

A Novel Approach for Securing Fingerprint Template in a Distributed Environment

Prof. Pratibha Mandave¹, Dr. Abhijeet Kaiwade²

*Assistant Professor, SIBAR, Kondhwa (Bk.),
Pune, Maharashtra, India*
¹pratibha.mandave@gmail.com

*Research Guide, Dr. DY Patil Institute of MCA,
Akurdi, Pune, Maharashtra, India*
²kaiwade@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.

In cryptography, secret sharing refers to a method for 3 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 the following three requirements, where a secret is represented 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 ($t \leq n$). The technique allows a polynomial function of order (t - 1) constructed as,

$f(x) = d_0 + d_1x_1 + d_2x_2 + \dots + d_{t-1}x_{t-1} \pmod{p}$, where the value d_0 is the secret and p is a prime number.

The secret shares are the pairs of values (x_i, y_i) , where $y_i = f(x_i)$, $1 \leq i \leq n$ and $0 < x_1 < x_2 < \dots < x_n \leq p - 1$.

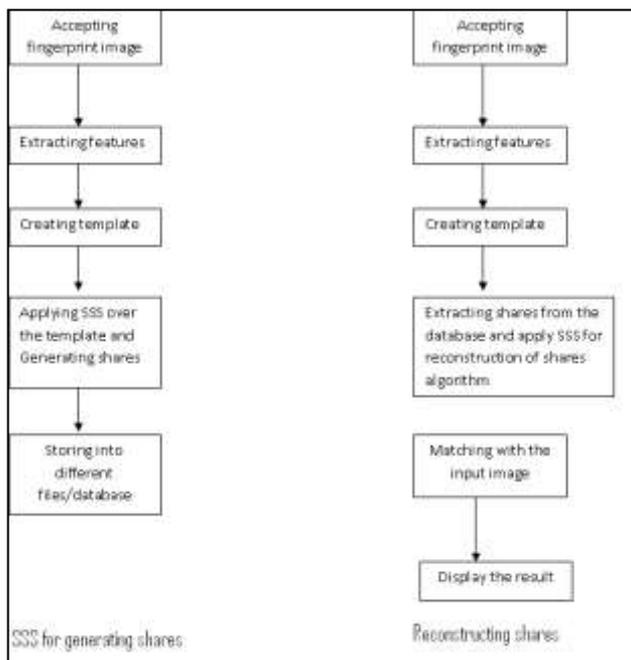
The polynomial function $f(x)$ is destroyed after each shareholder possesses a pair of values (x_i, y_i) so that no single shareholder knows the secret value d_0 . In fact, no groups of t - 1 or fewer secret shares can discover the secret d_0 .

On the other hand, when t or more secret shares are available, then we may set at least t linear equations $y_i = f(x_i)$ for the unknown d_i 's. The unique solution to these equations shows that the secret value d_0 can be easily obtained by using Lagrange interpolation.

1.2 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. Prepare the shares for the same and reconstruct the share and then matching of input data over stored database.

II. ALGORITHMS FOR SECRET SHARING : A REVIEW



The Experiment was carried using Shamir's secret sharing method over fingerprint database and the steps are as follows:-

All the proposed algorithms were programmed in JAVA version 1.8 using NetBean Editor. Performance was measured on a 2.0 GHz. Pentium IV with 1 GB of RAM running Windows XP Professional. The choice of language is due to a) JAVA is Robust b) Extensible with Web 3) Platform Independent.

The software can accept any biometric trait like (fingerprint, iris, face, etc.)

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 software.

Step III:-Procured the shares after applying SSS

Step IV:- Apply the chaos algorithm over the set of share

Step V:- Stored the shares into different files/database.

Step VI:- While reconstruction accept input as a fingerprint, use feature extraction algorithm and create template .

Step VII:-Extract the shares from the database and apply chaos reconstruction algorithm and then generates original shares from SSS reconstruction algorithm.

Step VIII:-Display the result.

This architecture gives an additional security to the template database



a) Fingerprint images



b) Loading an input image



c) Generating shares on a fingerprint template database.



d) Matching score

III. CONCLUSION

This paper review (2, 2) visual cryptography to overcome the issues like falsification and costly maintenance of large database. This implementation resulted in reduction of the time and space complexity of a system. The secret sharing scheme algorithms are discussed in this paper.

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.

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 Joint Symposium on Neural Computation, Pasadena, CA, May 17, 1997.
- [5] Jian Yang, David Zhang and Jing-yu Yang (2005) Is ICA Significantly 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 Eigen features 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) Eigen faces vs. Fisher faces: Recognition Using Class Specific Linear Projection IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 19, pp. 711-720, 1997.
- [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