International Journal of Pure and Applied Mathematics
Volume 117 No. 15 2017, 1129-1142
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

CONTINUOUS AUTHENTICATION SYSTEM USING MULTIPLE MODALITIES

B.Kokila	S.Pravinthraja	K.Saranya	S.J Savitha	N.S.Kavitha
Kokila.sai10@gmail.com	pravinthraja@gmail.com	Saranyak249@gmail.com	Savithaj12@gmail.com	nsksrit@gmail.com

Abstract:

Biometric identifiers are the unique, measurable characteristics used to label and describe each person. In the past few years, Continuous Authentication system is widely used verification system in biometrics to secure personal computers. Continuous Authentication system helps the PC user to check their system continuously when third 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. Continuous Authentication system is based on both hard and soft biometrics. A study on passive continuous Authentication system is carried out to analyse various techniques proposed by various researchers.Here a new model of passive Continuous Authentication system has been proposed using multimodal biometrics such as fingerprint, face and soft biometrics. Fingerprint images are captured through fingerprint mouse. Fingerprint, Face and soft recognition were implemented and their performances are evaluated.

Keywords: Key terms: Face Recognition; Fingerprint Recognition; Soft biometrics.

I INTRODUCTION

Security is the major concern in every field. Attacks to the system can come from different mode. One of the ways to provide security is through authenticating the user. Authentication facilitate to prevent from direct attacks i.e., Fake users using the system and access information. Authentication can be carried out by using various techniques. Traditional means of authentication is by providing system with user Name and password. Still the traditional way is utilized in day to day life. Traditional authentication is one time authentication. If the fake user knows the password, one can enter into the system and access information. Knowledge based and token based are the common approaches utilized to provide security. But these approached have number of flaws.(eg., password can be stolen,

forgotten because each person is provided with different account and to keep those account safer they end up with complex passwords). Those passwords are difficult to remember though they are secure [2]. Toovercome these issues biometric authentication is more secure when compared to conventional methods. Biometric authentication does not require user to remember passwords or to have smartcards. It is by authenticating user by using person's own physiological and behavioural traits. These traits are unique for each person. Physiological traits are face, fingerprint, palm, iris etc. Authentication is done by verification process by comparing the user's information with the templates stored in the system.

Initially biometric is also used for one time authentication. System cannot provide security after the person logs in with correct identity. Because authorized person might go for a break without proper shutdown of the system. Hence unauthorized person can utilize the system. To prevent the system from such attacks we go for continuous authentication. Continuous authentication system verifies the user throughout the work process by different mode of authentication. It can be through face, fingerprint, soft biometrics recognition. Soft biometric refers cloth color, color of eye, hair etc. It is not as unique as hard biometrics i.e., face, fingerprint. It can be used along the hard biometrics for authentication. In earlier stages, continuous authentication is done using unimodal biometric. Nowadays it is carried out with multimodal biometrics. In multimodal biometrics, integration of these modalities can be performed at sensor level, feature level, match score level, decision level.

II. LITERATURE SURVEY

Works related to Continuous Authentication

Pei-Wei Tsai et al. proposed Continuous authentication by both hard and soft biometrics i.e. face and skin color. Here the face is detected through webcam by utilizing boosted classifier at the same time skin color detection is made. Skin color detection module verifies whether the detected face region is human face. "1" denoted human skin pixel and "0" to represent non-skin pixel.Face matching module compares the extracted features with the database. Eigen face method is utilized for Face recognition and interactive artificial bee colony optimization algorithm helps to assist Eigen face to improve the recognition rate from 83.75% to 86.66%. They conclude that the user is genuine when there is match between training and testing face or else the system checks for soft biometric match. Here cloth color is utilized 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.

Terence Sim et al. proposed Continuous authentication using face and fingerprint biometric modalities. Images of theface were captured using webcam and fingerprints through fingerprint device. Verifier computes the score of each modality. These scores are integrated by Holistic fusion approach using Hidden Markov Model (HMM) [19]. Finally the system observe two set of states {safe, attacked} for time t=1, 2.. If the authorized user was present in front of the system, then state was said to be safe. The state attacked represents that an imposter has taken the control [3]. They measured the performance of CA system using different metrics 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. From the result obtained it was proved that the fingerprint is more reliable than face and the CPU time was 25% more when the continuous verification was turned on.

Antonia et al. proposed CA by using two biometric modalities such as face and fingerprint. These modalities are controlled by fuzzy controller which tends to calculate the trust value. The initial phase of authentication is carried as a traditional mode of authentication by entering password and then proceeds with the biometric authentication. The system identifies the face on the basis of face recognition matching and BIOFACE value is calculated. 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:

- Trust value is high to trust the face recognition, new face acquisition is performed and this process is repeated.
- When the trust value is too low, it ends the session.
- When trust value is low and if it requires further confirmation, new acquisition of face and fingerprint is carried.

Niinuma et al. proposed continuous authentication using soft biometric traits such as face colorand color of user Clothing. Detection of face is considered to be initial phase where the histogram of the face color, cloth color and Eigenface 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 and similarities are calculated as $\boldsymbol{S_{softface}}and\boldsymbol{S_{clothes}}$.

Bhattacharyya coefficient was used to calculatethe similarities between two histograms where $T_{cont}$is the threshold value. If $S_{cont} < T_{cont}$ it checks for illumination changes or absence of user 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.

Niinuma et al. uses the continuous authentication by monitoring the logged in user with the help of face and cloth color. In addition to face information, cloth color is used as enrolment template. System spontaneously registers the user information when the user is logged in. Pre-registration of user require user's 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 order to log off the system [14].

III 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. Based on this, fingerprint recognition is considered as the initial modality. A new model of Continuous Authentication System has been proposed. The modalities include both hard and soft biometrics.

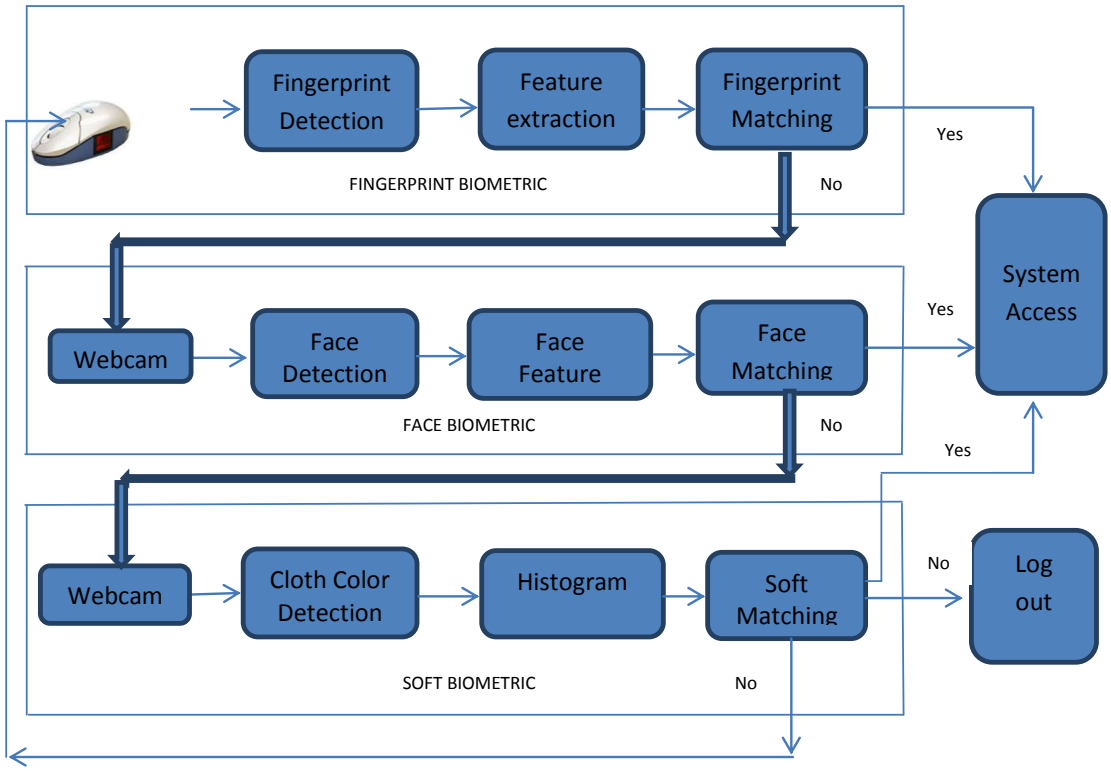

Fig.1. Architecture

Fig. 1 shows the architecture of continuous authentication system.Initial login of the system is done through fingerprint device. For continuous authentication, Device which is used for fingerprint extraction is Secugen fingerprint optimouse plus. While operating personal computer through mouse our fingerprint image is captured and series of minutiae matching algorithm is carried out as in Fig. 2.

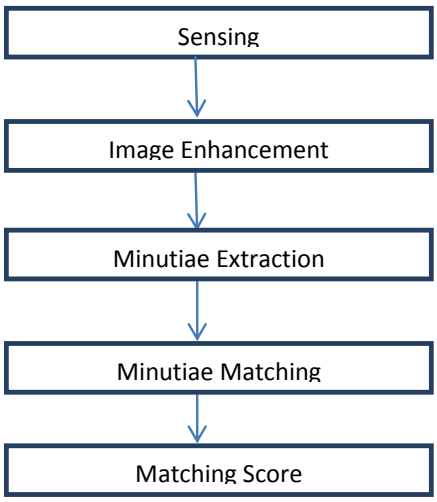

Fig.2. Steps for fingerprint recognition

Once the image is acquired, it is preprocessed by applying image enhancement technique through histogram equalization, binarization and thinning. The result of pre-processed stage is then moved to feature extraction. Feature extraction is done by minutiae based approach which uses ridges and valleys. From thinned fingerprint image we extract ridge endings and bifurcation by considering 8 neighbourhood pixel of each block. The extracted features are then applied to false minutiae removal to remove the invalid ridges, after successful extraction of minutiae we evaluate the score by applying by applying the formula

$$\text{Matching Score} = \frac{\text{Number of matched minutiae}}{Maximum\ \ number\ \ of\ minutiae} * 100\% \qquad (1)$$

If exact match found, user is genuine. If no match found or fingerprint is not recognizable, authentication is done through face recognition module.

In face recognition module, by using webcam images of the person are captured at the specific time interval when the video mode is turned on. From the captured image, face is detected using face detection algorithm. By Using Symmetric local graph structure (SLGS), features of face are extracted. SLGS has the symmetric graph structure which represents the relationship between neighbouring pixels. Centre pixel is surrounded with three pixels on the left and three on the right. Each pixel on both sides is compared with the pixel at the centre to obtain binary value. New value is obtained from the binary value for each pixel and histogram is generated for the new value. This algorithm is useful for extracting the texture information on left and right side. Fig. 3 shows the SLGS operation [6]. After extracting features of the faceit is compared with the trained set. Histogram which is generated for the training set is stored in the database. Euclidean distance is used for feature matching. If testing sample matches with the trained sample then the person is verified as an authorized user. In case the input face is not recognizable, then the process is switched to soft biometrics.

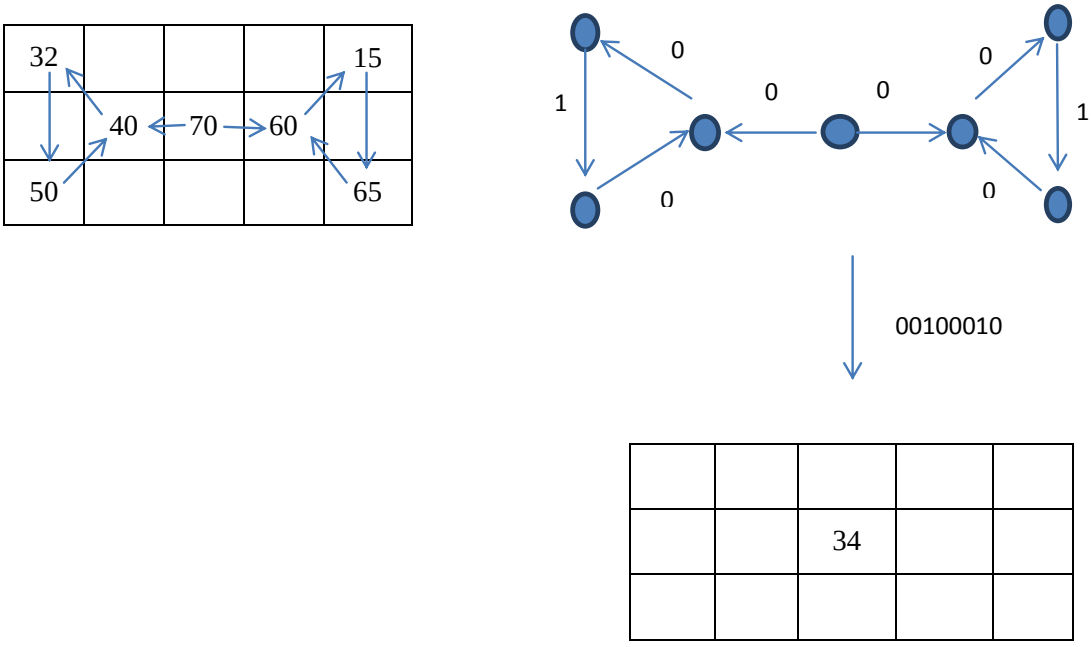

Fig.3. SLGS Operator

Soft biometrics recognition is done using skin and cloth color. This can be achieved through Bhattacharya coefficient [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. When the cloth color does not match with database person is known to be as imposter, consequently the system logs off. If is person is matched with the trained sample then he is said to be authorized so that he can access the system. This process of verification is carried out until the user shutdowns the system.

IV EXPERIMENTAL RESULT

We analyse the performance of each modalities to check effectiveness of Multimodal biometricsand the graph is plotted. 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. Therefore we obtain less FAR and FRR for testing large set of samples.

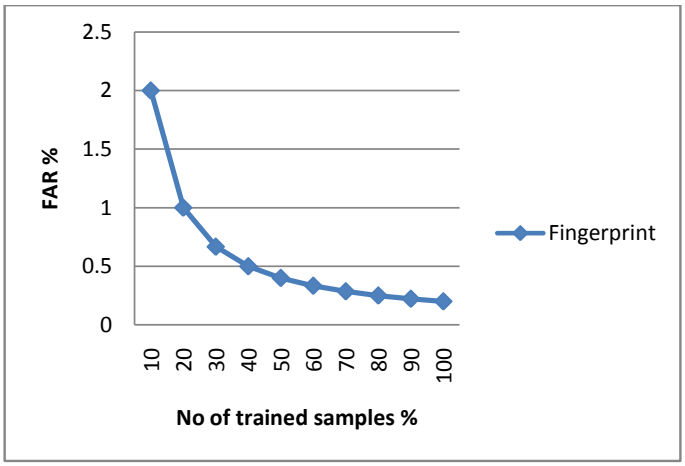

Fig.4. FAR of fingerprint Recognition

In Fig. 4, False Acceptance Rate of fingerprint recognition is shown against number of trained files. Here maximum of above 100 images are considered. When the number of trained sample increases the percentage of false acceptance rate reduces.

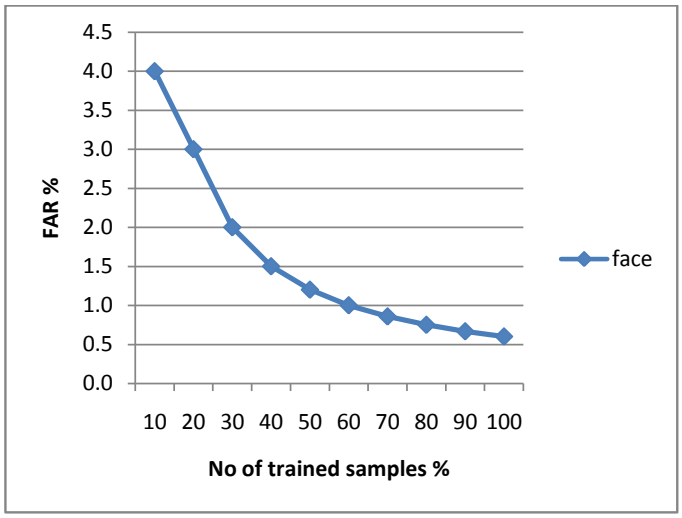

Fig.5. FAR of Face Recognition

In Fig. 5, False Acceptance Rate of face recognition is shown against number of trained files. For the 10 number of trained samples the FAR is 4.0 %, whereas when the trained sample increases to 80 FAR is reduced to 0.7percentage.

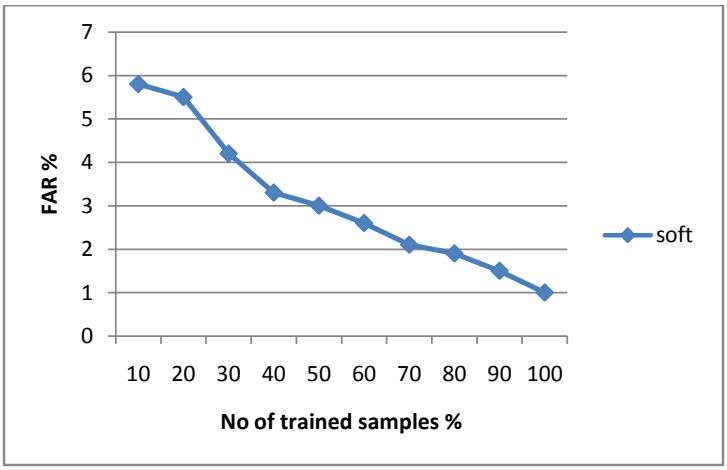

Fig.6. FAR of Soft Biometric Recognition

In Fig. 6, False Acceptance Rate of cloth recognition is shown against number of trained files. For the 10 number of trained samples the FAR is 4.0 %, whereas when the trained sample increases to 80 FAR is reduced to 0.7 Percentage.

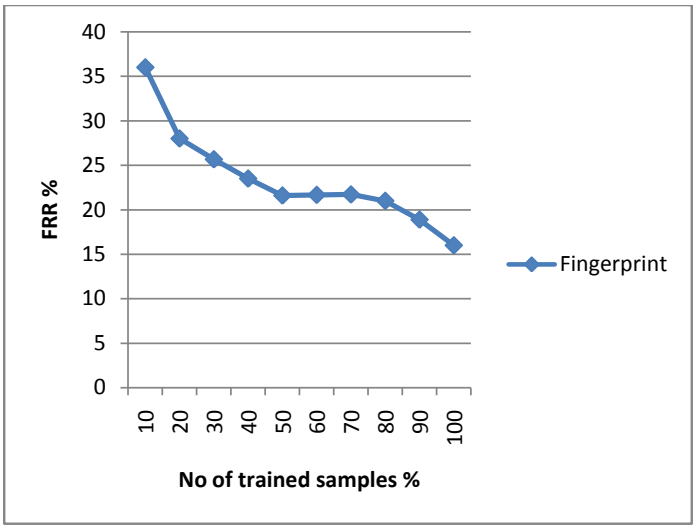

Fig.7. FRR of fingerprint Recognition

In Fig. 7, False Rejection Rate of fingerprint recognition is shown against number of trained files. Here maximum of above 100 images are considered. When the number of trained sample increases the percentage of false acceptance rate reduces.

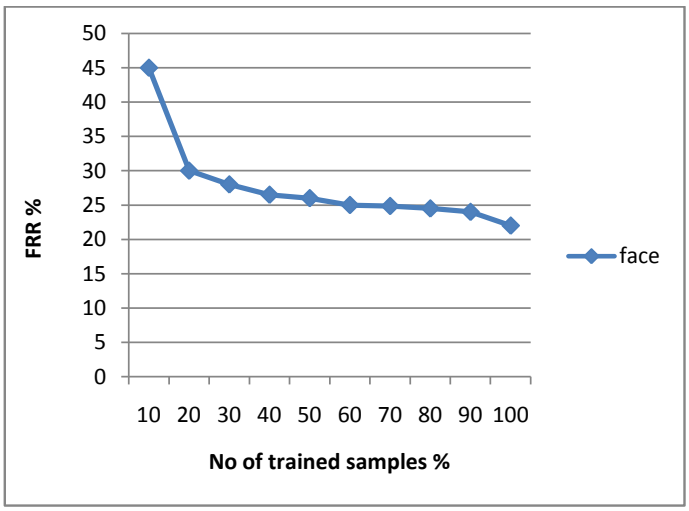

Fig.8. FRR of Face Recognition

In Fig. 8, False Rejection Rate of face recognition is shown against number of trained files. When the number of trained sample increases the percentage of false acceptance rate reduces.

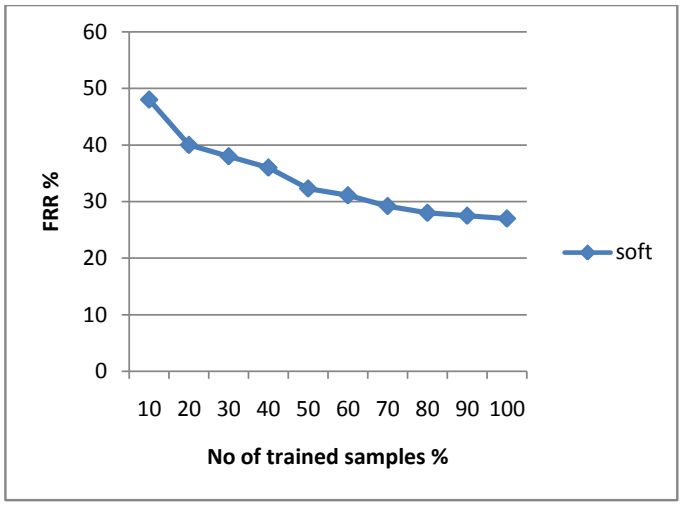

Fig.9. FRR of Soft Biometric Recognition

In Fig. 9, False Rejection Rate of Soft Biometric recognition is shown against number of trained files. Initially when the trained set is less FRR percentage is high. As the number of trained samples increases the percentage of false rejection rate falls low.

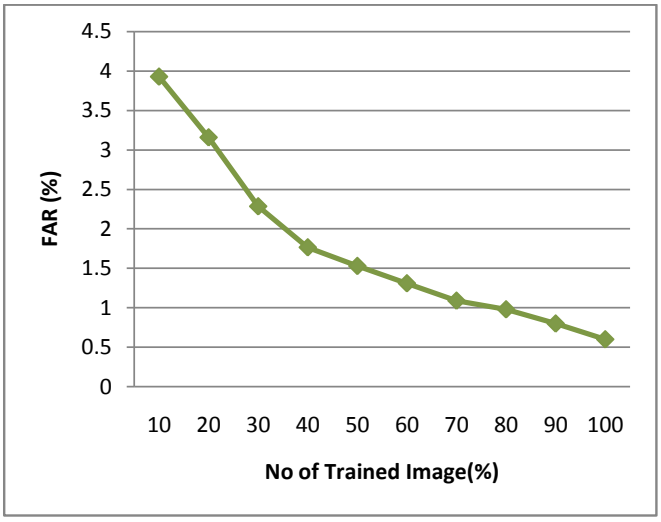

Fig.10. FAR after integration

Fig. 10 shows overall FAR by calculating the mean of three modalities which shows approximately 4% for 10 samples and the FAR is reduced to 0.6% for 100 samples.

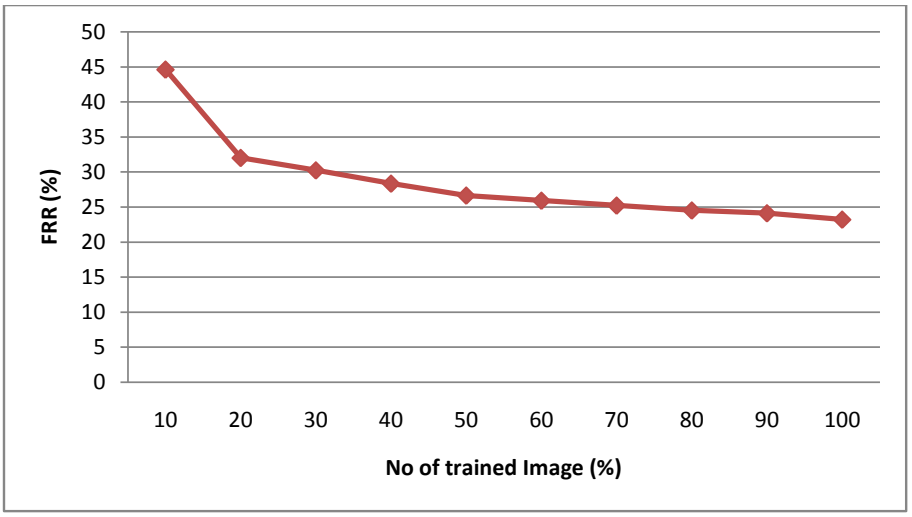

Fig.11.FRR after Integration

Fig. 11 shows overall FRR by taking the mean of three modalities which shows approximately 45% for 10 samples and the FRR is reduced to 23.2% for 100 samples.

V CONCLUSION

Traditional authentication schemes are inconvenient because users must focus on the authentication step every time they begin interacting with their device. System is vulnerable to the loss of data or attacks even if it is secured with password. When the system has privacy information, to prevent from attacks continuous authentication system plays a vital role. Continuous authentication approach would provide an additional line of defence, designed as a nonintrusive and passive security countermeasure. Lots of work related to continuous authentication has been done. Continuous Authentication using multimodal biometrics is more secured when compared to unimodal biometric. Therefore continuous authentication using face, fingerprint and soft biometrics was proposed which results in high security level than the existing system. In future different combinations of modalities will be considered to increase accuracy. Here the fingerprint verification is done with manual interference and in future automatic fingerprint verification will be carried out without involvement of user. Also system utilization will be considered for analysing its performance.

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, RajkumarJanakiraman, SandeepKumar,"Continuous Verification Using Multimodal Biometrics," IEEE Trans On Pattern Analysis and Machine Intelligence, Vol 29, No 4, April 2007.

[4] Alfredo Munoz-Briseno, AndresGago-Alonso, Jose Hernandez-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] MohdFikriAzli Abdullah , MdShohelSayeed, KalaiarasiSonaiMuthu, HousamKhalifaBashier, AfizanAzman, SitiZainab Ibrahim " Face recognition with Symmetric Local Graph Structure," 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] UmaraniJayaraman N, Aman Kishore Gupta, Phalguni Gupta, "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, MohammadGhanbari, "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] KoichiroNiinuma, 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.

Rajesh, M., and J. M. Gnanasekar. "Annoyed Realm Outlook Taxonomy Using Twin Transfer Learning." International Journal of Pure and Applied Mathematics 116 (2017): 547-558.

Rajesh, M. & Gnanasekar, J.M. Wireless Pers Commun (2017),https://doi.org/10.1007/s11277-017-4565-9

Rajesh, M., and J. M. Gnanasekar. "GCCover Heterogeneous Wireless Adhoc Networks." Journal of Chemical and Pharmaceutical Sciences (2015): 195-200.

Rajesh, M., and J. M. Gnanasekar. "CONGESTION CONTROL IN HETEROGENEOUS WANET USING FRCC." Journal of Chemical and Pharmaceutical Sciences ISSN 974: 2115.

Rajesh, M., and J. M. Gnanasekar. "GCCover Heterogeneous Wireless Ad hoc Networks." Journal of Chemical and Pharmaceutical Sciences (2015): 195-200.

Rajesh, M., and J. M. Gnanasekar. "CONGESTION CONTROL USING AODV PROTOCOL SCHEME FOR WIRELESS AD-HOC NETWORK." Advances in Computer Science and Engineering 16.1/2 (2016): 19.

RAJESH, M. "TRADITIONAL COURSES INTO ONLINE MOVING STRATEGY." The Online Journal of Distance Education and e-Learning 4.4 (2016).

Rajesh, M. "Object-Oriented Programming and Parallelism."

Rajesh, M., K. Balasubramaniaswamy, and S. Aravindh. "MEBCK from Web using NLP Techniques." Computer Engineering and Intelligent Systems 6.8: 24-26.