Available Online at http://www.recentscientific.com

ISSN: 0976-3031

*International Journal of Recent Scientific Research*
*Vol. 6, Issue, 8, pp.5849-5853, August, 2015*

*International Journal of Recent Scientific Research*

RESEARCH ARTICLE

# A NOVEL ENCRYPTION TECHNIQUE FOR VISUAL CRYPTOGRAPHY IN COLOR IMAGES

**Sreedevi. P and Arya Raj. S**

Dept. Of Computer Science & Eng. MG University, India

**ARTICLE INFO**

***Article History:***

Received 2nd, July, 2015
Received in revised form 10th, July, 2015
Accepted 4th, August, 2015
Published online 28th, August, 2015

***Key words:***

VC, Half toning, Error diffusion, Bit plane

**ABSTRACT**

Color Extended Visual Cryptography (CEVC) schemes have proved to be a successful method for providing security using color secret images. A half toning technique called error diffusion is commonly used in CEVC to attain a color visual cryptography encryption method that produces meaningful color shares with high visual quality. The major drawback of almost all VC schemes is that the decrypted image after stacking the shares will be of poor quality, though it reveals the original content. In the proposed work, a method overcoming this limitation have been developed and implemented. The method successfully generates good quality image at encryption, with no addition in the computational expenses of conventional CEVC schemes employing half toning methods.



## INTRODUCTION

A cryptographic technique called visual cryptography [1] was introduced by Naor and Shamir in 1994 for improving the security of visual information that are shared through networks. The method employs dividing the secret information into a number of shares and send to the selected participants. The shares separately reveal no information about the actual data. The main feature of this scheme is that the secret information can be retrieved only by stacking all these shares. i.e. unlike other cryptographic scheme there is no need for a decryption algorithm to decrypt the encrypted data , since decryption in VC can be done simply using human visual system. Naor and Shamir's k-out-n visual secret scheme can hide a secret image in n different shares. Any k or more shares can reveal the data. But any k-1 shares cannot reveal any information about the actual data. Each of these shares look like a collection of random pixels, hence they are called meaningless shares. Any single share before being stacked up with others reveal nothing about the secret image. When all k shares were overlapped the original image would appear, where n>= k. This way it is possible to improve the security and authentication of secret information that are transmitted through sensitive networks like internet.

To illustrate the basic principle of VC [1] scheme consider a simple (2, 2) VC scheme as shown in Figure 1. Each pixel from the binary image is embedded as black and white sub pixel in each share. If a white or a black pixel is to be encoded then one of the six columns is selected randomly with equal probability. Based on the pixel in the secret image it is replaced by a set of four sub pixels, two of them black and two white. Then continue the same for all the other remaining pixels to generate the complete share. The sub pixel gives no information about the original value of the pixel. A simple example of VC scheme is shown in the Figure I (a).

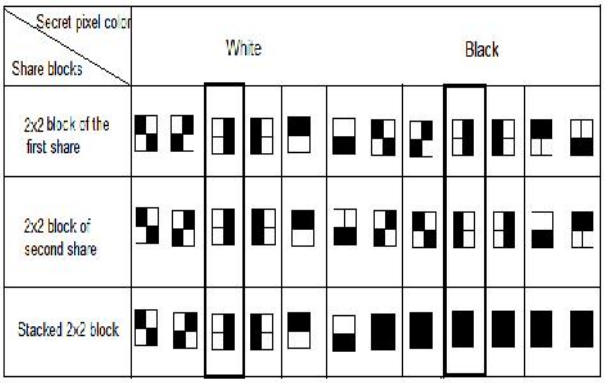



**Figure I a** VC Scheme

### Related Work

This survey elaborates the various methods of VC and focuses the merits and demerits of these techniques

Ateniese *et al*. [3] proposed a VC scheme based on General Access Structures (GAS) to improve the security of shares in (k, n) VC scheme. The access structure is specified as qualified

**Corresponding author:* **Sreedevi. P**
Dept. Of Computer Science & Eng. MG University, India

and forbidden subsets of share images. Only those participants in qualified subset can recover the original image. Thus the security of share can be improved from openness. Lin *et al*. [4] proposed visual cryptography for gray level images. In this paper, instead of using gray sub pixels directly to construct shares, a dithering technique is used first to convert a gray-level image into an approximate binary image. Then existing visual cryptography schemes for binary images are applied for creating shares. Blundo *et al*. [5] in 2000 proposed VC schemes with general access structures for gray scale share images. In this paper, it is assumed that the secret image consists of a collection of pixels, where to each pixel is associated a gray level ranging from white to black and each pixel is handled separately.

An Extended Visual Cryptography Algorithm for General Access Structures was developed by Kai- Hui Lee and Pei-Ling Chiu [7]. In this method during the encryption process an optimization technique is used to create meaningless shares. These shares are free from pixel expansions and cover image are added in each share by a stamping algorithm. In 2006 Zhou *et al*. [8] proposed Halftone Visual Cryptography which increases the quality of meaningful shares. The method is based on blue noise dithering principles by void and cluster algorithm encodes a secret into n shares having meaningful information.

In 2011, Gonzalo R. Arce *et al*. [9] proposed a new scheme for color visual cryptography called CEVC using VIP synchronization and Error diffusion. This paper introduces a color VC encryption method to generate meaningful shares. It is based on two fundamental concepts they are error diffusion and pixel synchronization. Error diffusion is a procedure that produces pleasing halftone images to human vision. VIP synchronization retains the positions of pixels carrying visual information of original images throughout the color channel.

**Error Diffusion Halftoning Techniques**

Error diffusion is the most commonly used half toning technique in CEVC. It is an efficient way to halftone a gray scale image. At each pixel, the quantization error is filtered and distributed to the neighboring pixels that have not been visited yet i.e. making changes at one pixel location cause changes at other pixels locations too. Hence the error depends not only upon the current input and output but also the entire history. Here discussing only the types of different error diffusion half toning algorithms. In the following sections, a number of the most commonly-used filters and some information on each are listed.

***Floyd - Steinberg Filter***

This error-diffusion algorithm is proposed by Robert. N. Floyd and Louis Steinberg [11] to process pixels in neighborhoods by diffusing error. The algorithm scans the image from left to right, top to bottom, quantizing pixel values one by one. At every step, the algorithm compares the gray scale value of the current pixel, represented by an integer between 0 and 255, to some threshold value (typically 128). If the gray scale value is greater than the threshold, the pixel is considered black and its output value is set to 1, else it is considered white and the output value is set to 0. The difference between the pixel's original gray scale value and the threshold is considered as error. To achieve the effect of continuous tone illusion without the diagonal visual artifacts, this error is distributed to four neighboring pixels that have not been visited yet. The matrix shown graphically is an error diffusion matrix proposed by Floyd and Steinberg .

$$\text{Filter}= \begin{bmatrix} & * & 7/16 \\ 3/16 & 5/16 & 1/16 \end{bmatrix}$$

In Floyd-Steinberg filter, each pixel communicates with 4 "neighbors". The pixel immediately to the right gets 7/16 of the error value, the pixel directly below gets 5/16 of the error, and the diagonally adjacent pixels get 3/16 and 1/16. The weighting shown is for the traditional left-to-right scanning of the image. If the line were scanned right-to-left, this pattern would be reversed. Floyd and Steinberg carefully chose this filter so that it would produce a checkerboard pattern in areas with intensity of 1/2. Also in order to get better results boundary conditions are ignored.

***Jarvis Filter***

Another error diffusion algorithm has been proposed by Jarvis, Judice and Ninke [12]. It diffuses the error in 12 neighboring cells instead of 4 cells as in the Floyd-Steinberg algorithm. While producing nicer output than Floyd-Steinberg, Jarvis filter is much slower to implement. With the divisor of 48, bit shifting can no longer be used to calculate the weights. This is further exacerbated by the fact that the filter must communicate with 12 neighbors; three times as many in the Floyd-Steinberg filter. Furthermore, with the errors distributed over three lines, this means that the program must keep two forward error arrays, which requires extra memory and time for processing.

$$\text{Filter}= \begin{bmatrix} & & * & 7/48 & 5/48 \\ 3/48 & 5/48 & 7/48 & 5/48 & 3/48 \\ 1/48 & 3/48 & 5/48 & 5/48 & 1/48 \end{bmatrix}$$

***Stucki Filter***

P. Stucki [13] offered a rework of the Jarvis, Judice, and Ninke filter in 1981 which is same as the Jarvis algorithm and spread the diffusion error to the 12 neighboring cells but the only difference is the fraction of error which is added to the neighboring pixels. Division by 42 is quite slow to calculate (requiring DIVs). However, after the initial 8/42 is calculated some time can be saved by producing the remaining fractions by shifts. The Stucki filter has been observed to give very clean, sharp output, which helps to offset the slow processing time.

$$\text{Filter}=\begin{bmatrix} & & * & 8/42 & 4/42 \\ 2/42 & 4/42 & 8/42 & 4/42 & 2/42 \\ 1/42 & 2/42 & 4/42 & 2/42 & 1/42 \end{bmatrix}$$

**Proposed Method**

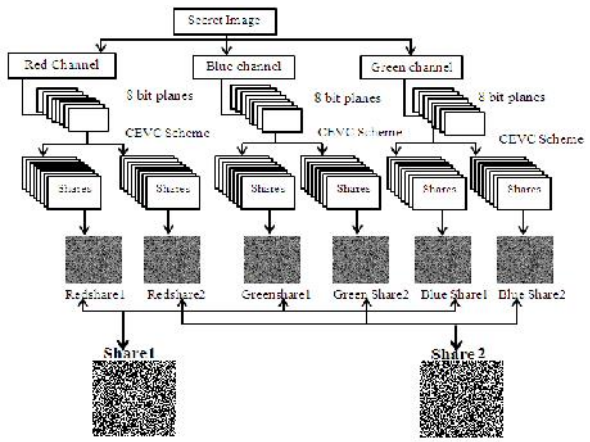
Color Extended Visual Cryptography (CEVC) is a Visual Cryptographic technique for enhancing the security of color images. It encrypt a secret color image into a set of color halftone shares and distributed among the selected participants. The secret can be retrieved only by the proper stacking of all these shares. Color Visual cryptography requires half toned images with minimum contrast loss and minimum time. Though the visual quality of half toned images using error-diffusion methods is good but they are too computationally costly to be implemented. One of the solutions is to use an algorithm other than half toning which performs operations on the image pixels to generate high visual quality decrypted image. Bit plane slicing can be applied on original color image which is separated to three color channels. Then shares are generated for each bit plane. The method successfully generates good quality image at encryption, with no addition in the computational expenses of conventional CEVC schemes employing half toning methods.

The proposed scheme mainly consists of two modules:

- Encryption
- Decryption.

***Encryption***

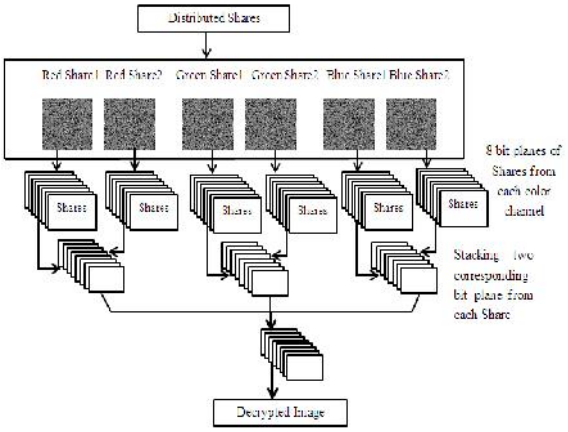
In the proposed system encryption is done using bit level decomposition. Each bit in pixels gray value is called a bit level and each binary image representing a bit level is a bit plane. Dividing a color image into these bit planes and working on each plane separately is called bit level decomposition. The proposed method does not change the contents of original image in the encryption phase. To encrypt the secret image into two shares first it is separated to three color channels. Each of the channels is given for bit plane slicing, and shares are generated for each bit plane.




The first shares of each bit are then concatenated to form the first share of a particular color. The second shares of each bit are then concatenated to form the second share of a particular color. Thus a pair of shares is generated for each color channel. Each set of shares are again concatenated to form two 3-dimensional image matrices i.e. the final two transmitted shares. Superimposing these shares reveals the secret.

***Decryption***

In the proposed method the encrypted image can be decrypted by the superimposing of the transmitted shares. The method first decomposes the shares into their planes. Secondly 8 bit planes of each shares is generated. Then, all the binary shares at the same bit plane are stacked. Stack operation can be implemented by doing bitwise XOR operation. Then for each color plane, select appropriate number of bits and convert to decimal number to form the color value and concatenate the shares for all color planes to form the image.




## EXPERIMENTAL RESULTS

The algorithm discussed above is implemented using MATLAB R2013a. To evaluate the performance of the proposed method color images belonging to different classes are used. Some experimental results are provided to illustrate the effectiveness of the proposed method. Examples are composed with (2, 2) Color VC scheme. Figure V(a) is the original color image .Figure V(b) and FigureV(c) are the shares generated by the proposed bit slicing method ( other than error diffusion technique). Figure V (d) shows the stacked result. Each share leaks no information about the original image.

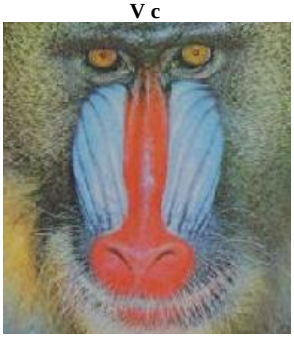
| Image | Floyd – Steinberg Half toning Algorithm | | Jarvis Half toning Algorithm | |
|---|---|---|---|---|
| | PSNR | R | PSNR | R |
| Image1 | 28.5479 | 0.7960 | 24.1022 | 0.3525 |
| Image2 | 38.6192 | 0.2674 | 35.1236 | 0.8449 |
| Image3 | 28.3091 | 0.7732 | 24.0763 | 0.3455 |
| Image4 | 28.3420 | 0.7656 | 24.0762 | 0.3802 |
| Image5 | 28.4760 | 0.8711 | 27.5625 | 0.1640 |

| Image | Stucki Half toning Algorithm | | Proposed Method | |
|---|---|---|---|---|
| | PSNR | R | PSNR | R |
| Image1 | 24.0971 | 0.3586 | 40.5478 | 0.9824 |
| Image2 | 26.2300 | 0.0750 | 39.4709 | 0.9881 |
| Image3 | 24.0812 | 0.3239 | 41.8998 | 0.9839 |
| Image4 | 24.0775 | 0.3546 | 46.3310 | 0.9892 |
| Image5 | 24.1494 | 0.4385 | 32.3756 | 0.9879 |

**V a**

**V b**

**V c**



**V d**

The proposed method is compared with other half toning techniques using parameters such as PSNR and Correlation . The result obtained are shown in the tables

## CONCLUSION

The proposed method presents an encryption method for color visual cryptography scheme with slicing of bit planes. Different error diffusion filters are compared with the proposed technique. From the result it is clear that the visual quality of the decrypted image is better than the existing error filters. The secret information is recovered by the superimposition of the shares. There is a scope of future work in this method as the size of the shares and the resulting image are twice larger than the original image. This can be solved to improve the utility of the proposed scheme.

## References


1. C.Blundo, A.D. Santis, and M. Naor, "Visual cryptography for grey level images", *Information Processing Letters Journal*, vol. 75, no. 6, pp. 255-259, 2000.
2. Chandramathi S., Ramesh Kumar R., Suresh R and Harish, "An Overview of Visual Cryptography“, *International Journal of Computational Intelligence Techniques*, PP-32-37, 2010
3. Chang-Chou Lin, Wen-Hsiang Tsai, "Visual Cryptography for gray level images by Dithering techniques“, Pattern Recognition Letters, 349-358, (2003).
4. Daniel Burkes, “Presentation of the Burkes error filter for use in preparing continuous-tone images for presentation on bi-level devices, in LIB”, CIS Graphics Support Forum, September15, 1988
5. G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Visual Cryptography for general access structures", *Information and Computation Journal*}, vol. 129, no. 2, pp. 86-106, 1996
6. InKoo Kang, Gonzalo R. Arce ,Heung Kyu Lee, "Color Extended Visual Cryptography Using Error Diffusion", IEEE Transactions On Image Processing, Vol. 20, No. 1, January 2011.
7. J. F. Jarvis, C. N. Judice and W. H. Ninke, "A Survey of techniques for the display of continuous tone pictures on Bi-Level Displays“, Computer Graphics and Image processing, 5 13-40, 1976.
8. Jena. D ”A Novel Visual Cryptography Scheme”, International Conference on IEEE, pp. 207-211, 2009.
9. Kai-Hui Lee and Pei-Ling Chiu, "An Extended Visual cryptography Algorithm for General Access Structures", IEEE Transactions on Information Forensics and Security, Vol 7, No. 1, February 2012.
10. M. Nakajima and Y. Yamaguchi, “Extended Visual Cryp-tography for Natural Images”, in Proceedings of WSCG, pp. 303-310, 2002.
11. M. Naor and A. Shamir, "Visual Cryptography”, In Proc. EUROCRYPT, pp. 1-2, 1994.
12. N.Ravia Shabnam, Praveen, Dr. M.Mohamed Sathik, "Feature Extraction by Bit Plane Slicing Technique”, *International Journal of Computing, Communication and Information System*, Vol 1, 2010.
13. P. Stucki, Mecca,"A Multiple Error Correcting Computation Algorithm for Bi-Level Image Hard Copy Reproduction“, Research Report Rz1060, IBM Research Laboratory, 1981.
14. Robert Floyd and Louis Steinberg, "An Adaptive Algorithm for Spatial gray scale“, Proceedings of the Society for Information Display, 75-77, 1976.
15. S. H. Kim and J. P. Allebach, "Impact of HVS models on Model based half toning", IEEE Transactions on Image Processing, vol. 11, pp. 25–269, Mar 2002.
16. T.Chen, K.Tsao, User-friendly random-grid based visual secret sharing, IEEE Transactions on Circuits and Systems for Video Technology 21(11) (2011)1693–1703.

17. Y. C. Hou, "Visual Cryptography for Color Images," Pattern Recognition Letters Vol. 36, Pp. 1619–1629, 2003.
18. Y.Chen, G.Horng, D.Tsai, Comment on “Cheating prevention in visual cryptography”, IEEE Transactions on Image Processing 21(7) (2012)3319–3323.
19. Z. Zhou, G. R. Arce, and G. D. Crescenzo, "Halftone Visual cryptography", IEEE Transactions on Image Processing}, vol. 18, no. 8, pp. 2441–2453, Aug. 2006.

**How to cite this article:**

Sreedevi. P and Arya Raj. S., A Novel Encryption Technique for Visual Cryptography in Color Images. *International Journal of Recent Scientific Research Vol. 6, Issue, 8, pp.5849-5853, August, 2015*

*******