International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Fingerprints Template Security Using Daes with Secure Fuzzy Vault

Silky Chhabra[1], Supreet Kaur[2]

[1, 2]Department of Computer Engineering, Punjabi University Patiala, Punjab, India

Abstract: ***Biometric systems are advanced technology, but this has also some security issues. Modules can be attacked by the attacker. Attackers mostly attacks on templates and databases which are critical parts of biometric systems because templates are stored record of an individual's features. To prevent the templates from intruders encrypt the templates. In recent years, most of the security techniques have been developed. In this paper, proposes a multilevel encryption layer to secure the templates. We have work on fingerprints templates. Firstly we encrypt the templates with double AES but it work as single layer and to provide more security again encrypt the double AES layer with Fuzzy vault. Fuzzy vault is Key binding biometric cryptosystem. Experimental results show that the proposed method performs well in improving security of templates and security method does not reduce the matching accuracy.***

Keywords: AES, Cryptography, Fuzzy vault, Attacks, Templates

1. Introduction

Biometrics systems gaining popularity in various applications for identify the individual's but there also increasing security issues. The term security means how much secure your system from intruders rather than authentication accuracy. By cryptography system can secure from hackers and for hackers has to difficult to find out the secret key and templates. Combination of cryptography and biometrics provide greater security to system rather than traditional system like passwords and token because biometric features can't be stolen, forgotten or malicious. A biometric system mainly comprises from four modules. Sensor module, feature extraction module, matching, decision module. The attacker usually attacks on these modules or channel between these modules. The following structure shows the attack points where attacker usually attacks.

- Type 1: The attacker attack on sensor module using fake fingerprints, image signature which cause a denial of service.
- Type 2: The attack on the channel between sensor and feature extractor. Biometric traits are stolen and stored somewhere else.
- Type 3: The feature set sends to matching module by attacker using Trojan Horse.
- Type 4: The attack on channel between feature extractor and matcher. The attacker steals feature values and resends them to the matcher module later.
- Type 5: The attack on matcher module. The matcher module is replaced with a Trojan horse which can produce the high or low matching score.
- Type 6: The attack on the stored database. The attacker modifies database where all the templates are stored.
- Type 7: The attack on the channel between system database and matcher. The attacker either steals replays or alters the data.
- Type 8: The attack on channel between matcher and user application. The attacker either steals replays or alters the data.

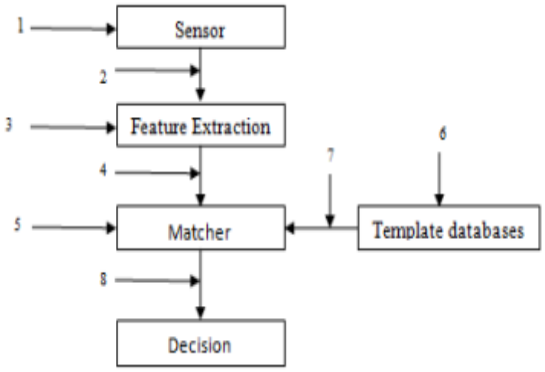

Figure 1: Attack points in Biometric system

Attacks on Templates: The following attacks perform on template databases. [7]

- Basic Brute Force: Attacker tries every possible bit combination till they guess the correct original feature data or key.
- Correlation Attack- From a cryptanalysis point of view, a good stream cipher should be resistant against a known-plaintext attack. In a known-plaintext attack the cryptanalyst is given a plaintext and the corresponding cipher text, and the task is to determine a key K. For a synchronous stream cipher, this is equivalent to the problem of finding the key K that produces a given key stream z1, z2,..., zN.
- Known Key Attack- Evaluate whether or not the fixed permutation with a randomly chosen key is ideal.
- Substitution Attack- "How difficult will it be to break into a folder containing biometric signatures and replace them with an attacker's biometric signature so that the attacker can get in with his/her own signature easily.
- Decidability Attack- Exploit available information to link across databases.
- Doppelganger Attack- If the FAR is 1 in X, then an attacker can try more than X different prints.
- Hill climbing Attack- Security attacks based on generating artificial data, injecting it in the system and after analyzing the output and modifies the data.

2. Literature Survey

Thi Thuy Linh Vo et al. [6] improves the technique key binding BCs: Fuzzy vault by removing x-coordinates out of the vault while indexing y-coordinates by evaluation of corresponding x-coordinates values based on a suitable hash function. The proposed Method prevents the fuzzy vault scheme from ARM, stolen key attacks and binding substitution attacks. The complexity of brute force attacks has also been increased. In proposed method , fuzzy vault scheme based on iris code. By improving scheme, the mint ropy has increased to 52 bits (it was 40 bits in the original scheme). The hash function which is constructed for indexing the new vault is only affected for ordered biometrics.

Bin Liang et al. [1] proposed a fingerprint encryption scheme based on threshold (t, n). The Threshold (t ,n) is fault tolerant scheme to protect the key. In this paper, ECC and quantization method are used to stabilize and compensate deformation of minutiae coordinates. In this proposed scheme, biometric cryptosystem does not need to store the templates and its biometric key is relatively long or it is available to work on-line as its database leak little information about biometric template. In proposed scheme, a low GAR, high time complexity, a coarse quantization and pr-aligned work.

Yoonjeong Kim et al.[10] proposed the scheme which used the bit plane fingerprint encryption and random block feedback RBF. Assume the randomness of the random number and proposed a method propagating the randomness to whole bit. In previous technique fingerprint encryption usually divides the 8 bit pixel image into bit plane and then performs full encryption for one bit plane and performs the simple operations on the remaining bit planes. So the security of this scheme is better than partial AES and even sometimes better than full AES in terms of human perception.

Shweta et al. [4] discussed to enhance the security of biometric system by using invisible watermarking technique with cryptography. Firstly it modifies the biometric traits with invisible watermarking and then further secured with cryptography. This techniques makes more secure by using parity check method in invisible watermarking techniques. This technique works on two phases template enrolment and template authentication. It satisfies the properties diversity, revocability, security and performances. It is suitable for any large scale data

O.P Verma et al. [2] analyses the performance comparison of algorithms (Blowfish, DES, Triple DES, AES) which have been used for encrypt the data. Performance results of algorithms have been checked on different hardware and two ciphers (block cipher, stream cipher). Blowfish is best perform under the speed and security but having many advantages and application it is still suffer from the weak key problem.

Yi.C.Feng et al. [9] developed a hybrid approach which takes advantages of biometric cryptosystem approach and transformed approach. Hybrid approach is defined by three steps random projection, discriminability preserving (DP) transform and fuzzy commitment scheme. This scheme provides security, discriminability and cancelability. Random projection makes a cancellable biometric template. DP transform improves the discriminability which has been losses by RP and coverts cancellable templates to binary templates and for security binary templates encrypt with fuzzy commitment scheme. Proposed algorithm is secure against brute force attacks and smart attacks. Smart attacks are Hill climbing, masquerade and affine transformation. To evaluate Hybrid approach, face databases have been taken from FERET, CMU-PIE, FRGC. By using Hybrid approach EER reduced from 12.58% to 8.55 for FERET database, 18.18% to 6.81% for CMU-PIE database, 31.75 to 16.68 for FRGC. This show DP transform can enhance the template discriminability in same subspace.

Walter J.Scheirer et al. [8] introduced privacy enhanced technologies BFV and BE and three classes of attacks against these technologies. Attacks via record multiplicity (ARM), surreptitious key Inversion (SKI), Binded subsititution Attacks .BFV compromised by all these attacks but BE is impacted by SKI via improved hill climbing attack and compromised by rest of attacks individual BFV and BE are not Secured enough for biometric systems.

Shih-Wei Sun et al. [4] presents key mixed templates (KMI) during feature extraction which mixes a user's templates with a secret key. A mixing function M (.) can mix the key determined random vector V_i and the template T_i as KMT_i = M (T_i, Vi). The KMT is useful for authentication process. It prevents from back end attack, snooping attack and tampering attack. Because it uses difficult key for different databases. If attacker attacks and going DB_1 in DB_2 for authentication. But the propose KMT_1 would not match for KMT_2 in DB_2.

P.Arul et al. [3] proposed a Biometric-Crypto system which generates a cryptographic key from the fingerprints for Encrypting and decrypting the voice data packets for VoIP Security. If your VoIP packets traverse the Internet to reach a destination, a number of attackers have a shot at your voice data. The calls are also vulnerable to hijacking or a man in the middle attack. In such a scenario, an attacker would intercept a connection and modify call parameters. The ramifications include spoofing or identity theft and call redirection, making data integrity a major risk. One way to help protect your privacy is to encrypt these conversations so that they aren't simply floating around out there for potential hackers to latch onto. In proposed system VoIP data packets encrypts using Advanced Encryption Standard (AES) with the novel method of Biometrics based Key Generation Technique.

3. Proposed Work

Figure 2: Block Diagram of Proposed Work

Algorithm of Proposed Work
Enrollment Algorithm

Begin

a) **Step 1: Image Acquisition**
b) **Step2: Test image pre-processing**
- *Step a: Compute gray scale conversion*
- *Step b: Median Filter*

c) **Step3: Apply Region growing technique for feature extraction**
- *Step a: get seed pixel e.g. starting pixel*
- *Step b: For every pixel in image*
- *Step c: Find shortest distance between neighbouring pixel using distance formula*
- *Select d: Select pixel with shortest distance in the region*

d) **Step 5:Apply Security on Region Growing Image**
- *Step a:First Level of Encryption using AES*
- *Step b:Second Level of Encryption using AES*
- *Step c:Save Image in Fuzzy vault*
- *Step d:Update Helper Data*

e) **Step 6:Stored Templates**

Authentication Algorithm

Begin

a) **Step 1: Image Acquisition**
- *Step a: Acquire test image*

b) **Step2: Test image pre-processing**
- *Step a: Compute gray scale conversion*
- *Step b: Median Filter*

c) **Step3: Apply Region growing technique for feature extraction**
- *Step a: get seed pixel e.g starting pixel*
- *Step b: For every pixel in image*
- *Step c: Find shortest distance between neighbouring pixel using distance formula*
- *Step d: Select pixel with shortest distance in the region*

d) **Step 4: Extract Minutiae Points**
- *Step a: Apply thinning technique to extract the fingerprints skeleton*
- *Step b: Extract Intersection Points(Minutiae)*
- *Step c: coordinates of Intersection Points(Minutiae coordinates)*

e) **Step 5: Load Training Image**

f) **Step 6:For Every Training Image**
- *Open Fuzzy Vault*
- *Decrypt Image level 1 using AES*
- *Decrypt Image level 2 using AES*
- *Apply step 4*
- *Return Minutiae Points*
- *Match with Test Data*
- *Return no of matching points*
- *If last Image*

Exit (Matching Decision)
Else
Repeat step 6

g) **Step 7: Return the training sample with most matching points as result**

4. Structure of AES in Proposed work

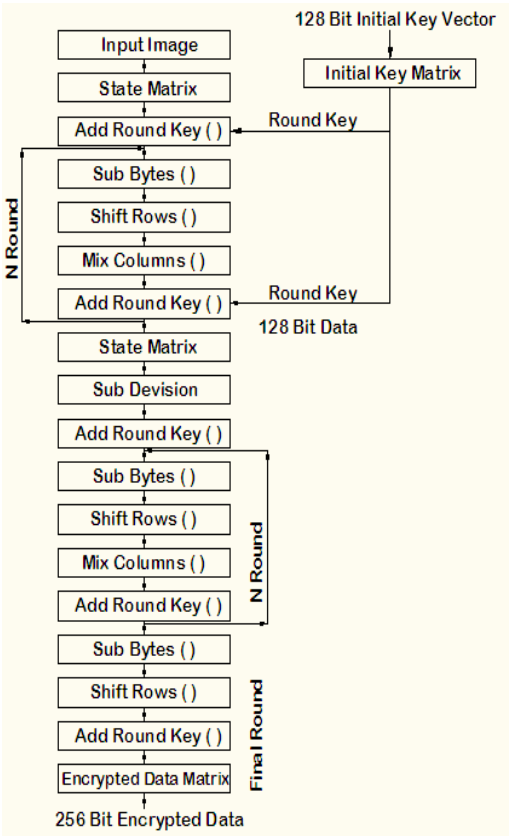

Figure 3: Encryption of AES

In Proposed work, we use double time AES algorithm, it uses 128 bit secret key. Before performing final round or fully encrypted the data, we subdivide the state matrix which gets after performing n rounds and then perform add round key step and again performs n rounds and at last performs final round and we get 256 bit encrypted bit data.

5. Results and Discussions

Images taken in the database are gray scale. A colored fingerprint image if given as input test image is to be first converted to gray scale image as gray scale images are easier for applying computational techniques in image processing. Matlab 2013a is used for coding. A gray scale fingerprint image is scaled for a particular size as 296x560 because many input images can be of different size whenever we take an input fingerprint for recognition. All the images in our database are of same size i.e. 296x560.

Based on experiment here computed the parameters value of FAR and FRR. We take 5 subjects means fingerprints of 5 persons and 8 samples of each person and perform testing on each samples 5 times and get the values of FRR and FAR.

Table 1: Values of FAR and FRR

Repetition Index	*FAR*	*FRR*
1	0.14	0.125
2	0.125	0.234
3	0.285	0.112
4	0.25	0.25
5	0.111	0

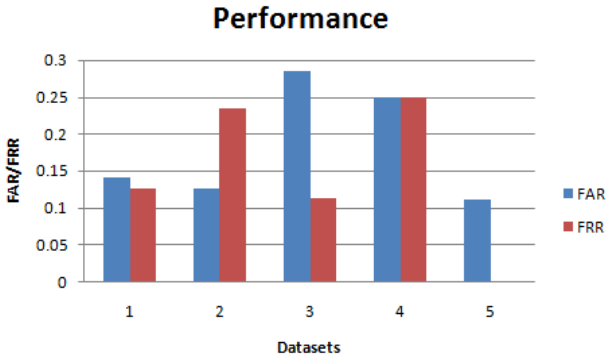

Figure 4: ROC curve of FRR and FAR

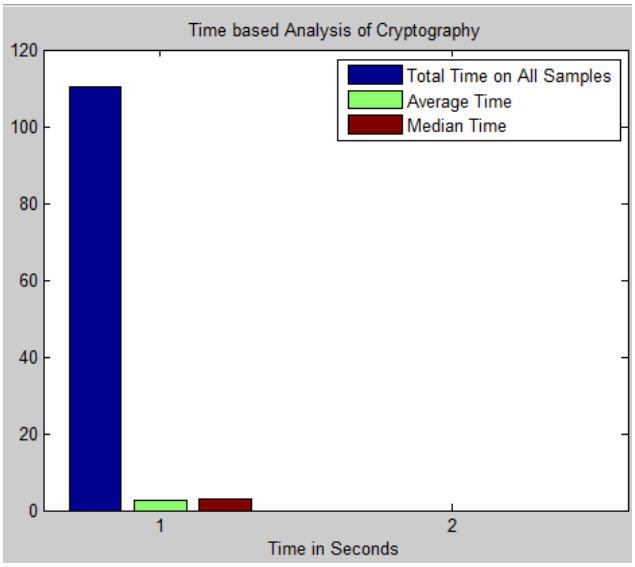

Figure 5: Time Graph of all samples

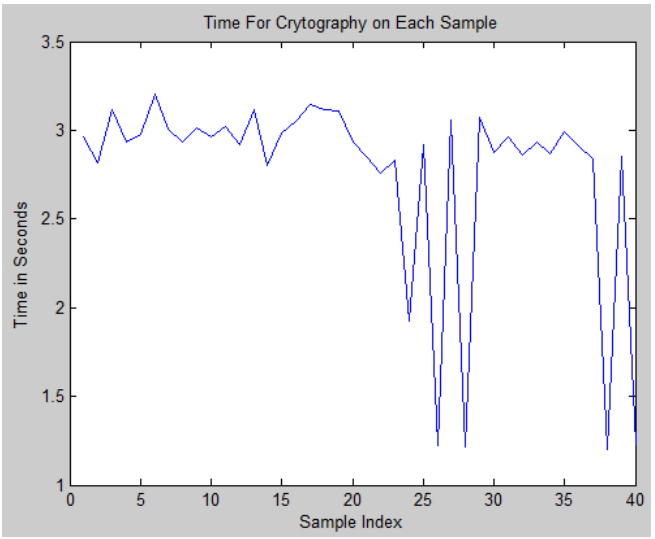

Figure 6: Time curve of each sample

6. Conclusion

In this paper, the fingerprints biometrics is secured using multi layer encryption, multi layer encryption means secure the system with combination of two techniques, Double AES and fuzzy vault. Firstly encrypt the templates using double time AES and then again encrypt it with fuzzy vault to provide more security. AES algorithm performs as double layer but it takes time as one layer. For research, we use 9 subjects or fingerprints of 9 persons and 8 samples of each subject. The total time taken by all samples after matching is 80s-100s approximately. The accuracy of system is 85% .AES algorithm also prevents from brute force attacks, differential attack and interpolation and square attacks.

7. Future Work

There is always a scope for improvement in every field of work, so here also. Security of system can be enhanced by combining other techniques like DAES combine with watermarking or using cryptography techniques. FAR, FRR and Time can be further reduced.

References

[1] Bin Liang, Zhendong Wu, LinYou, ”A novel fingerprint-based biometric encryption”, In Proceedings of IEEE , ninth international conference, 2014
[2] O P Verma, Ritu Agarwal, Dhiraj Dafouti, Shobha Tyagi, ”Performance analysis of data encryption algorithms” In Proceedings of IEEE , 2011.
[3] P.Arul, Dr.A.Shanmugam, ”Generate a key for AES using biometric for VOIP network security”, In Proceedings of JATIT,2009.
[4] Shih-Wei Sun,Chun-Shien Lu,Pao-Chi Chang, ”Biometric template protection: Akey mixed template approach”,In Proceedings of IEEE,2007.
[5] Shweta Malhotra, Dr.Chanderkant, ”A novel approach for securing biometric template”, In Proceedings of IJARCSSE, Vol. 3,Issue 5, May 2013.
[6] Thi Thuy Linh Vo, Tran Khanh Dang, Josef Kung, ”A hash-based Index Method for securing biometric fuzzy vaults”, In proceedings of Springer,2014.

[7] U.Latha1, Dr.K.Rameshkumar," A Study on attacks and security against fingerprint template database."
[8] Walter J.Scheirer, Terrance E.Boult, "Cracking fuzzy vaults and biometric encryption."
[9] Yi C.Feng,Pong C. Yuen, "A hybrid approach for generating secure and discriminating face template", In Proceedings of IEEE Transactions on Information's Forensics and Security, Vol. 5, No 1,March 2010.
[10] Yoonjeong Kim, Jihye Yoon, Jeong-Hyun Joo ,Kang Yi," Robust lightweight fingerprint encryption using block feedback", In Proceedings of Vol. 50 No.4,Feb 2014.

Author Profile

Silky Chhabra, Student (M.Tech), Punjabi university, Patiala,

Supreet Kaur, Assistant Professor, Punjabi university, Patiala,