Performance Evaluation of Floyd Steinberg Halftoning and Jarvis Haltonong Algorithms in Visual Cryptography

Pratima M. Nikate
Department of Electronics & Telecommunication Engineering,
P.G.Student,NKOCET, Solapur, India

Prof. I. I. Mujawar
Department of Electronics & Telecommunication Engineering,
Associate Professor,NKOCET, Solapur, India

Abstract- Colour Visual Cryptography (VC) is a technique which encrypts a colour secret image into n halftonedimage shares and this encrypted secret image can be reconstructed simply by stacking these shares, means no cryptographic computation is required at the time of decryption. The formed shares are very safe because separately they reveal nothing about the secret image. Halftoing is very important feature of visual cryptography, it provides security at the early stage of cryptography. The extensively used halftoning technique in VC scheme is nothing but Error Diffusion method. This method is simple and efficient to use. In this paper it is presented the review of error diffusion algorithms such as Floyd Steinberg halftoning and Jarvis halftoning algorithms along with compare them on the basis of parameters such as time PSNR, SNR, Entropy, Correlation.

Keywords: Digital Halftoning, Error Diffusion method, Visual Cryptography.

I. INTRODUCTION

Visual cryptography is a new type of cryptographic scheme that focuses on solving this problem of secret sharing. It uses the idea of hiding secrets within images. Multiple shares are formed by encoding these images and later decoded without any computation. This decoding is done by superimposing transparencies, so the secret image is recovered.

Visual cryptography was originally invented and pioneered by MoniNaor and Adi Shamir in 1994 at the Eurocrypt conference. As the name suggests, visual cryptography is related to the human visual system. When out of n shares,*k* shares are stacked together,the secret image get decryption. So that anyone can use the system without any knowledge of cryptography and without performing any computations. This is one more advantage of visual cryptography over the other popular conditionally secure cryptography schemes. This mechanism is very secure and

it can be easily implemented. An electronic secret can be shared directly or the secrets can be printed out onto transparencies and superimposed, so that the secret image can be reveal [1].

Any visual secret information (pictures, text, etc) is considered as image and encryption is performed using simple algorithm to generate n copies of shares. The very simple access structure is the 2 out of 2 scheme where the secret image is encrypted into 2 shares and both needed for a successful decryption. These shares are look like random dots and they does not revealing the secret information.

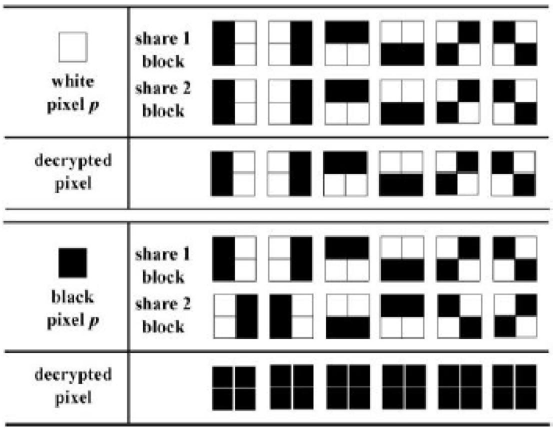


Figure 1. Construction of (2, 2) VC scheme

To illustrate basic principles of VC scheme, consider a simple (2, 2)-VC scheme shown in Fig.1. Each pixel from asecret (binary) image is encoded into black and white subpixels in each share. If is a white (black) pixel, one of the six columns is selected randomly with equal probability, replacing. Regardless of the value of the pixel, it is replaced by four subpixels. Two of them black and remaining two are white. Thus, the subpixel set gives no information about the original value of pixel. When two subpixels originating from two white are overlapped, the decrypted subpixels have two white and two black pixels. On the other hand, if a decrypted subpixel having four black pixels indicates that the subpixel came from two black pixels [1].

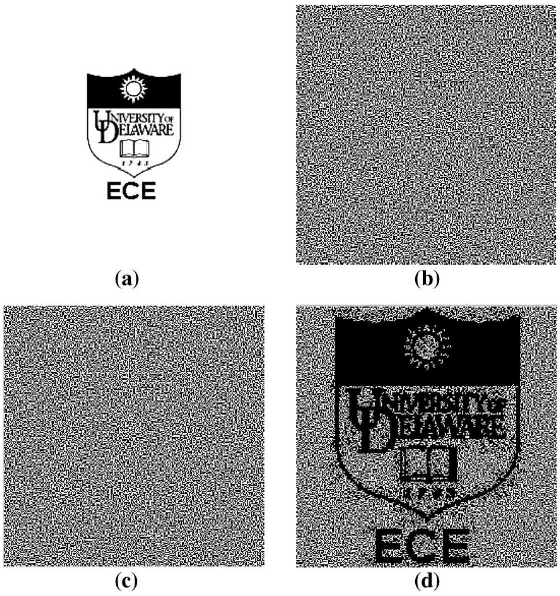


Figure 2. Example of 2-out-of-2 scheme (a) Binary secret message (b) Encrypted share 1. (c) Encrypted share 2. (d) Decrypted secret message

II.LITERATURE REVIEW

In 1996, Ateniese [2] proposed a more general method for VC scheme based upon general access structure. This paper provided a more efficient construction of threshold schemes. The VC scheme concept has been extended to grayscale share images by L. A. MacPherson [3]–[6]. Blundo [4] in 2000 proposed VC schemes with general access structures for grayscale 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 grey level ranging from white to black and each pixel is handled separately. Hou [7] transformed a gray-level image 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. Ateniese [8] developed a method of extended visual cryptography (EVC) in which shares contain not only the secret information but are also meaningful images. Zhou *et al.* [9] used half toning methods to produce good quality halftone shares in VC. Visual secret sharing for color images was introduced by Naor and Shamir [10] based upon cover semi groups. Hou [7] in 2003 proposed schemes for color shares by applying halftone methods and color decomposition. Hou decomposed the secret color image into three (yellow, magenta and cyan) halftone images. In 2011, Gonzalo R. Arce [11] proposed a new scheme for color visual cryptography which introduces Visual Information Pixel (VIP) synchronization to generate high quality shares.This paper has also introduced an error diffusion technique for generating halftoned shares which are more pleasant to human eyes.

III. SYSTEM MODEL

The system contains two phases. They are as follows:

- Share generation: It generates shares by using error diffusion halftoning algorithm and VIP synchronization.
- Stacking: The formed shares from first phase are overlapped to get secret image.

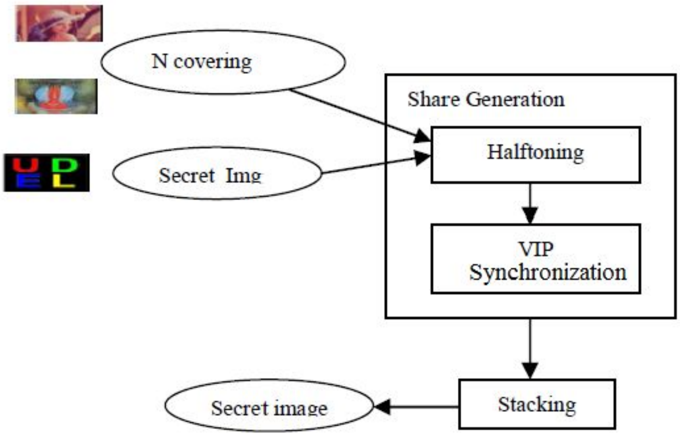


Figure 3. Block Diagram of System Design

HALFFTONING:
Halftoningis an intentionally applied form of noise called as "blue noise" used to randomize quantization error. It prevents large-scale patterns in the images such as color banding. It is often used in digital printing, where it is applied to bit-depth transitions.

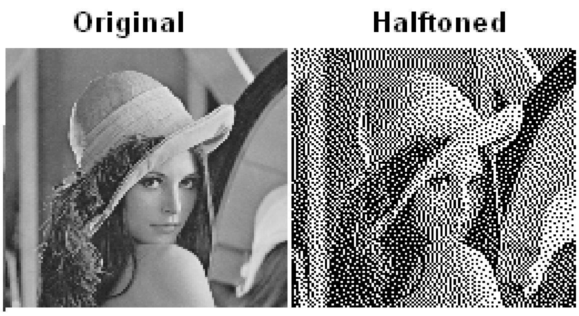


Figure 3. Example of Halftoning

Types of halftoning:
There are several types of half toning. We will discuss only the Error Diffusion Halftoning which is most commonly used in color visual cryptography.

a) Error-Diffusion Halftoning:
Error diffusion is a simple but efficient to use. The quantization error at each pixel is filtered and fed into a set of future inputs. The quantization error depends upon not only the current input and output but also the entire

past history. The error filter is designed in such a manner that the low frequency difference between the input and output image is minimized. The error that is diffused away by the error filter is high frequency or “blue noise.” These features of error diffusion produce halftone images that are pleasant to human eyes with high visual quality.

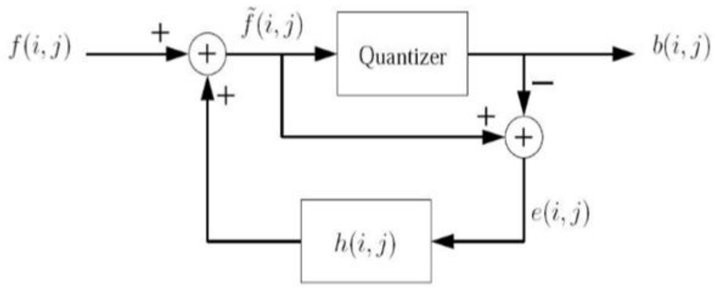
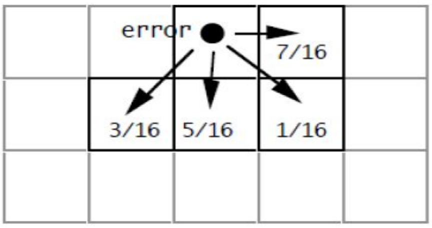


Figure 4. Error Diffusion Block Diagram

Algorithms for Error Diffusion Halftoning:

1. Floyd Steinberg Halftoning algorithm:
   This error-diffusion algorithm is proposed by Floyd and Steinberg. It raised the idea to keep track of the error. Figure 5(a) shows the process of Floyd-Steinberg algorithm. Algorithm-1 implements the error-diffusion halftoning of an *n* by *m* grayscale image. The boundary conditions are ignored. It is convenient to compute the output pixels in scan line order from upper left to lower right. At every step, the algorithm compares the grayscale value of the current pixel J(i, j) which is represented by an integer between 0 and 255, to some threshold value (typically 128). If the grayscale value is greater than the threshold, the output pixel I(i, j) is considered black (value 0), else it is considered white (value 1). The difference between the pixel's original grayscalevalue and the threshold is considered as an error.

1. Procedure HALFTONING AN IMAGE
2. for i = 1,……,n do
3. for j = 1,…..,m do
4. if J(i, j) < 128 is found then J(i, j) = 0
5. else J(i, j) = 1
6. error = J[i, j] - I[i, j]*255
7. Distribute (3/8) error to the right pixel
8. Distribute (1/8) error to the right diagonal pixel
9. Distribute (1/8) error to the bottom pixel
10. Distribute (3/8) error to the left diagonal pixel
11. end for
12. end for



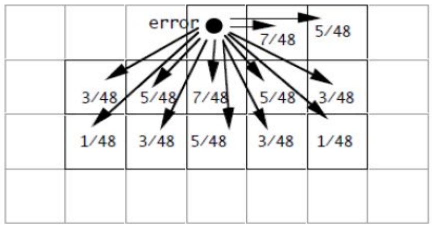


Figure 5(a).Floyd-Steinberg Error-Diffusion Matrix   figure 5 (b). Jarvis Error-Diffusion Matrix

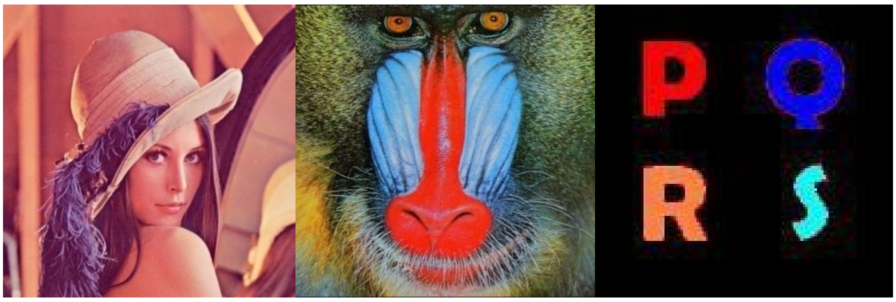
2. Jarvis halftoningalgorithm :
Another error diffusion algorithm has been proposed by Jarvis, Judice and Ninke. It diffuses the error in the 12 neighboring cells instead of 4 cells as in the Floyd-Steinberg algorithm. As a result, this algorithm is even slower, requiring at least 24·n·m floating point and memory access operations. Further, when printing color images, the running time increases by a factor of four. A diffusion matrix of Jarvis algorithm is shown in figure 5(b).

IV. EXPERIMENTAL RESULTS

Table-I shows the comparison between Jarvis and Floyd Steinberg error diffusion algorithms on the basis of parameters such as PSNR, SNR, Entropy and Correlation.

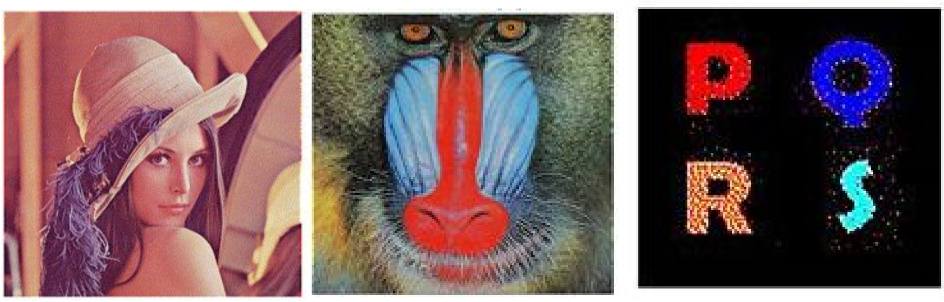
TABLE I: PARAMETERS USED FOR DIFFERENT IMAGES AND HALF TONE METHODS FOR 2 SHARES.

Parameters	Floyd Steinberg Halftoining algorithm	Jarvis Halftoning algorithm
PSNR	15.9902	16.2318
SNR	-1.8523	-1.8079
Entropy	0.38086	0.37811
Correlation	0.84420	0.84847



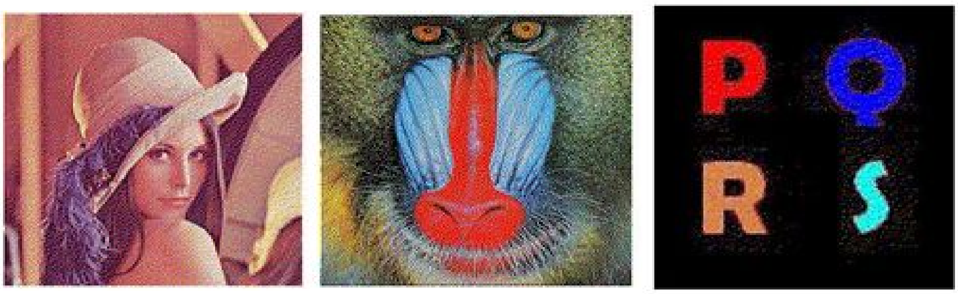
(a) (b) (c)

Fig.6. (a) & (b) covering input images (c) secret input image



(d) (e) (f)

Fig.7. (d) - (f) Halftoned images using Jarvis algorithm

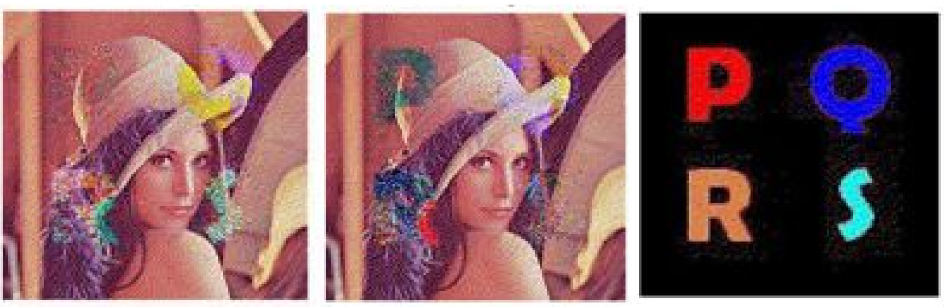


(g) (h) (i)

Fig.8. (g) - (i) Halftoned images using Floyd Steinberg algorithm

(j) (k) (l)

Fig.6. (j) & (k) Result of encrypting images (d) (e) & (f)(l) decoded image



(m) (n) (o)

Fig.6. (m) & (n) Result of encrypting images (g) (h) & (i)(o) decoded image

V.CONCLUSION

In this paper, Floyd Steinberg and Jarvis algorithms of error diffusion halftoning are compared. The comparison is done on the basis of parameters such as PSNR, SNR, Entropy and Correlation. Jarvis kernel gives better visual quality. For encryption VIP synchronization is used, which hold the original pixels in the actual VIP values to produce meaningful shares. The secret information is recovered by superimposition of meaningful shares.

REFERENCES

[1] Dr.D.Vasumathi M.Surya Prakash Rao M.Upendra Kumar Dr.Y.Ramadevi Dr.R.Rajeswara Rao "Novel Approach forColor Extended Visual Cryptography UsingError Diffusion" International Journal of Computer Trends and Technology- volume3Issue4-2012.

[2] 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.

[3] L. A. Macpherson, "Gray Level Visual Cryptography For General Access Structrue," M. Eng. Thesis, Univ. Waterloo, Ontario, Canada, 2000

[4] C. Blundo, A. D. Santis, and M. Naor, “Visual Cryptography for Grey Level Images,” Inf. Process. Lett, Vol. 75, No. 6, Pp. 255–259, 2000.

[5] Y. T. Hsu and L. W. Chang, “A New Construction Algorithm Of Visual Crytography For Gray Level Images,” In Proc. Ieee Int. Symp. Circuits Syst., 2006, Pp. 1430–1433.

[6] C. C. Lin and W. H. Tsai, “Visual Cryptography For Gray-Level Images By Dithering Techniques,” Pattern Recognit. Lett., Vol. 24, Pp. 349–358, 2003.

[7] Y. C. Hou, “Visual Cryptography For Color Images,” Pattern Recognit., Vol. 36, Pp. 1619–1629, 2003.

[8] 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.

[9] Z. Zhou, G. R. Arce, and G. D. Crescenzo, “Halftone Visual Cryptography,” Ieee Trans. Image Process., Vol. 18, No. 8, Pp. 2441–2453, Aug. 2006.

[10] Y. C. Hou, “Visual Cryptography For Color Images,” Pattern Recognit., Vol. 36, Pp. 1619–1629, 2003.

[11] Gonzalo R. Arce, Color Extended Visual Cryptography Using Error Diffusion IEEE Transactions On Image Processing, Vol. 20, No. 1, January 2011