A Multi-Biometric Template Security: An Application of Code-Based Cryptosystem

Ajay Sharma[1] and Deo Brat Ojha[2]

[1]Associate Professor, Department of Information Technology,
Raj Kumar Goel Institute of Technology, Ghaziabad, U.P., India
(Research Scholar Singhania University, Jhunjhunu, Rajesthan, India)
E-mail:ajaypulast@rediffmail.com

[2]Professor, Department of Mathematics,
Raj Kumar Goel Institute of Technology, Ghaziabad, U.P., India
E-mail: ojhdb@yahoo.co.in

Abstract

In this paper we enhanced the accuracy and security of Multi-biometric system using code-based cryptosystem. Uniqueness of our process is that we store biometric templates together in encrypted form both without the fusion of score level and decision level, which leads a successful way to combine multiple biometric technologies, different from earlier methods. Here, we used McEliece cryptosystem (Code-based cryptosystem) in addition of randomness is also probabilistic which give more susceptibility of template towards brute force attacks.

Keywords: Cryptography, Fuzzy Commitment Scheme, Biometric System, Template, algorithmic Noise. Enrollment phase

1. INTRODUCTION

Biometrics-based personal authentic-cation systems that use physiological (e.g., fingerprint, face) or behavioral (e.g. speech, handwriting) traits are becoming increasing-ly popular, compared to traditional systems that are based on tokens (e.g., key) or knowledge (e.g., password) [7]

Cryptography is considered to be one of the fundamental building blocks to protect the biometric data with the growing use of biometric recognition system. Biometric provides a person with a distinct characteristic that is always prevalent. It is a technique of authentication of a person's individuality from one or more behavioral or physiological feature [6]. The use of biometrics (e.g., fingerprints, irises, faces) for recognizing individuals is becoming increasingly popular and many applications are already available. Although these applications can be fundamentally different, they can still be grouped into one of two categories: *verification* and *identification* [7][8][9].

A well-known difficulty has been how to cope with the 10 to 20% of error bits within a biometric data and derive an error-free template. It is fundamentally impossible to avoid noise during biometric data acquisition, because "life means change". For example, faces age and iris patterns are not perfectly invariant to a contraction of a pupil. More noise is introduced by changes in the environmental conditions, which is again an unavoidable circumstance. Finally noise often finds its way into the sensor, during transmission or in the data processing process ("algorithmic noise"). The latter

noise sources can be reduced or even removed by improved engineering .To solve this problem, fuzzy commitment scheme play an important role. Fuzzy commitment scheme is a tool for handling the noise in template of a biometric recognition system, Juels and Wattenberg's fuzzy commitment scheme [5] has been introduced to handle the difference occurring between two captured of biometric data, using error correcting code.

The various approach here been proposed to protect the stored template, some are hardware based which is used stand alone biometric system-on-devices. Some are software based which is relay on feature transformation and biometric cryptosystems. Here on biometric cryptosystem common encryption technique, such as AES (Advance Encryption standard) or RSA cannot be used because of interclass variation in the biometric template [7, 8].

Finally, an approach to biometric data gathering, one can combine two or more actual biometric analyses and combine their results, i.e. use more than one uni-biometric system. This combination (Multi-Biometric Systems) yields better results than each of the combined analyses individually and thereby increases the reliability of the biometric system[2,3].

This paper, itself define an application of a fuzzy commitment scheme with McEliece's cipher [11]. The main idea is here the biometric matching problem is transformed into an error correcting issue. Here we store both biometric templates together in encrypted form, which are store separately earlier in multi-biometric systems or without use of score level fusion and decision level fusion which is successful ways to combine multiple biometric technologies earlier.

We carefully studied the error patterns within biometric data, and devised a two-layer error correction technique that combines Hamming code and Goppa code. The error-correcting methods remove noise in the template [10]. Along with accuracy, some enhancement in the privacy of biometric cryptosystem, common encryption technique, such as AES or RSA can't be used, so the auxiliary data can be masked using homomorphic encryption that allows certain arithmetic operation in the encryption domain [26].

2. PRELIMINARIES

2.1 Biometric System

The purpose for a biometric system configuration for positive verification ensures that the aim is the same that is enrolled in the security system as a template. Enterprise biometric template designed from a given sample is bound to an identifier by which they are known to the security system (Figure 1)

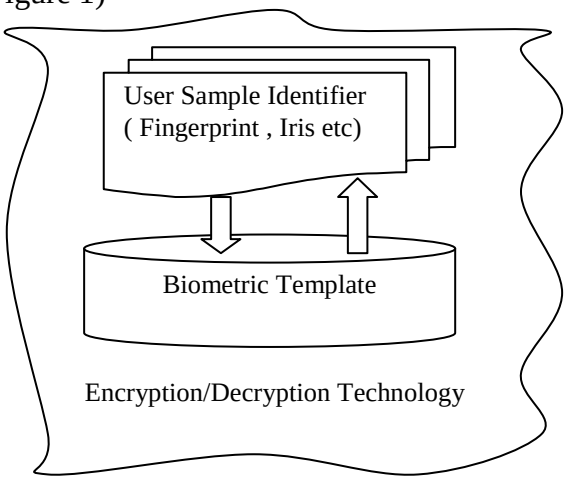


Figure 1. Component of enterprise biometric system [1]

A generic biometric system consists of five components: Sensor, feature extractor, template database, matcher, and decision module.

In general, a biometric based recognition system consists of two phase. In the enrollment phase, the biometric template b are processed from a user U and stored or

registered in the database. The second phase is the verification phase; In verification system captures a new biometric sample b' from U and compare it to the registered or reference data via a matching function. Let μ be the biometric measure of U and τ is a recognition threshold, b' will be accepted if $\mu(b,b') \le \tau$, else rejected. Mainly two kinds of errors are associated to this scheme: False Reject (**FR**), when a matching user, i.e. a legitimate user, is rejected; False Acceptance (**FA**), when a non-matching one, e.g. an impostor, is accepted. Note that, when the threshold increases, the **FR**'s rate (**FRR**) decreases while the **FA**'s rate (**FAR**) grows, and conversely [13].

2.2 Definition: A metric space is a set C with a distance function dist: $C \times C \to R^+ = [0,\infty)$, which obeys the usual properties(symmetric, triangle inequalities, zero distance between equal points)[15].

2.3 Definition: Let $C\{0,1\}^n$ be a code set which consists of a set of code words c_i of length n. The distance metric between any two code words c_i and c_j in C is defined by

$$dist(c_i, c_j) = \sum_{r=1}^{n} \left| c_{ir} - c_{jr} \right| \qquad c_i, c_j \in C$$

This is known as Hamming distance [15].

2.4 Definition: An error correction function f for a code C is defined as $f(c_i) = \{c_j / dist(c_i, c_j) \text{ is the minimum, over } C - \{c_i\}\}$. Here, $c_j = f(c_i)$ is called the nearest neighbor of c_i [14].

2.5 Definition: The measurement of nearness between two code words c and c' is defined by $\text{nearness}(c,c') = dist(c,c')/n$, it is obvious that $0 \le \text{nearness } (c,c') \le 1$ [15].

2.6 Definition: The fuzzy membership function for a codeword c' to be equal to a given c is defined as [12]

$FUZZ(c') = 0$ if $\text{nearness}(c,c') = z \le z_0 < 1$

$= z$ otherwise

2.7 Fuzzy Commitment Scheme with McEliece scheme: Protocols are essentially a set of rules associated with a process or a scheme defining the process. Commitment protocols were first introduced by Blum [4] . Moreover in the conventional commitment schemes, opening key are required to enable the sender to prove the commitment. However there could be many instances where the transmission involves noise or minor errors arising purely because of the factors over which neither sender nor the receiver have any control , which creates uncertainties. Fuzzy commitment scheme was first introduced by Juels and Martin [5]. The new property "fuzziness" in the open phase to allow, acceptance of the commitment using corrupted opening key that is close to the original one in appropriate metric or distance. Fuzzy commitment scheme is based on hash function [5] which causes them to share two shortcomings:

1. The hash functions used should be strongly collision free. However, this property can only be empirically checked. It actually turns out that some schemes are inadvertently based on weakly collision-free hash functions.
2. Hash functions alone cannot offer non-repudiability.

Here we use the speed of McEliece and its randomness to enhance the fuzzy commitment scheme by using code-based cryptosystem which is based on Goppa Code [11].

First select secret key W is a random $(k \times k)$ nonsingular matrix over $GF(2)$ called the scrambling matrix, T is a $(k \times n)$ generator matrix of a binary Goppa code T with the capability of correcting n–bit random error vector of weight less than or equal to α , and Q is a random $(n \times n)$ permutation matrix.

Public Key: $V = WTQ$

A tuple $\{P, H, M, f\}$ where $M \subseteq \{0,1\}^k$ is a message set which consider as a code , P is a

set of individuals, generally with three elements A as the committing party, B as the party to which commitment is made and TC as the trusted party, f is error correction function and $H = \{t_i, a_i\}$ are called the events occurring at times $t_i, i = 0,1,2$, as per algorithm $a_i, i = 0,1,2$. The scheme always culminates in either acceptance or rejection by A and B.

In the setup phase, the environment is setup initially and public commitment key CK generated, according to the algorithm $setup\lg(a_0)$ and published to the parties A and B at time t_0.During the commit phase, Alice commits to a message $m \in M$ then she finds $g : m \to mV$.

Encryption: $E_V(m) = mV + e$ where m is the k-bit message, $E_V(m)$ is an n-bit cipher text and e is an n-bit random error vector of weight α.

According to the algorithms $commita\lg(a_1)$ into string c i.e. her commitment $c = commita\lg(XOR, g(m), E_V(m))$, then after Alice sends c to Bob, which Bob will receive as $t(c)$, where t_f is the transmission function which includes noise.

In the open phase, Alice sends the procedure for revealing the hidden commitment at time t_2 and Bob use this so Alice discloses the procedure $g(m)$ and E to Bob to open the commitment.

$opena\lg(a_2)$: Bob constructs c' using $commita\lg$, message $t(m)$ and opening key i.e

$c' = commita\lg(XOR, t_f(g(m)), t_f(E_V(m)))$

and checks whether the result is same as the received commitment $t(c)$.

Fuzzy decision making

$if\ (nearness(t_f(c), f(c')) \le Z_0)$

Then A is bound to act as in m

Else he is free not to act as m.

Then after acceptance, Bob calculates $f(c')(WTQ)^{-1}$ and finally get the message.

3. RELATED WORK

Our work is inspired from a number of authors who combine well known technique from the area of error correcting code and cryptography to achieve a improve type of cryptographic primitive [4,5,11,15,16]. Further numerous works that suggest combination of biometrics and cryptography. A more detailed of related research work on this field can be found in [17, 18, 19]. An approach to biometric data gathering, one can combine two or more actual biometric analyses and combine their results, i.e. use more than one uni-biometric system. This combination (Multi-Biometric Systems) yields better results than each of the combined analyses individually and thereby increases the reliability of the biometric system[2,3].

4. PROPOSED SYSTEM ARCHITECTURE

In general, the identity theft problem is drastically exacerbated for the biometric systems. The proposed architecture of biometric system will have enhanced the security and accuracy with respect to traditional system by combine usage of code-based cryptosystem and error correcting code.

Here first, we improve the above scheme given section 2.7 according to our new proposed multi-biometric in single biometric template scheme. So select secret key W is a random $(k \times k)$ nonsingular matrix over $GF(2)$ called the scrambling matrix, T is a $(k \times n)$ generator matrix of a binary Goppa code T with the capability of correcting n–bit random error vector of weight less than or equal to α, and Q is a random $(n \times n)$ permutation matrix.

Public Key: $V = WTQ$

A tuple $\{P, H, M, f\}$ where $M \subseteq \{0,1\}^k$ is a message set which consider as a code , P is a set of individuals, generally with three elements A as the committing party, B as the party to which commitment is made and TC as the trusted party, f is error correction function and $H = \{t_i, a_i\}$ are called the events occurring at times $t_i, i = 0,1,2$, as per algorithm $a_i, i = 0,1,2$. The scheme always culminates in either acceptance or rejection by A and B.

In the setup phase, the environment is setup initially and public commitment key CK generated, according to the algorithm $setup\lg(a_0)$ and published to the parties A and B at time t_0.

During the commit phase, Alice commits to a message $m \in M$ where $m = m_1 \square m_2$ then she finds $g : m_1 \to m_1 V$.

Encryption: $E_V(m) = m_1 V + e$ where m is the k-bit message, $E_V(m)$ is an n-bit cipher text and $e = g(m_2)$, here g is an invertible function which maps m_2 in to an n-bit error vector of weight α.

According to the algorithms $commita\lg(a_1)$ into string c i.e. her commitment $c = commita\lg(XOR, g(m_1), E_V(m))$, then after Alice sends c to Bob, which Bob will receive as $t_f(c)$, where t_f is the transmission function which includes noise .

In the open phase, Alice sends the procedure for revealing the hidden commitment at time t_2 and Bob use this. So Alice discloses the procedure $g(m)$ and E to Bob to open the commitment. $opena\lg(a_2)$: Bob constructs c' using $commita\lg$, message $t(m)$ and opening key

i.e

$c' = commita\lg(XOR, t_f(g(m_1)), t_f(E_V(m)))$

and checks whether the result is same as the Received commitment $t(c)$.

Fuzzy decision making

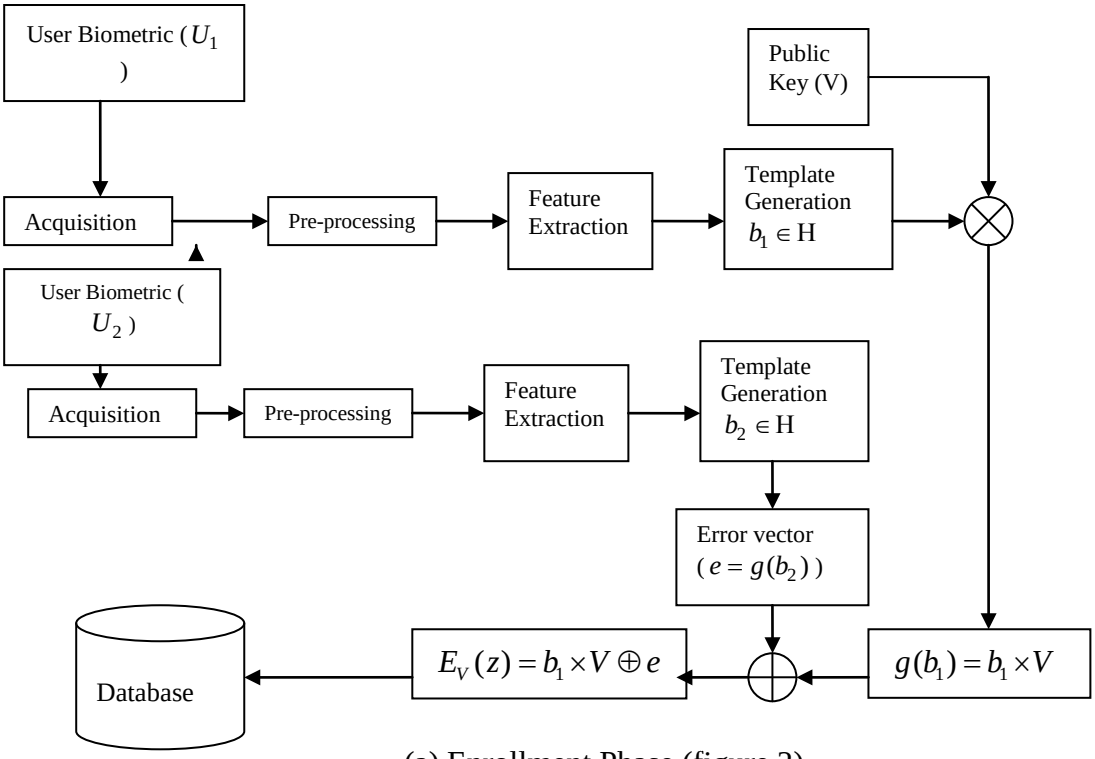
$if\ (nearness(t_f(c), f(c')) \le Z_0)$

Then A is bound to act as in m

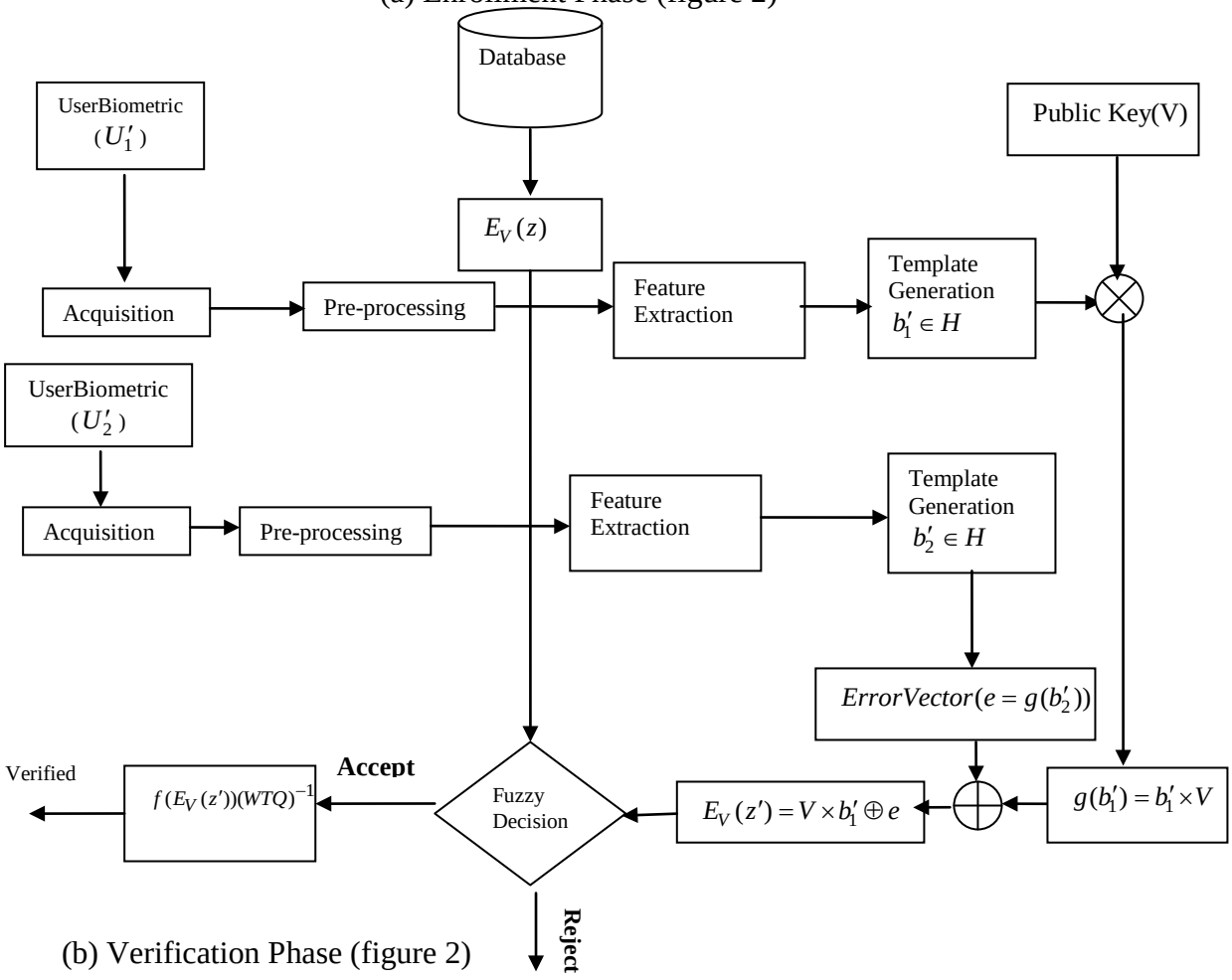
Else he is free not to act as m.

Then after acceptance, Bob decrypt the massage as first m_1 can be recovered by using the decryption algorithm in the original scheme. In the meantime, the value $g(R)$ can also be obtained. Then the receiver computes $m_2 = g^{-1}(g(m_2))$, where g^{-1} the inverse of is g. Finally Bob calculates $f(c')(WTQ)^{-1}$ and finally gets the message. Here Bob get the $m = m_1 \square m_2$ from the $E_V(m)$ to know the authenticity of the sender.

Here we use two different biometric template b_1 and b_2 to enhance the security but store as a single biometric trait in database. In the enrollment stage (as m_1 and m_2 in commitment phase of commitment scheme) (figure2 (a)) of a typical biometric recognition system, after the biometric acquisition module, some processing is applied in order to obtain the biometric template, which is then stored as encrypted form in a database. Here H is called the hamming space of length N e.g. $\mathrm{H} = \{0,1\}^N = F_2^N$, where $F_2 = \{0,1\}$. However, the biometric data is never stored in the database to prevent it from being stolen. Instead, after the biometric has been acquired and the biometric template has been generated, a cryptographic function will be applied to it [11]. The result of this operation will then be stored in the database; this will be referred to in the rest of the paper as the secure biometric template. It should be pointed out that it is impossible to recover any biometric data from this secure template as the cryptographic function is not invertible.



(a) Enrollment Phase (figure 2)



(b) Verification Phase (figure 2)

During the verification stage (open phase of commitment scheme) (figure1 (b)), the probe biometrics is acquired and the corresponding template, b_1' and b_2', is generated.. The problem here is that sample biometrics itself is not stored in the database, but only a encrypted version of it. To recovered the original biometric templates from the database, if the user is who he claims, or something completely different if he is not. Therefore, output of the feature extractor b_1' and b_2' needs to be encrypted. Only then, is the result compared to the encrypted that is stored in the database. If the $E_V(z')$ and $E_V(z)$ are equal, then the user is validated to be who he claims to be. With this system, the requirements above are verified. Finally, since the biometric data is never stored in a database, this guarantees that this information remains private.

4.1 Acquisition

The proposed system is implemented in Matlab 7.0. Fingerprint samples are taken from FVC2002 DB2 fingerprint database. Fingerprint images are resized to 256 X 136. The acquisition module, absolutely necessary in a real biometric verification system, has not been implemented but here Instead of implementation, it is replaced by a large database of iris images, like the one developed by the Chinese Academy of Sciences' Institute of Automation (CASIA) [22]. This database consists of 22051 iris images from more than 700 subjects. All iris images are 8 bit gray-level JPEG files, collected under near infrared illumination. A public version of fingerprint and facial are available on given link [27, 28].

4.2 Pre-processing

In this step after acquisition is to extract the iris and fingerprint database from the input eye and fingerprint images. The iris area is considered as a circular crown limited by two circles. The iris inner (pupillary) and outer (scleric) circles are detected by applying the circular Hough transform [23], relying on edge detection information previously computed using a modified Canny edge detection algorithm [24].The eyelids often occlude part of the iris, thus being removed using a linear Hough transform [26] .The presence of eyelashes is identified using a simple thresholding technique [21]. We extract phase information from the fingerprint image using a Fourier transform and apply majority coding to reduce the feature variation.

4.3 Feature Extraction

Once the iris texture is available, features are extracted from it to generate a more compact representation, also called the biometric template. To extract this represent-tation, the two-dimensional normalized iris pattern is convolved with a Log-Gabor wavelet [6]. The resulting phase information is quantized, using two bits per pixel. The resulting iris template is composed of 9600 bits, stored as a 20×480 binary matrix [21].

The fingerprint is filtered to remove background noise, secondly the image is "binarized" ; the third sub module extract the minutiae and we proceed at last to constellation creation. A minutia is set of coordinates and parameters. Here we extract the set of minutiae points from the fingerprint image. The number of points in each bin will be concatenated together to create the fingerprint code of size $360/\Delta$ degree.

4.4 Privacy-Protection and Error-Correction.

This is main module of this scheme, in this scheme, we are using McEliece cryptosystem, which add some random error at the time of encryption that makes the original template more secure than poorly chosen passwords and other cryptosystem due to its randomness.

At the time of enrollment phase, inputs are biometric templates b_1 and b_2 error vector ($e = g(b_2)$) here g is an invertible function which maps b_2 in to an n-bit error vector of weight α and public key(V) which has generating matrix that defines an error correcting code. The output of this phase is encrypted template which one is stored on system or on a data card (i.e. smart card). Now, it is not easy to gain the template from this data without the knowledge of key and error vector.

At the time of verification phase, a similar procedure is used with a new acquire template b_1' and b_2' with $e = g(b_2')$, and key and error correction coding is used to correct biometric templates. In this stage, the probe templates of a legitimate user is (error) corrected in order to recover the original templates, obtained during enrollment; this should be possible because both templates are fairly similar. However, for an illegitimate user, whose probe template is fairly different from the one originally enrolled by the legitimate user, it should not be possible to recover the original from the probe template.

Therefore, the selected error correcting code should be strong enough to correct templates of legitimate users, but not so strong as to also correct the templates of illegitimate users. Therefore, μ be the biometric measure of U and τ is a recognition threshold, it is known that uni-template b' and b will be accepted if $\mu(b, b') \leq \tau$ else rejected.

5. SECURITY ANALYSIS

Multi-Biometric systems are more secure compared to their single biometric counterparts. The accuracy of any biometric system depends on the ability of that system to separate genuine users from imposters. Here we describe a possible attack to the scheme and identify ways of preventing it. It is possible for an attacker to imitate a signer by obtaining a copy of their biometric data. For example, see [9] for methods of duplicating fingerprints. After obtaining a copy of the signer's biometric data, the attacker can sign a forged message that will appear genuine on verification by the signer. To prevent this attack, genuine messages can be signed in the presence of a trusted witness.

Some issue of security in stored template consider here as,

(1). Stored Template should not reveal any data and no close replica made from the stored data (Spoofing and mimicry attacks)

(2). Multiple systems using the same biometric information should not be able to link template corresponding to the same individual (Cross-system Risk**)**.

(3). If the stored data is compromised, remove that one and reissue a new one.

(4) The impostor is continuously attempting to enter the system by sending incrementally increased matching data to the matching function until a successful score is accomplished.

Solutions of these issues are as
Explanation of issue 1

Here we use goppa code in McEliece, first we encrypt a user biometric template and at the time of encryption an error vector of fixed weight α is added. To reveal any template; attacker should now the solution of decoding problem for unknown weight α of error vector which is very hard to solve. Coding theory based cryptosystem are secure because decoding is hard without the knowledge of secret.

Explanation of issue 2

If we consider error vector as $e = g(R)$ here g is an invertible function which maps R into an n-bit error vector of weight α. Where $R = Id_A \square m_2$ and Id_A is machine identification and Id_A is secret pseudo random vector. Since, each system has

unique Id_A so same biometric information should not be able to link template corresponding to the same individual.

Explanation of issue 3

It is possible to generate many different secure biometric templates from the same biometric trait; it is just a matter of using a different set of error vector ($e = g(R)$) Where $R = Id_A \square m_2 \square r$ and r is secret pseudo random vector. It is also easy to cancel a secure template by simply deleting the compromised template and generating a new one by using different error vector (e).

Explanation of issue 4

McEliece cryptosystem is also probabilistic which give more susceptibility of template towards brute force attacks.

In this scheme, adequately chosen biometric have higher entropy than poorly chosen passwords and therefore, are less susceptible to brute force attacks.

It also provides non-repudiation i.e. a legitimate user may access the facilities offered by an application and then do not claim that an intruder had circumvented the system. A bank clerk, for example, may modify the financial records of a customer and then can't deny responsibility by claiming that an intruder could have possibly stolen her biometric data. So our proposed scheme enhances the biometric security and accuracy from the previous available literature.

6. CONCLUSION

Multi-Biometric performs well compared to the traditional uni-biometric systems. Multi-biometrics provides better recognition accuracy, enhances very high security, flexibility and user convenience.

Using a public key cryptosystem to construct a commitment is a way to achieving non-repudiability and authentication, a property which cannot be offered by hash functions alone. By using McEliece in fuzzy commitment scheme, error vector e used to enhance the security of the function hiding, particularly against matrix factorization attacks. Main enhancement in this approach is randomness of the error vector, we cannot obtain any information about the positions in which the error occurs. Thus the information rate is increase and information leakage rate decrease.

Here we store both biometric templates together in encrypted form, which are store separately earlier. Since template representation satisfies above said constraints, then template is called as secure

REFERENCES

[1] A. Adler (2004), "Images can be regenerated from quantized biometric match score data", *Proc. Canadian Conf. Electrical Computer Eng.*, pp. 469-472.

[2] K. NandaKumar (2008), "Multibiometric Systems: Fusion Strategies and Template Security", PhD Thesis, Department of Computer Science and Engineering, Michigan State University, January.

[3] Anil K. Jain and Arun Ross (2004), "Multibiometric systems," *Communications of the ACM*, January, Volume 47, Number 1.

[4] M. Blum (1982), "Coin flipping by telephone: a protocol for solving impossible problems", *Proc. IEEE Computer Conference*, pp. 133-137.

[5]. A. Juels and M. Wattenberg (1999), "A fuzzy commitment scheme", In *Proceedings of the 6th ACM Conference on Computer and Communication Security*, pp.28-36, November.

[6] Sunil V. K. Gaddam, Manohar Lal (2010), "Efficient Cancellable Biometric

Key Generation Scheme for Cryptography" *International Journal of Network Security*, Vol.11, No.2, pp.61–69, September.

[7] A. K. Jain, S. Pankanti, S. Prabhakar, L. Hong, A. Ross (2004), "Biometrics: A Grand Challenge", *Proc. of the International Conference on Pattern Recognition*, Vol. 2, pp. 935–942, August.

[8] J. Wayman, A. Jain, D. Maltoni, D. Maio (2005), *Biometric Systems:Technology, Design and Performance Evaluation*, Springer-Verlag,.

[9] D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar (2003), *Handbook of Fingerprint Recognition*, Springer,.

[10] Daugman, J (2004), "How Iris Recognition Works", *IEEE Transactions On Circuits and systems for Video Technology*, 14 (1), pp.23-30

[11] Deo Brat Ojha, Ajay Sharma (2010), "A fuzzy commitment scheme with McEliece's cipher", *Survey in Mathematics and Its Application* Vol.5pp73-83.

[12] T. van der Putte and J. Keuning (2000), "Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned". *Proceedings of the Fourth Working Conference on Smart Card Research and Advanced Applications*.

[13] Andrew Burnett, Adam Duffy, and Tom Dowling (2004) "A Biometric Identity Based Signature Scheme", eprint.iacr.org/2004/176.pdf -

[14]. V. Pless (1982), *Introduction to theory of Error Correcting Codes*, Wiley, New York.

[15] A. A. Al-saggaf, H. S. Acharya (2007), "A Fuzzy Commitment Scheme", *IEEE International Conference on Advances in Computer Vision and Information Technology*, 28-30 November– India.

[16] F. J. MacWilliams and N. J. A. Sloane (1991), *Theory of Error-Correcting Codes*. North Holland.

[17] F. Hao, R. Anderson, and J. Daugman (2006), "Combining crypto with biometrics effectively," *IEEE Transactions on Computers*, vol. 55, no. 9, pp. 1081–1088.

[18] A. Cavoukian and A. Stoianov (2007), "Biometric encryption: A positive-sum technology that achieves strong authentication, security and privacy," *Information and privacy commissioner of Ontario*, White Paper, March.

[19] E. Krichen, B. Dorizzi, Z. Sun, S. Garcia-Salicetti, and T. Tan (2008), "Guide to Biometric Reference Systems and Performance Evaluation". Springer-Verlag, ch. *Iris Recognition*, pp. 25–50.

[20] L. Masek, P. Kovesi (2003), *MATLAB Source Code for a Biometric Identification System Based on Iris Patterns*, School of Computer Science and Software Engineering, University of Western Australia, Australia.

[21] J. G. Daugman (2004), "How Iris Recognition Works", *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 14, No. 1, pp. 21–30, January.

[22] CASIA website, http://www.cbsr.ia.ac.cn/IrisDatabase.htm

[23] T. Kawaguchi, D. Hidaka, M. Rizon (2000), "Detection of eyes from human faces by Hough transform and separability filter", *Proc. of the IEEE International Conference on Image Processing*, Vol. 1, pp. 49-52, Vancouver, Canada,.

[24] J. Canny (1986), "A Computational Approach to Edge Detection", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 8, pp. 679-714.

[25] R. Duda, P. Hart (1972), "Use of Hough Transformation to Detect Lines and Curves in Pictures: Graphics and Image Processing", *Communications of the ACM*, Vol. 15, pp. 11-15.

[26] J. Bringer and H. Chabanne (2008), "An Authentication protocol with encrypted biometric data", *Proc. Int. con cryptology. Africacrypt*. pp-109-124,.

[27]. ATT Laboratories Cambridge, ORL face database, www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html.
[28] FVC2002: Fingerprint database, http://bias.csr.unibo.it/fvc2002/
[29] R. Veldhius, F. Deravi, Q. Tao (2008), "Multibiometrics for Face Recognition", *ITSicherheit & Datenschutz*, 3, pp, 204-214