# Fundamental Monitoring on Iris Recognition Based on Cryptosystem and Fusion Technique

Nilesh M. Verulkar[1]
Assistant Professor
Department of E&TC
MGI- Mauli CoET,
Shegaon, Maharashtra
nileshverulkar@gmail.com

Bharat K. Chaudhari[2]
Assistant Professor
Department of CSE
Dr. V.B.Kolte CoE
Malkapur, Maharashtra
mit2bharat@gmail.com

Rahul R. Ambalkar[3]
Assistant Professor
Department of E&TC
MGI- Mauli CoET
Shegaon, Maharashtra
ambalkar.rahul@gmail.com

***Abstract*— In the past the technique used for personal authentication system included memory based method (e.g. password) and token based method (e.g. ID cards). Traditional technique of personal identification are unable to fulfill strict security requirements while biometric based authentication system provide a good alternative to the traditional method because biometric characteristics are difficult to copy, share and distribute with as much ease password and tokes. Since biometric can't be lost or forgotten and there is nothing to remember or carry so these scheme are more reliable and more user friendly. Recently , strong efforts have been made to explore the feasibility of new anatomical triads (e.g. teeth, ECG , brain, iris etc) as new biometric measure besides the face , fingerprint , iris and hand geometric , to achieve a much reliable identification system which is difficult to disguise.**

**This scheme focuses is on human iris, iris is so unique that no two irises are same in nature, although even identical twins, left and right eye of the any human being. Cryptography has one among most effective ways and has been recognized as the most popular technology for the security functions. This paper show a methodology to protect individual templates is to store only the secure sketch generated from the corresponding template using a biometric cryptosystem.**

***Keywords—Iris, Cryptosystem, Fusion Technique***

## I. INTRODUCTION

The human iris recently has attracted the attention of biometrics-based identification and verification research. The iris is so unique that no two irises are alike, even among identical twins or even between the left and right eye of the same person. Security has been a major concern and is becoming increasingly important. Cryptography has become one of simple ways and has been recognized as the most popular technology for their operation such as security purposes. [4]

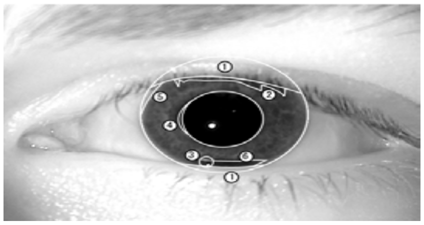

Fig. 1 Internal view of Human Iris

Iris recognition means is an automated method of identification of biometric like iris pattern that uses mathematical pattern-recognition techniques on images. This image is complex random patterns are unique and can be seen from some amount of distance. Figure 1 shows the internal view of a human iris.

The word "biometrics" is derived from the Greek words "Bio" means life and "Metrics" means to measure. Biometrics refers to the physiological or behavioral characteristics of a person to authenticate his/her identity [1] [2]. Many millions of persons in several countries around the world have been enrolled in iris recognition systems, for convenience purposes such as passport-free automated border-crossings, and some national ID systems based on this technology are being deployed. A key advantage of iris recognition, besides its matching speed and its extreme resistance to false matches is the stability of the iris as an internal, protected, yet externally visible organ of the eye.

The term iris recognition refers to identifying an iris image by computational algorithms. Iris recognition technology offers the high accuracy in identifying individuals as compared to any other method available in now days. Stability is a key advantage of iris recognition. The human different characteristic can be used as a biometric characteristic as long as it satisfies the following some requirements such as [4]

1. Universality 2. Distinctiveness 3. Permanence
4. Collectability 5.Performance 6.Acceptability
7.Circumvention

Comparison of some of the biometric identifiers based on the above seven factors as

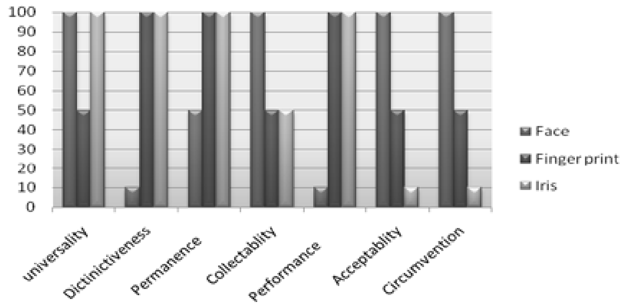

Fig. 2 Comparison of biometric identifiers

In today’s information technology world, security for systems is more important. The number of systems that have been compromised is ever increasing and authentication plays a major role as a first line of defence against intruders. The three main types of authentication technique as, as we know that passwords are notorious for being weak and easily crack able due to human nature. Cards and tokens can be presented by anyone and although the token or card is recognisable, there is no way of knowing if the person presenting the card is the actual owner. Biometrics, on the other hand, provides a secure method of authentication and identification, as they are difficult to replicate and steal.

The paper is organized as follow; section 2 emphasizes on a review of background information and shows relevant work. Section 3 focuses the overall system development. It also introduces embedding algorithm, fusion module and biometric cryptosystem. Section 4 expresses categorization of template protection schemes based on cryptosystem. Section 5 shows several different levels of the identification process for fusion technique. The conclusion is given at the end in section 6.

## II. BACKGROUND INFORMATION

### A. *Biometrics*

An automated recognition of individuals based on their behavioural and biological characteristics referred as biometric. Physiological and behavioural biometric characteristics are acquired applying adequate sensors to form a biometric template. Figure 3 shows that classification of biometric.

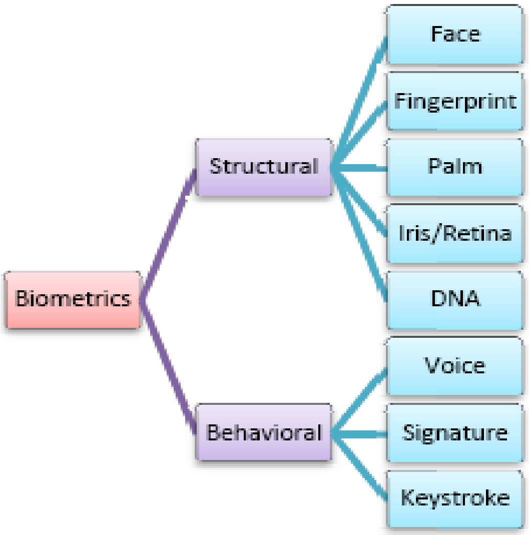

Fig. 3 Types of biometric

Biometrics is the “best” method for the identification and authentication purpose. The uniqueness of biometric is an undeniable reality known by all. Biometric can be basically divided into two categories which are structural e.g. face, hand geometry, veins patterns, fingerprints, iris patterns, retina patterns, DNA and behavioral e.g. voice, signature, keystroke.

### B. *Cryptosystem*

A mechanism which one can encode information content to an incomprehensible form and also recover the original content when required. It is well known that cryptography provides secrecy and authentication of data and ensures privacy in the communication by means of different cryptosystems.

### C. *Key management problem*

It is already known that the security of the standard cryptosystems relies on the assumption that both keys, the secret and the private keys, are unknown to anyone but the known to specific users. If the secret key or the private key is compromised, the security of the scheme is completely collapse [3].

### D. *Key bit length problem*

As the keys used are large (128–256 bits for symmetric cryptosystems and 1024–2048 for the asymmetric ones), it is impossible to be memorized. So, they are often stored in a password-protected place. As passwords can be easily stolen, forgotten or guessed using different attacks, it can be stated that a cryptosystem is as secure as it is the password used to store its secret key [3]. So ideally, the secure template should satisfy the following two properties:

- Non inevitability: given a secure template, it must be computationally difficult to find a biometric feature set that will match with the given template.
- Revocability: given two secure templates generated from the same biometric data, it must be computationally hard to identify that they are derived from the same data or obtain the original biometric data.

While biometric cryptosystems generally tend to have stronger noninvertibility, template transformation schemes typically have better revocability [1]. Cryptography means secret writing. It forms the basis for many technological solutions in computer and communication systems. The original message to be encrypted is called plaintext and the encrypted message is called cipher text. In order to get the original data back decryption is done.

### *E. Image Fusion*

Image Fusion produces a single image by combining information from a set of images using pixel and feature or decision level techniques. The fused image contains greater information than the individual image sources. Fusion strategies can be divided into two main categories: premapping fusion means before the matching phase and postmapping fusion means after the matching phase [4].

## III. System Development

It proposes a feature-level fusion framework for biometric cryptosystems that consists of three basic modules:

(i) Embedding algorithm ,
(ii) Fusion module , and
(iii) Biometric cryptosystem.

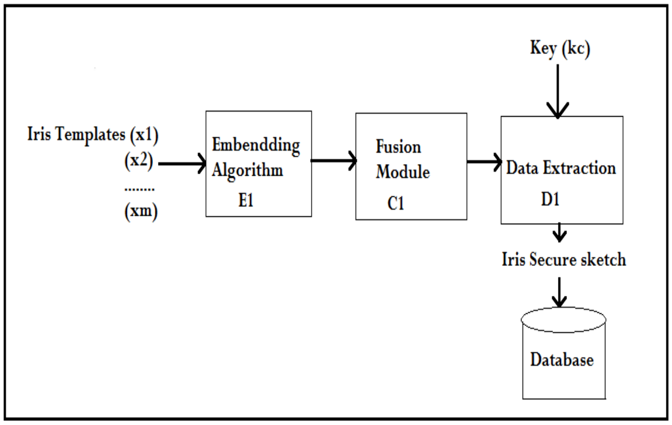

Fig. 4 biometric cryptosystem based on fusion module

The generic framework of the biometric cryptosystem is shown in above Figure 4. Suppose that we have a set of biometric feature representations, where represents the features corresponding to the biometric modality of a user, and represents the number of modalities, . The functionalities of the three modules are as follows:

- Embedding Algorithm:

The embedding algorithm transforms a biometric feature representation into a new feature representation, where, for all. The input representation can be a real-valued feature vector, a binary string, or a point-set. The output representation could be a binary string or a point-set that could be secured using fuzzy commitment or fuzzy vault, respectively.

- Fusion Module:

The fusion module combines a set of homogeneous biometric features Z= {z1, z2, ……, zm} to generate a fused biometric feature representation z. For point-set-based representations, one can use $z = C_s (Z) = U^{M}{}_{m=1}z_m$ .In the case of binary strings, the fused feature vector can be obtained by simply concatenating the individual strings, i.e. $z= C_b(Z) = \{z_1\ z_2 \ldots\ldots z_M\}$, Note that it is also possible to define more complex fusion schemes, where features could be selected based on criteria such as reliability and discriminability.

- Biometric Cryptosystem:

During enrollment, the biometric cryptosystem generates a secure sketch yc using the fused feature vector z^E (obtained from the set of biometric templates $X^E= \{x_1{}^E, x_2{}^E, \ldots\ldots\ldots,x_M{}^E\}$ and a key , i.e., $y_c=f_c (z^E, k_c)$. During authentication, the biometric cryptosystem recovers kc from yc and z^a(obtained from the set of biometric queries $X^A=\{x_1{}^A, x_2{}^A, \ldots\ldots\ldots,x_M{}^A\}$.

Fuzzy commitment is used if is a binary string, whereas a fuzzy vault is used if is a point-set. Each of the above three modules play a critical role in determining the matching performance and security of the multibiometric cryptosystem. The embedding algorithm should generate a compact representation that preserves the discriminability of the original biometric features. The fusion module should find the optimal trade-off between the discriminability and variability in the individual feature representations. The biometric cryptosystem should minimize the information leakage about the original biometric templates. Thus, optimizing each module is a challenging task in itself and is beyond the scope of this work.

## IV. CRYPTOSYSTEM

The main advantage of utilizing cryptography is its availability for high and adjustable security levels; on the other hand biometrics brings in nonrepudiation and eradicates the necessity to memorize passwords or to carry tokens. Several approaches, known as biometric template protection schemes, have been proposed. These schemes can be mainly classified into two categories: feature transformation approach and key formation.

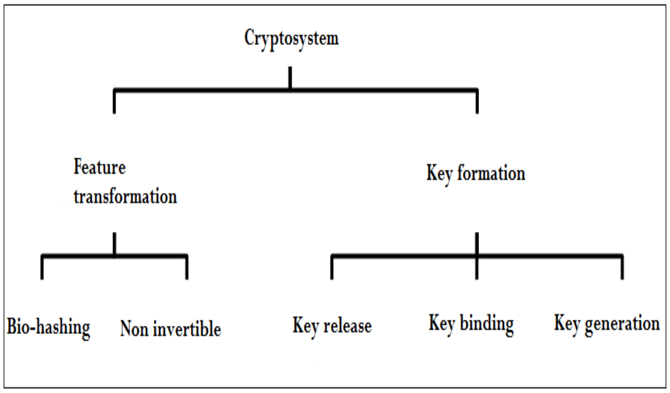

Fig 5 Categorization of template protection schemes

### A. *Feature transformation:*

Approach scheme basically consists of the application of a transformation function to the biometric template and subsequently, store the transformed template into a database. In the matching phase, the same function is first applied to the query templates and, then, the transformed query is directly matched with the transformed template in the transformed domain. Depending on the properties of the transformation function, the feature transformation schemes can be divided into invertible (salting) and non-invertible transformation [3].

1. Bio-hashing:

Bio-hashing is a template protection approach in which the biometric features are transformed using a function defined by a user-specific key or password. Since the transformation is invertible to a large extent, the key needs to be securely stored or remembered by the user and presented during authentication. This need for additional information in the form of key increases the entropy of the biometric template and hence makes it difficult for the adversary to guess the template. (Entropy of a biometric template can be understood as a measure of the number of different identities that are distinguishable by a biometric system.)

2. Non-invertible:

In this approach, the biometric template is secured by applying a noninvertible transformation function to it. Noninvertible transform refers to a one-way function, F, that is “easy to compute” (in polynomial time) but “hard to invert” (given F (x), the probability of finding x in polynomial time is small). The parameters of the transformation function are defined by a key which must be available at the time of authentication to transform the query feature set. The main characteristic of this approach is that even if the key and/or the transformed template are known, it is computationally hard (in terms of brute force complexity) for an adversary to recover the original biometric template.

### B. *Key Formation:*

It is either securing a cryptographic key using biometric templates or directly generating a cryptographic key from biometric templates. The main characteristic of these systems is that they need to generate public information related to the biometric template in order to perform the verification phase. This public information is called helper data and it should not reveal any important information about the biometric template [3].

Biometric cryptosystems classified into different ways:

1. Key release:

The biometric template and the key are stored as different entities in such a way that the key is to be released only after a successful biometric verification. Therefore the biometric verification phase and the key release mechanism are completely decoupled.

2. Key binding:

The biometric template is secured by binding it and a key within a cryptographic framework. Therefore they constitute a single entity depending on the biometric template, B, and the key K. In a key binding cryptosystem, the biometric template is secured by binding it and a key in a cryptographic framework, and both are stored in the database as a single entity as the helper data. E.g., fuzzy vault schemes, fuzzy commitment schemes.

3. Key generation:

A key is derived directly from the biometric template and it is stored in the database instead of the biometric template itself. E.g. fuzzy extractor.

## V. FUSION TECHNIQUE

Image Fusion produces a single image by combining information from a set of source images, using pixel, and feature or decision level techniques. The fused image contains greater information content for the scene than any one of the individual image sources alone. The reliability and overall detail of the image is increased, because of the addition of analogous and complementary information. Image fusion requires that images be registered first before they are fused.

### A. *Fusion Types:*

The biometric data can be combined at several different levels of the identification process as follow,

1. Data sensor level:

Data coming from different sensors can be combined, so that the resulting information are in some sense better than they would be possible when these sources were individually used.

2. Feature extraction level:

The data obtained from each sensor is used to compute a feature vector. As the features extracted from one biometric trait are independent of those extracted from the other, it is reasonable to concatenate the two vectors into a single new vector. The new feature vector now has a higher dimensionality and represents a person's identity in a different (and hopefully more discriminating) hyperspace. Feature reduction techniques may be employed to extract useful features from the larger set of features [11].

3. Matching-score level:

This is based on the combination of matching scores, after separate feature extraction and comparison between stored data and test data for each subsystem have been compiled. Starting from the matching scores or distance measures of each subsystem, an overall matching score is generated using linear or nonlinear weighting [4]. Each system provides a matching score indicating the proximity of the feature vector with the template vector. These scores can be combined to assert the veracity of the claimed identity. Techniques such as logistic regression may be used to combine the scores reported by the two sensors. These techniques attempt to minimize the FRR for a given FAR[11].

4. Decision level:

Each sensor can capture multiple biometric data and the resulting feature vectors individually classified into the two classes–accept or reject [9].Each biometric subsystem completes autonomously the processes of feature extraction, matching, and recognition. Decision strategies are usually of Boolean functions, where the recognition yields the majority decision among all present subsystems. Fusion at template level is very difficult to obtain, since biometric features have different structures and distinctiveness.

## VI. Conclusion

The main aim is to produce a simple and reliable iris recognition approach which is minimize the intra variance (FRR) and maximize the inter variance of the iris. Conventional biometric scheme are store templates directly in database. Hence if stolen, they will lose permanently and become unusual in that system. In this approach, an iris biometric template is secured using iris biometric and random key with the help of cryptosystems. A fusion framework design for biometric cryptosystem that, simultaneously protects the multiple templates of a user with the help of a single secure sketch. Iris patterns contain rich discriminative information and can be efficiently encoded in a compact binary form. Instead of storing iris codes directly a random secret can be derived such that user privacy can be preserved.

## References

[1] K. Nandakumar and A. K. Jain, "Multibiometric based on feature-level fusion," in Proc. IEEE 2nd Int. Conf. on information, and Security,vol.7,no.1, Feb.2012.

[2] Chung Chih Tsai, H. Y. Lin, Ching Wang Tao, "Iris recognition using possibilistic fuzzy matching on local features," IEEE Trans. on System, Man, and Cybernetics, vol. 42, no. 1, Feb.2012.

[3] R. A. Marino, F. H. Alvarner, L. H. Encias, "Cryptobiometric scheme based iris template with fuzzy extractor", information security institute, Marid, Spain,2012.

[4] V. Conti, C. Militello and D. Hu, "A new iris normalization for recognition systemwith cryptography technique," IJCSI international journal of computer science, vol. 08, no.1, July. 2011.

[5] Shaikh Ziaudddin and Mathew N. Daily, "Robust iris verification for key managment", computer management. Asian institute of technology, Thailand, 2010.

[6] Bo Fu,Simon X. Yang and Dekun Hu, "Multibiometric Cryptosystem: model structure and performance analysis," in Proc. IEEE Trans. on inf. forensic and Security, vol.4, no.4 Dec. 2009.

[7] Tanya Ignatenko, Frans M. J. Willems, "Biometric systems: privacy and secrecy aspects," in Proc. IEEE Trans .on inf. forensic and Security, vol.4, no.4 Dec. 2009.

[8] Youn Joo Lee, Kang R.Pank ,"A new method for generating an invariant iris private key based on the fuzzy vault system," IEEE Trans. on System, Man, and Cybernetics, vol. 38, no.5, Oct.2008

[9] Hao, F., Anderson, R., Daugman, J., 2006. Combining crypto with biometrics effectively. IEEE Trans. Comput. 55 (9), 1081–108,2006

[10] Uludag, U., Pankanti, S., Jain, A.K., 2005. Fuzzy vault for fingerprints. In: AVBPA, pp.310–319.

[11] Arjun Ross, Anil Jain, "information fusion in biometric".pattern recognition letters24(2003) 2115-2125.

[12] Goh, A., Ngo, D.," Computation of cryptographic keys from face biometrics." In: Communications and Multimedia Security, pp. 1–13.2003.

[13] A.Juels and M. Sudan, "A fuzzy vault scheme," in Proc. IEEE Int. Symp. Information Theory, Lausanne, Switzerland, 2002.

[14] Monrose, F., Reiter, M.K., Li, Q., Wetzel, S., 2001. "Using voice to generate cryptographic keys". In: SP'01: Proc. 2001 IEEE Symp. on Security and Privacy. IEEE Computer Society, p. 202.2001.

[15] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in Proc.Sixth ACM Conf. Computer and Communications Security, Singapore,Nov. 2000.

[16] Monrose, F., Reiter, M.K., Wetzel, S., 1999. Password hardening based on keystroke dynamics. In: ACM CCS 99: 6th Conf. on Computer and Communications Security, pp. 73–82.1999