Review Article | Impact Factor: 0.621 | ISSN: 2319-507X
Swati Jadhav, IJPRET, 2014; Volume 2 (8): 650-660 | IJPRET


INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

# A REVIEW ON TEMPLATE SECURITY SCHEME FOR SECURE BIOMETRIC AUTHENTICATION

**MRS. SWATI A. JADHAV**

PG Student, MCERC, Nasik, MH.

**Accepted Date: 15/02/2014 ; Published Date: 01/04/2014**

**Abstract:** With the fast evolution in sensor technology biometric authentication system becomes more popular in daily lives. However securing these biometric templates is primary need for researcher. The growing use of biometrics has lead to rising concerns about the network security, privacy, trust issues and accuracy. From the earlier research work it has been observed that there are many template protection schemes available to secure biometric template and provide remote authentication. But these systems are not full proof to provide better security. This review paper gives idea about existing biometric template protection schemes based on various approach such as feature transformation and cryptosystem. Biometric template data must be protected to prevent information leakage in case of template compromise. Recently there are many template protection schemes available to provide better security and maintain user's privacy. In this paper various technique are reviewed related with user's privacy, template protection, network security and comparison between them.

**Keywords:** Privacy, Security, Template Protection, ECC, RSA.

***PAPER-QR CODE***

**Corresponding Author: MRS. SWATI A. JADHAV**

**Access Online On:**

www.ijpret.com

**How to Cite This Article:**

Swati Jadhav, IJPRET, 2014; Volume 2 (8): 650-660

## INTRODUCTION

Biometric techniques offer a natural and reliable solution for identifying person with their physical and behavioral characteristics like fingerprint, face, iris, palm, etc. Previously, to provide template security the focus of biometrics researcher put on accuracy, speed, cost, and robustness challenges but only recently some attentions have been paid to security and privacy issues of biometric systems. That is the set of extracted biometric features stored in a central database or in a smartcard that makes up the unique features of biometric stored in a template. Biometric data is inherently linked to an individual and can reveal private information about that individual such as their forebears, personality or any confidential data. However, securing biometric template in insecure network is great challenge. Because once it is compromised or stolen it cannot be revoked. The growing use of biometric systems in many real life applications raises some privacy and security concerns [1]. Public acceptance of biometric systems has a critical impact on their success due to their potential misuse of biometric data. Unlike passwords and tokens, compromised biometric templates cannot be revoked and reissued. Therefore it is illegally acquired by an attacker, not only the security of the system is at risk but the privacy and the security of the user may be compromised forever too. So granting template security is one of the most important issues in practical. The need of protecting user sensitive information locally and performing secure user authentication remotely become more increasing in many real time applications.

A. bio-cryptography as solution

Biometric and cryptography could become complementary to each other. It is reasonable and feasible to incorporate biometric into the cryptographic infrastructure to provide network security. Bio-Cryptography is emerging as a powerful solution to provide template security which can combine the advantages of conventional cryptography and biometric security. Cryptography is a conventional method of authenticating users and protecting communication messages in insecure networks. Whereas user can access encrypted content of file only if he having right key. However, cryptography has its own drawbacks like sometimes an attacker may obtain the cryptographic key via an illegal ways and then act as an authentic user [3]. The capabilities of cryptosystems such as of RSA and Diffie-Hellman are inadequate to provide better security due to requirement of large number of bits[15].A lot of work done by researcher on various encryption algorithm [4] (AES, DES, 3DES, Diffie-Hellman, RSA-DSA,RC4,DES,Blowfish) to protect confidential data from unauthorized access. Current only few work done by researcher [5] on elliptic curve cryptography to provide security and privacy.

## II.LITERATURE SURVEY

This section reviews all existing biometric template protection schemes and compares their advantages and limitation in terms of security, revocability and matching of captured image. Over the years a number of attempts have been made to address the problem of template protection and privacy concerns.

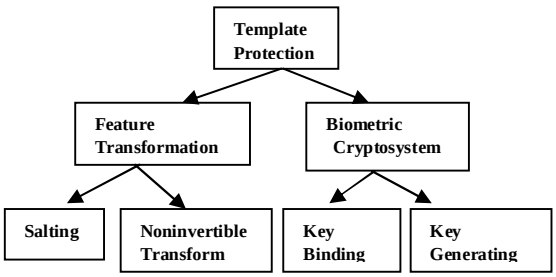



**Figure1: Template protection scheme**

The first feature transformation approach known as Salting [2] offers security using a transformation function seeded by a user specific key. The strength of the approach lies in the strength of the key. A classifier is designed in the encrypted feature space. Its disadvantage is made compromise between security and performance.

B. SALTING

Kong et al. [7] do a detailed analysis of the current bio-hashing based on biometric approaches. They conclude that the zero equal error rate (EER) reported by many papers is obtained in carefully set experimental conditions and unrealistic under assumptions from a practical view point.

C. NONINVERTIBLE TRANSFORM

In this approach a trait specific noninvertible function on the biometric template to secure it. Robust hashing and cancelable biometric [8] fall in this category to replace a leaked template, while reducing the amount of information revealed through the leak. Privacy is not maintained in this approach.

Boult et. al [9] extended the above approach to stronger encryption, and proposed an encrypted minutia representation and matching scheme of fingerprints. In which a Biotoken consists of the encrypted integer part and the increment information in plain. The approach

provides provable template security as a strong encryption is used. Its drawback is making compromised between security and accuracy. The third and fourth class, are both variations of Biometric cryptosystems. They try to integrate the advantages of both biometrics and cryptography to enhance the overall security and privacy of an authentication system.

D. KEY BINDING

Juels and Sudan [10] proposed a cryptographic construction called fuzzy vault. The general idea is to hide the cryptographic key in a scrambled list which is composed of genuine fingerprint features and fabricated chaff features. It lacks in diversity and revocability.

C. Soutar et al. [11] proposed a key-binding algorithm using correlation-based fingerprint matching method. In the algorithm, a cryptographic key extracts only limited features and the corresponding user's fingerprint image are bound at the enrollment stage. Recent research outcome on bio-cryptographic includes bio-hashing, cancelable template, fuzzy extractor and fuzzy vault.

E. KEY GENERAING

Fuzzy extractor is a type of key generating approach designed by researcher Y.Dodis [12] to convert noisy data. It is a combination of a primitive called a Secure Sketch and a Strong Randomness Extractor. The Secure Sketch generates public help data which are related to the input but does not reveal biometric information. To achieve high entropy random extractor maps the string uniformly.

Maneesh Upmanyu et.al.[ 13] proposed blind authentication protocol using biometric features and public key cryptography (RSA). In which server is become secure. While exchanging information between client and server, it does not reveal additional features about biometric than identity.

Recently work done on template security mostly focus on key generation and key binding approach. Although there are many encryption algorithms available among them RSA public key cryptography is widely used for authentication. Because it offers large key size and complex calculation for large prime thus gives better security. In 1986 Victor Miller and N. Koblitz introduces "Elliptic Curve Cryptography" technique as an alternative to established public-key systems such as DSA and RSA. The ECC has a smaller key size which offers the same security strength as the RSA. So ECC is preferable for constraint specified devices where small memory, low computational power and less time are expected such as smart card, portable devices, RFID

etc. Following Table 1 summarizes existing template security mechanism with their effects and researcher opinion.

## III. VULNERABILITIES OF BIOMETRIC SYSTEM:

A denial of service occurs when the system doesn't recognize a legitimate user, while an intrusion refers to the scenario in which the system incorrectly identifies an impostor as an authorized user. Unlike a password-based authentication system, which requires a perfect match between two alphanumeric strings, a biometric-based authentication system relies on the similarity between two biometric samples.

External adversaries can also cause a biometric system to fail through direct attacks on the user interface (sensor), the feature extractor and matcher modules, the interconnections between the modules, and the template database. Examples of attacks targeting the system modules and their interconnections include Trojan horse, man-in-the-middle, and replay attacks. As most of these attacks are also applicable to password-based authentication systems, several countermeasures like cryptography, time stamps, and mutual authentication are available to prevent them or minimize their impact. A false nonmatch occurs when two samples from the same individual have low similarity and the system can't correctly match them. A false match occurs when two samples from different individuals have high similarity and the system incorrectly declares them as a match.

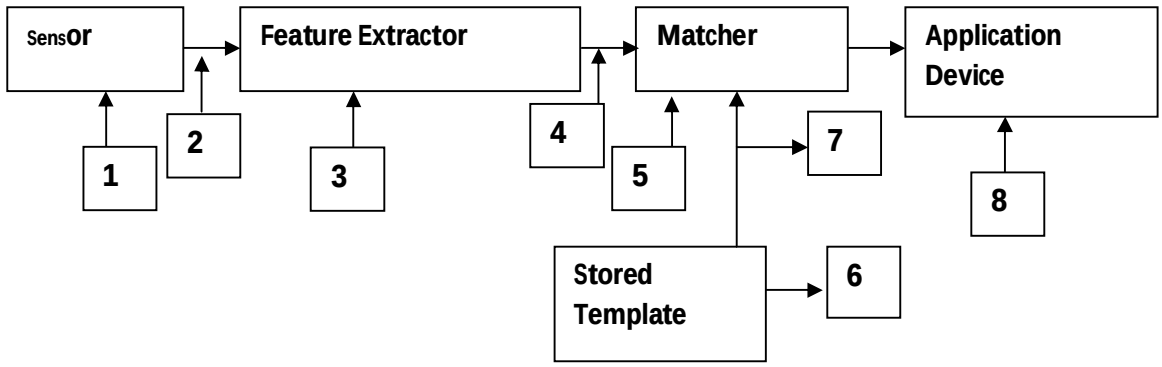



Figure 2: Attack places on a Biometric System

i. **Attack1:** Attack on sensor device cause a denial of service.

**Attack2**: Attack on the channel in that attacker intercepts the communication channel

iii. **Attack 3**: Attacker can replace the feature extractor module with a Trojan horse .

iv. **Attack 4**: Attacker can steal features of user and replay them to the matcher.

v. **Attack 5**: Attacker replaces the matcher with a Trojan horse. Then send commands to the Trojan horse to produce high matching scores and send a "Yes" to the application to bypass system.

vi. **Attack 6**: Attacker compromises the security of the database where all original templates are stored or trying to crack an account.

vii.**Attack7**:Attacker intercepts communication channel between the database and matcher to either steal and replay data.

viii.**Attack8**:Attacker intercept communication channel between the matcher and the application to replay previously submitted data or alter data.

ix. **Attack9**: Not every biometric system is full proof for better security. There should one bug in every software.

**IV. Existing System**

In existing system biometric is combined with public key cryptography such as RSA. Due to it's large key size RSA require large time for encryption thus increases computation time and key generation time. Also number of features is fixed for biometric key generation. Only black and white images are tested for verification of protocol.

**V. Proposed system**

In order to remove drawback of large key size in existing system new system is proposed. Proposed system uses Elliptic curve cryptography(ECC) as an alternative choice for RSA encryption algorithm. Also, Elliptic curve cryptography provide same security strength equivalent to RSA key size with small key size. This new protocol based on client-server architecture. In that during enrollment client register his biometric with personal details. Then using standard feature extraction algorithm features are captured and stored them as unique template. Authentication server perform secure authentication for claimed identity by calculating threshold value and matching score. This matching is done by using SVM classifier. Contribution in this system is use of ECC algorithm, random number generation and real time biometric images. Also number of feature is not fixed so system is more secured and gives more accuracy in verification process.

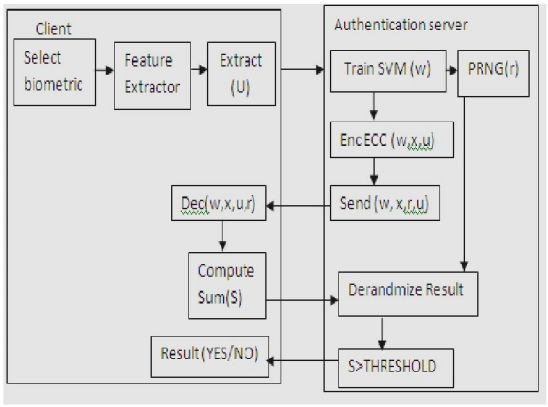
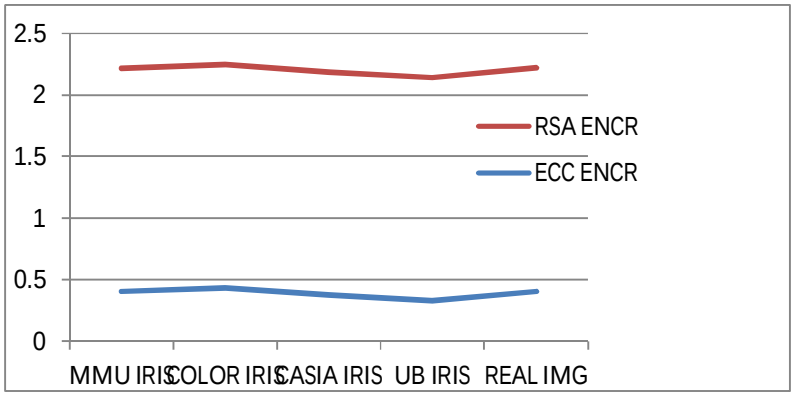



Figure 3.1 block diagram for Authentication




Graph1: Comparison between ECC &RSA Encryption

| Sr. No. | Researcher name | Year | Template Protection Scheme | Concluding Remarks |
|---|---|---|---|---|
| 1. | Koblitz and Miller et.al | 1985 | Using Elliptic curve cryptography how to generate a pseudo-random sequence | Gives security with short key size and Random no. difficult in discrete logarithm |
| 2. | Guang gong | 1991 | Uses the unconditional Randomness to measure the EC-sequences | |
| 3. | C. Souter | 2000 | Uses digital key for 2D images | Extract only limited feature of image |
| 4. | F. monrose | 2001 | When user speak it generate key from voice for securing biometric | User can speak password in its own device. intelligent user can recognize only 104 words |
| 5. | Sumanth Tamma | 2002 | Using matrix values Multiple dimension of face used | Changed expression unable to detect Face so use eigenfaces |
| 6. | Mayank et.al | 2005 | Robust biometric image watermarking | By use of wavelet watermark Embedding face image in fingerprint |
| 7. | Teddy Ko | 2005 | Multimodal biometric | Able to combine two or more biometric using local nonnegative matrix factorization |
| 8. | Muhammad | 2006 | Feature based, template based, appearance based | Knowledge about entire image |
| 9. | Jongsun Kim | 2007 | Changeable biometrics | compromised template |

| | | | | |
|---|---|---|---|---|
| | et.al | | | cannot be changed |
| **10.** | Yagitz sutcu | 2007 | Secure sketch | Is solution over digital key |
| **11.** | Deepthi | 2009 | Stream cipher based on elliptic curve point multiplication over GF(2m). | |
| **12.** | P. S. Revenkar et.al,<br>Pareek,<br>I. Ismail et.al | 2010 | 1.Visual cryptography<br>2.Generate random bit based on chaotic maps ,<br>3.Chaos-based stream cipher | 1.secret image encrypted into shares which does not reveal original image.<br>3.key is modify after encrypt of each pixel of plain image |
| **13.** | Emanuela Marasco | 2010 | Multimodal biometric scheme | Due to more than one biometric cost is more and not secure than unimodel, vulnerable to spoof attack |
| **14.** | Maria et.al | 2011 | Elliptic Curve based Key Generation for Symmetric Encryption | encryption/decryption of an image in spatial domain |
| **15.** | Mr. P. Balakumar et.al | 2011 | Key Generation Scheme for Cryptography using Combined Biometric Features of Fingerprint and Iris | Provide better security than RSA with small key size |
| **16.** | Devanathan | 2012 | Design architecture for ECC | |

## VI. Expected result

It is expected that Proposed system able to provide small key size for biometric template encryption. So it require less encryption time and key generation time. In RSA choosing large prime number say 200 digits and multiply together it is very large (400 digits) and factoring

large prime number is difficult. Also finding prime numbers from product is difficult and intractable. As NIST recommend some key size for ECC and RSA comparison. Due to ECC small key size it applicable in small devices such as RFID, Mobile OS, Smart card where limited memory is require. ECC offers similar level of security that can achieve with small key size. ECC is based on difficulties of solving discrete logarithm over integer and integer factorization. In future ECC is best choice for network security due to its strong mathematical structure.

## VII.SUMMARY

After studying detailed literature on template security scheme it has been observed that, although there are many template security mechanism available they lack in meeting requirement such as user's privacy, revocability, security, and accuracy in biometric verification. From the study of template security mechanism discussed in this paper many researcher put focus on biometric cryptography approach. Key generating approach is mostly suitable for template security and privacy in which due to random number generator additional information about biometric is not revealed. This review highlights the need of further research on combining standard cryptography technique with biometric to provide better security.

## REFERENCES

1. A. K. Jain et.al, "Biometric template security", EURASIP J. Adv. Signal Process. 2008.

2. A. Teoh, D. Ngo, and A. Goh, "Biohashing: Two factor authentication featuring fingerprint data and tokenised random number," Pattern Recognit., vol. 37, no. 11, pp. 2245–2255, Nov. 2004.

3. Kai Xi et.al "A fingerprint based bio-cryptographic security protocol designed for client/server authentication in mobile computing environment", Security and communication networks, Issue paper,2010.

4. R. L Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", MIT Laboratory for Computer Science and Department of Mathematics, ACM 0001-0782178/0200-0120.

5. Arun Kumar et.al., "A Comparative Study of Public Key Cryptosystem based on ECC and RSA", IJCSE, ISSN : 0975-3397, Vol. 3 No. 5 May 2011.

6. Yasser Salem Mohamed Ali, "Implementation of Elliptic Curve Cryptography using biometric features to enhance security services", Master of Comp. Science, Thesis, pp.17-38,July 2009.

7. A. L. Jeeva et.al "Comparative analysis of performance efficiency and security measures of some encryption algorithms", IJERA, Vol. 2, Issue 3, pp.3033-3037 ,May-Jun 2012.

8. A. Kong, K. Cheung, D. Zhang, M. Kamel, and J. You, "An analysis of biohashing and its variants", Pattern Recognition., vol. 39, no. 7, pp.1359–1368, July 2006.

9. M. Savvides and B. V. Kumar, "Cancellable biometric filters for face recognition", Int. Conf. Pattern Recognition (ICPR), 2004, vol. 3, pp. 922–925.

10. T. Boult, W. Scheirer, and R. Woodworth, "Revocable fingerprint biotokens: Accuracy and security analysis", IEEE Conf.(CVPR), pp. 1–8, June 2007.

11. A. Juels and M. Sudan, "A fuzzy vault scheme", Designs, Codes and Cryptography, vol. 38, no. 2, pp. 237– 257, 2006.

12. C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B. V. K. V. Kumar, "Biometric Encryption" in ICSA Guide to Cryptography, R. K. Nichols, Ed., McGraw Hill, New York, NY, USA, 1999.

13. Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data", Eurocrypt, pp. 523–540, 2004.

14. Maneesh Upmanyu, "Blind Authentication: A Secure Crypto-Biometric Verification Protocol", IEEE Trans, Information Forensics and Security, Vol. 5, No. 2, June 2010.

15. S. Maria et.al, "Nonce Based Elliptic Curve Cryptosystem for Text and Image Applications", Int. Journal of Network Security, Vol.14, No.4, PP.236-242, July 2012.

16. Eun-Jun , Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem", DOI,© Springer Science, 2010.