Neuro File Encryptor

Uživatelská příručka

2020

Výsledek vznikl za finanční podpory Technologické agentury České republiky v rámci projektu č. FW01010289.

Obsah:

1. Architektura

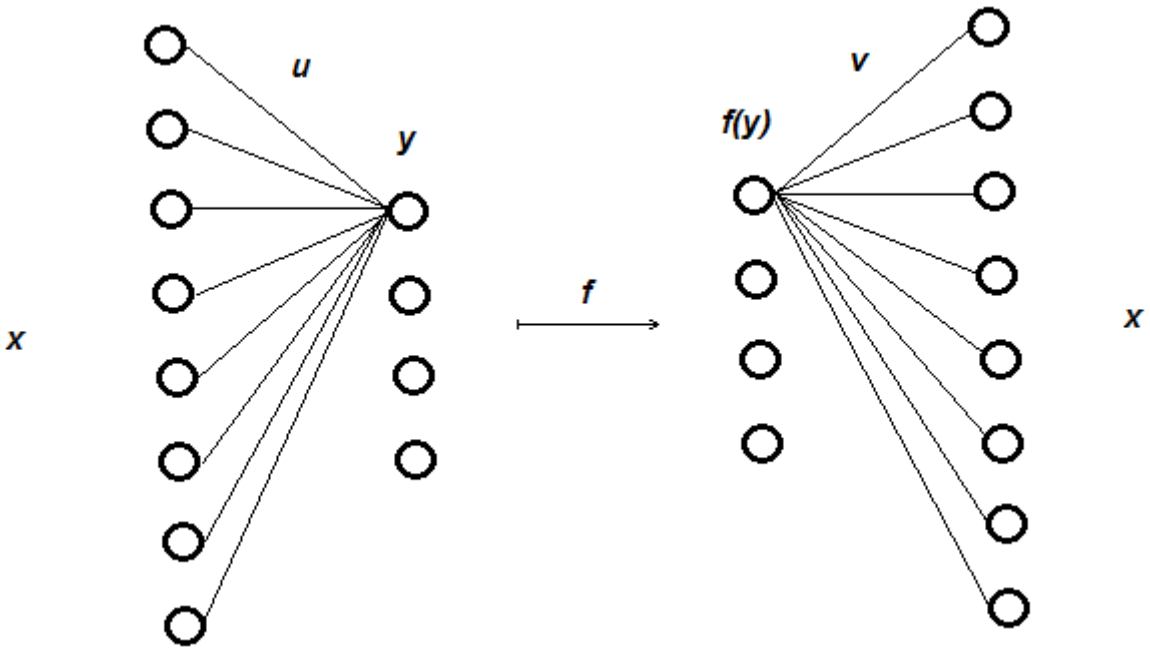
Symetrické šifrování libovolného počítačového souboru probíhá zakódováním každého jeho bajtu $\lfloor x_1, \dots, x_8 \rfloor$ do jemu příslušného vektoru $\lfloor y_1, \dots, y_4 \rfloor$:

$$\lfloor x_1, \dots, x_8 \rfloor \begin{bmatrix} u_{11} & \cdots & u_{14} \\ \vdots & \ddots & \vdots \\ u_{81} & \cdots & u_{84} \end{bmatrix} = \lfloor y_1, \dots, y_4 \rfloor$$

a posléze jeho následným dekódováním:

$$\lfloor f_1(y_1), \dots, f_4(y_4) \rfloor \begin{bmatrix} v_{11} & \cdots & v_{18} \\ \vdots & \ddots & \vdots \\ v_{41} & \cdots & v_{48} \end{bmatrix} = \lfloor x_1, \dots, x_8 \rfloor$$

kde $\vec{x}$ resp. $\vec{y}$ jsou vektory potenciálů neuronů vstupní/výstupní resp. skryté, tzv. *dělící* vrstvy, $\vec{f}$ je vektor aktivačních funkcí neuronů dělící vrstvy a $[\vec{u}_1, \dots, \vec{u}_4, \vec{v}_1, \dots, \vec{v}_4]$ je konfigurace sítě, tj. adaptovaný náhodně generovaný klíč.

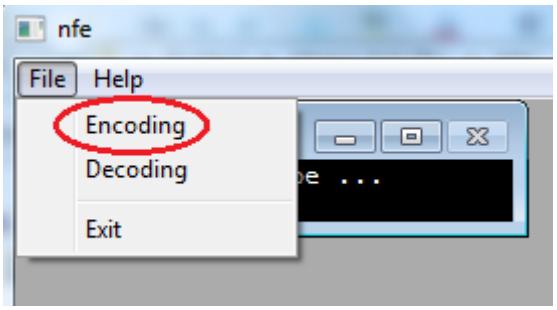


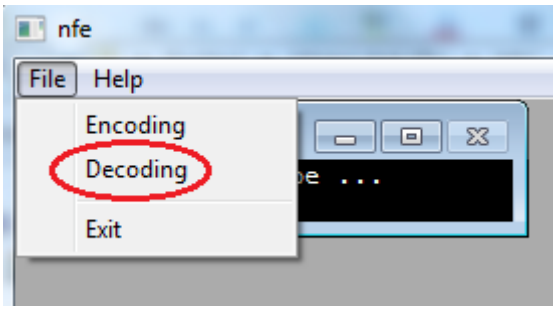
2. Data

V adresáři aplikace lze editací souboru PRJ.INI parametrizovat volbu pracovního adresáře PRJ1÷PRJ9 (zadáním čísla 0÷9) jakožto podadresáře adresáře aplikace, který je pak nutno v adresáři aplikace vytvořit, zadáním čísla nula je pak pracovní adresář přímo adresář aplikace.

2.1. Vstup/Výstup

Šifrovaný soubor musí být umístěn v pracovním adresáři pod názvem INPUT.DAT. Po spuštění šifrování (levý obrázek) se v pracovním adresáři vytvoří jeho zašifrovaná podoba (šifra) pod názvem DATA.BIN, který lze zpětně dešifrovat (pravý obrázek) do souboru v pracovním adresáři pod názvem OUTPUT.DAT:





2.2. Konfigurace

K šifrování souboru se užije šestnáct neuronových sítí o stejné topologii (pět vrstev o osmi, šestnácti, čtyřech, šestnácti a osmi neuronech), ale různých konfiguracích, uložených v binárních souborech (viz dále). Během spuštění šifrování resp. dešifrování musí být umístěn v pracovním adresáři šifrovací klíč v podobě šestnácti souborů CONFIGxx.BIN (xx=00÷15). Uvedené soubory lze vytvořit v aplikaci Data Mining Provider jako výsledek učení neuronové sítě na trénovacích datech obsahujících všechny kombinace nastavení osmi bitů, přiváděné během učení sítě současně na vstupní i výstupní vrstvu.

2.3. Omezení

Velikost šifrovaného souboru je omezena na 10 MB, tj. 10485760 bajtů.

3. Chyby

Skončí-li funkcionalita sítě zprávou „Action aborted“, popis chyby se zapíše do souboru ERROR.LOG vytvořeného v pracovním adresáři:

`Memory allocation error`

Chyba alokace vnitřní paměti.

`Input file error`

Chyba načtení šifrovaného souboru resp. klíče.

`Data consistency error`

Nekonzistentní šifrovací klíč.

`Activation error`

Chyba aktivace neuronové sítě.

`Output file error`

Chyba zápisu dešifrovaného souboru resp. šifry.

`Action aborted`

Vyskytla se neočekávaná chyba.