A Novel (2,n) Secret Image Sharing Scheme

Tapasi Bhattacharjeea, Jyoti Prakash Singhb, Amitava Nagc

aDepartment of Information Technology, Techno India, Kolkata-700091, India
bDepartment of Information Technology, National Institute of Technology, Patna, India
cDepartment of Information Technology, Academy of Technology, Hooghly-712121, India

Abstract

In this paper, we propose a novel and simple (2, n) secret sharing scheme with precise reconstruction for grayscale, binary and color image. The share construction phase is based on pixel division and XOR operation. The reconstruction is based on XOR and OR operation. The proposed scheme has no pixel expansion and can reconstruct the secret image precisely. This scheme can be directly applied to share grayscale images and can be easily extended to deal with binary and color images. Experimental results prove that the proposed scheme is efficient because of strong security and accuracy.

Keywords: Secret Image Sharing, contrast, peak-signal-to-noise ratio, structured similarity index metric, pixel expansion

1. Introduction

Secret image sharing refers to method for distributing a secret image amongst a group of participants, each of whom is allocated a share of the secret. Secret sharing method divides a secret into some shares called shadow images where each shadow image looks meaningless and individual shares are of no use on their own. The concept of secret sharing scheme was first introduced by Blakley [1] and Shamir [2] independently. Both the schemes were (k, n) secret sharing schemes. Brickell [3] was the first who introduced the notion of ideal structures of secret sharing scheme. A secret sharing scheme is called ideal if the shares are taken from the same domain as the secret. Thien and Lin [4] proposed a (k, n) threshold-based image Secret Sharing Scheme based on Shamir’s Secret Sharing Scheme [2] to generate image shares. Later on Tuyls et al. [5] proposed Secret Sharing scheme for binary images using XOR operation. (n,n), (k,n), (2,n) was proposed by them but (n,n) scheme was ideal with no pixel expansion and precisely reconstructed image. (k,n) and (2,n) had still bad pixel expansion and low contrast. Yi et al. [6] presented two (n, n) schemes for color image. The schemes also have no pixel expansion but the secret image was not precisely reconstructed. Wang et al. [7] proposed (2, n) scheme for binary image using Boolean operation. The scheme has no pixel expansion but contrast was 1/2. Till this the contrast of all the existing (2,n) scheme was not ideal. K.Y. Chao et al. [8] proposed a method to extend (n, n) scheme to (k, n) scheme by using shadows-assignment matrix. Lin Dong and Min Ku [9] proposed a new (n, n) secret image sharing scheme with no pixel expansion. In their scheme reconstruction is based on addition
which has low computational complexity. Lin Dong et al. [10] proposed a (2, n) secret sharing scheme based on Boolean operation. The reconstructed image is totally the same with the original secret image. Their scheme has no pixel expansion and contrast value was ideal. But this scheme requires each participant to store m (m>1) transparencies of equal size. J. P. Singh et al. [11] proposed an image secret sharing method based on some random matrices that acts as a key for secret sharing. The technique allows a secret image to be divided into four image shares with each share individually looks meaningless. Pixel expansion in the above scheme [11] is 1/3.

In this article we have suggested a novel and simple (2, n) secret sharing scheme. In our scheme the reconstructed secret image is absolutely similar with the original secret image, i.e. with contrast of 1. Our scheme has low computational complexity. It requires each participant to store only one share at a time. The proposed (2, n) secret sharing scheme has no pixel expansion and can recover the secret image precisely. The rest of the article is organized as follows: In section 2 we have described the idea of our secret sharing scheme. The results and perfectness of this scheme are given in section 3. Finally, Section 4 summarizes the paper and gives the concluding remarks.

2. Proposed Scheme

Novel (k, n) secret image sharing schemes are proposed in this section.

2.1 Proposed scheme for grayscale images

Our proposed (2,n) secret sharing scheme consists of shares construction phase and revealing phase. The corresponding algorithms are given below.

**Algorithm 1: The Shares construction phase**

Input: A gray-level secret image C of size h × w and one Random matrices R containing values between 0 to 255 of size h × w
Output: Secret images Si, of size h × w, i ∈ {1,…,n}

shareGen ()

for i=1 to (n-1) do {
  Ti = C / (n-1),
  S1=R;
  Si+1=R ⊕ Ti, i ∈ {1, …,n}
}

**Algorithm 2: The Revealing phase**

Input: Secret images Si, of size h × w, i ∈ {1,2,…n}
Output: A gray-level recovered image C’ of size h × w

imageRecons ()

M_i = S_1 ⊕ S_i+1, i ∈ {1, …,n}
C’ = \sum_i M_i

2.2 Proposed schemes for binary and color images

A binary image is an image that has only two possible values for each pixel. Typically the two colors used for a binary image are black and white. Each pixel is stored as a single bit 1 or 0. For binary image, in order to use our proposed scheme, a preprocessing step should be added to convert the binary image to corresponding grayscale image by combining every neighboring 8 bits to 1 byte. Then perform the
proposed scheme for the grayscale image. In revealing phase, a corresponding step should be added to split 1 byte of the revealed grayscale image into 8 bits to get the recovered secret image. For color image, any desired colors can be obtained by mixing primitive colors red (R), green (G) and blue (B). In true color system, R, G and B are respectively represented by 8 bits which can represent 0-255 variation of scale. To extend the proposed schemes for grayscale image to color image, three steps are needed. Firstly, decompose the color image into three components of R, G and B, each of which can be seen as grayscale image. Then perform the proposed scheme for grayscale image to each component R, G and B. Finally, compose R, G and B components to color shares.

3. Experimental Results and Comparison

Experimental results and comparison of the proposed schemes with some other schemes are illustrated in this section.

3.1 Experimental result

*Experiment A:* Construct (2, 4) secret image sharing scheme on grayscale secret image. Experimental results are showed in Fig.1: (a) is the grayscale secret image “lena.jpg”, with size 256 × 256. (b)-(e) are the four shares, $S_1$, $S_2$, $S_3$, $S_4$ generated by using the proposed method; (f) is the image revealed by share 1 and share 2 (g) is the image revealed by first three shares and (h) is the image revealed by all the shares.

![Fig. 1. Experimental results of a (2, 4) secret sharing scheme for grayscale secret image](image)

*Experiment B:* Construct (2, 3) secret image sharing scheme on binary secret image. Experimental results are showed in Fig.2: (a) is the binary secret image “logo.tiff”, with size 200 × 200. (b) is the corresponding grayscale image by combining every neighboring 8 bits to 1 byte. (c)-(e) are the three shares, $S_1$, $S_2$, $S_3$ generated by using the proposed method; (f) is the image revealed image (g) is the corresponding binary image which is identical to (a).
We have used the peak-signal-to-noise ratio (PSNR) to measure the similarity between the original image and reconstructed image (infinity for exact similarity). We have used structured similarity index (SSIM) metric [12] to measure the dissimilarity between secret and their shares. The formula of PSNR is described as follows: 

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE} \text{ dB}$$

MSE is the mean-square error between the original image and the reconstructed image. If the original image is sized $r \times c$, then MSE is defined as,

$$MSE = \frac{1}{r \times c} \sum_{i=1}^{r} \sum_{j=1}^{c} (x_{ij} - y_{ij})^2$$

where $x_{ij}$ and $y_{ij}$ denote the original and recovered pixel values, respectively.

SSIM compares local patterns of pixel intensities that have been normalized for luminance and contrast. SSIM values ranges from 0 to 1. 0 means two images are totally dissimilar and 1 means the reverse one.

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}$$

- $\mu_x$ and $\mu_y$ are the average of $x_{ij}$ and $y_{ij}$ respectively.
- $\sigma_x^2$ and $\sigma_y^2$ the variance of $X$ and $Y$ respectively; $\sigma_{xy}$ the covariance of $X$ and $Y$.
- $c_1=(k_1L)^2$, $c_2=(k_2L)^2$ are two variables to stabilize the division with weak denominator where $L$ the dynamic range of the pixel-values and $K1=0.01$; $k2=0.03$ by default.

PSNR and SSIM values for few binary, gray and color images we have used for our experimentation is given in Table I.

Table 1. PSNR and SSM Values between original image and recovered image

<table>
<thead>
<tr>
<th>Image Name</th>
<th>PSNR VALUES</th>
<th>SSIM VALUES (2,4 scheme)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena.jpg</td>
<td>Infinity</td>
<td>0.037 0.021 0.021 0.067 1</td>
</tr>
<tr>
<td>Lady.jpg</td>
<td>Infinity</td>
<td>0.089 0.017 0.017 0.016 1</td>
</tr>
<tr>
<td>Child.jpg</td>
<td>Infinity</td>
<td>0.078 0.059 0.059 0.045 1</td>
</tr>
<tr>
<td>Duck.jpg</td>
<td>Infinity</td>
<td>0.056 0.053 0.053 0.0524 1</td>
</tr>
<tr>
<td>Baboon.jpg</td>
<td>Infinity</td>
<td>0.0305 0.087 0.087 0.087 1</td>
</tr>
<tr>
<td>Flower.bmp</td>
<td>Infinity</td>
<td>0.011 0.031 0.031 0.108 1</td>
</tr>
<tr>
<td>Logo.tiff</td>
<td>Infinity</td>
<td>0.0425 0.0372 0.0372 0.0435 1</td>
</tr>
</tbody>
</table>

In Table 1 we can see that PSNR values and SSIM values between original secret image and reconstructed secret image generated using our scheme are coming as infinity and 1 respectively, which proves that our secret images and reconstructed images are exactly same. The SSIM values between original secret image and individual share are coming nearly equal to 0. That means that individual share reveals no information about the secret.
Hence, our proposed scheme satisfies the security and accuracy conditions required by any secret sharing scheme. All shares and reconstructed secret image has the same size with the original secret image, thus no pixel expansion. Boolean XOR and addition operation is used to reconstruct the secret image, which has low computational complexity.

3.2 Comparison

To further demonstrate the features of our proposed new category of secret sharing scheme, we have compared our \((2,n)\) scheme with other few popular \((2,n)\) secret sharing schemes in terms of five criteria: contrast, pixel expansion, number of shares held by each participant and reconstruction operation.

Table 2: Comparison of different \((k,n)\) schemes

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Contrast</th>
<th>pixel expansion</th>
<th>number of shares held by each participant</th>
<th>reconstruction operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tuyls [5]</td>
<td>&lt;&lt;1</td>
<td>&gt;&gt;1</td>
<td>1</td>
<td>XOR</td>
</tr>
<tr>
<td>Wang [7]</td>
<td>1/2</td>
<td>1</td>
<td>1</td>
<td>XOR</td>
</tr>
<tr>
<td>Dong [10]</td>
<td>1</td>
<td>1</td>
<td>&gt;&gt;1</td>
<td>XOR, OR</td>
</tr>
<tr>
<td>Proposed</td>
<td>1</td>
<td>1 (for grayscale and color)</td>
<td>1/8 (for binary)</td>
<td>XOR, OR</td>
</tr>
</tbody>
</table>

4. Conclusion

In this paper we have proposed a novel and simple \((2,n)\) secret sharing scheme. The proposed scheme has no pixel expansion and can reconstruct the secret image precisely. This scheme has low computational complexity. The probability of reconstruction of the image from individual shares is very less so this method ensures satisfactory results in the field of security. This scheme can be directly used to share grayscale images. It also can be extended with binary and color images. We will further design general \((k,n)\) secret sharing scheme with ideal contrast.

References