International Journal Of Electronics Engineering (Issn: 0973-7383)
Volume 10 • Issue 2 pp. 185-192 June 2018-Dec 2018 www.csjournals.com

Multimodal Systems: Fusion Strategies and Template Security

Mukesh Rani[1] and Chander Kant[2]
[1]M.Tech Scholar, [2]Assistant Professor,
Department of Computer Science and Applications, Kurukshetra University Kurukshetra,
[1]ranimukesh1991@gmail.com, [2]ckverma@redifmail.com

Abstract: Real user authentication has become very important with rapid advancements in networking with increased concerns about security. Biometric systems perform recognition with the help of specific physiological or behavioral characteristics of a person. Biometrics establishes identity on the basis of biological characters e.g., structure of DNA, facial features, voice, gait etc., instead of ID cards, PIN numbers, tokens, passwords, etc. A biometric system can be a unimodal and multi-biometric. Unimodal systems depend on the evidence of only one source of information whereas multi-biometric systems consolidate/combine multiple sources of biometric evidences. Multi-biometric systems are capable of enhancing the matching performance as they get the evidence presented by different modalities or biological characteristics and the use of multiple body traits improves the identification accuracy significantly. There are also some other traits such as skin color, age, height, hair color, eye color, gender called soft biometric trait. Soft biometric traits do not provide reliable verification because the nature of these traits are not permanent. Due to the lack of permanence and distinct property in soft biometrics, it can be used with other traits for improving performance of biometric system. In this paper, we proposed a framework by combining physical traits (face and fingerprint) with soft biometric trait (height) for enhancing biometric system security and performance.

Keywords: Soft Biometric, Multimodal Biometric, Normalization, Fusion**.**

I. Introduction

Biometric is the science of identifying an individual by extracting a feature set from data and evaluating with template stored in the database. A biometric system is used for identifying the person either real or imposter through using their physiological traits (hand geometry, face, fingerprint etc.) and behavioral traits (voice, gait, signature etc.). Biometric systems additionally provide the convenience in a sense that the person is no more required to design or remember passwords. Multi-biometric systems consolidate multiple resources of biometric evidences. The integration of evidences is known as fusion. The record from multiple sensors, multiple samples or multiple traits of an individual is consolidated by the multi-biometric system using various algorithms deployed on the same biometric trait. The fundamental requirement for various operations using biometrics is to verify an individual's identity. In order toprovide the genuine individual with the desired privileges given that they are provided at the correct time by having authenticated access, three approaches are available to establish an individual's identity [1]. The said methods used in various real life applications for verifying individual's identity include:

• **Something you have**:-Desired privileges can be accessed by the user when he/ she possess some physical objects like, keys, identitycard, smart card, etc. and these are shown to the authorities to get access of something or to be identified.
• **Something you know**:-When the user already knows some predefined objects like passwords and these objects are entered in order to verify the individual.
• **Something you are**:-A user can have access to a desired service with the help of measurable biometric traits.
The biometric traits are complex enough to share or steal and at the same time it is almost impossible that these traits cannot be forgotten or lost. Thus it can be stated that a higher security level can be achieved using biometrics for person identification/verification. There are several biometric traits which are used in various applications. Some examples of biometric traits are given in figure 1.

1) Multimodal Biometric Approach: Multimodal biometric system uses more than one trait for better and secure recognition as shown in Figure 2. The aim of multimodal system is to improve the rate of recognition.

International Journal Of Electronics Engineering (Issn: 0973-7383)
Volume 10 • Issue 2 pp. 185-192 June 2018-Dec 2018 www.csjournals.com

Multimodal biometric systems are more reliable than traditional authentication system like token based and knowledge based. Different fusion methods are used for making multimodal system by combining more than one trait [2]. This paper presents a proposed approach of multimodal biometric system with integration of face, fingerprint, and height. In this paper we use two modality face and fingerprint with soft biometric trait height. Soft biometric traits are discussed in next section. In this section we only discuss face and fingerprint physiological traits.

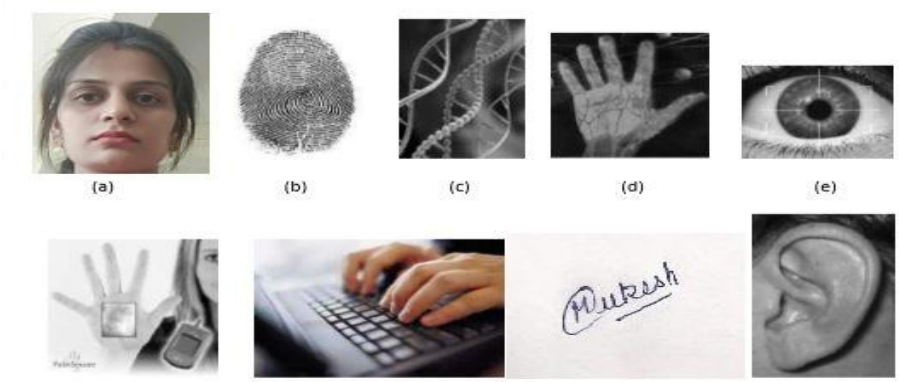

Fig. 1: Different Biometric Traits (a) Face, (b) Fingerprint, (c) DNA, (d) Hand veins, (e) Iris, (f) Palm print, (g) Typing, (h) Signature, (i) Ear, (j) Voice, and (k) Retina

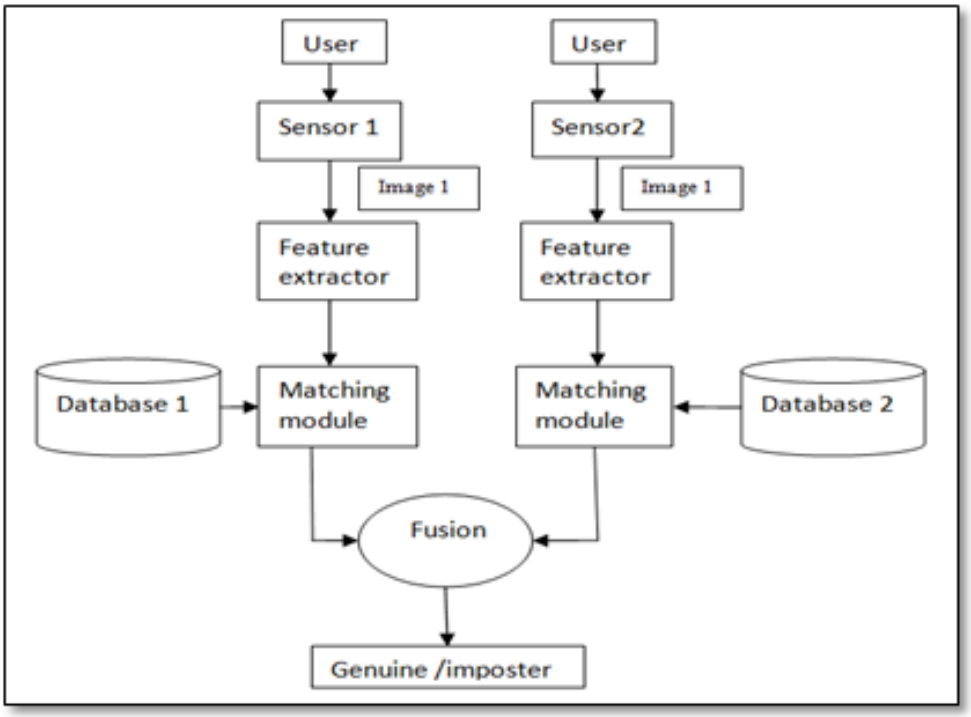

Fig. 2: Multimodal Biometric System

Face and fingerprint are highly accurate techniques for authentication because these traits are unique, user friendly, accurate, safe and secure [4]

2) Soft Biometric Traits:

Soft Biometric trends: Multimodal biometric systems provide higher security however also creates inconvenience to the user because of the problem of large verification time. So, soft biometric traits together with age, height, gender,

hair color, eye color may be used with multimodal system for improvingoverall performance of the system. Soft biometric traits offer some records about the person but statistics isn't always distinct and permanence in nature. There are especially two types of soft biometric traits [5]:
1) Continuous traits like height, weight, age and so on.
2) Discrete traits like gender, eye color etc.
We cannot use only soft biometric traits for recognition process because the information extracted from these traits is not unique and secure. Soft biometric traits are combined with physiological traits for providing secure and reliable authentication process. These traits are also improving the performance of a system by reducing verification time [6].

II. Related work

Antitza Dantcheva [7] gives introduction about soft biometric trait, their characteristics, advantages and disadvantages in his PhD thesis. Author discussed diverse things about the soft biometric traits such that soft biometric tendencies are non-intrusive, preserving human privacy, computationally efficient and classifiable from a distance. Soft biometric developments can be used with multimodal system for improving biometric system performance. Soft biometric traits have lack of permanence however it provide some proof about user identification and also enhance the performance after the usage of it with different biometric traits. Author proves the efficiency of purposed gadget with the assist of MUBI software program.
Sheena [8] Discussed study of multimodal biometrics system for better performance and security. Author discussed, obtained performance of unimodal biometrics system is not so much effective for security and performance of different applications. To enhance the performance and security level of unimodal biometrics system we can use multimodal biometrics system by combining more than one trait.
Ashraf AboshoshaET. Al [9] in this paper fusion of fingerprint, iris and face traits is used at score level in order to improve the accuracy of the system. Scores which obtained from the classifiers are normalized first using min-max normalization. Then sum, product and weighted sum rules are used to get fusion. Experimental results show that multimodal biometric systems outperform unimodal biometric systems and weighted sum rule gives the best results comparing with sum or product method.
SheetalChoudhary [10] This paper presents a robust multimodal biometric recognition system integrating iris, face and fingerprint based on match score level fusion using multiple support vector machines (SVMs). Here, multiple support vector machines are applied in parallel fashion to overcome the problem of missing biometric traits. It considers every possible combination of all the three biometric traits (iris, face and fingerprint) individually. Each possible combination of biometric traits has a separate SVM to combine the available match scores to generate the final decision.
T.Karthikeyanet. al [11] in our proposed system gives how to set a model to extract the feature of different irises and match them is especially important for it determines the results of the whole system directly. Gabor wavelets are capable of able to provide optimum combined representation of a signal in space and spatial frequency. A Gabor filter is built by modulating wave with a Gaussian. Feature Encoding was applied by convolving the normalized iris sample with 1-D Gabor filters. For Matching hamming distance will be calculated and accurate recognition was achieved.
Chander Kant [12] in this paper, a new approach is used that is integrating the soft biometrics with fingerprint and face for improving the performance of biometric system. Here we have proposed architecture of three different sensors to evaluate the system performance. The approach includes soft biometrics, fingerprint and face features, we have also proven the efficiency of proposed system regarding FAR (False Acceptance Ratio) and total response time, with the help of MUBI tool (Multimodal Biometrics Integration).

III. Proposed approach

Proposed scheme (as shown in figure 3) works by first comparing and matching the soft biometric trait. If the result is not matched then it will directly reject the user. If soft trait is matched then face and fingerprint traits are captured with the help of sensor. After that the feature set of face and fingerprint are extracted. The system compares these values with the existing values in the database, and generates match scores of the respective traits. This paper proposed an architecture and algorithm with the combination of face, fingerprint, and iris. This combination provides higher security as compare to other existing multimodal biometric systems. There are number of advantages of proposed approach over the conventional system, as discussed below: 1) the feature set of face and fingerprint are being calculated if and only if the user is found to be genuine at first stage (i.e. soft biometric phase).

International Journal Of Electronics Engineering (Issn: 0973-7383)
Volume 10 • Issue 2 pp. 185-192 June 2018-Dec 2018 www.csjournals.com

A. Image Acquisition and Feature Extraction:
Here in the proposed approach suitable sensors are used to acquire the face, fingerprint and soft biometric.

1. Image preprocessing:
The feature set originating from different sensors (face and fingerprint) are initially preprocessed. Raw images are difficult to recognize, hence the images are preprocessed for easier detection of the region from the surrounding area.

2. Feature extraction:
This stage is used for extracting the feature set that can be used to differentiate differentsubjects, creating a template that represents the most discriminate features of the face and fingerprint.

B. Architecture of Proposed Scheme:
It is present that face, iris and fingerprint biometric traits combination has better accuracy than other combination biometrics. Proposed scheme (as shows figure 2) works by first capture face, iris and fingerprint after that preprocessing is performed to remove the noise part of the images and then extracts their feature set, compare it with database, compute match score. The match score is obtained by Euclidean distance formula. Min-Max Normalization and then Simple Sum rule Fusion method apply on all three computed match score and generate a fused match score. If this fused score is less than and equal to threshold value then the query user is genuine otherwise imposter.
2) This system improves the FAR (false accept rate).
3) Accuracy of the system will increase.
The flow chart of the proposed system is shown below

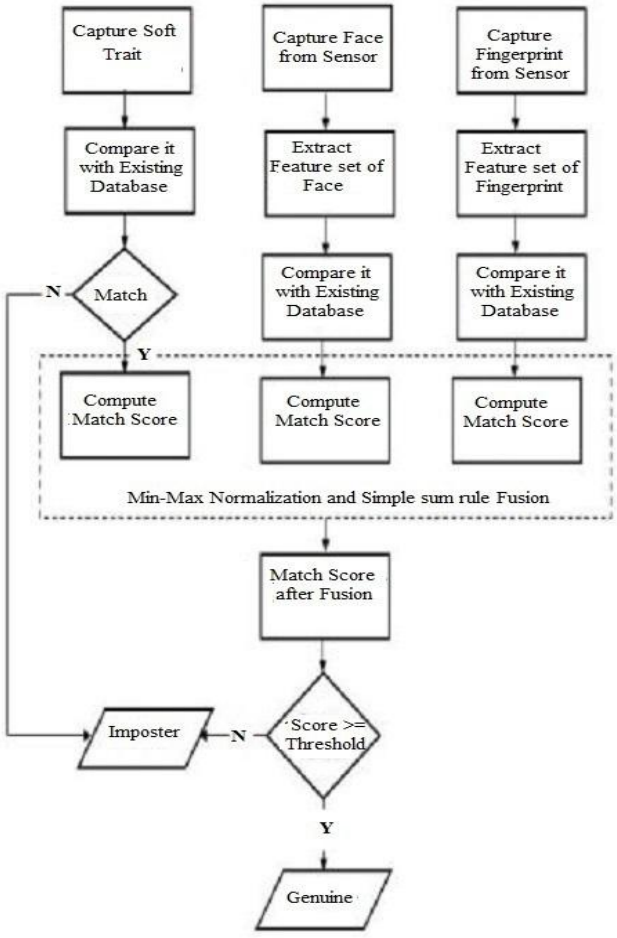

Fig. 3: Flowchartof the Proposed Approach

C. Algorithm for verification/identification in proposed scheme

1) Capture Soft trait (height)
2) Compare it with existing database
3) If (soft trait feature matched)
4) Compute match score of soft trait
5) Capture face from sensor
6) Extract feature set of face
7) Compare with existing database
8) Compute fingerprint match score
9) Capture face from sensor
10) Extract feature set of faces
11) Compare with existing database
12) Compute face match score.
13) Apply min-max normalization on soft, finger, face match scores
14) Apply simple sum rule fusion on normalized scores.
15) If (fusion score >= threshold)
16) Genuine
17) Else
18) Imposter
19) End If
20) Else
21) Imposter
22) End If
23) End

The parallel execution of the process results in improved false acceptance rate. In contrast if the process executes sequentially the false rejection rate will increase which will decrease the overall performance of the system. The proposed scheme is not free from all drawbacks.

1) It needs extra storage space to store the templates with soft trait data like age, gender, height.
2) Total response time of the system increases if user is genuine.
3) Soft trait varies over time, so it has to be used within aparticular time period. After the time period the soft trait needs to be captured again to maintain the performance of system.

D. Mathematical Terms

• Min max normalization is top suited where the Upper and lower bounds (maximum and minimum values) of the scores produced by the matcher are known. This method is not vigorous; therefore, it is highly sensitive to outliers [13]

1) Euclidean Distance: The Euclidean distance measure is used to calculate the minimum distance between the training and testing dataset is considered as the match score. Euclidean distance formula is defined mathematical as:

$$d(x,y) = \sqrt{\sum_{i}^{n} (x_i - y_i)^2}$$

2) Score Normalization: Min-Max normalization method used that map raw score in the range [0, 1]. It gives lower and upper bound values of score [14]. The normalized scores generated by the following equations:

$$N_{face} = \frac{MS_{face} - min_{face}}{max_{face} - min_{face}}$$

$$N_{fingerprint} = \frac{MS_{fingerprint} - min_{fingerprint}}{max_{fingerprint} - min_{fingerprint}}$$

3) Fusion: In the sum rule, to obtain the final score, normalized scores of individual matcher (soft trait, face and fingerprint) are sum together to obtain the final score. It is defined mathematical as:

$$Sum = \sum_{i=1}^{n} Si$$

International Journal Of Electronics Engineering (Issn: 0973-7383)
Volume 10 • Issue 2 pp. 185-192 June 2018-Dec 2018 www.csjournals.com

4) Soft Biometric Extraction:

For using soft biometrics, a mechanism should be there to automatically (i.e. without user interaction) extract these features from the user during the recognition phase [15]. This can be achieved using a special system of sensors. For example, a bundle of infrared beams could be used to measure the height, weighing machine can be used to measure the weight, a camera could be used for obtaining the facial image of the user, which can be used to obtain information like age, gender, and ethnicity [16]. The information obtained from soft biometrics could then be used to adjunct the identity information provided by the user primary biometric identifier. Extensive studies have been made to identify the gender, ethnicity, and pose of the users from their facial images. The gender, ethnicity and pose of human faces are classified using a mixture of experts by radial basis functions [17]. Their gender classifier classified users as either male or female with an average accuracy rate of 96 percent. Age determination is a more difficult problem because physiological or behavioral changes in the human body are very limited as the person grows from one age group to another [18]. Currently there are no reliable biometric indicators for age determination.

$$\text{Sum} = \sum_{i=1}^{n} Si.$$

IV. Results

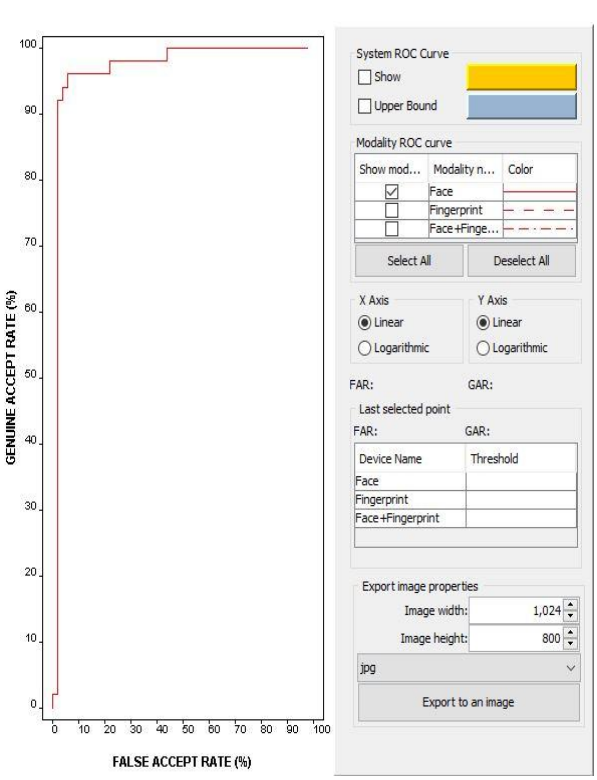

Fig.4: Roc curve for Face Modality

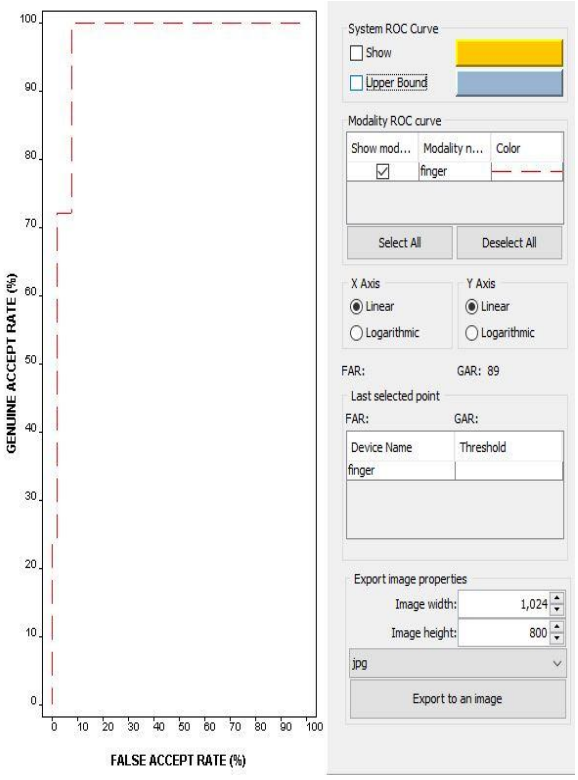

Fig.5: Roc curve for Fingerprint Modality

International Journal Of Electronics Engineering (Issn: 0973-7383)
Volume 10 • Issue 2 pp. 185-192 June 2018-Dec 2018 www.csjournals.com

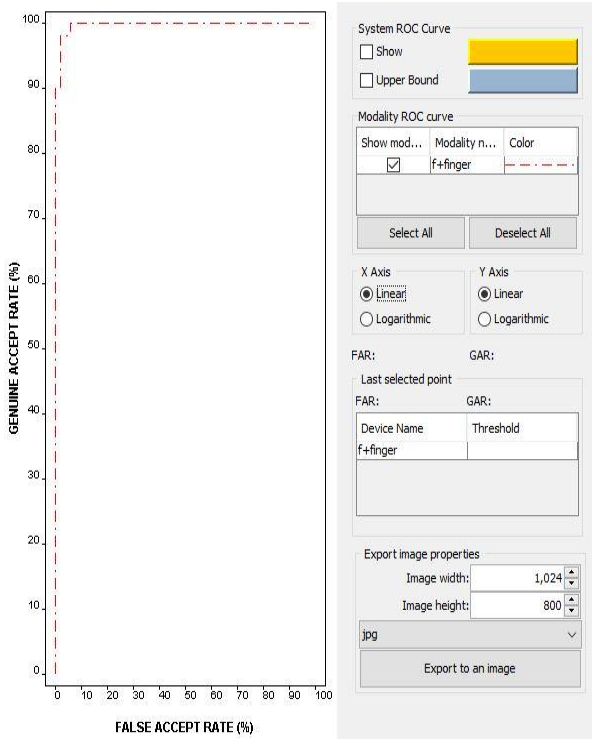

Fig.6:Proposed Schemes (Face + Fingerprint)

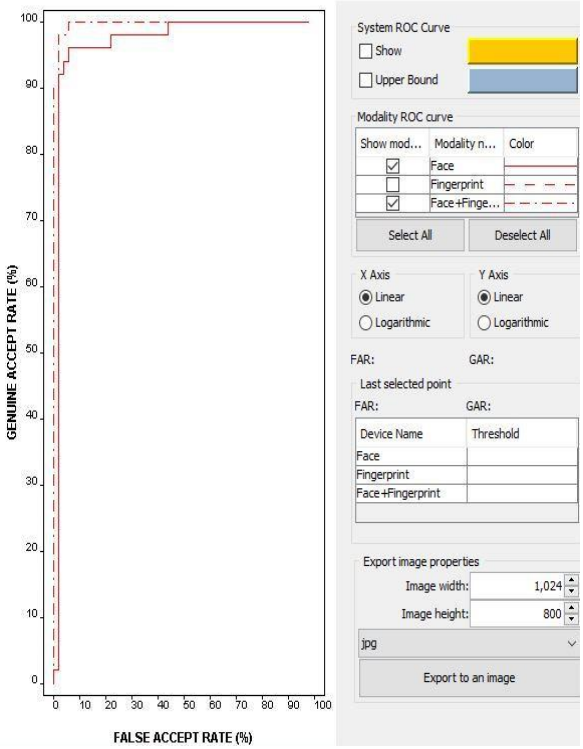

Fig.7: Proposed Schemes Face + Fingerprint vs. Face Modality

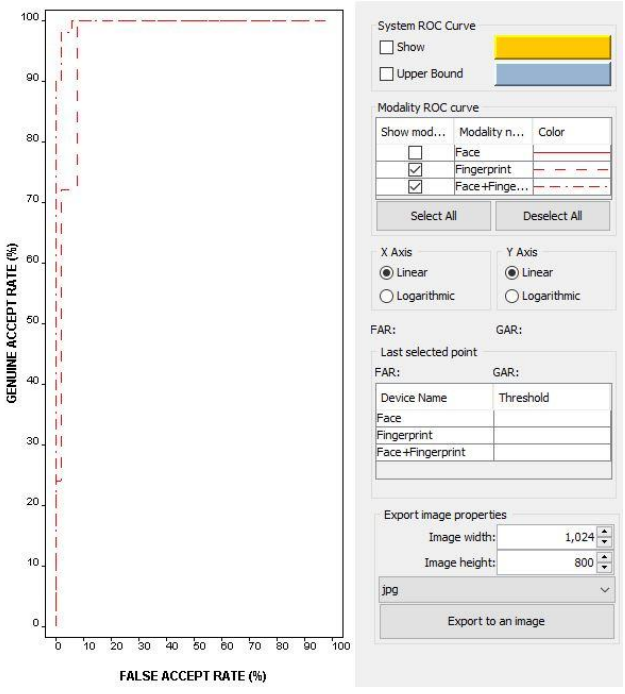

Fig.8: Proposed Schemes Face + Fingerprint vs. Fingerprint Modality

Table 1: Result of the proposed approach

S.No.	Biometric Technologies	FAR	GAR
1.	Face	90	2
2.	Fingerprint	90	8
3.	Face + Fingerprint	90	0

V. Conclusion

To remove the remedies and increase the efficiency of unimodal biometric system, a multimodal approach is defined. By the use of multimodal approach we can increase the aspect of security level in different application of different fields. In the purposed approach author fuse the soft biometric trait with multimodal system. The purposed approach is fusion of two primary traits (face and fingerprint) and one secondary soft biometric trait (height). To reduce the time period all through matching of database, purposed multimodal method can be used for better recognition. In future the proposed technique with three modalities can be used wherein the high degree of security in less verification time is required.

References

[1] J. D. Woodward, C. Horn, J. Gatune, and A. Thomas, "Biometrics a look at facial recognition," 2003.

[2] Mahesh.Pkand M. S. S. Nageshkumar.M, "An efficient secure multimodal biometric fusion usingpalm print and face image," vol. 2, 2009.

[3] M. Mohamadi and M. J. M. Abdolahi, "Multimodalbiometricsystem fusion using fingerprint and iris with fuzzy logic," vol. 2, no. 6, 2013.

[4] A. G. S. Gupta, "Proposed iris recognition algorithm through image acquisition technique," vol. 4, no. 2, February 2014.

[5] K. Nandakumar, X. Lu, and U. P. A. K. Jain, "Integrating faces and fingerprints and soft biometric traits for user recognition," In Proceedings Of Biometric Authentication Workshop and Lncs 3087 pp. 256-269, May 2004.

[6] D. C. Kant and M. Ahlawat, "A multimodal approach to enhance the performance of biometric system," vol. 4, 2015.

[7] S. M. Sheena, "A study of multimodal biometric system,"

[8] A. Dantchev,"Facial Soft biometrics methods and applications and solutions," 2011.

[9] A. Aboshosha and E. A. Karam, "Score level fusion for fingerprint and iris and face biometrics," International Journal of Computer Applications, vol. 111, no. 4, February 2015.

[10] SheetalChaudhary, "A robust multimodal biometric system integrating iris and face and fingerprint using multiple svms," International Journal of Advanced Research in Computer Science, vol. 7, no. 2, March-April 2016.

[11] T.Karthikeyan and B.Sabarigiri, "An efficient iris feature encoding and pattern matching for personal identification," International Journal of Advanced Research in Computer Engineering and Technology (IJARCET), vol. 2, March 2013.

[12] C. Kant, "A multimodal approach to improve the performance of biometric system," BIJIT - BVICAM International Journal of Information Technology BharatiVidyapeeth Institute of Computer Applications and Management (BVICAM) and New Delhi (INDIA), April and 2015.

[13] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Transactions On Circuits And Systems For Video Technology, no. 1, January 2004.

[14] A. K. Jain, K. Nandakumar, and A. Ross, "Score normalization in multimodal biometric systems," The Journal of Pattern Recognition Society and 38(12) and 2270-2285, 2005.

[15] X. Chen, P. J. Flynn, and K. W. Bowyer, "Irandvisible lightfacerecognition andcomputervision andimageunderstanding," September 2005.

[16] Jain, A.K., S. Dass, Nandakumar, and K., "Can soft biometric traits assist user recognition? In: Proceedings of spie international symposium on defense and security biometric technology for human identification," 2004.

[17] E. Erzin, Y. Yemez, and A. M. Tekalp, "Multimodal Speaker Identification using an Adaptive Classifier Cascade based on modality reliability," IEEE Transactions on Multimedia and 7(5) and 840-852, October 2005.

[18] Jain, A.K., Dass, S.C., and N. K, "Integrating faces and fingerprints and soft biometric traits for user recognition," Proceedings of Biometric Authentication Workshop and LNCS 3087.