A Review on Biometric Recognition and Authentication system for Biometric Fusion

Renuka Rattan

Guide Name: Er.Kumud Sachdeva

Computer Science and Engineering, Indo Global Colleges of Engineering

Punjab Technical University, Jalandhar, (India)

ABSTRACT

Biometric Fusion refers to combining two different biometric in order to enhance the security measures. A lot of biometric patterns are already being used in the daily life. For example, it is often seen that a smart phone comes with the finger print scanner which uses a finger as security pattern to unlock the phone. Nowadays fusion of biometric has gained a lot of attention in research industry. This paper reviews the existing techniques of Biometric Fusion. This paper also lights up classification techniques which includes Artificial Intelligence. The advantages and disadvantages associated with various modalities of biometric systems are represented in this paper along with a comparison between the different modalities of biometrics on the basis of biometric sample, accusation device, feature to be extracted and matching algorithm.

Keywords: Biometric, Fusion, Feature Extraction, Classification

I. INTRODUCTION

Traditionally, the identity management systems were relied on cryptographic methods requiring users to remember a secret text (password) or keep something with them (token, card) or a combination of both to prove their identity. Textual passwords and tokens were required in order to gain access to the desired resources, for instance; entrance control, computer logins, e-mail checking, making bank transactions, boundary control, welfare pay-outs etc. However, remembering secret passwords was a very difficult task for the user, and also the token/card for identity recognition could be stolen or misplaced. As an answer, the research community proposed the idea of human identification based on physiological or behavioral attributes of individuals very often termed as "Biometrics".

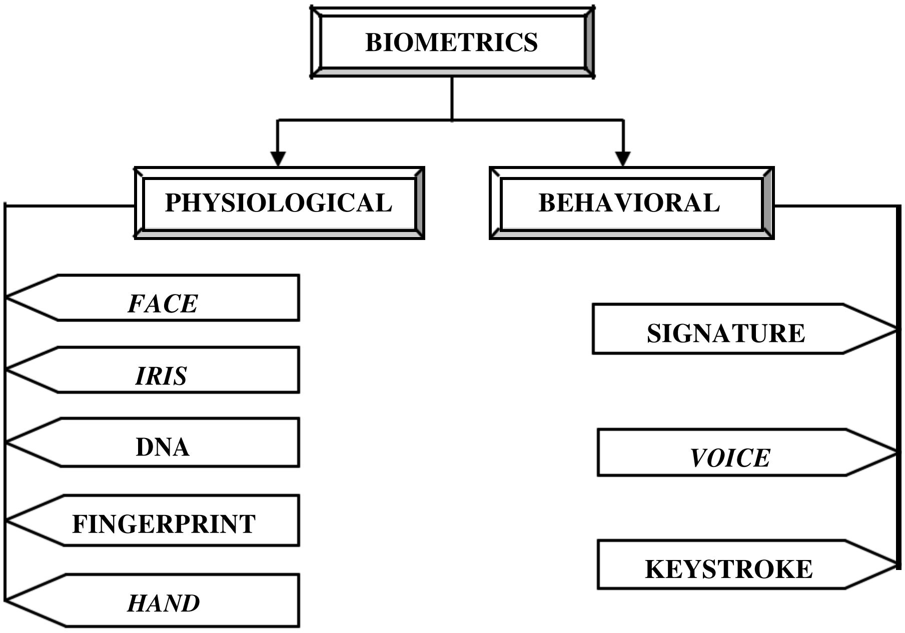

Figure 1: Classification of the biometric feature

Computer science describes biometrics as automatic recognition of individuals through their unique attributes i.e. Physiological (fingerprint, face, iris etc.) or Behavioral (voice, signature etc.). It offers several advantages over knowledge and possession based approaches in such a way that there is no need to remember anything. Besides, biometric attributescannot be lost, transferred or stolen, and ensures better security because they are very difficult to forge. Moreover, they require the presence of the genuine user while granting access to the particular resources.

Table 1: Comparison of different modalities based on biometric sample, Accusation device with the feature extracted and matching algorithms

MODALITIES	BIOMETRIC SAMPLE	ACCUSATION DEVICE	FEATURE EXTRACTED	POPULAR MATCHING ALGORITHM
Facial Scan	*Face Image*	*Video Camera, PC Camera*	*Distance of specific facial features (eyes, nose, mouth)*	*Euclidian distance*
Iris Scan	*Iris Image*	*IR enabled Video Camera*	*Texture of the iris (freckles, coronas, strips, furrow, and crypts)*	*Hamming distance*
Fingerprint	*Fingerprint Image*	*Sensor*	*A friction Ridge curves-a raised portion, pore structure, indents and marks*	*String matching*
Voice Recognition	*Voice Recording*	*Microphone, Telephone*	*Words, tone*	*Hidden Markova Model*

In order to become a qualified biometric trait, every physiological or behavioral trait must satisfy the following criteria:

- Universality: Inherited by all humans,
- Distinctiveness: discriminative amongst the population,
- Invariance: the elected biometric attribute must be consistent with time,
- Collectability: mustbereadily collectible in terms of acquisition, digitization and feature extraction from the community,

i) *Performance:* concerns to the availability of resources and intrusion of real constraints in terms of data collection and assure to deliver high accuracy,

ii) *Acceptability:* compliance of population to suggest that attribute to recognition system,

iii) *Circumvention:* susceptible to duplication or impersonation in the case of deceitful attacks toward the recognition system.

II. BIOMETRIC SYSTEM

Biometrics refers to the automatic identification (or verification) of an individual by using certain physiological or behavioral traits associated with the person. A wide variety of applications require reliable verification schemes to confirm the identity of an individual requesting their service. Examples of such applications include secure access to buildings, computer systems, laptops, cellular phones and ATMs. Biometric systems make use of fingerprints, hand geometry, iris, retina, face, hand vein, facial thermograms, signature or voiceprint in order to verify a person's identity. They have an edge over traditional security methods moreover they cannot be easily stolen, shared and imitate. A general biometric system has a sensor module, a feature extraction module and a matching module.

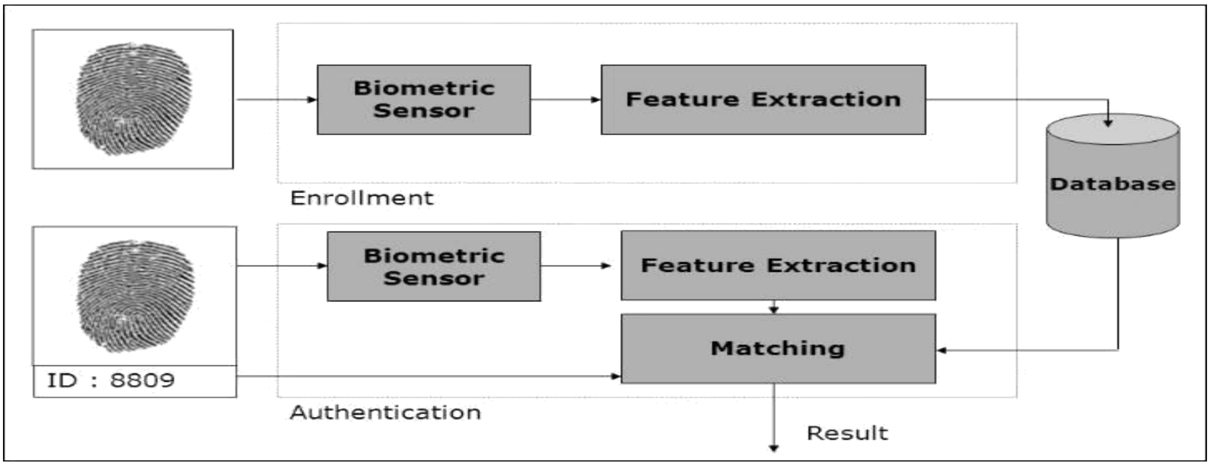

Figure 2: General Biometric System

Biometric systems based on single source of information are called as unimodal systems. The performance of a unimodal biometric system is largely affected by the reliability of the sensor used and the degrees of freedom offered by the features extracted from the sensed signal. Further, if the unimodal biometric trait being sensed or measured is noisy (a fingerprint with a scar or a voice altered by a cold, for example), the resultant matching score computed by the matching module may not be reliable. This problem can be addressed by installing multiple sensors that capture different biometric traits. Such systems, known as multimodal biometric systems are expected to be more reliable due to the presence of multiple pieces of evidence. These systems are also able to meet the stringent performance requirements imposed by various applications. For example, the feature extraction module of a fingerprint authentication system may be unable to extract features from fingerprints associated with specific individuals, due to the poor quality of the ridges. In such instances, it is useful to acquire multiple biometric traits for verifying the identity. Multimodal systems provide anti-spoofing measures that make it difficult for an intruder to spoof multiple biometric traits simultaneously. Studies have demonstrated . that multimodal biometric systems can achieve better performance compared with unimodal systems.

The performance of a biometric system can be measured by reporting its false accept rate (FAR) and false reject rate (FRR) at various thresholds. The FAR and FRR are computed by generating all possible genuine and impostor matching scores and then setting a threshold for deciding whether to accept or reject a match. A genuine matching score is obtained when two feature vectors corresponding to the same individual are compared, and an impostor matching score is obtained when feature vectors from two different individuals are compared.

2.1 FUNCTIONALITY OF BIOMETRIC SYSTEM

The functionality of the biometric system is defined in the terms of verification and identification.

VERIFICATION: It refers to 1:1 matching. Verification is also known as authentication, the user claims an identity and system verifies whether the claim is genuine or not

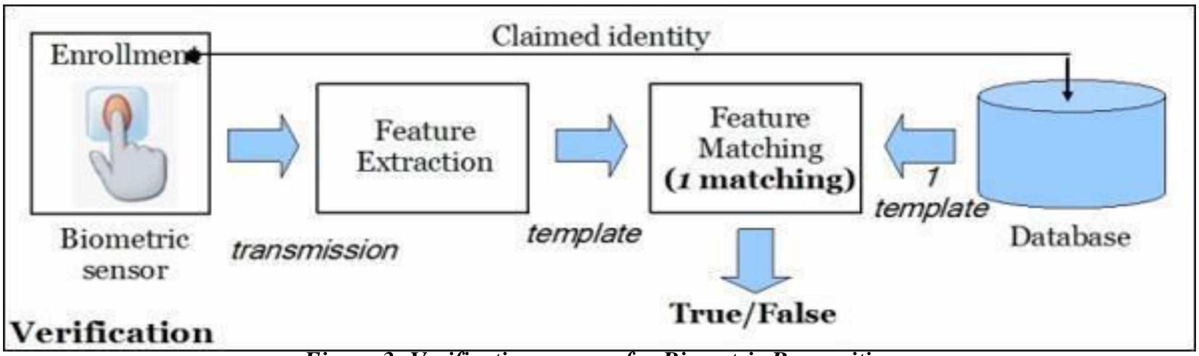

Figure 3: Verification process for Biometric Recognition

IDENTIFICATION: It refers to 1: m matching. In this situation user does not know its identity, it is simply presenting its bio-metrics for matching with whole database. User's template is matched with all the templates stored in database to identify with which template it has highest similarity.

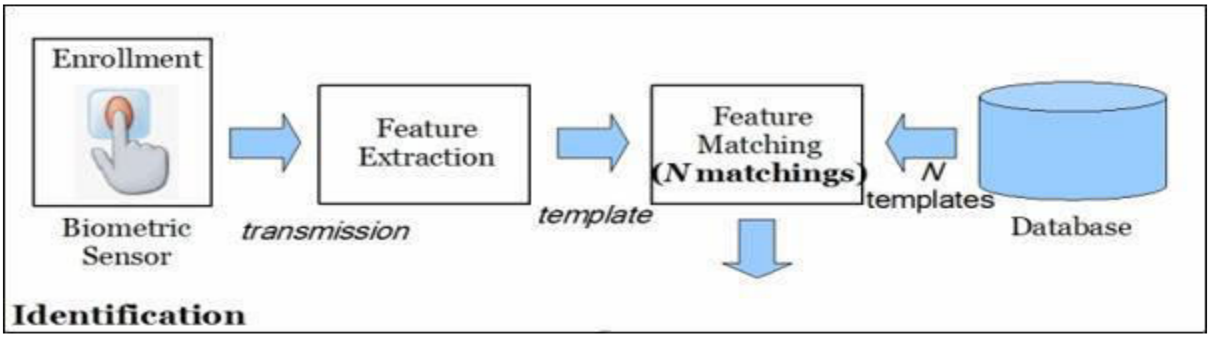

Figure3: Identification process for Biometric Recognition

III. WORKING OF A GENERAL BIOMETRIC SYSTEM

The working of a biometric system is quite simple and works in two phases training and classification respectively. Any biometric system if first trained with the data which will be used further for the classification. A lot of daily life examples are often seen, as for example, the working of a fingerprint sensor on any phone. It stores the pattern of the fingerprint in the system and then identifies the finger every time the finger is kept on the sensor. The process can be easily understood with the following architectural diagram.

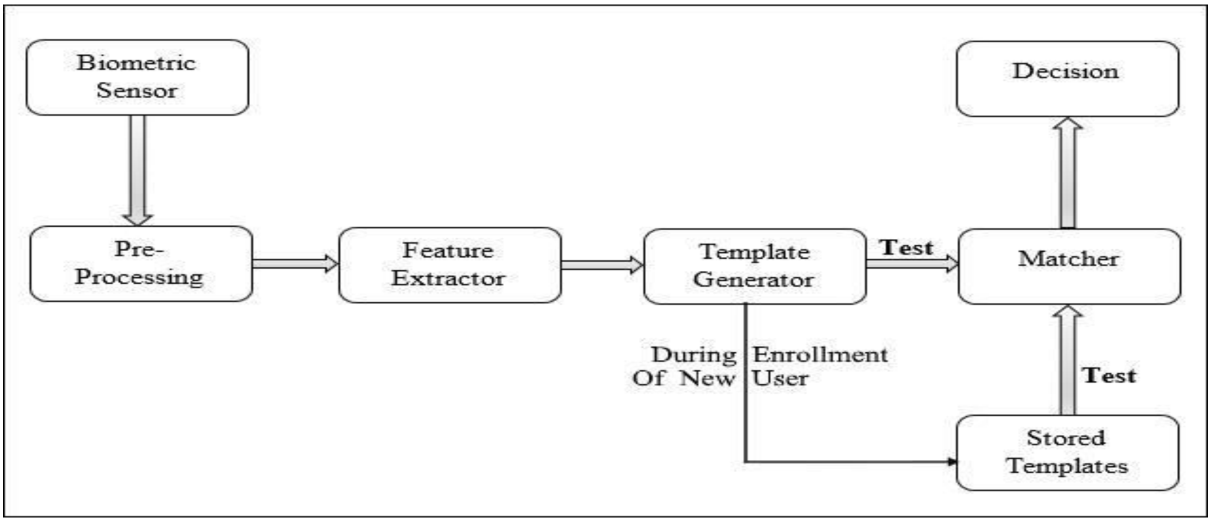

Figure 4: Working of a general Biometric System

The initial state is called as enrollment. In this stage, the information is stored by the user within the biometric system. Later while operating, the information in the biometric system is matched and identified with the previously collected information in the enrollment. Ensure that the retrieval and the storage of the information have been executed in a secure manner. The first block i.e. the Biometric Sensor, commonly known as 'sensor', acts as an interface between the biometric system and the real world and acquires all the necessary data. Usually, it is a picture acquisition system but can change depending on the desired characteristics of the system. The second block i.e. Pre-processing, performs the required pre-processing, eliminate the artifacts from the sensor, and enhances the input. In the next Block i.e. Feature Extractor, the essential and required characteristics are extracted. This is a crucial stage as one needs to extract the right features in an optimal way. In the following block i.e. Template generator, the image or vector of the numbers with specific properties is used for creating templates. The template is a combination of the related features extracted from the source. Elements of biometric measurements that are not expected for comparison algorithms are isolated in templates in order to reduce the size of a file and also for preserving the identification of an enrolled user. During the enrollment, the template is stored in the database or on a card. And while the matching process is executed, the procured template is carried on to the individual that is matching it with the existing one, judging the space between these two utilizing the algorithm. The matching program assesses template with input. This then becomes the output for particularized target.

IV. FUSION IN BIOMETRICS

As the feature set holds extended knowledge regarding the input biometric data than the matching score or the output decision of a matcher, therefore, fusion at the feature level is supposed to provide sufficient recognition results. However, fusion at this level is complex to achieve in practice because the feature sets of the several modalities may not be suitable, and most of the popular biometric systems do not grant access to the feature sets which they employ. There are three possible levels of fusion that are briefly described below:

i. Fusion at the feature extraction level

In feature extraction level of fusion, the signals are initially processed and feature vectors are extracted individually from the each biometric attribute. Subsequently, these feature vectors are merged to create a composite feature vector which is further utilized for classification. Since features bear abundant information of biometric attribute than matching score or decision of matcher, therefore the fusion at the feature level is presumed to give excellent results for recognition.

ii. Fusion at the matching score level

Match score-level fusion is also called confidence-level fusion. In matching score level, the feature vectors are processed exclusively and the individual matching score is determined and ultimately these matching scores are fused to create classification. Several statistical learning techniques may be employed to merge match scores.

iii. Fusion at the decision level

In decision level fusion, each modality is initially pre-classified individually i.e. each biometric attribute is apprehended, and later the features are extracted from that particular attribute. The final classification is based upon the fusion of the outputs of different modalities. This is the highest level of fusion with respect to human interface. In other words, the decision from each biometric system is gathered to deliver the final decision.

V. PROS AND CONS OF BIOMETRIC TECHNIQUES

There are various biometric techniques that are being used by various security system. All these techniques have some positive and some negative points associated with them.

Table 1: Pros and Cons of Biometric Modalities

BIOMETRIC MODALITIES	PROS	CONS
FACIAL	1. It does not require any co-operation of the test subject to do any work. 2. Systems set up in open public areas can easily identify an individual among the massive crowd. 3. It performs massive identification which usually other biometric system can't perform.	1. Facial recognition is not much effective for low resolution images. 2. Face recognition isn't perfect and faces challenges for instance associated with the varying position of face. 3. It doesn't work effectively in bad lighting, sunglasses, lengthy hair, or other objects that partly covers the subject's face.

IRIS	1. An iris scan can be carried out through 10 cm to a few meters apart. 2. High accuracy and High recognition process speed. 3. Data capturing can be carried out even though a user is putting contact lenses or glasses.	1. The scanning devices are often hard to adjust and may annoy multiple people of various heights. 2. The accuracy of scanning devices may impacted by unusual lighting effects and illumination from reflective types of surfaces. 3. Iris scanners tend to be more expensive in comparison with additional biometrics.
FINGERPRINT	1. It is easy to use along with the high verification process speed and accuracy. 2. A fingerprint pattern has individually distinctive composition and characteristic remains the same with time. 3. One should not have to remember long passwords, you simply swipe your finger on scanner and done it.	1. Fingerprint scanning system could be cheated by employing artificial fingers or perhaps showing another person's finger. 2. Sometimes it may take many swipe of fingerprint to register. 3. Cuts, marks transform fingerprints which often has negatively effect on performance.
VOICE/SPEECH	1. Speech can be recommended as a natural input as it does not demand any training and it is considerably quicker as compared to some other input. 2. This technique helps those people who have difficulty of using their hands. 3. One of the major advantages of voice recognition technique is to cut back misspelled texts of which many typists may perhaps suffers a problem during typing.	1. Voice recognition systems very often may make mistakes, when there is disturbance or some noise in the surrounding. 2. Voice Recognition systems may be hacked with some pre-recorded voice messages. 3. Several words sound very similarly. Case: two, to, too. This may sometimes confuse the system.

VI. RELATED WORK

Kamal Hajari et al, provided a brief review of challenges, databases, and algorithms for iris recognition. The noisy imaging conditions, as well as constrained conditions, influences the performance of iris recognition system. Most of the researchers concentrated on the steps of iris recognition system by taking up some concerns and their noise identification and extraction algorithms. From this study, it has been observed that most of the researchers are not able to find flawless and reliable resolution to all the challenges considered in this paper. Most of the methods and algorithms were examined on the databases gathered by various organizations and certain attempts were also made to estimate the accuracy of the systems designed. From the performance evaluation, it has been observed that there is still a scope for enhancements in the existing approaches dealing with the noisy environment.

Navjot Kaur et al, reviewed the steps associated in iris recognition system and several techniques used by different researchers for every recognition step. The need for iris recognition is expanding day by day because of the authenticity, efficiency, and uniqueness. It is the most effectual identification feature among all other biometric features as human iris remains constant throughout the whole of the life. The author eventually concluded that for the effective functioning of iris recognition system, researchers still have to work on numerous challenges like images taken in an unconstrained environment, noisy images, blurred images and several more.

Gursimarpreet Kaur et al, illustrated several biometric modalities and also these are analyzed on the basis of various aspects. Feature sets of these modalities are also represented Biometric is automated process of identifying an individual based on its biometric characteristics. It is quite reliable as compared to traditional methods of authentications. Biometric is primarily developed based on methods of pattern recognition. Nowadays, biometric is representing a vital component in various application areas such as military, forensic, controls, access etc. Iris seems to be most valid biometric but actual usage depends on the type of application. Although there are some difficulties with biometric systems but it is also becoming an emerging technology in the field of security.

Rupinder Saini et al,performed a comparison among the various biometric systems on the basis of their benefits and drawbacks. The author has provided an introduction to numerous biometric techniques undertaking the comparison examination concerning extensively used biometric identifiers and also the identification strategies. There are numerous apps along with alternative solutions employed in security techniques. Despite the fact the biometrics security systems have several issues like data privacy, physical privacy, and spiritual arguments etc., they still give benefits that may enhance our lives in such a way by raising security and efficiency.

VII. CONCLUSION

Biometric is defined as automatic recognition of individuals through their unique attributes i.e. Physiological or Behavioral. It offers several advantages over traditional approaches in such a way that there is no need to remember anything. Besides, biometric attributes cannot be lost, transferred or stolen, and ensures better security because they are very difficult to forge. In order to become a qualified biometric trait, every physiological or behavioral trait must satisfy certain specific criteria's. The functionality of the biometric system is defined in the terms of verification and identification. This paper will cover the various advantages and disadvantages associated with the biometric modalities. Nowadays fusion of biometric has gained a lot of attention in research industry, and in this paper the basic review of fusion in biometrics is presented along with the various levels of the fusion.

REFERENCES

1. Samarth Bharadwaj, MayankVatsa and Richa Singh, "Biometric quality: a review of fingerprint, iris, and face", EURASIP Journal on Image and Video Processing, pp. 34-62, 2014.
2. Mehdi Ghayoumi, "A review of multimodal biometric systems: Fusion methods and their applications", In IEEE/ACIS 14th International Conference on Computer and Information Science (ICIS), pp. 131-136, 2015.
3. Muhtahir o. Oloyede and Gerhard p. Hancke, "Unimodal and Multimodal Biometric Sensing Systems: A Review", In IEEE Access, Vol. 4, pp. 7532-7555, 2016.
4. Hajari, K. and Bhoyar, K., "A review of issues and challenges in designing Iris recognition Systems for noisy imaging environment", In International Conference on Pervasive Computing (ICPC), 2015 (pp. 1-6). IEEE.
5. Kaur, Navjot, and MamtaJuneja, "A review on iris recognition," In Engineering and Computational Sciences (RAECS), 2014 Recent Advances in, pp. 1-5. IEEE, 2014.
6. Mali, Kalyani, and Samayita Bhattacharya, "Comparative study of different biometric features," International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, no. 7, pp: 2776-2784, 2013.
7. Kaur, Gursimarpreet, and C. K. Verma, "Comparative analysis of biometric modalities," International Journal of Advanced Research in Computer Science and Software Engineering 4, no. 4 (2014): 603-613.
8. Saini, Rupinder, and NarinderRana, "Comparison of various biometric methods," International Journal of

Advances in Science and Technology (IJAST) 2, no. 1 (2014): 2.

9. Dolly Choudhary, Shamik Tiwari and Ajay Kumar Singh, "A Survey: Feature Extraction Methods for Iris Recognition", International Journal of Electronics Communication and Computer Technology (IJECCT), Vol. 2, No. 6, 2012, pp. 275-279.
10. Z. Sun, H. Zhang, T. Tan, and J. Wang, "Iris image classification based on hierarchical visual codebook," IEEE Trans. Pattern Anal. Mach. Intell., vol. 36, no. 6, pp. 1120–1133, 2014
11. J. Galbally, S. Marcel, and J. Fierrez, "Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition," IEEE Trans. Image Process., vol. 23, no. 2, pp. 710–724, 2014
12. Sudipta Roy, Abhijit Biswas, "A Personal Biometric IdentificationTechnique based on Iris Recognition,"
13. (IJCSIT) International Journalof Computer Science and Information Technologies, Vol. 2 (4) ,2011, 1474-1477
14. Elgamal, Mahmoud, and Nasser Al-Biqami, "An efficient feature extraction method for iris recognition based on wavelet transformation," Int. J. Comput. Inf. Technol 2, no. 03 (2013): 521-527.
15. X Li, Z Sun, T Tan, "Predict and improve iris recognition performance based on pairwise image quality assessment", in Proceedings of the International Conference of Biometrics, June 2013, pp. 1–8.