

Analysis of Visual Cryptography Schemes Using Adaptive Space Filling Curve Ordered Dithering

V.Chinnapudevi¹, Dr.M.Narsing Yadav²

1.Associate Professor, Dept of ECE, Brindavan Institute of Technology and Science, Kurnool, AP

2. Professor, Dept of ECE, Malla Reddy Institute of Engineering and Technology, Maisammaguda, Hyderabad, AP

Abstract: Visual cryptography Scheme (VCS), an emerging cryptography technology, uses the characteristics of human vision to decrypt encrypted images without requirement of complex computation. Naor and Shamir proposed the basic model of visual cryptography for binary images. In this work, a new technique for visual cryptography of gray-level image is proposed, which uses first halftone visual cryptography technique to convert a given gray level image into an approximate binary image. Then, the existing visual cryptography scheme for binary image is applied to accomplish creation of shares. On the similar grounds based on the method proposed by Naor and Shamir, where the cryptography technique is based on the (2 out of n shares) we extend the same idea to implement the Visual Cryptography for color images by considering the (k out of n shares) where more than two shares are used to extract the information which is visually cryptographed. In order to improve the quality of image ordered dithering and half toning techniques are used. The primary limitations of the above methods are that it has the poor detail rendition and the contour artifacts. In order to overcome the above limitations we use the new scheme known as "Space Filling curve ordered dithering" (SFCOD). The overall effect of the proposed method is the achievement of visual encryption and decryption functions for gray scale images, where the quality of decrypted image is better compared to the decrypted image obtained by VCS using Space-filling curve order dither technique. This is shown by experimental results based on the objective measurement technique.

Keywords: 1.VCS, 2. HVS, 3. SFCOD, 4. Halftone, 5. Dithering

I. INTRODUCTION

It is now common to transfer information via the Internet. With the coming era of electronic commerce, there is an urgent need to solve the problem of ensuring information safety in today's increasingly open network environment. The encrypting technologies of traditional cryptography are usually used to protect information security. With such technologies, the data become disordered after being encrypted and can then be decrypted by a correct key. So, there is computational overhead in decryption process. The concept of visual cryptography (VC) was introduced by Naor and Shamir in 1994, which requires no computation except the human visual system (HVS) to process decryption. They proposed a (k, n) threshold visual cryptography scheme which encodes a given secret image into n shadow images (shares), where any k or more of them can visually recover the secret image, but any $k-1$ or fewer of them fail to recover the secret image. The most notable feature of this approach is that it can recover a secret image without any computation. It exploits the human visual system to read the secret message from some overlapping shares, thus overcoming the disadvantage of complex computation required in the traditional cryptography. The Naor and Shamir visual cryptography scheme (VCS) serves as a basic model. It has been applied to many applications, which include information hiding, general access structures, visual authentication, identification, and so on. Unfortunately, these applications are all restricted to the use of binary images as input due to the nature of the model. This drastically decreases the applicability of visual cryptography because binary images are usually restricted to represent text-like messages. In 1997, Verheul and Van Tilborg first tried to extend visual cryptography into gray level images. They used the c number of gray levels existing in original images to form shares instead of using black and white values only. The size of decoded image will increase by a factor of c^{k-1} when $c \geq n$ for a (k, n) threshold scheme. So, in order to reduce the size of decoded image, input gray level image is first converted into an approximate binary image called *halftone image* using a technique known as Adaptive space filling curve order dithering (ASFCOD) technique. Then the shares are created by using a visual cryptography schemes (VCS) for binary image. In the ASFCOD technique, thresholds are assigned to the pixels of the image along a space-filling curve by subdividing the curve into congruent segments. This is achieved by replicating a one dimensional dithering adaptive threshold array over the space-filling curve. In this manner the cluster size is fixed in the process of half toning. This technique reduces the size of decrypted image for gray level image, but the quality of decrypted image depends upon the quality of halftone image (depends upon the size of cluster during half toning). On one hand, if cluster size is too small, the tone of the resulting image can be poor. On the other hand,

if cluster is too large, the resulting image can be grainy and thus blur out image details. In order to control the quality of halftone image, we propose to use ordered dithering method, called adaptive space filling curve ordered dither that does half toning by using a space filling curve to perform an adaptive variation of the cluster size. So by using this proposed scheme we get good quality of decrypted image as well reduction of size which is shown by experimental result based on picture quality evaluation such as such as Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), average difference, mean absolute error. This paper is organized as follows. Section 2 briefly reviews the basic theorem of visual cryptography. Section 3 introduces literature survey and then analyzes it. Section 4 introduces our proposed scheme. Result and Discussion is given in Section 5. Finally conclusion is given in section 6.

II. BASIC VISUAL CRYPTOGRAPHY SCHEME

Naor and Shamir first proposed a (k, n) -threshold visual secret sharing scheme to share a secret image. In this scheme, a secret image is hidden into n share images for participants and can be decrypted by superimposing at least k share images but any $k-1$ share cannot reveal it. This scheme not only provides the frontiers of visual cryptography but also inspires researchers to develop various visual secret sharing schemes for more flexible applications, various kind of secret images, meaningful share images, and so on. The $(2, 2)$ -VCS scheme is illustrated to introduce the basic concepts of threshold visual secret sharing schemes. In the encryption process, every secret pixel is turned into two blocks, and each block belongs to the corresponding share image. At last, two share images are obtained. In the decryption process, two corresponding blocks are stacked together to retrieve the secret pixel. Two share blocks of a white secret pixel are the same while those of a black secret pixel are complementary as listed in Fig.1. Consequently, a white secret pixel is represented by a block with the stacked result of half white sub-pixels, and a black secret pixel is all black. An example of the $(2,2)$ -VCS scheme is shown in Fig. 2, where the share images are 2×2 times larger than the original secret image. The disadvantage of conventional visual secret sharing schemes is that it applied for binary image only.

Secret image	Share1	Share2	Stacked image
□	◻◻	◻◻	◻◻
◼	◻◻	◻◻	◼◼

Fig.1 Sharing and Stacking scheme of Black and White Pixel image obtained by stacking share1 & share2

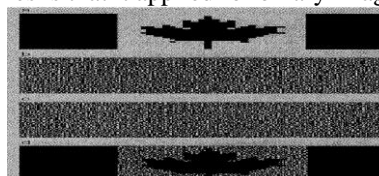


Fig2:2(a) Original binary image, 2(b) share1, 2(c) share2, 2(d) Decrypted

III. RELATED WORK

After, the introduction of visual cryptography by Naor and Shamir, many algorithms for visual cryptography were proposed; but they are limited to binary images only. Visual cryptography for gray level image is seldom discussed. A (k,n) threshold visual cryptography for gray-level image [2] whose pixels have g grey levels ranging from 0 (representing a white pixel) to $g-1$ (black pixel) where each pixel is expanded to m sub pixels of size $m \geq g^{k-1}$ is proposed. Here the size of decoded image is larger than the secret image compared to Naor and Shamir VCS scheme. In order to improve the quality of image ordered dithering and half toning techniques are used. In clustered dot dithering the consecutive thresholds are located in spatial proximity. For a constant threshold half toning patch, this method turns pixels on that are adjacent to one another, forming a cluster. The final halftone dot will thus be clustered in the centre of each screen. The clustered dot dithering method requires a tradeoff between the number of gray levels and the resolution. Due to the dot-center criterion and the limited gray levels, the final half toning image has poor detail rendition and obvious contouring artifact. In the dispersed dot dithering method, the threshold matrices are arranged in a way that the values of threshold grow separately. This method turns pixels on individually without grouping them into cluster, hence make the final halftone dots disperse in each screen. Corresponding input point. Unlike the block replacement and ordered dithering methods, which treat each pixel individually, error diffusion quantifies each pixel using a neighborhood operation. In this case, the value of each output point depends no longer only on the value of the corresponding input point. In order to overcome all the drawbacks of above methods we proposed a new method called space filling curve ordered dithering.

IV. PROPOSED METHOD



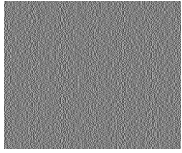

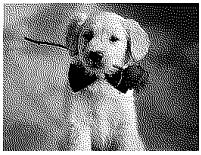
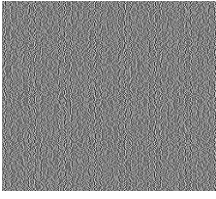
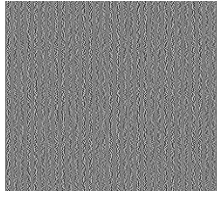


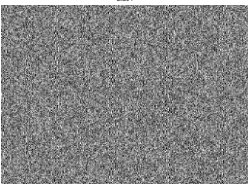
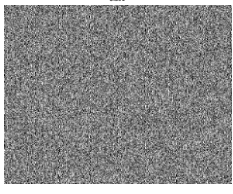
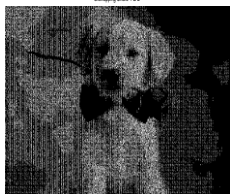
With (k, n) threshold visual cryptography scheme for gray level images using dithering technique, the reduction in size of decrypted image compared to technique is achieved but the quality of decrypted image depends upon the quality of halftone image. In order to reduce the size of decrypted image and improve the quality of image, ASFCOD technique is used.

HILBERT CURVES:

A Hilbert curve (also known as a Hilbert space-filling curve) is a continuous fractal space filling curve, as a variant of the space-filling curves.

In ASFCOD the pixels of the $m \times m$ gray level image I are divided into m classes by assigning each pixel value equal to the corresponding value of the traversal-order number along the space-filling curve in the image. Congruent segment of size $\sqrt{f} \times \sqrt{f}$ are created by replicating a one dimensional dithering threshold array D of length f over the space-filling curve that fills up the image. Each assigned pixel value i serve as index of an element of dither array D , then mapped value $D(i)$ is used as the threshold value to binarize the input gray-level image. Since, length of dither array D is fixed, the cluster size is fixed in the process of half toning. There is a difficulty in choosing an appropriate cluster size if the value is fixed in the process of half toning. On one hand, if cluster size is too small, the tone of the resulting image can be poor. On the other hand, if cluster is too large, the resulting image can be grainy and thus blur out image details. So, by this technique the reduction of size of decrypted image is achieved.

V. RESULTS

Original Image	Share-1	Share-2	Reconstructed Image
HALFTONE BY FLOYD			
Jarvis Halftoned Image 	Share 1 	Share 2 	Overlapping Share 1 & 2 
HALFTONE JARVIS			
Floyd Halftoned Image 	Share 1 	Share 2 	Overlapping Share 1 & 2 
ASFCOD-4			
	Share 1 	Share 2 	Overlapping Share 1 & 2 

VI. PICTURE QUALITY EVALUATION

1. Mean square error (MSE): It measures the average of the square of the "error." The error is the amount by which the pixel value of original image differs to the pixel value of decrypted image.

$$MSE = \frac{\sum_{i=1}^M \sum_{j=1}^N [f(i,j) - f'(i,j)]^2}{MN}$$

Where, M and N are the height and width of image respectively. $f(i, j)$ is the (i, j) th pixel value of the original image and $f'(i, j)$ is the (i, j) th pixel value of decrypted image.

2. Peak signal to noise ratio (PSNR): It is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. PSNR is usually expressed in terms of the logarithmic decibel.

$$PSNR = 10 \log \frac{(2^n - 1)^2}{MSE}$$

3. Average difference (AD): It measures the average error between the original image and the decrypted image.

$$AD = \frac{\sum_{i=1}^M \sum_{j=1}^N [f(i,j) - f'(i,j)]}{MN}$$

where, $[f(i, j) - f'(i, j)]$ represent error between the pixel value of original image and pixel value of decrypted image at height i and width j .

4. Maximum Difference (MD): It measures the maximum error between the original image and decrypted image.

$$MD = \max(|f(i,j) - f'(i,j)|)$$

5. Mean Absolute Error (MAE): The mean absolute error is a quantity used to measure how close forecasts or predictions are to the eventual outcomes.

$$MAE = \frac{\sum_{i=1}^M \sum_{j=1}^N [f(i,j) - f'(i,j)]}{MN}$$

where $f(i, j)$ is the original image and $f'(i, j)$ is the decrypted image.

Table 1: PQE calculation for decrypted image

PQE	SFCOD(with cluster length 4)	Half tone Flyord	Half tone Jarvis
MSE	0.1726	0.4727	0.4715
PSNR	55.7604	100.7542	100.7277
AD	0.1726	0.1928	0.1927
MD	45249	23752	23689
MAE	0.1726	0.4727	0.4715

VII. CONCLUSION

In this technique, for implementing visual cryptography using Space filling curves ordered dithering we use HILBERT curves for threshold matrices representation in an image. First we convert grayscale image into binary image through halftone with error diffusion and the ASFCOD. And then by applying extended visual cryptography scheme for binary image in creation of shares. This technique reduces the size of the decrypted image.

The quality of the decrypted image can be increased than the previous techniques which were mentioned above. This has been used by showing experimental results by evaluating picture quality evaluation since we are using ASFCOD for gray level images.

So, in future as the further work it can be extended to implementing these schemes for color images.

REFERENCES

- [1] M. Naor, A. Shamir, Visual cryptography, Advances in Cryptology Eurocrypt '94, Lecture Notes in Computer Science, Springer, Berlin, 1995, Vol. 950, pp. 1–12.
- [2] Verheul, Van Tilborg, Construction and Properties of k out of n visual secret sharing scheme Designs Codes Cryptography, 1997, Vol. 11, pp.179–196.
- [3] C. Lin, T.H. Tsai, Visual cryptography for gray-level images by dithering techniques, Pattern Recognition Letters 24, 2003, pp.349–358.
- [4] Yuefeng Zhang, Space-Filling Curve Ordered Dither, Elsevier, Computer & Graphics, 1998, Vol.22, No. 4, pp. 559±563.

[5] Yuefeng Zhang, Adaptive Ordered Dither, Graphical, Models and Image Processing, January, 1997, Vol. 59, No. 1, pp. 49–53, ARTICLE NO. IP960414.

[6] L.Velho and J. Gomes Stochastic screening dithering with adaptive clustering, in Proceedings of SIGGRAPH'95, ACM Computer Graphics, Annual Conference Series, 1995, pp. 273–276.