International Journal of Engineering Research and Advanced Technology (IJERAT)

E-ISSN : 2454-6135

DOI: 10.31695/IJERAT.2019.3402

Volume.5, Issue 3
March -2019

A Robust Fingerprint Recognition Technique Applying Minutiae Extractors and Neural Network

Aung Kyaw Oo[1] & Zaw Lin Aung[2]

[1] Information Technology Department, Technological University (Taunggyi), Shann State, Myanmar

[2] Computer Engineering and Information Technology Department, Yangon Technological University, Yangon, Myanmar

ABSTRACT

Fingerprint recognition is one of the interesting and mature biometric technique for personal identification or authentication application. The objective of the work is to retrieve personal data by using the fingerprint. In this paper, the fingerprint of a person is captured via Digital Persona U.are.U 4500 fingerprint scanner. The input fingerprint is firstly enhanced using contrast stretching and two morphological operations (dilation and erosion). Next, 160x160 size of the center region of the fingerprint is cropped and extracted minutiae such as ridges and bifurcations. These minutiae are used as the features of a particular fingerprint. These features are put into the Neural Network for person recognition. Various experiments will confirm and prove the accuracy and performance of the proposed fingerprint recognition system.

Key Words: *Fingerprint Recognition, Minutiae Extractor, Neural Network, Morphological Thinning.*

1. INTRODUCTION

Recognition of persons by means of biometric characteristics is an emerging phenomenon in modern society. It has received more and more attention during the last period due to the need for security in a wide range of applications. Among the many biometric features, the fingerprint is considered one of the most practical ones.

A fingerprint is the feature pattern of one finger. Each person has his own fingerprints with the permanent uniqueness. It is experienced from the research that all have their different finger prints and these finger prints are permanent for whole life. Fingerprint (FP) has the impressions of the minute ridge (called as dermal) of the finger. FP ridges and valleys are unique and unalterable. Hence, fingerprint biometric is used in numerous applications that include civilian and commercial applications like military, law enforcement, medicine, education, civil service, forensics, driver license registration, cellular phone access, computer log-in and so on.

Today live fingerprint readers based on optical, thermal, silicon, ultrasonic approach are used instead of old method of ink to capture fingerprint. Fingerprint recognition is based on minutiae or location and direction of the ridge endings and bifurcations (splits) along a ridge path. The two commonly used FP matching techniques are minutiae-based matching and pattern matching. Pattern matching just compares two image for checking similarity. Minutiae matching relies on minutiae points i.e. location and direction of each point.

There are many previous works in fingerprint recognition and identification. The recent developments in fingerprint recognition of a person lead to improvements in reliability and accuracy. The related work for Fingerprint Recognition (FR) technologies analysed with different parameters such as matching techniques, recognition methods, and security, are summarized as follow.

With respect to the matching techniques and recognition method, Zhifan Gao et.al. [1] Introduce a method for Fingerprint Recognition (FR) using neighbour local graphical structure to match the point in a pattern and global matching to overcome the problem of noisy data. Equal Error Rate (EER) of 3.5% to 5.6% is obtained on FVC2002 database. After that, Zin Mar Win et al. [2] use a correlation based FR system. The scheme uses Gabor filters for FP feature extraction. The test results of low False Acceptance Rate (FAR), False Rejection Rate (FRR) and 97% accuracy are reported. Next, Zhu Le-Qing [3] proposes a knuckle print recognition scheme based on Speeded-Up Robust Features (SURF) algorithm. The test results on PolyU database show accuracy of 96.91% and average matching time 0.106 for identification. Jucheng Yang et al. [4] propose a secured approach for FR based on set of assembled geometric moment and Zernike moment. The results on FVC2002 database show EER=2.27%, average enroll time=1.77s and average match time=0.19s. Fernando Cornelio Jimenez Gonzalez et al. [5] explain a method to overcome the problem of controlled pressure and humidity for image acquiring. The proposed method uses negative Laplace filter and non-stationary analysis of short time Fourier transform and algorithm to find match percentage in the verification process. The test results in varying conditions show the FRR=1.34%-4.88%, FA (False Acceptance) = 0%-1%, RR = 95.12% - 98.2%. Chomtip Pornpanomchai et al. [6] propose the FR by Euclidean distance method. The test results show a precision of 95% for the ST-BIO Card Reader Model: BCR100T V3.0, and 85% for the VeriFinger Sample DB database. The average access time reported is 19.68 seconds per image. A. C. Ramachandra et al. [7] designs a scheme for FR using Inter Ridge Variation (FRIRV) algorithm. The experimental results on FVC2002 show the improvement in RR by 80-100%. Liu Cuilin et al. [8] forwards a method using dynamic password and FR for high-security e-mail system. The method ensures improved safety for e-mails with lower efficiency. Kaisheng Zhang et al. [9] propose an Automatic FR System (AFRS). The technique utilizes embedded hardware, open source LINUX operating system and related tools. Wenzhou Liu et al. [10] brings to notice a novel idea in which the fingerprint is stored into IC cart of the ID card via microcomputer system. It is then matched with the information of the holder whenever required. The scheme ensures reliable performance, easy to use and higher security. Haiyun Xu et al. [11] depict a method for increasing matching speed by compressing spectral minutiae feature using Column PCA (Principal Component Analysis) and Line DFT (Line Discrete Fourier Transform) reduction techniques. The reduction rate of 94% and a speed of 125000 comparisons per second is reported and the experimental results on MCYT database show EER=0.29%, FAR=99.8% and on FVC2002-DB2 database show EER=3.72%, FAR=95.6%. T. Amornraksa and S. Tachaphetpi boon [12] formulate a method for FR based on the DCT features of a discrete image. The test results using k-nearest neighbour (k-NN) classifier show 100% RR and the low computational effort. Jinwei Gu et al. [13] recommend a novel representation for FPs that includes both minutiae and model-based orientation field. The test results prove the proposed system is more accurate and robust and takes less than 0.30s for matching. Naveena Marupudi et al. [14] depict multimodal biometrics using voice and FP. The novel method uses segmentation using morphological operations and minutiae marking using triple branch counting. The test results on FVC2002 and SDK 4.2 show 25% of FAR and FRR.

Related with security, Rajeswari Mukesh et al. [15] identify visual threshold cryptographic method to keep compressed FP template information securely at the server to avoid hacking. Lossy compression technique DCT is used for compressing. The results prove FAR and FRR of 0.2% and better efficiency, reduces falsification and maintenance cost. Ruyi Zheng et al. [16] appraise the problem of fast FP retrieval in a large database using clustering-based descriptors. The experimental results on NIST database using SVN classifiers and orientation image report the accuracy of 86.68% and fastest matching time 0.056s. Emile J. C. Kelkboom et al. [17] analyse the cross matching performance of the auxiliary data AD of the Fuzzy Commitment Scheme (FCS). The result on MCYT database show that cross matching performance is not as good as system performance. Lifeng Lai et al. [18] determine the performance of reusable biometric security systems, in which the same biometric information is reused in multiple locations is analysed. Lifeng Lai et al. [19] evaluate the single-use biometric system under a privacy security trade off frame work. The test results report adequate security. Francis Minhthang Bui et al. [20] explore various strategies related to key binding with QIM in a BE context are examined. The obtained results demonstrate that the QIM method facilitates tuning of the system performance. Maneesh Upmanyu et al. [21] formulate a provably secure and blind biometric authentication protocol, which addresses the concerns of user's privacy, template protection and trust issues. Experimental results on four biometric datasets (face, iris, hand geometry, and FP) show that the authentication in the encrypted domain does not affect the accuracy. Tanya Ignatenko et al. [22] address the privacy leakage in biometric secrecy systems. Biometric part assures the authenticity of a user, while the cryptographic part provides strong secrecy and avoids privacy leakage. Chun-I. Fan and Yi-Hui Lin [23] construct a three-factor authentication scheme which combines biometrics with passwords and smart cards to provide high-security. Bon K. Sy [24] illustrates a practical secure data retrieval and authentication techniques for complex distributed systems. The test result report ERR=8%, FAR=13.7% and FRR=3.8%.

The above all are some recent works on finger prints recognition and identification. The proposed method is one of the fingerprint recognition using minutiae features of fingerprint. This paper is composed of five section. In section I, introduction of fingerprint recognition and some previous works is presented. Section II is the theories background of the proposed method. In section III, proposed method will be discussed in detail. Accuracy measurement and performance estimation will be presented as section IV and final section V is about of the conclusion of this proposed method.

2. THEORIES BACKGROUND

In this section, the minutia of a fingerprint, thinning technique and overview of neural network are discussed as the theories background.

DOI : 10.31695/IJERAT.2019.3402

2.1 Minutia of a fingerprint

A fingerprint is the composition of many ridges and furrows. Finger prints can't distinguished by their ridges and furrows. It can be distinguished by Minutia, which are some abnormal points on the ridges. Minutia is divided in to two parts such as: termination and bifurcation. Termination is also called ending and bifurcation is also called branch.

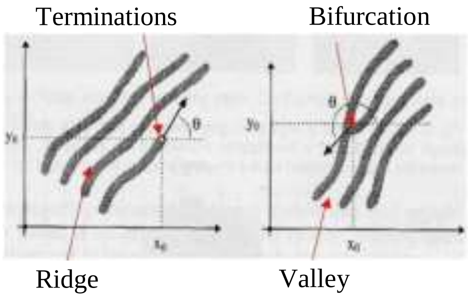


Figure 2.1: Diagram of Minutia [25]

Furthermore, the fingerprint pattern contains one or more regions where the ridge lines create special shapes. These regions may be classified into three classes: loop, delta, and whorl.

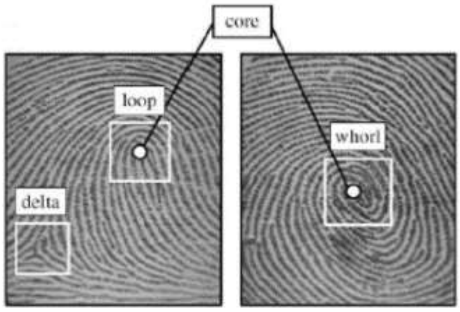


Figure 2.2: Special regions (white boxes) and core points (small circles) in fingerprint images [25]

In more details, there are many features in classification of fingerprint based on minutia. These feature types are distinguished from basic shapes to very complex and rare patterns and they are mainly characterized by the spatial location in the image, heir orientation and their shape type. The following are some of possible minutia features which are usually appeared in a fingerprint.

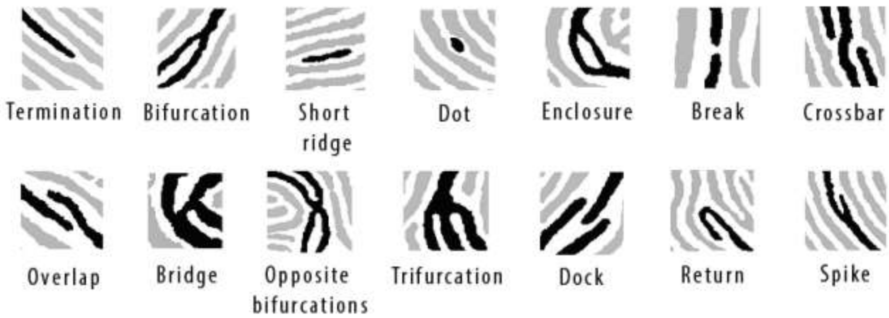


Figure 2.3: Description of some possible minutia feature in fingerprint classification [25]

Individuality of fingerprints based on these features as well as probability of correspondence of random fingerprints. Hence, these features are usually used by every fingerprint recognition systems.

2.2 Morphological Thinning

Thinning is a morphological operation that is used to remove selected foreground pixels from binary images, somewhat like erosion or opening. It can be used for several applications, but is particularly useful for skeletonization. The thinning operation is related to the hit-and-miss transform and can be expressed quite simply in terms of it. The thinning of an image I by a structuring element J can be shown as

- - - - - - - - - (1)

DOI : 10.31695/IJERAT.2019.3402

Thin(i,j) = I – hit-and-miss (i,j)

Where, the subtraction is a logical subtraction defined by $X - Y = X \cap \bar{Y}$.

In everyday terms, the thinning operation is calculated by translating the origin of the structuring element to each possible pixel position in the image, and at each such position comparing it with the underlying image pixels. If the foreground and background pixels in the structuring element exactly match foreground and background pixels in the image, then the image pixel underneath the origin of the structuring element is set to background (zero). Otherwise it is left unchanged. Note that the structuring element must always have a one or a blank at its origin if it is to have any effect. The choice of structuring element determines under what situations a foreground pixel will be set to background, and hence it determines the application for the thinning operation.

Original Image Thinning Output

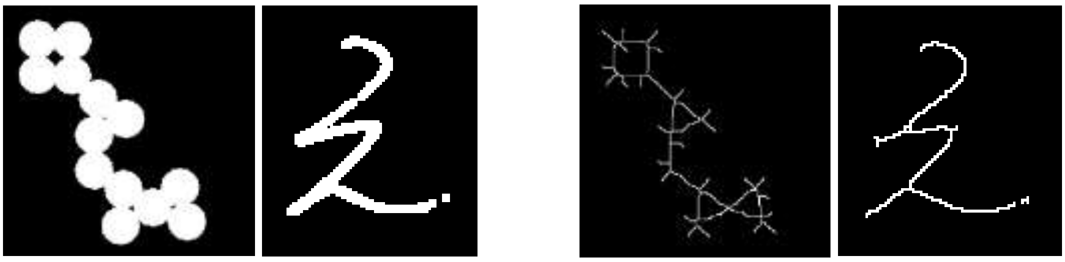
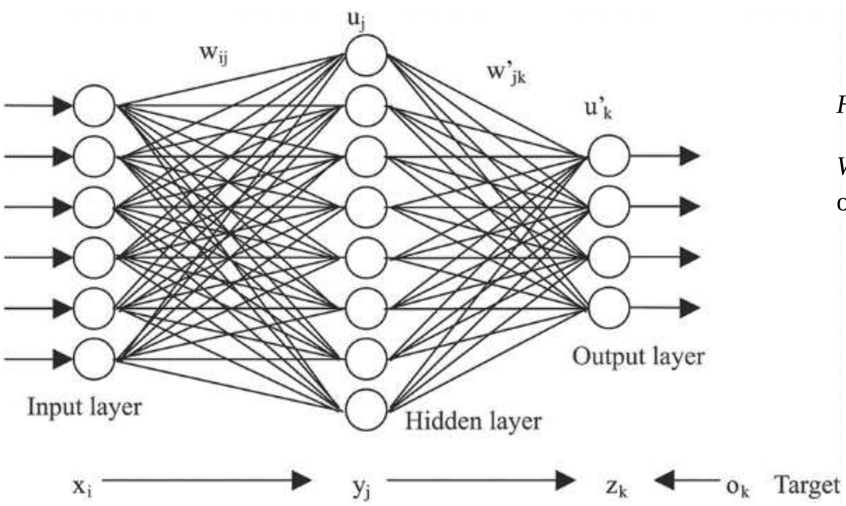


Figure 2.4: Output Image of Morphological Thinning process [26]

2.3 Overview of Neural Network

A neural network is a computational structure inspired by the study of biological neural processing. There are many different types of neural networks, from relatively simple to very complex, just as there are many theories on how biological neural processing works. A layered feed-forward neural network has layers, or subgroups of processing elements. A layer of processing elements makes independent computations on data that it receives and passes the results to another layer. The next layer may in turn make its independent computations and pass on the results to yet another layer. Finally, a subgroup of one or more processing elements determines the output from the network. Each processing element makes its computation based upon a weighted sum of its inputs.

The first layer is the input layer and the last the output layer. The layers that are placed between the first and the last layers are the hidden layers. The processing elements are seen as units that are similar to the neurons in a human brain, and hence, they are referred to as cells, neurotises, or artificial neurons. A threshold function is sometimes used to qualify the output of a neuron in the output layer. Synapses between neurons are referred to as connections, which are represented by edges of a directed graph in which the nodes are the artificial neurons. Nets consist of small units called cells, and these are connected to each other in such a way that they can pass signals to each other.



Here,

W_{ij} and w'_{jk} are weights of input and output layers at the position of *i,j* and *j,k*.

Figure 2.5: General architecture of a three layers feed forward neural network

DOI : 10.31695/IJERAT.2019.3402

3. PROPOSED METHOD

The proposed method is back propagation based fingerprint recognition using minutia. The proposed method can be seen into three main sections, image acquisition and pre-processing, minute features extraction and recognition. The system flow diagram of the proposed method can be presented as following figure 3.1.

3.1 Image Acquisition

In this proposed system, fingerprint is captured by U.are.U 4500 USB fingerprint reader. The captured image size is 357x392 with bitmap image format. The captured images are real time input using this reader and saved in the target folder for later processes.

3.2 Pre-Processing

This stage is very important for this proposed method because the input fingerprint image from USB reader is not perfectly good and cannot directly use for later processes. Some lines of fingerprint image are not clear and fade. Hence, the input finger print image is necessary to enhance image quality using many image enhancement processes. In this method, median filtering, contrast stretching, image normalization, image binarazation and some morphological processes are used to enhance the input fingerprint images.

In the input fingerprint, some lines are so fade and not connected. They appears as short lines and dots. They are not usable and can confuse with original main lines and dots. Hence, to remove these unnecessary features, median filter with 7x7 kernel is used.

To enhance the contrast and edges of fingerprint image, image contrast stretching is applied. Contrast stretching not only can improve the contrast and edges of an image but also can balance image brightness.

Even if the input image has enhanced using above processes, the fingerprint may be still unclear as the noise and some problems during scanning process. Hence, the fingerprint image is necessary to normalized to be more clear ridges and valleys. The image normalization can decrease the dynamic range of the gray scale between ridges and valleys of a fingerprint image. In this proposed method, image normalization is implemented by the following formula.

$$G(i,j) = \begin{cases} \mu_0 + \sqrt{\dfrac{VAR_0\,(I(i,j)-\mu)^2}{VAR}} & If\ I(i,j) > \mu \\ \mu_0 - \sqrt{\dfrac{VAR_0\,(I(i,j)-\mu)^2}{VAR}} & Otherwise \end{cases} \tag{2}$$

Where, *G(i,j)* and *I(i,j)* are the normalized gray-level value and original gray scale value at pixel *(i, j)*. μ_0 and μ are desired mean and global mean of input image. VAR_0 *and* VAR desired variance and global variance of input image.

To enhance and be clearer in ridges and valleys, two morphological processes, dilation and erosion with square strel object are applied. After these processes, enhanced fingerprint image with clear ridges and valleys is achieved. In this proposed system, the whole fingerprint image is not used. Centred region of an image with size of 160x160 is defined as Region of Interest (ROI). This region is cropped and put to feature extraction process.

DOI : 10.31695/IJERAT.2019.3402

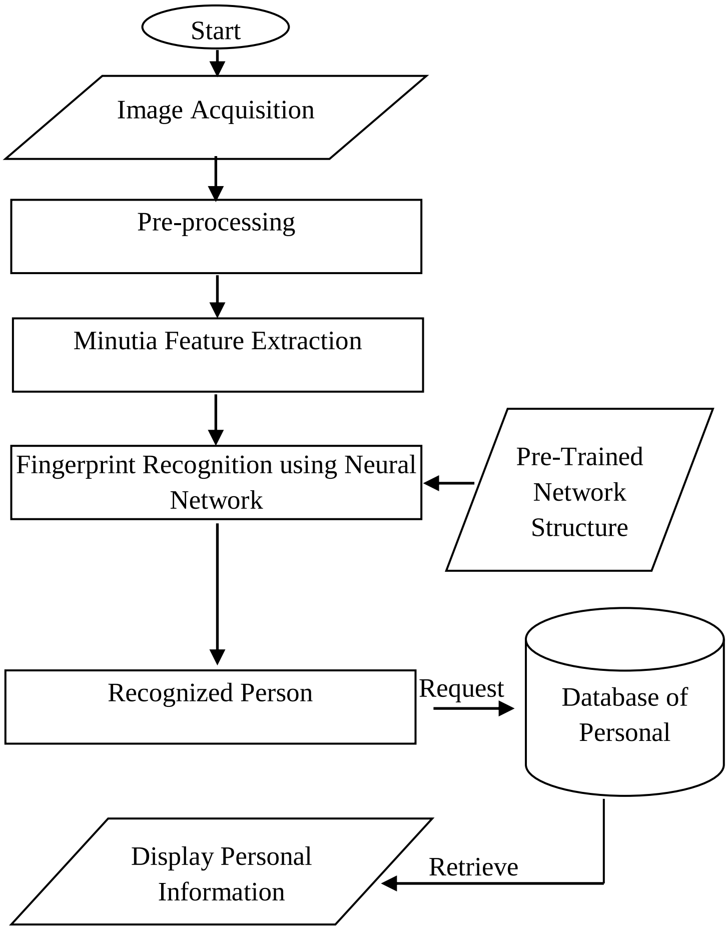


Figure 3.1: System flow diagram of proposed fingerprint recognition

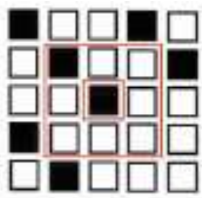
3.3 Minute Features Extraction

From each fingerprint image, four minute features, terminations, bifurcation, short lines and dots are extracted. In extracting terminations, the terminations lie at the outer boundaries are not considered as minutiae points, and Crossing Number is used to locate the minutiae points in fingerprint image. Crossing Number is defined as half of the sum of differences between intensity values of two adjacent pixels. If crossing Number is 1, 2 and 3 or greater than 3 then minutiae points are classified as Termination. Otherwise, they are normal ridges or Bifurcation respectively. These extraction can be seen as the following figure 3.2.

Short lines and dots are very clears and easily extracted. Short lines are connected components but its connected pixel is less than termination. Lines can be retrieved using regional properties and length of short line is defined by less than 50 pixels. Dots are only one or four groups of pixels within a kernel.

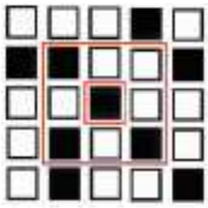
By this ways, these minute features can extract from a particular fingerprint image. These four features are put to the neural network to recognize a desired person.

Crossing Number =2.
Normal ridge pixel.



Crossing Number =1.
Termination point

DOI : 10.31695/IJERAT.2019.3402



Crossing Number =3.
Bifurcation point

Figure 3.2: Crossing Number and Type of Minutiae

3.4 Person Recognition using Neural Network

To recognize a person, back propagation neural network is used in the proposed system.Three layer neural net architecture is applied. For each fingerprint image, four minutiae features are extracted so there are four input neurons in the input layer. Hidden layer is implemented with 120 neurons and output layers is designed with 50 neurons which represent the numbers of person to be recognized.

In this neural net recognition section, there are two main sub-sections, training section and testing section. In the training time, 4x800 training data is put into the neural network. This training data is for 20 persons. For each person, 40 finger print image is used. Hence, total 800 fingerprint images are applied to train the neural net. For each image, there are 4 minutiae features are used. Hence, the training data set is size of 4x800. After training, output net with optimized weights is save to use in testing process.

In the testing process, 10 images for each person is tested. If the output of neuron over 0.95 or 1, the person 1 is recognized. Similarly, other person recognition is depended on the output result of a particular output neuron. The result of output neuron give the unique number of person which is the primary key for the personal database. Hence, this number is sent to the database to retrieve personal information.

3.5 Personal Data Retrieval and Expression

Personal information of recognized person is saved as a database. In this database, person number is used as primary key which is the output number of neural network. When neural network give the personal number to the database, personal information is searched and retrieved using SQL and displayed with table.

By this way, the proposed method can recognize a desired person and can also present with personal information. The accuracy and performance of the proposed system can be seen in next experimental result section.

4. EXPERIMENTAL RESULTS & DISCUSSIONS

This section is related to the measurement of accuracy and performance of the proposed fingerprint recognition system. Related experiments and results can be discussed as follow.

4.1 Experimental Setting

In this experiments, 10 testing image is applied for each person so one person is tested by ten time. In all experiments, 200 testing of 20 persons are used to measure the performance and accuracy of the proposed method. The following are some simple testing images and fingerprint scanner.

DOI : 10.31695/IJERAT.2019.3402

Figure 4.1: USB Fingerprint Reader and some testing fingerprint images

4.2 Accuracy Measurement

To measure the accuracy of proposed method, the following accuracy estimation is used.

$$Accuracy\ (\%) = \frac{no;of\ recognized\ images}{no;of\ total\ testing\ images}\ x\ 100 \qquad (3)$$

4.3 Experiments

As the above expressions, there are 200 testing images and 10 images are tested for each person. The following figures are some of the testing results of the proposed system.

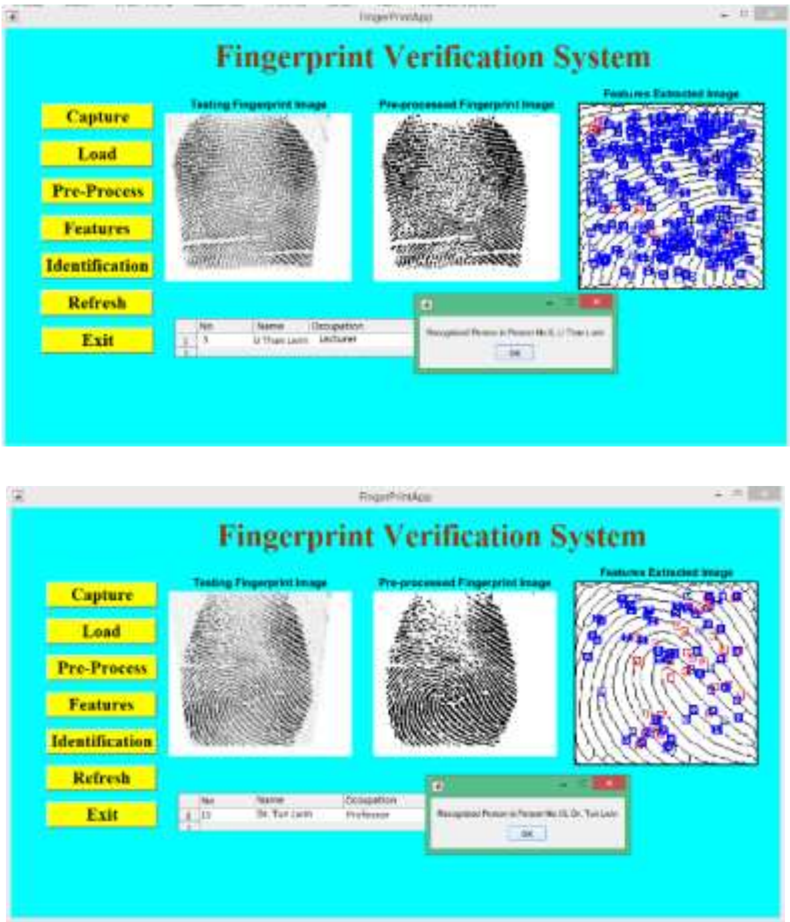


Figure 4.2: USB Fingerprint Reader and some testing fingerprint images

In these experiments, a few images cannot recognized because of some problem during scanning process. However, almost of testing images are recognized. The following table can show the accuracy of proposed method.

DOI : 10.31695/IJERAT.2019.3402

Table 4.1. Accuracy of Proposed Method Depending on Different Testing Images

No.	Person	Total Testing images	Recognized Images	Accuracy (%)
1	Person 1	10	10	100%
2	Person 2	10	10	100%
3	Person 3	10	9	90%
4	Person 4	10	10	100%
5	Person 5	10	10	100%
6	Person 6	10	8	80%
7	Person 7	10	10	100%
8	Person 8	10	10	100%
9	Person 9	10	10	100%
10	Person 10	10	10	100%
11	Person 11	10	10	100%
12	Person 12	10	10	100%
13	Person 13	10	9	90%
14	Person 14	10	10	100%
15	Person 15	10	10	100%
16	Person 16	10	10	100%
17	Person 17	10	10	100%
18	Person 18	10	7	70%
19	Person 19	10	10	100%
20	Person 20	10	10	100%
	Overall accuracy			96.5%

5. CONCLUSION

The proposed neural network based fingerprint recognition system has been presented. According to the experimental results, the proposed system achieved 96.5% of overall accuracy. Hence, the proposed system can give satisfied accuracy for every testing. In this system, as the some input image problem such as noise, wrong position of input fingers and so on, there is a few miss recognition. To fix these problem, better pre-processing processes should be applied. The fingerprint recognition and identification is very portable, applicable and more interesting of biometric authentication. Hence, in the future, our research will continue the biometric authentication research area including fingerprint in trying to achieve better results and more precise accuracy.

REFERENCES

1. Z. F. Gao, X. G. You, L. Zhou, and W. Zeng, "A novel matching technique for fingerprint recognition by graphical structures", in Proc. the Wavelet Analysis and Pattern Recognition, Guilin, IEEE, July 10-13, 2011.
2. Z. M. Win and M. M. Sein, "Fingerprint recognition system for lowquality images", presented at the SICE Annual Conference, Waseda University, Tokyo, Japan, Sep. 13-18, 2011.
3. L. Q. Zhu, "Finger knuckle print recognition based on SURF algorithm", in Proc. Eighth International Conference on Fuzzy Systems and Knowledge Discovery, IEEE, 2011.
4. J. C. Yang, N. X. Xiong, A. V. Vasilakos and Zh. J. Fang, "A fingerprint recognition scheme based on assembling invariant moments for cloud computing communications", IEEE Systems Journal, Vol. 5, no.4, Dec. 2011.
5. F. C. J. Gonz´alez, O. O. V. Villegas, and V. Gudalupe, "Fingerprint recognition using open algorithms in frequency and spatial domain, electronics", in Proc. Robotics and Automotive Mechanics Conference, IEEE, 2010, pp. 469-474.
6. C. Pornpanomchai and A. Phaisitkulwiwat, "Fingerprint recognition by euclidean distance", presented at Second International Conference on Computer and Network Technology, IEEE, 2010.
7. A. C. Ramachandra, K. B. Raja, K. R. Venugopal, and L. M. Patnaik , "Fingerprint recognition using inter ridge variation", presented at Third International Conference on Emerging Trends in Engineering and Technology, IEEE, 2010
8. C. L. Liu, Y. J. Shen, G. D. Zhang, and F. Wen, "E-mail system based on dynamic password and fingerprint recognition", in Proc. Management and Service Science, IEEE, 2010, pp. 1-4.
9. K. S. Zhang, J. She, M. X. Gao, and W. B. Ma, "Study on the embedded fingerprint image recognition system", in Proc. Conference of Information Science and Management Engineering, IEEE, 2010, pp. 169-172.

DOI : 10.31695/IJERAT.2019.3402

10. W. Z. Liu, Ch. Q. Cai, and Z. Zhang, "Fingerprint ID cards and the recognition system", in Proc. the 5th International Conference on Computer Science & Education, Hefei, China, IEEE, Aug. 24–27, 2010, pp. 1219-1221.
11. H. Y. Xu, R. N. J. Veldhuis, T. A. M. Kevenaar, and T. A. H. M. Akkermans, "A fast minutiae-based fingerprint recognition system", IEEE Systems Journal, vol. 3, no. 4, Dec. 2009.
12. T. Amornraksa and S. Tachaphetpiboon, "Finger print recognition using DCT features", Electronics Letters 27th, vol. 42, no. 9, April 2006.
13. J. W. Gu, J. Zhou, and Ch. Y. Yang, "Finger print recognition by combining global structure and local cues", IEEE Transactions on Image Processing, vol. 15, no. 7, pp. 1952-1964, July 2006.
14. N. Marupudi, E. John, and F. Hudson, "Fingerprint verification in multimodal biometrics", in Proc. Region 5 Conference, IEEE, 2006, pp. 130-136.
15. R. Mukesh and V. J. Subashini, "Fingerprint based authentication system using threshold visual cryptographic technique", in Proc. IEEE-International Conference on Advances in Engineering, Science and Management, Mar 30-31, 2012, pp. 16-19.
16. R. Y. Zheng, C. Zhang, S. H. He, and P. W. Hao, "A novel composite framework for large-scale fingerprint database indexing and fast retrieval", in Proc. Hand-Based Biometrics, IEEE, 2011, pp. 1-6.
17. E. J. C. Kelkboom, J. Breebaart, T. A. M. Kevenaar, I. Buhan, and R. N. J. Veldhuis, "Preventing the decodability attack based cross-matching in a fuzzy commitment scheme", IEEE Transactions on Information Forensics and Security, vol. 6, no. 1, IEEE, March 2011.
18. L. F. Lai, S. W. Ho, and H. V. Poor, "Privacy–security trade-offs in biometric security systems—part II: multiple use case", IEEE Transactions on Information Forensics and Security, vol. 6, no. 1, March 2011.
19. L. F. Lai, S. W. Ho, and H. V. Poor, "Privacy–security trade-offs in biometric security systems—part I: single use case", IEEE Transactions on Information Forensics and Security, IEEE, vol. 6, no. 1, March 2011.
20. F. M. Bui, K. Martin, H. P. Lu, K. N. Plataniotis, and D. Hatzinakos, "Fuzzy key binding strategies based on quantization index modulation(QIM) for biometric encryption (BE) applications", IEEE Transactions on Information Forensics and Security, vol. 5, no. 1, IEEE, March 2010.
21. M. Upmanyu, A. M. Namboodiri, K. Srinathan, and C. V. Jawahar, "Blind Authentication: A secure crypto-biometric verification Protocol", IEEE Transactions on Information Forensics and Security, vol. 5, no. 2, June 2010.
22. T. Ignatenko and F. M. J. Willems, "Biometric systems: privacy and secrecy aspects", IEEE Transactions on Information Forensics and Security, IEEE, vol. 4, no. 4, December 2009.
23. C. I. Fan and Y. H. Lin, "Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics", IEEE Transactions on Information Forensics and Security, IEEE, vol. 4, no. 4, December 2009.
24. B. K. Sy, "Secure computation for biometric data security—application to speaker verification", IEEE Systems Journal, IEEE, vol. 3, no. 4, December 2009.
25. L. H. Thai and H. N. Tam, "Fingerprint recognition using standardized fingerprint model", International Journal of Computer Science Issues, Vol. 7, Issue 3, No 7, pp. 11-16, May 2010.
26. https://homepages.inf.ed.ac.uk/rbf/HIPR2/thin.htm

DOI : 10.31695/IJERAT.2019.3402