ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

Enhancing Security in Secret Sharing with Embedding of Shares in Cover Images

Sonali Patil[1], Prashant Deshmukh[2]

Research Scholar, Computer Department, SIPNA, Amravati, India[1]

Professor, Computer Department, SIPNA, Amravati, India[2]

Abstract: A method is presented here in which a secret image is shared into n image shares using (k, n) threshold secret sharing. Further each image share is embedded in cover image. The original image can be reconstructed by applying reverse of the same embedding technique to obtain image shares from embedded cover images and by applying reverse of the same secret sharing scheme on at least k shares where k ≤ n. This technique uses highly reduced share size secret sharing and simple embedding technique. This technique enhances the security as created shares get embedded in cover images which help in not attracting attacker's attention. Experimental results proves the reduced image share size, increased security, less computational complexity and increased peak signal to noise ratio (PSNR).

Keywords: Secret sharing; Embedding, Matrix Projection; Steganography; Information Security; Network Security

I. INTRODUCTION

The general idea behind "secret sharing" [1] 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. These created shares look meaningless. Observing these image shares the attackers can attract towards it. Embedding [2] is a technique to hide the important data in cover-image. So by embedding created image shares into an ordinary cover images security gets added. Secret image sharing schemes and image hiding schemes have developed by many researchers over years. Some researchers have been integrating image sharing technique and image hiding technique with the purpose of hiding secret images and authentication. For security while transmission of image shares, embedding is needed in the worldwide computer network environment.

If highly reduced share size schemes are used to embed created image shares into cover images less data hiding capacity technique can also be very useful. The proposed method explores the combination of a highly reduced share size matrix projection secret sharing scheme [3] with less complex least significant bit (LSB) [4] embedding technique. The rest of the paper is organized as follows. Section II describes the literature survey for image secret sharing and embedding schemes. Section III describes the proposed scheme. Section IV shows the experimental results of proposed scheme. Section V presents the comparative study of implemented scheme with few existing schemes. Finally section VI concludes about the proposed scheme.

II. LITERATURE SURVEY

A. Secret Sharing

1. Shamir's Secret Sharing:

Shamir [5] developed the idea of a (k, n) threshold-based secret sharing technique (k ≤ n). The technique allows a polynomial function of order (k −1) constructed as, $f(x) = d_0 + d_1x_1 + d_2x_2 + \ldots + d_{k-1}x_{k-1} \pmod p$, 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 $y_i = f(x_i)$, $1 \le i \le n$ and $0 < x_1 < x_2 \ldots < x_n \le p - 1$.

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 k − 1 or fewer secret shares can discover the secret d_0.

On the other hand, when k or more secret shares are available, then we may set at least k 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.

The unique solution to these equations shows that k participants can compute the secret value d_0 by using following Lagrange interpolation.

$$f(x) = \sum_{j=1}^{k} \left(y_{i_j} \prod_{1<-t<-k, t \neq j} \frac{x - x_{i_t}}{x_{i_j} - x_{i_t}} \right) mod\ p$$

But it can be simplified, because the participants do not need to the whole polynomial f(x). It is sufficient to reduce it to constant term d_0. Shamir's SSS is regarded as a PSS scheme because knowing even (k − 1) linear equations doesn't expose any information about the secret. The share size is same as secret size.

2. Thien and Lin [6] Shamir's Secret Sharing:

Thein and Lin proposed a (k, n) threshold-based image SSS by cleverly using Shamir's SSS [5] 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 ×l pixels secret image (denoted as I) as, $S_x(i, j) = I(ik + 1, j) + I(ik + 2, j)\, x \ldots + I(ik + k, j)\, x^{k-1} \pmod p$.

Where $0 \le i \le \lfloor l / k \rfloor$ and $1 \le j \le l$. This method reduces the size of image shares to become 1/k of the size of the

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

secret image. Any k image shares are able to reconstruct every pixel value in the secret image. Thien and Lin also provided some research insights for loss less image recovery using their technique.

A secret image can be possibly recovered from less than k image shares because neighboring pixels are highly correlated. To address these security issues, Thien and Lin suggested an idea by per mutating the order of pixels (with a permutation key) in the secret image before the image shares are computed. Conversely, the secret image can still be reconstructed from any k image shares by solving the permutated image and applying inverse-permutation using the permutation key.

Nevertheless, the permutation key becomes the single-point-failure in the system because the key can get lost or corrupted. This scheme also prevents real-time processing because the permuted image has to be obtained before the secret image can be reconstructed.

Thien and Lin's method reduces the size of image shares to become 1/k of the size of the secret image.

III. MATRIX PROJECTION SECRET SHARING

Li Bai [3] proposed a secret sharing scheme based on matrix projection. The scheme uses invariance property of matrix projection to create the shares of the secret image. The technique allows a colored secret image to be divided as n image shares so that: i) any k image shares where $k \leq n$ are sufficient to reconstruct the secret image in the loss less manner and ii) any (k - 1) or fewer image shares cannot get enough information to reveal the secret image. It is an effective, reliable and secure method to prevent the secret image from being lost, stolen or corrupted. In comparison with other image secret sharing methods, this approach's advantages are its large compression rate on the size of the image shares, its strong protection of the secret image and its ability for the real time processing.

Let A be an m× k matrix of rank k ($m \geq k > 0$), and

$\$ = A(A'A)^{-1}A'$,

where $(\cdot)'$ is the transpose of a matrix. The m × m matrix \$ is the projection matrix of matrix A, \$= proj(A)

We can also compute vectors v_i using k linearly independent k×1 vectors xi, $v_i = Ax_i$ where $1 \leq i \leq k$. These $m\times 1$ vectors v_i can be placed in $B = [v_1\ v_2 \ldots v_k]$.

The invariance theorem shows \$ = proj (A) = proj (B).

For an l × l secret image with intensity level as I (i, j)

where $1 \leq i, j \leq l$, partition the secret image I as non-overlapped m × m blocks ($m > 2(k-1)-1$) for each RGB color. This produces roughly $(\lceil l/m \rceil)^2$ blocks.

Following steps describes the algorithm for embedding:

Construction of Secret Shares from Secret Matrix S

1. Construct a random m × k matrix A of rank k where $m > 2(k - 1) – 1$.
2. Choose n linearly independent k×1 random vectors xi.
3. Calculate share vi = (A×xi) (mod p) for $1\leq i \leq n$, where p is a prime number.
4. Compute \$ = (A (A'A)-1A') (mod p).
5. Solve R = (S - \$) (mod p).
6. Destroy matrix A, xi's, \$, S, and
7. Distribute n shares vi to n participants and make matrix R publicly known.

Secret Reconstruction

1. Collect k shares from any k participants, say the shares are $v_1, v_2, \ldots, v_k$ and construct a matrix $B = [v_1\ v_2 \ldots v_k]$.
2. Calculate the projection matrix $\$ = (B\ (B'B)^{-1}B')$ (mod p).
3. Compute the secret S = (\$ + R (mod p)).

The share size is reduced to 1/m of original secret image.

B. Embedding

In recent years, several information hiding techniques have been proposed. Most of these techniques use image data (cover image) as a container, for hiding the confidential information. The simplest and most common type of embedding technique is least significant bit (LSB) [4]. The one's bit of a byte is used to encode the hidden information. It uses the least significant bits of the image data (cover image) to hide the confidential information. Other programs embed the confidential information in a specific band of the spatial frequency component of the carrier. This is most popular technique when dealing with images. The key idea to this approach is to replace least significant bits with the message to be encoded.

Suppose we want to encode the letter A (ASCII 65 or binary 01000001) in the following 8 bytes of a carrier file.

01011101	11010000	00011100	10101100
11100111	10000111	01101011	11100011

Becomes

0101110<u>0</u>	1101000<u>1</u>	0001110<u>0</u>	1010110<u>0</u>
1110011<u>0</u>	1000011<u>0</u>	0110101<u>0</u>	1110000<u>1</u>

This embedding method has relatively small information hiding capacity and allows only 5-15% of the cover image to hide information. But this capacity is sufficient for highly reduced size shares.

C. Sharing and Embedding

Very few researchers have proposed the combination of secret image sharing and hiding techniques. These techniques give higher reliability and security at the same time compared to only sharing or only hiding techniques.

In [7] the secret sharing with embedding schemes are analyzed.

Chin-Chen Chang and Duc Kieu [8] have proposed a novel secret sharing and information-hiding scheme for grayscale images by embedding a secret image and a secret bit stream into two shadow images. It has limited reliability and shadow image size is more.

Y.S. Wu, C.C. Thien, and J.C. Lin [9] have proposed sharing and hiding of secret images but with size constraint. Sonali Patil [10] proposed secure (2, 2) binary secret sharing with embedding of shares in cover images.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

The scheme is not reliable as both the shares are required or reconstruction.

The next section describes the proposed combination technique of matrix projection secret sharing with LSB embedding method.

IV. PROPOSED SCHEME

The proposed method is a gets divided into 2 phases (a) Construction of secret image shares and embedding shares in cover images and (b) Reconstruction of original secret image.

I. CONSTRUCTION OF SECRET IMAGE SHARES AND EMBEDDING OF SHARES IN COVER IMAGES

The proposed method involves a "transmitter" and many "receivers". The transmitter chooses a secret image and applies matrix projection [3] secret sharing scheme on it to obtain the corresponding image shares.

Every share is `individually embedded into cover image using least significant bit [4] method.

The share generation and embedding of shares in cover images is shown in figure 1.

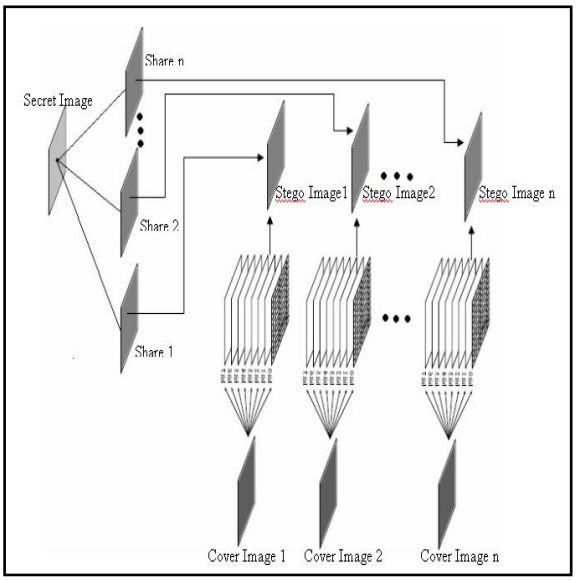

Fig. 1Construction of shares and embedding of Image Shares

As the created share image size is very less with LSB embedding method the shares can easily gets embedded in cover images.

Then the transmitter electronically transmits the images with embedded data (stego images) to the receivers.

II. RECONSTRUCTION OF ORIGINAL SECRET IMAGE

To reconstruct the secret image minimum k shares are required. The inverse operations of the embedding are above procedures construction of secret image shares and embedding is required.

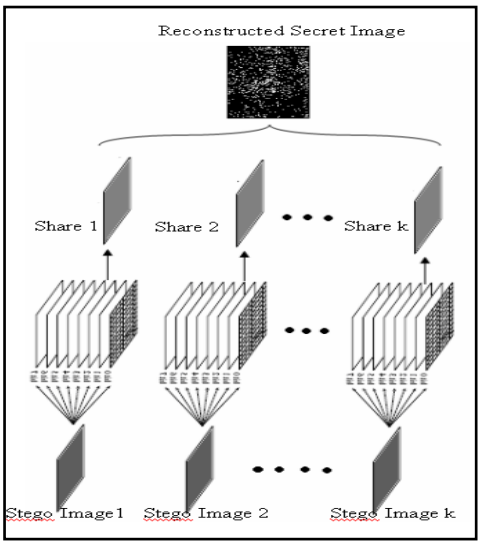

Fig. 2. Reconstruction of Secret Image

III. EXPERIMENTAL RESULTS

This section shows the implementation results of the proposed scheme for combination of *(2, 4)* threshold matrix projection secret sharing scheme with embedding by Least Significant embedding method.

The following figure 3 shows the original secret *Leena image* and created shares for the participants.

Fig. 3 Original Secret Image and Highly Reduced Share Size Shares

Fig. 4 Reconstructed Secret Image

Fig. 5 Stego Images

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

The next section shows the comparative study of the proposed scheme with the existing schemes.

IV. COMPARATIVE STUDY

This section describes the comparative results based on share size and peak signal to noise ratio (PSNR) for the proposed scheme with existing technique.

Table I shows the comparative results of Visual Cryptography schemes with reliable secret sharing method with respect to share size.

TABLE I COMPARISONS BETWEEN VC[11] AND MATRIX PROJECTION [3]

Share Image Size	Using Shamir's Method (2,4)							Using Matrix Projection Secret Sharing (2, 4)
	1	2	3	4	5	6	7	
Leena.jpg 512x512	512× 512	512× 512	1024× 1024	512× 512	512× 512	512× 512	512× 512	512x1
Baboon.jpg 256x256	256× 256	256× 256	512× 512	256× 256	256× 256	256× 256	256× 256	256x1
Hey.jpg 90x90	90× 90	90× 90	180× 180	90× 180	90× 180	90× 180	90× 180	90x1

Table II shows the results of PSNR. The result shows how the present method gives better results than the other ones. The hiding shares in cover images extending the capability of secret sharing scheme. The need of extended capabilities [12] [13] and possible applications [14] can use the proposed scheme.

TABLE 2. COMPARATIVE PSNR RESULTS OF VC [11] AND MATRIX PROJECTION [3]

PSNR Results *	Using Shamir's Method (2,4)							Using Matrix Projection Secret Sharing (2, 4)
	1	2	3	4	5	6	7	
Leena.jpg 512x512	343.48	315.27	375.33	310.43	389.77	255.12	237.65	INF
Baboon.jpg 256x256	398.34	453.65	471.37	445.76	412.87	411.67	357.81	INF

*PSNR: PEAK SIGNAL TO NOISE RATIO

V. CONCLUSION

Here a combination of highly reduced share size secret sharing and simple embedding scheme is proposed. The proposed scheme provides high security as original secret image is divided into image shares and each one of which is embedded in ordinary cover image making it least susceptible to attackers. Even if attackers are aware it is not possible to reconstruct original image with less than k image shares. The experimental results proves the reduced image share size, increased security, less computational complexity and increased peak signal to noise ratio (PSNR).

REFERENCES

[1] D. R. Stinson, "Cryptography: Theory and Practice", CRC Press, Boca Raton, 1995.
[2] Miroslav Goljan, et al., "Distortion-Free Data Embedding for Images", Proc. 4th Information Hiding Workshop, Pittsburgh, Pennsylvania, 2001.
[3] 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.
[4] J. Fridrich, et al., "Steganalysis of LSB Encoding in Color Images", ICME, New York, July 2000.
[5] Shamir A., "How to Share a Secret", Communications of the ACM, vol. 22, no.11, pp. 612–613, 1979.
[6] C.-C. Thien and J.-C. Lin, (2002), "Secret image sharing," Computers & Graphics, vol. 26, no. 5, pp. 765–770, Elsevier Science Ltd.
[7] Sonali Patil, Janhavi Sirdeshpande, Kapil Tajane, (2013), "Analysing Secure Image Secret Sharing Schemes Based on Steganography", International journal of Computer Engineering & Technology (IJCET), Vol. 4, Issue 2, pp. 172-178.
[8] Chin-Chen Chang, The Duc Kieu, (2006), "Secret Sharing and Information Hiding by Shadow Images".
[9] Y. S. Wu, et at., (2004), "Sharing and hiding secret images with size constraint," Pattern Recognition, vol. 37, no. 7, pp. 1277–1385.
[10] Sonali Patil et al.(2013), "Secure and Verifiable (2, 2) Secret Sharing Scheme for Binary Images", International Journal of Computer Science Issues (IJCSI), Vol. 10 Issue 1, pp 290-293.
[11] M. Naor, A. Shamir, (1994), "Visual cryptography", Proc. Eurocrypt '94, Lecture Notes Computer Sci., Vol. 950, pp.1-12.
[12] Sonali Patil, Prashant Deshmukh, (2012), "Analyzing Relation in Application Semantics and Extended Capabilities for Secret Sharing Schemes", International Journal of Computer Science Issues (IJCSI);May2012, Vol. 9 Issue 3, p219.
[13] Sonali Patil and Prashant Deshmukh, (2012), "An Explication of Multifarious Secret Sharing Schemes", International Journal of Computer Applications 46(19):5-10, pp. 6-10.
[14] Iftene, S, (2007), "Secret sharing schemes with applications in security protocols", Technical paper, University Alexandru Ioan Cuza of Ia¸si, Faculty of Computer Science.

PSNR Results *	Using Shamir's Method (2,4)							Using Matrix Projection Secret Sharing (2, 4)
	1	2	3	4	5	6	7	
Leena.jpg 512x512	343.48	315.27	375.33	310.43	389.77	255.12	237.65	INF
Baboon.jpg 256x256	398.34	453.65	471.37	445.76	412.87	411.67	357.81	INF