Secret Image Sharing Using Steganography with Different Cover Images

Noopa Jagadeesh, Aishwarya Nandakumar, P. Harmya, and S.S. Anju

Centre for Cyber Security, Amrita Vishwa Vidyapeetham, Coimbatore, India
{noopajagadeesh,aishwarya.nk12,
harmya.gopalan,anjuss.cys}@gmail.com

Abstract. A novel approach to secret image sharing based on a (*t,n*)-threshold scheme with steganography is proposed. A secret image is first processed into n-shares which are then hidden in n-user selected different cover/camouflage images. Any *t* out of *n* participants can cooperate to reveal the secret data. The important essential of secret image sharing approaches is that the revealed secret image must be lossless. In the earlier visual secret sharing (VSS) scheme, the secret image can be shared by generating *n* random like images, called shadows or shares. The produced shadows can be transmitted instead of the original secret image. Once involved participants stack more than *t* shadows, the secret image can be revealed by visual perception without computation. But the generated shadows are often meaningless. A malicious intruder may be attracted to such meaningless shadows delivered over an insecure channel. To handle such meaningless threat, the steganography approach is utilized to embed the shadows in different cover images, called stego images. From visual perception, the content of the stego image is meaningful and can conceal the shadows from intruders .This scheme is a novel image sharing technique that satisfies all of the essentials of the traditional secret sharing scheme. The use of *n* different cover images further prevent the intruders from imagining an secret being transferred when compared to the shares being embedded into *n* similar cover images.

Keywords: secret sharing, steganography, modulo operator, visual cryptography.

1 Introduction

The continuing improvements in computer technologies and the increase in Internet usage are responsible for the increasing popularity of network-based data transmission. In many important applications, such as the communication of commercial affairs or military documents, the images must be kept secret. Many image-protection techniques, such as data encryption and steganography have been proposed to increase the security of secret images. However, one common defect of all these techniques is their policy of centralized storage, in which an entire protected image is usually maintained in a single information carrier. If a cracker detects an abnormality in the information carrier in which the protected image resides, he/she try intercepting it, attempting to decipher the secret inside, or simply ruin the entire

A. Abraham et al. (Eds.): ACC 2011, Part II, CCIS 191, pp. 490–497, 2011.

information carrier (and once the information carrier is destroyed, the secret image is also lost forever). Further the transmission of secret through the same cover image further increases the suspicion of the intruder that some data is been transmitted. This brings the importance of sharing the secret using different types of cover images. Secret image sharing proposed is a protection mechanism that does not suffer from these problems. It works by splitting the secret image into *n* shadow images that are transmitted and stored separately. One can reconstruct the original image if at least a preset number of these *n* shadow images are obtained; but knowledge of less than *t* shadow images is insufficient for revealing the secret image.

A well-known principle in the analog world is the term reduced trust, meaning that in order to keep a secret, the less knowledge or power each entity has the better. This is the basic philosophy, and *secret sharing* or *secret splitting or shared control* is a method to achieve this in the digital world. The secret sharing mechanism [1-2] has been widely applied to share a secret key. In this mechanism, each participant has a private shadow; some authorized participants with integrated shadows can cooperate to recover the secret key. The purpose of secret sharing is to recover the secret key while some shadows are lost, distorted, or stolen. In 1979, Blakely and Shamir introduced the (*t*, *n*)-threshold secret sharing system. In this scheme, a dealer can encode and divide secret data into *n* shadows. The dealer then distributes these shadows to the involved participants. With any *t* out of *n* shadows, authorized participants can cooperate to reveal the secret data accurately.

Utilizing the (*t*, *n*)-threshold concept, Noar and Shamir designed a secret image sharing technique known as visual secret sharing (VSS). Using the VSS technique, the secret image can be shared by generating *n* random like images, called shadows or shares. The produced shadows are transmitted instead of the original secret image. Once involved participants collect and stack more than *t* shadows, the secret image can be revealed by visual perception without computation. The VSS technique, however, is applied to binary images due to this stacking property. These generated shadows often lead to problems of meaningless [3, 4]. A malicious intruder may be attracted to such random-like shadows delivered over an insecure channel.

To handle such meaningless threat, the steganography approach is utilized to camouflage the shares in cover images, called stego images (shadow images) [5-9]. The proposed scheme uses *n* different cover images instead of a same cover. From visual perception, the content of the stego image is meaningful and can conceal the shadows from intruders.

The rest of this paper is organized as follows. A brief introduction of various secret sharing schemes is given in Section 2.The proposed scheme is given in Section 3. The experimental results and analysis in Section 4. Finally, the conclusions and future work in Section 5.

2 Secret Sharing

Secret sharing schemes are normally set up by trusted authority, which computes all shares and then distributes them to participants via secure channels. The trusted authorities that setup the scheme is called a dealer. The participants hold their shares until some/ all of them decide to pool/stack their shares and recreate the secret. The

combiner, who on behalf of the cooperating group computes the secret, does the recovery of the secret. The combiner can be a mutually trusted participant who collects all shares, calculates the secret, and distributes it secretly to the active participants. The various secret sharing schemes are

2.1 (*t, t*) Threshold Schemes

The secret can be recovered only when all participants cooperate. Let the secret integer k be given. The dealer chooses a modulus p that can be any integer greater than k. Its value determines the security parameter. Next the dealer selects randomly, uniformly and independently (t - 1) elements. $S_1, S_2, \ldots S_{t-1}$ from Zp. The share S_t is given by

$$S_t = k - \sum_{i=1}^{t-1} S_i \pmod p \tag{1}$$

The shares are distributed securely to the participants from the set $P = \{P_1, P_2, \ldots, P_t\}$. At the pooling time, the combiner can reconstruct the secret only if he/she is given all shares as

$$k = \sum_{i=1}^{t} S_I \pmod p \tag{2}$$

Obviously, any (t -1) or fewer shares provide no information about the secret k.

2.2 *(t, n)* Secret Sharing

A (t, n) Shamir scheme is constructed by the dealer Don. First Don chooses n different points $x_i \in GF(p)$, for i=1,2…n. These points are public. Next Don selects at random coefficients $a_0, a_1, \ldots a_{t-1}$ from GF(p). The polynomial $f(x) = a_0 + a_1 x + \ldots + a_{t-1}x^{t-1}$ is of degree at most (t-1). The shares are $S_i = F(x_i)$ for i=1, 2,…n, and the secret is $k = F(0)$. The share S_i is distributed to the participant $Pi \in P$ via a secure channel and is kept secret. When t participants agree to cooperate, the combiner Clara takes the shares and tries to recover the secret polynomial $F(x)$. She knows t points on the curve $F(x)$.

$(x_i, F(x_i)) = (x_i, S_i)$ for i=1,2,… t. These points produce the following system of equation:

$$\begin{aligned} S_1 &= a_0 + a_1 x_1 + \ldots + a_{t-1}x_1^{t-1} \\ S_2 &= a_0 + a_1 x_2 + \ldots + a_{t-1}x_2^{t-1} \\ &\ldots\ldots\ldots\ldots \\ S_t &= a_0 + a_1 x_t + \ldots + a_{t-1}x_t^{t-1} \end{aligned} \tag{3}$$

The system has a unique solution for $(a_0, a_1, \ldots a_{t-1})$ since the corresponding Vandermonde determinant is different from zero. The Lagrange interpolation formula allows us to determine the polynomial $F(x)$ of degree (t-1) from the t different points

(x_i, S_i) .

2.3 Modular Scheme

Assume that every participant $P_i \varepsilon P$ is assigned a public modulus P_i , i =1,2…n. The modulo can be primes or mutually co primes. Let the modulo be such that $P_1 < P_2 < \ldots < P_n$. The dealer selects at random an integer S such that $0 < S < \prod_{i=1}^{t} P_i$. The secret $k \equiv S \pmod{P_0}$. Next the dealer distributes shares $S_i \equiv S \pmod{Pi}$ to the participants P_i (i =1,2…n) via secure channels. Assume that there is t or more participants who want to recreate the secret. The combiner takes their shares S_{i1}, S_{i2}, …S_{it} and solves the following system of congruence using Chinese remainder theorem. The secret $k=S \pmod{P_0}$.

2.4 Proactive Secret Sharing

There is a need for scheme that allows servers to generate a new set of shares for the same secret from the old shares without reconstructing the secret. Such a scheme is called as an *proactive secret scheme* (PSS).In reality, compromise to a server are very hard to detect, especially when the attacker/intruder simply steals certain secret information without modifying anything on the victim server. To strengthen the security of a replicated service, we can invoke PSS periodically (at regular intervals). Before the start of execution o PSS, every server checks the integrity of its code and state, and there by trying to remove any attackers that might exist in that server at that point in time.

To show how a proactive scheme can be achieved, let's study an example first. Let us first assume that an adversary can only break into a server and have access to information stored or collected by that server. The adversary can't change the code of the server. Suppose we have a simple (2,2) sharing scheme. To generate two shares for secret S, we randomly select $S_1$and S_2, so that $S_1 + S_2 = S$. We want the two servers with shares S_1 and S_2 to change their respective shares to S_1' and S_2', so that these two shares remain an (2,2) sharing of the same secret S and these two shares are independent from the old shares . The proactive secret sharing can be performed through the following steps:

1. Server 1 generates two sub shares $S_{11}$and S_{12} from its share S_1 using the same secret sharing scheme as the one used to generate S_1 and S_2 from S; that is, server 1 randomly selects two sub shares S_{11} and S_{12} , so that $S_1 = S_{11} + S_{12}$. Server 2 does the same thing to S_2 : It randomly generates two sub shares S_{21} and S_{22}, so that $S_2 = S_{21} + S_{22}$
2. Server 1 sends S_{12} to server 2 through a certain secure channel. Server 2 sends S_{21} to Server 1.
3. Server 1 has both S_{11} and S_{21} and can add them to get a new share $S_1' = S_{11} + S_{21}$.

Server 2, on the other hand, has both $S_{12}$and S_{22} and can generate a new share $S_2' = S_{12} + S_{22}$. Now we show that S_1' and S_2' constitute a (2, 2) sharing. The sum of these two shares is the sum of all the four sub shares, which is the sum of S_1 and S_2, which is S.

These two shares are independent from the old ones because these sub shares are generated randomly. Also, no servers know the secret during the entire process. Server 1 generates $S_{11}$and S_{12} and learns S_{21} from server 2, but server 1 never knows S_{22} and thus does not know S_2' or S. Server 2, on the other hand, never knows S_{11} , and thus does not know S_1'or S.

3 The Proposed Scheme

3.1 (t, n) Sharing Procedure

The dealer firsts selects a prime number m and assigns a unique key K_i for each participant, where i = 1, 2, .., n. To share the secret image S, the dealer converts S into the m-ary notational system. For instance, we assume that the chosen m is equal to 7. If two continuous secret pixels in S are 83 and 110, then the converted digits become $(1, 4, 6)_7$ and $(2, 1, 5)_7$.

Let us assume that the shared (t-1) digits of S are $S_1, S_2, \ldots S_{t-1}$. Suppose that $O_1,O_2,\ldots O_n$ be the chosen grayscale cover image with pixels $H \times W$, and P_{1i} is a pixel of O_1. The dealer first computes the value of d as

$d=P_{1i} \bmod m$

If 157 is the first pixel(P_{11}) of first cover image O_1, then value of d is 3.

With d and $S_1, S_2, \ldots S_{t-1}$, an invertible polynomial can be formulated as

$$F(x)= S_1+S_2x^1+\ldots+S_{t-1}x^{t-2}+dx^{t-1} \bmod m \quad (4)$$

The dealer can thereby generate n shadows y_i by feeding the secret key K_i into $F(x)$.

$$y_1=F(K_1) , y_2=F(K_2) ,\ldots., y_n=F(K_n) \quad (5)$$

Suppose if dealer intends to make 3 shares then $F(x)= (1+4x+2x^2) \bmod 7$ and$y_1=1$, $y_2=0$, $y_3=5$

In order to hide the values of $y_1,y_2,\ldots,y_n$, n different cover images $O_1,O_2,\ldots O_n$ are selected. For each of the cover images the following computations is done.

$$Q=\text{floor}\ (P_i /m) \times m , \quad (6)$$

$$P(new)_i= Q+ y_i \quad , \quad (7)$$

Where P_i represent the i'th pixel of each of the original cover images.

3.2 Secret Retrieval Procedure

Given any t out of n stego images O_i and the key K_i from the involved participants, the secret image S can be reconstructed. We first assume that $P(new)_i$ is the corresponding pixel value of O_i. To extract the secret digits, authorized participants must derive the polynomial $F(x)$ from $P(new)_i$. Thus, the participants utilize the modulo operation to obtain shadows y_i's by computing

$$y_i=P(new)_i \bmod m \quad (8)$$

With this obtained shadow y_i and secret key K_i, polynomial $F(x)$ can be reconstructed by Lagrange's interpolation formula:

$$F(x)= S_1+S_2x^1+\ldots+S_{t-1}x^{t-2}+dx^{t-1} \bmod m \quad (9)$$

Authorized participants can thereby obtain the secret digits $S_1, S_{2,..,} S_{t-1}$ by extracting the first (t-1) coefficients of $F(x)$.

4 Experimental Results and Analysis

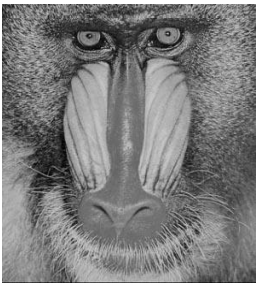
To demonstrate the performance of the novel (t, n)-threshold sharing scheme the size of grayscale cover images is set to 298 × 298 pixels. Figure 1 shows the shared secret image with 100× 100 pixel

Fig. 1. The secret image

Table 1 lists the qualities of the stego images with various test cover images. This experiment is implemented in the case of the (3,n)-threshold scheme. The prime number m is set as 7. In Table 1, we can see that the quality of the stego image is quite satisfactory for different secret images and stego images. We display three stego images in Figures. 2(a), 2(b) and 2(c). Judging from the visual perception of these three stego images, our scheme can successfully protect the shares from intruders. Authorized participants can later extract the secret image from these three different stego images.

(a)The stego image 1

(b)The stego image 2



(c)The stego image 3

Fig. 2. The resulting shares

Table 1. The PSNR of the shadow images for various images

Share1	Share2	Share3
Naturals=47.60	Lena=46.24	Baboon=45.20
Clown=46.53	Lena=46.21	Naturals=47.40
Pepper=45.63	Baboon=45.83	Naturals=47.00
Tiffany=43.38	Splash=37.43	Lena=47.42

5 Conclusion and Future Works

A common drawback of image sharing schemes using steganography approaches is that the revealed secret image is distorted. Although the distortion is small, it is unacceptable for significant secret content. In this approach, a novel sharing scheme that can reveal the lossless secret image and satisfy related sharing essentials is used. The secret image is revealed from any t of n different stego images. The lossless of the novel sharing scheme is a practical essential to preserve valuable secret images, such as military and medical images.

The future works include extending the secret sharing scheme for color images and sharing multiple secret. The (t,n) secret sharing scheme can be extended further in such a way that each authorized participant can be given a privilege/access level.

Acknowledgment. Special thanks to Chin-Chen Chang, Pei-Yu Lin, Chi-Shiang Chan authors of "Secret image sharing with revertible steganography".We also extend our thanks to Cyber Security Department, Amrita Vishwa Vidyapeetham, Coimbatore.

References

1. Shamir, A.: How to share a secret. Communications of the ACM 22(11), 612–613 (1979)
2. Naor, M., Shamir, A.: Visual cryptography. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 1–12. Springer, Heidelberg (1995)
3. Wang, R.Z., Su, C.H.: Secret image sharing with smaller shadow images. Pattern Recognition Letters 27(6), 551–555 (2006)
4. Chang, C.C., Lin, C.C., Lin, C.H., Chen, Y.H.: A novel secret image sharing scheme in color images using small shadow images. Information Sciences 178(11), 2433–2447 (2008)
5. Tsai, C.S., Chang, C.C., Chen, T.S.: Sharing multiple secrets in digital images. The Journal of Systems and Software 64(2), 163–170 (2002)

6. Thien, C.C., Lin, J.C.: Secret image sharing. Computer & Graphics 26(1), 765–770 (2002)
7. Lin, C.C., Tsai, W.H.: Secret image sharing with steganography and authentication. The Journal of Systems and Software 73(3), 405–414 (2004)
8. Wu, Y.S., Thien, C.C., Lin, J.C.: Sharing and hiding secret images with size constraint. Pattern Recognition 37(7), 1377–1385 (2004)
9. Chang, C.-C., Lin, P.-Y., Chan, C.-S.: Secret image sharing with revertible steganography., International Conference on Computational Intelligence and Natural Computing (2009)