IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 20, Issue 3, Ver. IV (May. - June. 2018), PP 54-62
www.iosrjournals.org

A Hybrid Approach for Raising Biometric System Security by Fusing Fingerprint and Iris Traits

Mukesh Rani[1] and Chander Kant[2]
[1]*M.Tech Scholar,*
[2]*Assistant Professor,*
[1,2]*Department of Computer Science and Applications, Kurukshetra University Kurukshetra,*
Corresponding author: Mukesh Rani

Abstract*—Biometric system uses physiological and behavioral characteristics for the purpose of verification and authentication of the user. The unimodal biometric approach includes only one characteristic of the user for the validation purpose. The unimodal approach provides limited accuracy for the recognition of a person due to some limitations like error rate is high, noise contained in sensed data etc. Multimodal systems are designed to overcome the limitations of unimodal biometric systems. The multimodal approach uses more than one trait of the user for authentication. This paper deals with liveness detection technique together with the multimodal approach used for authentication of a user. The liveness detection technique determines whether the enrolled user is live or not. This technique will be more helpful in more sensitive and secure areas like defense and banks. The current study provides an approach to increase the accuracy and security in biometrics combining fingerprint and iris characteristics simultaneously along with liveness detection technique.*

Keywords– *Unimodal biometric System, Multi-biometric System, Fingerprint Recognition, Iris Recognition, Liveness detection, Fusion level.*

Date of Submission: 20-06-2018 Date of acceptance: 04-07-2018

I. Introduction

Biometric systems provide a sharp edge over the traditional security methods like pin number, password, card, key etc. Because in biometric system approach the person need not remember the passwords or any number. The user will be identified and authenticated by his physical and behavioral characteristics. Based on the number of characteristics involved for recognition of user the biometric systems are classified into two:

- Unimodal biometric
- Multimodal biometric system

In unimodal approach, the user is identified and authenticated with the use of single physical or behavioral trait. But a single character is not able to provide accurate results for the identification of the user and sometimes it becomes difficult to sense fingerprint of a person if the finger is swelling. The face is not identified sometimes due to a slight change in expressions, Voice is not recognized due to a sore throat, illness etc. The unimodal biometric systems possess high error rate due to some contingency problems like lack of individuality, lack of different representation etc. The errorrate should be least and accuracy maximum for a secure application. Due to the limitations of the unimodal system, these are not preferred to be used for sensitive and secure areas where performance and security are of highest priority [1]. The limitations of the unimodal biometric system are eliminated to a certain extent by the multimodal biometric system. Multimodal systems are the extension of unimodal biometric systems. The multimodal system uses more than one biometric trait to authenticate the user with high accuracy and reliability [2].

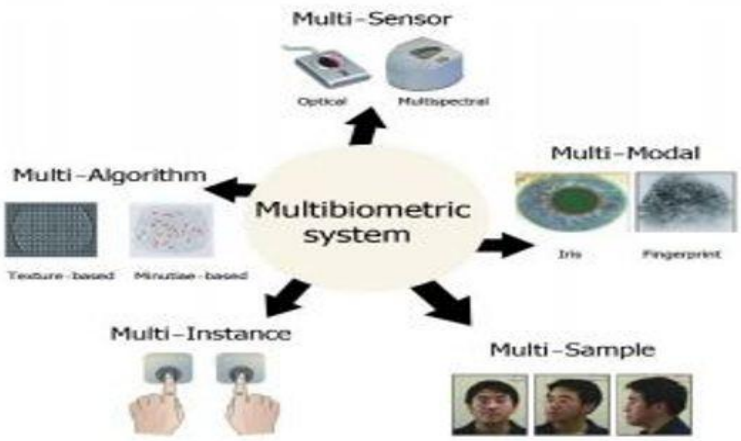

Fig. 1: The different types of multi-biometric system

The security level is also enhanced by this technique as compared to the unimodal system. The multimodal system is one of the classifications of the multi-biometric system as shown in Fig 1.

A. Classifications of Multi-biometric System

1) Multiple sensor systems: Multiple sensor systems use single biometric characteristic to authenticate the user with the help of two or more different sensors. For example, fingerprints are recorded by optical and solid state sensor to recognize the person [3].

2) Multiple representation systems: In this type, multiple representation methods are used for storing template. The template is generated by extracting their minutiae point and pattern from capturing sample.

3) Multimodal system (multiple biometric traits): In multimodal approach, more than one biometric trait is stored for the authentication purpose. For example, it can be correlated characteristics (voice and lip movement) and uncorrelated characteristics (fingerprint and face expressions).

4) Multiple instance system: In this approach, multiple samples of the same biometric trait are captured using single or different sensors. For example, face as a biometric trait can be captured as front view, left side view, right side view as shown in fig 1.

5) Multiple unit systems: In this type of approach, multiple units of a single biometric trait are recorded. For instance, left and right eye samples are considered as different units for identification.

B.Fusion levels in biometric system

The results of two or more unimodal biometric are combining using fusion for making multibiometric system. There is mainly two level of fusion which is further divided into four level of fusion (shown in fig 2) are discussed below [4]:

1) Sensor level fusion: At this level sample captured from the different sensor or multiple instances of the same trait from the same sensor are fused together. This is an early stage of fusion.

2) Feature extraction level fusion: Samples taken from the same or different sensor are preprocessed and send to feature extraction module for further processing. Feature extraction module extracts feature set individually. So the extracting feature set of both samples are fused Fusion level for multibiometric system. together to make a single combine vectorby this level of fusion.

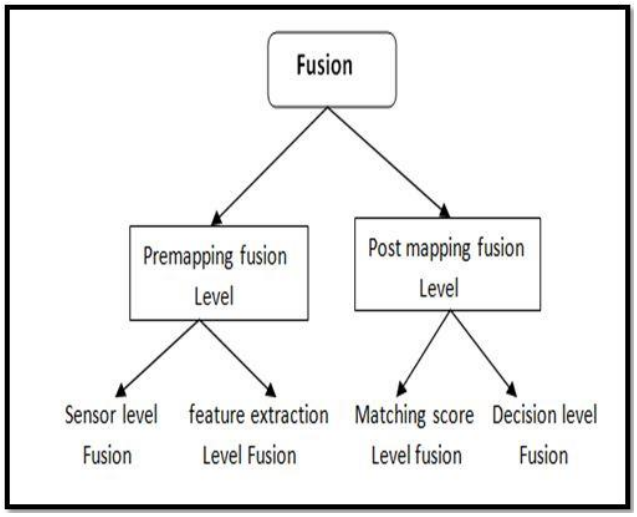

Fig. 2: Fusion level for multi-biometric system

3) Matching score level fusion: This type of fusion is used to getting match score from different matcher. All the results obtained from each matcher are fused together by matching score level fusion.
4) Decision level fusion: Decision level fusion can apply at the end of biometric system processing. This is the last stage of fusion where the outputs of all the decision modules are combined for providing better performance and accessibility. The multimodal biometric system performs any of the above fusion strategies for better output. In proposed model multimodal technique is used with decision level fusion of face and fingerprint biometric traits.

C.Liveness Detection
The live detection technology is used to determine whether a sample of any biometric trait given by the user is live or not. Liveness detection technique is used with the multimodal approach to ensure the security of biometric systems against the hoax. Liveness detection method is used after recoding the sample of some biometric trait by a sensor. These days the liveness approach has become very helpful to make the more secure biometric systems against the fake user [5].
Liveness detection approach in the biometric system is mainly performed at two stages:

- Acquisition stage
- Preprocessing stage

The current study uses liveness detection technique at sensor level (acquisition stage) for both biometric traits face and fingerprint. Liveness detection method at sensor level is generally used to guard against spoof attacks. Liveness detection technique is performed in mainly three ways which are discussed as under [6]:

1.Liveness detection is carried out for the intrinsic property of human beings like physical property (weight, elasticity), visual property (color) and body fluids (oxygen, blood, DNA) etc.
2. Liveness detection is carried out to sense the involuntary signal of the user such as heartbeat, blood flow, perspiration, blood pressure etc.
3. Liveness detection is carried out for the response made by the body of the person. The response may be either voluntary (when the user response is required) like Smiling, knee reflex etc. or involuntary (user response not needed) like pupil expansion, eye blinking etc.

II. Related Work

Identification and authentication of the user are prime requirements to secure any kind of transaction. In the modern era, biometric systems are playing a vital role to secure the transactions. Further to secure the biometric systems against all spoof attacks many researchers have discussed and talked about various methods to increase the security of biometric systems which are described as:

B. G [7]described various methods to secure biometric technology against all hoax in face recognition. Liveness detection approach using the facial features like lip movement, eye blinking, forehead movement etc. is discussed to increase the security of biometric systems. The different samplesand patterns are recorded with help of the camera and liveness of face sample are determined. This is very authentic approach discussed by the author to restrict the entry of the fake user. Thus, the performance, accuracy, and security of biometrics have been enhanced in face recognition.

Themultimodalbiometricapproachisdesignedtoovercome the limitations of the unimodal biometric approach. Gambhir[8] presented a multimodal system for authentication of a person. The two biometric traits such as face and ear were included by the author for the purpose of better recognition of the person. The model developed by the author comprises of PCA analysis algorithm in MATLAB for face recognition and ear authentication matcher module. The performance was significantly increased by combining these two characteristics.

The multimodal approach has a clear edge over the single biometric approach. Abdolahi [9] described the recognition system using the biometric traits fingerprint and iris with the fuzzy algorithm. The results were fused by the author by using decision level fusion method. The manifestation of each biometric result combination was carried out by fuzzy technique.

B.M [10] presented the multimodal approach by combining two traits finger vein and fingerprint for secure authentication. The author made the acquisition of finger vein and fingerprint simultaneously and the result is fused with the help of nonlinear fusion approach.

Preethi [11] presented an approach to guard against the fake user. The author includes the three biometric traits for this approach such as fingerprint, face, and iris. The authors also discussed the liveness detection approach to determine the liveness of a recorded sample.

Rui Chen et al. [12] 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 technique can arrange among live irises and phony irises with excessive precision and low computational value.

Arun Ross [13] in this paper author proposed a framework design in which a liveness detector is used with a fingerprint matcher. Bayesian notion community (BBN) scheme that fashions the connection between healthy scores and liveness values is brought. 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. [14] in this paper author has discussed the study of secure system needs liveness detection in order to protect against spoofing attacks.An efficient actual-time face liveness detection set of rules based on photo 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. [15] 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.

RupinderWahla et al. [16] 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.

III. Proposed Model

Inourproposed approach ivenessdetectionissuedatsensor level for better authentication. If an input user sample is live only then the further processing takes place else the input user sample is declared fake/dummy. In this model the liveness of fingerprint is detected by perspiration method using a sensor 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, there are two stages i.e enrollment verification. In our proposed system at enrolment stage, a template of fingerprint and iris traits are stored in the database which is further used for comparing new samples in the authentication phase.

A. 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.

1) Image Acquisition Stage: Here in the proposed approach, a single sensor is used to acquire the fingerprint image and camera is used to acquire the iris images. Firstly, the fingerprint image is acquired and features are extracted from it.

2) Feature Extraction: Feature extraction is used to extract the features of both the modalities fingerprint and iris. These extracted feature set are stored in the template for the authentication of the user. In our proposed approach at enrollment stage, the template of fingerprint and iris traits are stored in the database as (shown in

figure 3), which are further used for comparing new data in the authentication phase.

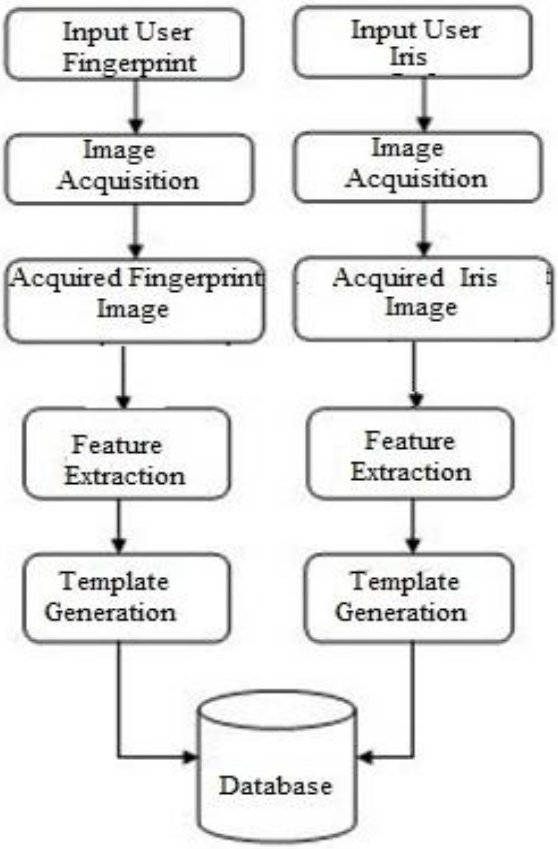

Fig. 3: Enrollment Phase

3) Authentication: In authentication phase firstly liveness detection is applied at sensor level for checking whether a newly captured sample is live or not as shown in figure 4. If the input user is alive, after that capture the fingerprint and iris extract 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 queried person is a genuine user otherwise its imposter.

B. Algorithm for authentication in proposed scheme

1) Acquisition stage.
2) Preprocessing stage.
3) Capture fingerprint from the sensor.
4) Liveness is checked at sensor level for both fingerprint and iris modalities by capturing user response of perspiration and eye blinking through a web camera.
5) If both inputs are live.
6) Then sample sends to feature extractor modules.
7) Else fake user.
8) Extract feature set.
9) Apply min-max normalization on both modalities.
10) Apply matching score level fusion using simple sum rule on normalization scores.

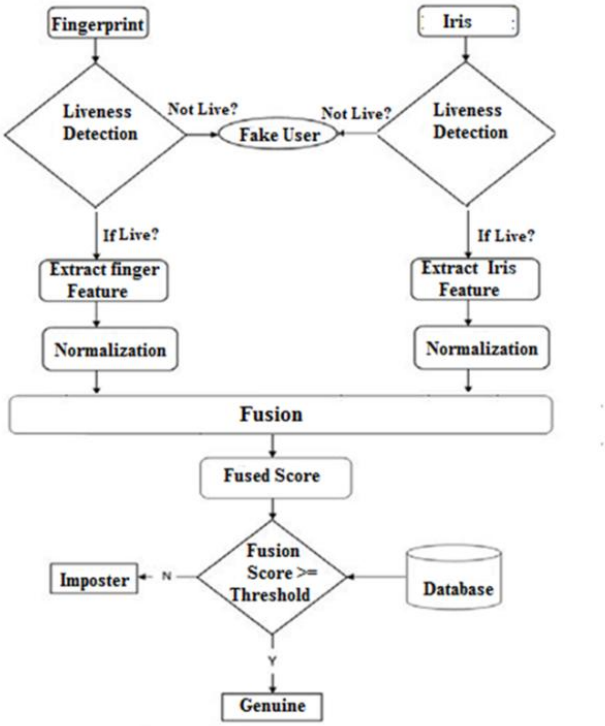

Fig. 4: Proposed Approach Architecture

1)Mathematical Terms: There are two mathematical terms that are using during algorithm.

Min-Max Normalization

The individual feature vectors of fingerprint and iris may be significantly different in terms of their range and distribution. For example, the value of fingerprint 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:

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

Here:
Si' −Normalized Score;
Si-Matching Score;
$Smin$-Minimum Matching Score;
$Smax$-Maximum Matching Score;

Simple Sum Rule Fusion Method

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

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

IV. Result and Implementation

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

The performance of proposed modal is measured using GAR (Genuine accept rate) and FAR (False accept rate) [17], [18].

$$\text{FAR} = \frac{Number\ \ of\ false\ \ acceptance}{Number\ \ of\ identification\ \ \ attempts}$$

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.

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

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 rat

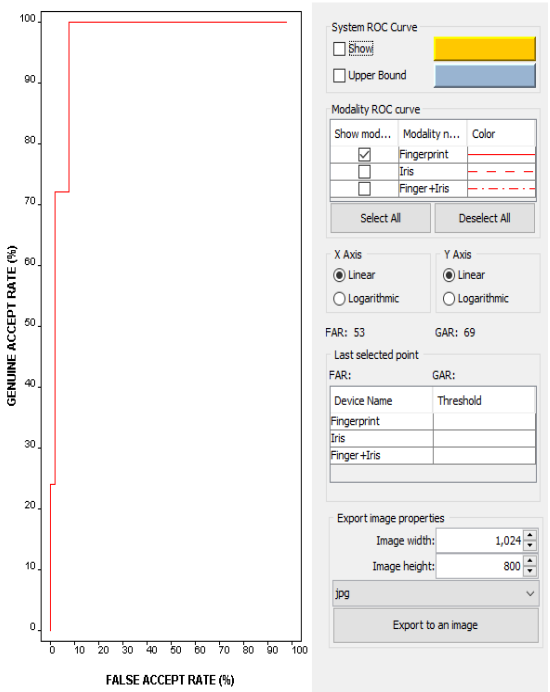

Fig. 5: Roc Curve for Fingerprint Modality

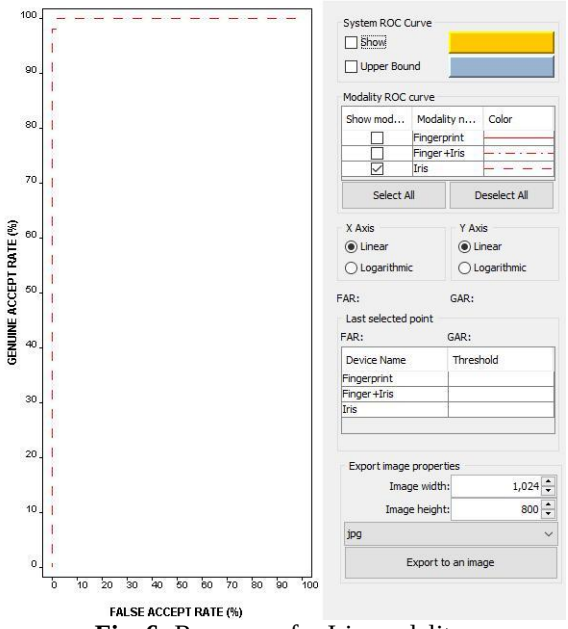

Fig. 6: Roc curve for Iris modality

Mubi integration tool is used for implementing the proposed scheme. The platform used for execution of the proposed scheme is 64 bit OS (Window 10) with i5 processor and 4GB RAM.

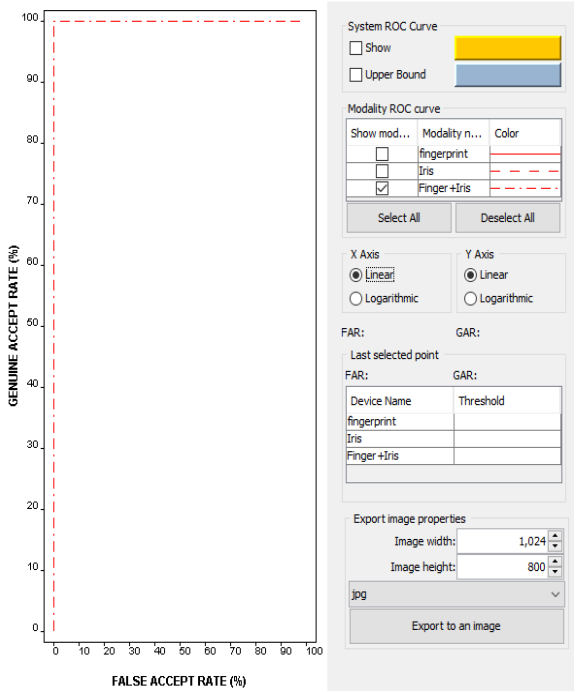

Fig. 7: Roc curve for Finger+Iris

Table 1: The result of the experiment

S.No.	Biometric Technologies	GAR	FAR
1.	Fingerprint	98	8
2.	Iris	98	2
3.	Finger + Iris	98	0

1) Advantages of the proposed scheme:
- FAR (false acceptance rate) and FRR (false reject rate) have been reduced.

2) Drawbacks of the proposed scheme:
- Extra storage space is required for storing the two (fingerprint, iris) modalities.

References

[1]. K. Sondhi and Y. Bansal "Concept of Unimodal and Multimodal Biometric System," International Journal of Advanced Research in Computer Science and Software Engineering, 4(6), 2014.
[2]. K. Sasidhar, V. L. Kakulapati, K. Ramakrishna, and K. K. Rao, "Multimodal Biometric Systems–Study to Improve Accuracy and Performance," Vol. 1, No. 02, 2010.
[3]. V. Sireesha and K. Sandhyarani, "Overview of Multimodal Biometrics," IJPAPER, Vol. 4, 170-173, 2013.
[4]. M. S. Ahuja and S. Chabbra, "A Survey of Multimodal Biometrics," 2011.
[5]. S. Chakraborty, D. Das "An Overview of Face Liveness Detection," 2014.
[6]. S. Girdhar and C. Kant, "A Novel Approach For Detecting FngerprintLiveness," IJIACS 4(6), 10-16, 2015.
[7]. G. Nalinakshi, S. M. Hatture, M. S. Gabasavalgi and R. P. Karchi, "Liveness Detection Technique For Prevention of Spoof Attack in Face Recognition System," Vol. 03, No. 12, 2013.
[8]. A.Gambhir, S. Narke, S, Borhade and G. Bokade, "Person recognition using multimodal biometrics," Int. J. Emerg. Technol. Adv. Eng., ISSN No: 2250-2459, 2014.
[9]. M. Abdolahi, M. Mohamadi, and M. Jafari, "Multimodal Biometric System Fusion Using Fingerprint and Iris With Fuzzy Logic," International Journal of Soft Computing and Engineering, 2(6), 504-510, 2013.
[10]. BM Shruti, MM Pooja, RG Ashwin, "Multimodal Biometric Authentication Combining Finger Vein and Fingerprint," International Journal of Engineering Research and Development, (10), 43-54, 2013.
[11]. P. V., and S. Chidambaram, "Fake Multi-Biometric Detection For Applications of Fingerprint and Iris and Face Recognition," 2013.
[12]. R. Chen, X. Lin, T. Ding, "Liveness Detection For Iris Recognition Using Multispectral Images," Pattern Recognition Letters, 33(1), 1513-1519, 2012.
[13]. E. Marasco, Y. Ding, A. Rose, "Combining Match Scores With Liveness Values in a Fingerprint Verification System," BTAS, 418-425, 2012.
[14]. S. Narayanan K, M. ReenaK.E, "Real Time Face Liveness Detection" International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering, Vol. 3, Issue 1, 2016.

[15]. M. Anusha, 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, 2016.
[16]. A. S. Buddharpawar, S. Subbaraman, "Iris Recognition Based on PCA For Person Identification," International Journal of Computer Applications, (0975 – 8887), 2015.
[17]. A. K. Jain, K. Nandakumar, A. Ross, "Score Normalization in Multimodal Biometric Systems", The Journal of Pattern Recognition Society, 38(12), 2270-2285, 2005.
[18]. A. K. Jain, A. Ross, and P. Flynn, "Handbook of biometrics," Springer, 2008.

Mukesh Rani "A Hybrid Approach for Raising Biometric System Security by Fusing Fingerprint and Iris Traits." IOSR Journal of Computer Engineering (IOSR-JCE) 20.3 (2018): 54-62.