A New Probabilistic Visual Secret Sharing Scheme for Color Images

Chin-Chen Chang\textsuperscript{1,2} \hfill Chia-Chen Lin\textsuperscript{3} \hfill T.Hoang Ngan Le\textsuperscript{4}
\textsuperscript{1}Department of Information Engineering and Computer Science, Feng Chia University, Taichung 407, Taiwan, R.O.C.
\textsuperscript{2}Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi 621, Taiwan, R.O.C.
E-mail: cccc@cs.ccu.edu.tw
\textsuperscript{3}Department of Computer Science and Information Engineering, Providence University, Taichung 433, Taiwan, R.O.C.
E-mail: mhlin3@pu.edu.tw
\textsuperscript{4}Department of Computer Science, Natural Science University, 227 Nguyen Van Cu, District 5, HCMC, Vietnam.
E-mail: {lhbac, lhngan}@fit.hcmuns.edu.vn

Abstract

In 2007, Wang et al. proposed two visual secret sharing (VSS) schemes based on Boolean operations. The first one is a probabilistic $(2, n)$ secret sharing scheme called $(2, n)$ ProbVSS scheme for binary images. The other is a deterministic $(n, n)$ secret sharing scheme for grayscale images. Although Wang et al.'s two schemes solve the problems of computational complexity and pixel expansion at the same time; they cannot be applied to color images. To expand core concept of Wang et al.'s $(2, n)$ ProbVSS scheme to color images, in this paper, we combine Shamir's scheme and Chang and Wu's gradual search algorithm for a single bitmap BTC (GSBTC) to design a new $(2, n)$ ProbVSS scheme for color images. Experimental results confirm that our proposed scheme not only generates reconstructed color images with high quality, reduces successfully shadow size but also gives random-like grayscale images as shadows for color images.

1. Introduction

In 1979, a secret sharing (SS) scheme also called a $(k, n)$ threshold scheme was first introduced by George Blakley and Adi Shamir, respectively. The first objective of SS is used to protect secret data by dividing it into $n$ pieces; each piece is called a shadow or a share. Later, the set of shadows are distributed to $n$ participants and each of whom holds one shadow. The secret data can be reconstructed if and only if there is complete knowledge of the $k$ shadows at least, where $k \leq n$. Based on this scheme, in 1995, Noar and Shamir first extended application of SS scheme to image domain named visual secret sharing (VSS).

Generally, four criteria are used to evaluate the performance of a $(k, n)$ VSS scheme: security, accuracy, computational complexity and pixel expansion. Many SS schemes for images have been proposed over the past decade. Although the reconstructed images in these schemes can be revealed by simply stacking the collected shadows, the pixel expansion problem is occurred. Some other VSS schemes solve this problem but increase computational complexity cost. To deal with these problems, Yang \cite{2}, Cimato at al. \cite{3} and Wang et al. \cite{6} propose a new probabilistic visual secret sharing scheme called ProbVSS scheme for binary images. This scheme is done on small areas instead of individual pixel of secret images with two Boolean operations: XOR and AND. There are some research works relate to ProbVSS scheme such as the relation between probabilistic schemes and deterministic ones \cite{3} or constructing an optimization model for general access structures based on probabilistic concept \cite{5}. However, all existing ProbVSS schemes are designed for binary images.

The experimental results show that Wang et al.'s $(2, n)$ ProbVSS scheme is superior to those existing ProbVSS schemes with respect to the criteria. In this paper, we extend the application of Wang et al.'s $(2, n)$ Prob VSS scheme designed for binary images to secret color image. By applying Shamir's secret sharing scheme and Chang and Wu’s gradual search algorithm for a single bitmap BTC (GSBTC) \cite{1} in combination
with Wang et al.'s (2, n) ProbVSS scheme, our scheme can generate high reconstructed color image quality and small shadows size without significantly increasing computational complexity.

The rest of this paper is organized as follows. Section 2 describes Shamir’s SS scheme, GSBTC technique and Wang et al.’s (2, n) ProbVSS scheme briefly. In Section 3, we present our proposed scheme in detail. Then, in Section 4, we offer the experimental results. Some conclusions are given in Section 5.

2. Related works

To give readers the essential background knowledge of our scheme, we respectively illustrate Shamir’s SS scheme, Chang and Wu’s GSBTC technique and Wang et al.’s (2, n) VSS scheme in detail, in the following subsections.

2.1. Shamir’s secret-sharing scheme

In 1979, Shamir proposed a (k, n) threshold scheme based on a polynomial interpolation function. His scheme is implemented by dividing secret data s into n pieces: s₁, s₂, ..., sₙ, and the secret data s can be reconstructed if and only if there is complete knowledge of k pieces at least. This secret data s is an outcome of a (k - 1)-degree polynomial function whose coefficients are based on Lagrange interpolation formula. This scheme has 2 phases demonstrated more precisely in following pseudo codes.

Input: Two integers n, k (n≥k≥1), and a secret data s

Shares construction phase:
Step 1: Generate (k - 1) random numbers: a₁, a₂, ..., aₖ₋₁ and a random prime number g, where g>aᵢ, ∀i ∈ [1, (k - 1)] and ∀b ∈ F, ∃t ∈ F, b × t ≡ 1(mod g).
Step 2: Define a polynomial function, f(x) = (a₀ + a₁x + ... + aₖ₋₁xᵏ₋₁) mod g, where a₀=s.
Step 3: Give s=f(0) as a share to ith participant.

Revealing phase:
Step 1: Compute the coefficients of polynomial function f(x) based on Lagrange interpolation formula.
Step 2: Derive the secret data: s=f(0).

2.2. Gradual search algorithm for one single bitmap BTC

To extend the BTC method to a color image, Chang and Wu’s GSBTC technique is adopted to compress one secret color image into one binary image and its mean values. The detailed descriptions of Chang and Wu’s algorithm are given in the following steps.

Step 1: Based on 3 color planes (Red, Green, Blue) in each color, we get 3 common bitmaps and 3 pairs of mean values after applying traditional BTC into each color block. Let (Rₓ, Rᵧ), (Gₓ, Gᵧ) and (Bₓ, Bᵧ) be three pairs of mean values and call Bₓ, Bᵧ and Bᵧ be 3 common bitmaps corresponding to 3 color planes.
Step 2: If sCB is the best common bitmap, the initial value of sCB is defined as sCB=[c₁,c₂,...,cₘₓₘₖ] where

\[ cᵢ = \begin{cases} rᵢ, & \text{if } rᵢ = gᵢ = bᵢ \\ ND, & \text{otherwise} \end{cases} \]

values of Bₓ, Bᵧ and Bᵧ, respectively.
Step 3: Let MSEₓ and MSEᵧ be the mean squared error (MSE) in the case ND element cᵢ is placed by bit ‘0’ and bit ‘1’, respectively. If cᵢ is a ND element, its value is specified as follows: cᵢ \[=\begin{cases} 0, & \text{if } MSEₓ < MSEᵧ \\ 1, & \text{otherwise} \end{cases}\]

After these steps are completed, we get one common bitmap and six mean values from each color block.

2.3. Wang et al.’s (2, n) ProbVSS scheme for binary images

Two phases of Wang et al.’s (2, n) ProbVSS scheme are illustrated in the following pseudo-codes.

Shares construction phase:
Input: An integer n, where n≥2, and a secret image A
Step 1: Generate (n + 1) random matrices B₁, ..., Bₙ₊₁.
Step 2: Compute n intermediate matrices C₁, C₂, ..., Cₙ with Cᵢ = Bᵢ ⊗ A, for i = 1, 2, ..., n.
Step 3: Compute n shadows A’₁, A’₂, ..., A’ₙ with A’ᵢ = Bᵢ₊₁ ⊗ Cᵢ, for i = 1, 2, ..., n.

Revealing phase:
Step 1: Compute the reconstructed images A’ᵢⱼ = Aᵢ ⊗ Aⱼ, for i, j = 1, 2, ..., n and i≠j.
Step 2: Calculate the number of bits ‘1’ in each reconstructed image A’ᵢⱼ for i, j = 1, 2, ..., n and i≠j.
Step 3: Output the reconstructed image A’.

To decide which outcome A’ᵢⱼ is the best, a probabilistic concept is adopted in their scheme.

3. Proposed scheme

This section discusses a new (2, n) ProbVSS scheme for color images based upon the techniques mentioned in the previous section. Figure 1 gives the overview and the relation among these techniques used in our scheme.
3.1. Shares construction phase

This phase divides a color image \( I \) into \( n \) grayscale shadows along with three steps.

**Step 1:** Break \( I \) into a collection of compression codes consisting of one common bitmap \( sCB \) and one group of mean values \( \{ R_XL, G_XL, B_XL, R_XH, G_XH, B_XH \} \). The details of Step 1 are described as follows:

**Step 2:** First, by adopting Wang et al.’s scheme to one \( sCB \), we get \( n \) common bitmap shadows. Second, by applying Shamir’s scheme to one mean values group, \( n \) mean shares groups are retrieved. Following above assumption, there are \( b \times n \) common bitmap shadows and \( b \times n \) mean shares groups are obtained from one grayscale image.

**Step 3:** A pixel shadow is created by appending one \( sCB \) to one group of \( 6 \) mean shares; therefore, there are totally \( b \times n \) pixel shadows spawned. It is noted that before appending, \( sCB \) is transformed into bytes sequence. In our scheme, one shadow is generated by uniting \( b \) pixel shadows together. Generally, there are \( n \) shadows created from \( b \times n \) pixel shadows and the size of each shadow is \( \left\lceil m \times m / 8 \right\rceil + 6 \times b \) bytes.

3.2. Revealing phase

This phase includes three steps, as shown in Figure 3:

**Step 1:** Divide each pixel shadow into two groups. The first group contains \( \left\lfloor m \times m / 8 \right\rfloor \) bytes and another contains 6 bytes. The second group is considered as a group of intermediate mean values: \( R_XL, R_XH, G_XL, G_XH, B_XL, B_XH \). Firstly, convert the first group into \( m \times m \) bits stream. Then, with a pair of pixel shadows \( sPB_{ix} \), we get a pair of intermediate common bitmaps \( sCB_{ix} \) and a pair of group of intermediate mean values \( sGM_{ix} \). Finally, based on \( b \) pairs of \( \{ sPB_{ix}, sPB_{kx} \} \), for \( x = 1, 2, …, b \), we have \( b \) common bitmaps by applying the second phase of Wang et al.’s scheme into \( b \) pairs of \( \{ sCB_{ix}, sCB_{kx} \} \) and \( b \) groups of mean values by adopting the second phase of Shamir’s scheme into \( b \) pairs of \( \{ sGM_{ix}, sGM_{kx} \} \).

**Step 3:** The reconstructed color image is generated by combining common bitmaps and groups of mean values as shown in Figure 4.
From Table 1, we can see that the reconstructed color image quality is high and independent of parameters: number of shadows \( n \), prime number \( g \), coefficients \( a \) of polynomial function, but the size of block \( m \times m \). The experimental results show that the larger \( m \) value gives worse quality of reconstructed color image with shorter computation time. It is noted that the computational time for generating shadows by dividing a color image into 4 blocks is almost five times of that for generating shadows by dividing a color image into 8 blocks. By dividing a color image into 4 blocks, the image quality of reconstructed image can be 2dB higher than that by dividing a color image into 8 blocks in the shares reconstruction phase. Therefore, there is a tradeoff between the image quality of the reconstructed color image and the required computation time.

In this scheme, each shadow reveals no information about the secret color image, a set of shadows generated when \( n \) is set as 5, \( m \) is set as 4 and 8 in turn are shown below.

**Table 2. Corresponding shadows for each test image with our scheme when \( n=5 \) and \( m=4 \)**

(Original color image size is 786,432 bytes and shadow size is 131,072 bytes)

<table>
<thead>
<tr>
<th>Original Images</th>
<th>Shado__w 1</th>
<th>Shado__w 2</th>
<th>Shado__w 3</th>
<th>Shado__w 4</th>
<th>Shado__w 5</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Image" /></td>
<td><img src="image2" alt="Image" /></td>
<td><img src="image3" alt="Image" /></td>
<td><img src="image4" alt="Image" /></td>
<td><img src="image5" alt="Image" /></td>
<td><img src="image6" alt="Image" /></td>
</tr>
</tbody>
</table>

**Table 3 Corresponding shadows for each test image with our scheme when \( n=5 \) and \( m=8 \)**

(Original color image size is 786,432 bytes and shadow size is 57,344 bytes)

<table>
<thead>
<tr>
<th>Original Images</th>
<th>Shado__w 1</th>
<th>Shado__w 2</th>
<th>Shado__w 3</th>
<th>Shado__w 4</th>
<th>Shado__w 5</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image7" alt="Image" /></td>
<td><img src="image8" alt="Image" /></td>
<td><img src="image9" alt="Image" /></td>
<td><img src="image10" alt="Image" /></td>
<td><img src="image11" alt="Image" /></td>
<td><img src="image12" alt="Image" /></td>
</tr>
</tbody>
</table>

From Tables 2 and 3, we can see that each shadow is about a random-like grayscale image; therefore, the security of the proposed scheme is guaranteed.

As mentioned in section 3, the size of each shadow is \( \left\lceil \frac{m \times m}{8} \right\rceil \times b \) bytes and the size of original color image is \( (3 \times m \times m \times b) \) bytes. This information shows that the presented scheme can efficiently reduce shadow size. The ratio of size in bytes between original color image and shadow, which is called \( \alpha \) is calculated as \( \alpha = \frac{3 \times m \times m}{(m \times m)/8} + 6 \). We can see that \( \alpha \geq 6, \forall m \geq 4 \). It means that the size of shadow can be efficiently shrunk.

**5. Conclusion**

We present a new SS scheme for color images. Our scheme is based on Wang et al.’s \((2, n)\) ProbVSS scheme, which was designed for binary images. To maintain the advantages of Wang et al.’s scheme: low computation cost and no pixel expansion problem, we use two strategies in combination with Wang et al.’s scheme: Shamir’s secret sharing scheme and Chang and Wu’s GSBTC technique. In our scheme, we replace a secret color image by smaller grayscale shadows. The reconstructed color image is obtained by combining at least two grayscale shadows.

Experimental results confirm that our proposed scheme gives not only high image quality with \( \text{PSNR} \) ranging from 27dB to 31dB but also smaller shadows size without significantly causing high computational complexity. Moreover, each shadow does not reveal any information of the original color image.

**6. References**


