International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 8
August 2017

Security And Privacy Aware Biometric Recognition System Using Multimodel Biometrics

[1]**Dr. M. Senthamil Selvi,** Professor and Head, Department of Information Technology,
Sri Ramakrishna Engineering College, Coimbatore, India
[2]**Mrs. J. Angel Ida Chellam,** Assistant Professor(Sr.Gr), Department of Information Technology,
Sri Ramakrishna Engineering College, Coimbatore, India

ABSTRACT

Security becomes the major problem in the real world application where biometrics based authentication can ensure the secured access permission. In the existing research method, secure advance system for fingerprint privacy protection by combining different biometrics fingerprint and face into a new identity is introduced. However, Authentication using the biometric is not produce better result in existing system where the more noises present in the test images would lead to failure of authentication. And face recognition result would be less accurate in case of some changes present in the test image like having beard etc. This is resolved in the proposed research method by introducing the novel framework namely Security and Privacy aware Biometric Recognition System (SPBRS). In the proposed system, finger print authentication result is improved by modifying the existing two-stage matching process. In the proposed research work triplets of minutiae is considered for the finger print authentication process. In this approach following features would be considered for the finger print authentication namely angles, triangle orientation, triangle direction, maximum side, minutiae density and ridge counts. And then face recognition is optimized by introducing the Locality Preserving Projections where face matching is done efficiently by preserving the locality structures. This method leads to quicker response time for matching the face features. The overall evaluation of the proposed research method is done in the MATLAB simulation environment from which it can be proved that the proposed research method leads to secured authentication than the existing research methods.

Keywords: Biometric authentication, Security, Privacy, Triplet miniature, locality based features, face recognition, finger print recognition

I. INTRODUCTION

In many Internet-based applications, remote authentication that establishes the identity of an entity under scrutiny is the first and the most critical link in the security chain. Reliable and secure authentication is thus of great importance [1]. Traditional security models for identity verification are based on passwords and tokens. However, passwords are relatively weak because they are liable to be guessed, shared or even stolen, and if a token is lost, it is likely that its finder will log on the system [2]. Biometrics [3] employs unique physical characteristics, e.g., fingerprints, irises, faces, hand geometry and hand-written signatures, as a testimony to verify an identity, thus setting up direct and strong links between physical persons and their identities that is difficult to guess or forge. Therefore, biometric authentication gains obvious advantages over the traditional security methods [4]. However, recognition based on any one of these modalities may not be sufficiently robust or else may not be acceptable to a particular user group or in a particular situation or instance.

Unimodal systems that use single biometric trait for recognition purposes suffer several practical problems like non-universality, noisy sensor data, intra-class variation, restricted degree of freedom, unacceptable error rate, failure to-enroll and spoof attacks. Therefore, the performance of single biometric system need to be improved, and the techniques of multimodal biometric system can offer a feasible method to solve the problems coming from single biometric system [5]. Multimodal biometric system makes use of different biometric traits simultaneously to authenticate a person's identity [6].

Biometric systems serve one of two foundational purposes either verification/authentication or identification [7]. Identification refers to the ability of a computer system to uniquely distinguish an individual from a larger set of individual biometric

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 8
August 2017

records on file (using only the biometric data). This is often referred as a "one-to many" match. Biometric verification or authentication involves a "one-to-one" search whereby a live biometric sample presented by an individual is compared to a stored sample previously given by that individual, and the match confirmed. The biometric system can also be attacked by the outsider or unauthorized person at various points. A biometric system can be either an 'identification' system or a 'verification' system, which are defined below.

Identification: Biometrics can be used to determine a person's identity even without his awareness or approval. Such as scanning a crowd with the help of a camera and using face recognition technology, one can verify matches that are already store in database. Verification: Biometrics can also be used to verify a person's identity. Such as one can allow physical access to a secure area in a building by using finger scans or can grant access to a bank account at an ATM by using retina scan.

II. RELATED WORKS

Abhishek Nagar[8] discussed that Security concerns regarding the stored biometric data is impeding the widespread public acceptance of biometric technology. In this work, it improved the recognition performance as well as the security of a fingerprint based biometric cryptosystem, called fingerprint fuzzy vault. The designed system incorporated minutiae descriptors, which capture orientation and frequency information in a minutia's vicinity, in the vault construction employing the fuzzy commitment approach.

Montesanto et al [9] designed a new algorithm for fingerprint verification based on local ridge discontinuities features (minutiae). They extract minutiae using two algorithms those following ridge lines and then recording ridge endings and bifurcations. Moreover they use a third algorithm are used for a minutiae verification processing a local area using a neural network (multilayer perception). Fingerprint distortion is filtered using a minutiae whole representation based on regular invariant moments. Here they designed a new method of matching for the problem of different numbers of minutiae extracted from the algorithms that use fuzzy operator to bypass. Sequential method and reactive agent is used in verification process of fingerprint matching.

He et al [10] introduce a novel algorithm based on global comprehensive similarity with three steps. In first step a minutia- simplex that contains a pair of minutiae as well as their associated textures, with its transformation-variant and invariant relative features. It is used for the broad similarity measurement and parameter estimation. To represent features among minutiae usually the ridge-based nearest neighborhood is used. The Euclidean space-based and ridge-based relative features among minutiae support each other in the image representation of a fingerprint.

Po and Korczak et al [11] designed a new hybrid biometric person authentication system using face and voice features. This prototype is based on several levels of abstractions: data representation and vectors and classifiers. Frontal face and text dependent voice biometrics are chosen to authenticate a user. For each of the biometric feature, an extractor, a classifier and a simple negotiation scheme have been designed. An extractor is made up of a sequence of operators which themselves are made up of signal processing and image processing algorithms. The face information is extracted using moments and the short speech information is extracted using wavelets. The extracted information, called vectors, is classified using two separate multilayer perceptrons. The results are combined using a simple logical negotiation scheme.

Chu et.al [12] introduced a face and palmprint fusion for personal identification based on ordinal features. To improve the identification performance the multimodal biometric identification method is introduced. Firstly, effective face and palmprint ordinal features are extracted for matching. By comparing with the templates stored in the database, the matching scores of each classifier (Hamming distance for AdaBoost Learning) are generated. Then, the scores output from the two classifiers are combined using several fusion strategies to give a unique matching score. Finally, a decision about whether to accept or reject a user is made.

III. SECURED AND PRIVACY AWARE BIOMETRIC RECOGNITION

Secured and privacy concerned bio metric recognition system is the most difficult task which needs to be done more concern for the improved security level. This is assured in the proposed

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 8
August 2017

research method by introducing the novel research method namely Security and Privacy aware Biometric Recognition System (SPBRS). In the proposed research method secured authentication is ensured by implementing the following steps:

- Finger print authentication using triplets of miniature
- Face recognition using Locality preserving projections

The proposed research method is explained in detail as follows:

3.1. FINGER PRINT AUTHENTICATION USIGN TRIPLETS OF MINIATURE DETAILS

In this work, we propose a two step fingerprint identification approach based on the triplets of minutiae. The features that we use to find the potential corresponding triangles include angles, triangle orientation, triangle direction, maximum side, minutiae density and ridge counts. In the first step, based on the number of corresponding triangles between the query fingerprint and the model database constructed offline, hypotheses are generated. In the second step, called verification, false corresponding triangles are eliminated by applying constraints to the transformation between two potential corresponding triangles.

3.1.1. Find required triangles

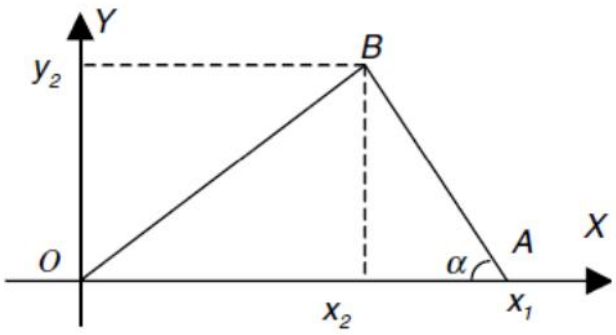

Figure 1. Illustration of variables

Figure 1 shows a triangle. Without loss of generality, we assume that one vertex, O, of the triangle is (0, 0), and it does not change under distortions. Since distance is invariant under translation and rotation and relatively invariant under scale and angles are defined in terms of the ratio of distance, it can be proved that angles are invariant under these transformations. However, in fingerprint recognition, because of the uncertainty of minutiae locations, which is associated with feature extraction and shear, the location of each minutia translates in a small local area randomly and independently. Suppose the locations of points A and B are $(x_1, 0)$ and (x_2, y_2), $x_1 > 0$, $y_2 > 0$ and $x_2 \in (-\infty, +\infty)$. Because of the uncertainty of minutiae locations, A and B move to A'$(x_1 + \Delta x_1, 0)$ and B'$(x_2 + \Delta x_2, y_2 + \Delta y_2)$, respectively, and α changes to $\alpha + \Delta\alpha$. Then

$$\tan\Delta\alpha = \frac{(x_1 - x_2)\Delta y_2 - y_2(\Delta x_1 - \Delta x_2)}{(x_1 - x_2)^2 + (x_1 - x_2)(\Delta x_1 - \Delta x_2) + y_2^2 + y_2\Delta y_2}$$

Suppose Δx_1, Δx_2 and Δy_2 are independent, and $-6 \le \Delta x_i, \Delta y_2 \le 6$, $i = 1, 2$ and Δx_i and Δy_2 are all integers, then

$$g(x_1, x_2, y_2) = E\{\Delta\alpha\} \approx \sum_{\Delta x_1=-6}^{6} \sum_{\Delta x_2=-6}^{6} \sum_{\Delta y_2=-6}^{6} (|\tan\Delta\alpha \times p(\Delta x_1)p(\Delta x_2)p(\Delta y_2)|)$$

Suppose $p(\Delta x_1)$, $p(\Delta x_2)$ and $p(\Delta y_2)$ are discrete uniform distributions in [-6, +6]. Let $0 < x_1, y_2, |x_2| < L$, where L is the maximum value of these variables in the image (in our experiments L = 300). We compute $g(x_1, x_2, y_2)$ at each point (x_1, x_2, y_2) based on whether α is the minimum, median or maximum angle in the triangle. Notice that, if $\alpha_{min} < \delta_\alpha$ or $\tau < \delta_\tau$, then the uncertainty of minutiae locations may have more effect on α_{min} and α_{med}, so we do not use these triangles in the model-base, where s is the minimum length of the sides in a triangle. Thresholds are $\delta_\alpha = 10^0$, $\delta_\tau = 20$. The features we use to find potential corresponding triangles are defined as:

Angles α_{min} and α_{med}: Suppose α_i are three angles in the triangle, $i = 1, 2, 3$. Let $\alpha_{max} = \max\{\alpha_i\}$, $\alpha_{min} = \min\{\alpha_i\}$, $\alpha_{med} = 180^0 - \alpha_{max} - \alpha_{min}$, then the label of the triplets in this triangle is: if the minutia is the vertex of angle α_{max}, we label this point as P_1; if the minutia is the vertex of angle α_{min}, we label it as P_2; the last minutia is labeled as P_3.

Triangle orientation Φ: Let $Z_i = x_i + jy_i$ be the complex number ($j = \sqrt{-1}$ corresponding to the coordinates (x_i, y_i) of point P_i, $i = 1, 2, 3$. Define $Z_{21} = Z_2 - Z_1$, $Z_{32} = Z_3 - Z_2$ and $Z_{13} = Z_1 - Z_3$. Let $\Phi = \text{sign}(Z_{21} \times Z_{32})$, where sign is the signum function and × is the cross product of two complex numbers.

Triangle direction η: Search the minutia from top to bottom and left to right in the fingerprint, if the

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 8
August 2017

minutia is the start point of a ridge or valley, then m = 1, else m = 0. g is the combination of m_i, m_i is the m value of point P_i, i = 1, 2, 3.

Maximum side λ: Let $\lambda = \max\{L_i\}$, where $L_1 = |Z_{21}|$, $L_2 = |Z_{32}|$ and $L_3 = |Z_{13}|$.

Minutiae densityχ: In a local area (32 · 32 pixels) centered at the minutiae P_i, if there exists n_χ minutiae, then minutiae density $\chi_i = n_\chi$. χ is a vector consisting of all χ_i's.

Ridge counts ξ: ξ_1 is the ridge count of the side P_1P_2, ξ_2 is the ridge count of the side P_2P_3, and n_3 is the ridge count of the side P_3P_1. ξ is a vector consisting of all ξ_i's.

If two triangles from two different fingerprints have the same feature values, then they are potential corresponding triangles.

3.1.2. Verify corresponding triangles

Suppose the sets of minutiae in the template and the query fingerprints are $\{(t_{m,1}, t_{m,2})\}$ and $\{(q_{n,1}, q_{n,2})\}$ respectively, where m = 1, 2, 3, . . . ,M, n = 1, 2, 3, . . . , N, M and N are the number of minutiae in the template and the query fingerprints respectively. Let Δt and Δq be two potential corresponding triangles in the template and the query fingerprints, respectively. The coordinates of the vertices of Δt and Δq are $(x_{i,1}, x_{i,2})$ and $(y_{i,1}, y_{i,2})$, respectively, and i = 1, 2, 3. Suppose $X_i = [x_{i,1}, x_{i,2}]'$, $Y_i = [y_{i,1}, y_{i,2}]'$, and the transformation $Y_i = F(X_i)$ between X_i and Y_i can be expressed as

$$Y_i = \begin{bmatrix} 1 & \delta h_x \\ \delta h_y & 1 \end{bmatrix} \begin{bmatrix} 1+\delta s_x & 0 \\ 0 & 1+\delta s_y \end{bmatrix} R.X_i + T$$

where $(\delta h_x, \delta h_y)$ and $(1 + \delta s_x, 1 + \delta s_y)$ are the shear and scale parameters;

$$R = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

θ is the angle of rotation between two fingerprints; and $T = [t_1, t_2]'$ is the vector of translation. Since $\delta h_x << 1$, $\delta h_y << 1$ and $\delta s_x \approx \delta s_y$, we can simplify Eq. (2) to

$$Y_i \, s.R. \, X_i + T$$

where s is the scaling factor. We can estimate the transformation parameters by minimizing the sum of the squared distances between the transformed query points and their corresponding template points. We compute

$$d = \underset{k}{\operatorname{argmin}} \left\{ \left| \hat{F}\left(\begin{bmatrix} t_{j,1} \\ t_{j,2} \end{bmatrix} \right) - \begin{bmatrix} q_{k,1} \\ q_{k,2} \end{bmatrix} \right| \right\}$$

If d is less than a threshold T_d , then we define the points $[t_{j,1}, t_{j,2}]'$ and $[q_{k,1}, q_{k,2}]'$ are corresponding points. If the number of corresponding points based on $\hat{F}(\hat{s}, \hat{\theta}, \hat{t}_1, \hat{t}_2)$ is greater than a threshold T_n, then we define Δt and Δq as the corresponding triangles between the template and the query fingerprints. The identification score is simply the number of corresponding triangles.

3.2. FACE RECOGNITION USING LOCALITY PRESERVING FEATURES

Face recognition technology has evolved as an enchanting solution to address the contemporary needs in order to perform identification and verification of identity claims. By advancing the feature extraction methods and dimensionality reduction techniques in the application of pattern recognition, a number of face recognition systems has been developed with distinct degrees of success. Locality Preserving Projection (LPP) is a recently proposed method for unsupervised linear dimensionality reduction. LPP preserve the local structure of face image space which is usually more significant than the global structure preserved by Principal Component Analysis (PCA) and linear Discriminant Analysis (LDA).

Locality Preserving Projections (LPP) are linear projective maps that arise by solving a variation problem that optimally preserves the neighborhood structure of the data set. LPP represents a linear approximation of the nonlinear Laplacian Eigen maps introduced. When high-dimensional data lies on a low dimension manifold embedded in the data space, then LPP approximate the Eigen functions of the Laplace-Beltrami operator of the manifold. LPP aims at preserving the local structure of the data. This is unlike PCA and LDA, which aims at preserving the global structure of the data. LPP is unsupervised and performs a linear transformation. It models the manifold structure by constructing an adjacency graph, which is a graph expressing local nearness of the data. This is highly desirable for face recognition compared to nonlinear local structure preserving, since it is significantly less computationally expensive and more importantly it is defined in all points and not just in the training points as Iso maps and Laplacian Eigen maps. Let x_i, i = 1, 2,… , n, denote the training patterns of m classes. We use $X = [x_1, x_2, \ldots, x_n]$ to denote the data matrix and use $l(x_i)$ to denote the label of x_i, say, $l(x_i) = k$ implies that x_i belongs to class k. LPP

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 8
August 2017

aims at preserving the intrinsic geometry of the data by forcing neighboring points in the original data space to be mapped into closely projected data. The algorithm starts by defining a similarity matrix W, based on a (weighted) k nearest neighbors graph, whose entry W_{ij} represents the edge between training images (graph nodes) x_i and x_j. Gaussian type weights of the form $W_{ij} = e^{-\frac{|x_i - x_j|^2}{t}}$ have been proposed in [23], although other choices (e.g., cosine type) are also possible. Based on matrix W, a special objective function is constructed, enforcing the locality of the projected data points by penalizing those points that are mapped far apart. Basically, the approach reduces to finding a minimum Eigen value solution to the generalized Eigen value problem.

ALGORITHM

Locality Preserving Projection (LPP) is one of the linear approximation obtained from the nonlinear Laplacian Eigen map [3]. The algorithmic procedure of LPP is stated below:

1) Construction of adjacency graph: Let G denote a graph with m nodes and an edge between nodes i and j, if x_i and x_j are close. There are two variations:

(a) ε-neighborhoods: Nodes i and j are connected by an edge if $\|x_i - x_j\|^2 < \varepsilon$, where the norm is the usual Euclidean norm in R^n .

(b) k nearest neighbors: Nodes i and j are connected by an edge if i is among k nearest neighbors of j or j is among k nearest neighbors of i .

2) Choosing the weights: We have two variations for weighting the edges. W is a sparse symmetric m×m matrix with W_{ij} having the weight of the edge joining vertices i and j, and 0 if there is no such edge.

(a) Heat kernel: If nodes i and j are connected, $W_{ij} = e^{-\frac{\|x_i - x_j\|^2}{t}}$

(b) Simple-minded: $W_{ij} = 1$, if and only if vertices i and j are connected by an edge.

3) Eigen maps: Compute the eigenvectors and eigen values for the generalized eigenvector problem:

$$XLX^T a = \lambda XDX^T a$$

Where D is a diagonal matrix whose entries are column (or row, since W is symmetric) sums of W, $D_{ii} = \sum_j W_{ji}$. $L = D - W$ is the Laplacian matrix. The i^{th} column of matrix X is x_i. Let the column vectors $a_0,\ldots,a_{l-1}$ be the solutions of equation (1), ordered according to their eigen values, $\lambda_0 <\ldots. \lambda_{l-1}$. Thus, the embedding is as follows:

$$x_i \rightarrow y_I = A^T x_i,\ A = (a_0, a_1, \ldots, a_{l-1})$$

Where y_i is a l -dimensional vector and A is a n×l matrix.

IV. EXPERIMENTAL RESULTS

To evaluate the performance of the proposed Security and Privacy aware Biometric Recognition System (SPBRS) and existing Secure Advance System for Fingerprint Privacy Protection (SAS-FPP) approaches, several parameters are used as such as false acceptance rate, genuine acceptance rate false rejection rate and accuracy.

FALSE ACCEPTANCE RATE (FAR):

FAR= Total false Acceptance /Total false Attempts

It defined as the probability of an impostor being accepted as a genuine individual. That is, in a biometric authentication system, the FAR is computed as the rate of number of people is falsely accepted (false people are accepted) over the total number of enrolled people for a predefined threshold.

FALSE REJECTION RATE (FRR)

It is defined as "the probability of a genuine individual being rejected as an impostor". That is, in a biometric authentication system, the FRR is computed as the rate of number of people is falsely rejected (genuine people are rejected) over the total number of enrolled people for a predefined threshold.

FRR= Total False Rejection/ Total True Attempts

4.1. DETECTION RATE

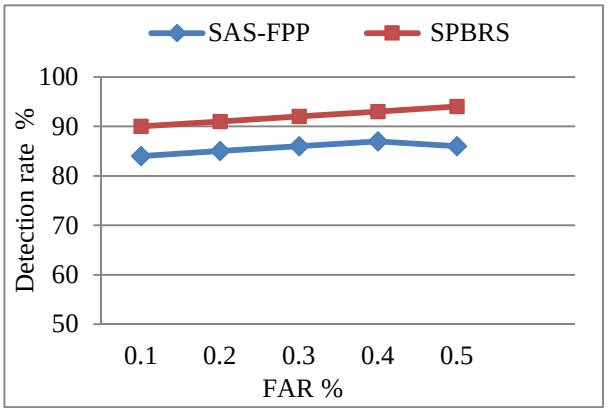

Figure 2. Detection Rate comparison

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 8
August 2017

Figure 2 compares the detection rate of the multimodal biometric system by using SPBRS approach and existing SAS-FPP approach. In x-axis false acceptance rate is taken and y-axis detection rate is taken. In this work, triplets of minutiae are considered for the finger print authentication process. It improves the detection rate. From the graph results, it is observed that, the proposed SPBRS is achieves better detection compared with existing methods.

4.2. FALSE ACCEPT RATE (FAR) VS FALSE REJECT RATE (FRR)

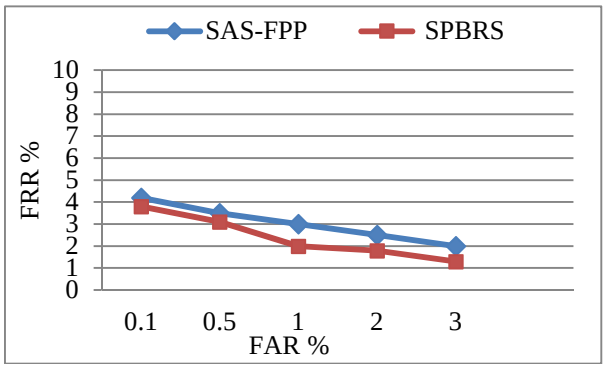

Figure 3. False reject rate (FRR) comparison

The comparison results of the proposed SPBRS approach and existing SAS-FPP approach in terms of false rejection rate shown in figure 3. In x-axis false acceptance rate is taken and y-axis false rejection rate is taken. In order produce more security; the face recognition is optimized by introducing the Locality Preserving Projections where face matching is done efficiently by preserving the locality structures. From the graph results, it is observed that, the proposed SPBRS is achieves better result compared with existing methods

4.3. GENUINE ACCEPTANCE RATE:

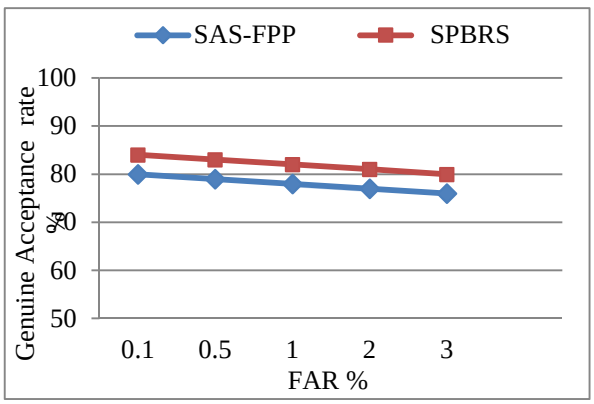

Figure 4. Genuine acceptance rate comparison

The comparison results of proposed SPBRS approach and existing SAS-FPP approach in terms of genuine acceptance rate shown in figure 4. In x-axis false acceptance rate is taken and y-axis genuine acceptance rate is taken. The GAR (1–FRR) is the fraction of genuine scores exceeding the threshold. It can be easily estimated from the ROC curves that the performance gain is very high as compared to the existing methods.

V. CONCLUSION

Biometric authentication is the most important application required by the various real world applications which need to be concentrated more to improve the security and flexibility of the system. This is ensured by introducing the novel framework namely Security and Privacy aware Biometric Recognition System (SPBRS). In the proposed system, finger print authentication result is improved by modifying the existing two-stage matching process. In the proposed research work triplets of minutiae is considered for the finger print authentication process. In this approach following features would be considered for the finger print authentication namely angles, triangle orientation, triangle direction, maximum side, minutiae density and ridge counts. And then face recognition is optimized by introducing the Locality Preserving Projections where face matching is done efficiently by preserving the locality structures. This method leads to quicker response time for matching the face features. The overall evaluation of the proposed research method is done in the MATLAB simulation environment from which it can be proved that the proposed research method leads to secured authentication than the existing research methods.

REFERENCES

[1] J.Wayman , A Jain, D. Maltoni, D.Maio, Biometric systems , Technology ,Degign Performance evaluation, Springer 2005.

[2] A.K.Jain, A.Ross and S.Prabhakar, “An introduction to biometric recognition “, IEEE Trans. On Circuits and Systems for Video Technology, vol 14, pp. 4-20, Jan 2004.

[3] Ajay K. and Venkata P., “Personal Authentication using Hand Vein Triangulation and Knuckle Shape,” IEEE Transactions on Image Processing, vol. 18, no. 9, pp. 2127-2136, 2009.

[4] Bounkong, S., Toch, B., Saad, D. and Lowe, D. (2003) ICA for watermarking digital images, Journal of Machine Learning Research, Pp. 1471-1498.

[5] R.W.Frischholz and U.Dieckmann,"Bioid: A Multimodal Biometric Identification System," IEEE Computer, vol-33,no-2, pp. 64-68, 2000.

[6] Monrose, F.,Rubin,A.D.,"Keystroke Dyanamics as a Biometric for Authentication" Future Generation computer systems, vol-16, no-4(2000) 351-359.

[7] A.K.Jain and A.Ross, "Learning User-Specific Parameters in a Multibiometric System",Proc. IEEE Int'1 conf. Image Processing , PP. 57-60, Sept. 2002

[8] Nagar, A., Nandakumar, K., & Jain, A. K. (2012). Multibiometric cryptosystems based on feature-level fusion. *IEEE transactions on information forensics and security*, *7*(1), 255-268.

[9] A. Montesanto, P. Baldassarri, G. Vallesi, G. Tascini, Fingerprints Recognition Using Minutiae Extraction: a Fuzzy Approach Image Analysis and Processing,2007.ICIAP 2007 Page(s):229-234

[10] Yuliang He, Jie Tian, Senior Member, IEEE, Liang Li, Hong Chen, and Xin Yang, Fingerprint Matching Based on Global Comprehensive Similarity, IEEE Transactions On Pattern Analysis And Machine Intelligence, Vol. 28, No. 6, June 2006.

[11] Poh, N., & Korczak, J. (2001, June). Hybrid biometric person authentication using face and voice features. In *AVBPA* (Vol. 1, pp. 348-353).

[12] Rufeng Chu, Shengcai Liao, Yufei Han, Zhenan Sun, Stan Z. Li and Tieniu Tan, " Fusion of Face and Palmprint for Personal Identification Based on Ordinal Features", 2007.