ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 5, May 2017

Biometric template protection techniques: A brief survey

[1] Shilpa N L, [2] Dr. R Aparna
[1] Siddaganga Institute of Technology, Tumakuru, [2] Siddaganga Institute of Technology, Tumakuru

***Abstract*— One of the natural and reliable solutions to user authentication problem is biometric recognition. Non universality, intra-class variation etc. are some problems in Unimodal biometric system. Therefore multimodal biometric systems are used to overcome these problems and to increase the level of security. The aim of this paper is to summarize the common attacks against biometric systems (fake biometrics, template modification etc.) and discuss techniques that can be used to counter them. The features that extracted from the biometric samples considered a critical part of biometric system which is called biometric template. Template security schemes are dependent on the overall performance parameters of the system and must be computationally hard to avoid modality reconstruction. This paper also summarizes different biometric template protection schemes (salting, visual cryptography etc.) and discusses their advantages and limitations.**

Keywords – Biometric, Multimodal biometric system, Template protection.

I.INTRODUCTION

Authentication is a process of identifying a person using security systems like bank, office etc. This process does not give any information about access rights of an individual but it guarantees that the individual is who he or she claims to be. Token based techniques, knowledge based techniques and biometric based techniques are three types of authentication methods. Biometric based techniques are based on physiological and behavioral characteristics of an individual for authenticating an individual. This technique gives higher security compared to other two authentication methods [1].
"Biometrics" is a term derived from two Greek words bio (life) and other word is metric (to measure), hence biological measurement is called as biometric. Passwords or pins can be forged, forgotten or shared. But biometrics is difficult to forge. The main drawback of biometric is its varying and noisy nature in acquisition process [2].Biometric recognition of an individual uses only physiological and behavioral characteristics. It can be divided into two types: physiological attributes & behavioral attributes [3].

1. Physiological attributes: These attributes point out the person on the basis of anatomical traits. Some of the physiological traits are face, fingerprint, ECG etc. Physiological traits cannot be lost, forgotten or shared and they provide strong connection between a person and his/her identity. At the time of authentication user should be present at biometric system.

2. Behavioral attributes: These attributes indirectly measure the characteristics of an individual while performing some task like signature, keystrokes, gait and voice etc. [3].

Attributes of any biometric should satisfy the following requirements: **universality, distinctiveness, invariance, performance, acceptability, circumvention, and collectability**. Biometric systems can be used either for verification/authentication or for identification [4].

- **Identification (1: n)** One-to-Many: Biometrics can be used to certify a person's identity [4].

- **Identification (1:1)** One-to-One: Biometrics can also used to prove a person's identity [4].

Biometric system has mainly 4 modules which are used for both enrollment and authentication shown in Fig 1:

1) **Sensor module:** It is used to extract input biometric data from sensor.

2) **Feature extraction module:** This method is used to extract the salient discriminatory information in the input data which helps in authentication process.

3) **Matching module:** It is used to check the similarity score between stored biometric data with new biometric data.

4) **Decision making module:** This module helps to provide final result of biometric system by using the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 5, May 2017

similarity score generated in matching module. This module is used to identify an individual.

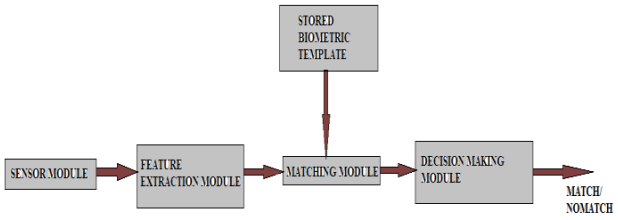


Fig 1: Block diagram of biometric system.

If single modality is used in the system, then it is called as unimodal biometric system. This system has some drawbacks: **noisy input data**, **intra-class variations**, **distinctiveness**, **non-universality**, **spoof attack**.

II. MULTIMODAL BIOMETRIC SYSTEM

Some drawbacks of unimodal biometric system can be solved by using multiple modalities. The system that uses multiple biometric traits is known as multimodal biometric system. By integrating 2 or more biometric traits, multimodal biometric system provides greater performance and higher reliability. There are five different types of integration scenarios which can be used to operate multimodal biometric system:1) multiple sensors, 2) multiple biometric, 3) multiple units of same biometric, 4) multiple instances\snapshots of same biometric, 5) multiple representations and matching algorithms for same biometric [5].

III. TEMPLATE PROTECTION TECHNIQUES

Every biometric is stored as template in database. Biometric template can be defined as compact representation of the sensed biometric trait containing salient discriminatory information that is essential for recognizing a person. There are 2 types of failure modes in biometric system [6]:

1) I**ntrinsic failure:** this is due to limitations in input biometric data, feature extraction, or due to other faults (incorrectness) in which may increase the error rates. 2) **Failure due to an adversary attack:** in adversary attack, attacker tries to bypass the system for personal benefits. The biometric system is exposed to various types of attacks.

To enhance the system's privacy and security template protection methods are used, which provides high level reliable authentication. We cannot apply traditional encryption techniques like Advanced Encryption Standard (AES) or RSA due to intra-class variations in biometric template. Different types of attacks that biometric system can suffer from [6,7] is shown in Fig 2.

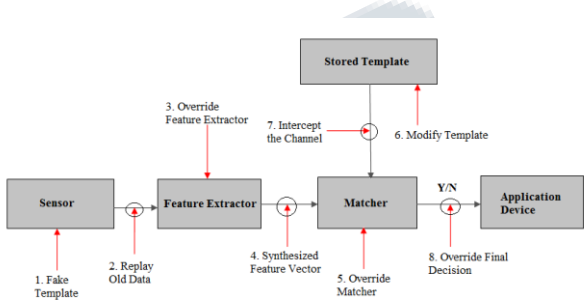


Fig 2: Point of attacks in a biometric system.

1. **Fake Biometric:** This is the attack on sensor. Anyone can present a fake biometric to override the sensor. Examples are fake finger, facial mask etc.

2. Replay Old Data: This attack can be done on between sensor module and the feature extractor module. By resubmitting the old biometric data anyone can bypass the sensor. Examples are old copy of fingerprint or replaying the recorded voice message etc.

3. **Override Feature Extractor:** To override the feature extractor, hacker must force the feature extractor to produce the feature values selected by him. This can be done using Trojan horse, so that feature extractor generates the feature values which are preselected by hacker.

4. **Synthesized Feature Extractor:** This is the attack on communicating path between the modules like feature extractor and the matcher. Here, hacker can replace the feature set generated by feature extractor with different feature set.

5. **Override Matcher:** This is the attack on matcher module of biometric system. Anyone can override matcher by forcing matcher to output matching score which is irrespective to input given.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 5, May 2017

6. Modified Template: This is the attack on stored biometric database. During enrollment, templates are stored in database for future use. Here, attacker tried to modify templates that are stored in the database.

7. **Intercept the channel:** This attack is done between the database and the matcher. Here hacker will select the template of his wish and send to matcher for matching process.

8. **Override Final Decision:** This is the attack on channel which is communicating between matcher and application device. Final decision of the system is changed according to hacker's wish.

IV. PROPERTIES OF TEMPLATE PROTECTION TECHNIQUES

Every template protection method should posses the following characteristics [6, 8, 9].

- **Diversity:** To ensure the privacy of user, the secured feature template should not permit cross-matching or function-creep**.**
- **Revocability:** This must be easy to remove the compromised feature template and then reconstruct the new feature template based on the same biometric data.
- **Security:** Generating the native template from the secured template must be computationally hard.
- **Performance:** Template protection method should not reduce the accuracy of the system. False Acceptance Rate (FAR) and False Rejection Rate (FRR) are used to measure the recognition performance of the system. Template protection methods improve FAR and FRR in multi modal biometric system.

The challenging task of designing template protection method that fulfils all the above requirements is handling intra-user variability. Feature set extracted for different images of same person are not similar. So, we cannot store template in an encrypted form (by using RSA, AES etc) and it is difficult execute matching process in the encrypted domain.

V. CLASSIFICATION

Biometric template protection techniques are categorized into two types [6,8,9] which is shown in Fig 3. They are: Feature Transformation based methods and Biometric Cryptosystem based methods.

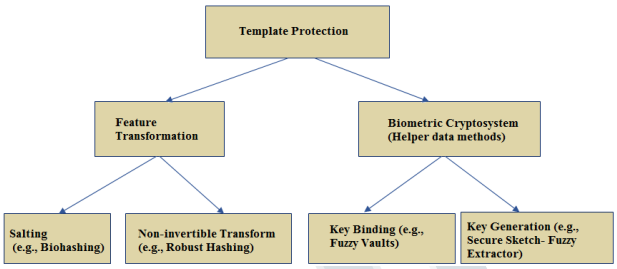


Fig 3: Types of template protection methods.

A. FEATURE TRANSFORMATIONBASED METHODS

In this method, a transformation function is applied for the template T, and transformed (encrypted) template T_f is stored in the database. We use random key or a password in transformation function. During authentication, same transformation function is applied on testing template. Then translated template is matched directly to the transformed (encrypted) template which is stored in the database. This method is sub-divided into two types based on characteristics of transformation function. Fig 4 shows the working of feature transformation.

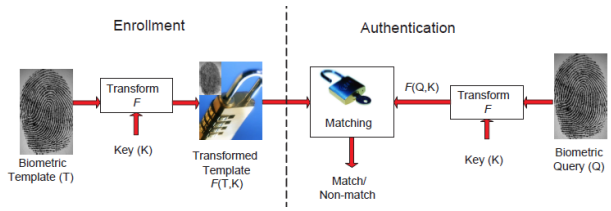


Fig 4: Working of feature transformation technique[6].

a) SALTING

In salting technique, transformation function is reversible, i.e., if hacker gains access to cryptographic key and transformed (encrypted) template, it is easy for hacker to recover the native template [2]. This is the main issue in salting method. One example for salting is random multi-scale quantization technique [10].

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 5, May 2017

Advantage of salting is use of key in transformation function that reduces the false acceptance rates

b) NON-INVERTIBLE TRANSFORM

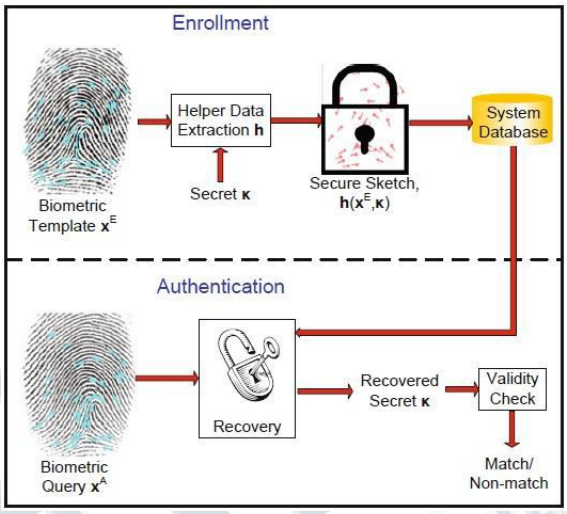
Non-invertible transform is another type of feature transformation method. It is referred as one-way function. It is easy to calculate but computationally difficult to translate transformed template to its native form even if the key is known. So it provides better security than salting method.

B. BIOMETRIC CRYPTOSYSTEM BASED METHODS

It is developed either to secure a cryptographic key by making use of biometric features or to generate cryptographic key directly using features of biometric trait. It is also used in protecting the biometric template. In this method, database stores only public information of template. This data is known as helper data. Therefore this method is also referred as helper data-based method. This data does not reveal any important information about native template. By testing the validity of the key, matching process will be performed. To handle intra-class variations, error correction coding is used. This method is categorized into two types based on the way the helper data is obtained: 1) key-binding cryptosystem and 2) key generation cryptosystem.

1. KEY BINDING BIOMETRIC CRYPTOSYSTEM

This method is used when the helper data is generated by combining a secret key with biometric template [6]. Here the key is independent of biometric features. Working of this method is shown in Fig 5. It is very difficult to recover either template or key by using only the helper data. When stored template is dissimilar from the query template within some error tolerance. The related codeword can be retrieved and that codeword can be decoded to get exact codeword and finally the embedded key can be retrieved. In matching process use query template features to retrieve key from helper data.



VI. OTHER TECHNIQUES

Other techniques that can be used for template protection are: Watermarking, Visual Cryptography, and Steganography.

a) VISUAL CRYPTOGRAPHY

Naor and Shamir proposed the basic visual cryptography system (VCS). It is a cryptographic method that allows for the encoding of visual data such that decoding can be performed using the human visual system. VCS allows secret sharing of images in a secure way. Basic scheme of visual cryptography is referred as k-out-o-n VCS or (k, n) VCS which deals with binary images [11,12].

Here the image Z is divided into two shares and sharing of pixel p is shown Fig 8. If pixel p is white, any one from first two rows of Fig 7 is randomly selected to encrypt A and B. If the color of the pixel p is black, then any one of the last two rows in Fig 7 is randomly chosen to encode A and B. Thus, both A and B does not give any information about binary color of p. When two shares are overlapped, we get two black sub-pixels if pixel p is black and we get one white and one black sub-

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 5, May 2017

pixel if pixel p is white as indicated in Fig 7. We can tell the color of the pixel p (white or black) based on the contrast of the reconstructed pixel.

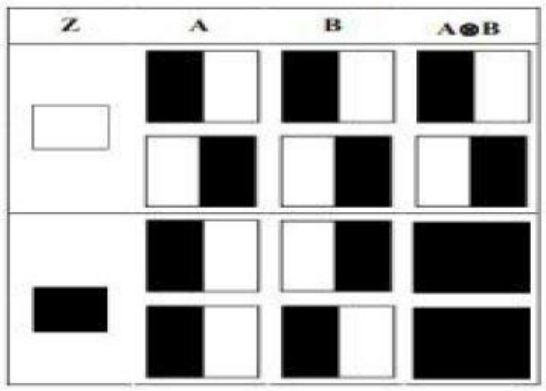


Fig 7: 2-out-of-2 VCS scheme with 2 subpixel construction.

b) STEGANOGRAPHY

Steganography comes from Greek word "steganos" means secret and "graphy" means writing. Goal of this technique is secure communication so that the communicating data should not be detectable by an intruder. We can use images, audio, video etc., as cover. Here the original image is embedded in cover image so the output is called as stego image. Then the stego image is transmitted over a channel to receiver. At receiving end, key and stego image is given to stego decoder to retrieve original image [13,14]. Working of steganography is shown in Fig 8.

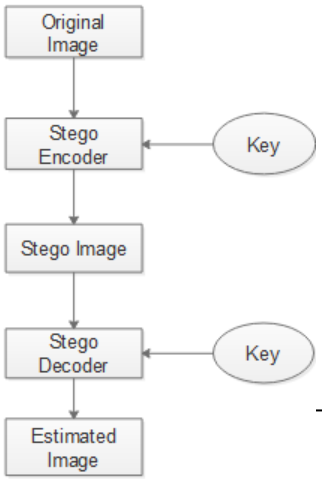


Fig 8: Steganography Model.

c) WATERMARKING TECHNIQUE

Watermarking is one type of the security technique which is used to embed the secret data (watermark) in the input signal. Watermarking with encryption gives higher security.
This technique can be used in many applications such as ownership identification, broadcast monitoring and copy control etc [13]. Watermarking can also be used in biometric template. Watermarking introduces extra information into biometric template.

Watermarking can be divided into different types based on embedding domain such as transform domain watermarking, and spatial domain watermarking. The working of watermarking technique is shown in Fig 9 which is performed on iris template. Input image i.e., host image is used embed the watermark. Then watermarked image is broadcasted. At the receiving end, watermark image will be retrieved and original image is obtained. Comparisons between different template techniques are listed in Table 1.

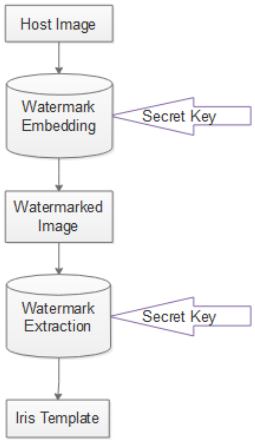


Fig 9: Watermark for iris template

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 5, May 2017

Table 1: Comparisons between different template protection methods

Approaches	Advantages	Disadvantages
Salting	Achieves less False Acceptance Rate (FAR). Easy to remove compromised template by new one.	Security given to template will be lost if the key is compromised.
Non-invertible transform	Tough to recover original template even after compromising key.	Trade-off between discriminability and noninvertibility of the transformation function.
Key binding biometric cryptosystem	Tolerant to intra-class variations.	Difficult to achieve diversity and revocability property.
Key generation biometric cryptography	Tolerant to intra-class variations. Provides security to cryptographic key	Tough to generate key with high stability and entropy.
Visual Cryptography	Provides higher security. Encrypts original template in several secret share, and are stored on distributed database.	Time consuming process.
Steganography	Difficult to identify the hidden data inside template. Achieves higher security.	Time consuming process. It is not matured enough to deploy in many applications.
Watermarking	Ensures high security to biometric template.	Takes more time during watermark insertion.

CONCLUSION

Biometric recognition of an individual uses only physiological and behavioural characteristics. To overcome problems in unimodal biometric system, multi modal biometric system was introduced. Every biometric data is stored as template in database which are prone to attack. Some of the attacks on generic biometric system are fake biometric, replay old data, modified template, intercept the channel, and override final decision etc., To provide security to the template in database one can use techniques like feature transformation technique and biometric cryptosystem. Other techniques like visual cryptography, steganography and watermarking can also be used for providing protection to template.

REFERENCES

[1] C.Prathipa, Dr.L.Latha, "A Survey of Biometric Fusion and Template Security Techniques", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) vol.3, Oct 2014.

[2] Peng Li et al., "An effective biometric cryptosystem combining fingerprints with error correction codes", Expert systems with applications, vol.39, no.7, 2012.

[3] Emad Taha Khalaf, Norrozila Sulaiman, "Multibiometric systems and template security survey", Journal of Scientific Research and Development, pp: 38-46, 2015.

[4] Sakshi Kalra , Anil Lamba, "A Survey on Multimodal Biometric", International Journal of Computer Science and Information Technologies, vol.5 , pp: 2148-2151, 2014.

[5] Soyuj Kumar Sahoo et al., "Multimodal Biometric Person Authentication: A Review", ITIE Technical Review, vol.29, 2012.

[6] Anil K. Jain et al., "Biometric Template Security", EURASIP Journal on Advances in Signal Processing, Jan 2008.

[7] Biruntha.S et al., "Survey on Security Schemes for Biometric Privacy", International Journal of Computer Applications (0975 – 8887) vol. 60, no.1, December 2012.

[8] Arvind Selwalet al., "Performance Analysis of Template Data Security and Protection in Biometric Systems", Proceedings of 2015 RAECS UIET Panjab University Chandigarh, Dec 2015.

[9] Praveer Tigga, Akash Wanjari, "A Survey on Template Protection Scheme for Multimodal Biometric System", International Journal of Science and Research , 2013.

[10] Sarika Khandelwal et al., "Survey of Threats to the Biometric Authentication Systems and Solutions", International Journal of Computer Applications, vol. 61, no.17, Jan 2013.

[11] Aswathy Elma Aby, K.Vijayakumar, "A data securing approach for face images in biometric database", IOSR Journal of Electronics & Communication Engineering.

[12] Ankita Gharat et al., "Biometric Privacy Using Visual Cryptography", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) vol.2, Jan 2013.

[13] Biruntha.S et al., "Survey on Security Schemes for Biometric Privacy", International Journal of Computer Applications, vol.60, no.1, pp: 0975 – 8887, Dec 2012.

[14] Andrew Lock, Alastair Allen, "Effects of Reversible Watermarking on Iris Recognition Performance", International Journal of Computer, Electrical, Automation, Control and Information Engineering, vol.8, no.4, 2014.