General Access Structure Secret Sharing in Matrix Projection

Sonali Patil
Computer Department, SGBAU, Amravati,
Computer Department, PCCOE,
Pune – 411 033, Maharashtra India

Prashant Deshmukh
Computer Department
Sipna College of Engineering and Technology
Amravati – 444 701, Maharashtra India

ABSTRACT
Image Secret Sharing is a technique which provides security to confidential images by dispersed storages. General access structure image secret sharing provides flexibility for deciding qualified subsets of participants which can reconstruct the original secret image. Non qualified subsets of participants cannot get any information about original secret image. This paper proposes general access structure image secret sharing based on matrix projection. The experimental results show high accuracy, high security and less overhead in the network due to highly reduced size of image shares.

Keywords
Network Security; General Access Structure, Secret Sharing; Information Security; Cryptography

1. INTRODUCTION
Significant electronic data kept with only one person is easily missed or ruined. Secret sharing is a method to share the secret information among a group of participants against destruction and alteration. The basic concept of secret sharing was introduced by Blakley [1] and Shamir [2] independently in 1979.

In the schema of threshold secret sharing schemes, *t* out of *n* participant's shares are needed to be able to determine the key. In many applications it is required that only certain specified subsets of the participants should be able to recover the secret.

The goal of the General Access Structure Secret Sharing (GASSS) [3] is to provide the flexibility to decide which specified subsets of participants will able to reconstruct the original secret and which of participants cannot.

In this paper, a general access structure secret sharing is proposed for gray/color images based on matrix projection secret sharing scheme. The proposed method is secure and keeps the size of addition of all shares with each participant less than the original secret image.

T*he rest of the paper is organized as follows. Section II focuses on the literature of general access structure schemes related to proposed technique. Section III describes the algorithm of proposed image general access structure secret sharing method with multiple assignments. Section IV shows high lights on the experimental results of proposed scheme. Finally section V concludes about the proposed scheme.*

2. LITERATURE SURVEY
General Access Structure secret sharing was introduced by Ito, Saito [4]. They have introduced the so-called cumulative array technique for monotone access structures. It is the pioneer method for general access structure for secret sharing schemes.

Benaloh and Leichter [5] gave a simpler and more efficient way to realize general access structure secret sharing schemes. The Monotone Circuit construction is attributed to Benaloh and Leichter [5]. The idea here is to take a Boolean circuit as input. The share distribution for participants is calculated by functioning in reverse way means from output to input.

K. Srinathan et al. [6] described non perfect general access structure. Pang et al. [7] proposed secure and efficient secret sharing scheme with general access structure. Slamet et al. [8] introduced a new scheme which shows how sum labelling can be used for representing the graphs of access structure of secret sharing scheme.

Most of the researchers have used Shamir's Secret Sharing as a base scheme while suggesting general access structure. Iftene [9] proposed general access structure based on Chinese Remainder Theorem (CRT). Yun, Pucha [10] proposed a low computational, multi-stage secret sharing scheme with general access structure in which each participant has to hold one share only to share more than one secret. It is possible to change the participants set and access structure dynamically without updating any participants secret share.

Sai-zhi et al. [11] evoked a novel general access structure for multiple secret sharing, which is based on Shamir's secret sharing scheme and the discrete logarithm problem. Sun Hua and Wang Aimin [12] nominated a new secret sharing scheme for general access structure based on Shamir's threshold scheme and elliptic curve. [13] [14] [15] [16] are recent scheme supporting general access structure. Farras et al. [17] suggested natural generalizations of threshold secret sharing.

The next section describes algorithm of the proposed scheme which extends the matrix projection based secret sharing scheme [18] to general access structure secret sharing for images.

3. PROPOSED SCHEME
The assumptions for the proposed scheme are as follows:

Secret color image to be shared: S

Size of secret color image: (m X m)

Total number of participants: n

Set of Participants P = {P1, P2, ... ,Pn}

Dealer: D

Access Structure: Γ

Here, it describes the procedure in two phases as construction of shares of secret image and distribution to participants and reconstruction of secret image by qualified participants.

Construction of Secret Shares from Secret Matrix S

i. *Get the total number of participants n and set of qualified subsets of participants.*
ii. *Construct forbidden subsets of participants from qualified subsets.*
iii. *The number of required shares to be created is equal to number of forbidden sets (j) from step 2.*
iv. *Random (m X m) matrix A of rank j where m > 2(j - 1) – 1.*

v. *Choose j linearly independent (m X 1) random vectors x1, x2 ,....xj.*

vi. *Calculate share vi = (A X xi) (mod p) for 1≤ i ≤j where p is a prime number (maximum within 255) and j is number of shares.*

vii. *Compute $ = (A (A'A)-1A') (mod p).*

viii. *Solve R = (S - $) (mod p).*

ix. *Design distribution matrix by multiple assignment of shares.*

At the end of the construction the dealer will delete the matrices A, xi's, $, S and make the matrix R public. And as per the design of distribution matrix assign multiple shares to all participants.

Reconstruction of Secret Image S

The below algorithm explains reconstruction of original secret image by qualified subsets of participants.

i. *Collect shares from any qualified subset of participants; say the shares are v1, v2 …… vn.*

ii. *Build B as B=[v1 v2 . . . vn].*

iii. *Calculate the projection matrix $ as $ = (B (B'B)-1B') (mod p).*

iv. *Compute the secret image S = ($ + R (mod p)).*

If the collected shares are not from the qualified participants the secret does not get revealed. The next section discusses experimental results of the proposed scheme.

4. RESULTS

The proposed method is implemented by coding the algorithm in MATLAB R2012b. The experimental results are discussed here for the access structure Γ = cl{{P1, P3}, {P2, P4}}.

The Boolean function of Γ (P1, P2, P3, P4) is = P1P3 + P2P4

Figure 1 Secret Image Lena.jpg

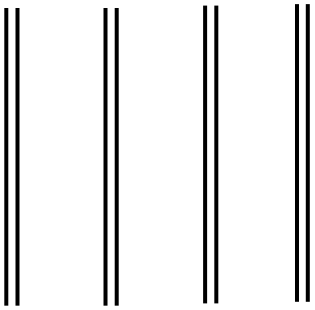

Figure 2 Shares with Participants (2 Shares with each Participant)

Reconstruction: Taking Access Structure {*P*1, *P*3} reconstructed secret is:

Figure 3 Reconstructed Secret

The forbidden subsets of participants can not reveal the original secret image. By taking Forbidden set of Participants {*P*1, *P*2} for above mentioned access structure, the reconstructed image is as shown below in figure.

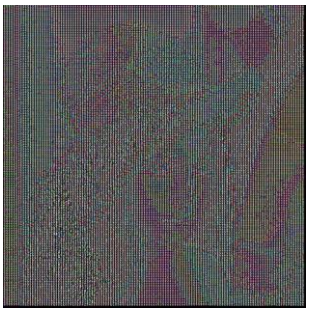

Figure 4 Reconstructed Image Using Forbidden Set of Participants

The below Table I shows information rate result for above mentioned access structure.

TABLE I. Results

Total No. of Participants	4
Secret Image	Lena.jpg
Secret Image Size	512 X 512
Access Structure	{{P1, P3}, {P2, P4}}
No. of Forbidden sets	4
Each Participants Share size	512 X 2
Information Rate	512 X 8

The information rate is greatly reduces as individual image share is of very small size.

The dissimilarity index is calculated for the reconstructed images by unqualified group of participants. The below table show the results.

TABLE II. DSSIM Results

Secret Image	**Reconstructed Secret by Unqualified Participants Shares**

	DSSIM
Lena.jpg	0.33665
Baboon.jpg	0.35145
Barbara.jpg	0.31555
Pepper.jpg	0.32485
Flower.jpg	0.34995

The table II and figure 5 shows the DSSIM values of reconstructed secrets by unqualified participants. The high DSSIM values proves the high security of the proposed scheme.

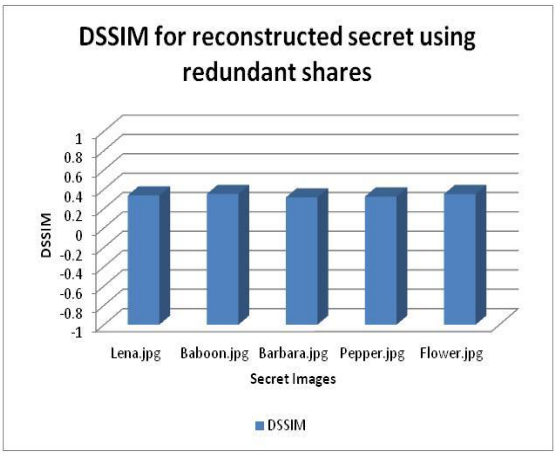

Figure 5 DSSIM for reconstructed secret using unqualified participants

Experimental results confirm that the proposed scheme is secure due to high dissimilarity index values.

The histograms are taken for the original secret image and the reconstructed secret by unqualified participants group as shown below.

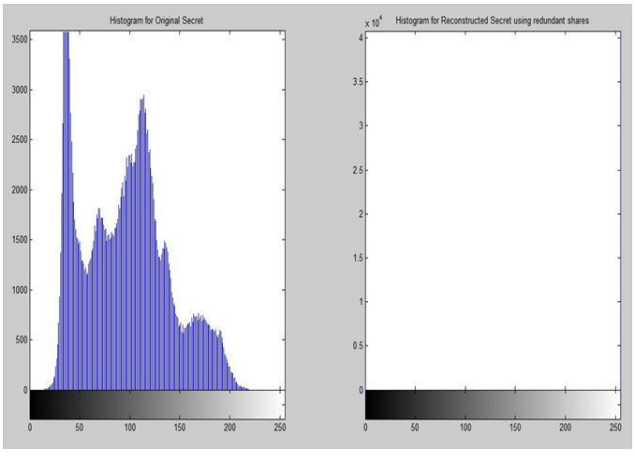

Figure 6 Histogram for Original Secret and Secret Reconstructed by Unqualified Participants

The above histogram shows huge difference between values of original secret and secret reconstructed by unqualified set of participants.

5. CONCLUSION

Images are preferably used in the network to send secret data. Image Secret Sharing provides security and reliability to images in the network. General access structure image secret sharing provides flexibility for deciding qualified subsets of participants which can reconstruct the original secret image. Non qualified subsets of participants cannot get any information about original secret image. The proposed method uses matrix projection and multiple assignment techniques. The experimental results showing high accuracy, high security and less overhead in the network due to highly reduced size of image shares.

6. REFERENCES

[1] Shamir, A., "How to Share a Secret", Communications of the ACM, vol.22, no.11, 1979.

[2] G. Blakely, "Safeguarding cryptographic keys", presented at the Proceedings of the AFIPS 1979 National Computer Conference, vol. 48, Arlington, VA, pp. 313–317, 1997.

[3] Sonali Patil, Prashant Deshmukh "An Explication of Multifarious Secret Sharing Schemes"International Journal of Computer Applications (0975 – 8887) Volume 46– No.19, May 2012.

[4] Mitsuru Ito, Akira Saito, Takao Nishizeki, "Secret Sharing Scheme: Realizing General Access Structure", GLOBECOM IEEE 1987.

[5] J. C. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In Proc. of CRYPTO '88, volume 403 of LNCS, pages 27–35. Springer-Verlag, 1990.

[6] K. Srinathan, N. Tharani Rajan, and C. Pandu Rangan, "Non-perfect secret sharing over general access structures," in INDOCRYPT, pp. 409–421, 2002.

[7] Pang, L.-J., Li, H.-X., Wang, Y.-M., "A secure and efficient secret sharing scheme with general access structures", Lecture Notes in Computer Science v 4223 LNAI, Fuzzy Systems and Knowledge Discovery - Third International Conference, FSKD, Proceeding pp. 646-649, 2006.

[8] Surjadi Slamet, Kiki Ariyanti Sugeng, Mirka Miller "Sum Graph Based Access Structure In a Secret Sharing Scheme" Journal of Prime Research in Mathematics Vol. 2, 1113-119, 2006.

[9] S. Iftene, "General secret sharing based on the Chinese remainder theorem with applications in e-voting", Electronic Notes in Theoretical Computer Science, vol. 186, pp. 67–84, 2007.

[10] WEI Yun, ZHONG Pucha, "A multi-stage secret sharing scheme with general access structures", IEEE 4th International Conference on Wireless Communications, Networking and Mobile Computing, pp.1-4, 2008.

[11] Sai-zhi Ye, Guo-xiang Yao, Quan-long Guan, "A multiple secret sharing scheme with general access structure, International Symposium on Intelligent Ubiquitous Computing and Education, 2009 IEEE.

[12] Sun Hua and Wang Aimin ," A Multi-Secret Sharing Scheme with General Access Structures based on Elliptic Curve" 3rd International Conference on Advanced Computer Theory and Engineering 2010 IEEE

[13] Cheng Guo and Chin Chen Chang, "A Construction for Secret Sharing Scheme with General Access Structure", Journal of Information Hiding and Multimedia Signal Processing, Vol. 4, Number 1, pp. 1-8, 2013

[14] Ching-Fang Hsu, Bing Zeng, Qi Cheng, "A Label Graph Based Verifiable Secret Sharing Scheme for General

Access Structures", Journal Of Communications And Networks, Vol. 15, NO. 4, pp. 407-409, AUGUST 2013

[15] V P Binu, A Sreekumar, "An Epitome of Multi Secret Sharing Schemes for General Access Structure", International Journal of Information Processing, vol. 8, Issue 2, pp. 13-28, 2014.

[16] V. P. Binu, A. Sreekumar, "Efficient Multi Secret Sharing with Generalized Access Structures", International Journal of Computer Applications, vol. 90, 2014

[17] O. Farras, C. Padro, Xing Chaoping, An Yang, "Natural Generalizations of Threshold Secret Sharing", IEEE transaction on Information Theory, vol. 60, Issue 3, pp. 1652-1664, 2014.

[18] Li Bai, "A strong ramp secret sharing scheme using matrix projection," presented at the Second International Workshop on Trust, Security and Privacy for Ubiquitous Computing, Niagara-Falls, Buffalo, NY, 2006.