Analysing Secret Sharing Schemes for Color Images

Priyanka Chaudhari[1], Anuja Pardeshi[2], Priyanka More[3] and Sayli Thanekar[4]
[1234] *Department of Computer Engineering, Pimpri Chinchwad College of Engineering, Pune University, India.*

Abstract

Images are of great importance in communication field for conveying messages. Using images we can convey these messages very easily to the audience and there is no need to read the text, hence security of these images is of big concern. In recent years, many techniques were proposed to provide security to images and image secret sharing is one of the effective approaches for the same. This paper analyses different image secret sharing schemes like Shamir's secret sharing scheme, Thien Lin's secret sharing scheme and Lie Bai's secret sharing scheme. Performances of these schemes are analysed based on parameters like ideal, perfect, threshold based, accuracy, share size, image type etc. The comparative study shows that Lie Bai's method of matrix projection is more effective and reliable secret sharing method. This scheme also satisfies the security and accuracy conditions required by any image secret sharing scheme.

1. Introduction

Secret Sharing Schemes [1] (SSS) refers to a method for distributing a secret amongst a group of participants and each participant have allocated share of a secret. To reconstruct the original secret sufficient number of shares needs to be combined together and individual shares are of no use on their own.

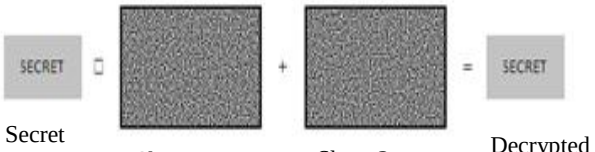
There are certain situations where the set of people needs to perform particular actions for executing it. Let us consider the example, suppose for accessing the confidential data or document minimum four authorize user's needs to perform certain actions and reveal the data. The scheme in which group of people come together and perform certain actions which regenerates the authorized or secret information is commonly

known as Secret Sharing Schemes.

In the worldwide computer network environment, secure transmission of data is needed on a wide range. In many commercial, medical and military applications the effective and secure protections of sensitive information which is mostly in the form of images are important. Image secret sharing is a better approach for these kinds of applications.

IMAGE SECRET SHARING: [2]

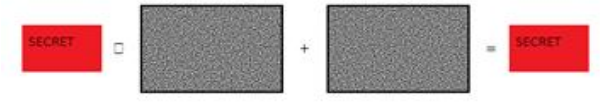
Image secret sharing operates directly on the bit planes of the digital input. The input image is decomposed into bit-levels which can be viewed as binary images. Using the $\{k,n\}$ threshold concept, the image secret sharing procedure encrypts individual bit-planes into the binary shares which are used to compose the share images with the representation identical to that of the input image. Depending on the number of the bits used to represent the secret (input) image, the shares can contain binary, grey-scale or color random information. Thus, the degree of protection afforded by image secret sharing methods increases with the number of bits used to represent the secret image.



Secret grey scale | Share 1 | Share 2 | Decrypted image

The decryption operations are performed on decomposed bit-planes of the share images. Using the contrast properties of the conventional $\{k, n\}$-schemes, the decryption procedure uses shares' bits to recover the original bit representation and compose the secret image. The decrypted output is readily available in a digital format, and is identical to the input image. Because of the symmetry constraint imposed on the encryption and decryption process, image secret

sharing solutions hold the perfect reconstruction property. This feature in conjunction with the overall simplicity of the approach make this approach attractive for real-time secret sharing based encryption/decryption of natural images.



Secret color image | Share 1 | Share 2 | Decrypted image

Color image secret sharing scheme supports the RGB color model. Red, Green, Blue are the primary color components of the RGB color space. All the other color can be obtained by using additive color mixing of different RGB color components. The intensity of the primary color can be defined as the grey level in the grey-scale palette. A primary color will have an intensity range between 0 and 1, with 0 representing black and 1 representing the maximum possible intensity of that color. The RGB color palette is created from the grey-scale palette, which represents the intensity palette 1for red, green, and blue. In real color system R,G,B are each represented by 8 bits, and therefore each single color based on R,G,B can represent 0-255 variations of scale.

2. Literature Survey

A) Shamir's Secret Sharing Scheme [3]

Shamir secret sharing scheme is explained in [4].Shamir developed the idea of a (k, n) threshold-based secret sharing technique (k <= n). The technique is to construct a polynomial function of order (k - 1) as,

$$\mathbf{f(x) = d_0 + d_1x + d_2x^2 + \ldots\ldots + d_{(k-1)}x^{(k-1)} (mod\ p)}$$

Where the value d_0 is the secret and p is a prime number.

Algorithm 1: (k, n)-threshold secret sharing

Input: Take secret d_0 in the form of an integer, n is number of participants and threshold is $k \leq n$.

Output: n shares are created in the form of an integer for the n participants to keep.

Step1: Choose a random prime number p larger than d_0.
Step2: select k-1 integer values $d_1, d_2 \ldots d_{k-1}$ range of 0 through p-1.
Step3: Select n distinct real values $x_1, x_2 \ldots x_n$
Step 4: Use the following (k-1) degree polynomial to compute n function values $f(x_j)$, For j=1, 2… n

$$F(x_j) = d_0 + d_1x_j + d_2x_j^2 + \ldots + d_{(k-1)}\, x_j^{(k-1)} \pmod p \quad \ldots\ldots..(1)$$

Step5: Deliver the secret shares as pairs of values $(x_i, f(x_i))$, $1<=i<=n$ and $0 < x1 < x2 \ldots < x_n < p-1$.

The polynomial function $f(x_i)$ is destroyed after each server Pi possesses a pair of values $(x_i, f(x_i))$ so that no single server knows what the secret value d_0 is. The following describes the equation for solving the process of secret recovery.

Algorithm 2: Secret recovery of shares

Input: Select k shares from the n participants and the prime number p with both k and p

Output: Secret d_0 is hidden in the shares and coefficients d_i used in (1) where i=1, 2, 3 … d- 1.

Step1: Use the k shares $(x_1, f(x_1))$, $(x_2, f(x_2))\ldots (x_k, f(x_k))$ to set up

$$F(x_j) = d_0 + d_1x_j + d_2x_j^2 + \ldots\ldots + d_{(k-1)}\, x_j^{(k-1)} \pmod p \quad \ldots..(2)$$

Step2: Lagrange interpolation formula [6] is commonly used to solve the secret value d_0.Solve the k equations by Lagrange's interpolation to obtain k as follows.

$$d0 = \sum_{i=0}^{k} \left(\prod_{\substack{j=1 \\ j \neq i}}^{k} \frac{-xj}{xi - xj} \right) f(xi)(mod\ p)$$

B) Thien and Lin's Image Secret Sharing Scheme [4]

Thien and Lin proposed a (k, n) threshold-based image SSS by cleverly using Shamir's SSS to generate image shares. The essential idea is to use a polynomial

function of order (k - 1) to construct n image shares from an l x l pixels secret image (denoted as I) as,

$$S_x(i,j) = I(i_k + 1,j) + I(i_k + 2, j)\, x \ldots\ldots + I(i_k + k, j)\, x_{k-1} \pmod p$$

where $0 \le I \le (l/k)$ and $1 \le j \le l$

This method reduces the size of image shares to become 1/k of the size of the secret image. Any k image shares are able to reconstruct every pixel value in the secret image.

An example of (2, 4) image secret share construction process is illustrated in Figure 1 where k = 2 and n = 4. According to the technique, a first order polynomial function can be created as

$$Sx\,(i,j) = (110 + 112x) \pmod{251}$$

Where 110 and 112 are the first two pixel values in the Lena image. For our four participants, we can randomly pick four x values, and substitute them into the polynomial function by setting p value to be 251 which is the largest prime number less than 255 which is maximum grey image value.

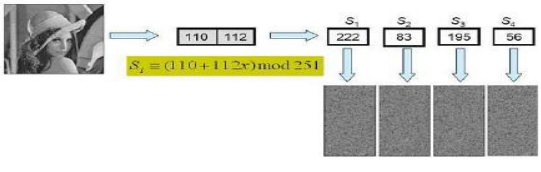


Fig. Secret sharing process for Lena image

Four shares are computed as (1, 222), (2, 83), (3, 195) and (4, 56). They become the first pixel in four image shares. The second pixel is computed in the same manner by constructing another first order polynomial function using next two pixels in the Lena image. This process continues until all pixels are encoded. Four image shares are the bottom right images shown in Figure 1, and the size of each image share is half (1/2) size of the original image. None of the image shares appear to reveal information about the secret image. However, the pixel values in a natural image are not random because the neighbouring pixels often have equal or close values. It is evident that the first two pixel values (110 and 112) are very close to each other. That creates the possibility that one image secret share may be used to recover the secret image by assuming the neighbouring pixels have the same values in the first order polynomial function.

C) XOR secret sharing scheme [5]

The (n,n) threshold scheme which can be constructed based on XOR operation have no pixel expansion and the time complexity for constructing shared image is O(k1,n),where k1 is size of shared image and this time complexity is excluding time needed for generating n distinct random matrices. This scheme also provides perfect secrecy. XOR color secret sharing scheme supports the RGB color model.

Assume that 0, 1…c is the set of all color appearing in an original image. Where $c \ge 2$ is the maximum color value of a color images.

$A = [a_{ij}]_{m*n}$ Where $a_{ij} \in \{0 \ldots c\text{-}1\}$, (i=1, 2….m and j=1… n)

Consider matrix A and matrix B and perform XOR and AND operation of matrices by using the following formula,

$\forall a_{ij} \in A$, $bij \in B$, A_{ij}

$C = A \oplus B = [a_{ij} \oplus b_{bij}]$ (i =1, 2… m; j=1….n)

$D = A \,\&\, B = [aij \& b_{ij}]$ (i =1, 2… m; j=1….n)

To express the model conveniently some assumptions were made which are as follows,

Assumption 1: The pixel matrix of secret image A is equal to secret image A.

Assumption 2: The matrix of secret image is $m \times n$, $Ai1 \ldots\ldots A_{in}$ are used to denote n distinct matrices of $A_1 \ldots\ldots A_n$ for convenience ($n \ge 2$).

If $n \ge 2$, then there must be n distinct matrices $A_1 \ldots\ldots A_n$ satisfying the following conditions:

$$\bigcup_{j=1}^{n-1}(\oplus \text{Aij}) \neq A$$

It means the XOR of any n-1 matrices cannot be used to obtain any information of matrix A.

$$\bigcup_{j=1}^{n}(\oplus \text{Aij}) = A$$

It indicates that only the XOR of n matrices can be used to recover information from matrix A.

D) Lie Bai's Matrix Projection scheme [6]

In this scheme the secret image will get divided into n image shares such that: i) any k image shares (k <=n) can be used to reconstruct the secret image in lossless manner and ii) any (k-1) or fewer image shares cannot get sufficient information to reveal the secret image. Here, we briefly describe the procedure in two phases:

Construction of Secret Shares from secret matrix S

i) Construct a random matrix A of size m x k of rank k where m>2(k-1)-1
ii) Choose n vectors of size (k x 1) where any k vectors are linear independent
iii) Calculate shares $v_i=(A \times x_i) \pmod p$ for $1 \le i \le n$
iv) Compute projection matrix
v) $\$ =(A(A^TA)^{-1}A^T) \pmod p$
vi) Solve remainder matrix $R=(S- \$) \pmod p$
vii) Destroy matrix A, x_i, S, $
viii) Distribute n shares v_i to n participants and make matrix R publicly known

Secret Reconstruction

i) Collect k shares from any k participants, say the shares are $v_1, v_2, \ldots, v_k$ and construct a matrix $B=[v_1\ v_2 \ldots v_k]$

ii) Calculate the projection matrix
$\$ = (B(B^TB)^{-1}B^T) \pmod p$

iii) Compute the secret $S=(\$ + R) \pmod p$

3. Comparative Analysis

In above section, we have studied different image secret sharing schemes. Comparative analysis of these schemes is done based on certain parameters like ideal, perfect, accuracy, image share size etc.

Schemes / Parameters	Shamir's scheme	Thien and Lin's scheme	XOR Scheme	Lie Bai scheme
Ideal	Yes	Yes	Yes	Yes
Perfect	Yes	No	Yes	Yes
Threshold scheme	Yes	Yes	No	Yes
Threshold Type	(k,n)	(k,n)	(2,2)	(k,n)
Share size	Same	1/k	Same	1/m
Secret Sharing	Single	Single	Single	Multiple
Secret sharing Based on	Polynomial	Polynomial	polynomial	Matrix Projection
Proactive	No	No	No	Yes
Accuracy	More	Less	Less	More
Image Type	NA	Grey	Grey	Color

Above table shows that Lie Bai's Matrix projection method is more efficient and secure on the basis of parameters like accuracy, proactiveness and share size. Also this scheme is an applicable for sharing multiple secrets.

Also the various extended capabilities [9] [10] are required in secret sharing schemes as per the need of an application.

4. Conclusion

In this paper several secret sharing schemes like Shamir's secret sharing scheme, Thien Lin's secret sharing scheme, XOR secret sharing scheme, Lie Bai's secret sharing scheme are discussed. Table 1 gives the Comparison of these schemes based on different

parameters like ideal, perfect, threshold based scheme, image type, image size, accuracy etc. This analysis shows that Lie Bai's method of matrix projection is **better** secret sharing method for images.

5. References

[1]D. R. Stinson, "Cryptography: Theory and Practice", CRC Press, Boca Raton 1995.Menezes, A., P. Van Oorschot, and S. Vanstone, Handbook of Applied Cryptography,CRC Press, 1996, pp. 524-528.

[2]http://www.colorimageprocessing.com/research_secureimaging2.htm

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

[4]Thien and Lin,"Secret image sharing", Computers &Graphics, vol. 26, no.5, pp. 765-770, 2002

[5] Wang Dao-Shun, ZangLei, MaNing"Secret color images sharing schemes based on XOR operation", 2013

[6] Lie Bai "A Reliable (k, n) Image Secret Sharing Scheme", 9th International Conference on Information Fusion, Sponsored by the International Society of Information Fusion (ISIF), Aerospace &Electronic Systems Society (AES), IEEE,2006

[7] Kai Wang, XukaiZou and Yan Sui,"A Multiple Secret Sharing Scheme based Matrix Projection", 33rd Annual IEEE

[8] E. D. Karnin, J.W. Greene, and M. E. Hellman, "On secret sharing systems," vol. IT-29,no. 1, pp. 35-41, Jan. 1983.

[9] Sonali Patil and Prashant Deshmukh, "An Explication of Multifarious Secret Sharing Schemes", *International Journal of Computer Applications* 46(19):5-10, May 2012.

[10] Sonali Patil and Prashant Deshmukh, "*Analysing Relation* in Application *Semantics* and Extended Capabilities for *Secret Sharing* Schemes", *International Journal of Computer Science and Issues Volume 9, Issue 3, No. 1,* 2012, 1694-0814