Secure and Verifiable (2, 2) Secret Sharing Scheme for Binary Images

Sonali Patil[1], Sandip Sathe[2], Pravin Mehetre[3], Deepak Shinde[4], Kiran Bhalerao[5], Pawankumar Pandey[6]

[1] Assistant Professor, Computer Department, Pimpri Chinchwad Colege of Engineering, Pune, Maharashtra, India

[2] Student, Computer Department, Pimpri Chinchwad Colege of Engineering, Pune, Maharashtra, India

[3] Student, Computer Department, Pimpri Chinchwad Colege of Engineering, Pune, Maharashtra, India

[4] Student, Computer Department, Pimpri Chinchwad Colege of Engineering, Pune, Maharashtra, India

[5] Student, Computer Department, Pimpri Chinchwad Colege of Engineering, Pune, Maharashtra, India

[6] Student, Computer Department, Pimpri Chinchwad Colege of Engineering, Pune, Maharashtra, India

Abstract

Visual Cryptography is a technique in which a secret is encrypted into several image shares and then decrypted later using a human visual system to stack all the share images. Conventional visual cryptography methods divide a secret image into n shares (shadows) and distribute these shares to n participants. But in network while transmission the shadows can be changed by attackers or damaged. To remedy such kind of vulnerabilities verifiability of shadows can be a solution. Watermarking can add verifiability to secret sharing, but the shadows are meaningless which can attract the attacker's attention. The proposed scheme embeds created shadows in cover images which make them more secure. In this paper we have explained how a low computational complexity visual secret sharing scheme is verifiable and more secure by combining Watermarking and Steganography.

Keywords: *Network Security, Visual Cryptography, Secret Sharing, Verifiable Secret Sharing, Steganography.*

1. Introduction

Secure transmission of data is more and more needed in the worldwide computer network environment. The effective and secure protections of sensitive information are primary concerns where only encrypting data is not a solution. Secret Sharing Schemes refers to method for distributing a secret amongst a group of participants, each of whom is allocated a share of the secret. The secret can be reconstructed only when a sufficient number of shares are combined together; individual shares are of no use on their own. Shamir [1] introduced a secret sharing in 1979. Visual cryptography (VC) is a secret-sharing scheme that uses the human visual system to perform the computations. Naor and Shamir [2] introduced Visual Cryptography (VC) in 1994.

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. Chin-Chen Chang and Duc Kieu [3] have proposed a novel secret sharing and information-hiding scheme 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 [4] have proposed sharing and hiding of secret images but with size constraint. Here in proposed scheme each shadow is individually embedded into cover image using BPCS (Bit Plane Complexity Segmentation) [5] method. Wang's [6] verifiable secret sharing method is used to create the shares/shadows for binary images.

2. Review

2.1 Review of Shamir's [1] Secret Sharing Scheme

Shamir developed the idea of a (k, n) threshold-based secret sharing technique ($k \leq n$). 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 [1].
Shamir's SSS is regarded as a perfect secret sharing scheme because knowing even $(k - 1)$ linear equations doesn't expose any information about the secret.

2.2 Review of Image Embedding Schemes

Image embedding hides a secret message in a cover image, this process is usually parameterized by a hide-key, and the detection or reading of embedded information is possible only by having this key.

2.2.1 Least Significant Bit Insertion [7]

In this method the secret message is embedded into the least significant bit plane of the image. Since this only affects each pixel by +/- 1, if at all, it is generally assumed with good reason that the degradation caused by this embedding process would be perceptually transparent. Hence there are a number of LSB based Steganography techniques available in the public domain. The problem with this method is that it does not provide protection against small changes resulting from lossy compression or image transformations. The other disadvantage of this method is that it is having very less data hiding capacity. Therefore, improvements as suggested by R. J. Anderson and F. A. P. Petitcolas [8] are urged for LSB.

2.2.2 Adaptive MELSBR Method [9]

To avoid changing the properties of cover-images, the message must be embedded in "random texture" areas of each bit-plane. For taking advantage of local characteristics, an adaptive Steganography method based on the Minimum Error LSB Replacement (MELSBR) method is proposed. First, the upper bound of embedding capacity for each pixel in the cover-image is evaluated. If the amount of message to be embedded is less than the total embedding capacity provided by the cover-image, whole secret message will be embed in a local area and it can be easier for the attacker to extract the secret. To treat this scattering method is provided.

3. Proposed Method

The proposed method is based on verifiable (2, 2) secret sharing for binary images proposed by Wang [6]. Wang used watermarking for verifiability of shares as well as reconstructed secret. The receiver end receives the share and then extract watermark image from the original image. If watermark image is same as what is sent by sender, the received secret image is verified. But in network the created meaningless shadows can attract attacker's attraction. In proposed method BPCS Steganography is added to make those meaningless created shadows in meaningful images which add more security to the scheme.

BPCS Steganography:

Suggested technique to embed secret data into a dummy cover image is based on BPCS. The key idea to this approach is that a binary image can be categorized as "informative" and "noise-like" regions, which are segmented by a "complexity measure". If the embedding data is noise-like, we can hide it in the noise-like region of the dummy image. If a part of embedding data is simple, then we apply "image conjugate" operation to it. This operation transforms a simple pattern into a complex pattern.
Following steps describes the algorithm for embedding:

a. Segment each bit-plane of the cover image into informative and noise-like regions by using a threshold value (α). A typical value is $\alpha = 0.3$.
b. Group the bytes of the secret file into a series of secret blocks.
c. If a block (S) is less complex than the threshold (α), then conjugate it to make it a more complex block (S*). The conjugated block must be more complex than α.
d. Embed each shadow image block into the noise-like regions of the bit-planes (or, replace all the noise-like regions with a series of secret blocks). If the block is conjugated, then record this fact in a "conjugation map."
e. Also embed the conjugation map as was done with the secret blocks.

When the stego image is ready for transmission it is transmitted over the network. This transmission is more secure and reliable in comparison to any other technique.
The proposed scheme is divided into 2 parts as follows:

Construction Phase and Reconstruction Phase

The flowcharts for construction phase and reconstruction phase are given below:

Construction phase

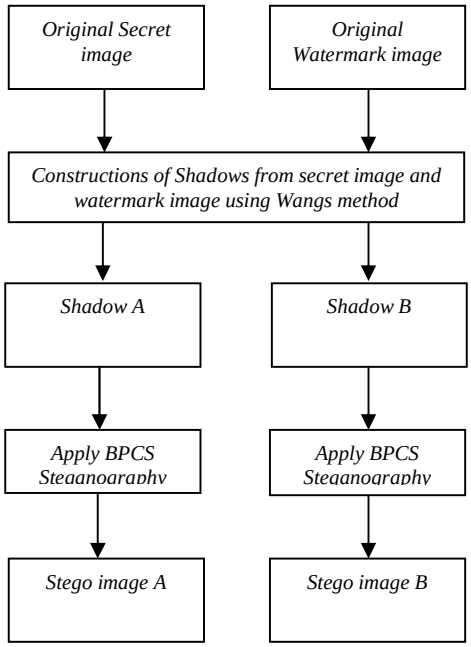

Fig. 1. Construction of secret image

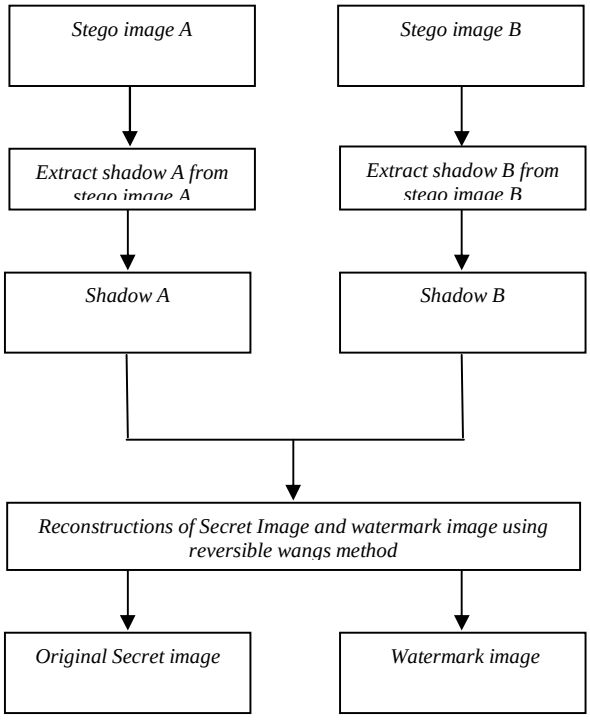

Fig. 2. Reconstruction of secret image

4. Experimental Results

The experimental results are produced to compare used BPCS Steganography with LSB method.

Table 1. Comparison Between LSB and BPCS Steganography methods

Cover Image	Share Image	Using LSB		Using BPCS	
		PSNR in db	DHC in %	PSNR in db	DHC in %
Brain.bmp 128×128	Share1.bmp 32×32	103.26	12.5	121.47	52.6
Baboon.bmp 512×512	Share2.bmp 32×32	97.23	12.5	117.83	57.13

PSNR: *Peak to Signal Noise Ratio* ***DHC:*** *Data Hiding Capacity*

5. Conclusion

By adding embedding in verifiable secret sharing a more secure secret sharing for binary images is obtained. The used embedding method provides high PSNR and also the data hiding capacity is more. The experimental results shows that the scheme is secure, verifiable and with low computation complexity. In future the proposed secret sharing scheme can be extended to color images and (2, 2) secret sharing can be extended to threshold (t, n) secret sharing scheme.

References

[1] Shamir, How to share a secret, Communications of the Association for Computing Machinery, vol. 22, no. 11, pp. 612-613, 1979.
[2] M. Naor and A. Shamir, Visual cryptography, Lecture Notes Computer Science, vol. 50, pp. 1-12, 1995.
[3] Chin-Chen Chang, The Duc Kieu "Secret Sharing and Information Hiding by Shadow Images", 2006.
[4] C.Thien, and J. C. Lin, Secret Image Sharing, Computers and Graphics, vol. 26, no. 1, pp. 765-770,2002.
[5] Michiharu Nimmi, Hideki Noda and Eiji Kawaguch, An image embedding in image by a complexity based region segmentation method, Proceedings of the 1997 International Conference on Image Processing (ICIP '97).
[6] Zhi-hui Wang, Chin-Chen Chang, Huynh Ngoc Tu, Ming-Chu Li, Sharing a Secret Image in Binary Images with Verification, Volume 2, Number 1, January 2011.
[7] N.F. Johnson, Z. Duric, and S. Jajodia, "Information hiding: Steganography and watermarking- attacks and countermeasures", Kluwer Academic Publishers, 2000.
[8] R. J. Anderson and F. A. P. Petitcolas, "On the limits of steganography," IEEE J. Select. Areas Commun, vol. 16, no. 4, pp. 474–481, May 1998.