Implementation of Multimodal Biometric Authentication using Soft Computing Techniques

P.Mahalakshmi
PG Scholar, Department of CSE,
Pavendar Bharathidasan College of
Engg & Tech,Tiruchirappalli,India.
pmaha.21@gmail.com

K.Gunasekaran
Assistant Professor, Department of CSE,
Pavendar Bharathidasan College of
Engg &Tech, Tiruchirappalli,India.
gunaasekarann@yahoo.co.in

D.Saravanan
Associate Professor, Department of CSEand Head,
Pavendar Bharathidasan College of
Engg & Tech,Tiruchirappalli,India.
dsarav23@gmail.com

***Abstract*— Identity Management refers to a challenge of providing authorized users with secure and easy access to information and services for personal identification system. The objective is to implement a secure identification system for determining an individual's identity. Conventional methods for personal identification include keys, tokens, access cards, PINs and passwords which leads to drawbacks such as stealing, duplicating, cracking and sharing. In order to overcome the drawbacks, biometrics based identification is implemented. Nevertheless, unimodal biometrics is suffered due to noise, intra class variations, spoof attacks, non-universality. To avoid these attacks, multimodal biometrics which is the combination of more modalities is adapted. The biometric traits such as fingerprint, palmprint and finger knuckle-print (FKP) are used as a source of authentication that has highly rich texture information and are the most emerging and leading technologies for user identification. Neural Networks one of the Soft Computing techniques has been proposed for feature extraction and minutiae point detection. Euclidean distance values are used for minutiae matching. These modalities are combined and fusion is applied at matching-score level. The proposed method achieves excellent recognition rate and are more secure in noisy environment.**

Keywords—Biometrics, 2D-Gabor Filter, K-Nearest Neighborhood Algorithm(KNN), Artificial Neural Networks(ANN), FeedForwardNeuralNetworks(FNN), MultilayerPerceptron(MLP), Backpropagation Algorithm, Euclidean distance.

I. INTRODUCTION

The area of personal identification is exploiting computer-aided systems as a safer and more robust method and biometrics is one of the most reliable features that can be used for personal recognition. In traditional identification systems passwords, ID cards have been used to moderate access to restricted systems. However, security can be breached when an unauthorized user or imposter tries to misuse them. Inconvenience with using traditional methods caused rapid increase in the application of biometrics.

Biometrics is an automatic identification that refers to a study of analyzing, comparing and measuring an individual's identity based on the physiological or behavioral characteristics associated with the user [4]. biometrics is used as a form of identity access management and access control.

There are two types of biometrics namely, Unimodal and Multimodal. The common place biometric features are fingerprints, facial features, iris patterns, speech patterns, hand geometry and palmprints.

A biometric verification system operates on two modes such as enrollment mode and verification mode. In enrollment mode, the system recognizes an individual by searching the templates of all the users in the database for a match. In the verification mode, system validates identity of person by comparing the captured biometric data with the own biometric template(s) which are stored system database.

Biometric systems which rely on the evidence of a single source of information for authentication are called Unimodal system [7]. Unimodal biometric systems suffer a variety of problems such as Noise in sensed data, Intra-class variations, Distinctiveness ability. The limitations of unimodal biometric system lead to high False Acceptance Rate (FAR) and False Rejection Rate (FRR), limited discrimination capability, upper bound in performance so multimodal biometric system is developed to meet the stringent performance requirements.

A biometric system which relies on presence of multiple pieces of evidence for personal identification is called multimodal biometric system [2]. A biometric system which relies on presence of multiple pieces of evidence for personal identification is called multimodal biometric system. It combines any number of independent biometrics and overcomes some of the limitations presented by using Unimodal biometric.

Multimodal biometrics are more vital to fraudulent technologies, because it is more difficult to forge multiple biometric characteristics than forging a single biometric characteristic thus provides higher accuracy rate and anti-spoofing measures by making it difficult for an intruder to simultaneously spoof the multiple biometric traits of a legitimate user [8].

The performance indicators for personal recognition system involve False Acceptance Rate (FAR) and False Rejection Rate (FRR).

False Acceptance Rate (FAR): If the biometric system incorrectly accepts an access attempt of an unauthorized user is known as False Acceptance Rate (FAR).A system's FAR states as the ratio between number of false acceptances and number of identification attempts.

$$\mathbf{FAR\ (\%) = (FA/N)*100} \qquad (1)$$

FA - Number of incidents of false acceptances.
N - Total number of samples.

False Rejection Rate (FRR): If the biometric system incorrectly rejects an access attempt of an authorized user is known as False Rejection Rate (FRR).A system's FRR states

(2)

as the ratio between number of false acceptances and number of identification attempts.

FRR (%) = (FR/N)*100

FR - Number of incidents of false rejections.
N - Total number of samples.

Thus, the equations (1) and (2) are used for performance evaluation in biometric system.

In this paper, fingerprint, palmprint and finger knuckle print biometrics are used for multimodal biometric system. The features are extracted using the classification algorithm Feed Forward Neural Networks (FNN). Minutiae based extraction and detection is done using Multilayer Perceptron (MLP) and Backpropagation Algorithm.

II. The Problem

The existing system deals with Unimodal biometric where fingerprint biometric was used for pattern recognition of an individual. It consists of features such as ridges and valleys. Fingerprint recognition is one of the oldest and most popular methods used for identification [15]. It has been used for criminal identification. The identity based on the frequency content and ridge orientation of a fingerprint.Fig.1 shows unimodal biometric fingerprint.

Fig.1. Unimodal Biometric

A. Feature Extraction

2D - Gabor Filter is used for feature extraction [13]. It is a framework for understanding the orientation and spatial frequency selectivity properties of the filter. In the local neighborhood the gray levels along the parallel ridges and valleys exhibit some ideal sinusoidal shaped plane waves associated with noise. The frequency is calculated as the inverse distance between two successive ridges. The features extracted will be used as input to the classifier. One of the drawback is the presence of symmetric filter has DC component when the bandwidth is large [13].

B. Classification

K-Nearest Neighborhood Algorithm (KNN) is used for classification. The classification is the grouping of the cluster of images between the test image and training image.KNN classifier consists of a collection of k images of an individual as per testing set [3]. The mean distance between the centroid of the images is calculated. The nearest point is chosen and plots the value which forms a cluster.Fig.2 shows the KNN algorithm works for two class problems. The KNN query starts at the test point x ad grows a spherical region until it encloses k training samples, and it labels the test point by majority vote of the samples. Here, the k values is 5, the test point x are the red points.

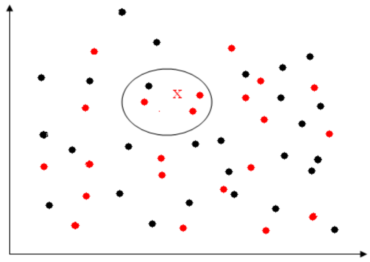

Fig.2. The KNN Algorithm

The disadvantages of the existing system include Non-universality; spoof attacks are possible; noise in sensed data, interclass variations. Thus, the proposed system overcomes the above problems.

III. System Design

The proposed system is based on Multimodal biometrics in which fingerprint, palmprint and finger knuckle print biometrics are used as a source of authentication.Fig.3 shows multimodal biometrics of fingerprint , palmprint and finger knuckle print. They are considered as the most popular, reliable and leading biometrics. Automatic Fingerprint Identification System (AFIS) employs techniques mostly based on minutiae points. Palmprint contains features such as wrinkles, principal lines and ridges from which minutiae points can be extracted [11]. The Finger Knuckle print refers to the inherent skin patterns on the outer surface of one's finger which has features such as lines/creases [11]. Due to rich texture information these traits are considered as powerful means in personal identification. Artificial Neural Networks (ANN), one of the Soft Computing techniques [12] used for Multimodal biometric identification.

Fig.3. Multimodal Biometrics

A. Biometric Trait Acquisition

The input image obtained is first normalized to reduce variations in gray level values along the ridges and valleys.Fig.4 shows histogram equalization and Segmentation for (a) fingerprint, (b) palmprint, (c) finger knuckle print. Histogram equalization is performed to enhance the clarity of the image. Binarization is performed to transform 8-bit gray scale image into binary image with 0 bit for ridges and 1 bit for valleys. Ridge segmentation is done to determine ridge ending, ridge branch and identify ROI. Then, the orientation process is performed to divide the binary image into w *w blocks [12].Fig.5 shows the Data Flow Diagram for Biometric Trait Acquisition.

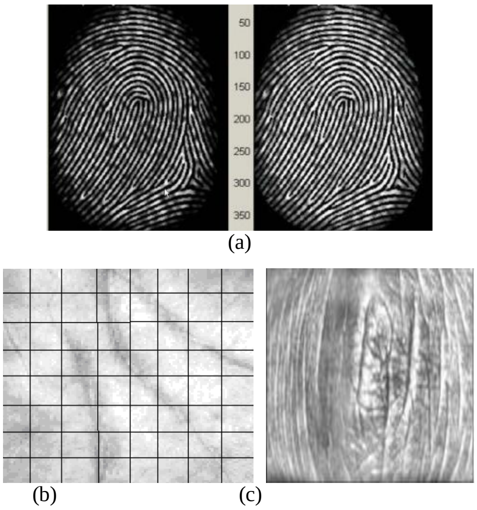

Fig.4. Histogram Equalization and Segmentation for (a) fingerprint; (b) palmprint; (c) finger knuckle print

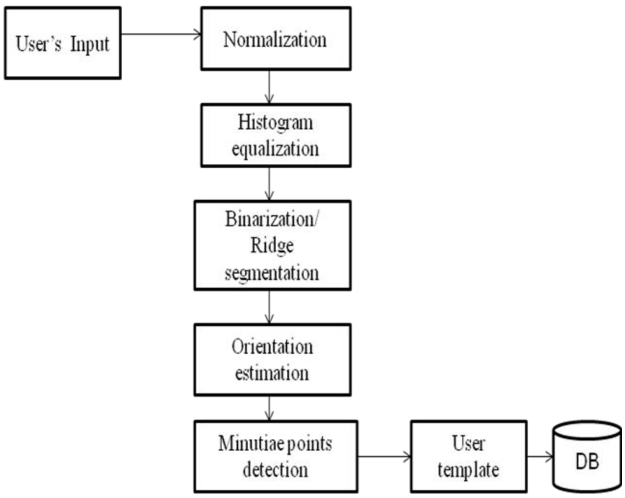

Fig.5. Data Flow Diagram for Biometric Trait Acquisition

B. Feature Extraction

Extraction of appropriate feature is the most important task. FNN is used for feature extraction. It is a classification algorithm that consists of large number of neurons (units) interconnected as layers [12]. Data is forwarded only in one direction and has no cycles or loops. The minutiae points are extracted by FNN from the ridges, valleys, principle lines and wrinkles,creases. Fig.6 shows the Minutiae Features for Finger, Finger Knuckle and Palm.

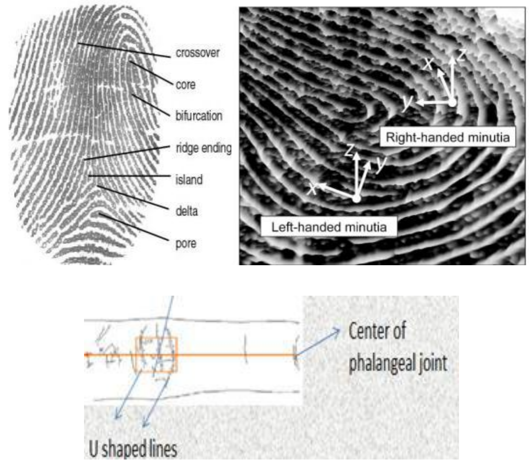

Fig.6. Minutiae Features of Finger, Finger Knuckle and Palm

C. Minutiae Detection

Multilayer Perceptron (MLP) one of the Feed Forward Neural Networks (FNN) techniques used to detect minutiae whether it is present on ridge branch or ridge ending. It consists of multiple layers such as input, hidden and output layers [12]. The network is analyzed using Backpropagation algorithm which is training or learning algorithm where neighborhood operation is performed by dividing the image into 3*3 window block size, when the window is placed on minutiae the value is 1 or else 0. If center pixel value is 1 and has only 1- one value neighbor then minutiae point is on ridge ending. If center pixel value is 1 and has only 3- one value neighbor then minutiae point is on ridge branch.Fig.7 shows the Structure of Multilayer Perceptron. Finally, Euclidean distance is calculated between minutiae points and stored in database [12].Fig.8 shows the Bifurcation and Termination Values for Minutiae Detection.

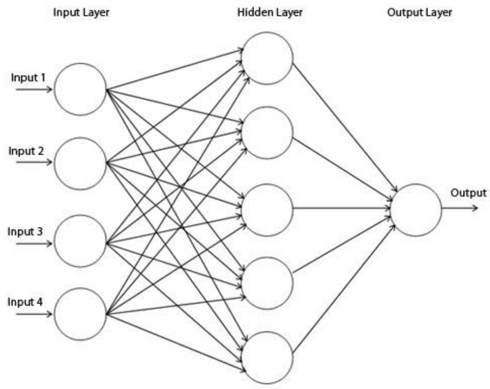

Fig.7. Structure of Multilayer Preceptron

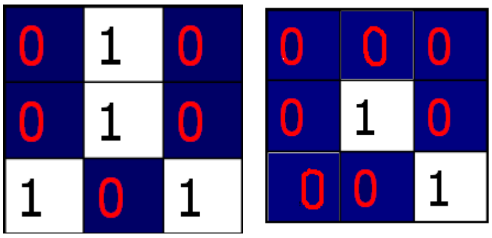

Fig.8.Bifurcation and Termination Values for Minutiae Detection

D. Minutiae Matching

Minutiae matching are done by comparing the minutiae values stored in database with the given input image. Fig.9 shows Minutiae Matching. Minutiae scores are generated with a range between 0 and 1. If the matching score is greater than predefined threshold value, the user is genuine otherwise is an imposter [5].Fig.10 shows Data Flow Diagram for Minutiae Score Validation.

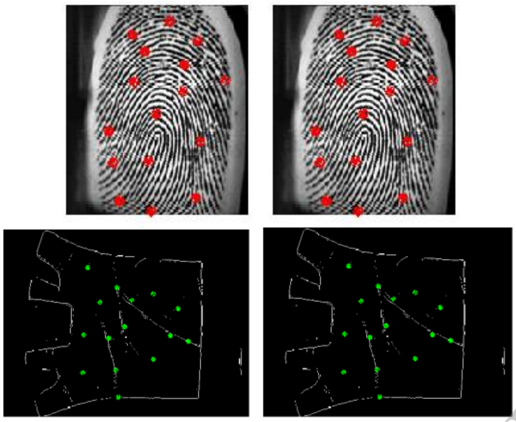

Fig.9. Minutiae Matching

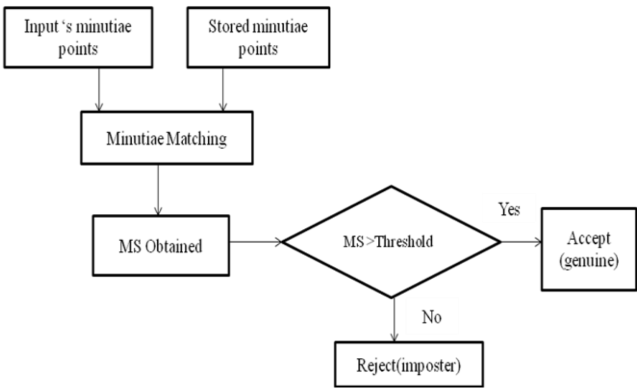

Fig.10. Data Flow Diagram for Minutiae Score Validation

IV. SYSTEM IMPLEMENTATION

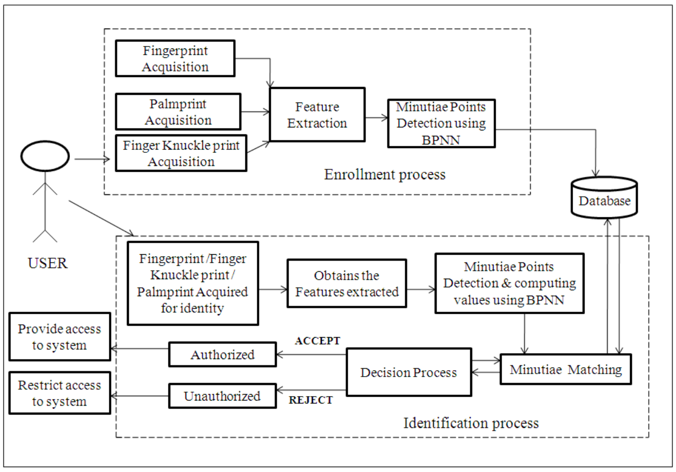

Fig.11. System Architecture for Minutiae Matching Based Personal Identification System

The architecture involves two step processes: Enrollment and Identification.Fig.11 shows System Architecture for Minutiae Matching Based Personal Identification System.

During enrollment process, the user enrolls fingerprint, finger knuckle print and palmprint as identity. The features such as ridges, valleys, principal lines, wrinkles, creases are extracted from minutiae points are obtained. At, minutiae detection, the minutiae points are differentiated as bifurcation and termination (ridge endings) points. Then along with the minutiae points, the Euclidean distance values are computed and stored in database.

During identification process, the biometric traits such as fingerprint, finger knuckle print and palmprint are acquired for identification. Similar process takes place until minutiae detection. At minutiae matching, the matching score values are computed by comparing the minutiae present in the given input and the one stored in database. The decision is done based on the matching score. If matching score is greater than the threshold value, the user is authorized and accepted. Otherwise, user is unauthorized and rejected.

V. RESULTS AND DISCUSSIONS

Using Matlab, the images of fingerprint, finger knuckle print and palmprint are enrolled and stored in MS-Access database. The biometric traits are obtained from PolyUDatabase. Then during the identification process, the images are loaded for image enhancement where normalization, histogram equalization and ridge orientation are performed. From the enhanced images, the minutiae points are extracted. Then the bifurcation and ridge endings are detected by performing neighborhood operation. Euclidean distance computation is performed. The minutiae values matching are done by computing the scores and authentication is verified.

The performance of Gabor filter varies for both real part and imaginary part in terms of FAR and FRR based on the number of samples. The variations are shown in Table 1 and Table 2. Fig.12 and Fig.13 indicates Gabor filter real and imaginary part

TABLE I. ACCURACY MEASURES FOR GABOR REAL PART

No of Samples	FRR	FAR	Accuracy
25	1.20	3.0	92.00
125	0.80	2.4	97.23
600	0.03	1.4	98.6.0

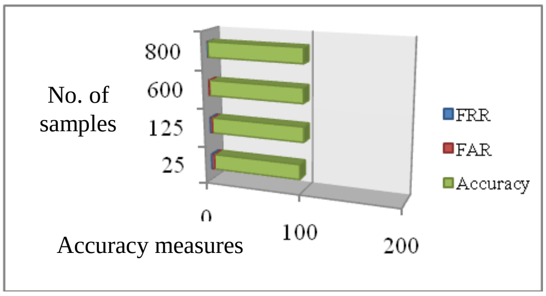

Fig.12. Gabor filter real part

TABLE II. ACCURACY MEASURES FOR GABOR IMAGINARY PART

No of Samples	FRR	FAR	Accuracy
25	1.20	3.0	92.00
125	0.80	2.4	97.23
600	0.03	1.4	98.6.0

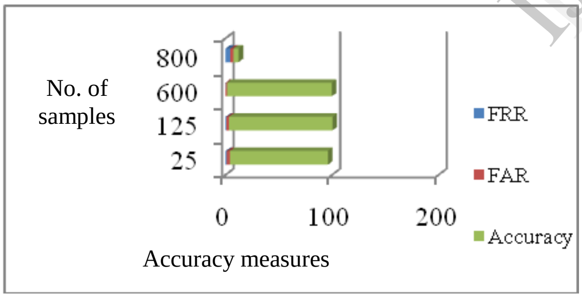

Fig.13. Gabor filter imaginary part

The performance of the proposed method with different thresholds, Tar, which control the false accept rate and false reject rate is shown Table 3.For optimal cases, the FAR is 0% and FRR is 0.91%. Fig.14 shows two distributions along with the threshold value.

TABLE III. EXPERIMENT RESULTS ON SELECTED THRESHOLD VALUES

Threshold Tar	False Accept Rate(%)	False Reject Rate(%)
0.325	0.00	1.56
0.335	0.00	0.91
0.345	0.37	0.65
0.355	0.92	0.65
0.365	2.50	0.39
0.375	5.36	0.13

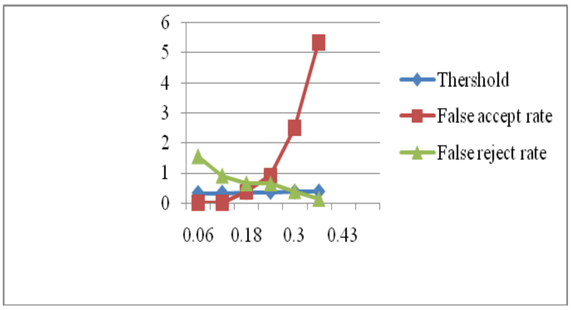

Fig.14. Imposter and Genuine Distributions

TABLE IV. BIOMETRIC TRAITS RECOGNITION PERFORMANCE USING EUCLIDEAN DISTANCE

S.No	Total No. of images used in database	Number of test images used	Average % of positive recognition		
			FP	FKP	PP
1	60	30	90	95.0	97.0
2	80	40	90	95.0	97.0
3	100	50	90	95.0	96.0
4	120	60	90	94.0	96.0
5	Average		90	94.75	96.5

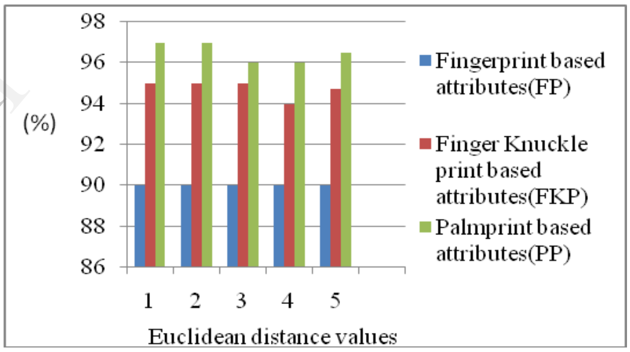

Fig.15. Performance Recognition for Fingerprint, Finger Knuckle print, Palmprint using Euclidean Distance

Fig.15 shows the performance recognition for fingerprint, finger knuckle print, palmprint using Euclidean distance. Table 4 shows biometric traits recognition performance using Euclidean distance.

$$\text{Euclidean Distance:} = \sqrt{((x1 - x2)^2 - (y1 - y2)^2)}$$

where, (x1, y1) and (x2, y2) are two pixel points or two data points. Thus, the proposed Neural Networks based methods improve classification accuracy between imposters and genuine users.

VI. CONCLUSION

Biometrics plays an important role in personal identification. The objective is to implement a secure personal identification system has been reliably achieved by means of using Multimodal Biometrics. Fingerprint, Finger Knuckle print and Palmprint which are rich in texture information achieves high accuracy .FNN based classification obtains excellent identification rate. Thus, the proposed method improves classification accuracy and impressive performance in noisy and clean conditions. The results provide reliable accuracy.

VII. Future Enhancement

Though Multimodal biometrics provides security, there is a possibility of minutiae being lost and presence of false minutiae during minutiae detection process. Hence, the future work deals with using hand vein to obtain security system with high accuracy.

Acknowledgment

I would like to convey my gratitude to the respected guide Mr.K.Gunasekaran, Assistant Professor, Department of CSE, for his moral support to complete the paper in a successful manner..

References

[1] Fanglin Chen, Jie Zhou, Chunyu Yang, ”Reconstructing Orientation Field From Fingerprint Minutiae-Matching Accuracy”, IEEE Transactions on Image Processing, July2009.

[2] Fawaz Alsaade,” Neuro-Fuzzy Logic Decision in a Multimodal Biometric Fusion System”, Scientific Journal of King Faisal University (Basic and Applied Sciences), Vol.11, No.02, 2010.

[3] Gayathri, R. and P. Ramamoorthy, “Palmprint Recognition using Feature Level Fusion”, Journal of Computer Science, ISSN 1549-3636, August 2012.

[4] A. K. Jain, A. Ross and S. Prabhakar, “An Introduction to Biometric Recognition”, In: IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, N. 1, pp 4-20, January 2004.

[5] Jianjang Feng , Jifeng Dai , Jie Zhou , “Efficient Ridge-Based Palmprint Matching ”,IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.34,No.08,August 2012.

[6] W.K. Kong and D. Zhang, “Palmprint Texture Analysis based on Low-Resolution Images for Personal Authentication”, 16th International Conference on Pattern Recognition, Vol. 3, pp. 807-810, August 2002.

[7] Mir .A.H, Rubab .S, Jhat .Z.A,” Biometric Verification: A Literature Survey “, International Journal of Computing & ICT Research, Vol.05, No.02, December 2011.

[8] MuthuKumar .A, Kasturi .C and Kannan .S, ”Multimodal Biometric Authentication using Particle Swarm Optimization Algorithm with Fingerprint and Iris”, ICTACT Journal on Image and Video Processing, Vol.02, No.03, Feburary 2012.

[9] Priyanka Somvanshi, Milind Rane “Survey of Palmprint Recognition” International Journal of Scientific & Engineering Research Volume 3, Issue 2, 1 ISSN 2229-5518, February-2012.

[10] Sabara Dinerstein, Jonathan Dinerstein, and Dan Ventura,”Robust Multimodal Biometric Fusion via Multiple SVMs”, Systems, Man and Cybernetics, ISIC, October 2007.

[11] Zhang, D., W.K. Kong, and M.Wong, Biometrics- online palmprint identification. IEEE Trans. Patt. Anal. Mach. Intell., 25: 1041-1050,2003.

[12] Sitalakshmi Venkataraman,”A Grid-Based Neural Network Framework for Multimodal Biometrics”, World Academy of Science , Engineering and Technology,2010.

[13] S.Valarmathy, M. A. Kumar, M. Sudha, “Improvement in palmprint recognition rate using fusion of multispectral palmprint images”, Proceedings of Int. Conf. on Computing Communication and Application (ICCCA), 2012.

[14] Weiping Chen and Yongsheng Gao,” A Minutiae-based Fingerprint Matching Algorithm Using Phase Correlation”, DICTA, 2007.

[15] Zhixin Shi , Venu Govindaraju,” A chaincode based scheme for fingerprint feature extraction”, Pattern Recognition Letters 27 , 2006.

[16] D. Zhang, W. K. Kong, J. You, and M. Wong,“Online palmprint identification,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 25, no. 9,pp. 1041–1050, Sep. 2003.

[17] X. Q.Wu, D. Zhang, and K. Q.Wang “Palm line extraction and matching for personal authentication,” IEEE Trans. Syst., Man, Cybern. A, Syst.,Humans, vol. 36, no. 5, pp. 978–987, Sep. 2006.

[18] F. Benhammadi, M. N. Amirouche, H. Hentous, K. Bey Beghdad, and M. Aissani, “Fingerprint matching from minutiae texture maps,” PatternRecognition, vol. 40, no. 1, pp. 189–197, 2007.

[19] K. N. Mutter, Z. M. Jafri, and A. A. Aziz, “Automatic fingerprint identification using gray hopfield neural network improved by run- length encoding,” International Conference on Computer Graphics, Imagingand Visualization, pp. 205–210, 2008.

[20] D. S. Huang, W. Jia, and D. Zhang, “Palmprint verification based on principal lines,” Pattern Recognit., vol. 41, no. 4, pp. 1316–1328, Apr. 2008.