A Lossless Secret Image Sharing Scheme based on Pixel Partitioning

Abstract—Secret sharing method divides a secret into some components called shadow images where each shadow image looks meaningless. Based on this idea, we propose a simple secret image sharing scheme in this article. This scheme is based on bitwise operations. We have used matrix addition and subtraction processes for share generation and reconstruction processes respectively. This technique allows a secret image to be divided as n image shares so that all n image shares have to be used to reconstruct the secret image and any (n−1) or fewer image shares cannot get sufficient information to reveal the secret image. The proposed scheme has no pixel expansion and can reconstruct the secret image precisely. It is an effective, reliable, and secure method to prevent the secret image from being lost, stolen or corrupted. Experimental results prove that the proposed scheme is efficient because of strong security and accuracy.

Keywords - Secret Sharing, Peak Signal-to-Noise Ratio, Structured Similarity Index Metric, Pixel Expansion, Boolean operation XOR

I. INTRODUCTION

Secret images are used in many commercial and military applications. The prime concerns in these applications are the storage and transmission security of certain secret images. To increase the security of secret images, many techniques like traditional encryption, image hiding, watermarking, steganography etc. are proposed in recent years. A common weakness of the entire above-mentioned security techniques viz. image hiding, watermarking and steganography is that the secret image is stored and transmitted as a single unit. If that single unit is somehow captured by an intruder, the secret may not remain secret. Secret sharing method on the other hand divides a secret into some components called shadow images where each shadow image looks meaningless. Secret image sharing is the art and science about the protection of important images by distributed storages. The concept of secret sharing was proposed by Blakley and Shamir independently in 1979. Secret sharing refers to the method of distributing a secret media like image amongst a group of participants. Each participant is allocated a share of the secret that looks meaningless. The secret can be reconstructed only when a sufficient number of shares are combined together. The sharing is performed in such a way that only certain specified subsets of players are able to reconstruct the secret, while smaller subsets have no information about this secret at all. More formally, in a secret sharing scheme there are one-dealer and n players. The dealer accomplishes this by giving each player a share in such a way that any group of k (k ≤ n) or more players can together reconstruct the secret but no group of fewer than k players can reconstruct that secret. Such a system is called a (k, n) threshold scheme. The (k, n) threshold scheme is a scheme designed to break the single master key into n different shadows, so that the shared secret is recoverable from any k : (k ≤ n) shadows and knowledge of (k - 1) or fewer shadows provided absolutely no information about the shared secret. If k is equal to n then this is called (n, n) secret sharing scheme. Based on bitwise operations, in this article we have suggested a novel and simple (n, n) secret sharing scheme. This scheme is absolutely different from any other secret sharing schemes discussed so far. In our scheme the reconstructed secret image is absolutely similar with the original secret image. It is a lossless scheme. We have used addition and subtraction operations for share generation and reconstruction respectively so it has low computational complexity. The proposed (n, n) secret sharing scheme has no pixel expansion and can recover the secret image precisely.

The rest of the article is organized as follows: We briefly describe some notable works done in the area of image secret sharing in section II. In section III, we describe the notations and some definitions related to secret sharing. Our proposed image secret sharing is given in section IV. The experimental set up and results of this scheme are given in section V. Finally, we conclude this article in Section VI.

II. RELATED WORKS

The concept of secret sharing scheme was first introduced by Blakley [1] and Shamir [2] independently. Both the schemes were (k, n) threshold secret sharing schemes. Shamir [2] was using polynomial-based technique to share the secret among n participants and Blakley [1] used a geometric approach. Shamir [2] developed the idea of a (k, n) threshold based secret sharing technique (k ≤ n). The technique allows a polynomial function of order (k − 1) constructed as,

\[ f(x) = d_0 + d_1x + d_2x^2 + \ldots + d_{k-1}x^{k-1}(\text{mod } p) \]
where the value $d_j$ is the secret and $p$ is a prime number. The secret shares are the pairs of values $(x_i, y_i)$ where $y_i = f(x_i)$, $1 \leq i \leq n$ and $0 \leq x_1 < x_2 \ldots < x_n \leq p - 1$.

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 one can 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. Blakley's [1] technique assumes that secret is in a point in a k-dimensional space. Hyper planes intersecting at this point are used to construct the shares. Coefficients of $n$ different hyper planes constitute the corresponding $n$ shares. Karin et al. [3] suggested the concept of perfect secret sharing (PSS) where zero information of the secret is revealed for an unqualified group of $(k-1)$ or fewer members. The unqualified group cannot obtain any information about the secret and the unqualified group cannot reconstruct the secret with some information. Brickell [4] 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. Later on the concept of multi secret sharing scheme was proposed by Jackson et al. [5]. In a multi-secret sharing scheme multiple secrets are generated and distributed during one secret sharing process. This scheme has several applications. First is to protect several secrets with the same amount of data usually needed to protect one secret. Second is to partition one large secret into $n$ pieces with these pieces protected with a smaller amount of data than is needed to protect the entire secret. According to Jackson et al. [5] secret sharing schemes were classified in two groups: the onetime-use scheme and the multi-use scheme. In a onetime use scheme, the secret holder must redistribute fresh shadows to each participant once some particular secrets have been reconstructed. On the other hand, in a multi-use scheme, the secret holder does not need to redistribute fresh shares. The shadows owned by one participant still remain secret to others, even after multiple secret-reconstruction operations have been performed. In 2002, Thien and Lin [6] proposed a $(k, n)$ threshold-based image secret sharing scheme by cleverly using Shamir’s secret sharing scheme [5] to generate image shares. The best part of their work was that $n$ secret shares can be used to recover any $k$ image shares from an $1 \times 1$ pixels secret image (denoted as I) as,

$$S_i(i, j) = I(ik + 1, j) + I(ik + 2, j)x \ldots + I(ik + k, j)x^{k-1} \mod p$$

where $0 \leq i \leq \lceil L/k \rceil$ and $1 \leq j \leq 1$. This method reduces the size of image shares to become $1/k$ of the size of the secret image. Any $k$ image shares are able to reconstruct every pixel value in the secret image. Thien and Lin also provided some research insights for lossless image recovery using their technique. Bai [7] developed a secret sharing scheme using matrix projection. The idea is based upon the invariance property of matrix projection. This scheme can be used to share multiple secrets. Although the reconstructed images in these schemes can be revealed by simply stacking the collected shadows but the pixel expansion problem occurred. Later on Tuyls et al. [8] proposed $(n, n)$ Secret Sharing (SS) scheme for binary images with no pixel expansion and precisely reconstructed image. Pixel expansion is an important factor for hardware requirements. Yi et al. [9] 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. [10] proposed $(n, n)$ scheme for grayscale image. The scheme has no pixel expansion and gives an exact reconstruction. All schemes in [8], [9] and [10] are constructed based on Boolean operation, which need bit-wise operation when sharing gray scale and color images. To reconstruction an image without distortion is an important issue. All the secret images are very important and valuable specially medical, military and artistic images. Every bit may be significant in those sensitive images. The reconstruction process can be applied to the secret sharing mechanism to preserve the fidelity of the secret sharing image. To share a lossless secret image, the schemes [11], [12] used two pixels to represent the exceeding gray values. Nevertheless, this results in the expansion of the secret image and may reduce the shared capacity as well as distort the quality of the shadow image. Nowadays all the devices or sensors have certain amount of computing power. Complex computation is not a major problem. Thus, how to develop secret sharing scheme with low computation complexity and high contrast is worth to study. As $(n, n)$ secret sharing scheme is a special case of $(k, n)$ secret sharing scheme. It is also important to construct $(k, n)$ secret sharing scheme. K.Y. Chao et al. [13] proposed a method to extend $(n, n)$ scheme to $(k, n)$ scheme by using shadows assignment matrix. Lin Dong and Min Ku [14] 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. Chen and Wu [15] presented an efficient $(n+1, n+1)$ multi-secret image sharing scheme based on Boolean operations which not only keep the secret images confidential but also increase the capacity of sharing multiple secrets. The Boolean-based VSS technology, used to encode the secret images, generates $n$ random matrices; then the $n$ secret images are subsequently encoded into the $n+1$ meaningless share images. The best part of their work was that secret images can be hid by means of sharing only $n+1$ share images instead of $2n$ share images as in traditional methods. Thus, their scheme has the combined benefit of reducing the image transmission bandwidth and management overhead of meaningless share images without any significant extra computational cost. J. P. Singh et al. [16] 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. The share generation algorithm works by converting three pixels of the secret image to one pixel each of four different shares based on four random matrices. So, each share is reduced by $1/3rd$ of the original secret image.

III. NOTATIONS AND DEFINITIONS

In this section, we will give some denotations and facts that are necessary in our scheme. Consider a secret image A of size $R \times C$. Each pixel of A can take any one of $C$ different colors or gray-levels. Image A is represented by an integer matrix A:
A = [aij] RxC , where i = 1, 2, . . . , R, j = 1, 2, . . . , C, and aij Є {0, 1, . . . , c − 1}.

We have c = 2 for a binary image, and c = 256 for a grayscale image with one byte per pixel. In a color image with one byte per pixel, the pixel value can be an index to a color table, thus c = 256. In a color image using an RGB model, each pixel has three integers: R (red), G (green) and B (blue). If each R, G or B takes value between 0 and 255, we have c = 2563. This integer matrix is also called A and will be treated as equivalent to the secret image A itself.

Definition: The (k, n) secret sharing scheme divides a secret image A into n shares S1, S2, . . . , Sn. Such that the following conditions are satisfied

Condition 1: The secret S is recoverable from any k shares, i.e., for any set of k indices, H(S|S1, S2, . . . , Sk)=0

Condition 2: Knowledge of k-1 or fewer shares provides absolutely no information about S, i.e., for any set of k-1 indices, H(S|S1, S2, . . . , Sk-1)=H(s)

The first condition is called precision or accuracy and the second condition is called security. When k = n then it is the definition of (n, n) secret sharing scheme.

IV. PROPOSED SECRET SHARING SCHEME

A. Proposed scheme for grayscale images

In our proposed scheme we have first converted each pixel of the secret image C into corresponding 8 bit binary values. Then we have created four groups taking two pixels in each group. For example say one pixel value of an image is 155. As (155)10 = (10110111)2. We have divided this value in four groups as given in Table 1.

<table>
<thead>
<tr>
<th>Table I: Partitioning of a pixel value</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Next, we convert each group’s binary value to corresponding decimal values. We keep the decimal value of B1 in a temporary matrix T1. Similarly the values of B2, B3 and B4 are kept in temporary matrices T2, T3 and T4 respectively. A random integer matrix having values from 0 to 255 for 8 bit grey level image is created. The random matrix is our first share. The second share is generated from random matrix R and first temporary matrix T1 by XORing them. The second share is generated from sum of T1 and T2 and R and so on. The detail process is outlined in the algorithm (i).

1) Share Generation Algorithm

Input: A gray-level secret image C of size h x w and one Random matrices R containing values 0 to 255 of size h x w.

Output: Secret shares S1: 1 ≤ i ≤ 5 of size h x w

shareGen()
{
    for each pixel
        Divide pixel in block of 4 groups B1, B2, B3 and B4
        for i = 1 to 4 do

    T1 = (B3)10
    S1 = R
    S2 = T1, R
    S3 = (T1 + T2) R
    S4 = (T1 + T2 + T3 + T4) R
}

The share reconstruction phase is just the reverse of share construction. First of all we create four random matrices by XORing different combination of S1 and M5 as given in algorithm ii. Then we rearrange the binary values of M5’s to get back the reconstructed image. The details process of image reconstruction form shares is given in algorithm 2.

2) Reconstruction Algorithm

Input: Secret shares Si: 1 ≤ i ≤ 5 of size h x w

Output: A gray-level recovered image C’ of size h x w

imageRecons()
{
    M1 = S1
    M2 = S2
    M3 = S3
    M4 = S4

    for each cell of M1
        Place the binary value in order of M1, M2, M3 and M4 in C’
}

B. Proposed schemes for binary and color image

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.

V. EXPERIMENTAL RESULTS

We have done our experimentation in Matlab 7.0 running on Microsoft Windows XP system with a Pentium Dual Core
For our experiment, we have used different images like: Lady.jpg, Child.jpg, Baboon.jpg, Lena.jpg, duck.jpg etc. The graphical results of two images called Lena and baboon images are shown here. For other images, we have given their properties in Table 1 and Table 2. The reconstructed images with all shares are exactly same as the original image.

**Example 1:** Figure 1 shows an application of our proposed secret sharing scheme. In this example we have taken n=5. Figure 1(a) is the grayscale secret image “lena.jpg”, with size 256x256. Figure (b)-(f) are the five shares generated using the proposed method. All the shares are of size 256x256. Figure (g) is the image reconstructed by all the shares, which is identical to (a). Figure (h) to Figure (j) is the reconstructed images generated from four out of five shares, three out of five shares, and two out of five shares respectively. The images of Figure (h) to Figure (j) give nothing about the secret image.

**Example 2:** Figure 2 shows an application of our proposed secret sharing scheme. In this example we have taken n=5. Figure (a) is the grayscale secret image “baboon.jpg”, with size 256x256. Figure (b)-(f) are the five shares generated using the proposed method. All the shares are of size 256x256. Figure (g) is the image reconstructed by all the shares, which is identical to (a). Figure (h) to Figure (j) is the reconstructed images generated from four out of five shares, three out of five shares, and two out of five shares respectively. The images of Figure (h) to Figure (j) give nothing about the secret image.

We have used the peak-signal-to-noise ratio (PSNR) to measure the loss of reconstructed image compared to original image. To measure the similarity between the original secret and reconstructed image as well as the dissimilarity between secret and their shares, we have used structured similarity index metric. The peak-signal-to-noise ratio (PSNR) is used to measure the image qualities of the shadow images. The formula of PSNR is described as follows

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

where MSE is the mean-square error between the cover image and the stego image. If the cover image is sized \( r \times c \), 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. MSE and PSNR are the most widely used video quality metrics during last 20 years.

The structural similarity (SSIM) index is designed to improve on traditional metrics like PSNR and MSE, which have proved to be inconsistent with human eye perception. It is basically a method for measuring the similarity between two images. The SSIM index is a full reference metric, in other words, the measuring of image quality based on an initial uncompressed or distortion-free image. SSIM compares local patterns of pixel intensities that have been normalized for luminance and contrast [17].

SSIM is defined as,

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

Where \( x \) and \( y \) denote the original and recovered image, respectively

\[
\mu_x \text{ the average of } x_{ij};
\]

\[
\mu_y \text{ the average of } y_{ij};
\]

\[
\sigma_x^2 \text{the variance of } X;
\]

\[
\sigma_y^2 \text{the variance of } Y;
\]

\[
\sigma_{xy} \text{ the covariance of } X \text{ and } Y;
\]

\[
c_1 = (k_1L)^2, c_2 = (k_2L)^2 \text{ two variables to stabilize the division with weak denominator};
\]

\[
L \text{ the dynamic range of the pixel-values (typically this is } 2^{\text{bit depth per pixel}} - 1);
\]

\[
K1=0.01 \text{ and } K2=0.03 \text{ by default}
\]
The resultant SSIM index is a decimal value between 0 and 1, and value 1 is only reachable in the case of two identical sets of data. The PSNR values for different images and their shares we have used for our experimentation is given in Table II. It can be seen from Table II that the PSNR values are infinity for reconstruction with 5 out of 5 shares. But for reconstructions with fewer shares results in PSNR values less than 8. The SSIM values between different images and their shares are listed in Table III. The SSIM values are very close to 0, which is an indication that there is hardly any relationship among the different shares, which is one of the major objectives of secret sharing. These results prove the security and accuracy of our scheme.

Figure 2. (a) baboon image, (b) – (f) shares of Baboon image, (g) reconstructed image using all five shares, (h) reconstructed image using first four shares, (i) reconstructed image using first three shares, (j) reconstructed image using first two shares
<table>
<thead>
<tr>
<th>Image Name</th>
<th>S_{1}+S_{2}</th>
<th>S_{1}+S_{2}+S_{3}</th>
<th>S_{2}+S_{3}</th>
<th>S_{1}+S_{2}+S_{3}</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena.jpg</td>
<td>Infinity</td>
<td>7.49</td>
<td>6.12</td>
<td>5.75</td>
</tr>
<tr>
<td>Lady.jpg</td>
<td>Infinity</td>
<td>7.54</td>
<td>5.94</td>
<td>5.60</td>
</tr>
<tr>
<td>Child.jpg</td>
<td>Infinity</td>
<td>7.43</td>
<td>6.06</td>
<td>5.55</td>
</tr>
<tr>
<td>Duck.jpg</td>
<td>Infinity</td>
<td>7.62</td>
<td>6.09</td>
<td>5.80</td>
</tr>
<tr>
<td>Baboon.jpg</td>
<td>Infinity</td>
<td>7.65</td>
<td>5.91</td>
<td>5.54</td>
</tr>
<tr>
<td>Flower.bmp</td>
<td>Infinity</td>
<td>7.58</td>
<td>5.96</td>
<td>5.45</td>
</tr>
<tr>
<td>Logo.tif</td>
<td>Infinity</td>
<td>7.49</td>
<td>6.15</td>
<td>5.49</td>
</tr>
</tbody>
</table>

**TABLE III : SSIM VALUES**

<table>
<thead>
<tr>
<th>Image Name</th>
<th>S_{1}</th>
<th>S_{2}</th>
<th>S_{3}</th>
<th>S_{4}</th>
<th>S_{5}</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena.jpg</td>
<td>0.025</td>
<td>0.067</td>
<td>0.053</td>
<td>0.047</td>
<td>0.034</td>
</tr>
<tr>
<td>Lady.jpg</td>
<td>0.053</td>
<td>0.029</td>
<td>0.030</td>
<td>0.025</td>
<td>0.029</td>
</tr>
<tr>
<td>Child.jpg</td>
<td>0.048</td>
<td>0.039</td>
<td>0.082</td>
<td>0.055</td>
<td>0.043</td>
</tr>
<tr>
<td>Duck.jpg</td>
<td>0.056</td>
<td>0.049</td>
<td>0.044</td>
<td>0.037</td>
<td>0.034</td>
</tr>
<tr>
<td>Baboon.jpg</td>
<td>0.030</td>
<td>0.015</td>
<td>0.016</td>
<td>0.015</td>
<td>0.015</td>
</tr>
<tr>
<td>Flower.bmp</td>
<td>0.065</td>
<td>0.053</td>
<td>0.044</td>
<td>0.062</td>
<td>0.023</td>
</tr>
<tr>
<td>Logo.tif</td>
<td>0.087</td>
<td>0.055</td>
<td>0.039</td>
<td>0.059</td>
<td>0.073</td>
</tr>
</tbody>
</table>

From Table II we can see that PSNR values between original secret image and reconstructed secret image generated using our scheme is coming as infinity, which proves that our secret images and reconstructed images are exactly same. From Table III 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.

**VI. CONCLUSION**

In this paper we have proposed a novel and simple secret sharing scheme based on Pixel Partitioning. 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 is applicable to all types of images namely: (i) binary, (ii) gray scale and (iii) color images. Our next endeavor is to generalize this scheme to make it (k, n) secret sharing scheme with ideal contrast.

**REFERENCES**