General Access Structure For Modulo-2 Secret Sharing Scheme

Sonali Patil
Assistant Professor

Kapil Tajane
ME Student

Janhavi Sirdeshpande
ME Student

Computer Department, Pimpri Chinchwad College of Engineering, Nigdi, Pune

Abstract

There are circumstances where an action is required to be executed by a group of people. The idea of secret sharing is to divide a secret into pieces called shares, which are then distributed amongst users by the dealer. In the outline of threshold schemes, we wanted t out of n participants to be able to determine the key. In practice, it is often needed to specify exactly which subsets of participants should be able to determine the key and those that should not. The Access structure describes all the authorized subsets to design the access structure with required capabilities. A method is presented here in which a color secret image is shared in n shares using modulo-2 secret sharing scheme. Then as per the need of an application qualified and forbidden sets get finalized. The multiple assignments of shares are done to fulfil the requirement of general access structure. The shares are created with no size expansion. The original image can be reconstructed by applying reverse of the same encoding technique on qualified subset of shares. Unqualified subset of shares can not reveal anything about the secret image. The advantage of this scheme is that it is less complex to understand and implement, idle, perfect and provides general access structure.

Keywords: *Secret Sharing, Visual Cryptography, General Access Structure, Information Security.*

1. Introduction:

Security is an important issue in information technology. How to keep the secret information, so that it does not depend on one authority only is a major concern in today's reduced trust world. While keeping the secret we want to ensure that no single entity is entrusted with too much knowledge or power, the question now, is how to ensure that the secret will not be exploited by the authority holding it. Secret Sharing Schemes provides solution to such kind of problems. Secret Sharing Scheme (SSS) [1] is a method whereby a secret is assigned in n pieces of information called shares or shadows in such a way that: i)The secret can be reconstructed from certain authorized groups of shares and ii) The secret key cannot be reconstructed from unauthorized groups of shares.

Many researchers have been proposed threshold secret sharing schemes for color images. But very few researchers have proposed the general access structure for color image secret sharing as it is difficult to add the extended capabilities in general access structure schemes. In the outline of threshold schemes, we wanted t out of n participants to be able to determine the key. But in practice, it is often needed to specify

exactly which subsets of participants should be able to determine the key and those that should not. The Access structure describes all the authorized subsets to design the access structure with required capabilities. Here we have proposed a general access structure for (n, n) modulo-2 secret sharing scheme for color images.

The rest of the paper is organized as follows. In Section 2 literature survey is given for secret sharing schemes and general access structure. Section 3 explains the proposed scheme in detail. In section 4, experimental results are given and section 5 summarizes the proposed scheme and future scope.

2. Literature Survey:

2.1 Secret Sharing Schemes:

Secure transmission of data is more and more needed in the worldwide computer network environment. Shamir [2] and Blakely [3] invented two (k, n) threshold-based SSS independently in 1979. The general idea behind "secret sharing" is to distribute a secret to n different participants so that any k participants can reconstruct the secret, and any (k − 1) or fewer participants cannot reveal anything about the secret. Karnin [4] suggested the concept of perfect secret sharing (PSS) where zero information of the secret is revealed for an unqualified group of (k −1) or fewer members. For these requirements in PSS schemes, a secret has zero uncertainty if k or more participants can discover the secret. On the contrary, the secret, in PSS schemes, remains the same uncertainty for (k − 1) or fewer members. Therefore, there is no information exposed to (k−1) or fewer members.

Naor and Shamir [5] extended the secret sharing concept into image research, and referred it as visual cryptography. Visual cryptography is a PSS scheme, and requires stacking any k image shares (or shadow images) to show the original image without any cryptographic computation. They are not applicable for lossless image recovery due to: i) image shares have larger image size compared to the size of the original secret image and ii) the contrast ratio in the reconstructed image is quite poor. Thien and Lin [6] have presented a better image secret sharing approach. With some cryptographic computation, they cleverly used Shamir's SSS to share a secret image.

2.2 General Access Structure Schemes:

The Access structure describes all the authorized subsets to design the access structure with required capabilities. A perfect secret sharing scheme using the general access structure Γ, is a method of sharing a key K among a set of n participants such that P is the set of all participants, in such a way that the following two properties are fulfilled:

If an authorized subset of participants $B \subseteq P$ pool their shares, so that they can determine the value of K.

If an unauthorized subset of participants $C \subseteq P$ pools their shares, then they can determine nothing about the value of K.

We notice that a (k, n)-threshold scheme creates the access structure $\{B \subseteq P \mid |B| \geq t\}$. This structure is referred to by Stinson [1] as the threshold access structure.

It is possible to create a SSS for any access structure as long as this access structure satisfies monotone property:

subset B Є Γ and B ⊆ C ⊆ P then C Є Γ

In other words a superset of an authorized set is again an authorized set. Let's denote Γ as being a set of subsets of P, and the subsets in Γ as being the subset of participants that should be able to compute the key. Then Γ is denoted as being the access structure and the subsets in Γ are called authorized subsets. Furthermore if we let K be the set of keys and S be the share set, we use the dealer D to share a key k Є K by giving each player a share Si Є S. Sometime later a subset of players might attempt to determine K from the shares they collectively hold.

For (k, n) threshold scheme design of a general access structures is difficult. Ito, Saito [7] provided a new methodology to design a secret sharing scheme realizing any given access structure. However the number of shadows used in the scheme might be quite large although it is bounded. K. Srinathan [8] describes non perfect general access structure. He considered the problem of non-perfect secret sharing (NSS) over general access structures, defined a more general notion of access hierarchies and studied their tolerability properties.

Benaloh [9] presented a view that a threshold scheme is only a particular case of general access structure. For any given polynomial P, the number of n-variable monotone formulae of size no more than P(n) is exponential in P(n). However the total number of monotone functions on n variables is doubly exponential in n. Therefore, most monotone access structure cannot be realized with a large number of polynomial sized shares. Pang [10] proposed an efficient sharing scheme with general access structure. Sai-zhi [11] proposed a novel general access structure for multiple secret sharing, which is based on Shamir's secret sharing scheme and the discrete logarithm problem. In this scheme, the dealer need not send any secret information to participants. And the shared secret, the participant set and the access structure can be changed dynamically without updating any participant's secret shadow. The degree of the used Lagrange interpolation polynomial is only one, which makes the computational complexity of the proposed scheme very low.

3. Proposed Scheme:

The proposed scheme is divided into 3 steps:

- Construction of n secret image shares using modulo-2 operation.
- Deciding General Access Structure and distribution of shares among the participants.
- Reconstruct the secret by getting shares from qualified subset.

3.1 Construction of secret image shares:

We have chosen secret sharing scheme proposed by Wang [12] for creating the image shares as it is a low complex method.

To construct the secret image shares for (n, n) modulo -2 scheme following steps are used.

- Choose a random matrix Xi,
- Where i=1 to n-1.
- Create Z1=X1.
- Zi= Xi-1^Xi where i = 2 to n-1.
- Zn= Xn-1^ S,

Where, S is a pixel value of a secret image. Apply the method on all pixel values of image matrix. Zi's are created secret shares. ^ indicates Modulo-2 operation. We can't reconstruct secret image unless all n shares are obtained this can be easily prove as follows:

Xi^ Xj is a random matrix, while Xj (j=1,….n-1) is a random matrix.

Xi^S is also a random matrix, from which we can get Zi ≠ Zj.

That is, no information of matrix S could be obtained by the modulo-2 operation of any n-1 matrices. .

3.2 General Access Structure

Let us assume that there are 6 participants A, B, C, D, E and F. The threshold for secret creation is (5, 5) i.e. n is 5 here. As the shareholders are 6. The power set is of 26 = 64.

Let us assume that the qualified subsets are as follows:

Tqual= { {A, B, D}, {A, E, F}, {A, B, F}, {C, D}, {D, E}}

The superset of qualified subsets is again a qualified set. The remaining sets are forbidden sets. The multiple assignments of shares will be based on qualified subsets of participants. To achieve above mentioned general access structure, the multiple assignments of shares will be as follows:

A: Sh1, Sh2

B: Sh1, Sh3, Sh4

C: Sh2, Sh3

D: Sh1, Sh4, Sh5

E: Sh2, Sh3, Sh4

F: Sh5

As per the above assignments the shares are distributed. The 3 participants A, B and C can only obtain Sh1, Sh2, Sh3 and Sh4. Hence secret cannot be revealed. The participants C and D can put together to get all the n shares Sh1, Sh2 … Sh5. Hence the original secret can be reconstructed. This way we can prove that only qualified subset of participants get the original secret image.

3.3 Reconstruction of the Secret

To reconstruct the original image the same modulo-2 operation is used on the secret image shares. When we will get the shares from qualified subsets of participants only then the original image can get reconstructed. As all the n shares are required to reconstruct the original image, the qualified subsets of participants can only provide all n shares. We can reconstruct the original secret image using following formula:

S= Z1^ Z2^Z3…. ^Zn.

4. Experimental Results:

The following figure shows the results of implemented scheme:

Figure1: Original Secret Image and Reconstructed Secret Image

Figure 2: Created shares of a secret image

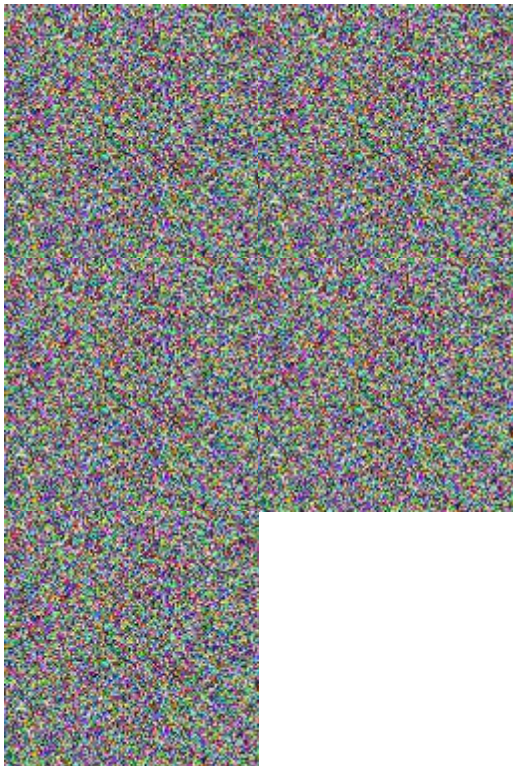

Table 1. Shows the size comparison of original secret image, shares constructed and reconstructed image and PSNR of reconstructed secret image.

Table I: Comparison of size of original image, created shares and reconstructed image and PSNR of reconstructed secret

	Original Image	Created Shares	Reconstructed Image
Size	256 x 256	256 x 256	256 x 256
PSNR			+ve ∞

5. Conclusion:

In this paper we have implemented a simple and lossless general access (n, n) secret sharing scheme using modulo-2 operation. The scheme is ideal as created shares are of same size as original secret image. The scheme is perfect as only qualified subsets of shares can reconstruct the original secret image. The forbidden group of shareholders cannot reveal anything about the original secret image. The complexity of implemented scheme is very low as the method used to create the shares and to get general access structure is very simple. In future parallel algorithm can be used to make this scheme faster.

6. References

[1] D. R. Stinson, "Cryptography: Theory and Practice", CRC Press, Boca Raton 1995.

[2] Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979.

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

[4] E. D. Karnin, J. W. Greene, and M. E. Hellman, "On secret sharing systems," vol. IT-29, no. 1, pp. 35–41, Jan. 83.

[5] M. Naor, A. Shamir, "Visual cryptography", Proc. Eurocrypt '94, Lecture Notes Computer Sci., Vol. 950, pp.1-12, 1994.

[6] C. Thien and J. C. Lin, "Secret image sharing," Computers & Graphics, vol. 26, no. 5, pp. 765–770, 2002.

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

[8] Benaloh, J., and J. Leichter, Generalized secret sharing and monotone functions, CRYPTO '88, Springer Verlag, pp. 27- 35.

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

[10] 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 2006, Proceeding 2006, p. 646-649.

[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] Daoshun Wang, Lei Zhang, Ning Ma, Lian-Sheng Huang: Secret color images sharing schemes based on XOR operation. IACR Cryptology ePrint Archive 2005: 372 (2005).