International Journal of Computer Engineering and Information Technology

VOL. 8, NO. 4, April 2016, 56–62
Available online at: www.ijceit.org
E-ISSN 2412-8856 (Online)

Mixed Noise Tolerant Fingerprint Authentication Using Neuro Computing

Fremina James[1], Prasanna V Kumar[2] and Manoj Kumar Singh[3]

[1] Asst.Prof. , Dept. Of ISE , Brindavan College of Engineering, Bangalore, Karnataka, India.

[2] Prof., Dept.of IT, R.V.College of Engineering, Bangalore, Karnataka, India.

[3] Director, Manuro Tech Research Pvt.Ltd., Bangalore, Karnataka, India.

[1]freminajames@gmail.com, [2]prasannakumar@rvce.edu.in, [3]mksingh@manuroresearch.com

ABSTRACT

In this paper, we have proposed a secure means for fingerprint biometric authentication, which has the capability to deliver the user's privacy, their fingerprint template protection, and robustness against the various variations in terms of noise. In this paper, principle based on correlation strength has been presented to defined fingerprint recognition requirement,to achieve the desired objectives and high quality of solution, computational intelligence basedconcept which uses the feed forward architecture of artificial neural network is applied as solution technology. Proposed methods provides numerous advantages like less memory requirement, very high level of security for stored information without any extra means, high speed and simple implementation approach. Proposed method has robustness against various types of noise available with fingerprint image.

Keywords: *Biometrics, Authentcation, Fingerprint, Artificial Neural Networks, Noise.*

1. INTRODUCTION

Reliable authorization and authentication are becoming necessary for many everyday actions(or applications),be it boarding an aircraft, performing a financial transaction, or picking up a child from daycare. Authorization is almost always vested in a single individual or in a small group of individuals. Identity verification becomes a challenging task when it has to be automated with high accuracy and hence with low probability of break-ins and reliable non-repudiation. The user should not deny having carried out the transaction and should be inconvenienced as little as possible, which only makes the task more difficult. Biometric identification or biometrics refers to identifying an individual based on his or her distinguishing characteristics. Moreprecisely, biometrics is the science of identifying, or verifying the identity of a person based on Physiological or behavioral characteristics.Physiological biometrics, like fingerprintor hand geometry are physical characteristics generally measured at some point in time. Behavioral biometrics like signature or voice on the other hand consist of the way some action is carried out and extend over time.Behavioral biometrics are learned or acquired over time and are time dependent on one's state of mind or even subject to deliberate alteration.Loosly speaking, physiological biometrics are rich enough that a onetime sample may suffice for comparing biometric identifiers. For behavioral biometrics, any given sample gives no information about a person's identity, but it is the temporal variation of signal that contains the information. It is being accepted by government and industry to an extent that automated biometricauthentication will become a necessary fact of life. Just as other methods of computerized authentication biometric authentication will become more widespread. But the publicity surrounding biometrics has been misinterpreted in various ways to make it appear that there are no remaining challenges in automatically identifying people.Consequently, biometrics is not just surrounded by much expectation, but also by myths and misunderstandings. This is a heavy burden for an emerging technology to bear, and there is a risk that biometric usage could die a premature death because of its failure to live up to the great expectations created by its strongest proponents.

Person authentication is not a new problem of course,and society has adopted ways to verify the identity of a person,i.e. to authenticate the person. There are three traditional modes of authentication: Possessions,

Knowledge, and Biometrics.In biometrics we distinguish two authentication methods:

(i)Verification is based on a unique identifier which single out a particular person (e.g. some ID number) and that person's biometrics,and thus is based on a combination of authentication modes.

(ii)Identification, on the other hand, is based only on biometric measurements.it compares these measurements to the entire database of enrolled individuals instead of just a single record selected by some identifier.

Biometric identification can be viewed as "pure" biometric authentication and is much harder to design and implement because of the biometric database search capabilities that are needed. Broadly there are five attributes that are necessary to make a biometric practical; Universality, Uniqueness, performance, collectability and acceptability. It is the combination of all these attributes that determines the effectiveness of a biometric and therefore, the effectiveness of a biometric authentication system that uses particular biometric in a particular application. There is no biometric that satisfies any of these properties absolutely, nor one which has all to a completely satisfactory level simultaneously, especially if acceptability is taken into account. This means that any biometric authentication solution is the result of many compromises.

2. RELATED WORKS

Extraction of minutiae from fingerprint images and to perform fingerprint matching based on the number of corresponding minutiae pairings is common in fingerprint recognition. But recognition performance is significantly influenced by fingertip surface condition, which may vary depending on environmental or personal causes. To handle this issue authors in [1], presented a fingerprint recognition algorithm using phase-based image matching. The use of phase components in 2D (two-dimensional) discrete Fourier transforms of fingerprint images makes it possible to achieve highly robust fingerprint recognition for low-quality fingerprints. Paper [2] has developed a fingerprint identification and recognition system based on neural network. In [3] a novel method for Fingerprint recognition is considered using a combination of Fast Fourier Transform (FFT) and Gabor Filters to enhance the fingerprint image. Extracting features out of poor quality prints is the most challenging problem faced in this area. In [4], the texture feature based approach for fingerprint recognition using Discrete Wavelet Transform (DWT) is developed to identify the low quality fingerprint from inked-printed images on paper. As an Automatic Fingerprint Identification System (AFIS), fingerprint recognition-based access control system of automobiles is presented in [5], in which fingerprint encryption technique utilized, has some advantages such as smartness, security, low power, low cost, etc. In [6], authors have presented a touch-less fingerprint recognition system by using a digital camera. They have addressed the constraints of the fingerprint images that were acquired with digital camera, such as the low contrast between the ridges and the valleys in fingerprint images, defocus and motion blurriness. Fingerprint matching method is proposed in [7], with which two fingerprint skeleton images are matched directly. In this method, an associate table is introduced to describe the relation of a ridge with its neighbor ridges, so the whole ridge pattern can be easily handed. . In [8], a direct approach for matching fingerprint pores is presented. It first determines the correspondences between pores based on their local features. It then uses the RANSAC (RandomSample Consensus) algorithm to refine the pore correspondences obtained in the first step. A similarity score is finally calculated based on the pore matching results. paper [9]shows how webcams can be used to take images in more or less uncontrolled manner to produce images that can be used for fingerprint matching. In [10],a new secure cryptographic authentication method using biometric features is presented. The proposed system combines the advantages of biometric identification and cryptographic techniques. By adding a subsystem to existing biometric recognition systems, we can simultaneously achieve the security of cryptographic technology and the error tolerance of biometric recognition. [11] describes a hybrid fingerprint matching scheme that uses both minutiae and ridge information to represent and match fingerprints. [12] Proposed a fingerprint pose estimation algorithm which can register fingerprints into a common finger coordinate system. Fingerprint pose estimation problem is viewed as a two-class classification problem and approached by sliding window classifiers trained on labeled data. [13] Proposed a fingerprint recognition technique which uses the linear binary patterns for fingerprint representation and matching. [14] Proposed a multibiometric fingerprint recognition system based on the fusion of minutiae and ridges as these systems render more efficiency, convenience and security than any other means of identification.

3. BIOMETRIC SUBSYSTEM

Any biometric authentication system can be viewed as a pattern recognition system as shown in Fig.1.Such system consists of biometric sensors, feature extractors to compare salient attributes from the input signals and feature matchers for comparing two set of biometric features. An authentication system consists of two subsystems: one for enrollment and one for authentication. Duringenrollment, biometric measurements are captured from subject, relevent information from the raw measurement is gleaned

by the feature extractor and this information is stored in the database. Along with the machine representation of the biometric features, some form of ID for the subject is linked to the representation along with other data. The task of the authentication module is to recognize a subject at a later stage, and is either identification of one person among many or verification that a person's biometric matches a clamed identity. For identification, the system acquires the biometric sample from the subject, extracts features from the raw measurements and searches the entire database formatches using the extracted biometric features. Forverification, a subject presents some form of identifier and a biometric. The system senses the biometric measurements, extractsfeatures, compares the input features with the features enrolled in the system database under the subject's ID.The system then either determines that the subject is who he claims to be or rejects the claim.

4. CHALLENGES IN BIOMETRIC AUTHENTICATION

Most biometric systems assume that the template in the system is secure due to human supervision (e.g., immigration checks and criminal database search) or physical protection (e.g., laptop locks and door locks). However, a variety of applications of authentication need to work over a partially secure or insecure network such as an ATM networks or the Internet. Authentication over insecure public networks or with untrusted servers raises more concerns in privacy and security. The primary concern is related to the security of the plain biometric templates, which cannot be replaced, once they are compromised .The privacy concerns arise from the fact that the biometric samples reveal more information about its owner (medical, food habits, etc.) in addition to the identity. Widespread use of biometric authentication also raises concerns of tracking a person, as every activity that requires authentication can be uniquely assigned to an individual.

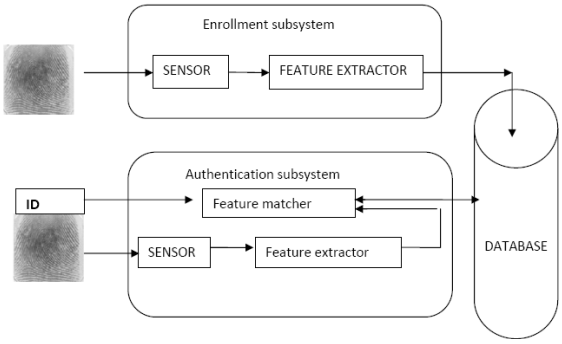

Fig. 1. Enrollment and authentication process in biometrics

5. PROPOSED SOLUTION

To overcome the issues of template security, computational speed with existing methods and to improve the performance with respect toauthentication, when finger print image is especially transferred through internet, rather than applying conventional methods, intelligent method based on artificial neural network is taken as solution platform. There are number of methods available in ANN which can be applied for making the solution better among them universal approximation, one to one mapping and one-way properties is selected to achieve the objectives as shown in Figure2. Description of these properties is given below.

(a) Universal approximation:

Let F be any Borel measurable or continuous function from $k \subset \Re^n$ on $(0, 1)^m$and let Φ be any strictly increasing continuous squashing function. Then, for any $\varepsilon > 0$ there exists a multilayer feed forward network N with the quashing function in the output layer and with only one hidden layer such that

$$\| N(x)-F(x)\| < \varepsilon , \quad \forall\, x \in K \qquad (1)$$

(b) One to one mapping:

If there is an interaction between two parameters under an environment and circumstances so that resultant outcome could be a unique value, then this unique value can be defined as the one to one mapping between these parameters. Mathematically this can be stated as:

$$\varphi(x_i, y) \neq \varphi(x_j, y) ; \forall\, j \text{ if } j \neq i ; \qquad (2)$$

Where x_i is external stimulus and having an established relationship with environment φ contains parameter y and x_j is a new test input in the same environment. This principle is also valid if stimulus is same for different parameter available in environment and this can express as

$$\varphi(x, y_i) \neq \varphi(x, y_j) ; \forall\, j \text{ if } j \neq i ; \qquad (3)$$

This mapping characteristic can be utilized for authentication and recognition purpose in various applications especially in the field of image recognition where authentication and recognition process is cascaded with automatic action as response of recognition.

(c) One-way Property

As it appears by the name a system that contains one-way property allows to compute the output from the input easily while makes it very difficult to compute the input from the output. There are two very clear reasons why neural network has one way property:

(i) Number of neurons having nonlinear characteristics are involved and interconnected to produce the output.

(ii) After learning all previous changes in iterations, the previous iterations are lost permanently i.e. no trace is available about how it has resulted in the output. Situation will become worse if weights are not available in fact it is impossible to find the input if weights are not available.

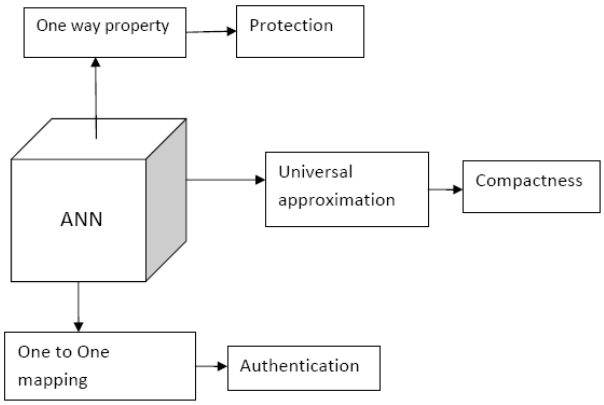

Fig. 2. ANN properties and its proposed application

5.1 Correlation Strength

If there is an interaction of two parameters happen under an environment and circumstances so that resultant outcomes could be a unique value, then this unique value can be defined as the correlation strength between these parameters. Mathematically this can be stated as:

$$\varphi(Xi, Y) \neq \varphi(X_j, Y) \quad ; \quad \forall j \text{ if } i \neq j \qquad (4)$$

Where Xi is external stimulus and has an established relationship with environment φ which contains parameter Y and Xj is a new test input in the same environment. This principle is also valid if stimulus is same for different parameter available in environment and this can be expressed as

$$\varphi(X, Y_i) \neq \varphi(X, Y_j) \quad ; \quad \forall j \text{ if } i \neq j \qquad (5)$$

This correlation strength can be utilized for recognition purpose in various applications of pattern recognition especially in the field of image recognition, where recognition process is cascaded with automatic action as response ofrecognition.

5.2 Neural modeling of correlation strength

The defined concept of correlation strength can be efficiently modeled with the artificial neural network. Let the environment presented by the architecture of feed forward neural network contain multilayer structure with single oupout node and unimodel sigmoid function as activation function. Required circumstance of maximum degree of coorelation between stimulas X and available connection weights can be established by applying the learning. After having the training of weights in neural parameter, Y appeared as trained weights for W .The neural modeling of (2) for recognition of input image X_i, which has more similar statistical and physical characteristices with image Xi compared to image Xj can be defined as

$$|f(\Phi(Xi, Wi) - f(\Phi(Xi', Wi)| > |f(\Phi(Xj, Wj) - f(\Phi(Xi', Wj)| \quad \forall i, j \text{ if } i \neq j \qquad (6)$$

Where Wi and Wj are set of trained weights corresponding to image Xi and Xj .In fact the phylosphy of learning can be defined as establishment of relationship w.r.t objective and this is possible by iterative adjustment of neural weights in association of input information for fixed value of target.

5.3. Proposed authentication method

Recognition is a recalling process in which past experience is used to classify and recognize the object. If the object exists inside the domain of experience, recalling is without error otherwise has an error value. Acceptable value of error depends upon application. Process of authentication is shown in Fig.3

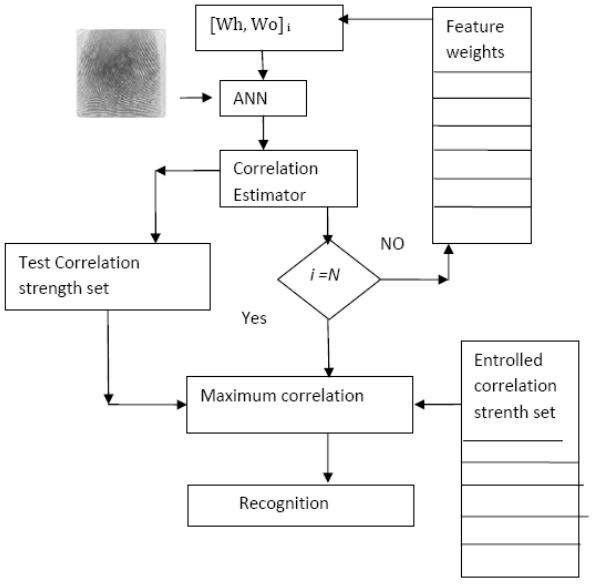

Fig. 3. correlation strength based authentication process

Preprocessing is a step which makes the raw data suitable for proper processing, without which either it is not possible to complete the processing or it may happen with error. From neural network perspectives two different stages are required for preprocessing (a) spatial block formation (b) normalization. In spatial block formation image is divided into number of block, each block having a size of m*n pixels, generally m = n. Depending upon the number of pixels in each block input layer neuron number can be decided. As a thumb rule the size of block should

not be too large otherwise it will carry more information which will make it difficult to extract local information or should not be too small otherwise block will not carry proper information about its neighbors. Any moderate size will give a better chance to capture the correlation of pixels in a small local region. Normalization will transfer the pixels value in the range of [0 1] so that it can be directly taken as an input for neural network.

The proposed principle has been applied in this paper for fixed image recognition with and without various noises. In fact having more inclination towards application in data mining where information has to be retrieved with fixed image as an input. To prove the principle experimentally 10 different gray scale fingerprint images are taken, each has a size of 512*512 pixels .Preprocessing is applied to each image in terms of normalization and divided each image as set of 10*10 pixels block. A feed forward neural architecture containing 100 input nodes, 5 hidden nodes and 1 output node is created. Bias with fixed input +1 also is applied to hidden nodes and output nodes. Initialization of all weights defined as random number by uniform distribution in the range of [-1 1].For each individual image, separate learning (a fixed number of iteration equal to 4)is defined using back-propagation with target equal to 1.Momentum is also applied with momentum constant equal to 0.1 to increase the learning speed. The value of learning rate is taken as 0.1 for all fingerprint images. Once, learning of one image is completed, the correlation strength for each block is taken as output generated by neural network for that block and stored in an array which is defined for that particular image. In result an array corresponding to each image carry as much number of DC values as the number of blocks available in an image. Trained weights corresponding to each image are also stored. In other words corresponding to each image there is an array containing degree of correlation and a set of trained weights in memory.

In test case, when any one of the image among those which have been trained is applied with or without some variation, preprocessing is applied to normalize and divide into same size of block (10*10).Degree of correlation is calculated with respect to stored set of weights. Absolute difference in correlation is obtained with each stored correlation value. Position of minimal total difference is established as final recognition of image and corresponding action is defined accordingly depending upon the nature of recognition, absolute or custom one. In the absolute recognition directly the position with minimal difference is the answer whereas for custom recognition depends upon defined threshold value decisions of recognition that appear. Fingerprint Images taken for simulation to create the data set is shown in Fig.3.Their correlation strength values are stored in same order as they have in Fig.4.

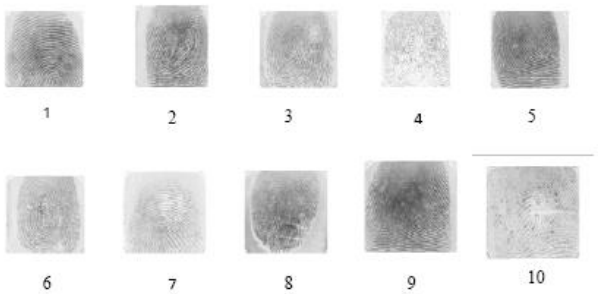

Fig. 4. Fingerprint images taken in experiment

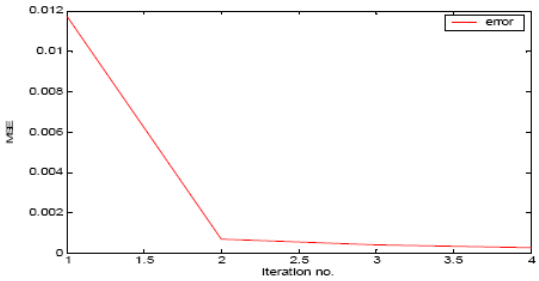

Fig. 5. learning characteristics for F1 image

It is clear from Fig.5 that within one iteration, there is sharp decline in MSE error and after that no significant change is observed hence termination is decided with 4 iteration only to make the speed faster.

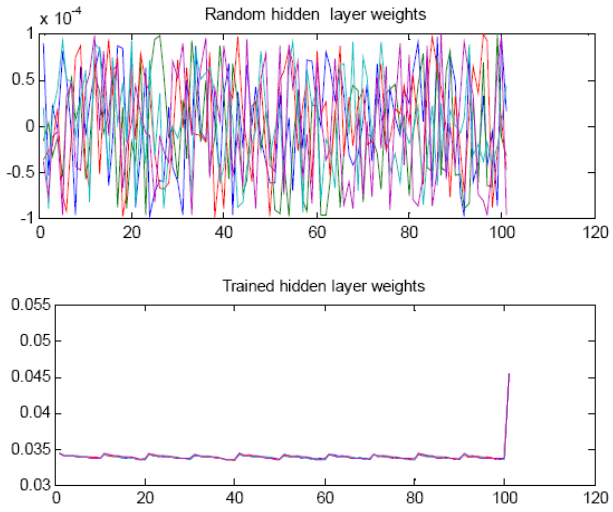

Fig. 6. Correlation strength development in trained weight

Development of correlation strength with learning phase by weights from no relation in the beginning to high bonding at the end of learning can be observed in Fig.6

Test Case 1: Fingerprint 1 without noise

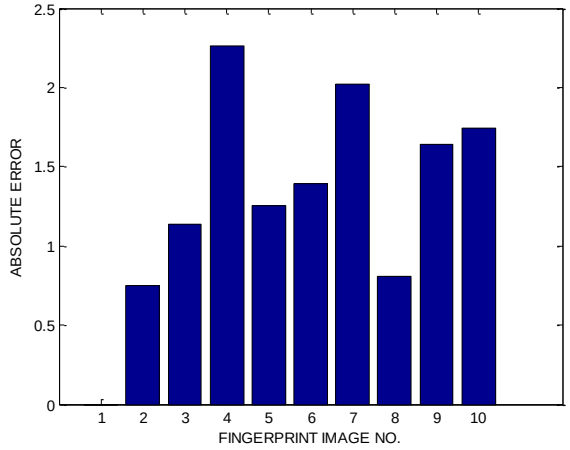

Fig. 7. Correlation strength with all 10 feature weights for F1

Test Case 2: Fingerprint 1 with Gaussian noise

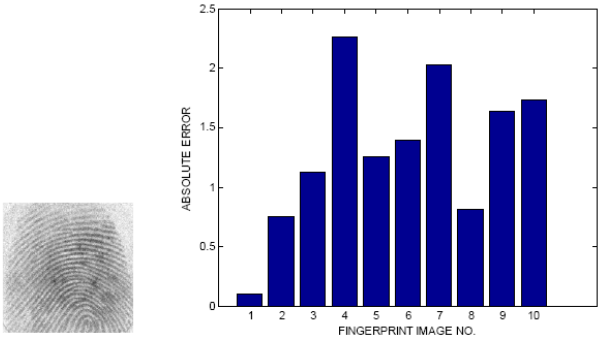

Fig. 8. Correlation strength with all 10 feature weights for F1

Test Case 3: Fingerprint 5 with Gaussian and Salt &Pepper noise

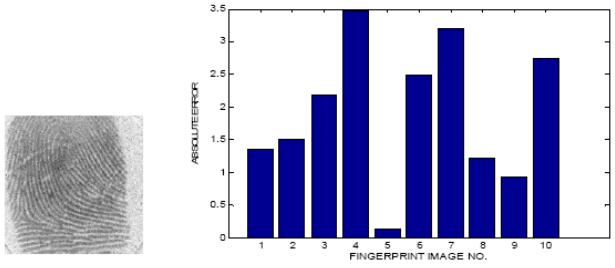

Fig. 9. Correlation strength with all 10 feature weights for F5

Test Case 4: Fingerprint 7 with Gaussian and Salt &Pepper noise

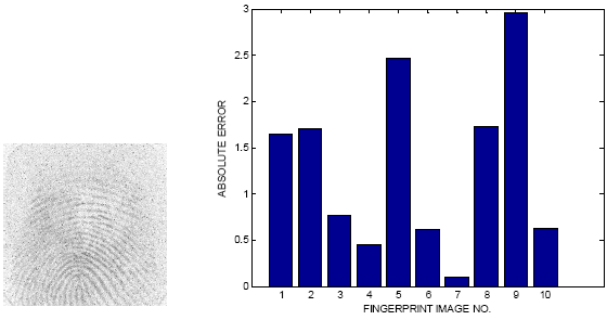

Fig. 10. Correlation strength with all 10 feature weights for F7

Four different test cases results are shown in Fig. 1 to Fig. 10 and their corresponding correlation strength in Table1.it is clear that there is minimum error in correlation strength corresponding to specified input fingerprint position which makes sure of authentication.

Table 1: Correlation strength for different test case

Test	Noise	CSE1	CSE2	CSE3	CSE4	CSE5	CSE6	CSE7	CSE8	CSE9	CSE10
F1	X	**0**	0.746	1.13	2.264	1.255	1.39	2.02	0.80	1.64	1.746
F1	(Gauss)	**0.10**	0.748	1.132	2.265	1.25	1.38	2.02	0.81	1.64	1.733
F5	(Gauss+SP)	1.35	1.50	2.17	3.46	**0.14**	2.49	3.20	1.21	0.93	2.73
F7	Gauss+SP)	1.64	1.70	0.76	0.44	2.46	0.60	**0.09**	1.72	2.95	0.62

6. CONCLUSION

We have proposed a neural network based approach to recognize the fingerprint images. Advantages of proposed solution are robustness against the various types of noise available with the test images which is very obvious in practicalenvironment. Correlation between the training image data and trained neural weights is utilized in decision process of recognition.Proposed solution is not just very efficient and robust but also it is very fast in computational domain. Proposed solution does not require storing the template of fingerprint images for recognition purpose hence there is high level of protection available with respect to personal information available with fingerprints and omit the chances of duplication.

REFERENCES

[1] K. Ito ; A. Morita ; T. Aoki ; T. Higuchi," A fingerprint recognition algorithm using phase-based image matching

for low-quality fingerprints “,Image Processing, 2005. ICIP 2005. IEEE International Conference on (Volume:2).

[2] L. H. Jin ; A. Chekima ; J. A. Dargham ; Liau Chung Fan,” Fingerprint identification and recognition using backpropagation neural network “,Research and Development, 2002. SCOReD 2002.

[3] G. Aguilar ; Nat. Polytech. Inst., Mexico D.F. ; G. Sanchez ; K. Toscano ; M. Salinas,”Fingerprint Recognition “,Internet Monitoring and Protection, 2007. ICIMP 2007.

[4] Z. M. Win ; M. M. Sein,” Texture feature based fingerprint recognition for low quality images”, Micro-NanoMechatronics and Human Science (MHS), 2011 International Symposium on

[5] Z. Zhu ; F. Chen,” Fingerprint recognition-based access controlling system for automobiles “Image and Signal Processing (CISP), 2011 4th International Congress on

[6] Y. Hiew ; A. B. J. Teoh ; Y. H. Pang,” Touch-less Fingerprint Recognition System “,Automatic Identification Advanced Technologies, 2007 IEEE Workshop on

[7] Xiaohui Xie,,Fei Su,, Anni Cai,” Ridge-Based Fingerprint Recognition”, Springer,Advances in Biometrics Volume 3832 of the series Lecture Notes in Computer Sciencepp 273-279, 2006

[8] Qijun Zhao, Lei Zhang,, David Zhang, Nan Luo,” Direct Pore Matching for Fingerprint Recognition”,springer,Advances in Biometrics,Volume 5558 of the series Lecture Notes in Computer Sciencepp 597-606, 2009.

[9] Bibek Behera, Akhil Lalwani,, Avinash Awate,” Using Webcam to Enhance Fingerprint Recognition”, Springer,Articulated Motion and Deformable Objects,Volume 8563 of the series Lecture Notes in Computer Sciencepp 51-60,2014.

[10] Shin-Yan Chiou,” Secure Method for Biometric-Based Recognition with Integrated Cryptographic Functions”, BioMed Research International,Volume 2013 (2013),

[11] Arun Ross, Anil Jain, James Reisman,” A hybrid "ngerprint matcher”, Pattern Recognition 36 (2003) 1661 – 1673

[12] Yijing Su , JianjiangFeng, , Jie Zhou ,” Fingerprint indexing with pose constraint”, Pattern Recognition ,Volume 54, June 2016, Pages 1–13

[13] A.T. Gowthami,H.R. Mamatha, “Fingerprint Recognition Using Zone Based Linear Binary Patterns” Procedia Computer Science,Volume 58, VisionNet’15, 2015, Pages 552–557

[14] Madhavi Gudavalli,,D. Srinivasa Kumar,, Viswanadha Raju,” A Multibiometric Fingerprint Recognition System Based on the Fusion of Minutiae and Ridges”, Volume 337 of the series Advances in Intelligent Systems and Computingpp 231-237,2015