore we need the origin of this oriented graph. The origin can be defined as the starting vertex in the closed oriented graph and let us call it *Reference Minutia* and denote it μ_R. The main condition for μ_R is its position – the closer is such minutia to the centre of the fingerprint $[C_X;C_Y]$ the higher is the probability that it will be selected as a reference minutia. The following equation can be used for the computation:

$$\mu_R = \left(\mu_m \,\middle|\, m \leftarrow \min\left(\sqrt{\left|C_X - x_i\right|^2 + \left|C_Y - y_i\right|^2} \right),\, i = 1 \ldots n_\mu \right) \tag{4.10}$$

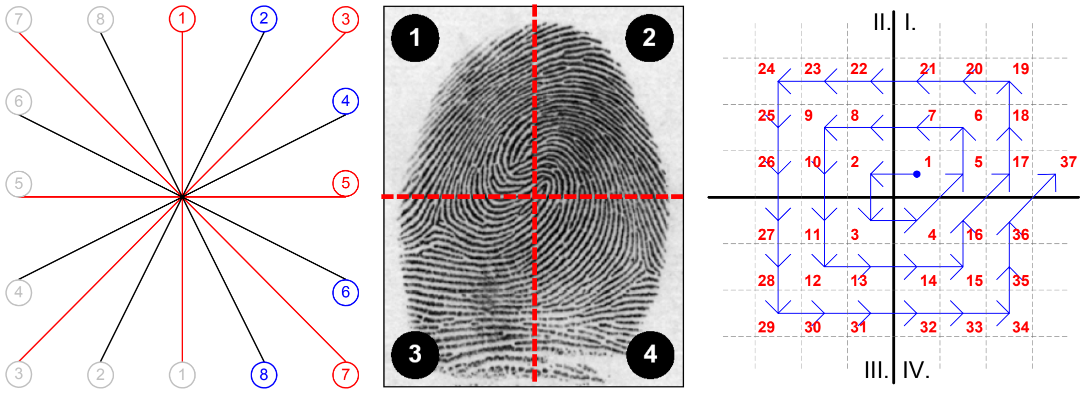

Fig. 4.2: a) Directions of OF; b) Block division of FP; c) Creation of rough matrix mask

Creation of Oriented Closed Graph

Oriented graph G is a pair of sets (V,E), where V is a set of vertices, E is a set of edges between the vertices. This graph can be expressed as $E = \{(u,v) \mid u,v \in V,\, u \neq v\}$.

The first task is to reorder the minutiae (The 1st minutia is the reference minutia, the next one is the 1st closest minutia to the reference minutia, etc.). The 2nd step is the translation – we can re-compute the coordinates of all items in μ as follows:

$$\mu^T = \left\{ \mu_i^T \mid \mu_i^T = \left(x_i - x_R, y_i - y_R, \phi_i, t_i \right), i = 1 \ldots n_\mu \right\} \tag{4.11}$$

where μ^T is the new minutiae set.

Now, the step for the rotational modification (the elimination of rotation) comes in consideration and this step consists in the rotation of all minutiae in the set μ^T. For the rotation, the angle α is used, which is computed as the angle between the x-axis and the abscissa from the reference minutia to the second minutia. Using α, we can rotate all components of μ^T:

$$G = \left\{ (\mu_i^T{}', \mu_{i+1}^T{}') \mid \mu_i^T{}', \mu_{i+1}^T{}' \in \mu^T{}' \;\&\; \mu_i^T{}' \neq \mu_{i+1}^T{}', i = 1 \ldots n_\mu \right\} \approx \mu^T{}' \tag{4.12}$$

By this procedure, an oriented closed graph has been created with the beginning and ending vertex in the μ_R. Its components, i.e. the edges E, represent vectors starting in the actual minutia and pointing to the next minutia in the set $\mu^{T}{}'$. The graph G can be considered as the full vector path, including all vertices.

Quantization

New places in the rough matrix mask are generated, using the principle shown in the Fig. 4.2c. The minutiae from the set $\mu^{T}{}'$ are then positioned to the particular cells of the rough matrix mask. The structure of the minutiae set change as follows:

$$\zeta = \left(n_i^\zeta, \phi_i^T, t_i \right), \; i = 1 \ldots n_\mu \tag{4.13}$$

where n_i^ζ is the cell number in the rough matrix mask. The vertices of the graph G are only the cell numbers in the rough matrix mask, the order of minutiae remains same. The graph is therefore modified as follows:

$$E = \left\{ (u,v) \mid u, v \in V \,\&\, u \neq v \right\} = \left\{ \left(n_i^\zeta, n_{i+1}^\zeta \right) \mid n_i^\zeta, n_{i+1}^\zeta \in \zeta, n_i^\zeta \neq n_{i+1}^\zeta \right\} \tag{4.14}$$

where $V = \zeta$, $i = 1 \ldots n_\mu$ and $G = (V,E)$.

Sub-Graph Generation

The number of all sub-graphs could be computed as the amount of combinations without repeating, using following equation $Nr_{Combinations} = (m!) / [(m - k)! \times k!]$, where m is the number of all minutiae of the complete graph ($m = n_\mu$) and k is the number of minutiae in the sub-graph. The sub-graph can be described as follows:

$$G_{Sub}^r = (V_{Sub}^r, E_{Sub}^r), \; V_{Sub}^r = \{\zeta_1, \ldots, \zeta_k\} \tag{4.15}$$

$$E_{Sub}^r = \left\{ \left(n_i^\zeta, n_{i+1}^\zeta \right) \mid n_i^\zeta, n_{i+1}^\zeta \in V_{Sub}^r \;\&\; n_i^\zeta \neq n_{i+1}^\zeta \right\} \tag{4.16}$$

where r denotes one of the combinations, i.e. $r = 1 \ldots Nr_{Combinations}$, and k is the number of used sub-vertices for the sub-graph. These sub-graphs represent the individual biometric keys. Then the biometric key set will be as follows:

$$K_r = \left\{ \left(n_l^\zeta, \phi_l^T, t_l \right)_r, \ldots, \left(n_o^\zeta, \phi_o^T, t_o \right)_r \right\} \;\&\; K = \left\{ K_r \mid r = 1 \ldots Nr_{Combinations} \right\} \tag{4.17}$$

where K is the set of all biometric keys, K_r is the rth combination and l & o assume the values from the interval <1, n_μ> ($l < o$), whereas the number of components is k.

4.2.3 Cryptomodule Phase

Hash Computation

Individual components from the biometric keys set K_r are taken as the input of the hash function h. After the computation of all hashes of all components from K_r, the output set is defined:

$$H = \{h(K_r) \mid K_r \in K \ \ \& \ \ r = 1 \ldots Nr_{Combinations}\} \tag{4.18}$$

where H is the whole set of hash values from all biometric key items from K. In H, only hash values of respective biometric key are saved. The positions of items in H correspond to the positions of items in K. The set H has $Nr_{Combinations}$ components.

Secret Encryption

If we call the plaintext (or open secret) as P, and the ciphertext (or enciphered secret) as C, then we can define the encryption process g as the transformation:

$$g : P \xrightarrow{K_r} C, \ C = g_{K_r}(P) \tag{4.19}$$

where K_r is the particular key from the set K, $r = 1...Nr_{Combinations}$ and follows:

$$S = \{g_{K_r}(P) \mid K_r \in K, \ r = 1 \ldots Nr_{Combinations}\} \tag{4.20}$$

This set S contains $Nr_{Combinations}$ of enciphered versions of the plaintext P, always using another key K_r.

Certificate Creation

We use the basic structure of the X.509 certificate and the part of *Extensions* is used for the storage of our data. The part *Extensions* of the certificate looks as follows:

$$Ext = \{id, false, \{(H_r, S_r) \mid H_r \in H, S_r \in S, r = 1 \ldots Nr_{Combinations}\}\} \tag{4.21}$$

4.3 Certificate Usage Concept

The phase of usage can be applied repeatedly; it requires no action of the certification authority (or the administrator). The only purpose is, if the confidentiality of the certificate can be proved, to present the public key of the certification authority (or the administrator), which (or who) has signed the certificate.

4.3.1 Acquirement Phase

The acquirement phase is very similar to the acquirement phase of the concept for the Certificate Creation. The only difference is that only one fingerprint is scanned and appropriate minutiae are extracted.

4.3.2 Key Generation Phase

Similarly as in the Chapter 4.2.2, the μ'_R needs to be found. The principle of creation of the oriented closed graph is again the same as in the Chapter 4.2.2. The whole computational process will not be repeated; only the result is presented here:

$$G' = \omega' = \{(\omega'_i, \omega'_{i+1}) \mid \omega'_i, \omega'_{i+1} \in \omega' \ \& \ \omega'_i \neq \omega'_{i+1}\}, \ i = 1 \ldots n_\omega \tag{4.22}$$

where ω' is the original set (ω) after the transformation and reordering of coordinates, and n_ω is the number of extracted minutiae. Follows the quantization. The only condition is that the rough matrix mask must have the same cell size!

The difference in relation to the Certificate Creation concept is that only one sub-graph is generated. One possibility of combinations from the whole graph is absolutely randomly selected and the corresponding sub-graph is extracted. The sub-graph, G'_{Sub}, of G' is generated as:

$$K' = \left\{(n_l^{\omega'}, \phi_l^{\omega'}, t_l^{\omega'}), \ldots, (n_o^{\omega'}, \phi_o^{\omega'}, t_o^{\omega'})\right\} \tag{4.23}$$

where l is the starting position and o is the end position of the sub-graph in relation to the graph G'. In this case, only one biometric key K' exists and no other keys are generated. The size of K' must be same as the size of the key K_r.

4.3.3 Cryptomodule Phase

Hash Computation and Comparison

First of all, the hash value of the key K' is computed. The following task is new. We have the hash value H' and the hash values H have been stored in the certificate. The first step is to check the validity of the certificate. The second is the searching in the set H for the occurrence of the value H'. We can obtain two possible results:

- A match has been found. It means that the hash value H' has been found in H (in the certificate).
- A match has not been found. The occurrence of H' in H has not been confirmed. In the next call of the sub-graph generation, another sub-graph needs to be generated. The repetition can be done only $Nr'_{Combinations}$ times. If we run out of all the $Nr'_{Combinations}$, then no sub-graph has built the right key and the decryption step cannot be processed or completed.

Secret Decryption

If a match has been found then the decryption can start. There are pairs – hash value of the biometric key and the encrypted secret using the biometric key, then we can decrypt the corresponding secret, using the key K' as follows:

$$q : C \xrightarrow{K'} P, P = q_{K'}(C) \tag{4.24}$$

where C is the encrypted secret (ciphertext) and P is the plaintext.

4.4 Proposal of Practical Usage

Two possible proposals are as follows:

- *Private key protection*. The first possibility is the protection of some private key. Let us assume that some application has generated a key pair. The condition is that the private key cannot be saved in an open form. These condition are guaranteed in our system. When the private key is requested by another application, the fingerprint needs to be scanned and the biom. key is generated.
- *Personal document extension*. The second proposed possibility is important for new extension of the information in the personal documents, with regard to biometrics. The personal document can include a smart chip on which the certificate can be stored, including all data as described in the certificate creation concept. Let us consider the photography of the user as the secret part (plaintext). This proposal can be used, e.g., for customs control.

5 PRACTICAL RESULTS AND SUMMARY

This final chapter describes the acquirement of the fingerprint database, the reliability testing using some industrial algorithms and testing of my own applications.

5.1 Fingerprint Database

Three sensors (from companies Bergdata, SecuGen and Veridicom) have been applied for the acquirement of the fingerprint database. Dactyloscopic cards (with their own format) were used as the fourth input for the database. The sensors Bergdata and Veridicom have included software development kits.

The final fingerprint database includes $N_{User} = 10$ users and $N_{Sensor} = 3$ sensors. The record of each user contains both hands ($N_{Hand} = 2$) and $N_{Finger} = 4$ fingers (index, middle, ring and thumb). In each session (1 user and 1 sensor), total $N_A = 65$ fingerprints of each finger were stored. It was necessary to reduce the database size (insufficient image quality). The final number of fingerprints per finger was set to $N_N = 50$ (instead of 65). This reduction step was done manually. The final number of all FPs in the DB is $N_{FP} = N_{User} \cdot N_{Sensor} \cdot N_{Hand} \cdot N_{Finger} \cdot N_N = 10 \cdot 3 \cdot 2 \cdot 4 \cdot 50 = 12.000$.

5.2 Database Enrollment and Matching (Industrial Algorithms)

Two industrial algorithms (Siemens and Veridicom) have been used for database quality testing. The analysis of applicable rates for both algorithms is included further in this chapter.

Failure to Acquire Rate (FTA). The **FTA** rate is related to the frequency of a failure to acquire and means the failure of biometric sensor to capture the biometric data. The results are as follows: $\mathbf{FTA}_{\text{Bergdata}}$ = 0,77%; $\mathbf{FTA}_{\text{SecuGen}}$ = 0%; $\mathbf{FTA}_{\text{Veridicom}}$ = 0,46%. No **FTA** rate for dactyloscopic fingerprints exists.

Failure to Enroll Rate (FTE). The **FTE** rate is related to the frequency of a failure to enroll and means the inability of the system to extract the biometric data for biometric record keeping (creation of a template). The **FTE** rates are as follows:
$\mathbf{FTE}_{\text{SBergdata}}$ = 2,71%; $\mathbf{FTE}_{\text{SSecuGen}}$ = 0%; $\mathbf{FTE}_{\text{SVeridicom}}$ = 5,88%;
$\mathbf{FTE}_{\text{ABergdata}}$ = 3,97%; $\mathbf{FTE}_{\text{ASiemens}}$ = 3,98%; $\mathbf{FTE}_{\text{AVeridicom}}$ = 0,72%.

*Receiver Operating Curve (**ROC**).* **ROC** is the graphical representation of the False Non-Match Rate (**FNMR**, eventually **FRR**) in relation to the False Match Rate (**FMR**, eventually **FAR**). First the **FMR** and **FNMR** areas have to be computed. The Fig. 5.1 displays the **ROC**s for Siemens and Veridicom algorithms. The x-axis represents the values of **FMR** and the y-axis the corresponding **FNMR** for all values of the threshold T within the interval from 0 to 100 on the Matching Score axis.

5.3 Key Generation

This chapter contains the results of testing of my own applications for the key generation from fingerprints.

Computation of centers

In the application for centers computation, the first method is based on the minutiae gravity center, the second one on the orientation field, and the last one is based on the ridge count maximums in horizontal and vertical directions. All fingerprints were examined and their cores (if present) and some other reference points (often delta points, especially at dactyloscopic fingerprints) have been determined. These two point types have been used for the computation of stability of respective methods. The results of computation of average proportional distances between the cores and reference points can be seen in the Fig. 5.2. The *x*-axis refers to the ID number of users and the *y*-axis refers to the proportional variation of the distance between the core and reference point (in %).

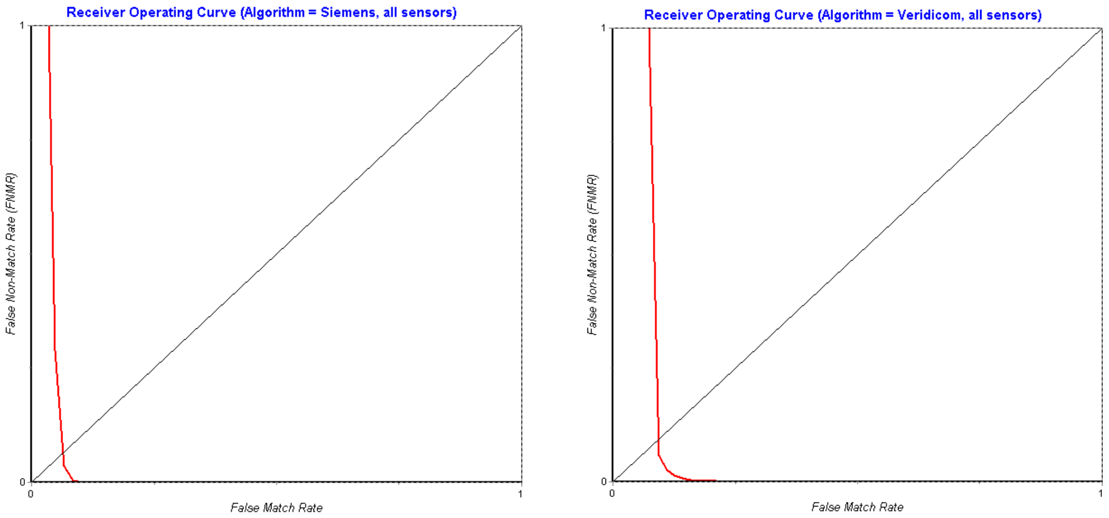

Fig. 5.1: ROC for the Siemens and Veridiom algorithms

The average proportional distance variations between Core and corresponding center resulting of each method, and between Reference and corresponding center resulting of each method have been computed. After considering all winners and losers, the best method is Method_2 (Orientation Field), the second best method is Method_1 (Minutiae Gravity Center) and the last (worst) method is Method_3 (Ridge Count). Therefore the Method_2 has been used in the following computations. The results of SecuGen cannot be compared with those of other sensors (very small amount of available data from this sensor) ⇒ they cannot be found in the following sections.

Reduction of minutiae amount

The amount of minutiae in fingerprints can vary much. The following values were defined as thresholds: 10, 15, 20, 25, 30 and 35. The maximal numbers of minutiae are: B = 71,8; D = 134,8; V = 75,3. The minimal numbers of minutiae are: B = 20,6; D = 97,14; V = 27,2. The threshold of 10 cannot be considered (12 rule), and for 25, 30 and 35 are the numbers of refused file too high. Only the thresholds of 15 and 20 are significant and used further.

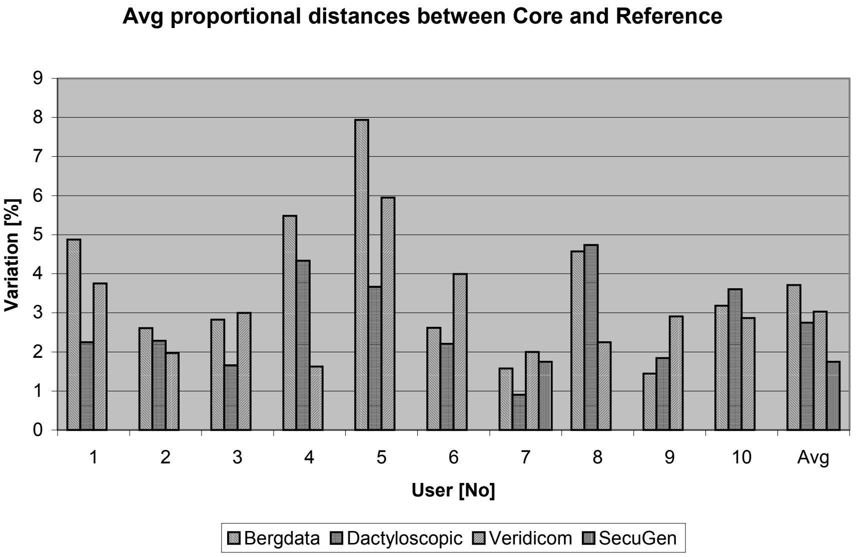

Fig. 5.2: Average proportional distances between Core and Reference

Reordering, translation and rotation

The next sub-step is reordering of minutiae. For the reordering of minutiae, the center of the Method_2 (winner) is used. The distances to this center have been computed for each minutia. The closest minutia to the center of the Method_2 has been selected as the Reference minutia and the following minutiae are reordered depending on the distance. The following sub-step is the translation. The Reference minutia is translated to the origin of the coordinate system and other minutiae are translated in the same direction. The last sub-step is the rotation. For the rotation, the angle between the Reference minutia and the next minutia (after reordering) is computed. The average rotation angle for Bergdata is 177,11°; for dactyloscopic fingerprints 196,40° and for Veridicom 114,99°.

Quantization

The quantization is the following step. This step includes putting of some art of rough mask on the image, with the beginning in the Reference minutiae. The minutiae are placed into respective rough matrix cells. The matrix cells have been defined as rectangle cells with the dimensions of $Factor \times \sigma_S$. The following four values were used as factors: 3, 5, 10 and 20. If a cell already contains a minutia and some other minutia is to be placed into the same cell, a collision is announced. The values 10 and 20 are too high. Therefore only the factors 3 and 5 are used further.

Computation of sub-graphs

Further, all ordered combinations of sub-graphs are computed. We have two file types – 15 and 20 minutiae pro file. In consequence, the sub-vectors with lengths 12 and 17, respectively, have been considered. For each file all (12 $\Rightarrow$ 455/ 17 $\Rightarrow$ 1140) sub-vector combinations were generated. The whole database volume after the computation of sub-vectors reaches around 2,6GB + 9,3GB = 11,9GB.

Sub-graphs comparison

The whole database with the volume of 11,9GB needs to be compared. The process of comparison has been divided into two steps (estimation of genuine and impostor distribution) and furthermore it has been realized on 5 computers. We have come to the following final results. In Fig. 5.3, we can see the comparison of best candidates from all **ROC** graphs. The best curve was obtained for the following settings: Bergdata sensor, 20 minutiae, rotated and quantization factor equal to 5. The other two curves are very similar; the same settings are: amount of 20 minutiae, two times rotation and two times quantization factor 5.

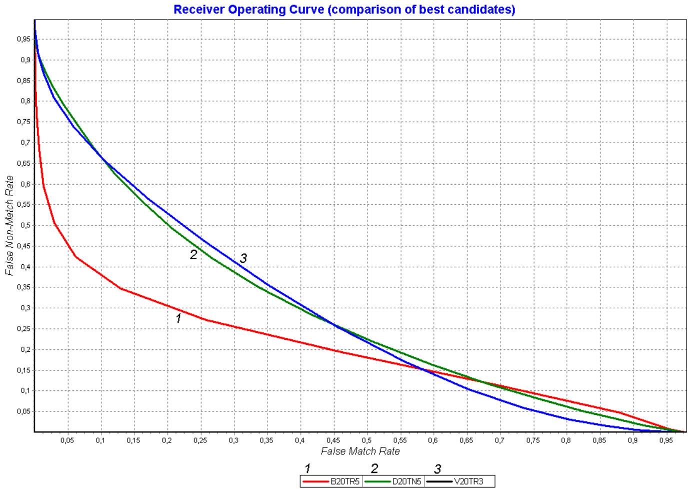

Fig. 5.3: Receiver Operating Curves for best candidates

Now, we want to decide, which settings have been the best ones. The best settings are characterized by the following set of data:

- Bergdata sensor, 20 minutiae pro file, non-rotated, factor 3 or 5.

5.4 Future Work

We can ask where the strong or weak points of this system are and what can be improved. The answer to the first part of this question can be actually found in the Chapter 4.4. These two usage proposals are not the only possibilities. This solution can be implemented on credit cards or for daily data protection. The strong point of this solution consists furthermore in the amount of entropy which is considerably greater than in passwords or PINs used for the protection of the access to cryptographic keys nowadays. The weaknesses include e.g. the fact that the user needs to repeat the acquirement of the fingerprint when no match of hash value is found, and of course another fact that the liveness testing is necessary.

What could be still improved in the system? Each sub-step of the whole key generation process has enough space for optimization. When we consider the percentage amounts of total matches (suitable for hash match), it is clear that the improvement of all sub-steps is needed because we surely would not want to repeat the acquirement of our fingerprints more times. Further we need an efficient data reduction.

6 REFERENCES

[1] Arnold, M., Busch, C., Drahansky, M., Ihmor, H., Reinefeld, T., Zwiesele, A.: *BioFinger – Evaluierung biometrischer Systeme (Fingerabdrucktechnologien)*, Darmstadt, FHG-IGD, 2004

[2] Black, P.E.: *Dictionary of Algorithm and Data Structures*, NIST, 2004

[3] Drahansky, M.: *Fingerabdruckerkennung mittels neuronaler Netze*, Diploma Thesis, Brno University of Technology, 2001

[4] Drahansky, M., Nötzel, R., Bonfig, K.W.: *Sensoren zur Fingerabdruckerkennung*, Sensoren, Signale, Systeme, Kreuztal, 2004, p. 49-60, ISBN 3-933609-19-4

[5] Drahansky, M.: *Nutzung biometrischer Daten zur Gewinnung personenbezogener kryptographischer Schlüssel*, Biometrie – BIOSIG2004, Fraunhoffer Gesellschaft – IGD, Darmstadt, 2004

[6] Hong, L.: *Automatic Personal Identification Using Fingerprints*, Michigan State University, Department of Computer Science, 1998

[7] Hong, L., Wan, Y., Jain, A.: *Fingerprint Image Enhancement: Algorithm and Performance Evaluation*, Michigan State University, Department of Computer Science, 1998

[8] Jain, A., Pankanti, S.: *Fingerprint Classification and Matching*, Michigan State University + IBM T.J. Watson Research Center, 2001

[9] Jozefek, A.: *Principy některých daktyloskopických klasifikačních systémů*, Ústav kriminalistiky Právnické fakulty UK, 1972

[10] Kay, K.: *Introduction to Fingerprint Recognition*, 2003

[11] Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S.: *Handbook of Fingerprint Recognition*, Springer, New York, 2003, ISBN 0-387-95431-7

[12] Menezes, A.J., Oorschot, P.C., Vanstone, S.A.: *Handbook of Applied Cryptography*, CRC Press, 1996, ISBN 0-8493-8523-7

[13] Orsag, F.: *Biometric Security Systems: Speaker Recognition Technology*, Dissertation Thesis, FIT BUT, 2004

[14] Pankanti, S., Prabhakar, S., Jain, A.K.: *On the Individuality of Fingerprints*, IBM T.J. Watson Research Center + DigitalPersona Inc. + Michigan State University, 2001

[15] Ratha, N.K., Senior, A., Bolle, R.M.: *Automated Biometrics*, IBM Thomas J. Watson Research Center, 2003

[16] Stinson, D.: *Cryptography: Theory and Practice*, CRC Press LLC, 1995, ISBN 0849385210

AUTHOR’S CURRICULUM VITAE

Personal Data

Name	Ing. Martin Drahanský
Born	04.04.1978, Brno, Czech Republic (CZ)
E-Mail:	drahan@fit.vutbr.cz
Internet:	http://www.fit.vutbr.cz/~drahan

Education

2001	MSc. - computer science, FEECS, Brno University of Technology, CZ
2001	MSc. - electrotechnics, FernUniversität in Hagen, Germany
1996	Grammar school aimed at mathematics and physics, Brno, CZ

Languages

German	Advanced
English	Intermediate

Praxis

2002 – 2005	External worker, Fraunhofer Gesellschaft, Institut für graphische Datenverarbeitung, Darmstadt, Germany
2002 – 2005	Scientist, Institut für Meßtechnik, Universität Siegen, Germany
1996 – 2002	External teacher of informatics, Grammar school tř. Kpt. Jaroše 14, Brno, CZ

Prizes

12/2001	Siemens prize for the diploma thesis

ABSTRACT

This dissertation describes certain special art of biometric systems. General biometric systems are well known in public and systems based on the fingerprint recognition belong, without question, to the most familiar ones. Fingerprints have been used for identification and authentication for a long time because their uniqueness and reliability have been proven in everyday life. Nowadays, there are a great number of such biometric systems based on fingerprint recognition on the market. One group of them is used for forensic purposes (these are called dactyloscopic systems and are used in tasks of person identification). Another group of biometric systems represents the topic of interest of this dissertation – access or verification systems.

Both such systems and related basic biometric terms and processes are described in the first and second chapters.

If we try to combine a biometric (fingerprint) system with some cryptographic system, we are confronted with the question, if there is enough information entropy in the fingerprint. Some computations of the similarity among fingerprints have already been published but they have considered the matching of fingerprints. For cryptographic tasks, it is more important to exploit the information strength hidden in fingerprint papillary line structures. The answer to this question can be found in the third chapter.

Finally, if the information strength is adequate to the cryptographic requirements, we can design a system, which uses fingerprint technology as a biometric information input and offers biometric keys to the cryptographic subsystem. The detailed description of such Biometric Security System can be found in the fourth chapter, where all processes needed for the computations and processing are described. The Biometric Security System was implemented and appropriate modules were tested. The test analyses and reports are presented in the last, fifth, chapter.