Secret Image Sharing Scheme Based on Pixel Replacement

Tapasi Bhattacharjee[1] and Jyoti Prakash Singh[2]

[1] Techno India, Salt Lake, Kolkata, India
tapasi.dgp@gmail.com
[2] National Institute of Technology Patna, Bihar, India
jyotip.singh@gmail.com

Abstract. Dividing an image in several components and sharing through different channel is popular way of sharing and storing sensitive image data. We proposes here a simple image secret sharing method based on random matrices. These random matrices act as key for secret sharing. The technique allows a secret image to be divided into three image shares where each share individually looks meaningless. To reconstruct the secret image all three shares have to be used. This method has no pixel expansion and can reconstruct the secret image precisely. This scheme can be directly applied on gray scale images and can easily be extended to binary and color images. Experimental results prove that this scheme can generate good quality of reconstructed images.

Keywords: Secret sharing, Visual Secret Sharing, Security, Structured Similarity Index Metric, Peak Signal to Noise Ratio.

1 Introduction

With the development of network technology, information can be distributed and transmitted over the internet rapidly and conveniently. Replicating the important information will offer more chances to intruders to gain access to it. On the other hand, having only one copy of the information means that if this copy is destroyed there is no way to retrieve it. Thus, there is a great need to keep information in a secure and reliable way. Hence, secret sharing came to use. Secret sharing method divides a secret into some shares called shadows, where each shadow looks meaningless and individual shares are of no use on their own. These shadows are distributed to the participants. Only a set of qualified participants can recover the secret, while the non-qualified participants can not even get a clue of the secret information. 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] used polynomial-based technique to share the secret among n participants and Blakley [1] used a geometric approach. Shamir's technique creates a $(k > 1)$ degree polynomial with random coefficients in the range $(0 \cdots p)$, where p is a prime number. The constant term of this polynomial is the secret message. Lagrangian interpolation

K. Singh, A.K. Awasthi, and R. Mishra (Eds.): QSHINE 2013, LNICST 115, pp. 517–526, 2013.

technique is used for the reconstruction of the secret from any k or more shares. Blakley's [1] technique assumes that secret is 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 n shares. Karnin 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. 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. Cimato et al. [5] proposed (n,n) threshold Visual Secret Sharing (VSS) schemes. But this scheme had the disadvantages of pixel expansion and low contrast. Thien and Lin [6] proposed a (k,n) threshold-based image Secret Sharing Scheme based on Shamir's Secret Sharing Scheme [2] to generate image shares. This method reduces the size of image shares to become $\frac{1}{k}$ of the size of the secret image. 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 scheme for binary images with no pixel expansion and precisely reconstructed image. 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 gray scale 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 share a lossless secret image, the schemes [11,12] used two pixels to represent the exceeding gray values. Nevertheless, this resulted in the expansion of the secret image and reduced the sharing capacity as well as distort the quality of the shadow image. Chao et al. [13] proposed a method to extend (n,n) scheme to (k,n) scheme by using shadows-assignment matrix. Dong and 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. Singh et al. [15] 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 looking 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 $1/3^{rd}$ of the original secret image. Peng Li et al. [16] proposed (n,n) visual secret sharing scheme without distortion by computation and get a better visual quality of the reconstructed image. But pixel expansion problem was still a major problem in this scheme.

We propose here a simple secret image sharing scheme based on two random matrices. The random matrices was used to scramble the pixel positions of the original secret images. For this scrambling operation, first random matrix give the row value and second random matrix give the column value where to place the pixel of the original secret image. This scheme has no pixel expansion and can reconstruct the secret image precisely. The proposed scheme can be directly applied on gray scale images and can be easily extended on binary and color images.

The rest of the paper is organized as follows: section 2 describes the idea of the proposed scheme. The results of this scheme and comparisons with other similar works are discussed in section 3. Finally, Section 4 summarizes the paper and gives the concluding remarks.

2 Proposed Scheme

Our proposed secret sharing scheme is discussed in this section. Our sharing algorithm is divided into two phases: Sharing phase and Reconstruction phase. Each phase is discussed in the following section with examples.

2.1 Sharing Phase

The pixels of the original secret image A is scrambled with the help of two random matrices, R_1 and R_2 to generate another image S_3. The random matrices R_1 and R_2 are considered as first two shares S_1, S_2 and the generated image is considered as the third share S_3. The pixel value of $(i,j)^{th}$ location of actual secret image is placed to (x,y) location of the third share S_3 if that location is not holding any other pixel value. The x value is the content of $(i,j)^{th}$ location of R_1 matrix whereas y is value of $(i,j)^{th}$ location of R_2 matrix. If $(x,y)^{th}$ location of S_3 is already occupied by some other pixel then we generate a random pair (x',y') and check if that location of S_3 is free. If it is not free, we choose another random pair and check it again. This process is repeated till we get (x',y') value which is a free position in S_3. When such (x',y') is found, we assign the $A[i,j]$ to $S_3[x',y']$. The corresponding location of random matrices are also updated by assigning $R_1[i,j] = x'$, and $R_2[i,j] = y'$. For an example, say the first position $(0,0)^{th}$ of the secret image is 136 and $(0,0)^{th}$ position of R_1 and R_2 matrices are 100 and 50 respectively. 136 is placed at $(100,50)^{th}$ position of a new matrix, S_3 which is the third share of the proposed scheme. Sat the 2^{nd} pixel value $(0,1)^{th}$ of the A, R_1 and R_2 are 116, 80, 100 respectively. Then 116 will be placed at $(80,100)^{th}$ location of S_3 matrix. This process will continue for all the pixel values of A which gives three shares S_1, S_2 and S_3. The share generation algorithm is given below in pseudo-code.

Share Generation Algorithm
Input: A gray-level secret image A of size $h \times w$ and two Random matrices R_1 and R_2 containing values between 0 to 255 of size $h \times w$
Output: Three shares S_1, S_2 and S_3 of size $h \times w$

```
$S_1 = R_1$ and $S_2 = R_2$
```

```
for i=1 to h do {
   for j=1 to w do {
      $X = R_1[i, j]$
      $Y = R_2[i, j]$
      if ($S_3[X, Y] == 0$)
         $S_3[X, Y] = A[i, j]$
      else {
         $X' = rand()$
         $Y' = rand()$
         while($!is\_blank\_position(X', Y')$){
            $X' = rand()$
            $Y' = rand()$
         }
         $S_3[X', Y'] = A[i, j]$
         $R_1[i, j] = X'$
         $R_2[i, j] = Y'$
      }
   }
}
```

2.2 Revealing Phase

In revealing phase, all the three shares, S_1, S_2 and S_3 are considered as three input images. Values at $(0, 0)^{th}$ positions of S_1 and S_2 matrices are accessed first. Say these are X' and Y' respectively. Then the value which is stored at (X, Y) position of S_3 matrix is stored as 1st pixel value of a new matrix, A'. Say the first values of location $(0, 0)^{th}$ of S_1 and S_2 are 100 and 50 respectively. The value stored at $(100, 50)^{th}$ location of S_3 matrix is 136. This value, 136 is set as 1^{st}, $(0, 0)^{th}$ pixel value of a matrix, A. Similarly the value of location $(0, 1)^{th}$ of S_1 and S_2 matrices are 80 and 100 respectively. The value stored at $(80, 100)^{th}$ location of S_3 matrix (116) set as $(0, 1)^{th}$ pixel value of A'. This process continues for all the values of S_1 and S_2 matrices. The complete reconstruction algorithm is given below in pseudo-code

Reconstruction Algorithm
Input: Three shares S_1,S_2 and S_3 of size $h \times w$
Output: A gray-level recovered image A' of size $h \times w$

```
for i=1 to h do {
   for j=1 to w do {
      $A[i, j] = S_3[S_1[i, j], S_2[i, j]]$
   }
}
```

2.3 Complexity Analysis

The time complexity of our share generation algorithm in best case is $O(n^2)$ because it just scans the original secret image once and places the pixels to another image S_3. In worst case, the time complexity turns out to be $O(n^4)$ because the while loop may run for $O(n^2)$ time for searching for a blank position. In average case it will be $O(n^2)$ only as it will find the blank position to a nearby position in finite number of steps. The time complexity of reconstruction algorithm is always $O(n^2)$.

2.4 Proposed Scheme for Binary and Colour Images

A binary image has only two possible values for each pixel: black and white which can be represented by a single bit only. To use our proposed scheme on binary images, the binary images are converted to gray scale image by combining neighbouring 8 bits to 1 byte. Now the proposed scheme for grayscale image can be applied on binary images. In revealing phase, a corresponding step should be added to split 1 byte of the revealed gray scale image into 8 bits to get the recovered secret image. A color image can be represented as three gray scale images corresponding to each color plane red, green and blue. To extend the proposed schemes for color images, decompose the color image into three components of R, G and B, each of which can be seen as grayscale images. Then perform the proposed scheme for grayscale image to each component R, G and B separately. Finally, compose R, G and B components are combined together to generate color shares.

3 Experimental Results

This section presents and analysis the experimental results by using the proposed method. Top evaluate the performance of our new scheme, we have used eight different images. The images are Lena.jpg, Airplane.jpg, Flower.jpg, Baboon.jpg, Duck.bmp, Child.bmp, Lady.jpg and Logo.tiff. The codes were developed in Matlab 7.0 running on Microsoft Windows XP system with a Pentium Dual Core Processor. Due to space limitations, the graphical result of two images are shown here. Our first secret image is a gray scale image of Duck shown Fig. 1 of size 150 × 170. Fig. 2, Fig. 3 and Fig. 4 are the three shares, S1, S2 and S3 each of size 150 × 170 generated by our algorithm. Fig. 5 is the recovered image of size 150 × 170 obtained by our algorithm.

Our second secret image is Lena image of size 512 × 512 which is shown in Fig. 6. The share generated by our proposed algorithm is shown in Fig. 7, 8 and 9. The shares are also of size 512 × 512. The reconstructed image obtained by the combining all three share images is shown in Fig. 10.

Our proposed technique is not lossless because some pixels of original image can not be written to third share because we can not get a free position in third share. But the visual quality of recovered image obtained by our algorithm is

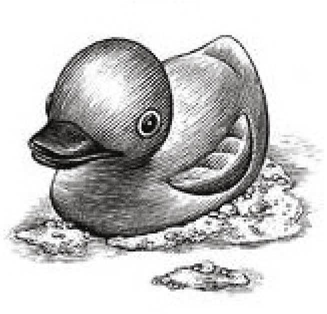

Fig. 1. The Duck image

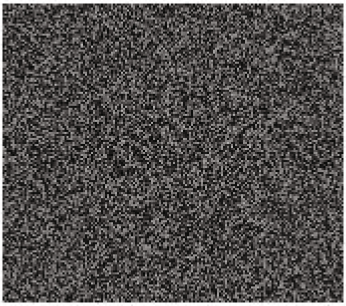

Fig. 2. First share of Duck

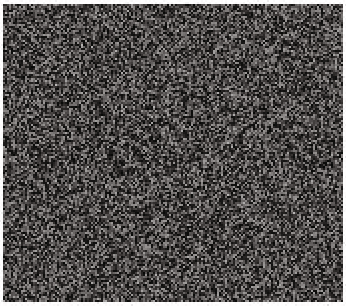

Fig. 3. Second share of Duck

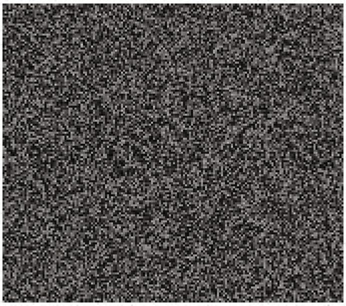

Fig. 4. Third share of Duck image

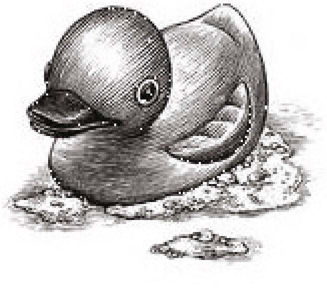

Fig. 5. The recovered Duck

good enough. To check the visual quality of the output images, we have used peak-signal-to-noise ratio (PSNR) metric which is defined as

$$PSNR = 10 \times log \frac{255^2}{MSE} \tag{1}$$

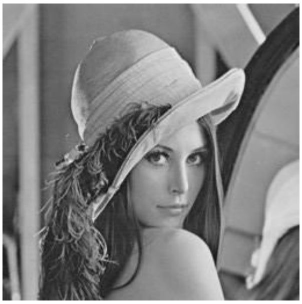

Fig. 6. The Original Lena image

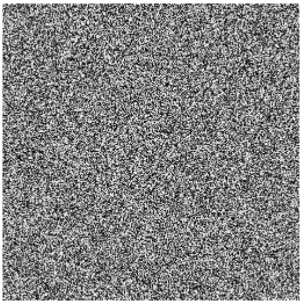

Fig. 7. First share of Lena

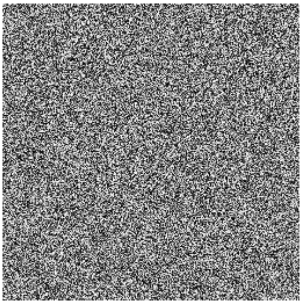

Fig. 8. Second share of Lena

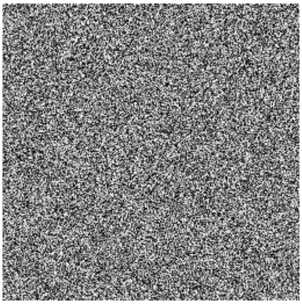

Fig. 9. Third share of Lena

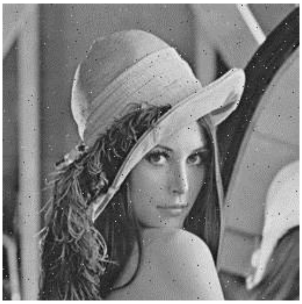

Fig. 10. The recovered Lena image

where

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (h_{i,j} - h'_{i,j})^2, \tag{2}$$

where $h_{i,j}$ is the pixel value of the original image and the $h'_{i,j}$ is the pixel value of the recovered image. MSE is the Mean Squared Error.

Table 1. The PSNR values and standard deviation of different secret images

Image Name	PSNR	Std. Deviation
Lena.jpg	31.36	58.9
Airplane.jpg	33.56	44.44
Flower.jpg	31.44	52.38
Baboon.jpg	26.52	69.92
Duck.bmp	29.76	60.39
Child.bmp	34.10	38.42
Lady.jpg	21.36	86.19
Logo.tiff	13.68	116.43

The PSNR values for various images we have used for our experimentation is given in Table 1. As one can see from Table 1 that the PSNR on different images range from 18 to 31. To find out the reason for this variation of PSNR, we studied the statistical properties of images. We found that for those images whose standard deviation is large, the PSNR is low whereas fro those images whose standard deviation is low, the PSNR is high. Our algorithm works well on those images whose standard deviation is low. The other criterion of secret sharing scheme is that none of the shares should posses any information about the original secret but the recovered image should be similar to the original secret. Structural Similarity Index Metrics (SSIM) is such a metrics for measuring the similarity between two images. SSIM compares local patterns of pixel intensities that have been normalized for luminance and contrast [17]. SSIM is defined as,

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{3}$$

Where x and y denote the original and recovered image, respectively.
μ_x the average of x_{ij};
μ_y the average of y_{ij};
σ_x^2 the variance of X;
σ_y^2 the variance of Y;
σ_{xy} the covariance of X and Y;
$c_1 = (k_1L)^2$, $c_2 = (k_2L)^2$ two variables to stabilize the division with weak denominator;
L the dynamic range of the pixel-values (typically this is $2^{\#bits/pixel} - 1$);
$K_1 = 0.01$ and $k_2 = 0.03$ 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 SSIM values for various shares and reconstructed images with their respective images is given in Table 2. The SSIM value of each individual share of every image is very low signifying that shares do not reveal any information about the original secret. The SSIM values of reconstructed images are nearly 1 signifying that the reconstructed images are similar to original images.

Table 2. The SSIM values for different of shares and reconstructed image with secret images

Image Name	Share1	Share2	Share3	Recons Image
Lena.jpg	0.0479	0.0558	0.1179	0.9985
Airplane.jpg	0.0704	0.1015	0.0565	0.8995
Flower.jpg	0.0090	0.0047	0.0047	0.9557
Baboon.jpg	0.0626	0.0508	0.1928	0.9593
Duck.bmp	0.0737	0.2683	0.0298	0.9930
Child.bmp	0.0102	0.0113	0.0384	0.9564
Lady.jpg	0.0093	0.0030	0.0059	1
Logo.tiff	0.0508	0.0395	0.0261	0.9817

3.1 Comparison with Similar Works

We have compared our proposed scheme to other similar published works in terms of contrast, pixel expansion, and reconstruction operation. As one can see from table 3 that our scheme is better than existing schemes in terms of contrast ratio. We achieve a contrast ration of 1. In terms of reconstruction, we use pixel replacement whose algorithmic complexity is $O(n^2)$ only.

Table 3. Comparison of different secret sharing schemes

Category	Contrast	Pixel Exp	Reconstruction
Yi [9]	≤ 1	1	XOR
Cimato [5] & Li [16]	$\ll 1$	$\gg$1	OR (Stacking)
J.P.Singh [15]	$\ll 1$	$\frac{1}{3}$	Bitwise
Proposed Scheme	1	1	Pixel Replacement

4 Conclusion

In this paper we have proposed a simple secret sharing scheme based on two random matrices which can generate three shares. The proposed scheme does not increase the size of the secret image by expanding pixels. The individual shares do not reveal any information about the original secret image. This scheme can be directly used to share gray scale images. It also can be extended with binary and color images. We also find a relationship of image statistical properties with our sharing scheme. Our scheme gives better results for images whose standard deviation is low. We are in the process of extending this scheme to (k, n) secret sharing scheme with ideal contrast.

References

1. Blakley, G.R.: Safeguarding cryptographic keys. AFIPS NCC 48, 313–317 (1979)
2. Samir, A.: How to share a secret. Communications of ACM 22(11), 612–613 (1979)
3. Karnin, E.D., Greene, J.W., Hellman, M.E.: On secret sharing systems. Information Theory 29(1), 35–41 (1983)
4. Brickell, E.F.: Some ideal secret sharing schemes. J. Comb. Math. Comb. Comput. 6, 105–113 (1989)
5. Cimato, S., De Prisco, R., De Santis, A.: Optimal colored threshold visual cryptography schemes. Designs Codes and Cryptography 35(3), 311–315 (2005)
6. Thien, C.C., Lin, J.C.: Secret image sharing. Computers and Graphics 26(5), 665–670 (2002)
7. Bai, L.: A strong ramp secret sharing scheme using matrix projection. In: 2nd Intl. Workshop on Trust, Security and Privacy for Ubiquitous Computing, pp. 656–660. IEEE (2006)
8. Tuyls, P., Hollmann, H.D.L., van Lint, J.H., Tolhuizen, L.: Xor-based visual cryptography schemes. Designs Codes and Cryptography 37, 169–186 (2005)
9. Yi, F., Wang, D.S., Luo, P., Dai, Y.Q.: Two new color (n, n)-secret sharing schemes. Journal on Communications 28(5), 30–35 (2007)
10. Wang, D., Zhang, L., Ma, N., Li, X.B.: Two secret sharing schemes based on boolean operations. Pattern Recognition 40(10), 2776–2785 (2007)
11. Chang, C.C., Hsieh, Y.P., Lin, C.H.: Sharing secrets in stego images with authentication. Pattern Recognition 41(10), 3130–3137 (2008)
12. Zhao, R., Zhao, J.J., Dai, F., Zhao, F.Q.: A new image secret sharing scheme to identify cheaters. Computer Standards and Interfaces 31(1), 252–257 (2009)
13. Chao, K.Y., Lin, J.C.: Secret image sharing: a boolean-operations based approach combining benefits of polynomial-based and fast approaches. International Journal of Pattern Recognition and Artificial Intelligence 23(2), 263–285 (2009)
14. Dong, L., Ku, M.: Novel (n, n) secret image sharing scheme based on addition. In: 6th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 583–586 (2010)
15. Singh, J.P., Nag, A., Bhattacharjee, T.: Random matrices based image secret sharing. International Journal of Advanced Research in Computer Science 2(4), 104–108 (2011)
16. Li, P., Ma, P.-J., Su, X.-H., Yang, C.-N.: Improvements of a two-in-one image secret sharing scheme based on gray mixing model. Journal of Visual Communication and Image Representation 23(3), 441–453 (2012)
17. Wang, Z., Bovik, A.C.: Image quality assessment: From error visibility to structural similarity. IEEE Transactions on Image Processing 13(4), 600–612 (2004)