International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Verifiable Secure Secret Image Sharing Scheme

Angel Rose A[1], Sinu Maria Kurian[2]

[1,2]Department of Computer Science, SJCET Palai, Kerala, India

Abstract: ***Many visual secret sharing schemes for digital images have been developed in recent years. The new progressive secret sharing scheme for grayscale images proposed in this paper is based on a combination of bit-plane slicing of an image and equation based secret sharing scheme. First, n*n secret image and n*n cover images are decomposed into bit-plane images. Then higher bit-plane images of the both are utilized to produce shadows. The proposed scheme progressively recovers the secret. After collecting all shadow images, the secret image can be completely recovered.***

Keywords: Secret Image sharing, Bit-plane slicing

1. Introduction

In cryptography, Secret sharing refers to a method for distributing a secret amongst a group of participants, each of which is allocated a share of secret. Secret sharing was developed in 1979 by Shamir [1] and Blakley [2], who presented two different methods to construct a threshold scheme,one is based on the Lagrange interpolating polynomial and the other is based on linear projective geometry.

In a secret sharing scheme, a dealer is responsible for creating shares of secret, known as shadows of the secret data, and distributing these shadows to the participants. By using a secret sharing scheme, secret data can be protected among a finite set of participants in such a way that only pre-determined, valid subsets of participants can cooperate to recover the secret data, and no unqualified subset of participants can get any information about the secret data.

2. Proposed Method

Our proposed secret image sharing scheme consists of two phases: Shadow construction phase and Revealing phase. Detailed Description of each phase is mentioned below.
Input: Original Secret Image, Cover Image
Output: Eight Shadow Images
Steps are as follows:

1) Decompose the 8-bit gray-level original secret image into eight bit-planes
2) Similarly, decompose the 8-bit gray-level cover image into eight bit-planes
3) Input higher 8th bit-plane of both secret and cover images into shadow-pair construction procedure so that we obtain a pair of shadow corresponds to 8th bit-plane
4) Do the step 4 for the next three higher bit-planes and obtain shadow pairs

Shadow-Pair Construction Procedure

Input: An H×W k th Bit-plane of secret image I = (I_{ij}), and H × W k th Bit-plane of cover image C= (C_{ij}), where i = 0, 1, · · · , H - 1 and j =0, 1, · · · , W – 1, k=8, 7, 6, 5 (higher bit planes)

Output:Two H × W shadow images
$Shadow^1=S^A_{ij}$ and $Shadow^2=S^B_{ij}$
where i = 0, 1, · · · , H - 1 and j =0, 1, · · · , W – 1

Step 1: Set i = 0 and j = 0, which means that the first pixels of both I and C are considered. Read pixels from I and read pixel from C

Step 2: Obtain pixel of shadow S^A by computing

$$\mathbf{Shadow^1_{ij}= \lfloor((I_{ij}\times 2 + C_{ij}+ 1)mod4)=2\rfloor} \quad (1)$$

Step 3: Find the value for pixel of shadow S^B, using the formula

$$Shadow^2{}_{ij}= (I_{ij}\times 2 + C_{ij}+ 1) \bmod 2 \quad (2)$$

Repeat Steps 2 and 3 until all pixels are processed. The outputs of this algorithm are two shadows, $Shadow^1$ and $Shadow^2$. This shadow doesn't reveal information of secret.

A. Revealing Phase

Input: Eight Shadow Images
Output : Original Secret Image
Steps are as follows:

1. Input the shadow-pair corresponds to 8th bit-plane to secret revealing procedure and obtain 8th bit-plane of secret
2. Do the step 1 for the next three higher bit-planes and obtain corresponding bit plane of secret
3. Combine the bit-planes images of secret to reconstruct the original secret image

Secret revealing procedure

Input : An H×W k th Bit-plane of $shadow^1$ = ($S^A{}_{ij}$), and
H × W k th Bit-plane of $shadow^2$ = ($S^B{}_{ij}$),

where i = 0, 1, · · · , H - 1 and j =0, 1, · · · , W – 1 k=8, 7, 6, 5 (higher bit planes)
Output: H × W k th Bit-plane image of secret I' = (I'_{ij})

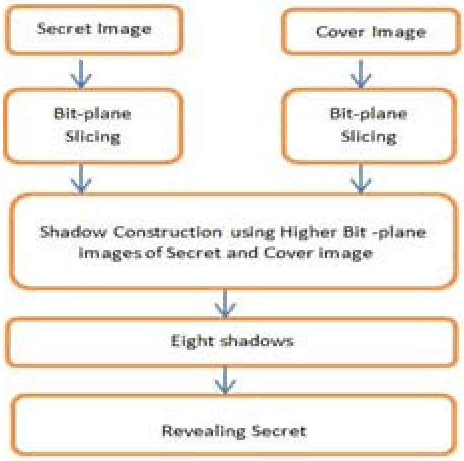
Step 1: Set i = 0 and j = 0, which means that the first pixels of both $shadow^1$ and $shadow^2$ are considered. Read pixels from S^A and read pixel from S^B

Step 2: Obtain pixel of secret I' by computing

$$I'_{ij} = \lfloor((shadow^1_{ij} \times 2 + shadow^2_{ij} + 1)mod4)=2\rfloor \quad (3)$$

Repeat Steps 2 until all pixels are processed. The outputs of this algorithm are k^{th} bit-plane image of secret.

Flow chart of the proposed scheme is shown below



3. Experiments

The experimental result presented in this section demonstrates the performance of our proposed scheme. To conduct the experiment, two 512×512 grayscale images "baboon" (secret image) and "lena" (cover image) were used. Our proposed scheme was implemented in Matlab 7.12.

Figure 1 (a): below shows the result of bit-plane slicing over secret image, baboon.png (512×512)

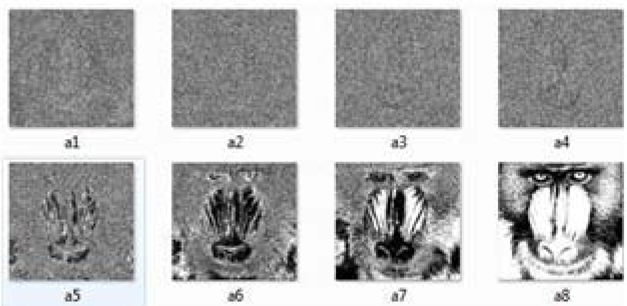


Figure 1 (a): Eight bit-plane image of "lena"

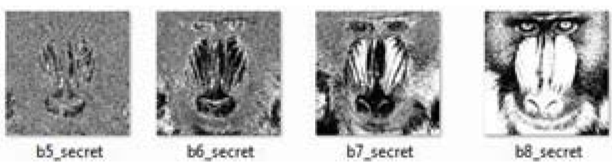


Figure 1: (b) shows the result of bit-plane slicing over cover image, lena.png (512×512)

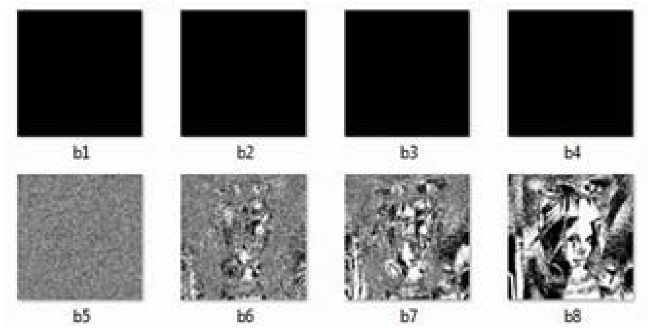


Figure 1: (a) Eight bit-plane image of "baboon"

Out of eight bit-plane images obtained, only higher bit-plane images carries information related to the actual image. From the above observation, in our scheme we considered four higher bit-plane images of both secret image (a4-a8) and cover image (b4-b8) and obtained two shadows corresponding to each higher plane. Resulted shadows are shown in Fig. 2

Figure 2 (a): shadow 1 of four higher bit-plane obtained

Figure 2 (b): shadow 2 of four higher bit-plane obtained

Upon revealing phase we input these shadows and obtain the higher bit-planes of secret image. Resulting 4 higher bit-plane of secret is shown in Fig. 3.These biplane can progressively combined to obtain the secret. When all the bit-plane are combined, the secret is exactly reconstructed.

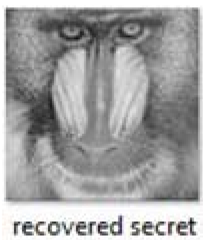


Figure 3: 4 higher bit-plane of secret image

Peak Signal to Noise Ratio is used to evaluate the image quality of the reconstructed grayscale image. In general, a higher PSNR means that the quality of the reconstructed image is better.

Basically, PSNR value should range from 30dB to 40dB if a scheme offers good visual quality.

$$PSNR = 10 \times \log_{10} (255^2/MSE) \quad (4)$$

where MSE is the mean square error between the original image and reconstructed image. For an original grayscale image with a size of H×W, the corresponding MSE is defined in Equation (5).

$$MSE(Q) = \frac{1}{W\times H} \sum_{X=1}^{W} \sum_{Y=1}^{H} (Q_{xy} - Q'_{xy})^2 \qquad (5)$$

4. Conclusion

In this paper, we proposes a new secret sharing scheme applicable to grayscale images based on equation based visual secret sharing and bit-plane slicing . The proposed (8,8) visual secret sharing scheme is capable of accurately reconstruct the secret image . During final stage of revealing phase we make use of only 4 critical shadows to recover the secret .So in future we can work on this scheme to improve security and add verification capability against cheating problems.

References

[1] A. Shamir, How to share a secret, Communications of the Association for Computing Machinery, vol. 22, no. 11, pp. 612-613
[2] G. R. Blakley, Safeguarding cryptographic keys, Proc. of National Computer Conference, American Federation of Information Processing Societies, pp. 313-317, 1979
[3] Zhi-hui Wang ,"Sharing a Secret Image in Binary Images with Verification", Journal of Information Hiding and Multimedia Signal Processing, Ubiquitous International, 2011
[4] R. Lukac, and K. N. Plataniotis, Bit-level based secret sharing for image encryption, Pattern Recognition, vol. 38, no. 5, pp. 767-772, 2005
[5] C. N. Yang, and C. S. Laih, New colored visual secret sharing schemes,
[6] Designs, Codes and Cryptography,vol. 20, no. 3, pp. 325-335, 2000.
[7] http://www .datahide.com/BPCS
[8] M. Naor and A. Shamir, Visual cryptography, Lecture Notes Computer Science, vol. 50, pp. 1-12,1995
[9] G. J. Simmons, An introduction to shared secret and/or shared control schemes and their application, Contemporary Cryptology, The Science of Information Integrity, IEEE Press, New York, 1992
[10] D. Jin, W. Q. Yan, and M. S. Kankanhalli, Progressive color visual cryptography, Journal of Electronic Imaging, vol. 14, 2005