FINGERPRINT RECOGNITION SYSTEM USING ARTIFICIAL NEURAL NETWORK AS FEATURE EXTRACTOR: DESIGN AND PERFORMANCE EVALUATION

Pavol Marák — Alexander Hambalík

ABSTRACT. Performance of modern automated fingerprint recognition systems is heavily influenced by accuracy of their feature extraction algorithm. Nowadays, there are more approaches to fingerprint feature extraction with acceptable results. Problems start to arise in low quality conditions where majority of the traditional methods based on analyzing texture of fingerprint cannot tackle this problem so effectively as artificial neural networks. Many papers have demonstrated uses of neural networks in fingerprint recognition, but there is a little work on using them as Level-2 feature extractors. Our goal was to contribute to this field and develop a novel algorithm employing neural networks as extractors of discriminative Level-2 features commonly used to match fingerprints.

In this work, we investigated possibilities of incorporating artificial neural networks into fingerprint recognition process, implemented and documented our own software solution for fingerprint identification based on neural networks whose impact on feature extraction accuracy and overall recognition rate was evaluated. The result of this research is a fully functional software system for fingerprint recognition that consists of fingerprint sensing module using high resolution sensor, image enhancement module responsible for image quality restoration, Level-1 and Level-2 feature extraction module based on neural network, and finally fingerprint matching module using the industry standard BOZORTH3 matching algorithm. For purposes of evaluation we used more fingerprint databases with varying image quality, and the performance of our system was evaluated using FMR/FNMR and ROC indicators. From the obtained results, we may draw conclusions about a very positive impact of neural networks on overall recognition rate, specifically in low quality.

1. Introduction

Fingerprints are physiological traits and can be viewed as texture patterns formed by ridge skin impressions on the surface of various materials. When digitized they can be used to identify an individual based on peculiar characteristics in fingerprint pattern in an automated manner. We can divide patterns of fingerprints into 3 categories [5]. They differ in complexity of automated classification and discrimination power in matching two fingerprints (see Figure 1).
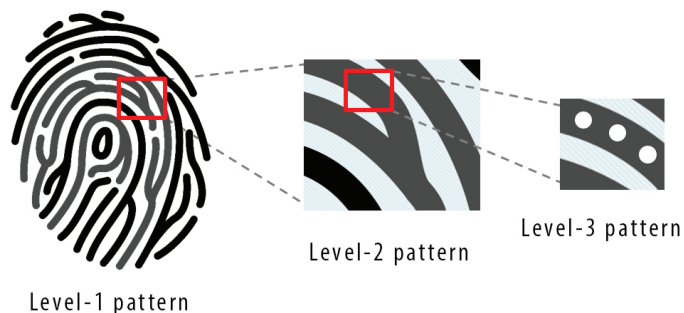

FIGURE 1. Illustration of taxonomy of fingerprint feature levels (Level-1 represents global fingerprint patterns, Level-2 represents local ridge details, Level-3 are fine details at microscopic scale like sweat pores).

Level-1 pattern represents overall fingerprint ridge flow. These patterns are usually divided into 5 categories (left loop, right loop, whorl, arch and tented arch) [13]. Global ridge flow is a well-defined pattern and can be retrieved easily even when the image quality is not sufficient. After successfully resolving Level-1 pattern category the whole search space in fingerprint database is narrowed down to only specific fingerprint pattern subset what drastically reduces computation time [13]. In [5], authors extensively studied and compared performance of more state-of-the-art Level-1 classification techniques. We refer to this process as coarse fingerprint classification and it is discussed in Section 3.2 in more detail.

Level-2 features or minutiae are local ridge characteristics that make every fingerprint a unique pattern. The premise of fingerprint uniqueness has been generally accepted, but still lacks proper scientific validation. Individuality of fingerprints based on Level-2 features as well as probability of correspondence of random fingerprints is discussed in [15]. These features are used by our fingerprint recognition system presented in this paper. More Level-2 feature types are distinguished from basic shapes to very complex and rare patterns with extremely high discrimination power in fingerprint matching process (see Figure 2). Level-2 features are mainly characterized by the spatial location in the image,

their orientation and their shape type [13]. The two Level-2 features mostly used are the ridge ending, referred to as termination, and the bifurcation, which refers to a ridge splitting into two ridges. Despite such a wide range of Level-2 patterns, only ridge terminations and bifurcations are preferred in majority of commercial or civil fingerprint identification systems thanks to simplicity of their automated extraction. Fingerprints are considered identical when a matching algorithm finds sufficient number of correspondences of Level-2 features. Probably the best known and most widely used matching algorithm is called *BOZORTH3* that is a part of NIST Biometric Image Software. It uses two sets of Level-2 features to establish a similarity score between two fingerprints [21].
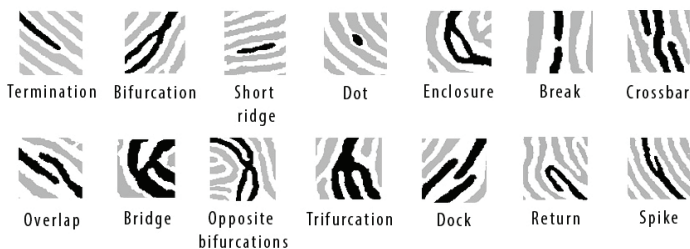
FIGURE 2. Level-2 feature types.

Level-3 features are microscopic level patterns that are almost exclusively used by forensic examiners. They consist of sweat pore locations, ridge geometric details, scars and other very small characteristics. Lately, their computer automated extraction has been seriously considered as more and more biometric system vendors begin to adopt 1000 PPI (pixels per inch) sensing resolution of fingerprint images in their recognition systems [22]. Latent fingerprints often lack a large portion of fingerprint pattern. This is the case where Level-3 features step in. They make identification possible even with limited amount of information.

Patterns made of Level-2 features are highly individual and differ even between identical twins [1]. Importance and complexity of Level-2 features is the main source of inspiration that resulted into our software implementation of complete biometric system that performs fingerprint identification.

At early stages of development, we used multiple structural approaches for feature extraction like analyzing patterns in fingerprint skeletons or time consuming computation of local ridge curvature [18]. All of them turned out to be ineffective either in terms of time needed for computation or insufficient accuracy of recognition. To overcome this issue, we implemented a new neural network-based algorithm for extraction of Level-2 features. Firstly, instead of exploring the entire image, our algorithm detects only critical image regions with high probability of Level-2 feature occurrence using Crossing Number method [13].

Using locations of the critical regions we extract blocks from the original fingerprint image to be able to work with original unmodified patterns. Blocks from the original image are then passed as input data to our neural network trained on considerably large database of fingerprint patterns that we manually obtained from various individuals and sensors. We also employed a neural network at the fingerprint coarse classification stage. In coarse classification, fingerprint is classified into one of the five categories according to Level-1 features. This way the database of candidate fingerprints is reduced to a smaller subset which is searched by matching algorithm at the final stage.

Feature extraction is just one module of our biometric system. Our system as a whole is able to capture fingerprints using a high-resolution sensor, performs image enhancement by means of adaptive filtering, and finally matches two fingerprint Level-2 feature sets using NIST's widely used BOZORTH3 matching algorithm. These consecutive processes were developed as a fully automated system with possibility to be switched to manual mode with user interaction that enables adjusting various parameters for enhancement and extraction.

Finally, we evaluated performance of the proposed automated system on databases of fingerprints captured by sensors of various manufacturers with various resolution and quality. We carried out experiments separately on good and poor quality fingerprints and compared the results with selected top performing algorithms in the field to evaluate strong and weak aspects of our solution.

The rest of this paper is organized as follows: Section 2 describes the problem of fingerprint recognition, reviews the related literature and emphasizes the most important sources of our motivation. Section 3 is the core of this paper concentrating on the design of our fingerprint recognition system with providing explanation of the most relevant aspects of enhancement and feature extraction. In Section 4 we discuss the results obtained from several experiments aimed at the evaluation of accuracy of individual system modules the same as well as the overall recognition rate. Finally, Section 5 provides summary of our research, identifies our contribution and brings forward our future work intentions.

2. Motivation and problem analysis

Despite intense development efforts, there is still one open research problem that has been addressed by many researchers but it still cannot be considered a solved task. We talk about acquisition of reliable fingerprint features for matching from poor quality images [1].

There are generally two different fingerprint representations. One is based on Level-2 features and another makes use of other fingerprint image properties like response to image filters [23], average gray level values in image regions or

120

other characteristics derived from fingerprint pixels. We may think of Level-2 features as the most important peace of information carrying the uniqueness of each fingerprint. We dedicated our research to developing methods of extraction of these features. Reliable detection of the features is also dependent on the underlying fingerprint structure representation which can be divided as follows:

- *Raw fingerprint image.* There are many methods that detect and classify minutiae directly in a raw fingerprint image [18], [12] and [19]. Authors of these techniques claim that using original fingerprint image with no prior enhancement leads to detection of true features as the original pattern structure is not touched. Another advantage is the reduction of computational load since no enhancement is employed. On the other hand, computational time can be increased by a process of analyzing an original image where patterns are not well defined.

- *Fingerprint skeleton.* A different family of techniques first transform arbitrary fingerprint image by means of adaptive filtering techniques to its improved representation with enhanced structure clarity, and then a ridge thinning algorithm is applied to produce a fingerprint skeleton. The skeleton is a black-and-white image where all ridge lines are 1 pixel wide. Two methods of obtaining fingerprint skeleton are described in [7] and [17]. The fingerprint skeleton is very convenient representation for automated pattern recognition. Unfortunately, the process of filtering and skeletonizing is not perfect, and introduces unwanted pattern modifications and sometimes suppresses true features.

In our research, we wanted to overcome limitations of both these fingerprint representations by combining advantages of fingerprint skeleton and original gray-scale image to create a robust Level-2 extraction system and to incorporate a neural network as a feature extractor.

Limited number of Level-2 features in incomplete or noisy fingerprints makes it necessary to discriminate the type of Level-2 feature and treat it with due importance since the match of rare patterns is more significant than the match of frequent patterns. Fingerprints are prone to image structure imperfections and that is why we always need to incorporate image enhancement into fingerprint recognition systems. The most effective techniques are so called adaptive filters that after convolution with the original image restore the original structure of fingerprint thanks to adjustable smoothing capability. Overview of adaptive filtering techniques is presented in chapter 3.6 of [13] and the most popular technique of contextual filtering, Gabor Filters, are described in [8]. Quality of fingerprints influences the overall recognition rate. Considering this fact, a robust fingerprint extraction must be a principal component of the whole recognition system.

Automated detection and extraction of intrinsic properties of Level-2 features is a rather challenging task. The vast majority of feature extraction methods is based on an extensive examination of image pixel configurations or texture properties. This approach is time consuming often resulting in missing very important features or detecting false features. Furthermore, a robust feature extractor must be able to deal with rotation, translation and skin distortion. This way, the same pattern may occur multiple times in slightly different form.

These problems motivated us to study machine learning algorithms, especially properties of feedforward artificial neural networks and their possible designs to solve the problem of fingerprint pattern classification, more specifically Level-2 features. Neural networks are learning algorithms which keep their knowledge of observed set of patterns in their internal parameters. Neurons as their processing elements represent non-linear functions. Multiple neurons can be used to model very complex relationship between inputs and outputs.

Machine learning approach represented by neural networks makes extraction of highly distinctive and variable Level-2 features feasible. By means of this research we want to demonstrate feasibility of training a feedforward neural network to accurately recognize Level-2 patterns of various quality. Neural network--driven fingerprint feature extraction is the principal component of our software solution of user identification and it also can be viewed as a contribution to the field of fingerprint recognition techniques as only very limited number of publications deal with neural networks used as Level-2 feature extractors and if, their technology background has not been presented in an understandable way and their performance has not been rigorously studied.

3. Design of the proposed fingerprint recognition system

The system proposed in [2] was one of the first publications dealing in more detail with possibilities of Level-2 feature extraction using a multi-layer feedforward network. The system as presented by the authors performed recognition of variously shaped features in fingerprint skeleton. Features were presented to the neural network as small image blocks containing white or black pixels. Ridge terminations and bifurcations were the only feature types extracted by their network. Their system had some drawbacks as it was not able to adapt to a different resolution because of the fixed block size and the fact that the patterns were extracted from the skeleton image may cause that many important details will be lost during the process of skeletonizing.

However, this system served as a starting point for our own research. We made a couple of steps further and developed fully functional recognition system, not just a feature extraction system.

The proposed system works in several consecutive stages:

- *Acquistion* – is the way system receives fingerprint images.
- *Enhancement and Coarse Fingerprint Classification* – enhancement is the process of restoring fingerprint structure clarity and coarse classification is the process of selecting only the most similar fingerprints from the database according to Level-1 pattern. Classification of Level-1 pattern is based on neural networks.

- *Extraction* – here, we designed the second neural network capable of extraction of Level-2 shapes and gave it the ability to detect these crucial details directly in the original fingerprint image rather than skeleton what later proved to be a considerable improvement over the work in [2]. After enhancement, image blocks are presented to the neural network for Level-2 feature detection and classification. After classifying, all recognized features in the fingerprint form a feature vector.

- *Matching* – the final decision making step where we compare two vectors of Level-2 features extracted by the neural network and select the best matching vector from the database of fingerprints (enrolled users).

For programming purposes, we used optimized C language implementation of neural networks' construction, training and testing in FANN library (more details about the library can be found in [14]). Overall scheme of our automated fingerprint identification system is depicted in Figure 3.
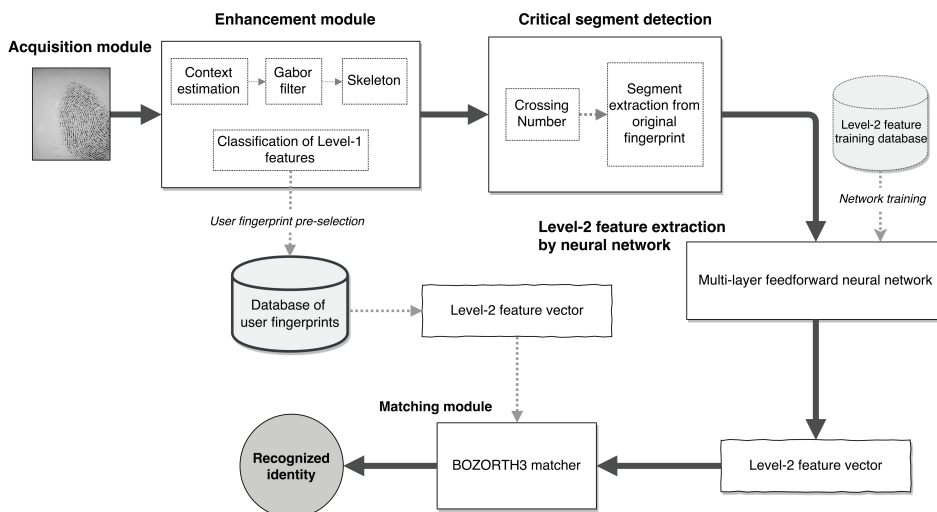

FIGURE 3. Overview of our software solution for fingerprint recognition.

3.1. Fingerprint acquisition

Our system acquires fingerprints in two ways. One is selecting an image file from a collection of fingerprint images from a number of publicly available databases. The second way is to directly capture fingerprint using Biometrika HiScan-PRO 1000 PPI scanner that interacts with our software. Sensor is capable of dual resolution scanning in both 500 PPI and 1000 PPI. This sensor is a FBI-certified product so it can be used for forensic applications as well.

3.2. Enhancement and coarse fingerprint classification

Image quality is the top factor predetermining rate of successful identifications so adequate attention must be paid to image enhancement. The priority is to improve a structure quality of fingerprints but leave local features intact. This is possible by means of adaptive filters. We used Gabor filters as described in [20] for smoothing ridge patterns. Gabor filter makes use of so-called local fingerprint context that is local ridge orientation and frequency. We estimated local ridge orientations by computing ridge orientation map that encodes directions of the ridges in a particular location of the fingerprint area expressed as angle in radians [13]. Ridge frequency is estimated using the method described in [8] by detecting grayscale value maxima in direction orthogonal to local ridge orientation. Last step in enhancement is skeletonizing that converts gray-scale fingerprint image to black-and-white image where ridges are only 1 pixel wide. In case of skeletonizing, we followed the implementation instructions in [9].

To reduce computation time, we employed specific neural network with one hidden layer to work as a Level-1 pattern recognizer. Since Level-1 features represent overall ridge flow that changes its direction based on location in the image we used values from the orientation map calculated in the previous steps to train the neural network in order to learn the relationship between the orientation map and one of the five Level-1 classes. In each training image, the orientation map was calculated by dividing each image into 17×17 blocks. This way we obtained 812 blocks from each image. Estimated orientation values in each of these blocks were passed to input layer of the neural network. Number of hidden neurons can be manually adjusted but the best results were obtained using 200 hidden neurons with symmetric sigmoid as a transfer function. There are 5 neurons in output layer encoding the final response. Individual Level-1 classes are mapped to specific target responses. Target response with the smallest Euclidean distance from the output response is then selected as a classification result.

3.3. Extraction of Level-2 features using neural network

This section introduces our new method of Level-2 feature extraction. Once the fingerprint enhancement process is finished and the fingerprint pattern was assigned one of the five Level-1 classes, our system continues by detecting critical
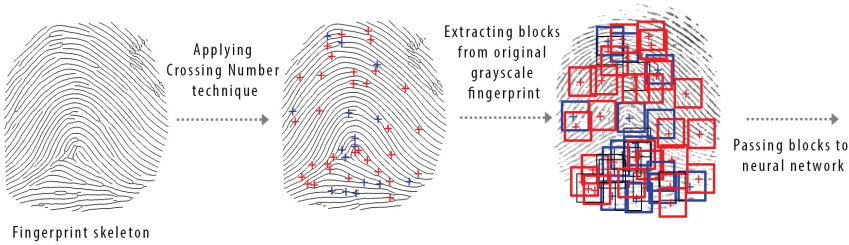
FIGURE 4. Detection of Level-2 candidate locations in fingerprint skeleton (in the center) and extraction of small image blocks centered at candidate locations sent to neural network.

segments or blocks of the fingerprint which contain Level-2 features. These blocks represent possible places of Level-2 feature occurrence. Crossing Number method is widely used method to detect simple patterns in fingerprint skeleton [13]. We used it to mark positions of all ridge bifurcations and terminations as these two types are building blocks of derived and more complex Level-2 features. After finding positions of all bifurcations and terminations we used them as central pixels of small 11×11 square blocks in the original image (see Figure 4). Pixels inside these blocks in the original image were passed to the input layer of Level-2 neural network extractor.

Our Level-2 extraction neural network uses one input layer consisting of 121 input elements (number of pixels in 11×11 block). The number of hidden neurons is 200, the same as in he neural network for Level-1 feature classification. The 11×11 block was used to extract only ridge bifurcations and terminations to be able to compare our solution to other methods in literature since they focus on these types of features only. For this reason, the number of output neurons is 2. Output neurons form a response vector which encodes the class of Level-2 feature. Size of 11×11 is suggested to use only when working with 500 PPI fingerprint images. During evaluation, we constructed different networks working with larger block sizes appropriate for recognition of more complex Level-2 features often occupying more space in the image. Figure 5 shows process of distributing image pixels of the original fingerprint to input layer of our neural network for classification.

3.4. Feature matching

After the classification of all image blocks in the original fingerprint, a final feature vector is produced. In this feature vector, each extracted Level-2 feature is represented by its x and y coordinate, orientation expressed in degrees and shape type. The vector is then passed to BOZORTH3 algorithm for matching. BOZORTH3 is one of the best publicly available open-source matching
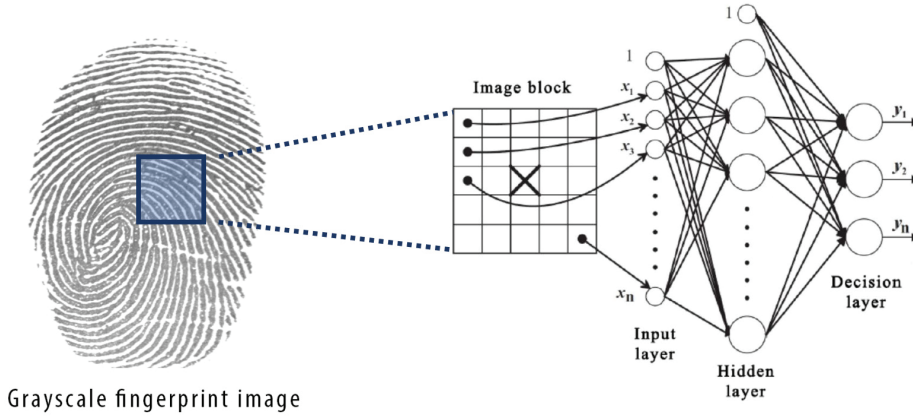
Grayscale fingerprint image

FIGURE 5. Process of passing pixels from the original fingerprint to input layer of neural network for classification.

algorithms. It is very fast and often outperforms its competitors in recognition rate as documented in [16]. This algorithm compares two fingerprint representations and produces a similarity score which varies in the range 0–999 (where 0 stands for no similarity and 999 is the highest possible similarity measured in our tests). The database of fingerprints, represented by their feature vectors, is searched and matched against the unknown fingerprint. Feature vector from the database with highest similarity score and exceeding the decision threshold is selected as the resulting identity of the unknown fingerprint.

4. Results and performance evaluation

4.1. Fingerprint databases used for evaluation

To simulate the maximum possible variability of fingerprint images, we collected a database of 5851 fingerprint images from multiple sources. This database consisted of images captured by Cross Match Verifier 300 sensor, Digital Persona U.are.U 4000 sensor, popular FVC evaluation databases from 2000, 2002, 2004 and a collection of special latent fingerprint samples from NIST Special Database 27a. All images have a resolution of 500 PPI and their dimensions are 504×480 pixels. The effort was to simulate real life conditions by testing our algorithm on a wide range of fingerprint patterns differing in quality, sensor type used to capture fingerprint, image contrast, many sources of degradation and noise. Fingerprints vary in gender of the fingerprint originator, age and geographic

location. NIST's special database ensures inclusion of fingerprints of low quality on digitized ten-print cards. Furthermore, FVC databases contain computer generated fingerprints using SFinGe method which is described in [3]. For better visualization, we illustrate the difference between fingerprint quality of various sources in Figure 6.

FIGURE 6. Samples of fingerprints from our evaluation database (from left to right: NIST Special Database 27a, CrossMatch Verifier 300 sensor, Digital Persona U.are.U 4000 sensor, FVC2004 optical scanner, FVC2004 thermal sweep scanner, SFinGE fingerprint.)

4.2. User interface

As we mentioned before, our fingerprint identification system can work in a fully automated manner where the user only selects the fingerprint and software automatically performs identification with no user input. For experimental and educational purposes, we implemented graphical user interface for experimenting with parameters, construction of user defined neural networks and customization of training on user selected training databases. Figure 7 on the page 128 shows the screens of graphical user interface of our software.

4.3. Neural network training

We used two instances of neural networks in our software. Both were trained using the improved version of resilient backpropagation algorithm described in [10] and implemented in FANN library. One for coarse fingerprint classification using Level-1 patterns. A training database for this network consisted of 5200 fingerprints. Testing database consisted of 651 images. These databases did not overlap. Level-1 classification success rate of 97 % was achieved on the testing database.

Another network was used for Level-2 feature classification. Here, the training database was much smaller than the one for Level-1 classification. Training database creation was a rather time consuming process since training samples had to be manually collected using our special software tool for manual Level-2 feature marking and extracting in the form of image blocks that were saved as separate files. For experimental evaluation, we manually collected 920 training samples (all ridge endings and terminations) and 70 testing samples. Level-2 classification achieved overall classification success rate of 98.64 %.
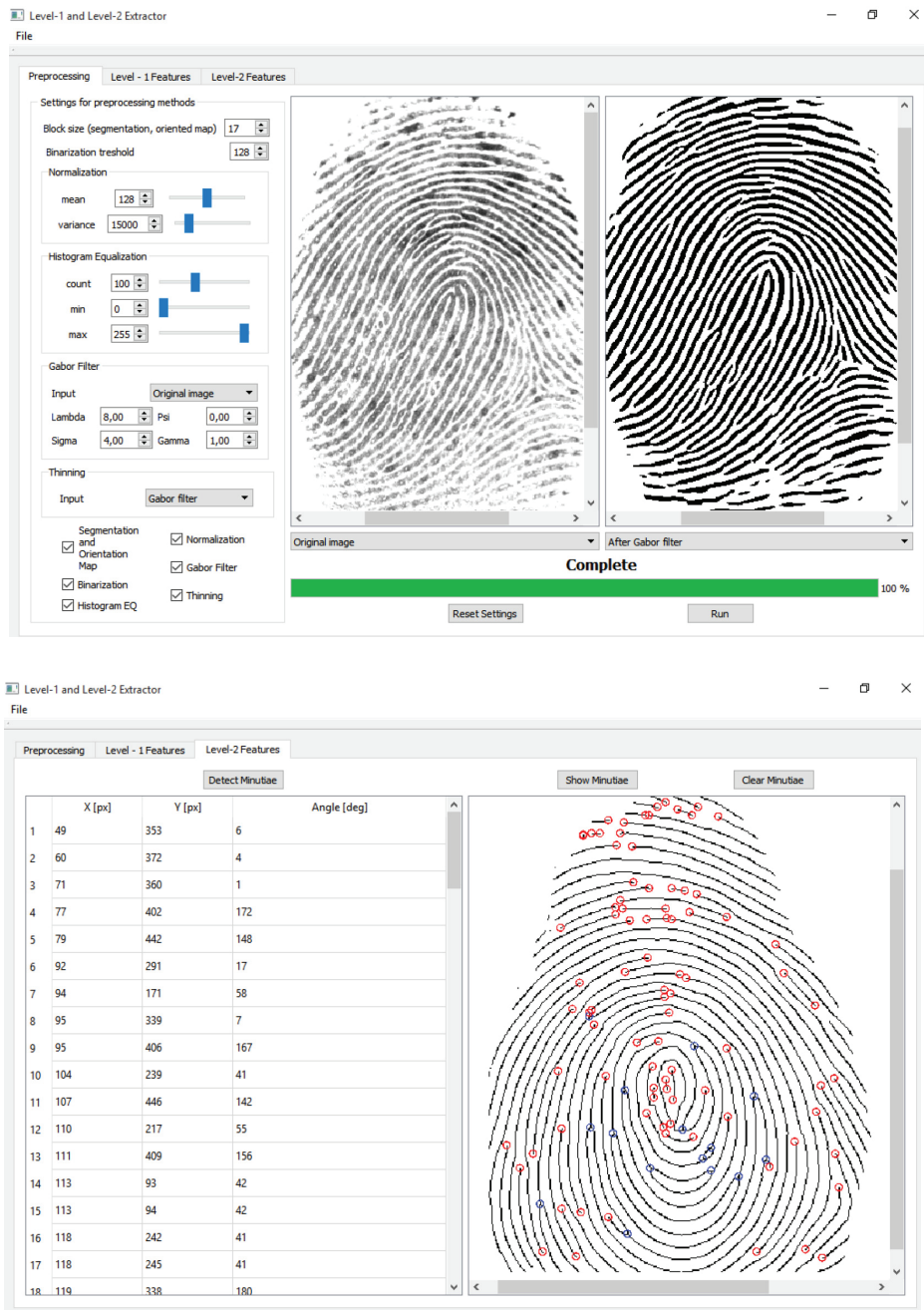
FIGURE 7. Screenshots of graphical user interface (top: image enhancement interface, bottom: visual inspection of extracted Level-2 features).

4.4. Performance indicators and testing

Source codes of our software developed in C/C++ using Qt 5.7.0 library can be found online at `http://fingerprint.re-search.info`. All instructions to set up, build and use the software are available at the mentioned website. Our solution was developed and tested under the OS Windows 10 64-bit.

Overall recognition rate was evaluated on two different databases: high quality database of fingerprints captured by CrossMatch Verifier 300 sensor (51 different fingers each represented by 8 fingerprint impressions captured in different conditions) and popular FVC2002 DB3A database (100 different fingers each represented by 8 fingerprint impressions) containing some challenging cases of fingerprints. Recognition rate was calculated as a percentage of successful recognitions out of all recognition attempts.

We carried out two different experiments to evaluate false match rate FMR and false non-match rate FNMR, respectively. Tests were run on both testing databases. To determine FMR, we performed all possible comparisons of impostor fingerprint pairs and calculated the number of all impostor pairs incorrectly classified as a genuine pair. We repeated this experiment for a number of decision threshold values from 0 to 999. Decision threshold value serves as a minimum similarity score computed by BOZORTH3 matcher that two fingerprints must exceed to be considered identical [21]. Similar experiment was carried out to calculate FNMR. We performed all possible comparisons of genuine fingerprint pairs and detected only those which were incorrectly classified as an impostor pair. When studying FMR/FNMR plots of biometric algorithm we often want to know what is the equal error rate EER. This is the decision threshold value where FMR and FNMR are equal [13]. During evaluation, we also examined EER values.

Another very important performance indicator commonly used in biometric system evaluation and benchmarks is a ROC curve. It is a plot of the genuine match rate (also known as true positive rate) against the false match rate (also known as false positive rate) for the different decision threshold values [13]. The closer the curve follows the left-hand border and then the top border of the ROC space, the more accurate the algorithm. We compared our fingerprint recognition system on FVC2002 DB3A database against 12 top-performing public algorithms in [16] in terms of ROC curves. In [16] readers may find references to papers where individual algorithms were published.

4.5. Results on cross match verifier 300 database

Recognition rate reached a value of 92 % of correctly identified subjects when using decision threshold corresponding to *EER* point. EER reached 8 %. FMR/FNMR graph in Figure 8 shows the behavior of individual error types at

different decision threshold values. As we can see, there is a rather good separation between two error curves, FMR reaches the highest values near 0 decision threshold while FNMR is spread on the entire plot space. ROC curve in Figure 8 confirms this acceptable performance as it is stretched to top-left corner of graph space.
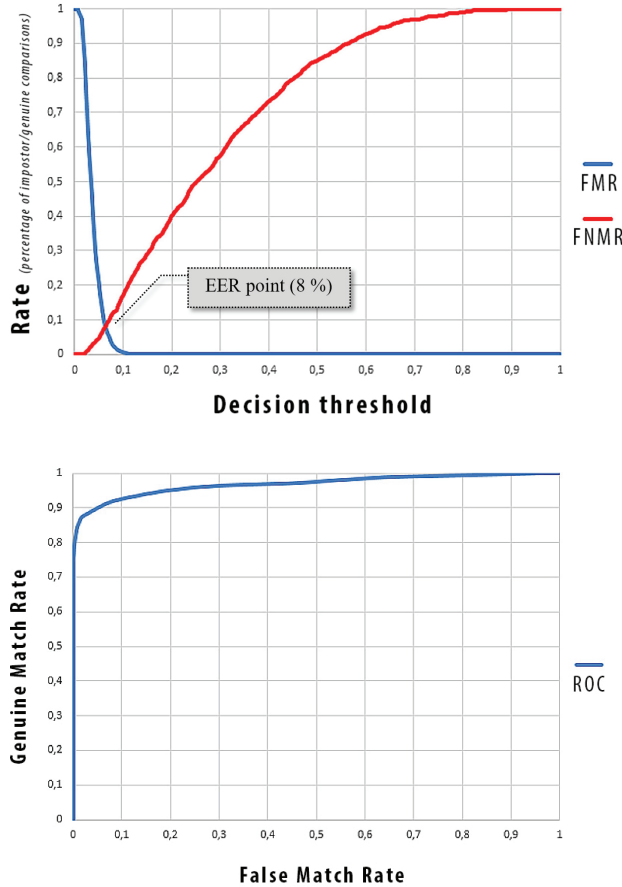

FIGURE 8. Performance results for Cross Match Verifier 300 database (top: FMR/FNMR plot, bottom: ROC curve).

4.6. Results on FVC2002 DB3A database

Recognition rate in this case reached a value of 67 % of correctly classified subjects when using decision threshold corresponding to EER point. We need to remind that quality of fingerprints in this database was much worse than

in Cross Match database. EER point was detected at 33 % indicating that separation between FMR and FNMR is not as ideal as on Cross Match database. Regarding ROC curve, our algorithm ranked acceptable position within competing algorithms from [16] as we can see in Figure 9.
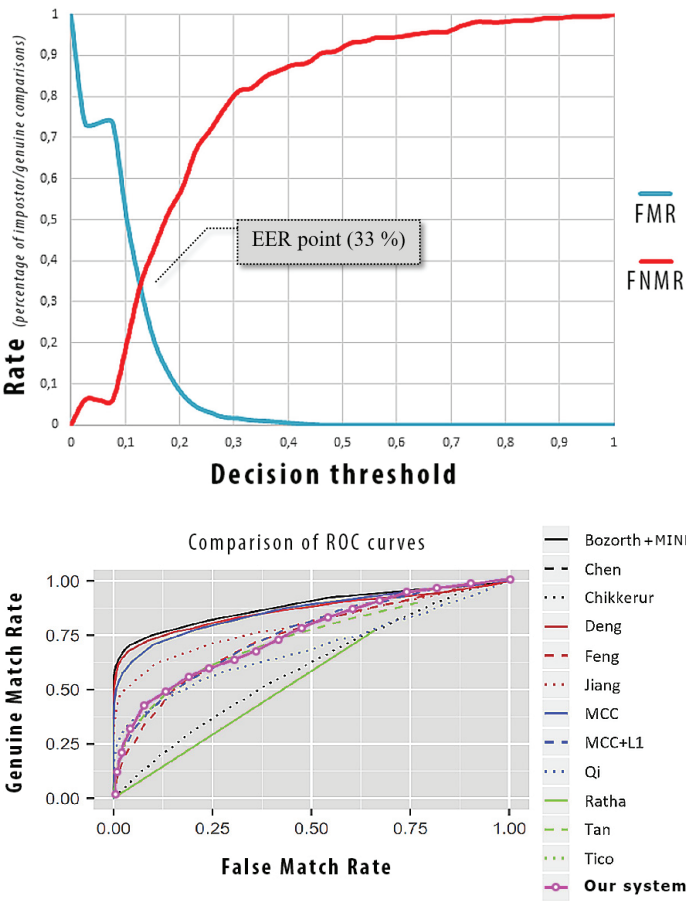

FIGURE 9. Performance results for FVC2002 DB3A (top: FMR/FNMR plot, bottom: comparison of ROC curves of different algorithms including our system).

It could not reach the performance of top algorithms like MCC [4] and algorithm proposed by D e n g et al. [6], but it outperformed many other algorithms using different approaches than neural networks. This is a promising observation since there is a great potential to improve recognition rate of our algorithm

by extending the training database of Level-2 features and incorporating more complex features to strengthen the discrimination power of fingerprints.

Another important finding was the significant reduction of time needed to perform identification of single fingerprint when using coarse classification of Level-1 features. With coarse classification module enabled, we achieved 60–70 % reduction of identification time per fingerprint compared to identification time with disabled coarse classification module. Average identification time per fingerprint with enabled coarse classification was 784 milliseconds (2511 milliseconds without coarse classification). All tests were carried out on a machine with Intel Core i7–4800MQ at 2.7 GHz and 16 GB RAM. Unfortunately, it was not possible to directly compare our time results with those in [16] since they used parallel computation framework on 12 powerful computers in a cluster.

5. Conclusion and future work

We proposed the automated fingerprint recognition system that works in identification mode and represents a complete biometric system capable of fingerprint sensing, image enhancement, feature extraction and matching. Two neural networks represent the core of our extraction engine. One for coarse classification and another for Level-2 feature extraction. Coarse classification played a crucial role in speeding up the computation per one fingerprint yielding 60–70 % identification time reduction. Level-2 feature extraction based on neural network also proved to be reliable since Level-2 extraction accuracy reached 98.64 % on the mixed high and low quality fingerprint database. However, its accuracy can be further improved by extending the training database. In addition, the network's architecture can be easily modified to support more complex Level-2 feature extraction. Overall recognition rate of 92 % correctly classified high-quality fingerprints and performance that keeps up with the best public algorithms on low quality images can be attributed to our extraction algorithm that classifies features in the original gray-scale fingerprint pattern rather than fingerprint skeleton that usually suffers from various image defects introduced by enhancement process. Full automation of fingerprint identification process that uses neural network for Level-2 feature extraction along with evaluation and comparison with the results from relevant literature can be viewed as a contribution to the field of biometric authentication.

Since fingerprint enhancement, neural network training and traversal of huge database of users may be computationally expensive we plan to extended our existing software solution by harnessing the computing power of GPU using publicly available libraries like ArrayFire and OpenCV to accelerate some of the

critical processes. Another part of our future research currently underway is effective computer implementation of 2 D curved Gabor filters that locally adapt their orientation and frequency properties to fit local fingerprint context and provide better enhancement results than traditional Gabor filters. In addition, we started with extending our training database of complex Level-2 patterns in order to improve recognition rate of incomplete and poor quality fingerprints where the amount of biometric information is rather limited. Recently, we have investigated contribution of Level-1 and Level-2 feature set fusion to create more robust representation of fingerprint combining its global and local characteristics. Our interest is also aimed at deep learning by means of convolutional neural networks that have proved their exceptional performance in multitude of biometric applications. One of the future prospects is to extend the proposed solution by incorporating NVIDIA's cuDNN library to design a convolutional neural network for extracting noisy patterns from latent fingerprints what is one of the top open research issues in modern fingerprint recognition, particularly in forensic and law enforcement applications.

REFERENCES

[1] BARTŮNĚK, J. S.: *Fingerprint Image Enhancement, Segmentation and Minutiae Detection*, Doctoral Dissertation, Blekinge Institute of Technology (2016), 168 p.

[2] BARTŮNĚK, J. S., J. S.—NILSSON, M.—NORDBERG, J.—CLAESSON, I.: *Neural network based minutiae extraction from skeletonized fingerprints*, in: TENCON 2006, IEEE Region 10 Conference (2006), 4 p.

[3] CAPPELLI, R.: SFinGe*: an approach to synthetic fingerprint generation*, in: International Workshop on Biometric Technologies (2004), Calgary, Canada, 147–154.

[4] CAPPELLI, R.—FERRARA, M.—MALTONI, D.: *Minutia cylinder-code: a new representation and matching technique for fingerprint recognition*, IEEE Transactions on Pattern Analysis Machine Intelligence **32**, (2010), no. 12, 2128–2141.

[5] CAPPELLI, R.—FERRARA, M.: *A fingerprint retrieval system based on level-1 and level-2 features*, Expert Systems with Applications **39** (2012), 10465–10478.

[6] DENG, H.—HUO, Q.: *Minutiae matching based fingerprint verification using delaunay triangulation and aligned-edge-guided triangle matching*, Proceedings of the 5th Int. Conference on Audio-and Video-Based Biometric Person Authentication (2005), 270–278.

[7] GOLABI, S.—SAADAT, S.—HELFROUSH, M. S.—TASHK, A.: *A novel thinning algorithm with fingerprint minutiae extraction capability*, International Journal of Computer Theory and Engineering **4** (2012), no. 4, 514–517.

[8] GOTTSCHLICH, C.: *Curved-region-based ridge frequency estimation and curved Gabor filters for fingerprint image enhancement*, IEEE Transactions on Image Processing **21** (2012), no. 4, 2220–2227.

[9] GUO, Z.—HALL, R.: *Parallel thinning with two sub-iteration algorithms*, Communications of the ACM **32** (1989) no. 3, 359–373.

[10] IGEL, CH.—HÜSKEN, M.: *Improving the* Rprop *learning algorithm*, in: The Second International Symposium on Neural Computation (NC 2000), ICSC Academic Press, 2000, pp. 115–121.

[11] KULKARNI, S.: *Fingerprint feature extraction and classification by learning the charac-teristics of fingerprint patterns*, Neural Network World (2011), **21** (2011), no. 3, 219–226.

[12] MAIO, D.—MALTONI, D.: *Direct gray-scale minutiae detection in fingerprints*, IEEE Transactions on Pattern Analysis and Machine Intelligence **19** (1997), no. 1, 27–40.

[13] MALTONI, D.—MAIO,D.—JAIN,A.K.—PRABHAKAR,S.: *Handbook of Fingerprint Recognition*, 2nd Edition, Springer-Verlag London (2009), 494 p.

[14] NISSEN, S.: *Implementation of a fast artificial neural network library* (FANN) , Depart-ment of Computer Science, University of Copenhagen (DIKU) (2003), 92 p.

[15] PANKANTI, S.—PRABHAKAR, S.—JAIN, A. K.: *On the individuality of fingerprints*, IEEE Transactions on Pattern Analysis and Machine Intelligence **24** (2002), no. 8, 1010–1025.

[16] PERALTA, D. ET AL.: *A survey on fingerprint minutiae-based local matching for veri-fication and identification: Taxonomy and experimental evaluation*, Information Sciences **315** (2015), 67–87.

[17] POKHRIYAL, A.—LEHRI, S.: MERIT*: Minutiae extraction using rotation invariant thinning*, Int. Journal of Engineering Science and Technology **2** (2010), 3225–3235.

[18] SHI, Z.—GOVINDARAJU, V.: *A chaincode based scheme for fingerprint feature extrac-tion*, Pattern Recognition Letters **27** (2006), 462–468.

[19] SHORT, N.—ABBOTT, L.—HSIAO, M.—FOX, E.: *Robust feature extraction in fin-gerprint images using ridge model tracking*, Center for Embedded Systems for Critical Applications, Bradley Department of Electrical and Computer Engineering (2014), 9 p.

[20] THAI, R.: *Fingerprint image enhancement and minutiae extraction*, The University of Western Australia (2003), 71 p.

[21] WATSON, C. I. ET AL.: *User's Guide to* NIST *Biometric Image Software* (NBIS), National Institute of Standards and Technology Gaithersburg, MD, 2004, 207 p.

[22] ZHAO, Q.—JAIN, A. K.: *On the utility of extended fingerprint features: A study on pores*, IEEE Comp. Soc. Confer. on Comp. Vision and Pattern Recognition (2010), 8 p.

[23] ZHI, V. T. D.—SUANDI, S. A.: *FingerCode for identity verification using fingerprint and smart card*, in: 10th Asian Control Conference (2015), 6 p.

Received December 1, 2016

Institute of Computer Science and Mathematics
Slovak University of Technology
Ilkovičova 3,
SK–812-19 Bratislava
SLOVAKIA

E-mail: pavol.marak@stuba.sk
         alexander.hambalik@stuba.sk