Proceedings of International Conference on Advances in Computer Technology and Management (ICACTM)
In Association with Novateur Publications IJRPET-ISSN No: 2454-7875
ISBN No. 978-81-921768-9- 5
February, 23rd and 24th, 2018

AN IMPLEMENTATION OF SHAMIR'S SECRET SHARING SCHEME OVER FINGERPRINT DATABASE

PROF. PRATIBHA MANDAVE
Assistant Professor, SIBAR, Kondhwa(Bk.),Pune
pratibha.mandave@gmail.com

DR.ABHIJEET KAIWADE
Research Guide ,Dr. DY Patil Institute of MCA,Akurdi,Pune
kaiwade@gmail.com

ABSTRACT

Security of secret data is major concern in today's digitized world. It is an important task to preserve the secret data from the probable threats, during the transmission. Various techniques [1,2,3,4,5,6] have been proposed in literature for secure transmission of data but not much work has been done on the secret transmission of images which is one of the difficult task to accomplish. One of the secret sharing schemes [11,7] which are used in literature to share the image transmission side can be applied either by using Blakeley's secret sharing scheme [2]) or Shamir's scheme [1] for sharing a secret. In this paper Shamir's secret sharing scheme is analyzed and implemented on a fingerprint biometric trait. The motivation for secret sharing [1,2] comes from the concept of secure key management. The schemes allow a user to divide portions of a secret among a participants group. Any t or more participants from a participants group of n members can cooperate to regain the original secret while (t-1) or fewer participants cannot reveal anything about the original secret.

KEYWORDS: Secret Sharing, Image Transmission, Network Security, Information Security, Cryptography

I. INTRODUCTION

Security of secret data is major concern in today's digitized world. The secret image sharing approach has been introduced by Adi Shamir [1].In some situations, there is usually one secret key that provides access to many important files. If such a key is lost (e.g., the person who knows the key becomes unavailable, or the entire computer which stores the key is destroyed), then all the important files becomes
inaccessible. The basic idea in secret sharing is to divide the secret key into pieces and distribute the pieces to different persons so that certain subsets of the persons can get together to recover the key.
Some important concepts are defined below related to secret sharing.

1. ALGORITHMS FOR SECRET SHARING : A REVIEW

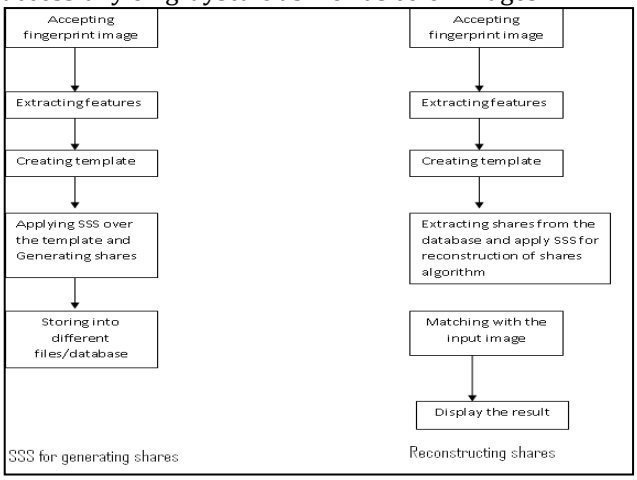
In cryptography, secret sharing refers to a method for distributing a **secret** amongst a group of participants, each of which is allocated a share of the secret.
The secret can only be reconstructed when the shares are combined together; individual shares are of no use on their own.

1.1 Shamir Secret sharing Scheme:-

The secret sharing scheme was first proposed by Shamir [3] and Blakley [2] in late 1980s. It is also called (k, n) threshold scheme which should meet thefollowing three requirements, where a secret isrepresented by a positive integer S. At the sender end, sharing process undergo the following steps from chosen number of shares k to retrieve the secret with total number of shares n. Shamir secret sharing is based on polynomial interpolation over a finite field. Shamir developed the idea of a (t, n) threshold-based secret sharing technique (t ≤ n). The technique allows a polynomial function of order (t −1) constructed as,
$f(x) = d0 + d1x1 + d2x2 + \ldots + dt-1xt-1 \pmod p$, where the value d0 is the secret and p is a prime number.
The secret shares are the pairs of values (xi, yi), where
$yi = f(xi)$, $1 \le i \le n$ and $0 < x1 < x2 \ldots < xn \le p - 1$.
The polynomial function f(x) is destroyed after each shareholder possesses a pair of values (xi, yi) so that no single shareholder knows the secret value d0. In fact, no groups of t − 1 or fewer secret shares can discover the secret d0.
On the other hand, when t or more secret shares are available, then we may set at least t linear equations yi = f (xi) for the unknown di's. The unique solution to these equations shows that the secret value d0 can be easily obtained by using Lagrange interpolation.

2. IMPLEMENTATION OF SSS OVER FINGERPRINT BIOMETRIC TRAIT

This section introduces implementation of SSS algorithm.
The major objective is to use SSS algorithm over fingerprint template database.
SSS is one of the robust secret sharing schemes. With this we can achieve secure transmission of images and nobody can come to know the complete useful information about the image. Here we required minimum of 3 shares out of 5 shares for reconstruction of the secret image. It is found that the SSS applied over fingerprint trait works successfully on grayscale as well as color images.



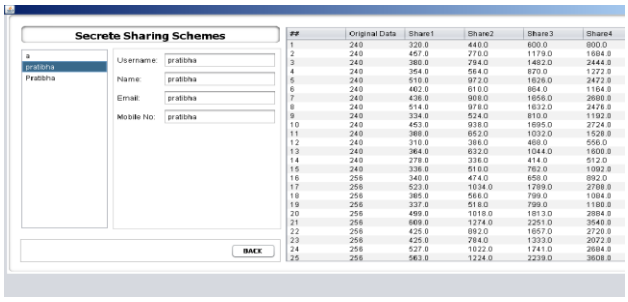
The Experiment was carried using Shamir's secret sharing method over fingerprint database and the steps are as follows:-
Step I:-Procured fingerprint images
Step II:- SSS algorithm implemented by means of a software.

The software follows the algorithm and generates shares and successfully matches the fingerprint.

The screenshots of the experiment are given below

a) Fingerprint images

b) Loading an input image



c) Generating shares of a fingerprint template database.

d) Matching the stored and generated fingerprints

3. CONCLUSION

In this paper we have presented the implementation of secret sharing scheme over fingerprint template. The experiment shows the successful generation and reconstruction of shares of fingerprint database. This is the first step of our proposed method of securing biometric database. In our future work we are going to give the additional security to the template database and generating new algorithm.

4. ACKNOWLEDGMENTS

I have a great pleasure in presenting this paper. I have completed this paper under the guidance of Dr. Abhijeet Kaiwade Sir. I would like to express my sincere thanks and gratitude to my guide for her guidance and support.

5. REFERENCES

[1] W. Zhao, R. Chellappa, A. Rosenfeld, and P. Phillips (2002) Face recognition: A literature survey. Technical Report CAR-TR-948,
UMD CS-TR-4167R, August, 2002

[2] M. Turk and A. Pentland (1991) Eigenfaces for recognition J. Cognitive Neuroscience, 1991, 3(1), pp. 71-86.

[3] A. Hyvrinen, J. Karhunen, E. Oja (2001) Independent Component Analysis Wiley,New York, 2001.

[4] M. S. Bartlett and T. J. Sejnowski (1997) Independent components of face images: a representation for face recognition Proceedings of
the 4th Annual Jount Symposium on Neural Computation, Pasadena, CA, May 17, 1997.

[5] Jian Yang, David Zhang and Jing-yu Yang (2005) Is ICA Signi_cantly Better than PCA for Face Recognition? Proceedings of the
Tenth IEEE International Conference on Computer Vision (ICCV'05) 1550-5499/05, 2005

[6] D. Swets and J. Weng (1996) Using Discriminant Eigenfeatures for Image Retrieval IEEE Transactions on Pattern Analysis and
Machine Intelligence, vol. 18, pp. 831-836, 1996.

[7] P. Belhumeur, J. Hespanha, and D. Kriegman (1997) Eigenfaces vs. Fisherfaces: Recognition Using Class Speci_c Linear Projection
IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 19, pp. 711-720, 1997.

[8]Sonali Patil, Kapil Tajane, Janhavi Sirdeshpande,"Secret Sharing Schemes For Secure Biometric Authentication", International Journal of
Scientific & Engineering Research, Volume 4, Issue 6,June-2013 2890 ISSN 2229-5518

[9] G. Ulutas, M. Ulutas, and V.V. Nabiyev, "Secret image sharing scheme with adaptive authentication strength",Pattern Recognition Letters, Vol.34, No.3, 283-291, 2013.

[10] T.L. Lin, S.J. Horng, K.H. Lee, P.L. Chiu, T.W. Kao,Y.H. Chen, R.S. Run, J.L. Lai, R.J. Chen, "A novel visual secret

sharing schemes for multiple secrets without a pixel expansion", Experts Systems with Applications, Vol.37, 7858-7869,2010.

[11] K. Etemad and R. Chellappa (1997) Discriminant Analysis for Recognition of Human Face Images journal of Optical Society of
America A, pp. 1724-1733, Aug.1997

[12]VinayRishiwal and Ashutosh Gupta "An Efficient Secret Image Sharing Scheme", Special section for proceeding of International e-Conference on Computer Engineering (IeCCE) 2012, World Applied Programming, Volume (2), Issue (1), January 2012. 42-48

[13] Dr. P. R. Deshmukh and Miss. Aarti G. Ghule,
"An Effective Implementation of Image SecretSharing Scheme",Paripex - Indian Journal of Research,Volume : 2, Issue : 4 April 2013

[14]Prof. SonaliPatil, Dr. PrashantDeshmukh"A Novel (t, n) Threshold Secret Sharing Using Dot Product of Linearly Independent Vector", International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013 2894 ISSN 2229-5518

[15]C. Asmuth and J. Bloom, "A Modular Approach toKey Safeguarding," IEEE Trans. On InformationTheory, Vol.29, No.2, 208-210, 1983