International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Volume 1 Issue 10 (November 2014) www.ijirae.com

Improved Visual Secret Sharing Scheme for Cryptographic Application

[1]L.sudha, [2] B.R.K Singh
[1]*M.Tech Student of DVR & DHS MIC College of Technology, DECS, Kanchikacharla, AP-India,*
[2]*Assistant Professor, ECE Dept., DVR & DHS MIC College of Technology, Kanchikacharla, India,*

Abstract- Visual secret sharing has received more and more attention over the past few years. Currently Weakly secure (WS) VSS schemes are consider but the back drop is that the share image does not have any meaning and the pixel expansion is done in the generated secret image. Pixel expansion and the quality of the reconstructed secret image has been a major issue of visual secret sharing (VSS) schemes. So, considering the issue of sharing the secret image at multiple image resolutions with the meaningful shadows and non-expanding of the pixels this paper presents a progressive visual secret sharing scheme without expanding the image size in shadows and in reconstructed secret image.

Keywords—Visual secret sharing, Pixel expansion, multiple image resolution

I.INTRODUCTION

Secret sharing, which is one of the oldest and most important issues in cryptography, can enable a secret, such as the cryptographic key, to be shared and protected among a group of participants. The concept of a (t, n) - threshold-based mechanism for secret sharing, where $t \leq n$, was individually pioneered by Blakley and Shamir in 1979 in a way that the secret can be divided into 'n' shares (or participants), and any t or more shares can cooperate to reconstruct the secret, while any (t−1) or fewer shares reveal absolutely no information about the secret. Certainly, since the secret is not held any longer in only one location or by a single person, but is divided into 'n' parts for 'n' participants, the probability that the secret is destroyed intentionally or is lost accidentally due to a single misfortune can be reduced. In addition, the danger of security is also reduced because not many copies of the secret are made. On the other hand, collecting any t parts instead of the total n parts to reconstruct the secret can achieve both safety and convenience. So far, many extended secret sharing schemes have been released over the past several decades. For example, there are some multi-secret sharing schemes to share multiple secrets during a secret-sharing procedure. In addition, some verifiable secret sharing schemes were developed to identify the cheaters. However, due to the fact that the computer technology facilitates the development of electronic devices such as digital cameras, digital images have been widely used in many applications. Consequently, the secret sharing mechanism exposes the security problem relating to the protection of secret images such as military, commercial, and private images. Therefore, protecting image-based secrets becomes a critical issue in secret sharing. In general, there are two common approaches to deal with this issue. One approach is polynomial-based secret image sharing, which embeds the pixels of the secret image into the coefficients of the polynomials so as to be used to generate the noise-like images, namely shadows (or shares), for a group of participants. This approach can provide better or distortion-free visual quality in the reconstructed secret image. This paper proposes the Visual secret sharing scheme for gray scale images. Gray scale images are the images that have a range of shades of gray without apparent color. The darkest possible shade is black, which is the total absence of transmitted or reflected light. The lightest possible shade is white, the total transmission or reflection of light at all visible wavelengths.

II. PROPOSED SYSTEM

This system is proposed for the goal of making no pixel-expansion in both the shadows and the reconstructed halftone secret image and also using the meaningful shadows to recover the halftone secret image.

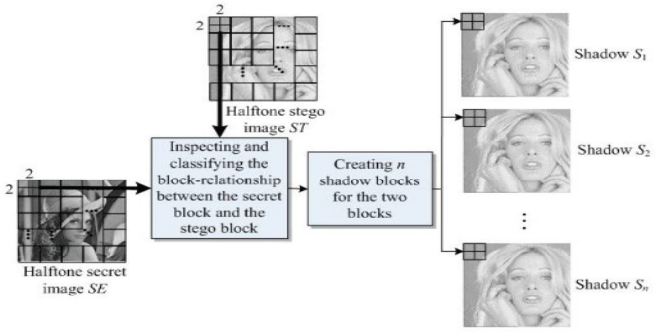


Fig. 1 Proposed sharing method

The proposed sharing scheme applies a 2×2-sized, block-wise operation to inspect the block relationship between the secret block in the secret image and the stego block in the stego image and to generate the corresponding shadow blocks according to the type of the block relationship. A flowchart that shows the proposed sharing method is presented in Fig.1. Let the halftone secret image and the halftone stego image be denoted as SE and ST, respectively. And, let the two images SE and ST have the same size, i.e., $m_1 \times m_2$. In addition, for generality, let the image SE be split into n shadows (i.e., $S_1, S_2, \cdots, S_n$) for n participants.

A. BLOCK DIAGRAM

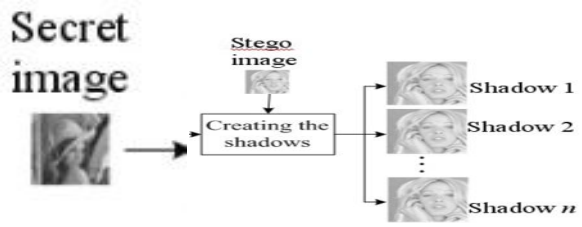


Fig. 2 Block Diagram

Fig. 2 shows the block diagram of the approach. Fig. 3 is the secret image which is to be sent.

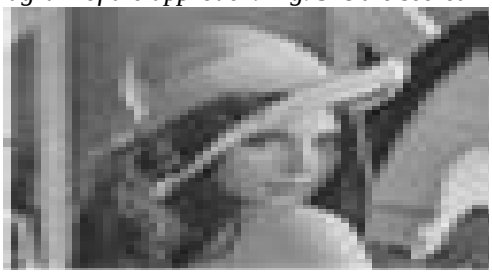


Fig. 3 Secret Image

Fig. 4 is the stego image. This stego image is used to protect the secret image. The stego image is placed on the secret image. So, that who sees this image they visualize other image but not the secret image inside it.

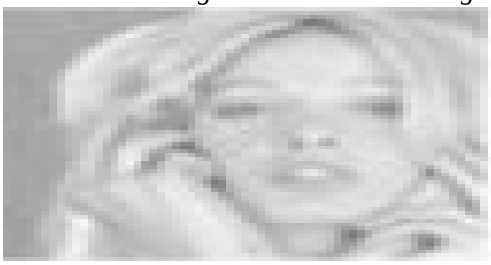


Fig. 4 Stego Image

B. *Classifying The Block Relationship*

1) *If the number of black pixels in the compared block is larger than or equal to 2 the block relationship of the two blocks belong to the type-1.*
2) *If there is only one black pixel in the compared block , the block relationship of the two blocks belong to type-2.*
3) *If there are no black pixels in the compared block , the block relationship of the two blocks belong to type-3.*

The Fig. 5 shows the compared blocks of secret and stego images.

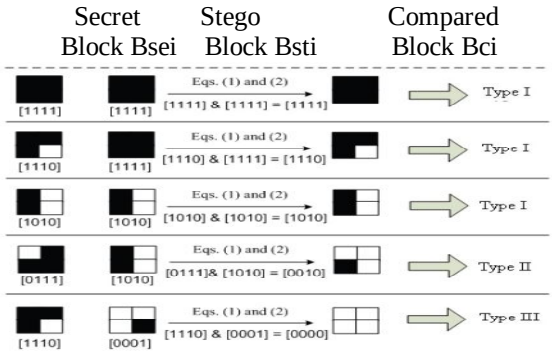


Fig. 5 Compared Blocks of secret and stego blocks

C. *Creating Three Shadow Blocks*

The proposed scheme creates n shadow blocks sized 2×2 pixels for the two blocks Bse_i and Bst_i by depending on the type of their block relationship. If the block relationship of the two blocks Bse_i and Bst_i is Type I, then the generation of each shadow block is that any two black pixels are randomly chosen from the compared block Bc_i as the corresponding black pixels in the shadow block. Accordingly, each shadow block consists of two black pixels and two white pixels. If the block relationship between the two blocks Bse_i and Bst_i belongs to Type II, then each shadow block is created by two steps. In the first step, when there is only one black pixel in the compared block Bc_i, the pixel is always chosen as the corresponding black pixel in the shadow block. In the second step, a quality factor, defined as $Q_f=1/q$ with $q\geq 1$, is used in the proposed scheme to decide whether or not another one black pixel is randomly chosen from the secret block Bse_i as another corresponding black pixel in the shadow block. Here, when Q_f is equal to 1, the proposed scheme executes the selection as described above. It is noted that the pixel to be randomly selected from the secret block Bse_i must be located at a position that is different from the position of the black pixel in the compared block. Consequently, each shadow block also comprises two black and two white pixels. Obviously, because the proposed scheme chooses another black pixel at random from the secret block Bse_i to construct a shadow block during the sharing procedure, the information of the secret block may be completely exposed when more shadow blocks are stacked together. In contrast, when Q_f is smaller than 1, not every shadow block needs to do such a selection for construction. More precisely, for each shadow block, the probability that another one black pixel is chosen from the secret block Bse_i to be another corresponding black pixel in the shadow block is 1/q. It is obvious that some shadow blocks can have a slight degradation of image quality because the stego block is not totally destroyed. If the two blocks Bse_i and Bst_i have a Type III block relationship, then each shadow block is also generated by two steps. In the first step, because the two blocks are dissimilar to each other and in order to maintain the characteristic shape of the stego block in the shadow blocks, any one black pixel is randomly chosen from the stego block Bst_i as the corresponding black pixel in the shadow block. In the second step, the proposed scheme also uses the quality factor Q_f to decide whether or not another one black pixel is randomly chosen from the secret block Bse_i to be another corresponding black pixel in the shadow block.

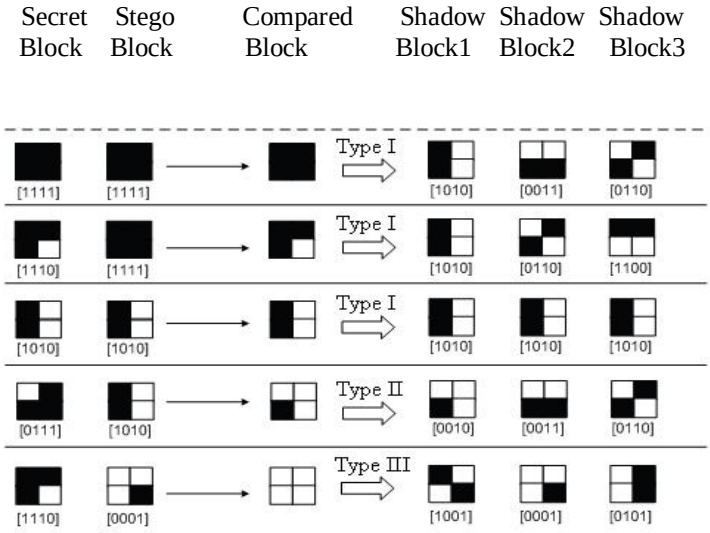
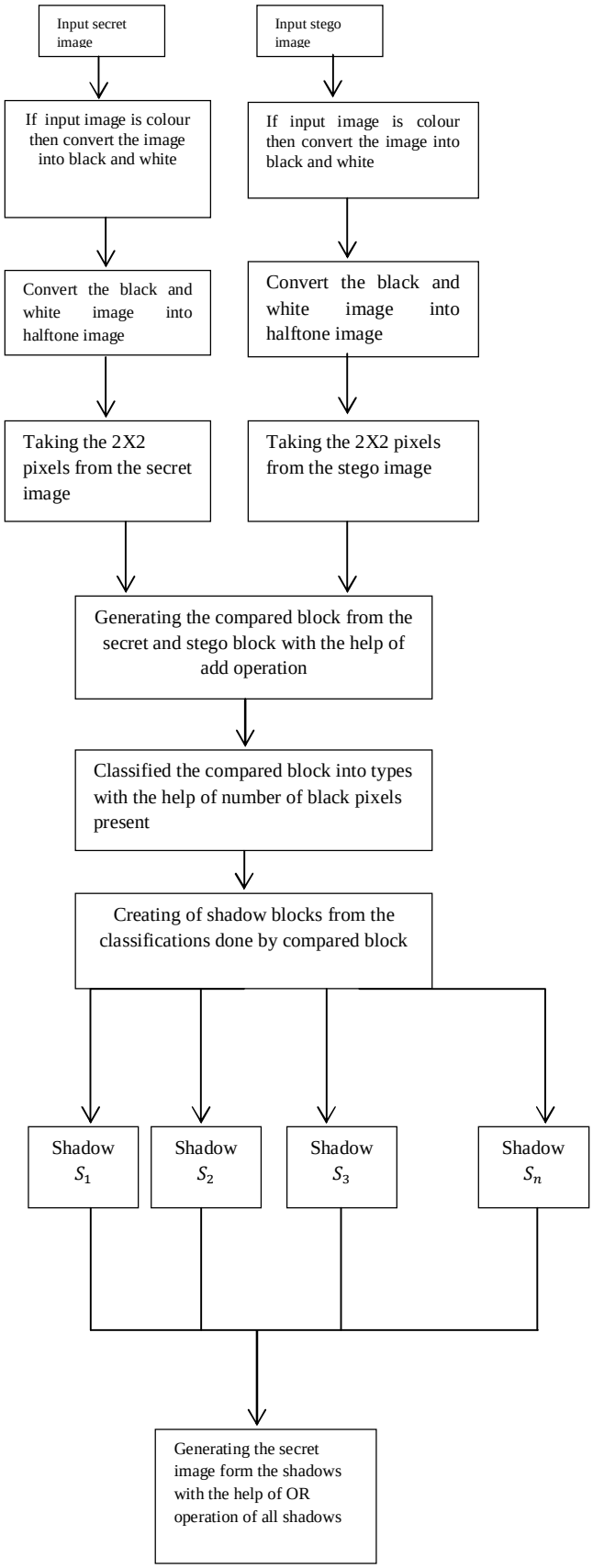


Fig 6 Shows different shadow blocks for respective compared blocks of secret and stego blocks.

D. *Algorithm*



Secret Image

Fig. 7 Secret Image

Stego Image

Fig. 8 Stego Image

Halftone Secret Image

Fig. 9 Halftone Secret Image

Halftone Stego Image

Fig. 10 Halftone Stego Image

Shadow Images

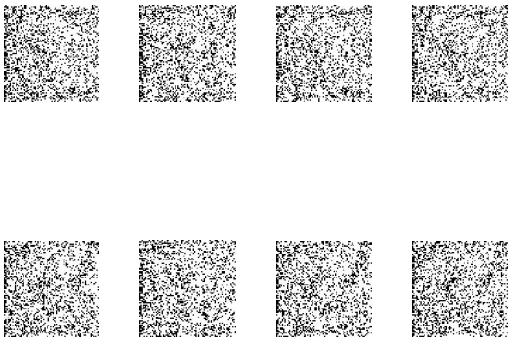


Fig. 11 Shadow Images

Halftone Output image

Fig. 12 Halftone Output Image

Output Image

Fig. 13 Output Image

IV. ADVANTAGES

1. *The generated shadows are meaningful, and their sizes are not expanded.*
2. *The secret image can be recovered at different resolutions by stacking different quantities of shadows together.*

V. APPLICATIONS

1. *Used in military.*
2. *Used in industries and companies.*

VI. CONCLUSION

In this paper, a progressive visual secret sharing scheme with the property of friendly management is proposed. Herein, a 2×2-sized, block-wise operation is applied to map each secret block into an equal-sized block in each shadow such that the proposed scheme is non-expansible. In addition, by inspecting the block relationship between each secret block and the corresponding stego block and by producing all the shadow blocks according to the type of block relationship, the proposed scheme can maintain the characteristics of the stego image and simultaneously ensure that the secret image can be exposed with different image resolutions after the stacking action. The experimental results also show that the proposed scheme achieved better performance than the compared methods.

REFERENCES

[1] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. of the National Computer Conf.*, New York, 1979, pp. 313–317.
[2] A. Shamir, "How to share a secret," *Communications of ACM*, vol. 22, no. 11, pp. 612–613, 1979.
[3] H.-Y. Chien, J.-K. Jan, and Y.-M. Tseng, "A practical (*t*, *n*) multi-secret sharing scheme," *IEICE Trans. on Fundamentals of Electronics, Communications and Computer Science*, vol. E83-A, no. 12, pp. 2762–2765, 2000.
[4] C.-C. Yang, T.-Y. Chang, and M.-S. Hwang, "A (*t*, *n*) multi-secret sharing scheme," *Applied Mathematics and Computation*, vol. 151, no. 2, pp. 483–490, 2004.
[5] M. H. Dehkordi and S. Mashhadi, "An efficient threshold verifiable multi-secret sharing," *Computer Standards & Interfaces*, vol. 30, no. 3, pp. 187–190, 2008.
[6] R.-J. Hwang and C.-C. Chang, "An on-line secret sharing scheme for multi-secrets," *Computer Communications*, vol. 21, no. 13, pp. 1170−1176, 1998.
[7] J. Shao and Z. Cao, "A new efficient (*t*, *n*) verifiable multi-secret sharing (VMSS) based on YCH scheme," *Applied Mathematics and Computation*, vol. 168, no. 1, pp. 135–140, 2005.
[8] J. Zhao, J. Zhang, and R. Zhao, "A practical verifiable multi-secret sharing scheme," *Computer Standards & Interfaces*, vol. 29, no. 1, pp. 138–141, 2007.
[9] C.-C. Chang, Y.-P. Hsieh, and C.-H. Lin, "Sharing secrets in stego images with authentication," *Pattern Recognition*, vol. 41, no. 10, pp. 3130–3137, 2008.
[10] J.-B. Feng, H.-C. Wu, C.-S. Tsai, and Y.-P. Chu, "A new multi-secret images sharing scheme using Largrange's interpolation," *Journal of Systems and Software*, vol. 76, no. 3, pp. 327–339, 2005.
[11] C.-C. Thien and J.-C. Lin, "Secret image sharing," *Computers & Graphics*, vol. 26, no. 5, pp. 765–770, 2002.
[12] Y.-S. Wu, C.-C. Thien, and J.-C. Lin, "Sharing and hiding secret images with size constraint," *Pattern Recognition*, vol. 37, no. 7, pp. 1377–1385, 2004.
[13] C.-N. Yang, T.-S. Chen, K.-H. Yu, and C.-C. Wang, "Improvements of image sharing with steganography and authentication," *Journal of Systems and Software*, vol. 80, no. 7, pp. 1070–1076, 2007.
[14] Y.-C. Hou, "Visual cryptography for color images," *Pattern Recognition*, vol. 36, no. 7, pp. 1619–1629, 2003.
[15] N. Noar and A. Shamir, "Visual cryptography," in *Advances in Cryptology: Eurocrypt'94*, Berlin: Spring-Verlag, Germany, 1995, pp. 1–12.
[16] D. R. Stinson, "Visual cryptography and threshold schemes," *IEEE Potentials*, vol. 18, no. 1, pp. 13–16, 1999.
[17] S. J. Shyu, "Efficient visual secret sharing scheme for color images," *Pattern Recognition*, vol. 39, no. 5, pp. 866–880, 2006.
[18] C.-N. Yang and T.-S. Chen, "Aspect ratio invariant visual secret sharing schemes with minimum pixel expansion," *Pattern Recognition*, vol. 26, no. 2, pp. 193–206, 2005.
[19] C.-N. Yang and T.-S. Chen, "Reduce shadow size in aspect ratio invariant visual secret sharing schemes using a square block-wise operation," *Pattern Recognition*, vol. 39, no. 7, pp. 1300–1314, 2006.
[20] W.-P. Fang, "Friendly progressive visual secret sharing," *Pattern Recognition*, vol. 41, no. 4, pp. 1410-1414, 2008.
[21] D. Jin, W.-Q. Yan, and M. S. Kankanhalli, "Progressive color visual cryptography," *Journal of Electronic Imaging*, vol. 14, no. 3, pp. 033019.1–033019.13, 2005.
[22] C.-C. Thien and J.-C. Lin, "An image-sharing method with user-friendly shadow images," *IEEE Trans. on Circuits and Systems*, vol. 13, no. 12, pp. 1161–1169, 2003.
[23] C.-N. Yang, K.-H. Yu, and R. Lukac, "User-friendly image sharing using polynomials with different primes," *International Journal of Imaging Systems and Technology*, vol. 17, no. 1, pp. 40–47, 2007.
[24] W.-P. Fang, "Friendly progressive visual secret sharing," *Pattern Recognition*, vol. 41, no. 4, pp. 1410–1414, 2008.

