Visual Cryptography for Color Images Using Jarvis Halftone Method

Bharati Pannyagol
Asst. Prof,Computer Department, DPCOE Wagholi ,Pune, Maharashtra,India

***Abstract*: VCS allows one to encode a secret image into sheet images, where each sheet image does not reveal any information about the original. VCS is kind of secret sharing scheme that focuses on shares secret images. This paper produces visual cryptography encryption method which use the Jarvis error diffusion and visual information pixel (VIP) synchronization Techniques for color images. Jarvis Error diffusion method consequently produces pleasing color halftone images to human vision.**

***Keywords*: Visual Cryptography, error diffusion, visual information pixel (VIP), half toning.**

I. INTRODUCTION

Visual Cryptography (VC) is a data security technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption operation does not require a computer. Visual Cryptography (VC) for black and white was first formally introduced by Naor and Shamir [1]. In which one secret binary image is cryptographically encoded into n shares of random binary patterns. The n shares are distributed amongst group of n participants, one for each participant. No participants can retrieve any information from his own transparency, but any k or more participants can visually reveal the secret image by polling there transparencies together. The secret cannot be decoded by any k-1 or less participants, even if higher computational power is available to them.

In VC the decryption process requires only human visual system. This property makes visual cryptography especially useful for the low computation load requirement. VC scheme has been applied to many applications. VC can also be used in a number of other applications such as threshold cryptography, electronic cash, water marking[2,3],private multiparty computations, and digital electronics etc.

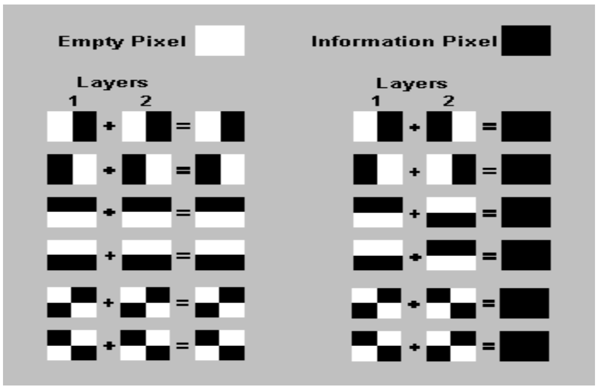

Fig.1: Construction of (2, 2) VC scheme .

Generally, the black-and-white (2, 2) visual cryptography decomposes every pixel in a secret image into a 2×2 block in the two transparencies according to the rules in figure 1, two of them black and white. If pixel is white (black) one of the above six rows of figure 1 is chosen to generate Share1 and hare2. Then, the characteristics of two stacked pixels are: black and black is black, white and black is black, and white and white is white. Therefore, when stacking two transparencies the blocks corresponding to black pixels in the secret image are fully black and those corresponding to white pixels are half-black-and-half-white. As concern to information security, one of the six columns is selected with equal probability.

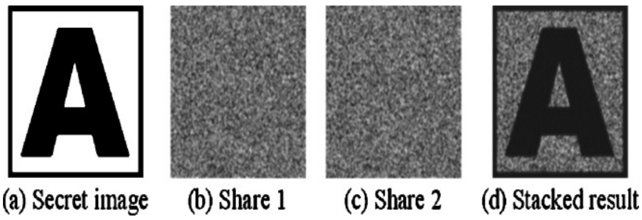

Fig.2: Example of 2-out-of-2 scheme. The secret image is encoded into two shares showing random patterns. The decoded image shows the secret image with 50% contrast loss.

Figure 2 shows an example of a simple (2, 2)-VC scheme with a set of sub pixels shown in figure 1. Figure 2(a) shows a secret binary message, Figure 2(b) and 2(c) depict encrypted shares for two participants. Stacking these two shares leads to the output secret message as shown in figure 2(d).

II. ITERATURE SURVEY

Little research has been carried out on VC, a more general method for VC scheme is based upon general access structure [4]. In that visual cryptography scheme is a set $\mathscr{P}$ of n participants is a method of encoding a secret image SI into n shadow images called shares, where each participant in $\mathscr{P}$ receives one share. Certain qualified subsets of participants can "visually" recover the secret image, but other, forbidden, sets of participants have no information (in an information-theoretic sense) on SI. A "visual" recovery for a set $X \subseteq \mathscr{P}$ consists of Xeroxing the shares given to the participants in X onto transparencies, and then stacking them. The participants in a qualified set X will be able to see the secret image without any knowledge of cryptography and without performing any cryptographic computation. But this technique gives good result on binary images.

In extended visual cryptography (EVC)[5] method, a shares contain not only the secret information but are also some

ISSN: 2278 – 1323

meaningful binary images are developed. A general technique to implement EVCS, which uses hyper graph colorings. This technique yields (k,k)-threshold EVCS which are optimal with respect to the pixel expansion. Since, hypergraph colorings are constructed by random pixels distribution, the resultant binary shares contain strong white noise leading to insufficient results.

Y. C. Hou[6] introduced VC for gray images in which he transformed a gray-level images into halftone images and then applied binary VC schemes to generate grayscale shares. Although the secret image is grayscale, shares are still constructed by random binary patterns carrying visual information which may lead to suspicion of secret encryption.

Yang and Chen[7] has propose new Color VC scheme whose pixel expansion is fixed and improves the previous CVCS. They adopted the distinctive feature of probabilistic VCS's where the share has no pixel expansion to construct CVCS. This scheme has a fixed pixel expansion of 3 regardless of not only the number of colors but also what the value of k and n are.

III. SYSTEM DESIGN

System is designed into 2 phases. The first phase generates shares by using the error diffusion [11] algorithm and Pixel Synchronization. And in the second phase secret image is decrypted by stacking the colored meaningful shares. The Figure 3 explains the working of the system.

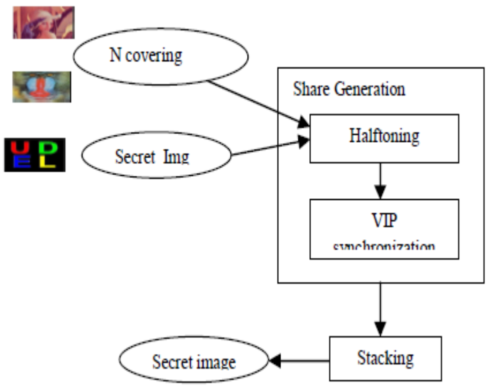

Fig.3 Block Diagram of System Design

A. *Error Diffusion*

Error diffusion[8,9] is a efficient algorithm for image halftone generation. The quantization error at each pixel is filtered and fed to future inputs. The error filter is designed in such a way that the low frequency differences between the input and output images are minimized and consequently it produces pleasing halftone images to human vision.

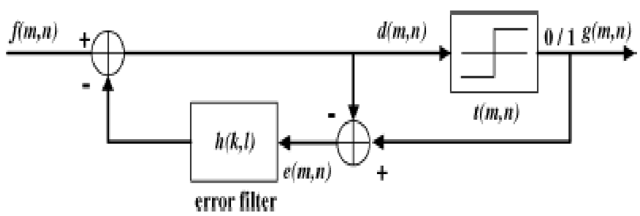

Fig.4: Error diffusion Block Diagram

Figure. 4 shows a binary error diffusion diagram where f(m,n) represents the pixel at (m,n) position of the input image

$$d(m,n) = f(m,n) - \sum_{k,l} h(k,l)e(m-k,n-l)$$

d(m,n).

is the sum of the input pixel value and the diffused errors, g(m,n) is the output quantized pixel value. Error diffusion consists of two main components. The first component is the thresholding block where the output is given by g(m,n)

$$g(m,n) = \begin{cases} 1, & \text{if } d(m,n) \geq t(m,n) \\ 0, & \text{otherwise.} \end{cases}$$

The threshold t(m,n) can be position dependant. The second component is the error filter h(k,l) where the input is the difference between d(m,n)and g(m,n) . Finally, we compute where $h(k,l) \in H$ and H is a 2-D error filter .And h(k,l)= (*1/48)

		●	7	5
3	5	7	5	3
1	3	5	3	1

Fig 5: error diffusion weight matrixes of Jarvis

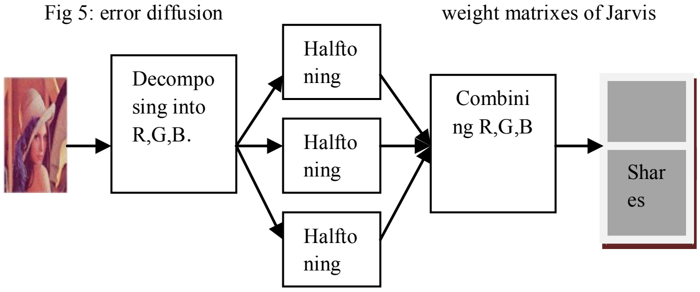

Fig.6.Working of the Jarvis error diffusion method

B. *VIP Synchronization*

Visual Information Pixel (VIP) is pixel [12] on the encrypted shares that have color values of the original images, which make shares meaningful. In the proposed method each sub pixel n carries visual information as well as message information ,while other methods in [1] and [5] extra pixels are needed in addition to the pixel expansion n to produce meaningful shares.

The VIP synchronization process is independently applied to each Red(R),Green(G) and Blue(B) color channels. The below fig illustrate the Matrices distribution along with a message pixel. Every message pixel composed of 3 b is encoded into four subpixels for each color channel by referring the bit value on each channel of message bit. Each encrypted share has the VIPs at the same position throughout the color channels, where colored in gray in the below fig. This feature makes the shares carry accurate colors of the original image after encryption.

ISSN: 2278 – 1323

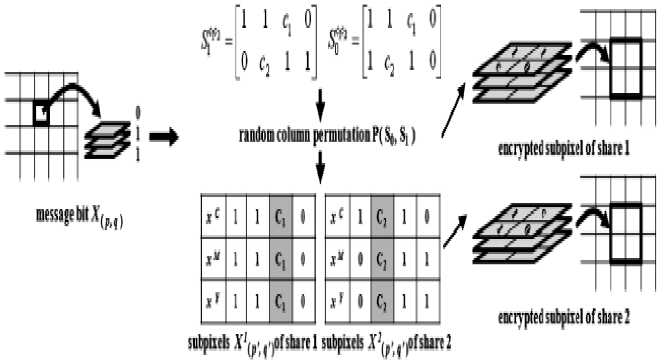

Fig.7: General illustration of matrices distribution of (2,2) color VC

C. STACKING

Decoding does not need any algorithm. The meaningful shares are XORed to reconstruct the secret image by simply human vision system.

IV. IMPLEMENTATION

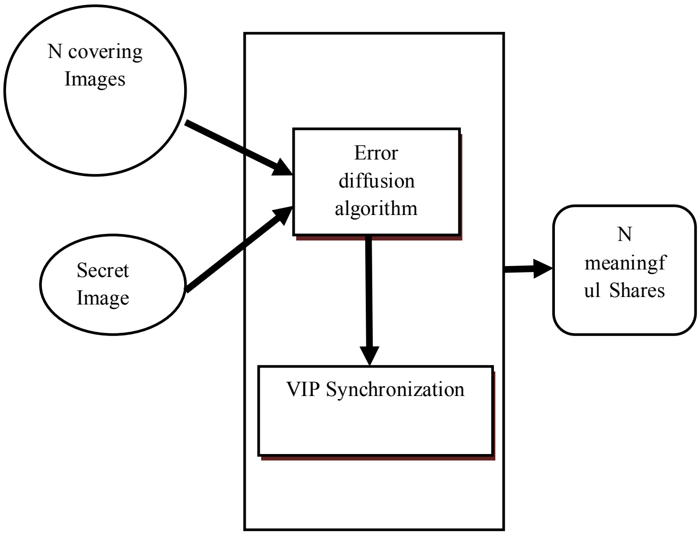

Fig 8.1 Block Diagram of system Design at sender side

A. WORK PROCESS OF THE SYSTEM AT SENDER SIDE

In the above figure 8.1 N covering images and one secret image is taken as the input.

1. A error diffusion algorithm is applied on N covering images to get halftone images
2. The same algorithm is applied on secret image to convert it into halftone image.
3. Shares are generated by synchronizing the secret image and the covering image.
4. Then these n shares are distributed among n participants.

B. WORK PROCESS OF THE SYSTEM AT RECEIVER SIDE

In the figure 8.2 k shares are taken as the input and Superimposed or XORed them to get the secret image

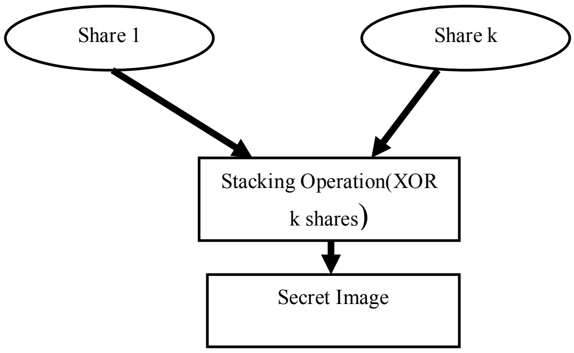

Fig 8.2 Block Diagram of system Design at Receiver side

.

V. EXPERIMENTAL RESULT ANALYSIS

This section presents the simulation results illustrating the performance of the proposed cryptosystem. The test image employed here is the true color image the secret message of size 128x128 pixels and covering images of size 256x256 are provided for the share generation. Figure 9 to 11 represent the results of each step of the system. Size of images is resized to fit in the paper.

A. (2, 2) Visual Cryptography

Fig.9 (a) – (d) Covering Input Images of size 256x256 (e) secret input image of size 128x128

Fig.10.Halftone shares using Jarvis error diffusion method

Fig.11 (a)Share 1 (b) Share (c) Reconstructed secret image

We can see from the experiments that shares are meaningful color shares and the stacked images have good visual quality. So the error diffusion and VIP synchronization improve the visual quality of shares and stacked images.

ISSN: 2278 – 1323

VI. CONCLUSION

The proposed system presents an encryption method for color Visual Cryptography scheme with Jarvis Error diffusion and VIP Synchronization for visual quality improvement. For encryption VIP synchronization is used. It hold the original pixels in the actual VIP values to produce meaningful shares. The secret information is revealed by overlapping of meaningful shares.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT , 1994, pp. 1–12.

[2]M. S. Fu and O. C. Au, "Joint visual cryptography and watermarking," in Proc. IEEE Int. Conf. Multimedia Expo, 2004, pp. 975–978.

[3] M. Naor and B. Pinkas, "Visual authentication and identification," Adv.Cryptol., vol. 1294, pp. 322–336, 1997.

[4] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Visual cryptography for general access structures," Inf. Comput., vol. 129, no. 2, pp. 86–106, 1996.

[5] G. Ateniese, C. Blundo, A. Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," ACM Theor. Comput. Sci., vol. 250,pp. 143–161, 2001.

[6] Y. C. Hou, "Visual cryptography for color images," Pattern Recognit., vol. 36, pp. 1619–1629, 2003.

[7] C. N. Yang and T. S. Chen, "Visual cryptography scheme based on additive color mixing," Pattern Recognit.,vol. 41, pp. 3114–3129, 2008.

[8] S. Gooran, "Digital Halftoning",Thesis, Linkoping University, Linkoping,Sweden.

[9] InKoo Kang,Gonzalo R.Arce,heung-Kyu Lee, "Color Extended Visual Cryptography Using Error Diffusion," IEE Trans. On Image processing,vol.20.no.1.2.11

[10] Sadan Ekdemir, Xunxun Wu, "Digital Halftoning Improvements on the Two-by-Two Block Re-placement Method".333,jan 2011.

[11] Z. M. Wang, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography via error diffusion,"IEEE Trans. Inf. Forensics Security, vol.4, no. 3, pp. 383–396, Sep. 2009

[12] InKoo Kang, Gonzalo R. Arce, and Heung-Kyu Lee, "Color Extended Visual Cryptography Using Error Diffusion", IEEE Transactions on image Processing,vol.20.no.1,January 2011

ISSN: 2278 – 1323