Visual Secret Sharing Using Cryptography

Shital B. Pawar, Prof.N.M.Shahane

K.K.W.I.E.E.R, Nashik, Maharashtra India

bhandareshital@yahoo.com ,nmshahane@yaho.com

Abstract*— *The Visual Cryptography Scheme (VCS) is a kind of secret sharing scheme that focuses on sharing secret images. The basic idea of the visual cryptography scheme is to split a secret image into number of random shares (printed on transparencies) which separately reveals no information about the secret image other than the size of the secret image. The secret image can be reconstructed by stacking the shares. The underlying operation of this scheme is logical OR operation. The Embedded Extended Visual Cryptography Scheme (EEVCS) uses meaningful covering shares. The scheme EEVCS can be implemented by embedding random shares of secret image into meaningful cover images.The halftoning method is used to convert the gray scale image into binary image. After Studying existing Dithering technique of half toning, Otsus Thresholding method is proposed. Least Significant Bit (LSB) matching steganography technique is used to hide the secret pixel information into the covering images.Related works on visual cryptography scheme are also investigated and it was observed that visual quality of recovered secret images are low by using existing dithering halftone based EEVCS techniques.Including Otsus Thresholding method for halftoning of an image can produce bright image in a better way. LSB matching steganography is a useful method to hide the secret image. This research aims at employing LSB matching steganography with Otsu's method to develop an efficient EEVCS system. Index Terms - **Embedded extended visual cryptography scheme, Otsu's Method, Dithering technique, Least Significant bit, Visual cryptography Scheme.**

IntroductionTHE basic principle of the visual cryptography scheme (VCS) was first introduced by Naor and Shamir. VCS is a kind of secret sharing scheme [1], [2] that focuses on sharing secret images. The idea of the visual cryptography model proposed in [3] is to split a secret image into two random shares (printed on transparencies) which separately reveals no information about the secret image other than the size of the secret image. The secret image can be reconstructed by stacking the two shares. The underlying operation of this scheme is logical operation OR. In this paper, we call a VCS with random shares the traditional VCS or simply the VCS. In general, a traditional VCS takes a secret image as input, and outputs shares that satisfy two conditions: 1) any qualified subset of shares can recover the secret image; 2) any forbidden subset of shares cannot obtain any information of the secret image other than the size of the secret image. An example of traditional (2,2)-VCS is shown in Fig. 1.In the scheme of Fig. 1, shares (a) and (b) are distributed to two participants secretly, and each participant cannot get any information about the secret image, but after stacking shares (a) and (b), the secret image can be observed visually by the participants. VCS has many special applications, for example, transmitting military orders to soldiers who may have no cryptographic knowledge or computation devices in the battle field.

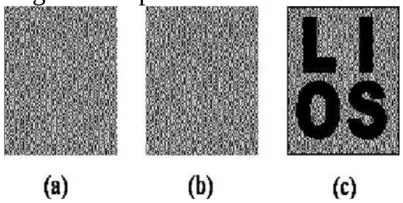


Fig. 1. Example of traditional (2, 2)-VCS with image size 128 128

Visual cryptography scheme eliminates complex computation problem in decryption process, and the secret images can be restored by stacking operation. This property makes visual Cryptography useful especially for the low computation load requirement.

2 EXISISTING SYSTEMS

The existing method of VCS uses dithering technique to generate halftoned images. The problem of black ratio is introduced in this method. Unfortunately, these embedded EVCS techniques are sensitive to image noise, quality and have less visual quality. On the other hand, Dithering method of halftoning to convert into binary image are robust to noise.The EVCS using halftoning technique can treat gray-scale input share images[3]. Zhou et al. [3]made use of the complementary images to cover the visual information of the share images. EVCSs includes an error diffusion halftoning technique [19] to obtain shares with good visual quality. The method has limitations such as the visual quality of the recovered secret image is decreased.

In Visual Cryptography Scheme (VCS) there are five phases i.e. halftoning, shrare Generation, Embedding secret, Extracting secret, reveal secret. Halftoning is used to convert the grayscale image to binaty image.Shares are generated from binary image depending on scheme chosen.There are two methods to generate shares.First method is General Access Structure (n, n) for which n shares are required to reconstruct the secret.The second method is Threshold Access Structure (k, n) where k number of shares will recover the secret from available n shares where k is less than or equal to n. Cover images are halftoned to generate covering shares.Secret image is embedded into cover image. Reconstructed shares are generated from the embedded shares.

3. PROPOSED SYSTEM

VCS using cryptography is the method which uses Otsus Threshold method to generate halftone image.Where LSB matching steganography is used to generate embedded shares(EM).Key is used to generate the offset value. It converts the secret data into number of bits.Read each pixel of the cover image.If the LSB of the next cover pixel matches the next bit of secret data then do nothing else it adds or subtract one from the cover pixel value at random.By decrypting the shares original shares are recovered and stacked together to reveal secret image. To recover the secret, embedded shares are desteganograph with the help of key and reverse procedure is applied to reveal the secret. Performance of the system is measured by using PSNR and MSE parameters.

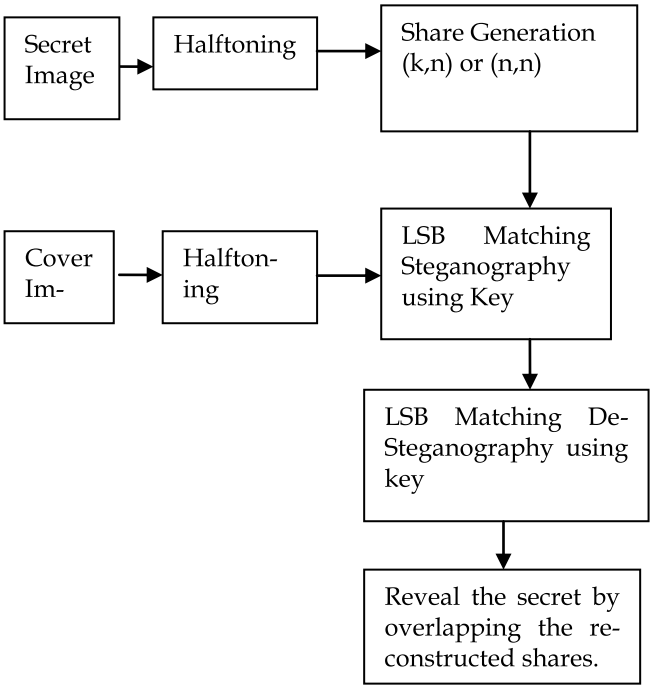

Secret Image
Halftoning
Share Generation (k,n) or (n,n)
Cover Im-
Halfton-ing
LSB Matching Steganography using Key
LSB Matching De-Steganography using key
Reveal the secret by overlapping the re-constructed shares.

Figure 2: Proposed Method

Secret image is halftoned to generate binary image(BI).Depending on scheme the original shares(OS) are generated.With the help of key original shares are embedded into cover images to generate embedded shares(ES). Reconstruct shares (RS) from embedded share with the help of same key.To reveal the secret overlap the reconstructed shares.Otsus method is used for halftoning and LSB matching is used to generate steganograph image.

4. EXPERMENTS AND RESULTS

To evaluate the performance of proposed system we have implemented Cryptography based VCS using Otsus Threshold method and LSB matching steganography. LSB steganography is a powerful method to convey the secret data

Database:
Images shown in Figure 3 are of type .png and of dimension 512x512 .The size of each image is different. The TEST is the secret image of type jpeg and size 2.95 KB.

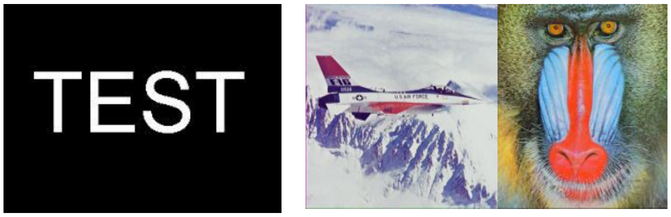


Figure 3: Database Images

Figure 4 shows the embedded shares of size 121KB and 123 KB respectively.

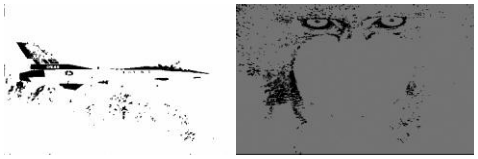
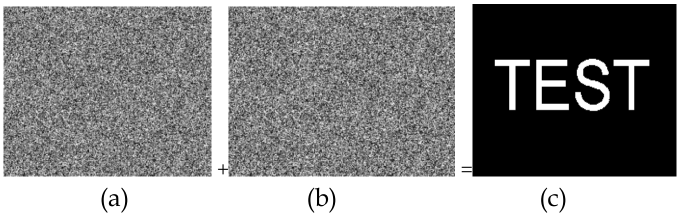


Figure 4: Embedded Shares

After Desteganography the reconstructed shares are generated which are of same size i.e. 36.9 KB with previous original shares.



(a) (b) (c)

Figure 5: (a) Reconstructed Share1 (b) Reconstructed Share2 (c) Resulted Secret by overlapping (a) and (b)

The method mentioned in [1] shows the PSNR values of embedded share 1and embedded share 2 are 9.54db and 0.51db respectively. By using this method the PSNR values of embedded share 1 and embedded share 2 are 9.93db and 5.53db.Experimental result shows that the proposed method is more effective than existing system.

5. Conclusion

This paper has presented the analysis of Otsus threshold method and LSB matching steganography algorithm for addressing the challenging problem of visual quality of embedded shrares in cryptography based visual secret sharing system.

The proposed method not only increases the visual quality of recovered secret but also gives better results. It also improves the PSNR as compared to other methods.

5 REFERENCES

i. *Feng Liu,Chuankun Wu Embedded Extended Visual Cryptographic Schemes, Vol.6,No.2 IEEE Transaction on Information Forensics ans Security, June 2011.*

ii. *M. Naor and A. Shamir, Visual cryptography in Proceeding. EUROCRYPT 94,Berlin, Germany,vol.950, Springer-Verlag, LNCS,1995.*

iii. *Z. Zhou, G. R. Arce, and G. Di Crescenzo, Halftone visual cryptography,Vol.58,No.7 IEEE Transaction on Image Processessing ,Aug. 2006.*

iv. *C. Blundo, A. De Bonis, and A. De Santis, Improved schemes for visual cryptography,vol. 24, Designs, Codes and Cryptography,2001.*

v. *G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, Visual cryptography for general access structures, vol. 129, No. 7 Information Computation, 1996.*

vi. *Haibo Zhang,Xiaofei Wang,Wanhua Cao,Youpeng Huang, Visual cryptography for general access structure by Multi-pixel Encoding with Variable Block Size, Pages340 - 344 Knowledge Acquisition and Modeling, 2008.*

vii. *P. A. Eisen and D. R. Stinson, Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels, vol. 25 Designs, Codes and Cryptography, 2002.*

viii. *S. Droste,New results on visual cryptography,vol. 1109 in Proc. CRYPTO 96 ,Springer-Verlag Berlin LNCS,1996.*

ix. *G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, Extended capabilities for visual cryptography,vol. 250 ACM Theoretical Computer Science 46,2001.*

x. *D. S. Wang, F. Yi, and X. B. Li,On general construction for extended visual cryptography schemes,vol. 42 Pattern Recognition,2009.*

xi. *L. A. MacPherson,Grey Level Visual Cryptography for General Access Structures, Volume 1, Issue 4, Master Thesis, University ofWaterloo,Waterloo,Canada, 2002*

xii. *C. C. Lin and W. H. Tsai, Visual cryptography for gray-level images by dithering techniques, Vol. 24 Issue 8 Pattern Recognit. Lett, October 2003*

xiii. *P.S.Revenkar,Anisa Anjum Survey of Visual Cryptography Schemes, Vol.4 Issue 2 International Journal of Security and its Applications,April 2010.*

xiv. *Andrew Ker Steganalysis of LSB matching in grayscale images, Vol. 12 Issue 8IEEE Signal processing Letters, January 2005.*

xv. *Joyshree Nath,Sankar das A Challenge in Hiding Encrypted Message in LSB and LSB+1 Bit Positions In various Cover Files, Vol.2 Issue 4 Journal of Global Research in Computer Science,April 2011.*

xvi. *Wei-Qi Yan, Duo Jin, Mohan S Kankanhalli Visual Cryptography for Print And Scan Applications, Vol.5 IEEE Proceedings of Circuits and Systems,May 2004.*

xvii. *Ming Sun Fu ,Au, O.C. Joint visual cryptography and watermarking , Vol.3 IEEE International Conference on Multimedia and Expo. June 2004.*

xviii. *Youmaran R. Adler A, Miri A An Improved Visual Cryptography Scheme for Secret Hiding , Vol.3 Biennial Symposium on Communication June 2006.*