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

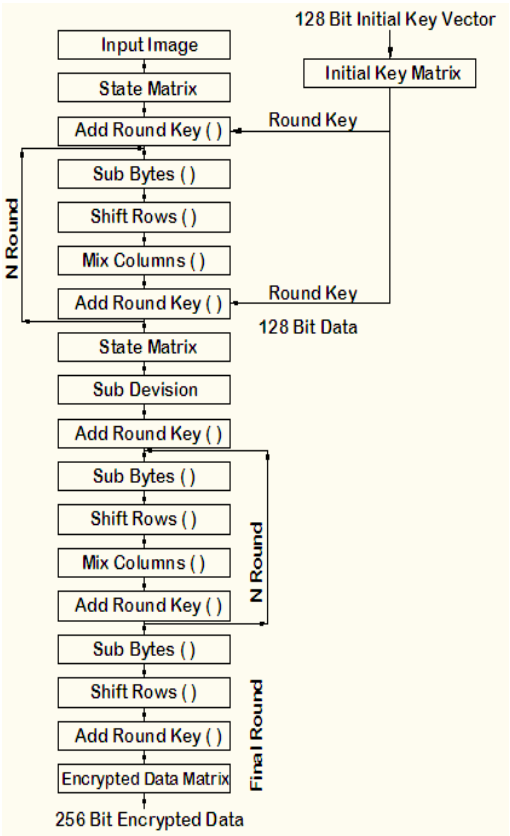

Figure 3: Encryption of AES

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

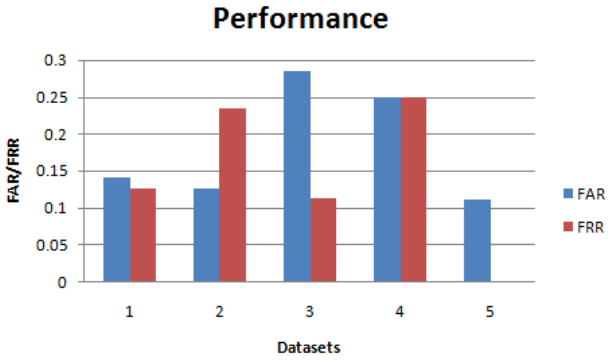

Figure 4: ROC curve of FRR and FAR

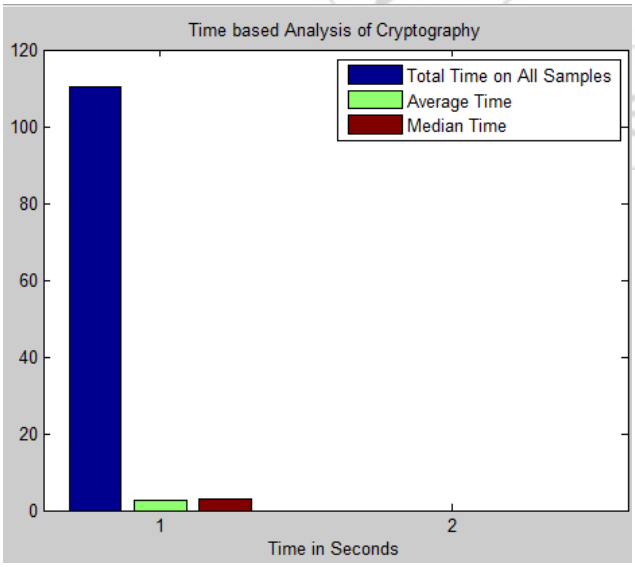

Figure 5: Time Graph of all samples

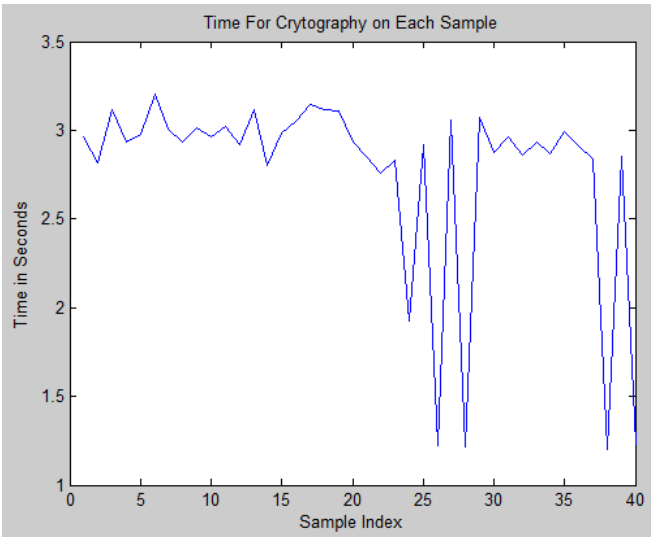

Figure 6: Time curve of each sample

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,