International Innovative Research Journal of Engineering and Technology

ISSN NO: 2456-1983

International Conference on Emerging Innovation in Engineering and Technology

ICEIET-2017

FASTER ENCRYPTION AND DECRYPTION SCHEME FOR VISUAL CRYPTOGRAPHY USING ERROR DIFFUSION AND SEGMENTATION

Mr. V. Saranraj [1], Mrs. B. Ramathilagam [2]
[1] M.E Communication Systems, Student
[2] Department of ECE, Assistant Professor
Mailam Engineering College,Tamil Nadu,India.
[1]ecesaran.94@gmail.com
[2]bramathilagam716@gmail.com

Abstract— A faster and easier color visual cryptography encryption method is introduced which produces meaningful color shares. Color shares are produced via half toning. Visual Cryptography uses the idea of hiding secrets within images .Before the encryption process, the secret image which is to be encrypted on to the shares is divided equally into four segments. These four segments are all equal in size and each segmented image is called a message image. Error diffusion is a simple and efficient algorithm for image halftone generation. The partitioned message images are to be interpolated to match with the size of half toned share images. These images are encoded into multiple shares and later decoded without any computation. The decrypted images are to be decimated to obtain the original message images. The four message images retrieved so are concatenated to obtain the secret image.

Keywords: Decryption, Encryption, Error diffusion, Share image, Visual cryptography.

I.INTRODUCTION

Visual cryptography is a new type of cryptographic scheme that focuses on solving this problem of this secret sharing. Visual cryptography uses the idea of hiding secrets within images. These images are encoded into multiple shares and later decoded without any computation. This decoding is as simple as superimposing transparencies, which allows the secret to be recovered. Image sharing is a subset of secret sharing because it acts as a special approach to the general secret sharing problem. The secrets in this case are concealed images. Each secret is treated as a number, this allows a specific encoding scheme supplied for each source of the secrets. Image sharing proposes a scheme which is identical to that of general secret sharing. In (k,n) image sharing , the image that carries the secret is split up into n pieces and the decryption is totally unsuccessful unless at least k pieces are collected and superimposed.

II. RELATED WORK

The visual cryptography was initially introduced and used only on binary images. Recently, some visual cryptography schemes for gray and color image have been proposed. Again Naor and Shamir [2] introduced VCS (k,n), the idea of cover based semi-group to further improve the contrast in 1996. Ateniese et al. [3] provided the first construction of VCS (2,n) having the best possible contrast for any nl2. Verheul and Tilborg [4] are first to present a secret sharing scheme for images with c colors in 1997. The principle of this scheme is to transform one pixel of image to b sub-pixels, and each sub pixel is divided into c color regions. In each sub-pixel, there is exactly one color region colored, and all the other color regions are black. The color of one pixel depends on the interrelations between the stacked sub-pixels. A major disadvantage of this scheme is that the number of colors and the number of sub pixels determine the resolution of the revealed secret image. If the number of colors is large, coloring the sub-pixels will become a very difficult task. Tzung-Her Chen et al [5] anticipated a multi-secrets visual cryptography which is extended from traditional visual secret sharing. The codebook of traditional visual secret sharing implemented to generate share images macro block by macro block in such a way that multiple secret images are turned into only two share images and decode all the secrets one by one by stacking two of share images in a way of shifting. This scheme can be used for multiple binary, gray and color secret images with pixel expansion of 4.

III. EXISTING WORK

This research presents an information sharing scheme in halftone images. Some gray level images of the same resolution are selected and transferred to halftone ones, which are responsible for carrying a secret halftone image. Given the pixels of secret image as the constraint, the host images are generated using Multi-scale Error Diffusion (MED). The original pixels of host images are examined and the modified MED ensures that the pixels of the host images should satisfy the required conditions. After grouping all the processed halftone images, the secret image can be successfully revealed. The research objective is maintaining the quality of all the halftone images in this information sharing Scenario. The experimental results demonstrate the interesting characteristics of the proposed scheme.

IV. PROPOSED WORK

The proposed a new VC encryption scheme which provides a faster algorithm for producing meaningful color shares. This scheme reduces the time required for encryption and decryption and also also produces a share image with high PSNR value and good visual quality..

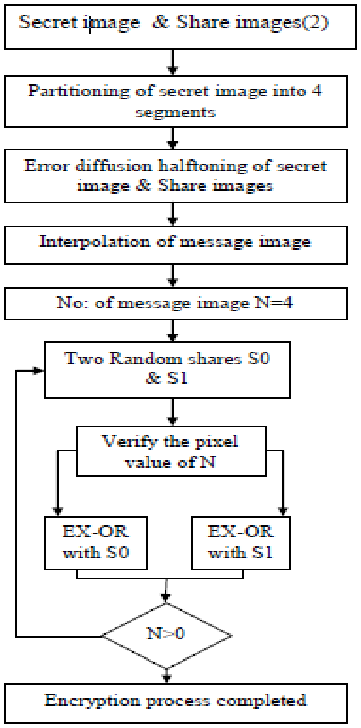
Secret image & Share images(2)
Partitioning of secret image into 4 segments
Error diffusion halftoning of secret image & Share images
Interpolation of message image
No: of message image N=4
Two Random shares S0 & S1
Verify the pixel value of N
EX-OR with S0
EX-OR with S1
N>0
Encryption process completed

Figure 1. Explanation of encryption scheme

Figure 2 and Figure 3 shows the brief explanation of the proposed encryption and decryption/recovery mechanism respectively The proposed encryption process starts with segmentation of the half toned secret image. The half toned secret image is partitioned into four segments. These segments also called as “message images” are to be interpolated to match with the size of half toned share images. After interpolation, every pixel of the message image is verified for two values, “0” or “1”.

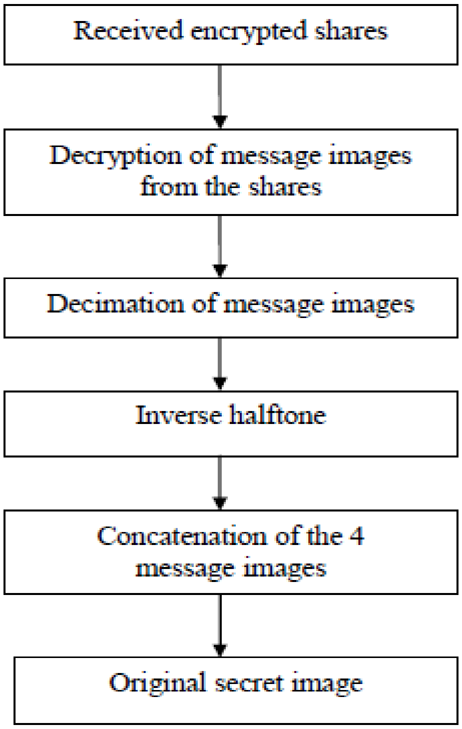
Received encrypted shares
Decryption of message images from the shares
Decimation of message images
Inverse halftone
Concatenation of the 4 message images
Original secret image

Figure 2. Explanation of decryption scheme

If the message pixel is „0‟, it is EX-OR ed with share S0 otherwise EXOR ed with share S1 and the resultant pixel is stored. The decryption process is exactly reverse to that of the encryption process. The decrypted images are to be decimated to obtain the original message images. The four message images retrieved so are concatenated to obtain the secret image. Decimation is the reverse process of interpolation. In the decimation process, the original size of each message image(segments of secret image) are obtained. Concatenation is the joining process where all the four message images are joined together to obtain the original secret image.

V. EXPERIMENTAL RESULTS

In the experiment, we have made an image encryption scheme based on visual cryptography scheme for images, this can be extended to work with Identity Based Cryptography. Share-l is generated with equal number of O's and 1 's with height and width of secret image. Simulation results of proposed image encryption scheme shown in figure 3. It has half-toning and inverse half-tone method to encrypt and recover the image with better visual quality respectively. Figure 3(a) shows the original color image. It is segmented into four images and half-toned using Stucki error diffusion method.

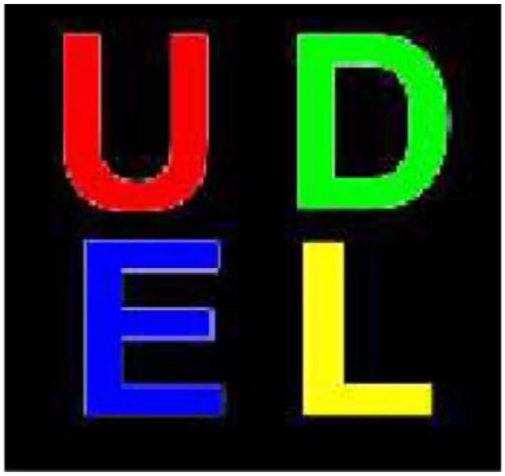

Figure 3(a) Original image

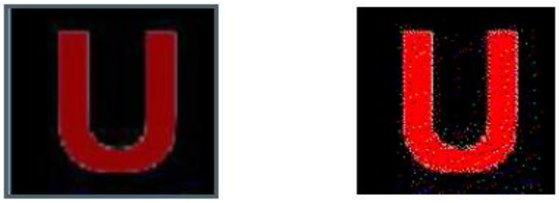

Figure 3(b) Message image 1 and its half toned image

It has half-toning and inverse half-tone method to encrypt and recover the image with better visual quality respectively.

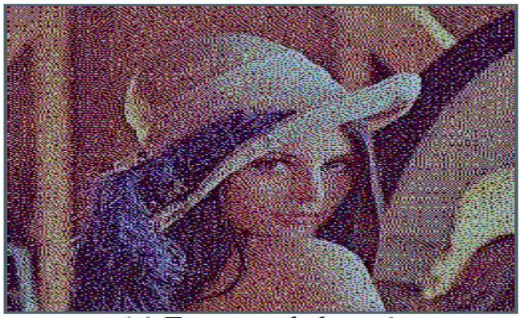

Figure 3 (c) Encrypted share 1

Figure 3(a) shows the original color image. It is segmented into four images and half-toned using Stucki error diffusion method.

Figure 3(c) shows the shares image l generated with equal numbers of black and white pixels. Figure 3(d) shows the halftoned share image. Figure 3(e) shows the encrypted share image. Figure 3(e) shows the decrypted image (complete secret image).

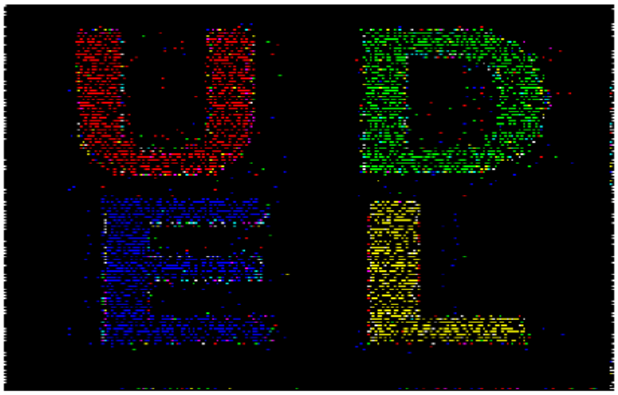

Figure 3 (d) Decrypted image

VI. CONCLUSION

We have developed an encryption method to construct color EVC scheme with segmentation and Stucki error diffusion for visual quality improvement. Segmentation of the secret image is done to reduce the encryption time. Reducing the number of share images used for encryption also helps in providing good visual quality of the decrypted image. Error diffusion is used to construct the shares such that the noise introduced by the predetermined pixels is soft away to neighbors when encrypted shares are generated. It is clear that there is a exchange between contrast of encryption shares and the decryption share; however, we can be familiar with the colorful secret messages having even low contrast. Error diffusion and segmentation can be mostly used in many VC schemes for color images.

REFERENCES

[1] R. Lukac and K. N. Plataniotis, “Color image secret sharing,” *Electron.Lett.*, vol. 40, no. 9, pp. 529–531, Apr. 2004.

[2] M. Naor and A. Shamir, "Visual cryptography 2: Improving the contrastvia the cover base," 1996, a preliminary versionappears in "Security Protocols", M. Lomas ed. Vol. 1189 of *Lecture Notes in Compute Science*, *Springer-Verlag, Berlin,* 1997, pp.197-202.

[3] A. D. S. G. Ateniese, C. Blundo and D. R. Stinson, "Constructions and bounds for visual cryptography," in *23rd International Colloquium on Automata, Languages and Programming, ser. Lecture Notes in Computer Science, F. M. auf der Heide and B. Monien, Eds.*, vol. 1099. Berlin: Springer-Verlag, 1996, pp. 416-428

[4] E. Verheul and H. V. Tilborg, "Constructions And Properties Of K Out Of N Visual Secret Sharing Schemes." *Designs, Codes and Cryptography*, 11(2), pp.179-196, 1997.

[5] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "*Multi-Secrets Visual Secret Sharing*", *Proceedings of APCC2008*, lEICE, 2008

Author Biography

Mr. S. Saran Raj pursued him B.E. in Electronics and Communication Engineering at Mailam Engineering college at Villupuram in the year of 2015. He is doing him M.E in Communication systems at Mailam Engineering college, Mailam. Her area of interest is Digital Image Processing .