Mar. 31
International Journal of advanced studies in Computer Science and Engineering
IJASCSE, Volume 4 Issue 3, 2015

Hybrid Protection Mechanism to secure Iris Template

Rajeev Gupta
MMICT&BM (MCA)
Maharishi Markandeshwar University
Mullana (Ambala), INDIA

Ashok Kumar
Department of Computer Engg., MMEC
Maharishi Markandeshwar University
Mullana (Ambala), INDIA

***Abstract*—** Iris Template protection is a crucial requirement when designing an iris based authentication system. It refers to techniques used to make the stored iris template inaccessible to unauthorized users. Securities as well as accuracy are the major factors for the iris template protection algorithms. Here, we propose a hybrid protection mechanism that combines both non-invertible feature transformation and key-binding biometric cryptosystem using fuzzy commitment scheme to secure an iris template.

Keywords-Hybrid mechanism; Non-invertible feature transformation; Key-binding biometric cryptosystem;Iris template protection; Fuzzy commitment scheme

I. INTRODUCTION

A secure iris recognition system for personal authentication is the major demand of society in order to conflict the epidemic growth in identity theft. It is urgently needed to meet the increased security requirements in a variety of applications to secure information in databases. Iris template security is one of the most crucial issues in designing a secure iris recognition system for personal authentication [1]. In the iris based authentication system, a huge amount of iris data in the form of iris template is stored in the database; which leads to serious concern about privacy leakage and identity theft. An ideal iris template protection scheme should possess the following four properties [2].

- *Diversity:* The secure iris template must not allow cross-matching across databases, thereby ensuring the user's privacy.
- *Revocability:* It should be straightforward to revoke a compromised iris template and reissue a new one based on the same existing data.
- *Security:* It must be computationally hard to obtain the original iris template from the secure iris template. This property prevents an adversary from creating a physical spoof of the biometric trait from a stolen iris template.
- *Performance:* The iris template protection scheme should not degrade the recognition performance (FAR and FRR) of the iris recognition system.

The iris template protection techniques [1] can be broadly classified into five categories: Feature Transformation, Biometric Cryptosystem, Watermarking, Hybrid and Haptic Biometric Techniques (see Fig. 1).

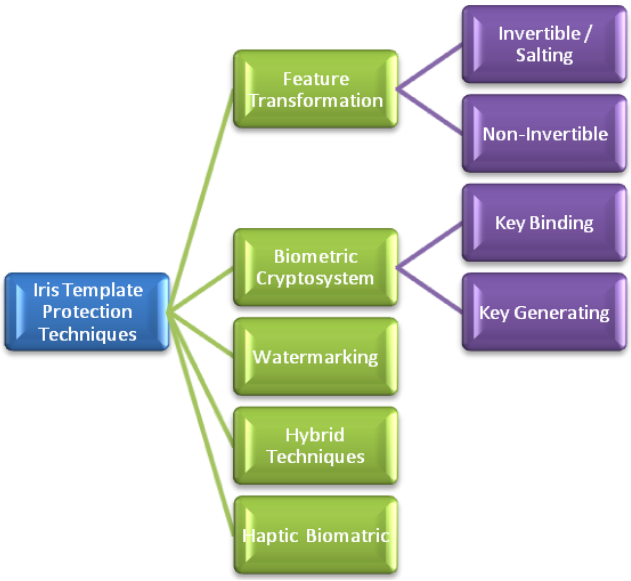

Figure 1 Categorization of Iris Template Protection Techniques [1]

In this paper, we propose a hybrid protection mechanism that combines both non-invertible feature transformation and key-binding biometric cryptosystem using fuzzy commitment scheme to secure an iris template. Part II focuses on proposed hybrid protection mechanism to secure an iris template. Part III presents the experimental analysis of proposed mechanism; and Part-IV presents the conclusion and future scope.

II. PROPOSED HYBRID PROTECTION MECHANISM TO SECURE AN IRIS TEMPLATE

The block diagram of proposed hybrid protection mechanism is shown in Figure 2. The proposed mechanism compensates the shortcomings and maintains the advantages of individual approach in the hybrid scheme. The proposed hybrid protection mechanism to secure an iris template combines both non-invertible feature transformation and key-binding biometric cryptosystem to secure an iris template.

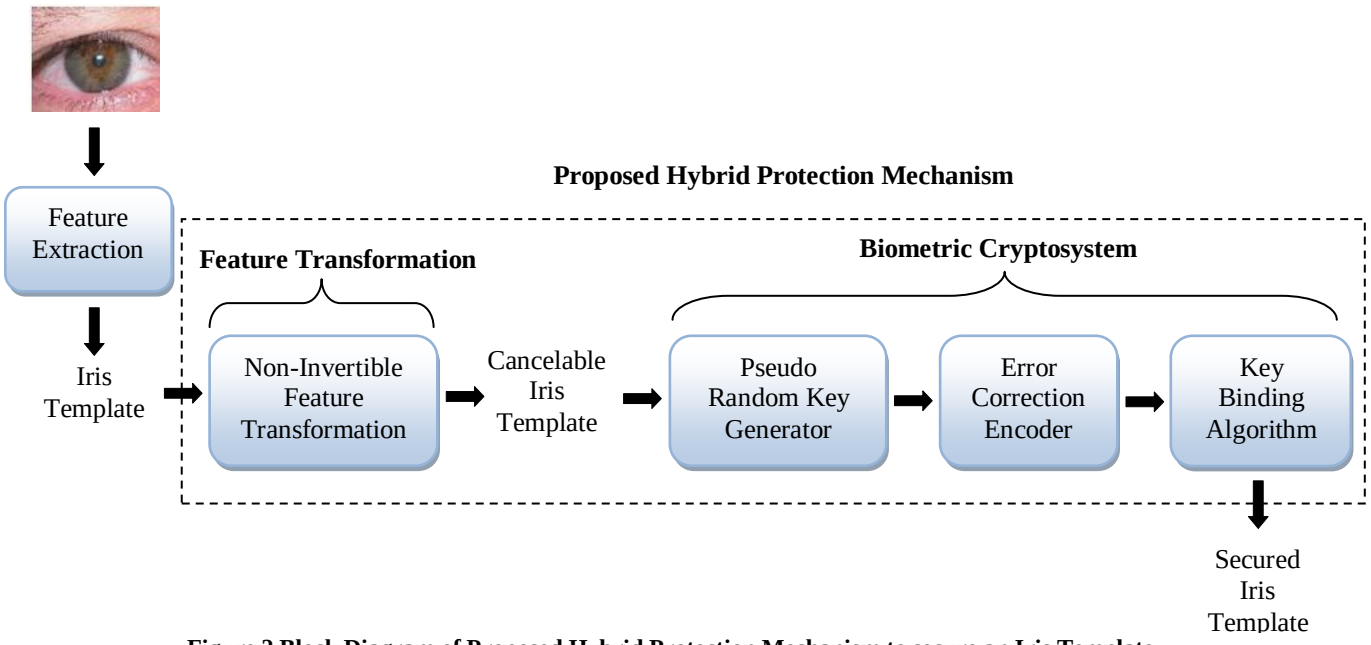

Figure 2 Block Diagram of Proposed Hybrid Protection Mechanism to secure an Iris Template

To secure an Iris template, hybrid protection mechanism will be investigated using the following steps:

Algorithm: Hybrid Protection Mechanism to secure an Iris Template
Input: Iris Template
Output: Secured Iris Template
Procedure:
Step-1: Select an Iris Image
Step-2: Generate an Iris Template / Iris Code
(a) Segment an Iris from an image
(b) Convert a segmented iris into normalized iris
(c) Generate an Iris Template from normalized iris
Step-3: Apply Non-Invertible Feature Transformation on available Iris Template (Iris Code).
Step-4: Apply Key-binding Biometric Cryptosystem approach
(a) Generate a random key by using Pseudo Random Key Generator.
(b) Encode the key by applying the Error Correction Encoder and store the resultant value into codeword.
(c) Integrates both the codeword and Iris template by applying Key-binding biometric cryptosystem using fuzzy commitment scheme.

As per the block diagram of proposed hybrid protection mechanism, the proposed work is divided into two main modules. The first is non-invertible feature transformation which is used to provide cancelability. The second is the key-binding biometric cryptosystem approach, which is used to enhance security and bind cryptographic key for cryptographic applications.

Non-Invertible Feature Transformation is a popular iris template protection approach, in which, iris template is secured by applying a non-invertible transformation function to it. Non-invertible transform refers to a one-way function, *F*, that is "easy to compute" but "hard to invert" in the Cartesian, polar and transformation domain. The main characteristic of this approach is that even if the key and/or the transformed template are known, it is computationally hard for an adversary to recover the original iris template.

The advantages of this approach are: it is hard to recover the original biometric template even when the key is compromised, so, this scheme provides better security than the salting approach; and diversity & revocability can be achieved by using application-specific and user-specific transformation functions, respectively. The main drawback of this approach is the trade-off between discriminability and non-invertibility of the transformation function.

An example of non-invertible feature transformation approach is Ratha et al. [3] [4] introduced the concept of cancelable biometrics. They proposed one-way transformations in the Cartesian, polar and transformation domain. In [5] they suggest two different ways of creating cancelable iris templates by applying non-invertible one-way transformation. The first method involves shifting and combining rows of the unwrapped iris image or binary iris template, and the second method uses a key to add a random noise pattern or a synthetic iris pattern again to the original unwrapped iris or the binary template to generate the cancelable template.

Biometric cryptography is the science of combining traditional cryptographic methods with biometrics either

for securing the cryptographic keys or also for securing biometric templates. In other words, Biometric cryptosystems refer to algorithms that combine biometrics with cryptography. However, they can also be used as an iris template protection mechanism. In a biometric cryptosystem, some public information about the biometric template is stored. This public information is usually referred to as helper data and hence, biometric cryptosystems are also known as helper data-based methods [6]. Depending on how the helper data is obtained, Biometric cryptosystems can be further categorized as: Key Binding Biometric Cryptosystems and Key Generating Biometric Cryptosystems

In a *Key binding biometric cryptosystem*, the biometric template is secured by monolithically binding it with a key within a cryptographic framework. In other words, Key-binding biometric cryptosystems transfer a key (generated by a pseudo random number generator and encoded by an error correction encoder.) into the stored identity code. The key-binding algorithm integrates both the codeword and biometric template into the stored identity code. When a biometric query differs from the template within certain error tolerance, the associated codeword with similar amount of error can be recovered which can be decoded to obtain the exact codeword and hence, recover the embedded key.

The advantage of this approach is that it is tolerant to intra-user variations in biometric data and this tolerance is determined by the error correcting capability of the associated codeword. The main drawback of this approach is matching has to be done using error correction schemes and this precludes the use of sophisticated matchers developed specifically for matching the original biometric template.

Fuzzy commitment scheme [7] is one of the popular approaches of key-binding biometric cryptosystem. Juels and Wattenberg [8] combined techniques from the area of error correcting codes and cryptography to achieve a type of cryptographic primitive referred to as fuzzy commitment scheme. A fuzzy commitment scheme consists of a function F, used to commit a codeword $c \in C$ and a witness $x \in \{0,1\}^n$. The set C is a set of error correcting codeword c of length n and x represents a bitstream of length n, termed witness (biometric data). The difference vector of c and x, $\delta \in \{0,1\}^n$, where x = c + δ, and a hash value h(c) are stored as the commitment termed F(c, x) (helper data). A hash of the result is tested against h(c). With respect to biometric key-binding the system acquires a witness x at enrollment, selects a codeword $c \in C$, calculates and stores the commitment F(c, x) (δ and h(c)).

III. Experimental Result

The implementation of the proposed hybrid protection mechanism has been done in Java technology. The following screenshots demonstrate the working of the different steps of the proposed hybrid protection mechanism to secure an iris template.

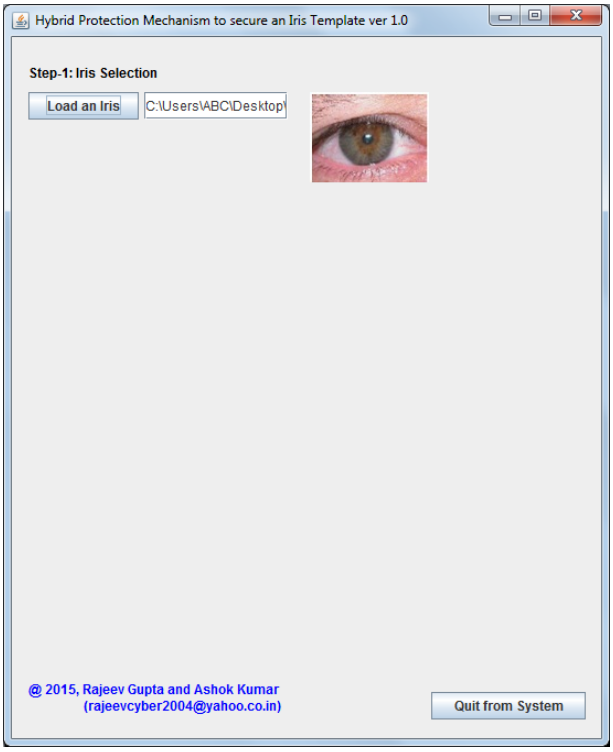

Figure 3 Iris Selections (Step-1)

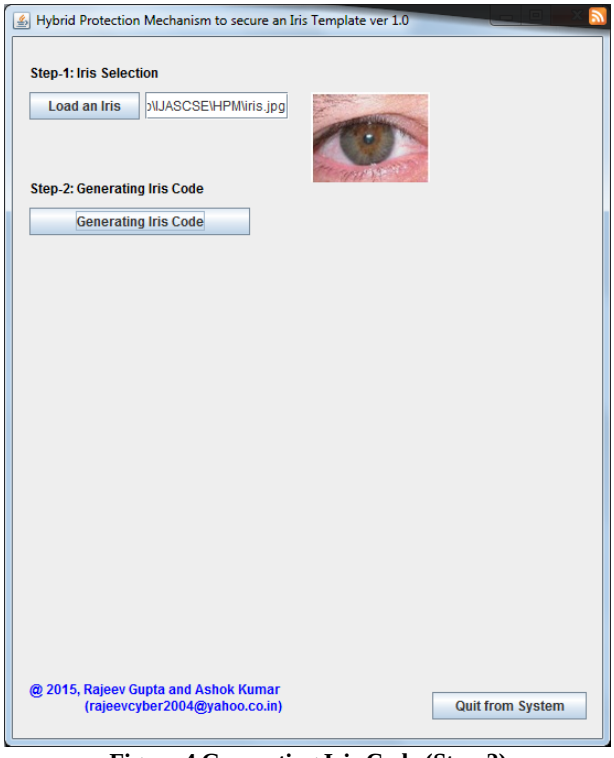

Figure 4 Generating Iris Code (Step-2)

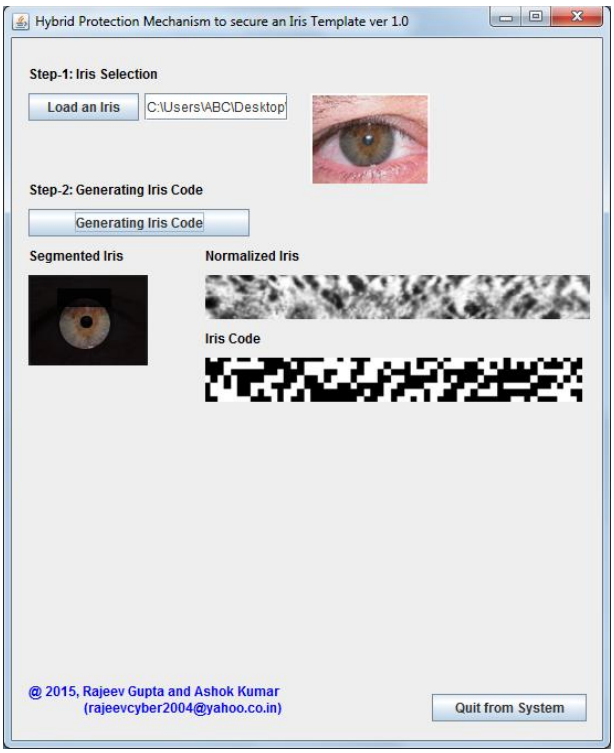

Figure 5 Segmented Iris, Normalized Iris and Iris Code of selected Iris

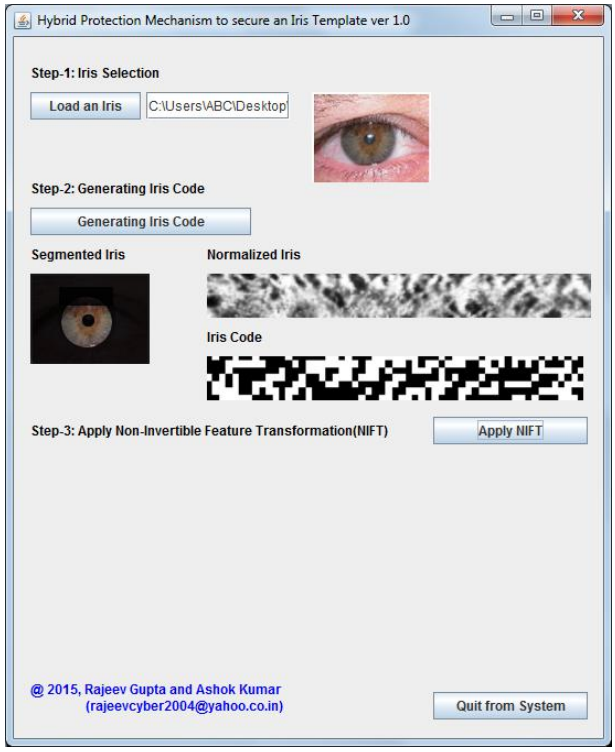

Figure 6 Apply Non-Invertible Feature Transformation (Step-3)

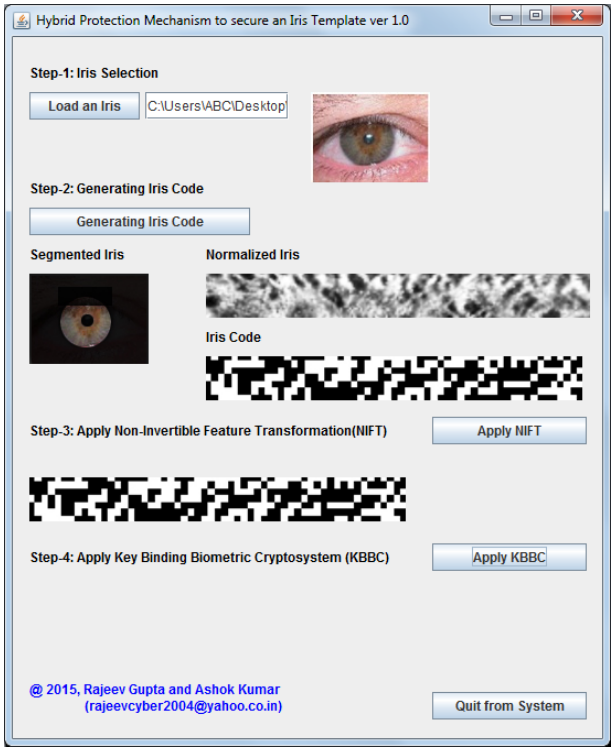

Figure 7 Apply Key Binding Biometric Cryptosystem (Step-4)

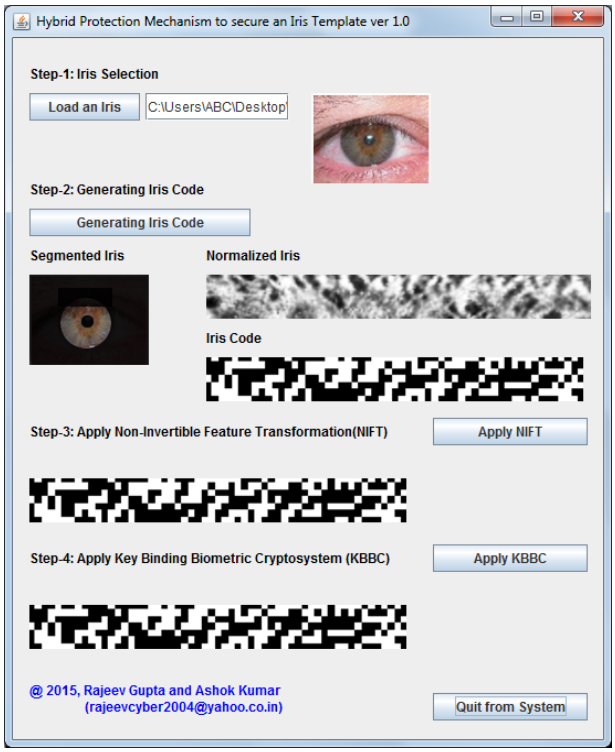

Figure 8 Secured Iris Template (Final Output)

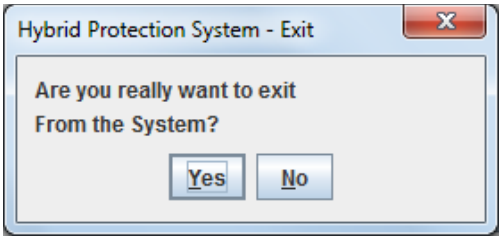

Figure 9: Exit from the Hybrid Protection System

IV. Conclusion and Future Scope

Proposed hybrid protection mechanism provides the security to an iris template with the combination of non-invertible feature transformation and key-binding biometric cryptosystem by using fuzzy commitment scheme. The future work will concern to security analysis of the proposed hybrid mechanism on noisy irises when the lower or upper eyelids and eyelashes cover the pupil of the iris.

References

[1] Rajeev Gupta and Ashok Kumar, "A Study of Iris Template Protection for a Secure Iris Recognition System", *International Journal of Engineering Research & Technology*, February 2015, Vol 4 Issue 02, pp. 557-561.

[2] D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar, "Handbook of Fingerprint Recognition", *Springer-Verlag*,2003.

[3] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems", *IBM Systems Journal*, 2001, Vol. 40, No. 3, pp. 614-634.

[4] N. Ratha, and J. Connell, "Cancelable Biometrics", presented at *Biometric Consortium 2000 Conference*, Sept. 2000.

[5] J. Zuo, N.K. Ratha and J.H. Connell , "Cancelable iris biometric", *19th International Conference on Pattern Recognition (ICPR)*, December 2008, pp.1-4.

[6] A. Vetro and N. Memon, "Biometric System Security," Tutorial presented at *Second International Conference on Biometrics, Seoul, South Korea*, August 2007.

[7] Rathgeb and Uhl, "A survey on biometric cryptosystems and cancelable biometrics", EURASIP Journal on Information Security, 2011.

[8] Juels A, Wattenberg M, "A fuzzy commitment scheme", 6th ACM conference on Computer and Communications Security, 1999, pp. 28-36.