International Journal of Computer Applications (0975 – 8887)
Volume 4 – No.5, July 2010

Template and Database Security in Biometrics Systems: A Challenging Task

Manvjeet Kaur
Lecturer CSE Deptt.
PEC University of Technology

Dr. Sanjeev Sofat
Prof. and Head CSE Deptt.
PEC University of Technology

Deepak Saraswat
ME (CSE) Student
PEC University of Technology

ABSTRACT

Security is a very important aspect in the biometric system. There are number attacks and there remedial solutions discussed in the literature on different modules of biometrics system and communication links among them. But still the researchers are not able to secure every module of a biometric system against these attacks. Template and database are the very important parts of biometric systems and attacker mostly attack on template and database of biometric system so securing them is a very crucial issue these days. In this research paper our focus is on template and data base security in biometrics system and we develop a system to encrypt and decrypt the biometric image using helper data of a fingerprint and password to make it secure so that even if someone gains access to the encrypted image stored in the database he will not able to reproduce the original image from it and it will be useless for him.

Keywords

Biometric, Fingerprint, Features, Fuzzy vault, Cryptography, Security, Polynomial.

1. INTRODUCTION

This paper discusses in brief about various attacks and different schemes and methods to secure the biometric system from these attacks. This work focuses on template and data base security. A fuzzy vault cryptographic biometric system is developed for securing the template and database in the biometric system.

Cryptographic biometric [1] i.e. merging of biometric and cryptography has been introduced as an effective means to address the security issues of privacy enhancing technologies with respect of personal data protection. It is also solves most of the cryptographic key management problems, because all cryptographic algorithms fully depend on the assumption that the keys will be kept in absolute secrecy. It intends to bind a cryptographic key with the user's biometric information in a manner to meet the distortion tolerance and discrimination requirements. Therefore, Crypto-Biometric merging can be done broadly at two different modes [2]

a. Loosely-coupled mode (biometric key release), the biometric matching is decupled from the cryptographic part. Biometric matching operates on biometric templates, if they match; cryptographic key release from it is at secure location, e.g. a server or smart card.
b. Tightly-coupled mode (biometric key generation), biometric and cryptography are merged together at a much deeper level, i.e. the biometric signals are monolithically bounded to the keys. The matching at this level can effectively take place within cryptographic domain. Cryptographic construct, i.e. Fuzzy Vault, is an example of biometric crypto bounded mode.

Section 2 discusses about the attacks on Biometric Systems, section 3 discusses about Template Protection Schemes. In section 4 the proposed technique is described and section 5 discusses the result analysis. Section 6 is about conclusion and future scope.

2. ATTACKS ON BIOMETRIC SYSTEMS

2.1 Generic Security Threats

Any system (including biometric systems) is susceptible to various types of threats. These threats are discussed below:

i. **Denial of Service:** An adversary overwhelms computer and network resources to the point that legitimate users can no longer access the resources.
ii. **Circumvention:** An adversary gains access to data or computer resources that he may not be authorized to access.
iii. **Repudiation:** A legitimate user accesses the resources offered by an application and then claim that an intruder had circumvented the system.
iv. **Covert acquisition:** An adversary compromises and abuses the means of identification without the knowledge of a legitimate user.
v. **Collusion:** In any system, there are different user privileges. Users with super-user privileges have access to all of the system's resources. Collusion occurs when a user with super-user privileges abuses his privileges and modifies the system's parameters to permit incursions by an intruder [4].
vi. **Coercion:** A legitimate user is forced to give an intruder access to the system. For example, an ATM user could be forced to give away her ATM card and PIN at gunpoint [4].

2.2 Biometric security threats

Figure 1 shows biometric system modules and nine different points of attack. These points of attack are discussed in below [5].

i. **Type 1:** This point of attack is known as "Attack at the scanner". In this attack, the attacker can physically destroy or fake the recognition scanner and cause a denial of service as described in 2.1.

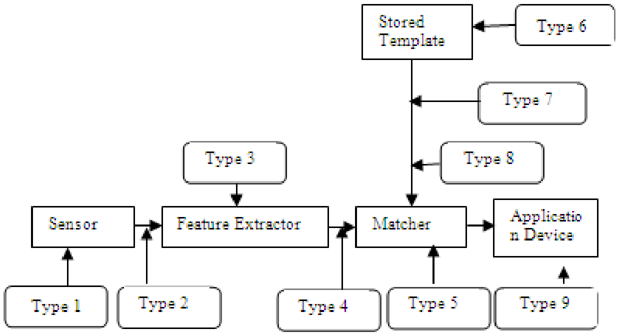

Figure 1: Attack points on a Biometric System

ii. **Type 2:** This point of attack is known as "Attack on the channel between the scanner and the feature extractor" or "Replay attack". In this attack, the attacker intercepts the communication channel between the scanner and the feature extractor to steal biometric traits and store it somewhere. The attacker can then replay the stolen biometric traits to the feature extractor to bypass the scanner.

iii. **Type 3:** This point of attack is known as "Attack on the feature extractor module". In this attack, the attacker can replace the feature extractor module with a Trojan horse [6]. Trojan horses in general can be controlled remotely. Therefore, the attacker can simply send commands to the Trojan horse to send to the matcher module feature values selected by him.

iv. **Type 4:** This point of attack is known as "Attack on the channel between the feature extractor and matcher". This attack is similar to the attack described in 2.1. The difference is that the attacker intercepts the communication channel between the feature extractor and the matcher to steal feature values of a legitimate user and replay them to the matcher at a later time.

v. **Type 5:** This point of attack is known as "Attack on the matcher". This attack is similar to the attack described in 2.1. The difference is that the attacker replaces the matcher with a Trojan horse. The attacker can send commands to the Trojan horse to produce high matching scores and send a "yes" to the application to bypass the biometric authentication mechanism. The attacker can also send commands to the Trojan horse to produce low matching scores and send a "no" to the application all the time causing a denial of service.

vi. **Type 6:** This point of attack is known as "Attack on the system database". In this attack, the attacker compromises the security of the database where all the templates are stored. Compromising the database can be done by exploiting vulnerability in the database software or cracking an account on the database. In either way, the attacker can add new templates, modify existing templates or delete templates.

vii. **Type 7:** This point of attack is known as "Attack on the channel between the system database and matcher". In this attack, the attacker intercepts the communication channel between the database and matcher to either steal and replay data or alter the data.

viii. **Type 8:** This point of attack is known as "Attack on the channel between the matcher and the application". In this attack, the attackers intercept the communication channel between the matcher and the application to replay previously submitted data or alter the data.

ix. **Type 9:** This attack is called "Attack on the application" [7]. Bugs are a consequence of the nature of the programming task that no one can deny. It is a fact that any software has at least one bug in it. Since biometric authentication systems are not 100% accurate, most of these systems use traditional authentication schemes as a backup.

3. TEMPLATE PROTECTION SCHEMES

An ideal biometric template protection scheme should possess the following four properties [8].

i. **Diversity:** the secure template must not allow cross matching across databases, thereby ensuring the user's privacy.

ii. **Revocability:** it should be straightforward to revoke a compromised template and reissue a new one based on the same biometric data.

iii. **Security:** it must be computationally hard to obtain the original biometric template from the secure template. This property prevents an adversary from creating a physical spoof of the biometric trait from a stolen template.

iv. **Performance:** the biometric template protection scheme should not degrade the recognition performance (FAR and FRR) of the biometric system.

Figure 2 shows various template protection schemes as discussed by Anil K Jain et al in their review article on Biometric Template Security [7]. Template protection schemes are broadly classified into feature transform and biometric cryptosystem as shown. The paper discusses about the merits and demerits of all the protection schemes.

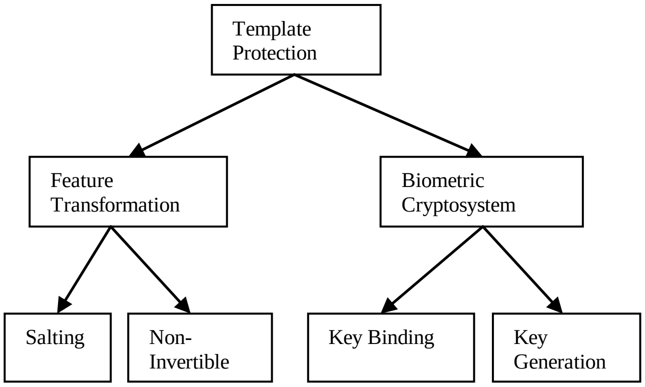

Figure 2: Categorization of template protection schemes.

4. PROPOSED TECHNIQUE TO SECURE BIOMETRIC TEMPLATE AND DATABASE

This technique focuses on securing biometric template for any image (face, palm print, iris etc.). It makes use of fingerprint and password to secure the images. Figure 3 represents the block diagram of the encryption process.

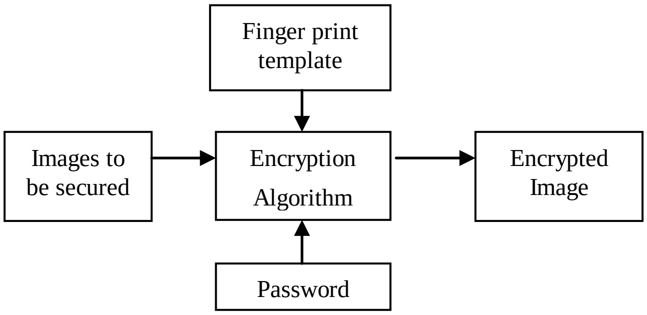

Figure 3: Block diagram of the Encryption process

4.1 Encryption algorithm to secure the image using the fingerprint and password

Given below is the step wise procedure for Encryption process:

Step 1: Choose a password. Password must be numerical value of any length.

Step 2: Choose an image which is to be encrypted. Image can be of any size.

Step 3: Form the polynomial using the password. If the length of the password is 6 digit than polynomial will be Polynomial(x) = $d_1x^5 + d_2x^4 + d_3x^3 + d_4x^2 + d_5x^1 + d_6$ [12, 14]

Step 4: Secret key is to be generated from the polynomial. To generate the secret key take the coefficients of the variable x. suppose the password is 340608, than polynomial will be $3x^5 + 4x^4 + 6x^2 + 8$ and the secret key will be 3468.

Step 5: Choose a fingerprint image and extract the termination and bifurcation points as T_x, T_y and B_x, B_y respectively. Suppose there are 5 terminator and 15 bifurcations. Then size of T_x = [5][1], Size of T_y = [5][1]. Size of B_x = [15][1], Size of B_y= [15][1].

Step 6: Choose high size of matrix among there because if you choose lower size of matrix algorithm will encrypt less effectively. So choose higher size matrix i.e. B_x[15][1]. Matrix B_x [15][1] will be used to encrypt the image.

Step 7: Generate a square matrix from the derived matrix.

Step 8: Calculate determinant of square matrix, name it as D and calculate W as square root of the Secret key minus D

Step 9: Calculate X subtracting W from each pixel of the image.

Step 10: The X obtained is the Encrypted image.

4.2 Decryption Algorithm

To obtain the original image from the encrypted image encryption steps can be reversed.

5. RESULT ANALYSIS

The results are analyzed on a database containing 50 images of fingerprint templates, 50 images of any biometric traits or any other data which needs to be encrypted or decrypted and a password which is required for secret key generation during the encryption and decryption process. The password to be chosen can be of any length. Image size of finger print template taken is 256X256 and resolution is set to 72 dpi. Two types of tests are performed on the database, during Test1 50 different images to be encrypted, 50 different passwords and 50 fingerprint templates are considered. During Test2 results are analyzed on 50 different images and 50 different passwords and with one fingerprint template. Discussed below is the result analysis from both the tests.

5.1 Test 1

Password -Any numerical value (Password must be longer for security purpose)
Images which are encrypted or decrypted- Take any biometric traits or pictures.

Table 1: Encryption and decryption of the 50 biometric traits or other images by 50 finger print templates and 50 passwords

Number of input fingerprint templates	50
Number of input password	50
Number of images	50
Number of images successfully encrypted	50
Number of images successfully decrypted	47
Number of unauthorized users successfully decrypt the image	2
Number of authorized user unsuccessful in decrypting image	1

Numbers of unauthorized users successfully decrypt the image defines the number of false users who enters the system by trying various combinations and got successful to access the systems. Number of authorized user unsuccessful in decrypting the image defines the users who are unable to access the system inspite of being authorized users due to some reasons. So the accuracy of the system can be calculate as percentage of unauthorized users successfully decrypt image and percentage of authorized user unsuccessful in decrypting image , as show below.

Percentage of unauthorized users successfully decrypt image =2/50*100=4.0%

Percentage of authorized user unsuccessful in decrypting the image =1/50*100=2.0%

Percentage accuracy with which genuine user decrypt the image =48/50*100=96.00%

In the table mentioned above there is one case where authorized user was unsuccessful in decrypting the image because he/she cannot decrypt the image. There are also two cases in which are number of unauthorized users successfully decrypt image means that they decrypted others persons data. So the accuracy or percentage accuracy with which genuine user decrypts the image = 96.00% for two attributes (fingerprint template and other images).Next section describes same process with 50 images and one fingerprint template

5.2 Test 2

Password -Any numerical value (Password must be longer for security purpose)

Images which are encrypted or decrypted- Take any template image or pictures.

Table 2: Encryption and decryption of the 50 templates or other images by 1 finger print template and 50 passwords.

Number of input fingerprint templates	1
Number of input password	50
Number of Images	50
Number of Images are successfully encrypted	50
Number of images are successfully decrypted	50
Number of unauthorized users successfully decrypt image	0
Number of authorized user unsuccessful in decrypting the image	0

Percentage of unauthorized users successfully decrypt image =0/50*100=0.00%
Percentage of authorized user unsuccessfully decrypted image =0/50*100=0.00%
Percentage accuracy with which genuine user decrypt the image = 50/50*100 =100%
Following figure show the relation between polynomial degree and inaccuracy

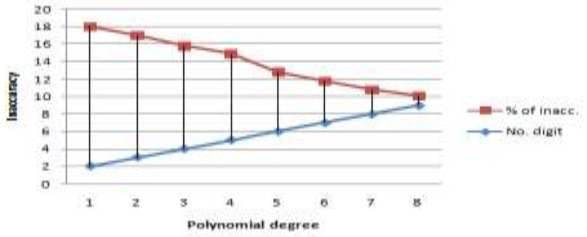

Figure 4: The inaccuracy varies according to the degree of polynomial

This is clear in Figure 4 that if the degree of polynomial increases than the inaccuracy decreases and hence accuracy increases.

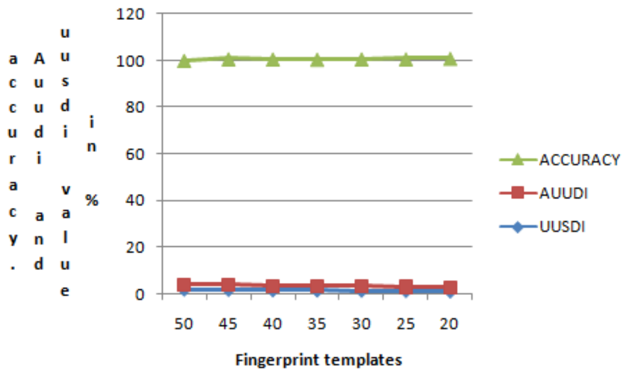

Figure 5 Show the relation among the UUSDI, AUUDI and ACCURACY

In Figure 5 UUSDI stand unauthorized users successfully decrypt image, AUUDI stand authorized user unsuccessful in decrypting the image.
This is clear to above figure 6.12 if the number of finger print template decreases that UUSDI, AUUDI decreases and accuracy increases.

6. CONCLUSION AND FUTURE SCOPE

6.1 Conclusion

This work concludes that since securing the biometric data is one of the important research aspects these days so a technique is proposed to secure any image based biometric traits using helper data. The results have been discussed by taking database of fingerprint traits, images and passwords. Images are encrypted and decrypted in this thesis and results have been shown. The results are analyzed on database containing 50 images of finger print template, 50 images of other biometric traits and 50 different passwords. When the 50 images of biometric traits are encrypted and decrypted by using 50 images of finger print template and 50 different passwords than this developed technique gives 96% security. When the 50 images of biometric traits are encrypted and decrypted by using 1 image of finger print template and 50 different passwords than this developed technique gives 100% security.
The result analysis shows that as we keep on raising the length of password the security of system increase. User can also take any size of image because this technique encrypt and decrypt properly any size of images.

6.2 Future scope

In this work fingerprint template and passwords are used for secure the biometric template and database. The images are encrypted using extracted features of finger print template and password. So combination of these two attribute give more security. This can be further extended if two or more biometric templates used to secure the data this means a encryption and decryption technique developed for secure the biometric templates and database by the help of feature vectors of two or more templates to provide more secure solution.

7. REFERENCES

[1] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," IEEE Transactions on Computers, vol. 55, pp. 1081-1088, 2006.

[2] S. Al-Tarawneh, L. C. Khor, W. L. Woo, and S. S. Dlay, "Crypto key generation using contour graph algorithm " in Proceedings of the 24th IASTED international conference on Signal processing, pattern recognition, and applications Innsbruck, Austria ACTA Press, 2006 pp. 95-98.

[3] A.K. Jain, A. Ross and U. Uludag, "Biometric template security: Challenges and solutions", Proceedings of 13th European Signal Processing Conference (EUSIPCO), 2005.

[4] D. Maltoni, D. Maio, A. K. Jain and S. Prabhakar. "Handbook of Fingerprint Recognition", Springer, 2003.

[5] Fargana Abdullayeva, Yadigar Imamverdiyev, Vugar Musayev, James Wayman "Analysis of security

vulnerabilities in biometric systems”, Science Direct 2006.

[6] Ao Shan, Ren Weiyin, Tang Shoulian “Analysis and Reflection on the Security of Biometrics System” 2008 IEEE.

[7] Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar” Review Article Biometric Template Security”, Hindawi Publishing Corporation EURASIP Journal on Advances in Signal Processing Volume 2008.

[9] Y. Sutcu, H. T. Sencar, and N. Memon, “A geometric transformation to protect minutiae-based fingerprint templates”, SPIE International Defense and Security Symposium, 2007.

[10] Salil Prabhakar, Phd thesis report on “Fingerprint Classification and Matching Using a Filterbank” 2001.

[11] Anil K. Jain, Salil Prabhakar, Lin Hong, and Sharath Pankanti “Filterbank-Based Fingerprint Matching” IEEE Transactions on Image Processing, Vol. 9, No. 5, May 2000.

[12] M. S. Al Tarawneh, W.L. Woo and S.S Dlay “Fuzzy Vault Crypto Biometric Key Based on Fingerprint Vector Features”, 2008 IEEE.

[13] Walter J. Scheirer and Terrance E. Boult, “Cracking Fuzzy Vaults And Biometric Encryption”, Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2007.

[14] Daesung Moon, Woo-Yong Choi and Kiyoung Moon “Fuzzy Fingerprint Vault using Multiple Polynomials” World Academy of Science, Engineering and Technology 59 2009.