Survey on Security Schemes for Biometric Privacy

Biruntha.S
PG student,
Department of Computer Science and Engineering,
SNS College of Technology
Coimcatore, Tamilnadu,

Dhanalakshmi.S
Associate Professor,
Department of Computer Science and Engineering,
SNS College of Technology
Coimcatore, Tamilnadu,

Karthik.S, PhD.
Dean and Professor,
Department of Computer Science and Engineering,
SNS College of Technology
Coimcatore, Tamilnadu,

ABSTRACT
Biometric is the science of establishing the identity of on individual based on physical or behavioral traits such as face, fingerprint, Iris. The increasing popularity of biometrics offers personal identification systems greater security and convenient than password authentication system. A biometric system operates by acquiring raw biometric data from a subject, extracting a feature set from the data and comparing the feature set against the template stored in a database in order to identify person. At the same time there is a possible to intruder can access the database which stored the biometric data. So the security and privacy of biometric system is a major concern due to their issues like fake biometric, override matcher and etc. We present an overview of various biometric template protection schemes and discuss their advantages and limitations.

Keywords
Biometrics, watermarking, steganography, cryptography , Visual cryptography.

1. INTRODUCTION
Biometric is one of the authentication system it comes from the greek words 'bios and metricos' which means 'life measure'.It is more reliable,consistent and also user friendly.So it is used for many application such as computer login control, passport control,border crossing,secure e-banking,ATM, credit cards,airport ,etc.

1.1 Biometric data types
The biometric data classified as physiological or behavioral. Physiological biometrics based on the physical part of the body such as fingerprint,iris,eye retina,face,palm,hand. Behavioral type is based the behavior of human such as voice,signature and keystroke.

1.2 Biometric Template Properties
a**. Security:** This property prevents the biometric template from stolen template
b. **Diversity:** The secure template must not allow cross matching across databases
c. **Revocability:** It should be straightforward to revoke a compromised
d. **Performance:** The recognition performance of the biometric system should not reduced by biometric template protection scheme.

1.3 Biometric System Modules
There are basically four modules that are used for enrollment and authentication phases in biometric system. The **sensor module** is used in extracting the biometric data which may be image, audio or video. The **feature extraction module** is used in obtaining the template that is generated from the features of the biometric data. Each feature is labeled with a user's identity. The **Matching module** is used in authentication phase, where the template data is compared with data which is obtained from user and that it estimates the similarity between these data. These similar elements are processed in **Decision making module** which is used to identify the individual.

1.4 Biometric Vulnerabilities
The failure in the biometric system is classified into intrinsic system and adversary attack. Intrinsic attack is due to the incorrectness in the decision making of biometric system which may lead to false accept and false reject. In adversary attack the hacker will try to circumvent the biometric system for personal gains. These are classified into three types administrator attack, Non-secure Infrastructure and Biometric Overtness [1].

Any system (including biometric systems) is susceptible to various types of threats such as Denial of Service, Circumvention, Repudiation,Covert acquisition,Collusion and Coercion.There are various types of attacks on Biometric Systems shown in this figure.

1.Fake Biometric
Attack on the sensor. Sensor can be overridden by presenting fake . Like a fake finger, face mask or a copy of signature.

2.Replay Old Data
The Attack on the channel between the sensor and the feature extractor. Biometrics which was submitted can be resubmitted or replayed by bypassing the sensor. Like an old copy of fingerprint or face image.

3. Override Feature Extractor
Feature extractor can be override by attacking it and forcing it toproduce feature values selected by the hacker.

4.Synthesized Feature Extrator
Attack on the channel between the feature extractor and the matcher. Features extracted by the extractor can be replaced by a different feature set. This type of attack is difficult because the feature extractor and matcher are not separate. This attack is possible only if the matcher is remote and the features extracted have to be sent to the matcher for matching purpose.

5.Override Matcher
Attack on the matcher. Matcher can be overridden by attacking it and forcing it to produce high or low matching score irrespective of the input.

6.Modified Template
Attack on the stored database. The database can be local or remote. Templates which are stored at the time of enrollment

can be attacked by modifying one or more templates in the database. This could result in fraudulent authorization of an individual or a denial of service.

7.Intercept the channel

Attack on the channel between the system's database and the matcher. Respective template is selected and sent through a channel to the matcher for identification. This template can be changed accordingly by the hacker.

8. Override Final Decision

Attack on the channel between the matcher and application device. The decision whether the user can access the application device can be changed by the hacker accordingly.

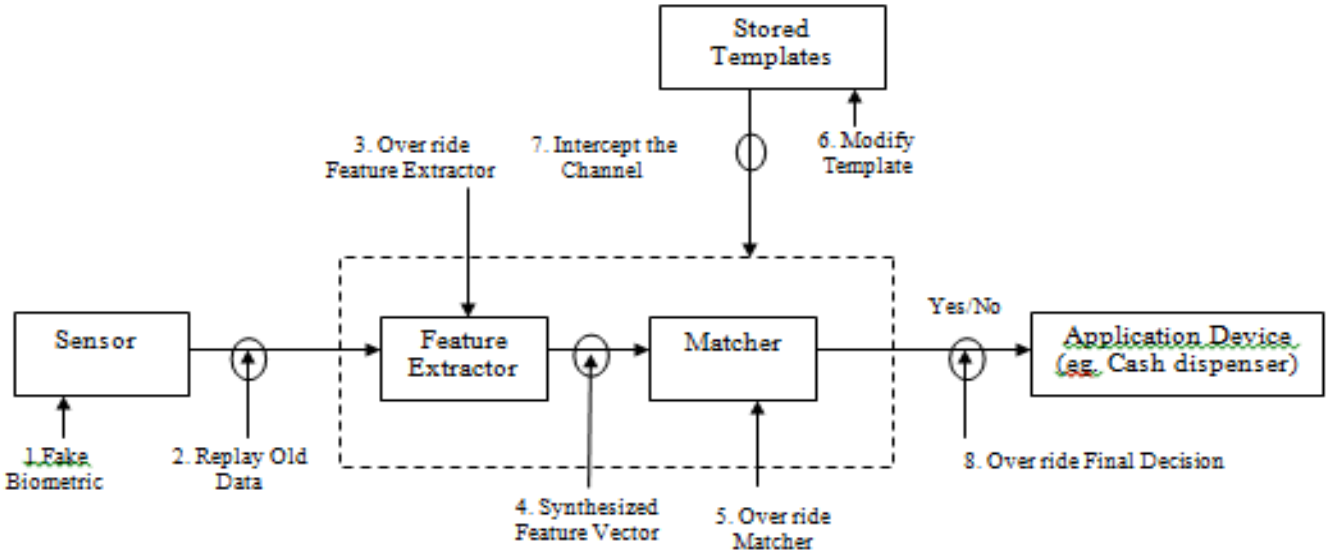

Fig 1: Biometric System with possible attack

2. LITERATURE SURVEY

2.1 Steganography Techniques for Biometric Template Security

Steganography means "covered writing" which comes from the Greek word steganos which means covered or secret and graphy means writing or drawing. The main objective of steganography is to securely communicate in a way that is not detectable by intruder. The covers used in steganography method is digital images, audio, video and other computer files that contain perceptually redundant or irrelevant information. After the embedding of secret image into cover image we have obtained an image called stegno image.

Here the original image is embed in digital image using a key which is done by stegno encoder system. The stego or covered image is than transmitted over a channel to the destination where the same key is employed to decode this stegno image by stegno decoder system. By this the biometric template is preserved. But this steganography is used highly during the transmission of biometric data.

Digital signals typically have high redundancies with respect to human perceptibility which can be exploited to embed data imperceptibly with high data hiding rate and tractable data extraction methods. We also require that data extraction methods in steganographic systems be blind to cover signals. Some popular methods in steganography include where different redundancies of a cover image are exploited for hiding the message.

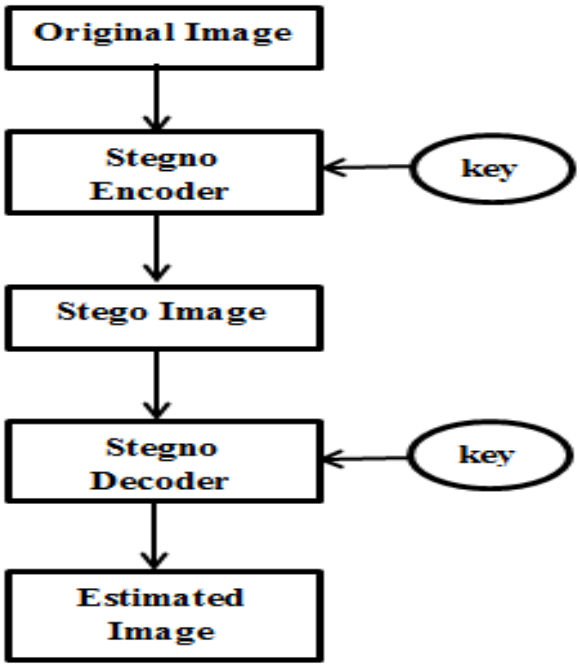

Fig 2: Steganography Model

2.2 Watermarking Techniques for Biometric Template Security

Water marking is one of the security technique which is defined as embedding information (watermark) in the host signal.Water marking with encryption technique provides more security,and it is useful in many application such as copyright protection,tempering detection,broadcast monitoring and data authentication.Watermarking techniques can be classified as transform domain watermarking,spatial domain watermarking which is based on embedding domain.The watermark can be classified as three types:Robust,Fragile, Semi fragile.

However watermarking introduces extra information into the biometric template[3].In this figure the watermark embedded in the host image. The watermarked host image is transmitted through communication channel. After that the watermark will extracted and get the original image.

In some other watermarking technique[4],the watermark is embedded in biometric Template it may be person name or address or some other unique feature of the person .Here the same watermark is embedded at four times in biometric template using secret key. It will give more security if one watermark changed by attacker other watermarks remains intact. The database manager maintain that secret key.

Thus watermarking avoids the forging and replacement of biometric template by attacker. If we combine watermarking with cryptography it increase the security of biometric system

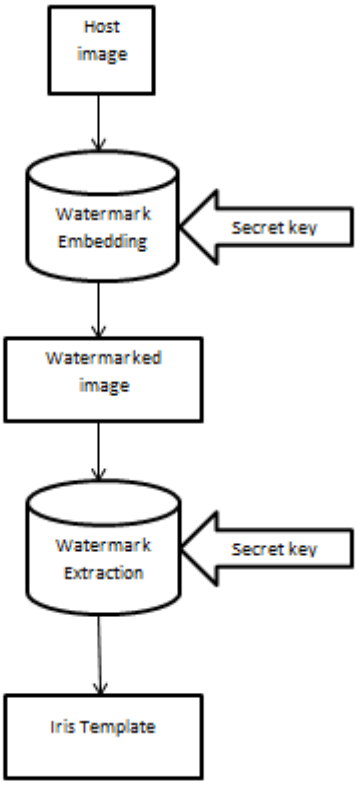

Fig:3 Watermark for iris template[7]

However watermarking introduces extra information into the biometric template[3].In this figure the watermark embedded in the host image. The watermarked host image is transmitted through communication channel. After that the watermark will extracted and get the original image. In some other watermarking technique[4],the watermark is embedded in biometric Template it may be person name or address or some other unique feature of the person .Here the same watermark is embedded at four times in biometric template using secret key. It will give more security if one watermark changed by attacker other watermarks remains intact. The database manager maintain that secret key. Thus watermarking avoids the forging and replacement of biometric template by attacker. If we combine watermarking with cryptography it increase the security of biometric system.

2.3 Visual Cryptography Technique For Biometric Template Security

Cryptography is used to securely communicate with each other. Its main objective is to protect not only the data alteration and theft but also used for user authentication. These are done through various techniques such as symmetric cryptography, asymmetric cryptography and hash function which employ with the public and private key.

Visual cryptography is introduced by Noar and Shamir. It is another form of cryptography in which secret communication is done in the form of images. This can be used to protect the biometric templates in which the decryption doesn't require any complex computations, it is done by human visual system. Using this visual cryptography the biometric data capture from the authorized user.These original image is divided into two shares .Each share stored in two different databases. When both images are simultaneously available then only we can get the original image. The individual share do not reveal any information about the original image.

However the fingerprint image is divided into two shares which means each pixel is divided into two sub pixels using visual cryptography.Each share stored in two different databases which is done in Enrollment phase.In authentication phase,each share requested from that corresponding database,then two shares are overlaid. Using XOR operation we get target image which will be compared with original image get from the user whenever entering. When two shares are overlaid the original pixel value can be determined.If the pixel is black,then we will get two black pixels.If it is white pixel then we will get one black and one white subpixel.so the reconstructed image 50% loss in contrast.

This technique is also used for iris codes.So the visual cryptography scheme is more secure for biometric template security.But it requires more space for storing sheets due because of pixel expansion.

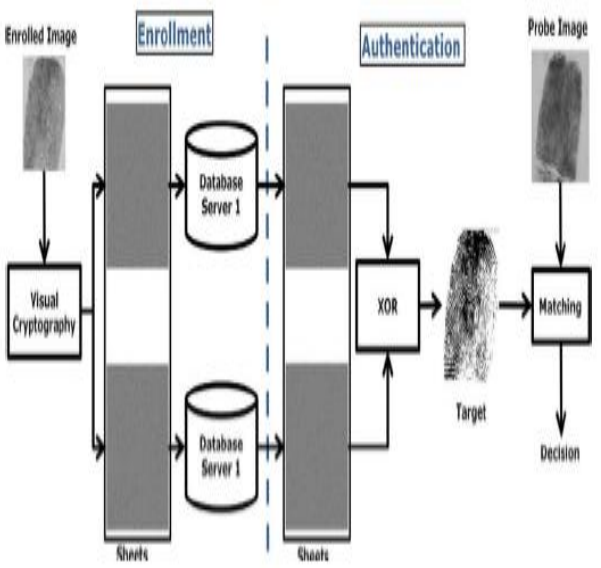

Fig:4 Fingerprint template security using visual cryptography scheme[21]

3. CONCLUSION

Various types of approaches developed by researches to secure the biometric data and template in database .In these paper three techniques discussed which are used to secure the biometric template. Each technique has its own advantages as well as limitations. We can combine any two techniques and achieve an effective solution to keep the biometric template more secure.

4. ACKNOWLEDGMENTS

The authors are grateful to Dr.S.Karthik**,** Professor & Dean**,** Prof.T.Kalaikumaran**,** Professor & HoD, Department of Computer Science and Engineering, for their valuable suggestion and guidance.

5. REFERENCES

[1] Agrawal .N and Savvides.M, "Biometric data hiding: A 3 factor authentication approach to verify identity with a single image using steganography, encryption and matching," in Proc. Computer Vision and Pattern Recognition Workshop, 2009, vol. 0, pp. 85–92..

[2] Ateniese.G, Blundo.C, Santis.A, and Stinson.D, "Extended capabilities for visual cryptography," Theor. Comput. Sci., vol. 250, no. 1–2, pp. 143–161, 2001.

[3] Bitouk.D, Kumar.N, Dhillon.S, Belhumeur.B, and Nayar.S.K, "Face swapping: Automatically replacing faces in photographs," ACMTrans. Graph., vol. 27, no. 3, pp. 1–8, 2008.

[4] Chen.Y, Chan.Y, Huang.C, Tsai.M, and Chu.Y, "A multiple-level visual secret-sharing scheme without image size expansion," Inf. Sci.,vol. 177, no. 21, pp. 4696–4710, 2007.

[5] Cootes.T et al., "Active appearance models," IEEE Trans. Pattern Anal. Mach. Intell., vol. 23, no. 6, pp. 681–685, Jun. 2001.

[6] Davida G.I, Frankel.Y, and Matt.B.J, "On enabling secure applications through off-line biometric identification," in Proc. IEEE Symp. Security and Privacy, 1998, pp. 148–157.

[7] Dong.J and Tan.T, "Effects of watermarking on iris recognition performance," in Proc. 10th Int. Conf. Control, Automation, Robotics and Vision, 2008 (ICARCV 2008), 2008, pp. 1156–1161.

[8] Feng.Y, Yuen.P, and Jain.A, "A hybrid approach for face template protection," in Proc. SPIE Conf. Biometric Technology for Human Identification, Orlando, FL, 2008, vol. 6944.

[9] Gross.R, Sweeney.L, De la Torre.F, and Baker.S, "Model-based face de-identification," in IEEE Workshop on Privacy Research in Vision, Los Alamitos, CA, 2006.

[10] Jain.A and Uludag.U, "Hiding biometric data," IEEE Trans. Pattern Anal. Mach. Intell., vol. 25, no. 11, pp. 1494–1498, Nov. 2003.

[11] Jain.A, Nandakumar.K, and Nagar.A, "Biometric template security," EURASIP J. Advances Signal Process., pp. 1–17, 2008.

[12] Maltoni.D, Maio.D, Jain .A, and Prabhakar .S, Handbook of Fingerprint Recognition. Secaucus, NJ: Springer-Verlag New York, Inc., 2003.

[13] Moskovich.B and Osadchy.M, "Illumination invariant representation for privacy preserving face identification," in Proc. IEEE Computer Society and IEEE Biometrics Council Workshop on Biometrics, San Francisco, CA, Jun. 2010, pp. 154–161.

[14] Naor .M and Shamir .A, "Visual cryptography," in Proc. EUROCRYPT, 1994, pp. 1–12.

[15] Nakajima. M and Yamaguchi.Y, "Extended visual cryptography fornatural images," J. WSCG, vol. 10, no. 2, pp. 303–310, 2002.

[16] Prabhakar.S, Pankanti.S, and Jain.A, "Biometric recognition: Security and privacy concerns," IEEE Security Privacy, vol. 1, no. 2, pp. 33–42,Mar./Apr. 2003.

[17] Pravin M Sonare,Shubhangi Sapkal, "Stegano-CryptoSystem for Enhancing Biometric-feature security with RSA", Int. Conf.Information and Network Technology IPCSIT Vol.4 2011.

[18] Revenkar.P, Anjum.A, and Gandhare.W, "Secure iris authentication using visual cryptography," Int. J. Comput. Sci. (IJCSIS), vol. 7, no. 3, pp. 217–221, Mar. 2010.

[19] Soutar.C, Roberge.D, Stoianov.A, Gilroy.R, and Kumar .B, "Biometric encryption," in ICSA Guide to Cryptography. New York: Mc-Graw-Hill, 1999.

[20] Thuraisingham.B and Ford.W, "Security constraint processing in a multilevel secure distributed database management system," IEEE Trans. Knowl. Data Eng., vol. 7, no. 2, pp. 274–293, Apr. 1995.

[21] A. Ross and A. A. Othman, "Visual cryptography for Biometric privacy,"in IEEE transaction on information Forensics and security,vol.6,No.1,March 2011.