ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 569– 574 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India

Visual Cryptography Using Space Filling Curve Ordered Dithering With Adaptive Clustering

G. Ruthwik Sharma[1], G. Shirisha[2], Dr. M. Narsing Yadav[3]

1. Senior UG student, Dept. of ECE, MRIET, Hyderabad, AP email:ruthwiksharma92@gmail.com
2. Senior UG student, Dept. of ECE,MRIET , Hyderabad, AP email:siri.g2010@gmail.com
3. Professor, Dept. of ECE, MRIET , Hyderabad, AP email: nursing.mriet@gmail.com

Abstract: *In this project we investigate the problem of varying the size of dots in the digital halftoning processes. The reproduction of grey scale images in bi-level graphic displays is achieved through a process called halftoning. Given a grey scale image it consists in generating a binary image which causes the impression of continuous variation. This process an be analog or digital. Analog halftoning is done using photographic means to generate high contrast halftone screens. Digital halftoning is done using a technique called dithering to determine the binary state of the elements of the output image. We show that the dot size is the main factor determining the tradeoff between tonal and spatial resolution in the reproduction of gray scale images. We understand the control of pixel aggregation in the context of dithering algorithms like Ordered dither algorithm and the Floyd Steinberg algorithm. The dithering methods can be sub-divided into two main groups according to the types of images they produce.Dispered dot dithering methods generate images in which black and white pixels are evenly distributed throughout the image area. Clustered dot dithering generate images in which black and white pixels are concentrated together forming clusters. The ordered dithering employs a spatial lookup table to perform the quantization of intensity values, while the Floyd Steinberg algorithm modulates the quantization threshold to distribute the local discretization error. The clustered dot ordered dither generates periodic patterns with dot sizes determined by a square integer sub lattice of the image. The space filling curve dither generates a periodic patterns with dot sizes that can vary in one pixel increments. In particular, we extend the dither with space filling curves method, introduced to change the size of pixel clusters according to local characteristics of the image. This makes possible to achieve optimal rendition of gray shades while preserving image details. This entire process is evaluated with the help of* ***Matlab software.***

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

1.EVOLUTION:

How to keep a secret is always an important issue in many applications. Two major approaches to this aim are information hiding and secret sharing. A common method for information hiding is to use the watermarking technique (Coxetal.,2001; Katzenbeisser and Petitcolas, 2000; Johnsonet al.,2000).And a well-known technique for secret sharing is the cryptography method proposed by Shamir (1979). For sharing images, Naor and Shamir proposed further the idea of visual cryptography(Naor and Shamir, 1995) in 1994.Following their work, several extensions have been proposed(Droste, 1996;Hofmeisteret al.,1997; De Bonis and De Santis, 2000).A (n,k) threshold visual cryptography scheme is a method to encode a secret image into n shadow images called shares, where any k or more of them can be combined visually to recover the secret image, but any k -1 or fewer of them gain no information about it. The visual recovery process consists of xeroxing the shares onto transparencies, and then stacking them to obtain a ‘‘decoded’’ image visually approximating the original secret image. This basic model has been applied to many applications, which include information hiding (Naor and Shamir, 1995), general access structures (Ateniese et al., 1996a,b), visual authentication and identification (Naor and Pinkas, 1997), and so on. Unfortunately, these applications are all re-stricted 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. The characteristics of images for showing object shapes, positions, and bright-ness thus cannot be utilized. It is not sufficient that visual cryptography schemes can only deal with binary images. Verheul and van Tilborg (1997) first tried to extend visual cryptography into gray-level images. They used the gray levels existing in original images to form shares instead of using black and white values only. But in ordinary situations, their method has the disadvantage of

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 569– 574 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India

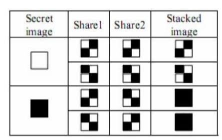
size increase in the de-coded image. So in this paper, we propose a new method suitable for sharing gray-level images. The method utilizes the technique of digital image halftoning first to transform a gray-level image into an approximate binary image. Then the visual cryptography scheme used for binary images is applied.

2.ALGORITHMS AND TERMINOLOGY:

Halftoning is the process the of reproduction of gray scale images in bilevel graphic display devices.The halftoning may be analog ordigital.Analog halftoning is done to generate high contrast images using photographic means, while digital halftoning is done using a technique called ***dithering*** to determine the state of the elements of the output stage. The dithering methods are divided into two main groups according to the types of images produced by them.Dispersed dot dithering which generates images in which the black and white pixels are evenly distributed throughout the image. Clustered dot dithering generates the images where the black and white pixels together form clusters.Dispersed dot dithering is used with low resolution devices i.e.,bitmap displays where as the clustered dot dithering works with the high resolution devices like the digital photo typesetters. The early work in this field was started mainly in the Dispersed dot dithering.The classical Dithering algorithms are the ***ordered dithering algorithm(****limb1969****)*** **and the** ***Floyd Steinberg algorithm(****Floyd-steinberg algorithm..,1975****)***The ordered dither employs a spatial look-up table for performing the quantization of intensity values.The main difference between the methods are related to the nature of the patterns they create and the degree of control over the cluster size allowed by them. The ***clustered dot dithering*** generates periodic patterns with dot sizes determined by a square integer sublattice of the image.The ***space filling curve dither*** generates aperiodic patterns with dot sizes that can vary in one pixel increments.This method has better advantages than the ***clustered dot dither*** due to changes in the dot size of the halftone screens.

3.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.



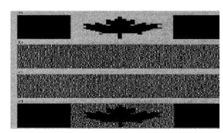


Fig.1 Sharing and Stacking scheme of Black
Fig2:2(a) Original binary image, 2(b) and White Pixel
share1, 2(c) share2, 2(d) Decrypted image obtained by
stacking share1 & share2

4.SPACE FILLING DITHER:

The method takes advantage of the characteristics of space filling curves to perform the neighborhood operations that are necessary to the special dithering process. The space filling curve trace approximation is used to scan the *Image* generating the parameterization of the image element with many desirable properties.

The method consists of the following steps*:*

- *Sub division of the image into regions:*
- *Computation of the average intensities of each region*
- *Generation of corresponding dot patterns for each corresponding regions.*

The sub division of the image is performed by following the path of the space filling curve until the number of the elements visited is equal to the cluster size

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 569– 574 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India

The computation of the accurate intensity for each region is performed as each one of its elements is visited ,by this a corresponding dot pattern is generated by selecting a group of contiguous elements proportional in number to the total intensity, In this manner the region is subdivided into two subregions of respectively black and white pixels such that its average intensities is the same as the original image

Due to the discrete nature of the representation there is a quantization error associated with each region. It is the difference between average intensity of the continuous and quantized values. Note that this residue decreases as the size of the region increases.

5.THE METHOD PROPOSED:

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.

The space filling curve algorithm subdivides the image in cluster blocks and at each block it approximates the image function f(x,y) by some bi-level image function f'(x,y).the adaptive clustering dithering consists of changing the size of cluster,based on some adaptive criteria,in order to get better approximation **f'** of the image function f

The space filling dithering algorithm lends itself very nicely to adaptive clustering.in fact,it is the only dithering algorithm which allows fine control of the halftone screen resolutionThe adaptive criteria to compute the cluster size depends on the desired effect to be obtained by the halftone screen.

6.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× 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 binaries 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.

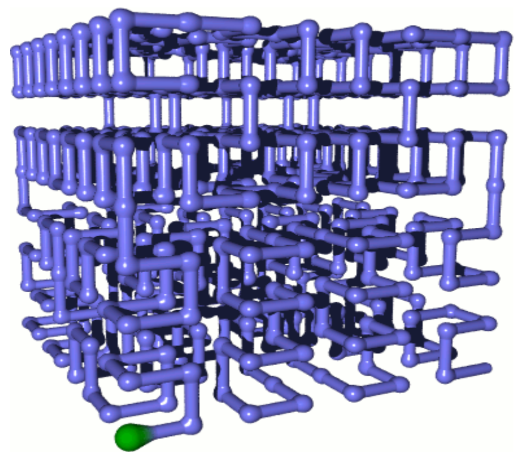


Fig:6.1 3D structure of Hibert Curve of order4

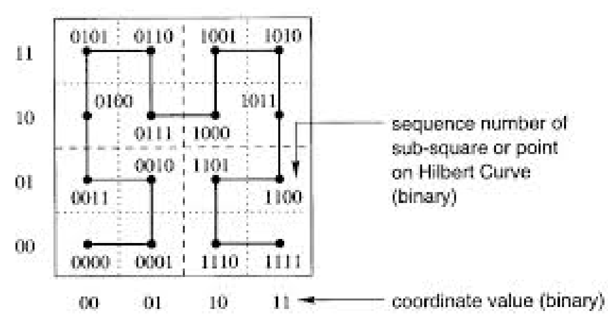


Fig:6.2 Structure of Hibert Curve of Order 4

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 569– 574 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India

RESULTS:

7.1 ERROR DIFFUSION IMPLEMENTATION:

Figure 7.1.1 The Original Gray Scale Image

Figure 7.1.2 The Gray Scale Image after Error Diffusion

7.2 HALFTONING USING FLOYD-STEINBERG ALGORITHM:

Figure:7.2.1 Original Gray Scale Image

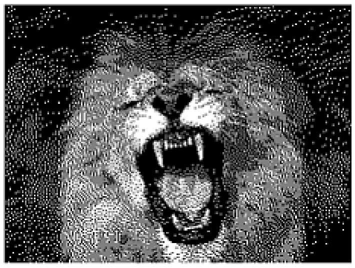


Figure 7.2.2:The Floyd-Steinberg Halftoned Image

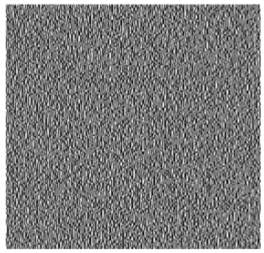


Figure 7.2.3 Share1

Figure 7.2.4 Share2

Figure 7.2.5:The Final Result After The Overlapping Of Both The Shares1&2

7.3 HALFTONING USING JARVIS ALGORITHM:

Figure 7.3.1 The Original Gray Scale Image

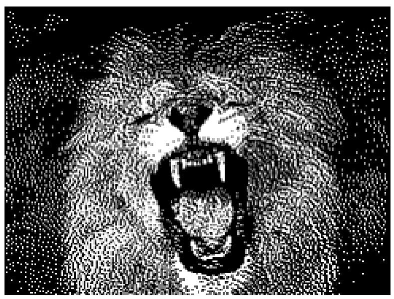


Figure 7.3.2:The Jarvis Halftoned Image

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 569– 574 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India

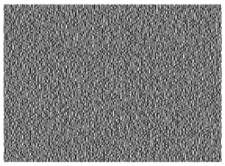


Figure 7.3.3 Share1

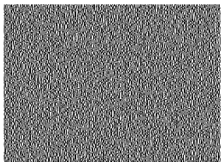


Figure 7.3.4 Share2

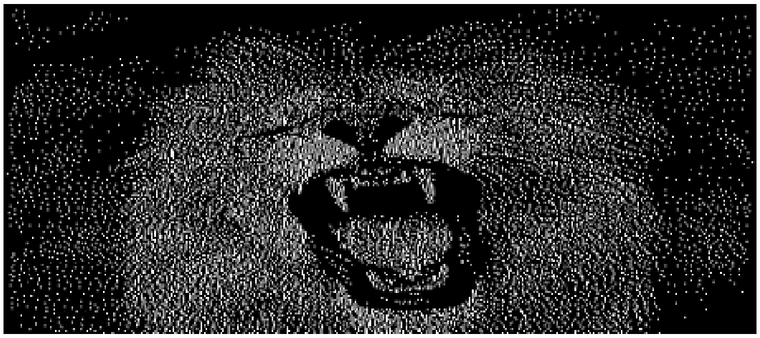


Figure 7.3.5:The Final Result After The Overlapping Of Both The Shares1&2

7.4 HALFTONING USING ORDERED DITHERING ALGORITHM:

Figure 7.4.1 Original Gray Scale Image

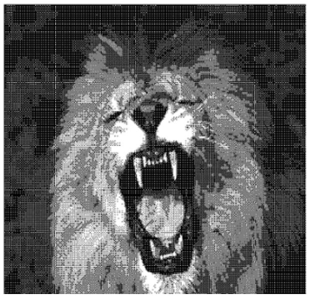


Figure 7.4.2 The Secret Image Obtained After Ordered Dithering

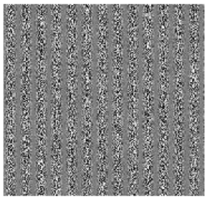


Figure 7.4.3 Share1

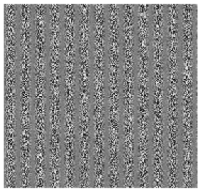


Figure 7.4.4 Share2

Figure 7.4.5:The Final Result After The Overlapping Of Both The Shares1&2 using Ordered Dithering Algorithm Of Order 4

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 569– 574 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India

7. PICTURE QUALITY EVALUATION

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

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

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.

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

3.Average difference (AD): It is 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

Table7. 1: PQE calculation for decrypted image

Picture Quality Evaluation	SFCOD (With Cluster Length 4)	Ordered Dithering	Half-Tone with JARVIS	Half-Tone with
MSE	0.1275	0.1272	0.1575	0.1587
PSNR	-111.5481	-111.5280	-106.284	-106.3
AD	0.1769	0.2262	03.1426	0.1410
MD	6.9899e+004	6.9759e+04	41292	41610
MAE	0.2666	0.2661	0.1575	0.1587

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