Image Secret Sharing in Stego-Images with Authentication

Amitava Nag[1], Sushanta Biswas[2], Debasree Sarkar[2], and Partha Pratim Sarkar[2]

[1] Academy of Technology
West Bengal University of Technology
Hoogly 721212 - India
amitavanag.09@gmail.com
[2] Département of Engineering and Technological Studies
University of Kalyani
Kalyani 741 235 – India
ppsarkar@klyuniv.ac.in

Abstract. Recently, a polynomial-based (t,n) image sharing and hiding schemes with authentication was proposed to hid n shares of a secret image into n ordinary cover images and form n stego-images that can be transmitted securely. But each stego-image of all existing method should be expanded to 4 times of the secret image. In this paper we propose an enhanced scheme, where the size of the stego-image is reduced to $\frac{4(2n-t)}{n^2}$ times of the secret image. In addition our proposed scheme provides better authentication using hash function.

Keywords: Secret sharing, stego-image, authentication, hash function.

1 Introduction

With the rapid growth of Internet technologies as communication channel, digital media can be transmitted conveniently. But Internet is an open system; therefore, how to protect secret messages during transmission becomes an important issue. Two methods, cryptography and steganography have been used to protect secure data from malicious users on the internet. Cryptography transforms a secret data into disordered and meaningless form, which make suspicious enough to attract malicious users during transmission on the internet. The other method steganography is used to provide secure transmission by hiding a secret data into a cover media to generate gtego-media. Thus by steganography the observation of the existence of the embedded secret can be avoided. However, the weak point of steganography is that a secret message is protected in a single media carrier. Thus both cryptography and steganography are Single Point of Failure (SPOF) type as they use single storage mechanism. To overcome the weakness of Single Point of Failure (SPOF), several secret sharing techniques [1],[2],[3],[4],[5] have been proposed. It is a technique of protecting secret data like images by dividing secret data into n pieces (each piece is known as shadow share) and distributes the shares among a group of participants.

K. Singh, A.K. Awasthi, and R. Mishra (Eds.): QSHINE 2013, LNICST 115, pp. 764–770, 2013.

A secret sharing scheme is called a (t, n) threshold secret sharing scheme for $t \leq n$ if the following two conditions are satisfied: i) knowledge of any t or more shares can reconstruct the original secret; ii) knowledge of any t - 1 or less shares cannot recover the original secret. However, the shadow images produced by secret image sharing are noise-like, which may cause attacker's attention. From the view point of secure transmission, it is better if a (t,n) secret sharing and steganography are combined, where shadow images are embedded into cover images to form the stego-images. Moreover if authentication technique is added to detect integrity of shadow images, this scheme is called steganography and authentication based secret sharing. Some steganography and authentication based (t,n) secret sharing techniques were proposed in [6-9].

In [6], Lin and Tsai proposed a (t,n) secret sharing techniques with steganography and authentication to prevent fake stego-images. However, the authentication technique is too weak. Yang et al. [7] proposed an improved scheme that avoided Lin-Tsai's authentication weakness by hash function with secret key. But Yang et al's evaluate hash value for each pixel separately which lead a high computational cost of the authentication process. In [8], Chang et al. proposed sharing techniques with steganography and authentication scheme, where the concept of Chinese remainder theorem (CRT) is used to improve authentication ability. Eslami et al. in [9] proposed another method of secret sharing using cellular automata, where the author used double authentication to reduce the number of authentication bits. Main drawback of this method is that if all bits in stego-blocks are changed and the same eight shared bits are maintained, then tampere stego-blocks can not be located at receiver side. All these methods [6],[7],[8],[9] suffer from the problem that the size of the stego image is four times of the secret image. In this paper the size of cover images are reduced to $\frac{4(2n-t)}{n^2}$.

2 Related Work

We have already highlighted several (t,n) threshold-based Secret Sharing(SS) and (t, n)-based secret sharing in stego-images with authentication schemes. In this section we briefly describe one Secret Sharing and one secret sharing in stego-images with authentication schemes.

2.1 Lin and Wang's (k,n) Secret Image Sharing

In 2010, Lin and Wnag proposed a scalable (k,n) $2 \leq t \leq n$ secret image sharing scheme[5]. Their share generation process involves three steps:

Step 1. The secret image G is partitioned into n disjoint set of image partitions $\{P_1,P_2,\ldots,P_n\}$, such that

$$\bigcup_i P_i = G, \quad for\ 1 \leq i \leq n$$

$$P_i \bigcap P_j = \emptyset, for\ 1 \le i \ne j \le n$$
$$|P_i| = \frac{1}{n}|G|, for\ 1 \le i \le n$$

where | . | denotes the size. The authors applied the three sharing modes 1) multisecret, 2) priority, and 3) progressive mode, in their sharing scheme to execute different reconstructing effects.

Step 2. Each image partition P_i $(1 \le i \le n)$ is further divided into (2n – t) share images $\{L_1, L_2, \ldots, L_n\}$, using Thien-Lin (n,2n – t) secret image sharing technique[3].

Step 3. The n share images, referred to as S_i, i $(1 \le i \le n)$ are generated as:

$$S_i = \bigcup_j L_{jk},\ (1 \le j \le n)\quad and$$

(a) If j = i, then $j \le k \le j + n - k$
(b) If j > i, then k = i
(c) If j < i, then k = i + n – k

In this (t,n) sharing method, the size of each generated shadow image is $\frac{4(2n-t)}{n^2}$ times of that the original image.

2.2 Review of Chang et al's Sharing Secrets in Stego-Images with Authentication Scheme

The main shortcoming of the steganography and authentication based secret sharing [6][7] is that the weak authentication cannot well protect the integrity of the stego-images and thus complete recovery of secret image is not possible. To overcome this drawback, in [8] Chang et al. propose a (t,n) secret sharing technique by combining LSB-based steganography and Chinese remainder theorem (CRT) based authentication together. In [8], the authors first computes four authentication bits using CRT method. Then they combine these four bits with watermark bits and produce four parity bits (p_1,p_2,p_3,p_4). Then stego-block is produced with modified pixels $\overline{W_k}$, $\overline{X_k}$, $\overline{Y_k}$ and $\overline{Z_k}$ as follows :

$$\begin{cases} \overline{W_k} = \left(w_7 w_6 w_5 w_4 w_3 \boxed{\overline{w}_2 \overline{w}_1 \overline{w}_0}\right) = \left(w_7 w_6 w_5 w_4 w_3 \boxed{s_1 s_2 p_1}\right) \\ \overline{X_k} = \left(x_7 x_6 x_5 x_4 x_3 \boxed{\overline{x}_2 \overline{x}_1 \overline{x}_0}\right) = \left(x_7 x_6 x_5 x_4 x_3 \boxed{s_3 s_4 p_2}\right) \\ \overline{Y_k} = \left(y_7 y_6 y_5 y_4 y_3 \boxed{\overline{y}_2 \overline{y}_1 \overline{y}_0}\right) = \left(y_7 y_6 y_5 y_4 y_3 \boxed{s_5 s_6 p_3}\right) \\ \overline{Z_k} = \left(z_7 z_6 z_5 z_4 z_3 \boxed{\overline{z}_2 \overline{z}_1 \overline{z}_0}\right) = \left(z_7 z_6 z_5 z_4 z_3 \boxed{s_7 s_8 p_4}\right) \end{cases}$$

3 The Proposed Scheme

The proposed scheme consists of two main phases: the first phase is sharing and embedding and the second phase is authentication and recovery.

A. The sharing and embedding phase

In sharing phase, the secret image is shared into n shadow images in a (t,n), $2 \leq t \leq n$, scalable image sharing manner in progressive mode by Lin and Wang's technique[5]. Now generated shadow images are embedded into cover image. Before embedding the cover image I of size $M \times N$ is divided into several sections of size 10×16 pixels. Each section is then further subdivided into 40 cover blocks $B_1,B_2,\ldots\ldots,B_{40}$ of size 2×2 pixels as $B_k=\{W_k,X_k,Y_k,Z_k\}$, where $W_k=(w_7,w_6,\ldots\ldots w_0)$, $X_k=(x_7,x_6\ldots\ldots x_0)$, $Y_k=(y_7,y_6,\ldots\ldots y_0)$ and $Z_k=(z_7,z_6,\ldots.z_0)$. Let S be a shadow pixel to be embedded in B_k block, whose binary representation is $(s_7,s_6,\ldots\ldots\ldots s_0)$, then this secret bits are inserted into cover pixels $B_k=\{W_k,X_k,Y_k,Z_k\}$ and producing stego block $\overline{B_k}$ with pixels $\overline{W_k}$, $\overline{X_k}$, $\overline{Y_k}$ and $\overline{Z_k}$ as follows :

$$\begin{cases} \overline{W_k} = \left(w_7w_6w_5w_4w_3w_2\boxed{\overline{w}_1\overline{w}_0}\right) = \left(w_7w_6w_5w_4w_3w_2\boxed{s_7s_6}\right) \\ \overline{X_k} = \left(x_7x_6x_5x_4x_3x_2\boxed{\overline{x}_1\overline{x}_0}\right) = \left(x_7x_6x_5x_4x_3x_2\boxed{s_5s_4}\right) \\ \overline{Y_k} = \left(y_7y_6y_5y_4y_3y_2\boxed{\overline{y}_1\overline{y}_0}\right) = \left(y_7y_6y_5y_4y_3y_2\boxed{s_3s_2}\right) \\ \overline{Z_k} = \left(z_7z_6z_5z_4z_3z_2\boxed{\overline{z}_1\overline{z}_0}\right) = \left(z_7z_6z_5z_4z_3z_2\boxed{s_1s_0}\right) \end{cases}$$

To prevent the manipulation of shadow images from malicious users, a check bits stream is needed. In our proposed scheme, SHA 1 hash function is used to generate the authentication bits. The MSB of all pixels (160) of all blocks in all section are used as watermark bits (160 watermark bits). Now according to the 160 SHA-1 based authentication bits and 160 current watermark bits, 160 check bits are calculated i.e. 4 check bits per block are generated. The authentication bits of each section are evaluated as follows:

$$\begin{aligned} &(a_{159}a_{158} \ldots\ldots\ a_1a_0) \\ &\quad = SHA1\Big(\left(\overline{W}_{39} - c_{159}\right)\Big|\Big|\left(\overline{X}_{39} - c_{158}\right)\Big|\Big|\left(\overline{Y}_{39} - c_{157}\right)||\left(\overline{Z}_{39}\right. \\ &\quad \left. - c_{156}\right)||\ \ldots||\left(\overline{W}_0 - c_3\right)||\left(\overline{X}_0 - c_2\right)||\left(\overline{Y}_0 - c_1\right)||\left(\overline{Z}_0\right. \\ &\quad \left. - c_0\right)\Big) \ \ldots\ldots\ldots\ldots (1) \end{aligned}$$

Where $\left(\overline{W}_k - c_i\right)$ represents 7 bits exclusive the check bit c_i and "||" represent the concatenation operation. Now check bits $c_{159},\ldots\ldots.c_1,c_0$ are computed by

$$(c_{159}c_{158} \dots\dots\ c_1c_0) = \left(MSB(\overline{W}_{39})\ MSB(\overline{X}_{39})MSB(\overline{Y}_{39})MSB(\overline{Z}_{39}) \dots MSB(\overline{W}_0)\ MSB(\overline{X}_0)MSB(\overline{Y}_0)MSB(\overline{Z}_0)\right) \text{ XOR } (a_{159}a_{158} \dots\dots\ a_1a_0) \dots\dots\dots\dots\dots (2)$$

Finally, the proposed scheme replaces the 3rd LSB of cover pixels for example w_2,x_2,y_2,z_2 with the computed check bits c_3,c_2,c_1,c_0.

B. Authentication and Recovery Phase

In order to generate the secret image, any t or more number of stego images are gathered together. After that, each stego-image is divided into several sections of size 10×16 pixels and each section once again subdivided into 40 blocks of size 2×2 pixels. For each section, the hash value is evaluated using (1) and check bits $(\overline{c}_{159}, \dots, \overline{c}_1, \overline{c}_0)$ of the current section are generated using (2). Now extract the 160 3rd LSB ($c_{159},\dots\dots\dots c_1,c_0$) from each stegopixels of the current section. If the computed check bits $(\overline{c}_{159}, \dots, \overline{c}_1, \overline{c}_0)$ are matched to those extracted bits ($c_{159},\dots\dots\dots c_1,c_0$), the current section is verified successfully. Now one shadow pixel is extracted from the 2 LSB of the stego-pixels of each 2×2 stego-block. In this way, 40 shadow pixels are correctly extracted from the current verified section. Otherwise, the stego-image has been manipulated by malicious users. Thus when any t or more shadows are extracted from the stego-images, the original secret image is recovered using Lin and Wang's[5] reconstructed algorithm.

4 Experimental Results

This section presents the experimental results of the proposed scheme. The stego-images visual quality is evaluated by the Peak Signal to Noise Ratio (PSNR). The definition of PSNR is given below

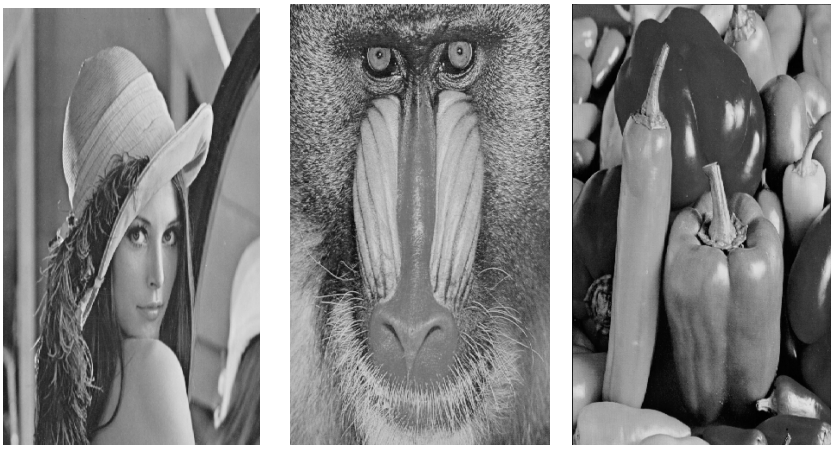
$$\text{PSNR(dB)} = 20\log_{10}\frac{255}{\sqrt{\text{MSE}}} \quad (12)$$

MSE is the mean squared error between the original image and the modified image which is defined as

$$\text{MSE} = \frac{1}{\text{M}\times\text{N}}\sum_{\text{x}=1}^{\text{M}}\sum_{\text{y}=1}^{\text{N}}\left(\text{I}(\text{x},\text{y}) - \text{I}'(\text{x},\text{y})\right)^2 \quad (13)$$

where M and N denotes the width and height of the cover and stego image respectively. In our experiment we used (2,3) secret sharing. The image Airplane shown in figure 1 of size 256×333 pixels is chosen as secret image and three cover image Lena, pepper and baboon with 512×300 pixels are chosen as cover image as shown in figure 2. Table 1 shows the PSNR values of the stego-images.

Fig. 1. The secret image - Airplane



(a) (b) (c)

Fig. 2. Cover images (a) lena, (b) pepper, (c) baboon

Table 1. The experimental results for four (2,3) secret image sharing schemes

Images	Lin et al.'s schemes	Yang et al.'s schemes	Chang et al.'s schemes	The proposed scheme
Lena	39.21	36.20	40.97	40.9718
Pepper	39.17	36.17	40.96	40.9701
Baboon	39.18	36.19	40.93	40.9521

In addition we also used detection ratio(DR) for integrity verification. The detection ratio(DR) is defined as follows:

$$\text{detection ratio(DR)} = \frac{\text{Number of the tampered pixels (NTP)}}{\text{Number of the tampered pixels that are detected(NTPD)}}$$

The detection ration (DR) in Lin et al.'s, Yang et al.'s, Chang et al.'s , Eslami et al's and the proposed methods are 0, 0.51,0.97,0 and 0.97 respectively as given in table 2. From table 2 it is also clear that our proposed method reduces the size of expansion of stego-image and provides better authentication.

Table 2. Comparison of (k,n) secret image sharing schemes

	Lin et al.'s schemes	Yang et al.'s schemes	Chang et al.'s schemes	Eslami et al's scheme	The proposed scheme
Expansion of stego-image	4	4	4	4	$\frac{4(2n-t)}{n^2}$
Detection Ratio (DR)	0	0.51	0.97	0	0.97
The size of detection unit	-	Block of size 2×2 pixels	Block of size 2×2 pixels	-	Block of size 10×16 pixels
Authentication bits: pixel	1	1:4	1:1	0	1:1

5 Conclusion

In this paper we propose an steganography and authentication based secret sharing technique. Compared with other existing method, the size of each stegoimage is only $\frac{4(2n-t)}{n^2}$ times of the size of the secret image. This small size helps in both storage and transmission. Moreover the authentication is implemented by SHA1 which enhance the authentication ability.

References

1. Blakely, G.R.: Safeguarding cryptography keys. In: Proc. of AFIPS National Computer Conference, vol. 48, pp. 313–317 (1979)
2. Shamir, A.: How to share a secret. Communications of the ACM 22(11), 612–613 (1979)
3. Thien, C.C., Lin, J.C.: Secret image sharing. Computer Graphics 26(5), 765–770 (2002)
4. Thien, C.C., Lin, J.C.: An image-sharing method with user-friendly shadow images. IEEE Transactions on Circuit System 13(12), 1161–1169 (2003)
5. Lin, Y.Y., Wang, R.Z.: Scalable Secret Image Sharing with Smaller Shadow Images. IEEE Signal Processing Letters 17(3), 316–319 (2010)
6. Lin, C.C., Tsai, W.H.: Secret Image sharing with steganography and authentication. Journal of Systems and Software 73, 405–414 (2004)
7. Yang, C.N., Chen, T.S., Yu, K.H., Wang, C.C.: Improvements of image sharing with steganography and authentication. Journal of Systems and Software 80, 1070–1076 (2007)
8. Chang, C.C., Hsieh, Y.P., Lin, C.H.: Sharing secrets in stego images with authentication. Pattern Recognition 41, 3130–3137 (2008)
9. Eslami, Z., Razzaghi, S.H., Ahmadabadi, J.Z.: Secret image sharing based on cellular automata and steganography. Pattern Recognition 43(1), 397–404 (2010)