Certain Investigations on Continuous User Authentication System using Biometrics

S.Pravinth Raja
Assistant Professor(Sr.Grade)
Dept of CSE
Sri Ramakrishna Institute of Technology, Coimbatore

K.Umamaheswari, Ph.D
Professor
Dept of IT
P.S.G College of Technology, Coimbatore

B. Kokila
M.E Scholar
Dept of CSE
Sri Ramakrishna Institute of Technology, Coimbatore

ABSTRACT

In the past few years, Continuous Authentication system is most widely used verification system for personal computers. Continuous Authentication (CA) system verifies the user continuously once a person is logged in. Continuous Authentication system prevents the intruders from invoking the system. It passively verifies the system without interrupting the users work progress. CA system is based on both hard and soft biometrics. In this paper, a study on passive continuous Authentication system is carried out to analyze various techniques and their performance which was proposed by various researchers. Here e also proposed new model of CA system using fingerprint, face and cloth color. This proposed technique is implemented in our future work.

General Terms

Multimodal Biometrics, Pattern Recognition, Continuous Authentication Systems.

Keywords

Face Recognition, Fingerprint Recognition, and Soft biometrics

1. INTRODUCTION

Authentication is required in every computer system. Traditional method of authentication is
Classified into knowledge based and token based. Knowledge based e.g., passwords and token based e.g., smart cards and these are known to be conventional authentication [2].

But these are one time authentication. Once the password is known, anyone can access the system. Hence there are number of security flaws in the system.

Later biometrics was introduced for authentication. It is highly secured than traditional method. Instead of using token based and knowledge based one can use biometric for one time verification. Biometric is based on person's behavioral or physiological traits.

Physiological traits are face, fingerprint, palm, iris etc., whereas behavioral traits are keystroke, voice etc. Biometrics is broadly classified into hard and soft Biometrics. Hard biometrics refers to recognition of face, fingerprint, iris, and so on and soft biometrics refers to skin color, clothing, height etc. Hard biometrics is used to uniquely identify the person or object and soft biometrics does not differentiate the individual user.

The soft biometrics is required when the device is not able to

Recognize users face, fingerprint etc. Initially, biometric is used for one time authentication. Consequently there is no security after the user is logged in. To overcome such difficulties continuous verification is required.

CA is an authentication system which verifies the user and determine whether person is an authorized user or not and this can be done without interruption of users work. Such kind of authentication is done by using hard and soft biometrics. Biometric can be unimodal or multimodal. Unimodal is the use of single biometric for authentication. This leads to some problem like noise in the samples or unavailability of the observation [3]. To resolve such problems multimodal biometrics was introduced. Multimodal biometrics uses more than one modality for verification. Use of Multimodal biometrics can increase the accuracy and reduce vulnerability [17].Integration of modalities can also be done at different levels: sensor level, feature level, matching score level, decision level [15, 16, 21].

2. LITERATURE SURVEY

2.1 Continuous Authentication

2.1.1 CA Using Multimodal Biometrics

In this paper, Continuous authentication is made using two modalities i.e., face and fingerprint biometrics. Images of face and fingerprint are captured and each verifier observes the score of each modalities. These scores are integrated by Holistic fusion approach over time. Hidden Markov Model (HMM) [19] is used for integration which is sequence of states. The state may be {safe, attacked}. If the user is present in front of system, the state is safe. The state attacked represents that an imposter has taken the control [3]. They have used several metrics to measure the performance of CA system i.e. Time to Correct Reject, Probability of Time to Correct Reject, Usability, Usability-Security curve. Here usability is generally high for various activities and the imposter attacks are detected well within 3 seconds. The usability can also be improved by the use of keystroke dynamics. From the result obtained it is obvious the fingerprint is more reliable than face and the CPU time was 25 percent more when the continuous verification was turned on.

2.1.2 Soft Biometric Traits

Continuous authentication is done using soft biometric traits such as face color and color of user Clothing. In initial mode, face is detected. Histogram of the face color, histogram of cloth color and Eigen face representation are computed and stored as enrolled templates. The system tracks the face and the body separately based on histograms by applying mean shift algorithm. During continuous authentication, face and body identification is done. Similarities are calculated s and h the similarities between two histograms are calculated using Bhattacharyya method. Whether user is absent in front of observance. When there is change in illumination, enrolment template is updated. The system gets re-login and tries to re-authenticate when the user is no longer in front of console and this process is repeated [2]. No false accept rate and the false rejection rate is very low for different postures of user.

2.1.3 Interactive Artificial Bee Colony Supported Passive CA System

It is based on both hard and soft biometrics for Continuous Authentication. Initially face is detected through webcam using boosted classifier along with that skin color detection is made. Skin color detection module verifies whether the detected face region is human face. “1” indicated human skin pixel and “0” to represent non-skin pixel. When the face etection is done it is then sent to eye detection module which extracts left eye and right eye features. Face matching module compares the extracted features with the database. Eigen face method is used for Face Recognition and interactive artificial bee colony assist Eigen face to improve accuracy from **83.75 %** to **86.66%**. If there is match found with the ORL face database the user is genuine otherwise it checks for soft biometric match. Here cloth color is used for verification and if match is found system can be accessed otherwise system logs off [1]. This technique is able to operate with low system resource.

2.1.4 Temporal Integration

In this work, channel integration is not their primary goal, so they chose a simple naive Bayes classifier to handle channel integration as a binary classification problem incorporating uncertainty measures. Similarity scores from individual biometric channels are normalized to the interval [0*;* 1] and integrated using the Bayes classifier. Their temporal integration method generates an expected score distribution and an estimated related uncertainty about this distribution. They weight class priors by the associated uncertainty before classification. It should be noted that weighting class priors would not scale well with larger data sets presenting a potential limitation, especially since they are concerned with real-time operation.

Logically, they have the choice of first integrating temporally or over channels (horizontally or vertically). Perhaps the best approach, but also the most complex to formulate, is to integrate in both directions (across channels and across time) simultaneously, rather than sequentially.

Just as in integrating channels, for temporal integration they can choose to integrate information at level of features, scores, or decisions. Their method works in continuous time by computing expected values of scores as a function of time difference between the last observation and current time. The main idea is based on the assumption that an authentication score is still valid for some amount of time, ±*t*. As time passes, they should be less and less certain about this value. To formulate this idea as a function of time they estimate an uncertainty measure of scores per channel from the recent past, until a new observation is recorded. The joint posterior distribution of a score is approximated and then propagated over time until they obtain a new score from that channel. Due to the propagation of the score distribution over time, they use a degeneracy model for the uncertainty measure of each score [12].

Naturally, they would prefer their integration method to be as general as possible. On the other hand, the later the integration, the more information is discarded, so early integration may achieve better results, using an appropriate set of features.

2.1.5 Fuzzy Approach

CA exploits two biometric modalities such as face and fingerprint. These modalities are controlled by fuzzy controller which evaluates trust value. Initial authentication is carried out by entering password and then it is moved to biometric authentication. The system identifies the face on the basis of face recognition matching value BIOFACE. BIOFACE is compared with the threshold value, if it is below the threshold then fingerprint acquisition is required. Fingerprint matching value BIOFINGER is calculated. Both BIOFACE and BIOFINGER is sent to fuzzy controller [13]. Fuzzy controller computes and determines any of the following options:

1) When the trust value is too low, it ends the session.

2) When trust value is low and if ti requires further confirmation, new acquisition of face and fingerprint is carried.

3) Trust value is high to trust the face recognition, new face acquisition is performed and this process is repeated.

2.1.6 Temporal Information

In this paper, they monitor the logged in user by face and cloth color. In addition to face information, cloth color is used as enrolment template. System automatically registers the user information when logged in [14]. For CA, three criteria are considered:

Usability: Re-authentication of the user is not required when the user is in front of console.

Security: Re-authentication is required when user moves away from front of console.

Cost: Cost is one of the important factors. Hence, to authenticate the system they use only the standard devices (keyboard, mouse, webcam).

Pre-registration of user require users posture in order to capture image. Instead, this method registers a new enrolment template in mode 1. In mode 2, system verifies whether the user is in front of console or not. If the user moves away from the console, the mode is switched to the next. In mode 3, the system is terminated (e.g., logs off).

2.2 Face Recognition

2.2.1 Symmetric Local Graph Structure (SLGS)

SLGS is the local graph structure where each pixel represents the graph structure of other pixel. SLGS represent same number of left and right hand pixel. For Recognition nearest neighbour classifier was used which includes Euclidean distance, correlation coefficient and chi square measure. SLGS extracts the texture information. It is robust to facial expression, facial detail, and illumination. Accuracy of recognition is 99.73% [6].

2.2.2 Generalized Weber Face

Weber face is based on Webers law which extracts multi scale information from face image. This assigns weights to inner and outer ground and it is to be known as Weighted GWF. By selecting weights it eliminates un discriminate parts. It is robust to illumination changes and the recognition rate is 99.48% [5].

2.2.3 DCT Pyramid

Discrete Cosine Transform is used to extract features by decomposing the image into various sub bands. By repeated decomposition, it creates a pyramid of images to form feature vector to describe texture of image. This method is used to recognize the face with low computation complexity and low memory requirement [10].Its recognition rate is 89.9% for FERET database.

Table 1: Face Recognition Rate

METHOD	**RECOGNITION RATE (%)**
SLGS	97
LGS	96
DCT PYRAMID	95.7
WGWF	98.64
EIGENFACE WITH PCA	83.75
IABC WITH EIGENFACE	86.88

Table 1 above shows various method of face Recognition and its Rate of Recognition.

2.2.4 Eigen Face

Here face image is decomposed into set of feature images called Eigen faces. In the testing phase, face is treated as column vector and each entry corresponds to pixel of the image. The image vector is normalized with average image.

The Eigen vector of covariance matrix is indentified for the normalized face. The Eigenvector is multiplied by each of the face vectors. Threshold is computed by using maximum distance between any two projection. In recognition phase, face is normalized with the average face and projected onto face space. Euclidean distance is calculated between projections. This minimum value is selected and compared with threshold value. If the value is above the threshold face is new otherwise face is familiar [11].

2.3 Fingerprint Recognition

2.3.1 Incomplete FR using Feature fusion and pattern Entropy

Fingerprint recognition might suffer from Incomplete Fingerprint. To overcome these difficulties, feature of Minutiae and orientation field is extracted and it is fused so that it become robust to scale and rotation. Pattern entropy technique is used to measure the similarity and it Eliminates the false matches. Pattern entropy is done by using Gaussian weights [7].

2.3.2 Minutiae based Geometric Hashing

This paper , uses indexing and searching technique. Model fingerprint is pre-processed and core points in Minutiae are extracted. From those false minutiae is removed. Indexing technique is used to represent the feature vector from model fingerprints into hash table. It does not maintain redundant information. During searching feature are extracted and processed and it is searched with the database in the hash table to find the match [8]. Minutiae Binary Patterns are used to identify the exact match from the database.

2.3.3 Fingerprint Classification

Complex filters are used to detect the singularities in the fingerprint. It detects core and delta points and provides type, position, direction and certainties of singularity. Fingerprint classification which is known as adaboost classifier is used to combine the singularity information to extract as many features [9].

2.3.4 Indexing

Fingerprint indexing is a key technique in Fingerprint identification system. This is the extension of Delaunay triangle. Using minutiae of the fingerprints, triangle set is constructed and it is refined. In the index stage, feature vectors are extracted from the triangles and stores in the index table. From the computed triangles, many of the triangles are eliminated due to bad quality zones. In retrieving stage, query impression is compared with the list of indices and the best match is found. This narrows the search space [4]. The method is robust to distortion than other triplet based algorithm. Correct Index Power is one of the most used measures for evaluating Indexing algorithm.
Correct Index Power and the Penetration Rate are expressed as:

$$CIP(N) = 100 * c(N)/E$$

$$PR(N) = 100 * N/E,$$

where E is the number of experiments and c(N) is the number of times where the correct result is within the list with the first N hypothesis. These are the few fingerprint algorithm for recognition.

2.4 Soft Biometric Recognition

Soft biometrics could be gender, height, color of eye, hair, cloth, gait or other features. Though soft biometrics does not provide uniqueness for identification of a person it helps to identify without cooperation. By using multiple data, recognition can be done.

Soft biometrics work together with hard biometrics to identify and ensure better result.

Hard biometrics is difficult to recognize at a distance but soft can work in different environment. Single information is not sufficient to identify, it can be identified by combining using multimodal biometric method. One of the techniques for recognition of cloth color is done through quantization based on octree.Other technique which is popular to measure the similarity is Bhattacharya coefficient. It is based on the color histogram to correlate object by using spatial information or be spectral features.

3. PROPOSED METHOD

In the recent Continuous Authentication research work, face and soft biometric was used for authentication. Indeed, the uniqueness of fingerprint is high when compared with face and soft biometrics. In concern to this we go for fingerprint recognition as the initial modality. We have proposed Continuous Authentication System with different modalities. The modalities include both hard and soft biometrics. Fingerprint is captured using fingerprint mouse when the user is operating mouse. By fingerprint recognition algorithm features are extracted and it is verified with the images in the database. If exact match found, user is genuine. If no match found or fingerprint is not recognizable, authentication is done through face recognition module. This is by capturing frames through webcam. By face recognition algorithm features are extracted and compared with the face database. If exact match found person is authorized. In case the input face is not recognizable then the process is switched to soft biometrics.

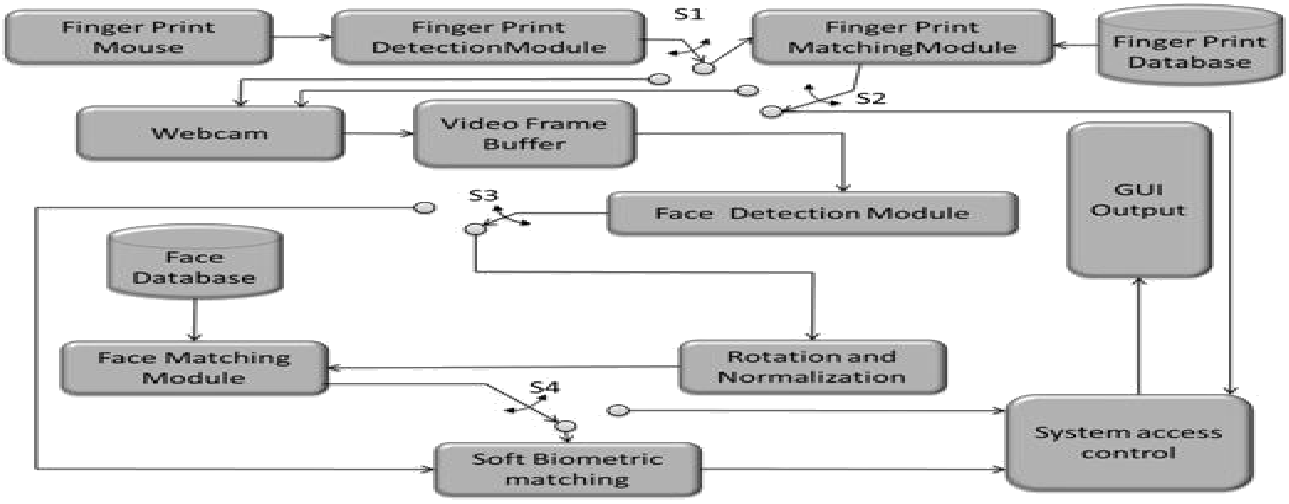


Fig.2. Architecture of Proposed System

Soft biometrics recognition is done using cloth color. This can be achieved through Bhattacharya coeffient [18] by using color histogram. Number of color pixels for various ranges are chosen and verified. Soft biometrics like cloth color is for temporary verification because same color cloth is used only for a day. It also does not require huge database. If all the modalities fail the person is recognized as imposter, consequently the system logs off.

Figure 2 shows the architecture of the proposed Continuous Authentication system after the investigation of various papers.

Pre-Processing

It is the first step after image acquisition. It involves removing noise, normalizing the intensity of the image, removing reflection. It is the used for enhancing image. Pre-processing can be done using various technique such as Image Re-sampling, Noise Removal such as Spatial Filtering, Mean Filtering, Median filter. Manual corrections can be processed using lines and splines, Pixel by pixel and many other methods.

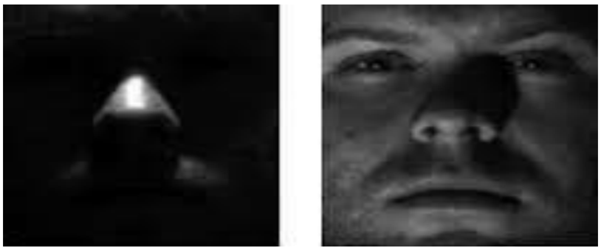


Fig 3: Image Before and After Pre-processing

Segmentation

Segmentation is needed for improving analysis of an image. It is Labelling the pixels of the image according to semantic content. Segmentation involves Remove unwanted region, Finds boundary between regions, partitioning of image into non-overlapping regions. Algorithms involved in segmentation are C-Means, K-Means, Fuzzy C-Means, Fuzzy K-Means, Adaptive Fuzzy K-Means, Rough Set based Fuzzy K-Means.

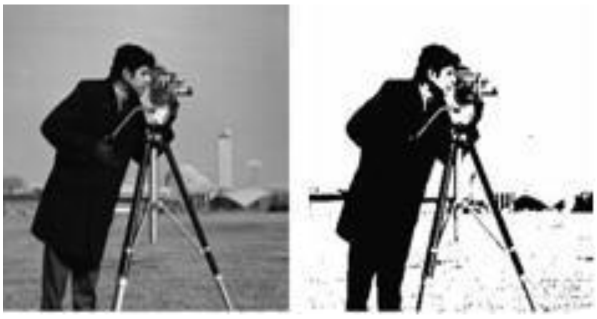


Fig 4: Image Before and After Segmentation

Classification

Classification categories detected objects into predefined classes using suitable method that compares image template with the target template. Some of the techniques include Support Vector Machine SVM, HMM, Minimum Distance Classifier, Maximum Likelihood Classifier, Decision tree, Bayesian Formalism, Artificial Neural Networks.

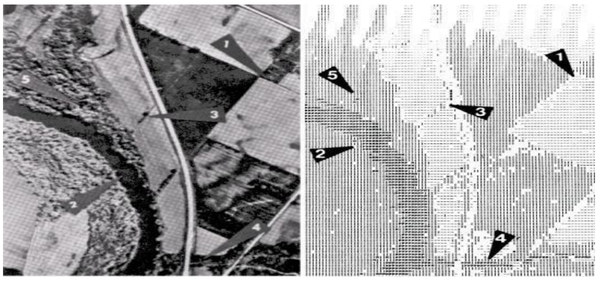


Fig 5: Image Before and After Classification

Initial login is done through fingerprint device. For continuous authentication, Fingerprint is captured using fingerprint Optimouse Plus while operating mouse. Histogram equalization is done to enhance the captured image. Image segmentation Region of Interest is applied to extract the features and false minutiae are removed. After extracting minutiae, scores are calculated and compared with the database. If exact match found, user is genuine. If no match found or fingerprint is not recognizable, authentication is done through face recognition module. This is by capturing frames through webcam. Face is detected using face detection algorithm.

By Symmetric local graph structure (SLGS), features are extracted. SLGS represent the relationship between neighbouring pixels. Centre pixel is surrounded with same number of pixel on the left and right. Figure 2 shows the SLGS operator [6]. After extracting features it is compared with the database. If exact match found person is authorized. In case the input face is not recognizable, then the process is switched to soft biometrics.

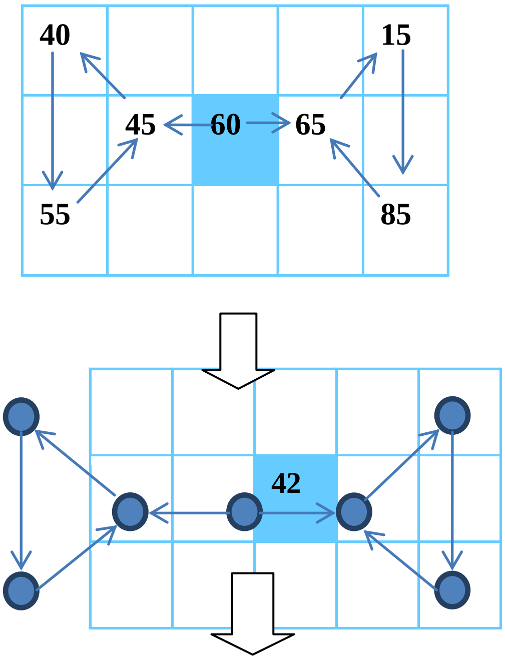
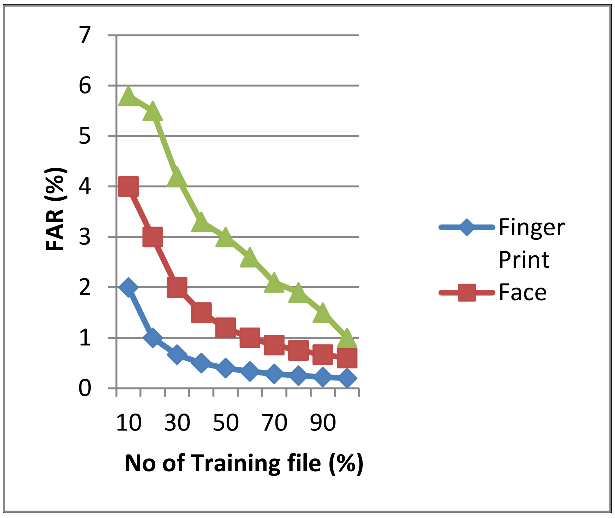


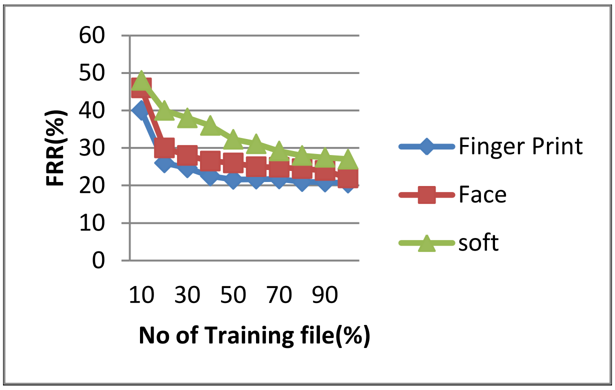
Fig.6. SLGS Operator

Soft biometrics recognition is done using skin and cloth color. This can be achieved through Bhattacharya coefficient (bhattacharya 1943) by using color histogram. Number of color pixels for various ranges are chosen and verified. Soft biometrics like cloth color is for temporary verification because same color cloth is used only for a day. It also does not require huge database. If all the modalities fail the person is recognized as imposter, consequently the system logs off. Figure 3.1 shows the architecture of the proposed Continuous Authentication system based on the survey.

4. EXPERIMENTAL RESULTS

Experiment was conducted to analyze the performance of each modalities and overall effectiveness of Multimodal biometrics. Performances of fingerprint, face and soft biometrics are evaluated using False Acceptance Rate FAR and the False Rejection Rate FRR. Test was conducted using different number of training files. FAR is the percentage of illegal users that are accepted as genuine. FRR is the percentage of legal user rejected as imposter. From the result, FAR and FRR is high for small number of trained samples. As the number of training samples increases, FAR and FRR is reduced.





5. CONCLUSION

System is vulnerable to the loss of data or attacks even if it secured with password. When the system has privacy information, to prevent from attacks continuous authentication system plays vital role. Lots of work related to continuous authentication has been done. We propose a new model of continuous authentication using face, fingerprint and color of clothing. Technique used for face recognition is Weighted Generalised Weber Face WGWF and for fingerprint Minutia based Geometric hashing. TO achieve these recognition, Rough set based Fuzzy k-Means is used for segmentation and HMM is applied for classification of image. Color Histogram of soft biometric is through Bhattacharya Coefficient. By applying these methods we enhance Continuous Authentication system and try to obtain better result other than state-of-art method.

6. REFERENCES

[1] Pei-Wei Tsai, Khan M.K, Jeng-Shyang Pan, Bin-Yih Liao"Interactive artificial Bee Colony Supported passive Continuous Authentication System," IEEE Systems Journal, vol.8 No.2 , june 2014.

[2] K. Niinuma, U. Park, and A. K. Jain, "Soft biometric traits for continuous user authentication," *IEEE Trans. Inform. Forensics Security, vol.*5, no. 4, pp. 771–780, Dec. 2010.

[3] Terence Sim, Sheng Zhang, Rajkumar Janakiraman, Sandeep Kumar, "Continuous Verification Using Multimodal Biometrics,“ IEEE Trans On Pattern Analysis and Machine Intelligence, Vol 29, No 4, April 2007.

[4] Alfredo Munoz-Briseno, Andres Gago-Alonso,JoseHernandez-Palancar,"Fingerprint indexing with bad quality areas," Expert Systems with Applications, 1839–1846, 2013.

[5] Yong Wu , Yinyan Jiang, Yicong Zhou , WeifengLi , Zongqing Lu , QingminLiao, "Generalized Weber-face for illumination-robust face recognition," NeuroComputing 2014.

[6] Mohd Fikri Azli Abdullah , Md Shohel Sayeed, Kalaiarasi Sonai Muthu, Housam Khalifa Bashier, Afizan Azman, Siti Zainab Expert Systems with Application 41 (2014) 6131–6137.

[7] ZHANG Jie, JING Xiao-jun, CHEN Na, WANG Jian-li, " Incomplete fingerprint recognition based on feature fusion and pattern entropy," The Journal of China Universities of Posts and Telecommunications, June 2014.

[8] Umarani Jayaraman N, Aman Kishore Gupta,PhalguniGupta, "An efficient minutiae based geometric hashing for fingerprint database," Neuro Computing 137(2014) 115–126.

[9] Manhua Liu, "Fingerprint classification based on Adaboost learning from singularity features," Pattern Recognition 43 (2010) 1062 – 1070.

[10] Randa Atta, Mohammad Ghanbari, "Low – Memory Requirement and Efficient Face Recognition System Based on DCT Pyramid," IEEE Trans on Consumer Elecronics, Vol 56, No.3, August 2010.

[11] M. Turk and A. Pentland, "Eigenfaces for recognition," Int. J. Cognitive Neuroscience, vol. 3, no. 1, pp. 71–86, 1991.

[12] A. Altinok and M. Turk, "Temporal integration for continuous multimodal biometrics," in Proc. Workshop on Multimodal User Authentication, 2003, pp. 131–137.

[13] Antonia Azzini, StefaniaMarrara, Roberto Sassi and Fabio Scotti, "A fuzzy approach to multimodal biometric continuous authentication, "Fuzzy Optimal Decision Making, vol. 7, pp. 243-256, 2008.

[14] Koichiro Niinuma, Anil K. Jain, "Continuous User Authentication Using Temporal Information," proc. SPIC7667 Biometric Technology of Human Identication, April 14, 2010.

[15] Cimato, S., Gamassi, M., Piuri, V., Sassi, R., &Scotti, F, " Personal identification and verification using multimodal biometric data," IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety, pp. 41– 45,2006.

[16] Hong, L., & Jain, A, Multimodal biometrics chapter 16 In A. Jain, R. Bolle, & S. Pankanti (Eds.), *Biometrics: Personal identification in networked society*. Norwell: Kluwer Academic Publishers, 1999.

[17] A.Ross and A.K.Jain, „ Information Fusion in Biometrics," Patters Recognition Letters, vol 24, no 13,pp, 2115-2125, 2003.

[18] A. Bhattacharyya, "On a measure of divergence between two statistical populations defined by their

probability distributions," Bull. Calcutta Math .Soc., vol. 35, pp. 99–109, 1943.

[19] L.R. Rabiner,"A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition," Proc. IEEE, vol. 77, no. 2, pp. 257-286, 1989.

[20] P.-W. Tsai, J.-S.Pan, B.-Y.Liao, and S.-C. Chu, "Enhanced artificial bee colony optimization," *Int. J.* Innovative Comput. Inform. Control, vol. 5, no. 12, pp. 5081– 5092, Dec. 2009.

[21] S S. Pravinthraja*, Dr.K. Umamaheswari, "A Survey on Multimodal Biometrics," Int. J. Engineering and Technology Research, Volume-1, Issue-2, October-December, 2013.