INTERNATIONAL JOURNAL FOR TRENDS IN ENGINEERING & TECHNOLOGY
VOLUME 4 ISSUE 2 – APRIL 2015 - ISSN: 2349 - 9303

A NEW VISUAL CRYPTOGRAPHY TECHNIQUE FOR COLOR IMAGES

P.G.Haritha
PG Student, Department of CSE
Sethu Institute of Technology
hari.ravijeyam@gmail.com

Mrs.M.MathinaKani
Associate Professor, Department of CSE
Sethu Institute of Technology
mathinakani@yahoo.co.in

Abstract - Visual Cryptography (VC) is an emerging cryptography technology that uses the characteristics of human vision to decrypt encrypted images. This cryptographic system encrypts it by dividing a secret image into n number of share and decryption is done by superimposing a certain number of share (k) or more. The secret information can be retrieved by anyone only if the person gets at least k number of share. No clue about a secret image is revealed if less than k-1 share are superimposed. The Visual cryptography technique is not only applied for binary messages, grayscale images, but also for color images such as scenic photos or pictures. Color visual cryptography (VC) is used to generate a color halftone image share by encrypting a color secret image. In order to preserve the visual quality and size of the color share without expansion, the concept of size invariant Visual Secret Sharing (VSS) scheme and error diffusion is introduced. Experimental result shows that the proposed method can improve the reconstructed image quality compared with previous techniques. Also, it produces clearer and higher contrast for all kinds of color images.

Index Terms: Error Diffusion, Halftone, Size invariant VSS, Visual cryptography, Visual secret sharing.

1. Introduction

Cryptography is the practice and study of techniques for secure communication. in the presence of third parties. The sender retained the ability to decrypt the information and therefore avoid unwanted persons being able to read it. Visual Cryptography is a cryptographic technique[1] which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. It needs neither cryptography knowledge nor complex computation.

The principle of VC is that each and every pixel of the image is divided into several blocks .The number of white (transparent) and black blocks will be same in number [2]. There would be one white and one black block if a pixel is divided into two parts. If the pixel is divided into four equal parts, then it has two white and two black blocks. The system can be used by anyone without any cryptography knowledge and without performing any complex computations.

Visual secret sharing for color images was introduced by Naor and Shamir based upon cover semi-groups. A 2-out-of-2 VC scheme is presented by applying the idea of color mixture. Stacking two transparencies with different color rises a third mixed color. The approach of Rijmen and Preneel indeed produces visual cryptography for color images. But from the viewpoint of either the additive model or the subtractive model of chromatology, it is not appropriate to fill the blocks with red, green, blue, and white (transparent) colors. Besides, if the average of the four-pixel colors is used in the stacking blocks to represent the corresponding pixel color in the original image, the problem of circular permutations occurs.

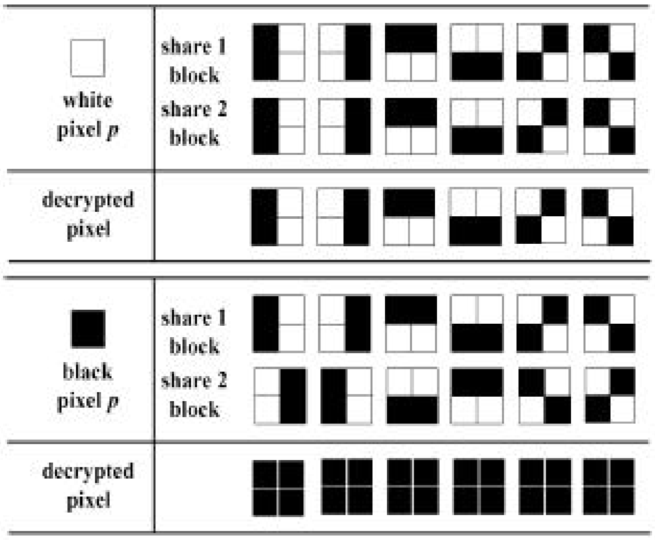

Fig.1. Construction of (2, 2) VC scheme

Following the rules in fig 1, the black-and-white (2, 2) visual cryptography decomposes every pixel in a secret image into a 2×2 block in which two of them are black and other two are white. The characteristics of two stacked pixels are: black and black is black, white and black is black, and white and white is white. During stacking of two transparencies the block corresponding to black pixels in a secret image are fully black and those corresponding to white pixels are half-black-and-half-white.

For describing the constitution of colors, two models are widely used. First is the additive color model that comprise of three primary colors red, green, and blue (RGB), which can be obtained by mixing different RGB channels. The amount of all the three color channels can be modulated by controlling the intensity. The brightness would be increased if more colors are mixed together. White color will be obtained as a result if red, blue, and green channels are mixed in the same amount. One of the best examples of the additive color model is Computer screen. Second is the subtractive model, in which the colored-lights that is reflected from the object's surface is used in combination to obtain a single color. Variety of colors can be produced by mixing cyan, Magenta and Yellow. If more pigments are added the intensity of the light would be lower and the light would be darker. The primitive colors that cannot be composed from other color are cyan, magenta and yellow. One of the best examples of this model is printer.

An extended visual cryptography (EVC) technique[4] is developed which takes n no. of the original image and a secret image as input and produces n no. of encrypted share as output. The following three conditions are needed to satisfy that the obtained share preserve the same approximation of the original image.[6]

• To reconstruct a secret image any k out of n share can be overlapped.
• Even a single part of the secret information cannot be obtained with less than K share.
• Both of the encrypted share and the reconstructed secret images are meaningful images; both images are colored.

Share in an EVC scheme, however, provide very low quality visual information and suffer from low contrast between hyper-graph black and white pixels. The EVC approach is extended to natural grayscale images and color to improve the image quality. The halftone share that carry the Visual information is generated by using joint visual cryptography and watermarking. A method to generate meaningful halftone image by using threshold arrays .The major shortcomings with these methods are that either the security property is not strictly guaranteed or the decoded image is not immune to the interference from the share images.

The method uses the density of the net dots to simulate the graylevel is called "Halftone"[3] and transforms an image with graylevel into a binary image before processing. Halftones are created through a process called dithering, in which the density and pattern of black and white dots are varied to simulate different shades of Gray. Every pixel of a transformed halftone image has only two possible color levels (black or white). Because human eyes cannot identify too tiny printed dots and, when viewing a dot, tend to cover its nearby dots.

Digital Halftoning means deciding how to place the dots by using computer algorithms. All Halftoning uses a high frequency/low frequency dichotomy. The ratio of the inked area to the non-inked area of the output cell corresponds to the luminance or graylevel of the input cell. From a suitable distance, the human eye averages both the high frequency apparent graylevel approximated by the ratio within the cell and the low frequency apparent changes in graylevel between adjacent equally spaced cells and centered dots.

Digital Halftoning uses a raster image or bitmap within which each monochrome picture element or pixel may be on or off, ink or no ink. Consequently, to emulate the photographic halftone cell, the digital halftone cell must contain groups of monochrome pixels within the same-sized cell area. The fixed location and size of these monochrome pixels compromises the high frequency/low frequency dichotomy of the photographic halftone method. Clustered multi-pixel dots cannot "grow" incrementally, but in jumps of one whole pixel. In addition, the placement of that pixel is slightly off-center. To minimize this compromise, the digital halftone monochrome pixels must be quite small, numbering from 600 to 2,540, or more, pixels per inch. However, digital image processing has also enabled more sophisticated dithering algorithms to decide which pixels to turn black or white, some of which yield a better result than digital Halftoning.

2. Proposed system

The main objective of the proposed system is to produce meaningful color share with the same size as the original image and without pixel expansion. Also the reconstructed image should provide better quality and without any contrast loss, for that the concept of Size invariant Visual Secret Sharing (VSS) and an error diffusion is introduced.

VSS scheme generates the color share from a halftone image in the same size as per the original image so that it is convenient for carrying and also the transmission cost would be reduced. Error diffusion generates meaningful color share that are pleasant to human eyes with high visual quality. The error filter used in an error diffusion affects the quality of the share. The Proposed Visual cryptography provides a friendly environment to deal with all kinds of brighter darker and normal color images. [8].The overall block diagram is shown in fig 2.

It comprise of three blocks:

- ✓ Encoding,
- ✓ Share generation and
- ✓ Reconstruction.

In the encoding stage, first the original image (color image) is pre-processed in order to enhance the image feature and to avoid the data loss in a secret image. Then by using the concept of error diffusion it is converted into a halftone image. The obtained halftone image comprises of only a few dots which can be easily identified by human eyes and is further used to generate n no. of color share.

In each and every share a part of the secret is encoded and is distributed to a group of participants so that the problem of hacking can be avoided. In the final stage the generated share are overlapped in correct order to reconstruct a original secret image with high visual quality and without any contrast loss.

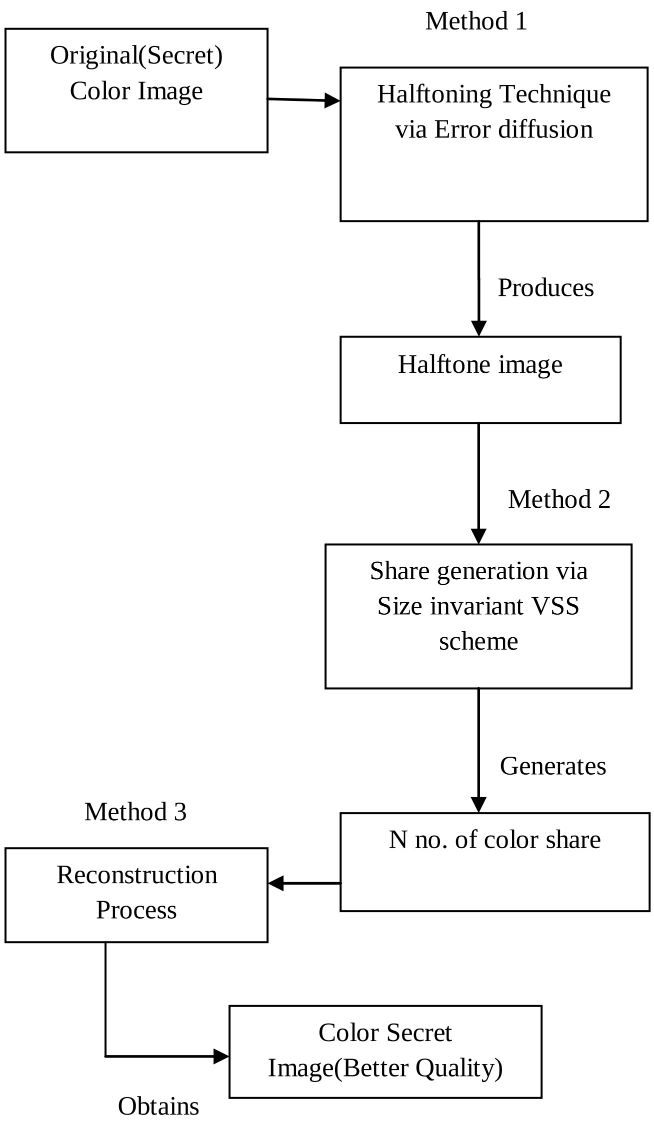

Fig2: Overall System diagram

.

A. Halftoning via Error Diffusion

Initially the input (Color) image is converted into a halftone image by using the concept of an error diffusion technique. This techniques are used in most Halftoning transformations to convert a multiple-level color image into a two level color image. One of the simple and efficient algorithm for producing a halftone image with high visual quality is an Error Diffusion.[9] The edges of the image can be enhanced and also the text in images would be more readable compared to the other Halftoning technique. The Floyd Steinberg error diffusion filter is used to minimize the quantiza tion error between the neighboring pixels.

Error Diffusion is a type of Halftoning [5] in which the quantization residual is distributed to the neighboring pixels that have not yet been processed.. The quantization error at each pixel is filtered and fed to the future inputs. The error filter is designed in a way that the low frequency differences between the input and output images are minimized and consequently it produces pleasing halftone image to human vision.

Usually the color systems comprises of R,G,B[8] which is represented by 8 bits. There would be 0-255 variations of scale in each of the single color, which result in 16.77 million possible colors. While describing a color pixel if (R, G, B) is used, then the representation of (0; 0; 0) indicates fully black and (255; 255; 255) indicates fully white.

Color Visual cryptography [10] divides three colors such as Cyan, Magenta, and Yellow from colors within every pixel of the image. Monochromatic images form by using three components in which every pixel has its own color level and has to be transformed into a halftone image before printing. The three monochromatic halftone image will be(cyan, white), (magenta, white) and (yellow, white) binary images, respectively. The colors in the original images can be obtained by stacking all of the images. In order to transform a color secret image into three C, M, and Y halftone image, every pixel of a halftone image is expanded into a 2×2 block. There would be two transparent (white) pixels and two color pixels in every block of the sharing images so that the entropy reaches its maximum to conceal the content of a secret image.

The Floyd and Steinberg filter [7] is used for an error diffusion. Pixels *J[n]* of the continuous-tone digital images are processed in a linear fashion, left-to-right and top-to-bottom. At every step, the algorithm comparing with the grayscale value of the current pixel, represented by an integer between 0 and 255, to some threshold value (typically 128). If the grayscale value is greater than the threshold, the pixel is considered as black and its output value *I[n]* is set to 1, else it is considered as white and *I[n]* is set to 0. The difference between the pixel's original grayscale value and the threshold value is considered as an error. The pseudo code for Floyd – Steinberg is as follows

```
for i = 1 to n
    for j = 1 to m
        I[i,j] = (J[i,j] < 128)? 0 : 1
        err = J[i,j] - I[i,j]*255
        J[i,j+1] += err*(7/16)
        J[i+1,j-1] += err*(3/16)
        J[i+1,j+1] += err*(1/16)
        J[i+1,j]+=err*(5/16)
    end for
end for
```

The algorithm achieves dithering by diffusing the quantization error of a pixel to its neighboring pixels, according to the distribution

$$\frac{1}{16}\begin{bmatrix} & * & 7 \\ 3 & 5 & 1 \end{bmatrix}$$

The advantages of Floyd - Steinberg error diffusion enhance edges and retain high-frequency image information.

B. Share Generation Via Size Invariant VSS Scheme

In color extended visual secret sharing (VSS)scheme an image was broken up into" n" color share so that only someone with all n share could decrypt the image, while any n-1 share revealed no information about the original color image. Each share was printed on a separate transparency, and decryption process was performed by overlaying all the color share. When all "n" color shares were overlaid, the original image would appear.

Share generation is performed using Size invariant Visual Secret Sharing (VSS) scheme. Each and every color share contains a part of secret information. These share are distributed to a group of participants in order to avoid the problem of hacking. The secret information can be reconstructed only if the sufficient number of color share is combined together. Finally, the share generation and the reconstructed image will be in the same size as the original image by using Chen's technique.

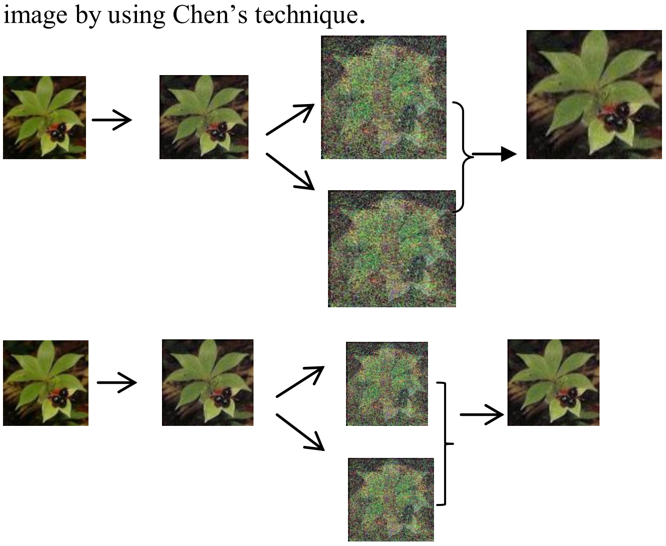

Fig3: Chen'sTechnique a) Size Expansion b) Non-expansion

First, a secret image or the original image (OI) is divided into many blocks, each block will contain mn=s pixels. Next, a single block is encoded in the image at a time. A share images is generated from each and every block that is composed of various colors with the representation of white and black pixels in the amount of s/2. By this way the final reconstructed image will have the same size as the original image.

The scheme first dispatches all the possible values of average intensity into s/2 + 1 level and computes the average color intensity of the blocks in the original image. At the same time, the block containing s/2 + x black pixels is mapped on the each block as in the original image with color image intensity level x (x rangesfrom0to s/2). The proposed scheme shows major improvement compared to the previously mentioned scheme.

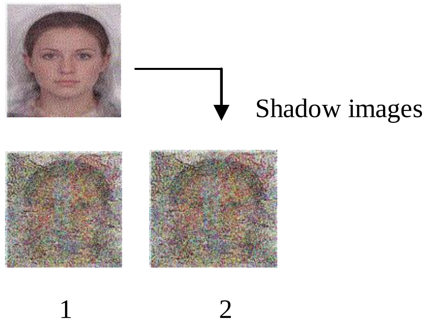

Fig4: Generation of two share(2,2 VC) from a Halftone image

C. Reconstruction of the Original Image

In this phase, the generated color share are taken as input and combined together to produce Secret images with high visual quality. Here t-out-of-n VC scheme is used to combine the n no. of color share in order to produce a halftone image. Then, the Reverse Halftoning process is performed to extract a secret image with high visual quality. Finally, the original image is obtained with better quality, clearer and higher contrast.

Fig5: Reconstructed image of the Proposed scheme

Conclusion

The Proposed model produces meaningful color share with high visual quality by using the concept of Size invariant Visual Secret Sharing (VSS) and error diffusion.VSS scheme generates the share in the same size as per the original image with high visual quality and error diffusion generates color share pleasant to human eyes The Proposed scheme is suitable for different kinds of color secret images such as brighter, darker, and normal images. The result show that the proposed technique provides better quality of the reconstructed image.

Future enhancement

The proposed scheme only improves the visual quality of the color image, but some contrast loss will be occurring if the same VC scheme is applied for 2D and 3D images. Hence, in the future work, the 2D and 3D a secret image is used and is encoded in another image by using the concept of Visual Cryptography. Also, some of the additional security concerns will be introduced to preserve the Visual quality and contrast of the decrypted image.

Acknowledgement

I express my heartfelt gratitude to my project guide Mrs.M.Mathinakani M.E., Assistant professor, department of computer science & Engineering,Sethu Institute of Technology ,Kariapatti, for valuable guidance,encouragement and generous help for the successful completion of this project work.

References

[1]Cheng-Chi Lee, Hong-HaoChen, Hung-TingLiu, Guo-WeiChen, Chwei-ShyongTsai "A new visual cryptography with multi-level encoding", Journal of Visual Languages and Computing,2013.

[2]Roberto De Prisco ,Alfredo De Santis "Color visual cryptog raphy schemes for black and white secret images"., 2013

[3] 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.

[4] Ching-Nung Yang, Yao-Yu Yang."New extended visual cryptography schemes with clearer shadow images",2014.

[5] Zhongmin Wang and Gonzalo R. Arce," Halftone Visual Cryptography through Error Diffusion", IEEE ICIP, 2006.

[6] TengGuo FengLiu a, ChuanKunWu " k out of k extended visual cryptography scheme by random grids".,2013

[7]] Xuehu Yan & Shen Wang & Ahmed A. Abd El-Latif & Xiamu" Random grids-based visual secret sharing with improved visual quality via error diffusion".,2013

[8] Dr.D.Vasumathi,M.Surya Prakash Rao, M.Upendra Kumar, Dr.Y.Ramadevi,Dr.R.Rajeswara Rao "Novel Approach for Color Extended Visual Cryptography Using an Error Diffusion", 2012

[9] Ahmed A.AbdEl-Latif XuehuYan a, LiLi NingWang Jia-LiangPeng XiamuNiu"A new meaningful secret sharing scheme based on random grids, error diffusion and chaotic encryption".,2013

[10] Anuprita Mande, Manish Tibdewal "A Fast Encryption Algorithm for Color Extended Visual Cryptography "Volume 3, Issue 4, April 2013