A Biometric Fusion Based on Face and Fingerprint Recognition using ANN

Navneet Kaur Sandhu
Student, Dept. of ECE
UCOE, Punjabi University
Patiala, Punjab
navneetsandhu90@ymail.com

Manjeet Singh Patterh
Professor, Dept. of ECE
UCOE, Punjabi University
Patiala, Punjab
mspattar@yahoo.com

Abstract— Biometric systems are used for identifying and recognizing individual characteristics on the basis of biological or behavioral features. In the research work, a biometric fusion system based on fingerprint and face using the artificial intelligence technique is proposed. To achieve better accuracy of the biometric fusion system, the uniqueness of feature is significant. To find out the unique feature set from the data, we have used different feature extraction algorithm in the proposed biometric fusion system. Initially, pre-processing has been applied on the test images which is used to remove the unwanted data from the uploaded image and return an appropriate data for further process. In the fingerprint part, minutia extraction is used as a feature of fingerprint whereas Extended Local Binary pattern (ELBP) is used for extracting features of face and creates a pattern of face features. To create a unique feature set, optimization algorithm is needed and we have used genetic algorithm as a feature optimization technique. In the proposed fusion system, ANN is used to classify the test data according to the trained ANN structure with optimized feature data of fingerprint and face. To check the efficiency of proposed fusion system, we have calculated the performance parameters like FAR, FRR and Accuracy. From the analysis of proposed fusion system, we have observed that the accuracy of the proposed work is better than the previous ones and it is more than the 94%. To design a proposed biometric fusion system, image processing toolbox is used under the MATLAB environment.

Keywords- *Fingerprint recognition, Face recognition, Biometric system, Genetic algorithm (GA), Artificial neural network (ANN)*

*****

Introduction

Over the past decade, personal identifying demand has been greatly increased. Previously, biometric (e.g., fingerprint identification or facial recognition) was limited to criminal proceedings. Some experts may meet with the needs [1]. With the rise in terrorist activities, building entry restrictions and other related applications, the need for automated biometric technology is increasingly important. A biometric system recognizes human identity by using their physiological and behavioral traits. Biometric systems have advantages over the traditional security methods like they cannot be easily stolen or shared. A simple biometric system comprises of a sensor unit, extraction unit along with a matching unit [2].

The output of the biometric system is mainly affected by the sensors used and the type of feature extraction techniques that are used to extract the features of the sensed data. If the biometric traits like fingerprint with dirty hands adds noise and thus, affects the matching [3]. Thus, the matching score generated by dirty fingers has a great difference. To resolve this problem, multiple sensors with different biometric traits are used; this system is known as Multimodal-Biometric System. By using multimodal system, it become difficult for an intruder to spoof multiple biometric traits simultaneously and hence, provide a secure biometric system [4].

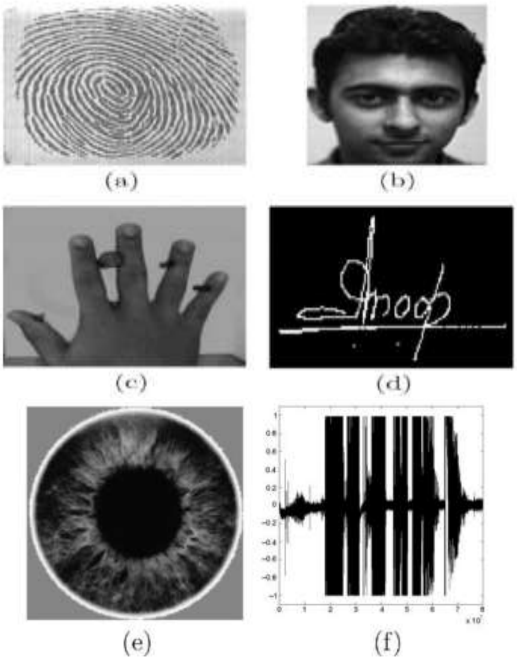


Figure 1. Example of some biometric traits (a) fingerprint (b) face (c) hand geometry (d) signature (e) Iris and (f) voice.

A. A Biometric system

A biometric system works in two modes, namely, Enrollment mode and authentication mode.

1) *Enrollment mode:* In this phase, person's biometric traits are read and stored into the database. The stored data is marked with an identity like name, ID number etc. so that recognition become easy.
2) *Authentication mode:* In this mode, the biometric traits are scanned and compared with the stored data for recognizing appropriate person [5].

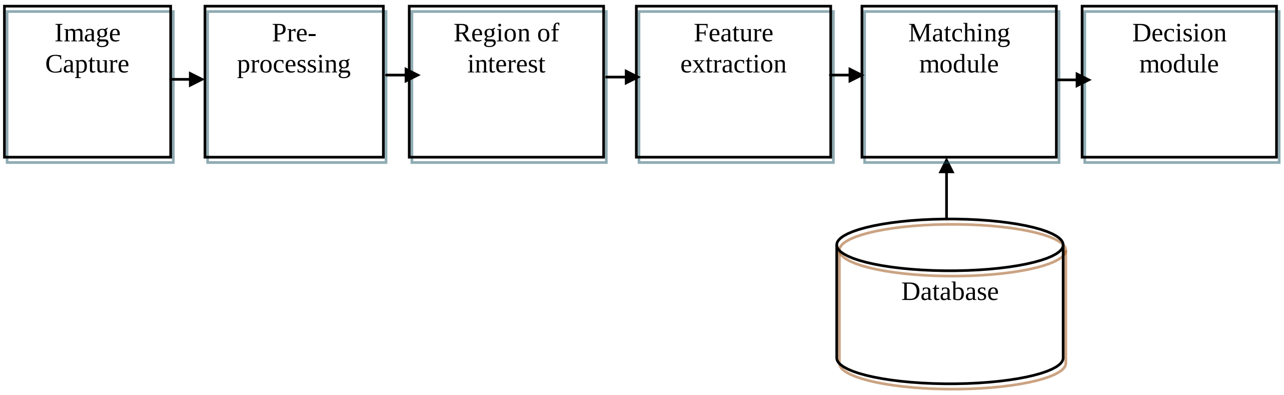


Figure 2. Biometric system

A biometric system mainly consists of image captured unit, Pre-processing, feature extraction unit, image matching unit and decision stage as shown in Fig. 2. Pre-processing always reduces the noise and gets the accurate image for feature extraction. After pre-processing, the regions of interest of the captured image are extracted. Then, features are extracted by using feature extraction techniques. The extracted features are later matched with the database images and matched score is generated [6].

In the proposed multimodal biometric system (Face and fingerprint), the features are fused on the basis of distance function. For identifying face, the objects are considered as face images and the features are the Local Binary Pattern (LBP) descriptor. LBP is a well known image representation technique mostly used for recognizing face. LBP is a kind of image descriptor that is used to capture image texture [7]. It is a simple, efficient and high performance technique that is used mostly in face recognition and texture analysis. Local Binary Pattern (LBP) is a very effective method for feature extraction. It encodes variations among pixel intensities in a local region of a pixel. It finds applications in various computer vision applications. For recognizing a face, histograms of LBP values are used [8]. The face is normally separated into rectangular sections and histograms are measured of each of them. The succession of these histogram values is used as the face image. The principal power of this method has the high capability to maintain essential information in the images. Nevertheless, utmost existing LBP-based face recognition schemes performs the computation of LBP histograms on a continuous and fixed grid in the image and thus, do not repeat the properties of the appropriate images. After LBP, genetic algorithm is applied to find the best possibility for every discontinuous segment in an image. At last, the optimized image is given as an input to neural networks based on trained scheme to diagnose and match finger print with data set. A large number of feature sets are used to train the network and thus, performance of the biometric system gets increased [9].

II. Related Work

D. Menotti *et al*. [2015] has used two research methods for identifying spoofing in various biometric systems. Experimental results have proved that the performance of the biometric system has shown an improvement and attained accuracy up to 100%. **T. Larrain et al. [2017]** has proposed a system for solving unconstrained problem by using a method known as sparse fingerprint classification algorithm. In training phase, a grid of patches is extracted form face images and constructs a dictionary. In testing phase, the extracted features are converted into binary images. **J. Galbally et al. [2014]** has presented a face recognition system that is used to identify different kinds of fraudulent events. **Lin Hong and Anil Jain [1998]** has developed a multi-biometric system for the identification of faces and fingerprints. The proposed scheme resolves the problems occurred in both face and finger print verification system. **A. Rattani et al [2007] has** studied fusion at feature extracted level for both face and fingerprint biometric system. Different parameters like FAR, FRR and accuracy are measured. **S. Chaudhary and R. Nath [2009**] has proposed a fused biometric system (palmprint, fingerprint and face) based on score level fusion. Pre-processing is used for all the three images. Then, their feature sets are compared with the stored images. For identifying an image, performance score is generated. **Wei-Shi Zheng et al. [2005]** has used principle component analysis method for reducing the dimension of identifying image. For optimizing the performance of the system, Genetic algorithm is used. **N. Harun et al. [2010]** has proposed a biometric system for keystroke recognition of an individual on the basis of time interval between each stroke. Neural network with back propagation method is used to train and find the features.
method is used to train and find the features.

III. Methodology

To verify the efficiency and accuracy of proposed, an effective biometric fusion system based on face and fingerprint recognition using genetic algorithm along with the artificial neural network has been proposed; we have performed several experiments with this procedure on several images. In proposed biometric fusion system, there are several steps used for recognizing the accurate result from the testing images. The methodology of proposed work is given below:

Step 1: Design and develop a proper GUI for the proposed biometric fusion system.

Step 2: Upload the face and fingerprint images for Training and Testing of proposed biometric fusion system.

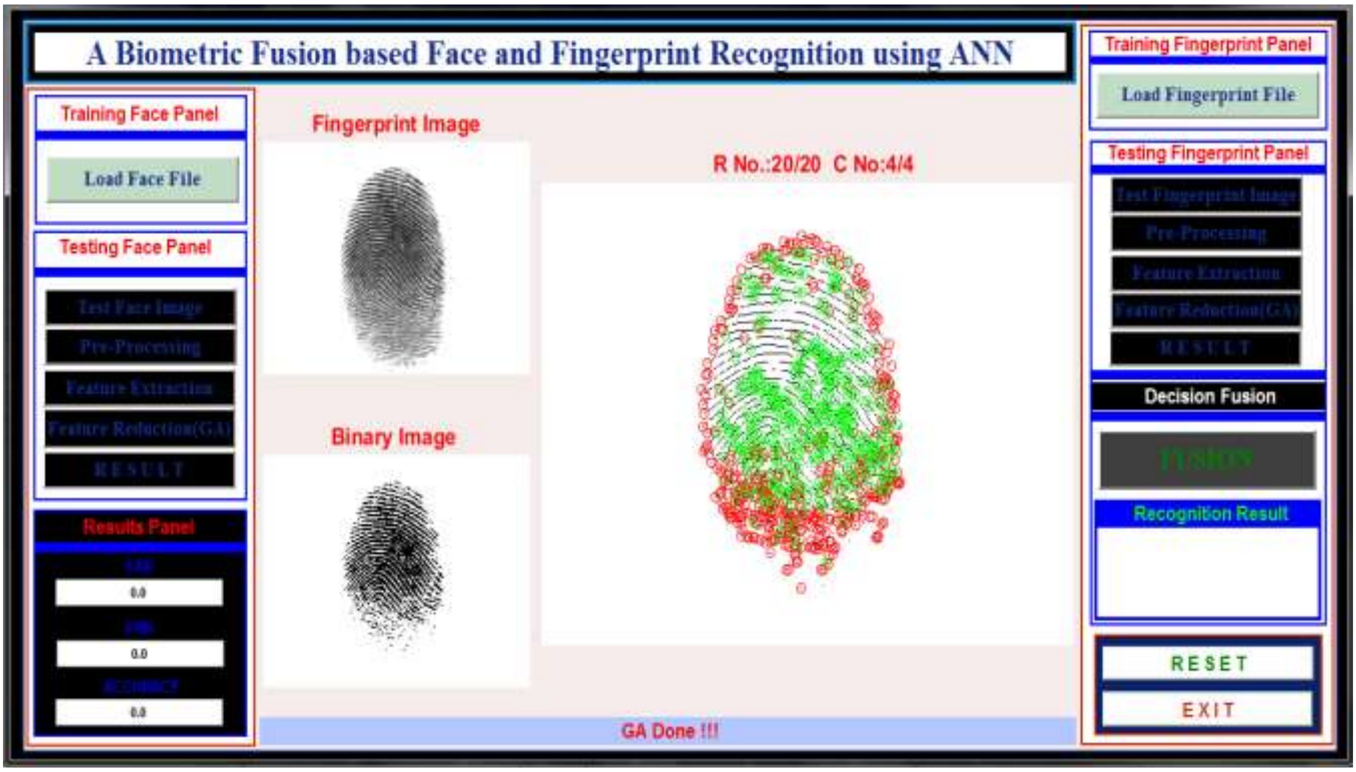
Step 3: Apply pre-processing on uploaded images in both section.
Step 4: Develop a code for the face detection from the pre-processed face images in training as well as testing section and same procedure is applied for fingerprint image with the thinning technique.
Step 5: Apply ELBP for the feature extraction from the detected face and minutia for the feature extraction from the fingerprint.
Step 6: Initialized Genetic Algorithm to optimize features and remove the unwanted feature sets using the novel objective function.
Step 7: Apply artificial neural network on optimized data to train the database and train the data using following steps:

- Select optimized feature as an input of artificial neural network for training and testing data.
- Compute the total categories which are generated by the training of optimized data using artificial neural network.

Step 8: After that, in the classification section we have classified the test data according to the trained artificial neural network structure.
Step 9: In the both recognition panel, we have created a test matching number and on the basis of the matching number in the fusion part, we have checked the recognition result.
Step 10: At last of module, we calculate the performance parameters of proposed biometric fusion system like FAR, FRR and Accuracy.

IV. Simulation Results

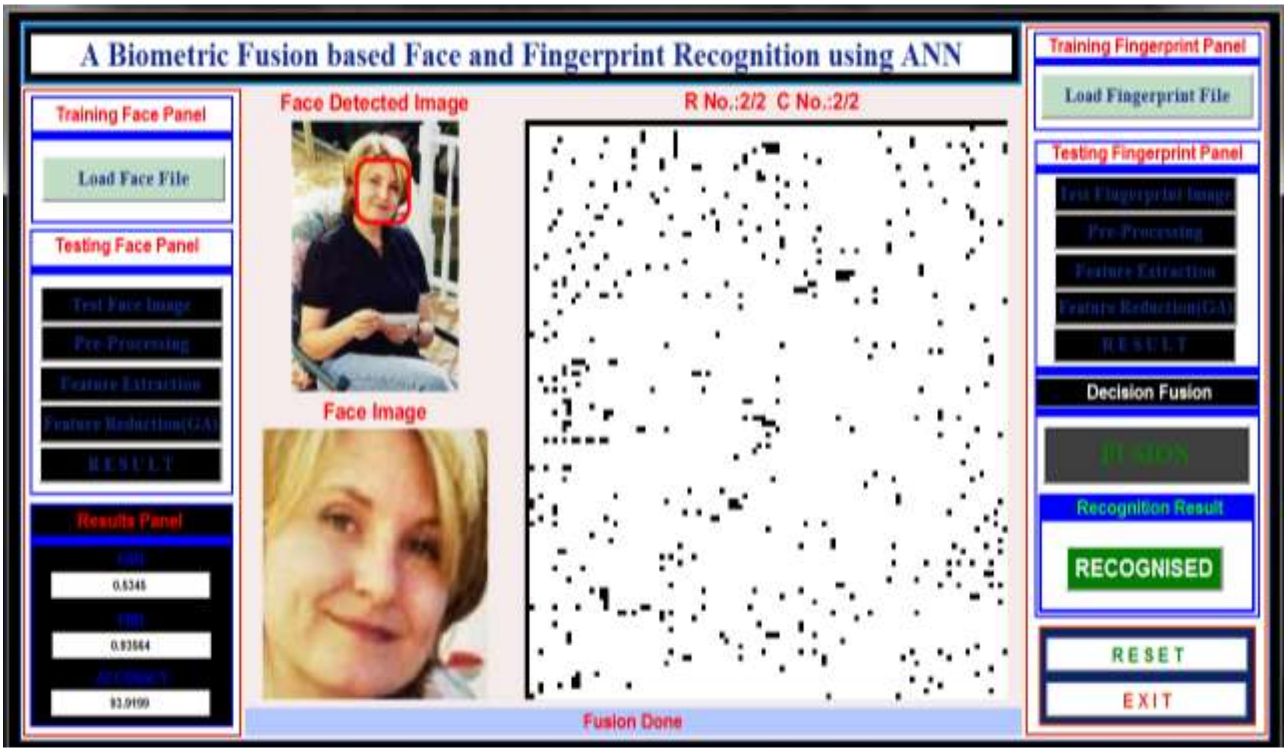
In this section, simulated results for the proposed biometric fusion based face and fingerprint recognition using ANN are described. The simulation has been carried out in MATLAB environment.



FAR 0.0
FRR 0.0
ACCURACY 0.0

Figure 3. Fingerprint Recognition System

In the above figure, three images of fingerprints are displayed, namely, Fingerprint image, binary image and R No, 20/20 C no. 4/4 image. Firstly, pre-processing is applied on the scanned fingerprint which is used to reduce the unwanted and dirty areas of the scanned image. Now, the pre-processed image is converted into binary image in the form of 0 and 1. This process is known as Binarization. Then, features are extracted by using Minutia feature extraction technique and then optimization technique known as genetic algorithm along with neural network is used.



0.5345

0.93564

93.9199

Recognition Result

RECOGNISED

Fusion Done

Figure 4. Fusion System

Initially, the uploaded image for face identification is cropped by using pre-processing process as the aim of the research for identifying the face. After cropping face feature extraction technique known as extended, Local Binary pattern is used by recognizing the face pattern. Genetic algorithm is used to optimize the extracted features and neural network is used to classify that optimized feature. After that both the classified images are fused. When the fingerprint and face of the same person is matched, only then, the biometric system displays a message like "Recognized". If both the features are not matched with the stored data in database then a message "Not recognized" is displayed on the screen. After recognition of the parameters like FAR, FRR and accuracy are measured and are shown below.

TABLE1. PERFORMANCE PARAMETERS

Number of Samples	FAR	FRR	ACCURACY
1	0.5345	0.93564	93.9199
2	0.5344	0.9012	94.5648
3	0.5247	0.9245	93.5781
4	0.5147	0.9275	95.2147
5	0.5487	0.9357	94.0278
6	0.5272	0.9247	93.0124
7	0.5312	0.8957	92.0157
8	0.5347	0.8976	95.0124
9	0.5248	0.9125	95.2345
10	0.5348	0.9254	975213

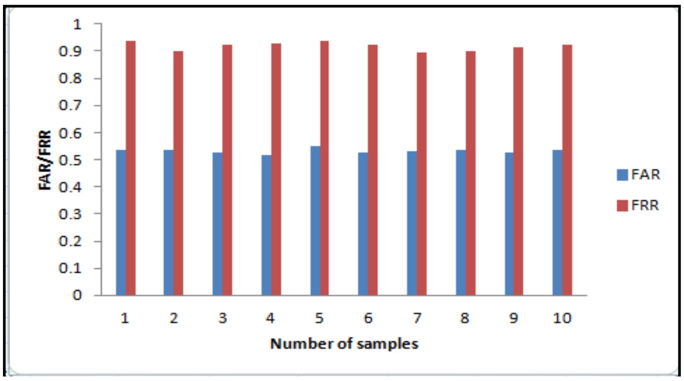


Figure 5. FAR and FRR of the proposed work

In the figure above, red bar line indicates the values of FRR obtained for the fused fingerprint and face image. The blue bar line indicates the FAR values for the proposed work. The average value of FAR and FRR obtained for the proposed work are 0.53097 and 0.918044 respectively.

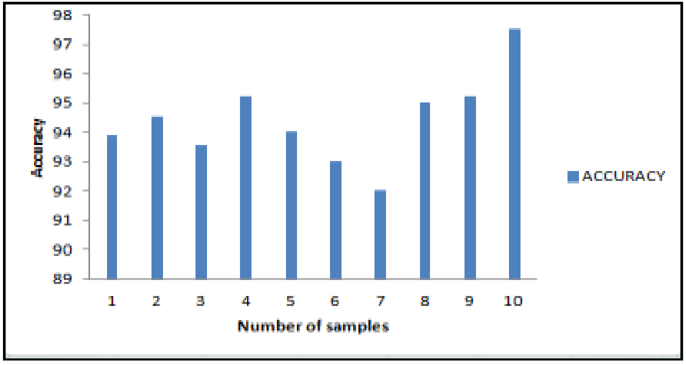


Figure 6. Accuracy of the proposed Work

The accuracy for the proposed work for ten numbers of samples is displayed in figure above. Maximum accuracy up to 97.5213 % is obtained for the last uploaded sample. The average value obtained for the proposed system is 94.41%.

V. CONCLUSION

In the proposed work, an efficient biometric fusion system based on the fingerprint and face using the artificial intelligence technique has been presented. Biometrics authentication system has become popular because it uses the unique physical features, such as fingerprints, palm, voice, iris and face verification and identification. This technology helps private and public enterprises and governments to combat identity theft and fraud. As it is known that every individual's biometric feature remains the same for lifetime. In the proposed work, test images are gone through different processes named as pre-processing, feature extraction, optimization and classification. Fingerprint feature are extracted by using Minutia feature extraction techniques whereas for face ELBP feature extraction technique is used to create a unique feature sets. For feature optimization, genetic algorithm is used to remove the unwanted features according to the objective function of proposed work. On the basis of ANN training and classification, we have achieved better recognition rate as compare to the previous work and the accuracy of proposed work is more than 94%.

In the future, SIFT feature descriptor technique can be used along with different optimization algorithms like PSO, GA, ABC ACO etc. and can generate a hybrid optimization algorithm. By using the combination of SIFT along with optimization technique the chances of recognition rate can be increased.

REFERENCES

[1] M. O. Oloyede and G. P. Hancke, “Unimodal and Multimodal Biometric Sensing Systems: A Review,” in IEEE Access, vol. 4, no. , pp. 7532-7555, 2016.

[2] Y. Xu, Z. Zhang, G. Lu, and J. Yang, “Approximately symmetrical face images for image preprocessing in face recognition and sparse representation based classification,” Pattern Recognition, vol. 54, pp. 68-82, 2016.

[3] A. Rehman and T. Saba, “Neural networks for document image preprocessing: state of the art,”Artificial Intelligence Review, vol. 42, pp. 253-273, 2014.

[4] Subban, Ravi, and Dattatreya P. Mankame, “A study of biometric approach using fingerprint recognition,” Lecture Notes on Software Engineering vol.1, pp.209-215, 2013.

[5] J. S. Pierrard and T. Vetter, “Skin detail analysis for face recognition,” IEEE Conference on Computer Vision and Pattern Recognition, Minneapolis, MN, , pp. 1–8, June 2009.

[6] B. Saropourian, “A new approach of finger-print recognition based on neural network,” 2009 2nd IEEE International Conference on Computer Science and Information Technology, Beijing, 2009, pp. 158-161.

[7] T. Larrain, J. S. Bernhard, D. Mery and K. W. Bowyer, “Face Recognition Using Sparse Fingerprint Classification Algorithm,” in IEEE Transactions on Information Forensics and Security, vol. 12, no. 7, pp. 1646-1657, July 2017.

[8] J. Galbally, S. Marcel and J. Fierrez, “Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition,” in IEEE Transactions on Image Processing, vol. 23, no. 2, pp. 710-724, Feb. 2014.

[9] Guo, Zhenhua, Lei Zhang, and David Zhang. “Rotation invariant texture classification using LBP variance (LBPV) with global matching.” Pattern recognition 43.3 (2010): 706-719.

[10] Tan, Xiaoyang, and Bill Triggs. “Fusing Gabor and LBP feature sets for kernel-based face recognition.” International Workshop on Analysis and Modeling of Faces and Gestures. Springer, Berlin, Heidelberg, 2007, pp.235-249.

[11] D. Menotti et al., “Deep Representations for Iris, Face, and Fingerprint Spoofing Detection,” in IEEE Transactions on Information Forensics and Security, vol. 10, no. 4, pp. 864-879, April 2015.

[12] T. Larrain, J. S. Bernhard, D. Mery and K. W. Bowyer, “Face Recognition Using Sparse Fingerprint Classification Algorithm,” in IEEE Transactions on Information Forensics and Security, vol. 12, no. 7, pp. 1646-1657, July 2017.

[13] J. Galbally, S. Marcel and J. Fierrez, “Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition,” in IEEE Transactions on Image Processing, vol. 23, no. 2, pp. 710-724, Feb. 2014.

[14] Lin Hong and Anil Jain, “Integrating faces and fingerprints for personal identification,” in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, no. 12, pp. 1295-1307, Dec 1998.

[15] A. Rattani, D. R. Kisku, M. Bicego and M. Tistarelli, “Feature Level Fusion of Face and Fingerprint Biometrics,” 2007 First IEEE International Conference on Biometrics: Theory, Applications, and Systems, Crystal City, VA, 2007, pp. 1-6.

[16] S. Prabhakar, S. Pankanti and A. K. Jain, “Biometric recognition: security and privacy concerns,” in IEEE Security & Privacy, vol. 1, no. 2, pp. 33-42, Mar-Apr 2003.

[17] S. Chaudhary and R. Nath, “A Multimodal Biometric Recognition System Based on Fusion of Palmprint, Fingerprint and Face,” 2009 International Conference on Advances in Recent Technologies in Communication and Computing, Kottayam, Kerala, 2009, pp. 596-600.

[18] Wei-Shi Zheng, Jian-Huang Lai and P. C. Yuen, “GA-fisher: a new LDA-based face recognition algorithm with selection of principal components,” in IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), vol. 35, no. 5, pp. 1065-1078, Oct. 2005.

[19] N. Harun, W. L. Woo and S. S. Dlay, “Performance of keystroke biometrics authentication system using artificial neural network (ANN) and distance classifier method,” Computer and Communication Engineering (ICCCE), 2010 International Conference on, Kuala Lumpur, 2010, pp. 1-6.