IJCSC 0973-7391 Volume 8 • Issue 2 March 2017 - Sept 2017 pp. 72-80 available online at www.csjournals.com

A Novel Approach to Improve the Biometric Security using Liveness Detection

Gurmeet Kaur[1], Parikshit[2], Dr. Chander Kant[3]
[1]M.tech Scholar, Assistant Professor[2, 3]
[1, 2]Doon Valley Institute of Engineering and Technology, Karnal, India
[3]Department of Computer science and Application, Kurukshetra University, Kurukshetra, India
gurmeet0047@gmail.com, par7901@gmail.com, ckverma@redifmail.com

Abstract: A biometric system automatically authenticate individuals based on their physical and behavioral features like face, iris retina, ear, voice, signature keystroke dynamics etc. A biometric system which uses only a single trait for recognition is known as unimodal system. In Unimodal biometric system contains some limitation such as high error rate, non-universality, noise in sensed data, and spoof attacks etc. These problems could be overcome by multimodal approaches which combine more than one trait of user for authentication. The main purpose of using liveness detection with multimodal biometric is that we can use this approach in highly secured application such as defense, labs, pharmacies and bank applications. So in this paper liveness detection technique is used with multimodal approach. Initially, it checks the liveness of the person. If the person is found alive, only then the further calculations are performed. The main purpose of the purposed scheme is to reduce the FAR (false acceptance rate), FRR (false reject rate) and provide protection against spoof attacks. Proposed scheme was implemented using MUBI (Multimodal Biometrics Integration) software.
Keywords: Biometrics, Fusion, Liveness Detection, Multimodal

1. Introduction:

In today's world, there is a high demand to authenticate individuals automatically. So, biometric systems are best suited for providing secure personal identification. Biometric system are those systems which recognize individuals based upon their physiological (iris, fingerprint, retina, face etc.) and behavioral (signature, keystroke dynamic etc.) traits. Although these systems are more secure than the traditional systems such as key, password, token etc. Biometric systems use two types of system that is unimodal and multibiometric system. The system use a single source of information to authenticate an individual is known as unimodal system. As unimodal system have some problems for example lack of individuality, spoof attack etc. Due to these problems unimodal system are not used where are high security is required.Multibiometric system can address the problem encountered by unimodal biometric system. Multibiometric systems use more than one modalities of a single user for providing high security, accuracy and performance [1, 2]. The main objective of using multi-biometrics system is to reduce the:

- False acceptance rate (FAR)
- False reject rate (FRR)
- Failure to enroll rate (FTE)

1.1 Classification of Multibiometric system:

Multibiometric system based upon the nature of source can be categorized as:

1. Multi-Sensor Systems:

In multi-sensor systems a single biometric trait of a person is acquired by two or more sensors. For e.g. fingerprint from a solid state and optical sensor.

2. Multi-Algorithm Systems:

These are those systems which over the same biometric data, multiple feature extraction or matching algorithms are used. This means that each algorithm creates independent results which are then used in the merger.

3. Multi-Instance Systems:
Those systems which use multiple instances of a single biometric trait are known as multiple instance systems. For example instance of face are front view, left side view, and right side view are used for recognition.
4. Multi-Sample Systems:
System where multiple samples of the same biometric trait can be captured using a single sensor. Left and right eye sample are used as different unit for authentication.

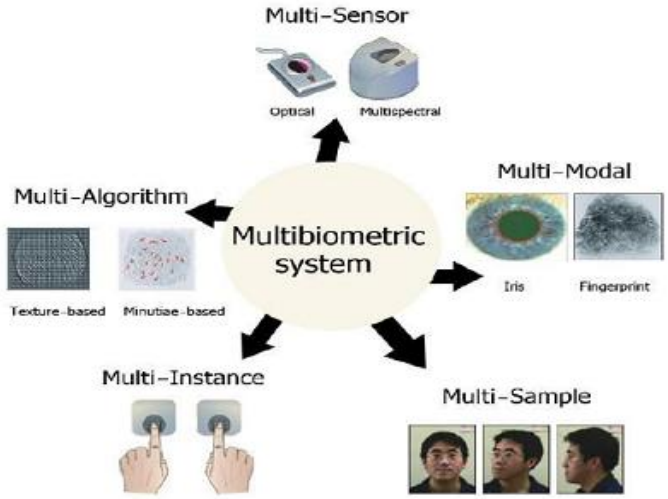

Figure 1: Classification of Multibiometrics

5. Multimodal Systems:
These are those systems where authentication of an individual is provided using different biometric traits. For example, a system integrating fingerprint, gait and iris features for recognition would be considered as a "multimodal system" [3].

1.2 Fusion levels in Multibiometric system:
Multimodal biometric system uses different fusion methods for combining the different biometric modalities. Fusion of biometric modalities takes place at various levels in the biometric system [4].
Some fusion methods commonly used in biometric authentication system are as follows:

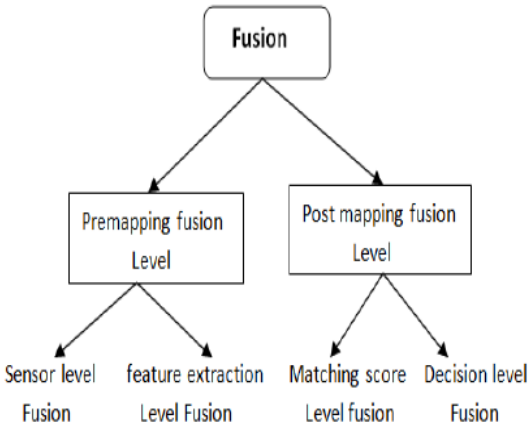

Figure 2: Different types of fusion

1.2.1. Sensor level fusion: This is a primary stage of fusion. In sensor level fusion raw data from the sensor are fused together. At this level multiple samples of same trait from same sensor or sample capture from different sensor are fused together.

1.2.2. Feature extraction level fusion: In features extraction level fusion the feature sets extracted from different modalities can be fused into a composite feature set by using particular algorithm and passed to matching module.

1.2.3. Matching level fusion: After the extraction of feature set from different modalities comparison is done with the stored database which generates matching score for each modality. All the match score obtained from each matcher are fused together in a composite match score.

1.2.4. Decision level fusion: This is the last stage of fusion where the outputs obtained from different modules are combined to make final decision. Different methods are used to take decision for example AND, OR, majority vote decision and Bayesian network.

1.3 Liveness Detection:

Liveness detection is also known as vitality detection. In biometric system liveness detection means the proficiency of the system to recognize a user during enrollment and authentication process. This is mainly used for differentiating whether the user is live or not. If the system is designed to secure against spoof attacks with dummy face, fingerprint and iris, it must also check that the presented biometric data belongs to the live human being or not who was firstly enrolled in the system. In fingerprint system scan be fooled with synthetic fingerprints, static facial images can be used to fool face recognition systems, and static iris images can be used to fool iris recognition systems. For making a secure biometric system, liveness detection is a very good technique that determines whether the sample given by user is live or not [5].

1.3.1 Liveness detection in multimodal biometric systems:

Liveness detection technology is also used with multimodal system for protection against spoof attacks. By using this technology performance and security of the system are improved. In our proposed approach liveness detection is used at authentication stage for both modalities face and iris.

If input sample = live then

    Live user

Else if input sample = not live

    Fake user

Liveness detection at sensor level is mainly used for reducing spoofing attacks.

2. Related work:

Rui Chen et al. [6] proposed the specific multispectral features of conjunctival vessels and iris textures. They used Support Vector Machine classifier to classify the feature vectors extracted from live and fake irises samples. The proposed method can classify between live irises and fake irises with high accuracy and low computational cost.

Arun Ross [7] in this paper author proposed a framework design in which a liveness detector is used with a fingerprint matcher. Bayesian Belief Network (BBN) scheme that models the relationship between match scores and liveness values is introduced. All experiments are done on a publicly available database of the Fingerprint. Liveness Detection shows the efficiency of assuming a positive point of impact of liveness values on match scores.

Sreenath Narayanan K et al. [8] in this paper authors has discussed the study of a secure system needs in liveness detection in order to protection against spoofing attacks. An efficient real time face liveness detection algorithm based on image distortion analysis has been proposed. They have used two different features such as blurriness and chromatic moment are extracted from the image. A fuzzy classifier is used to distinguish between live and spoof faces.

MenduAnusha et al. [9] in this paper defined the limitations faced in unimodal systems. To overcome these problems author represents a multimodal biometric system by integrating iris, face and fingerprint to identify a

person. In this paper performance ratio is defined in term of False Accept Rate and Genuine Accept Rate is demonstrated with the help of (MUBI) Multimodal Biometrics Integration software.

Chander Kant [10] in this proposed modal a new approach has been used soft biometrics with fingerprint and face for improving the performance of biometric system. Soft biometric feature have deficiency of permanence but it provide some evidence about user identity and also improve the performance after using it with other biometric traits. Author proves the efficiency and performance of purposed system with the help of MUBI software.

ManishaKumari et al. [11] discussed study of multimodal provides better performance, accuracy and security over a unimodal biometric system. She proposed a liveness detection with multimodal biometric is used this approach in a highly secured application such as defence and bank application. She proves the new approach for increasing security and performance by the combination of face and fingerprint biometric together with liveness detection technique.

RupinderWahla et al. [12] proposed a multimodal biometric fusion system that fuses results from both Wavelets transform and PCA. In this system they have used three biometric traits like face, fingerprint and iris. The performance of the system is shown in form ROC (receiver operating characteristics) curves. The comparative study shows that multimodal systems are much more accurate than unimodal systems.

3. Proposed Model:

In our proposed approach liveness detection is used at sensor level for better authentication. If an input user sample is live then the further processing takes place else the input user sample is fake/dummy. Face liveness is checked by user response of smiling face and iris liveness is checked by eye blinking captured by a web camera. There is no need of extra hardware device for checking the liveness for both traits.

In every biometric system requires two stages for verification and identification of user. First is enrollment and second is authentication. In our proposed system at enrolment stage, template of face and iris traits are stored in database which are further used for comparing new samples in authentication phase.

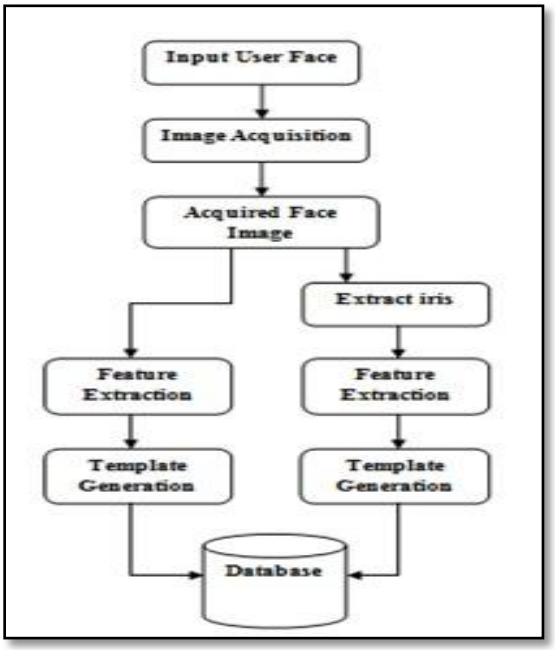

Figure 3: Enrollment Phase

3.1 Enrollment: Enrollment is a process that is used for registering individuals in the biometric system database. During the enrollment process, the biometric feature of a person is acquired by a biometric sensor. In enrollment

process image acquisition and feature extraction stages are used to enroll an individual data sample into the template.

3.1.1 Image Acquisition Stage: Here in the proposed approach a single camera is used to acquire both face and iris images. Firstly, the whole face image is acquired and then iris image is extracted from it.

3.1.2 Feature Extraction: Feature extraction is used to extract the features of both the modalities face and iris. These extracted feature set are stored into the template for the authentication of the user.

In our proposed approach at enrollment stage, template of face and iris traits are stored in database as (shown in figure 3). Which are further used for comparing new data in authentication phase.

3.2 Authentication: In authentication phase firstly liveness detection is apply at sensor level for checking whether newly captured sample is live or not as shown in figure 4. If the input user is alive, after that capture the face and iris images, extracts their feature set, and Min-Max Normalization and then Simple sum rule Fusion method apply on both computed match score and generate a fused score. If this fused score is greater than and equal to threshold value then the query person is a genuine user otherwise its imposter.

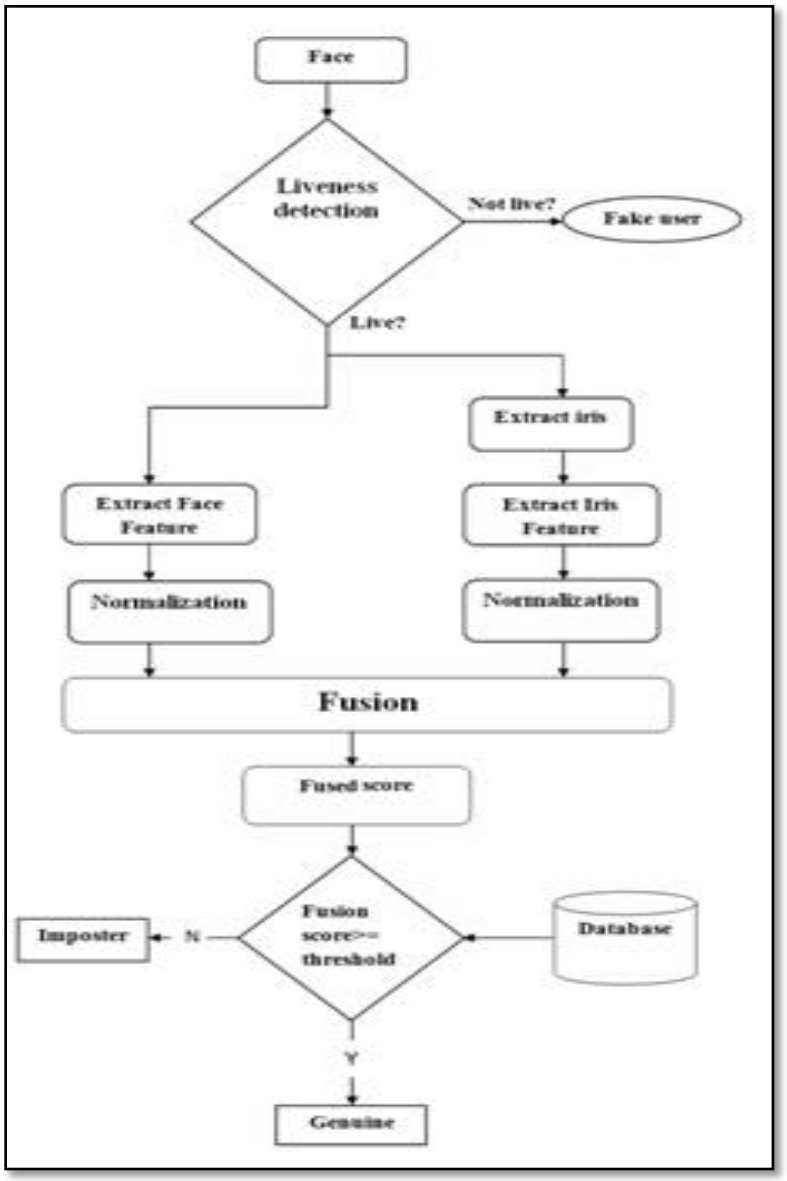

Figure 4: Proposed Approach Architecture

3.3 Algorithm for authentication in proposed scheme:

1) Capture face from sensor.
2) Liveness is checked at sensor level for both face and iris modalities by capturing user response of smiling face and eye blinking through web camera.
3) If both input are live.
4) Then sample sends to feature extractor modules.
5) Else fake user.
6) Extract feature set.
7) Apply min-max normalization on both modalities.
8) Apply matching score level fusion using simple sum rule on normalization scores.
9) Generate the fusion score.
10) If (fused score>=threshold) then.
11) Acceptance/genuine.
12) Else
13) Rejected/imposter.

3.4 Mathematical Terms:

There are two mathematical terms that are using during algorithm.

A. Min-Max Normalization:

The individual feature vectors of face and iris may be significantly different in terms of their range and distribution. For example, the value of face may be in the range of [0,100] while iris value may be in range of [0, 1]. Min-Max normalization method used that map raw score in the range [0,1]. It gives lower and upper bound values of score.
Then, the formula used for computing the normalized score using min-max normalization is:

$$S_i = \frac{Si - Smin}{Smax - Smin}$$

where s_i' is the normalized score, s_i is the matching score, s_{min} is the minimum match score and s_{max} is the maximum match score for i^{th} biometric trait[13].

B. Simple sum rule fusion method:

In the sum rule, to obtain the final score, normalized scores of individual matcher (face, iris) are sum together to obtain the final score. It is defined mathematical as

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

4. Results:

The ROC (Receiver Operating Characteristics) curves are obtained after applying the simple sum rule fusion over the normalized face and iris modality. These curve plots the genuine accept rate (GAR) against the false accept rate (FAR).

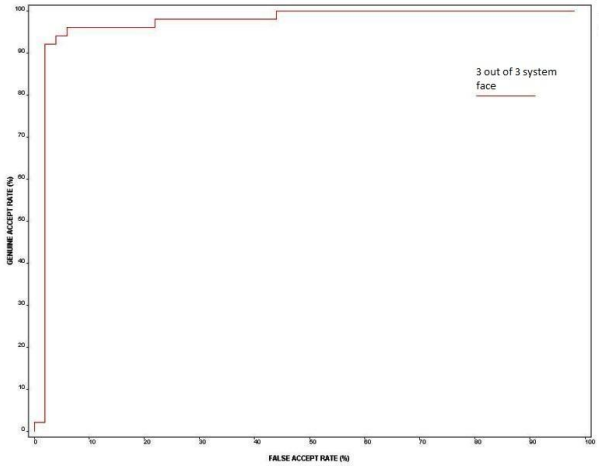

Figure 5: Roc Curve for Face Modality

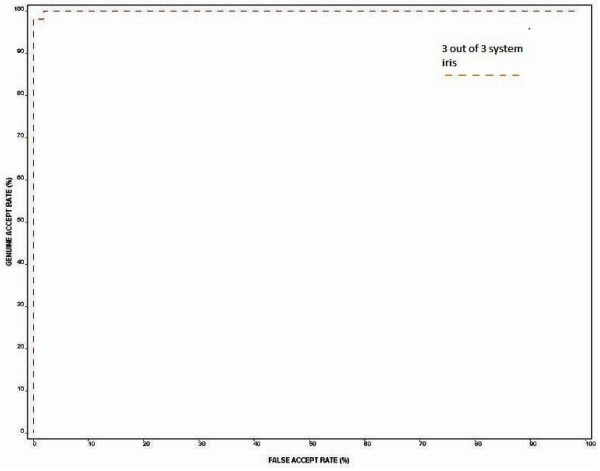

Figure 6: Roc Curve for Iris Modality

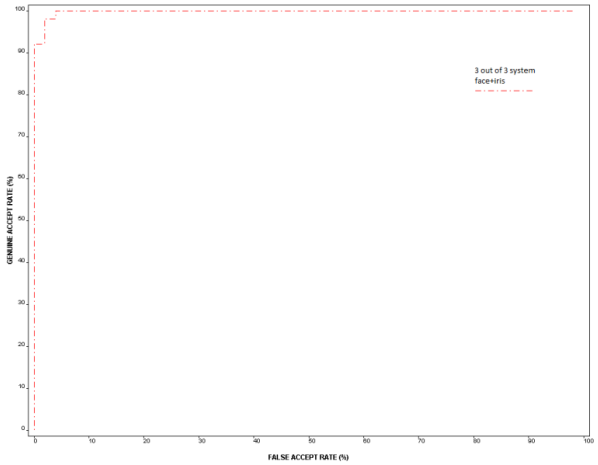

Figure 7: Proposed Scheme (Face + Iris)

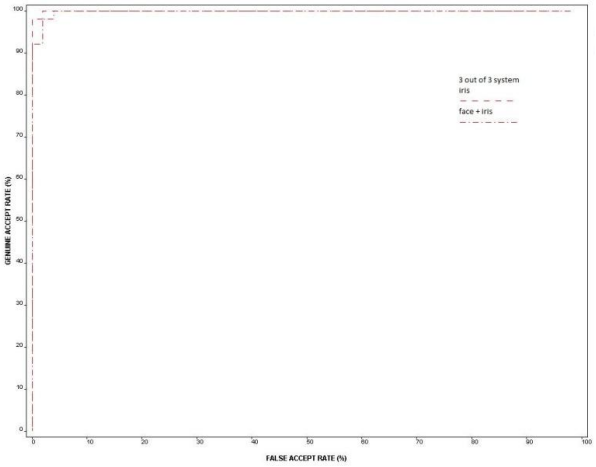

Figure 8: Proposed Scheme (Face + Iris) v/s Iris

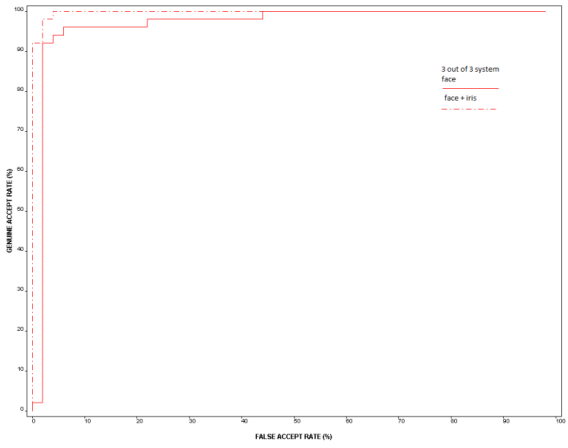

Figure 9: Proposed Scheme (Face + Iris) v/s Face

The performance of proposed modal is measured using GAR (Genuine accept rate) and FAR (False accept rate) [14, 15].

$$\mathbf{FAR} = \frac{Number\ of\ false\ acceptamce}{Number\ of\ identification\ attempts}$$

It refers the possibility where a false user is accepted by the biometric authentication system as an authenticated user. False accept rate is also named as false match rate.

$$\mathbf{FRR} = \frac{Number\ of\ false\ rejection}{Number\ of\ identification\ attempts}$$

It refers the probability for a real user is rejected by the biometric authentication system as an unauthenticated user. It means the percentage of incorrectly rejected real user. False reject rate is also named as false non match rate.

$$\mathbf{GAR = 1\text{-}FRR}$$

Table 1: Comparison of proposed scheme with existing biometric techniques:

S. No.	Biometric Technologies	GAR	FAR
1.	Face	94	4
	Proposed scheme		2
2.	Iris	97	2
	Proposed scheme		1

- **Advantages of the proposed scheme:**

A. Single device has been used for acquiring both face and iris images.
B. FAR (false acceptance rate) and FRR (false reject rate) have been reduced.

- **Drawbacks of the proposed scheme:**

A. Extra storage space is required for storing the two (face, iris) modalities.
B. Total response time of the system increases for real user.

5. Conclusion:

Biometric authentication system based on the single trait have some limitation such as (high error rate, non-universality, noise in sensed data etc.) which can be removed by using combination of more than one traits. We have proposed this novel approach by combining face and iris biometric traits for better recognition. Liveness detection technique is also used with the presented multimodal approach for better authentication. Liveness detection is used at the sensor level for checking the dummy users. The purposed approach can be applied in highly secured applications such as defense and bank applications. And the proposed approach provides better security, accessibility and performance than the existing multimodal approaches.

6. References:

[1] Ashish Mishra, "Multimodal Biometrics it is: Need for Future Systems," International Journal of Computer Applications, vol. 3, pp. 28-33, June 2010.

[2]Sondhi Komal And Bansal Yogesh Concept Of Unimodal And Multimodal Biometric System Unimodal And Multimodal Biometric System - Cse&BaddiUniversity, India : International Journal Of Advanced Research In Computer Science And Software Engineering, Vol. 04, 06-2014.

[3]Zhifang Wang, Erfu Wang, Shuangshuang Wang and Qun Ding, "Multimodal Biometric System Using Face-Iris Fusion Feature", Journals of computers, Vol. 6, No. 5, May 2011.

[4] Dr.N.RadhaS.R.SorubaSree, "A Survey on Fusion Techniques For Multimodal Biometric Identification," Vol. 2, No. 12, December 2014.

[5]Karunya.R, S.Kumaresan,"A Study of Liveness Detection in Fingerprint and Iris Recognition Systems using Image Quality Assessment", International Conference on Advanced Computing and Communication Systems ICACCS -2015.

[6] Rui Chen, Xirong Lin, Tianhuai Ding, "Liveness detection for iris recognition using multispectral images", Pattern Recognition Letters, pp. 1513–1519, 2012.

[7]Arun Ross, EmanuelaMarasco, Yaohui Ding, "Combining Match Scores with Liveness Values in a Fingerprint Verification System", pp. 978-1-4673-1228, IEEE 2012.

[8] Sreenath Narayanan K, Mary ReenaK.E, "Real Time Face Liveness Detection" International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering, Vol. 3, Issue 1, Feb-2016.

[9] MenduAnusha, T.V.VamsiKrishna, "Multimodal Biometric System Integrating Fingerprint Face and Iris", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 10, Oct- 2016.

[10]Chander Kant, "A Multimodal Approach to Improve the Performance of Biometric System", BVICAM's International Journal of Information Technology, Vol. 7 No. 2; ISSN 0973 – 5658, Dec-2015.

[11]Manishakumari, Chander Kant, "A Hybrid Approach for Raising Biometric System Security by Fusing Face and Fingerprint Traits", International Journal of Scientific & Engineering Research, Volume 7, Issue 12, Dec-2016.

[12]Aniket S.Buddharpawar, "Iris Recognition based on PCA for Person Identification," International Journal of Computer Applications (0975 – 8887) 2015.

[13] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition", IEEE Transactions On Circuits And Systems For Video Technology, vol. 14, no. 1, pp. 4–21, January 2004.

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

[15] Anil K. Jain, Arun Ross, Patrick Flynn, "Handbook of Biometrics", Springer, 2008.