# OPTIMIZING ANDENHANCEMENT OF SECURITY OF MULTIMODAL BIOMETRIC SYSTEM– A Research

**Poonam[1], Asst. Prof. Santosh Kumar Mishra[2]**

*[1, 2] Department Of Computer Science & Engineering BRCM College Of Engineering And Technology, Bahal MDU, (India)*

## ABSTRACT

*Cryptography is used for security and authentication of data. Therefore it is used in biometrics system for keeping it safe and away from frauds. When we are using biometrics we ensure that, it is specially used for authentication and verification for the person's template. This template can be misused if it is stolen by any non-authenticate person. Focusing on biometric template security is the main discussion of our paper. Basically biometrics used two modalities Fingerprint and Iris biometrics characteristics. This significant feature of biometric helps us to identify any person template. That features are stored using feature level fusion and that fused vector is encrypted using different security technologies. Mixing is done using extracting important features and characteristics of modalities. In this review paper we focus on how our system is secure when we are using selective encryption method for encrypting the biometric template.*

**Keywords: Biometrics, Cryptography, Encryption Fused Vector, Fusion, Multimodal, Templates,**

## I. INTRODUCTION

Now a days, biometrics has been using in every area for giving authority to the authorize user of the esteemed organization. Biometrics and cryptography are the significant points of the recognizing the person and providing security to that template.

Biometrics gives identification and verification to the template of authorize user where as cryptography gives authentication to that template. So, both the technologies are interconnected based on providing security to the user's essential object.

### Biometric operations & modules

A biometric system can be either an 'identification' system or'verification'
(authentication) system, which are defined below.

a) **Identification** (1: n) One-to-Many: Biometrics can be used to determine a person's identity even without his awareness or approval. Such as scanning a crowd with the help of a camera and using face recognition technology, one can verify matches that are already store in database.

b) **Verification** (1:1) One-to-One: Biometrics can also be used to verify a person's identity. Such as one can allow physical access to a secure area in a building by using finger scans or can grant access to a bank account at an ATM by using retina scan.

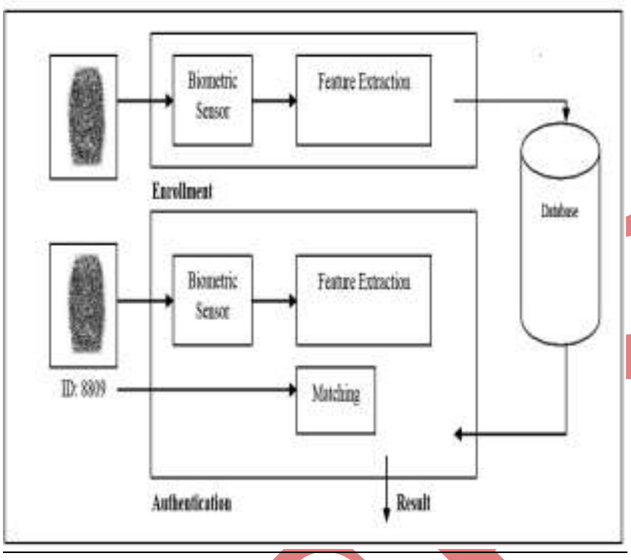


**Fig.1.1 Biometric System Modules**

## Biometric Characteristics

"Biometrics" means "life measurement" but the term is generally coupled with the use of unique physiological characteristics to identify a person, some other characteristics of biometrics are:

a) **Universal**: Every person must possess the characteristic. The trait must be one that is universal and seldom lost to accident or disease.

b) **Invariance of properties:** They should be constant over a long time. The trait should not be focus to considerable differences based on age either episodic or chronic disease.

c) **Measurability**: This should be suitable for capture without waiting time and must be easy to gather the attribute data passively.

d) **Singularity:** Each expression of the element must be distinctive to the person. The characteristics should have adequate distinctive properties to distinguish one person from other. Height, weight, hair and eye color are all elements that are unique assuming a mostly accurate measure, but do not offer enough points of separation to be useful for more than categorizing.

e) **Acceptance**: The capturing should be possible in a manner acceptable to a large fraction of the residents. Excluded are particularly persistent technologies, such technologies which is require a part of the human body to be taken or which (apparently) impair the human body.

f) **Reducibility:** The captured data should be able of being reduced to a file which is easy to handle.

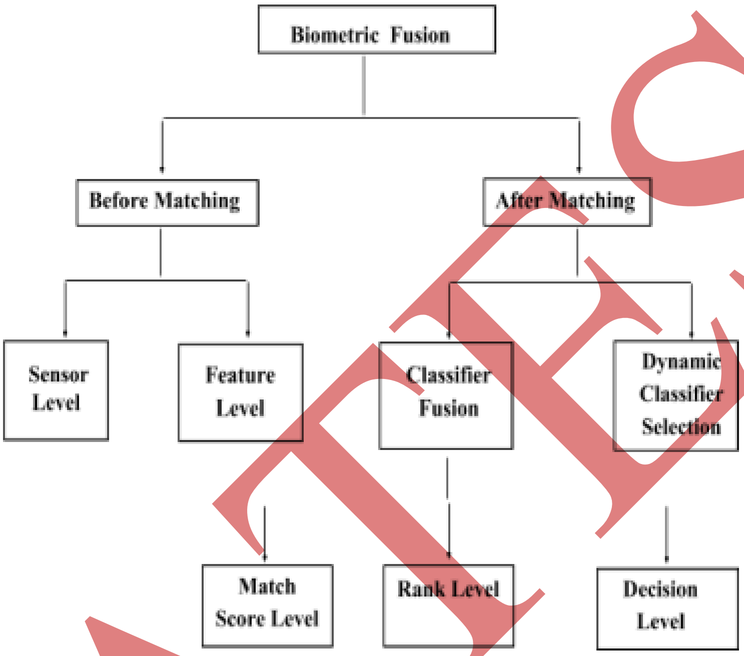
g) **Reliability and tamper-resistance**: The attribute should be impractical to mask or modify. Process should make sure high reliability and reproducibility.

h) **Privacy:** This process should not break the privacy of the individual.

**i) Comparable**: They should be able to reduce the trait to a state that makes it is digitally comparable from others. It has less probabilistic for similarity and more dependable on the identification.

j) **Inimitable**: The trait must be irreproducible by other way. The less reproducible the trait, the more likely it will be reliable.

**Biometric Authentication System** The process of identifying an individual using security systems is called authentication. It simply ensures that the individual is who he or she claims to be, but tells nothing about the access rights of the individual. Current authentication methods can be classified into three main areas.



**Fusion at Various Levels in Biometric Systems**

a) **Token based techniques** are widely used for authentication using key cards, bank cards and smart cards. Many token-based authentication systems also use knowledge based techniques to enhance security. For example, ATM cards are generally used together with a PIN number.

b) **Knowledge based techniques** are the most widely used authentication techniques. These techniques include both text-based and picture-based passwords.

**Biometric based authentication techniques** uses a biometric authentication system which is essentially a pattern recognition system that operates by acquiring biometric data from an individual such as fingerprints, iris scan, or facial recognition, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. However, this technique provides highest level of security. Passwords and cards can be shared and thus cannot provide reliability. Biometric identifiers cannot be shared, misplaced, And they intrinsically represent the individual's identity. Templates are used during the biometric authentication process where a biometric template (or simply template) is a digital reference of distinct characteristics that have been extracted from a biometric sample. A biometric authentication system mainly comprises following functional units. Sensor device for acquisition of biometric raw data, feature extraction for template creation, matcher to compare the actual biometric template with the stored templates and system database for storing the biometric templates. Biometric systems serve one of two foundational purposes either verification/authentication or identification. Identification refers to the ability of a computer system to uniquely distinguish an individual from a larger set of individual biometric records on file (using only the biometric data). A biometric system consists of modules which work perpetually to authenticate and verify users. Widespread application of biometric based authentication leads to new problem of security and privacy. Security is a significant aspect of any authentication system and there are various ways to secure the system. The most potentially damaging attack on a biometric system is against the biometric templates that are stored in the system database. Biometric templates are actually compared in a biometric recognition system. So, special attention is given to Template Security which is achieved by Feature Transformations or Biometric Cryptosystems. A cryptographic construction that operates in the key binding mode proposed by Ari Juels and MadhuSudan[5] is Fuzzy vault i.e. state of the art technique. Fuzzy vault can handle intra-class variations in the biometric data. In this scheme, real minutiae points are evaluated using single polynomial and chaff points are added to vault for concealing real minutiae points. Biometrics and cryptography are the significant points of the recognizing the person and providing security to that template. Biometrics gives identification and verification to the template of authorize user where as cryptography gives authentication to that template. So, both the technologies are interconnected based on providing security to the user's essential object. Here, we are using two modalities Fingerprint and Iris are the two modalities discuss in our paper. Fingerprint module takes fewer times, in taking the fingerprint template, as its size is smaller it will take reasonable time in taking the Fingerprint template and accepting the template. In Iris system what happens that this system is accepting everywhere, at the time of capturing the eye image no physical interaction is needed with the sensors. Biometrics recognition is done through two distinct methods Evidence Identity, Confirmation of Template.

**1) Evidence Identity**: In identity provision the unknown person's template is first checked with the stored database then identity is given to the unrecognized person. The identity is given with the name and the Identification Number and the record is stored successfully.

2) **Confirmation of Template**: When the identified person is giving his identity then the sensors should verified the person.

## II. MULTIMODAL BIOMETRIC SYSTEMS

In unimodal system we are using only one system as only single Fingerprint System, Iris System or Face Recognition System. Lots of problems has to face, when we are using uni modal biometrics system. When the trait of biometrics has taken then the sometimes noise enters with the trait, that results in higher the false rejection rate. Also, when we are using the only single system then the database template can be stolen and it can be revoked by any intruder as it contains only one template. If person has been facing difficulty in giving template because of injury or damage of physical part of that person then the he can't use that system.

### Why Multimodal Biometric

In this case multimodal system is the best choice for identification of the person without fail. In multimodal biometrics system we are using two modalities for recognition of person. In our paper we discuss the Fingerprint and Iris characteristic. We discuss here how we are fusing the two biometric system and that fused method is storing in the database using encrypting method. Multi biometrics system has lots of advantage as follows:

(i) Its makes better system operation .

(ii) Its accuracy is better as compared to the uni biometric system.

(iii) It prevent from stolen the templates of biometric system as at the time it stores the two characteristics of biometric system in the database.

## III. RELATED STUDY

**In [1] Rupesh wagh , in august 2013**. Here, author discussed regarding how our system is secure when we are using selective encryption method for encrypting the biometric template. Cryptography is used for security of data. This cryptography we used in biometrics system. Where he ensured that while using biometrics, which is basically used for authentication and verification by the person's template. But that template can be misused if it is stolen, by any perpetrate. Focusing on biometric template security is the main discussion of his paper. Multimodal biometrics used two modalities Fingerprint and Iris biometrics characteristics. The significant features are taken from biometric template. That features are stored using feature level fusion and that fused vector is encrypted using different security technologies. Fusion is done using extracting important features of modalities [1].

**In [2] Abhishek Nagar in july 2009** discussed that Security concerns regarding the stored biometric data is impeding the widespread public acceptance of biometric technology. Though a number of bio-crypto algorithms have been proposed, they have limited practical applicability due to the trade-off between recognition performance and security of the template. In this paper, we improve the recognition performance as well as the security of a fingerprint based biometric cryptosystem, called finger print fuzzy vault. We incorporate minutiae descriptors, which capture orientation and frequency information in a minutia's neighborhood, in the vault construction using the fuzzy commitment approach. Experimental results show that with the use of minutiae descriptors, the fingerprint matching performance improves from an FAR of 0.7% to 0.01% at a GAR of 95% with some improvement in security as well. An analysis of security while considering two different attack scenarios is also presented [2].

**In [3] Karthik Nandakumar in 2011** here author purposed that Multi biometric systems are being increasingly deployed in many large scale biometric applications (e.g., FBIIAFIS,UIDAI system in India) because they have several advantages such as lower error rates and larger population coverage compared to uni biometric systems. However, multi biometric systems require storage of multiple biometric templates (e.g., finger print, iris, and face) for each user, which results in increased risk to user privacy and system security. One method to protect individual templates is to store only the secure sketch generated from the corresponding template using a biometric cryptosystem .This requires storage of multiple sketches. In this paper, he proposed a feature level fusion framework to simultaneously protect multiple templates of a user as a single secure sketch. His main contributions include: (i) practical implementation of the proposed feature level fusion framework using two Well known biometric cryptosystems, namely, fuzzy vault and fuzzy commitment, and (ii) detailed analysis of the trade-off between matching accuracy and security in the proposed multi biometric cryptosystems based on two different databases (one real and one virtual multimodal database), each containing the three most popular biometric modalities, namely, fingerprint, iris, and face. Experimental results show that both the multi biometric cryptosystems proposed here have higher security and matching performance compared to their uni biometric counterparts [3].

**In [4] Kevin W. Bowyer in 2006** , The author categorizes approaches to multi-modal biometrics based on the biometric source, the type of sensing used, and the depth of collaborative interaction in the processing. This paper also attempts to identify some of the challenges and issues that confront research in multimodal biometrics [4].

**In [5]Shweta Malhotra in May 2013** , here author presents an approach to enhance the invisible watermarking technique with cryptography. The biometric trait is modified using invisible watermark information and is further secured using cryptography. The encryption algorithm which has been used is highly suitable for multimedia as well as text data. We can use different encryption techniques like AES, MAES etc .The template is made more secure using encryption and finally stored in database [5].

**In [6] Debnath Bhattacharyya** Advances in the field of Information Technology also make In separable part of it. In order to deal with security, Authentication plays an important role. This paper presents a review on the biometric authentication techniques and some future possibilities in this field. In biometrics, a human being needs to be identified based on some characteristic physiological parameters. A wide variety of systems require reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user, and not anyone else. By using biometrics it is possible to confirm or establish an individual's identity. The position of biometrics in the current field o f Security has been depicted in this work. We have also outlined opinions about the usability of biometric authentication systems, comparison between different techniques and their advantages and disadvantages in this paper [6].

## IV. METHODOLOGY

We implement the image enhancement and minutiae extraction on biometrics in order to separate the original image from the noise so that perfect minutiae can be extracted for further processing and provide security to the original template stored in the database. Here biometrics used two modalities Fingerprint and Iris biometrics characteristics. Steps included:-

## V. ALGORITHM LEVEL DESIGN

To implement a minutiae extractor, five-stages are used by me. They are as follows:

1. Contrast Limited Adaptive Histogram Equalization (CLAHE)
2. Segmentation
3. Ridge Orientation Estimation
4. Filtering
5. Minutiae Extraction
6. Minutiae Matching

For fingerprint image processing, CLAHE and Fast Fourier Transform are used for image enhancement. The image segmentation task is fulfilled by a three-step approach: block direction estimation, segmentation by direction intensity and Region of Interest extraction by Morphological operations.

## VI. CONCLUSION

We focus on the past study done by various authors in variety of parameters in order to improve the security of data. By using bio-metrics it is possible to confirm or establish an individual integrity. Many researches give their contribution in one or the other aspect towards the efficiency of data through biometric verification, some focused on the pattern reorganization using fuzzy commitment approach, some uses the sketches approach, other tries to improve the type of sensing method and depth of collaborative interaction, some uses various algorithms such as AES for improvement. In this review paper we focus on how our system is secure when we are using selective encryption method for encrypting the biometric template. The template stored in the database is not secure .In order to provide security to the template, cancelable biometrics is used which hides the original template from the intruders. To raise the security to the next level the template thus obtained from cancelable biometrics is encrypted using cryptography.

## REFERENCES

[1] Anil K. Jain, KarthikNandakumar, and Abhishek Nagar, Review Article Biometric Template Security, Department of Computer Science and Engineering, Michigan State University, 3115 Engineering Building, East Lansing, MI48824, USA

[2]. A. K. Jain, R. Bolle, and S. Pankanti, eds., Biometrics: Personal Identification in Networked Society. Kluwer Academic Publishers, 1999.

[3]. A. Juels and M. Sudan, “A fuzzy vault scheme,” in Proceedings of the IEEE International Symposium on Information Theory, p. 408, Piscataway, NJ, USA, June-July 2002.

[4.] Phillips, P. J., P. J. Flynn, T. Scruggs, K. W. Bowyer and W. Worek, “Preliminary Face Recognition Grand Challenge Results,” Aut. Face and Gesture Recog., 2006.

[5]. N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, “Generating cancelable fingerprint templates,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 561–572, 2007.

[6]. Y. Sutcu, H. T. Sencar, and N. Memon, “A secure biometric authentication scheme based on robust hashing,” in Proceedings of the 7thMultimedia and SecurityWorkshop (MMand Sec ’05), pp. 111–116, New York, NY, USA, August 2006.

[7]. A. B. J. Teoh, K.-A. Toh, and W. K. Yip, “2N discretisation of BioPhasor in cancellable biometrics,” in Proceedings of 2nd International Conference on Biometrics, pp. 435–444, Seoul, South Korea, August 2007.

[8]. RajkumarYadav, Rahul Rishi &SudhirBatra, “A New Steganography Method for Gray Level Images using Parity Checker”,International Journal of Computer Applications (0975-8887) Volume 11-No. 11, December 2010

[9]. RajkumarYadav et al. / International Journal on Computer Science and Engineering (IJCSE)

[10].D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, Springer, Berlin, Germany, 2003.

[11].A biometric template encryption by A.K.Mohapatra1, Madhvi Sandhu2 IGIT,GGSIP University, Kashmere Gate, Delhi Published in International Journal of Advanced Engineering & Application, Jan. 2010.

[12] Wayman, J. L., “A path forward for multi-biometrics,”ICASSP ’06, to appear.

[13] R.N. Kankrale, Prof. S. D. Sapkal. Template Level Fusion of Iris and Fingerprint in Multimodal Biometric Identification Systems, Department of Information Technology SRES.