Halftoning Visual Cryptography Using Secret Sharing

[1]Kiran Kumar Kinthada, [2]T. Rajendra Prasad
[1,2]Dept. of CSE, Kakinada Institute Engineering and Technology, Korangi, Kakinada, AP, India

Abstract
In this paper a new visual cryptography scheme is proposed for hiding information in images which divide secret images into multiple shares. In order to provide more security to existing schemes a new Technique called Digital Halftoning with error diffusion is used, to improve the quality and size of images. Secret information can be retrieved by stacking any k number of decrypted shares. Which reduces the color sets that renders the halftone image and chooses the color whose brightness variation is minimal.

Keywords
Digital Halftoning, Image Formats, Secret Sharing, Visual Cryptography

I. Introduction

Visual cryptography [1] is a cryptographic technique 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. As network technology has been greatly advanced, much information is transmitted via the Internet conveniently and rapidly. At the same time, the security issue is a crucial problem in the transmission process. For example, the information may be intercepted from transmission process. This method aims to build a cryptosystem that would be able to encrypt any image in any standard format, so that the encrypted image when perceived by the naked eye or intercepted by any person with malicious intentions during the time of transmission of the image is unable to decipher the image.

Firstly an image and key is fed into cryptosystem. The encryption algorithm produces a cipher image which is sent into receiver through a commu- nication channel. When the cipher image reaches the destination, the receiver enters the key and the original image is decrypted. Figure 1 shows the block diagram of the cryptosystem. The key we used is the symmetric key with minimum size of 47 bits. Two important factors are used to determine the efficiency of any cryptographic scheme [2], namely: 1) the quality of the reconstructed image and 2) the resizing factor ("fac"). Any loss of information during the reconstruction phase leads to reduction in the quality of the recovered image. On the other hand resizing factor refers to enlarging or reducing the original image. To enlarge an image, specify resizing factor greater than 1. To reduce an image, specify resizing factor between 0 and 1. For bandwidth constrained communication channels it is desirable to keep resizing factor ("fac") as small as possible. For color images, reducing resizing factor is of paramount importance since they occupy more space and consume more band width compared to grayscale and binary images.

Digital halftoning is the process of representing continuous-tone (a.k.a. grayscale and color) images with a finite number of levels for the purpose of display or printing on devices with finite reproduction palettes.

Examples include conversion of a 24-bit color image to a three-bit color image and conversion of an 8-bit grayscale image to a binary image. Halftoning methods in current use may be categorized as classical screening, dithering with blue noise, direct binary search (DBS), and error difusion. Classical screening, which is the oldest halftoning method in printing, applies a periodic array of thresholds to each color of the multi-bit image. Pixels can be converted to 255 (black) if they are above the threshold or 0 (white) otherwise. The human visual system may be roughly approximated as a linear spatially invariant (LSI) system that is lowpass to the luminance component of a color image. Dithering with blue noise (i.e., high-frequency noise) [1] attempts to place the quantization noise from the halftoning process into the higher frequencies. Noise shaping is a characteristic of error difusion as described later, but large periodic masks of thresholds (e.g., 128 x 128 pixels) can be designed to produce halftones with blue noise [2-3]. Although, a plethora of screen design techniques have been proposed [4], they do not produce halftone image quality comparable to DBS. Direct binary search [5] produces blue noise halftones by iteratively searching for the best binary pattern to match a given grayscale image by minimizing a distortion criterion. The distortion criterion incorporates a linear spatially-invariant model of the human visual system as a weighting function [6]. The direct binary search method produces halftones with the highest visual quality to date. Due to its implementation complexity, it is impractical for use as a halftoning method in desktop printers. However, direct binary search can be employed to design screens [7] and error difusion parameters.Error difusion produces halftones of much higher quality than classical screening, with the trade of requiring more computation and memory [8-9]. Screening amounts to pixel-parallel thresholding, whereas error difusion requires a neighborhood operation and thresholding. The neighborhood operation distributes the quantization error due to thresholding to the unhalftoned neighbors of the current pixel. The term error difusion" refers to the process of diffusion using the quantization error along the path of the image scan; e.g., in the case of a raster scan, the quantization error difuses across and down the image. This difusion of errors occurs in a feedback arrangement [8], which causes the quantization error to be highpass filtered.

In 1994, Naor and Shamir proposed a cryptography scheme called the "(k, n)-threshold visual secret sharing scheme," and the idea they raised has ever since been referred to as "visual cryptography (VC)" [7]. The major feature of their scheme is that the secret image can be decrypted simply by the human visual system without having to resort to any complex computation. Naor and Shamir's scheme can hide the secret image in n distinct images called shares. The secret image can be revealed by simply stacking together as many as k of the shares.Each of the shares looks like a collection of random pixels and of course appears meaningless by itself. Naturally, any single share, before being stacked up with the others, reveals nothing about the secret image. This way, the security level of the secret image when transmitted via the Internet can be effectively lifted up. Since Noar and Shamir published their VC scheme, many related methods have been developed and proposed [1-4, 8]. However, in addition to the meaningless shares they produce, those schemes take only binary images as secret images, which mean the contents of the secret images in most cases can be nothing but text or simple black-and-white designs. It is only natural now that researchers are more interested in developing new cryptography schemes that can also process secret color images [5, 9-12] that are more

complex. Verheul et al. proposed a (k, n)-threshold color visual secret sharing scheme [11] based on pixel expansion for pcolor images. Each pixel is expanded to p sections, and each section is divided into p subpixels and can produce n shares with p sections. When the k shares are stacked together, the p-color secret image is revealed. If p is large, then the pixel expansion is great too. Unfortunately, this scheme tends to produce many blocks with large numbers of black subpixels when revealing the secret image; in other words, the visual quality is a weakness. Besides, the shares are meaningless. In order to reduce the expansion size of the secret pixel, Yang and Laih [12] proposed a c-color (k, n)- threshold visual secret sharing scheme. Their scheme can indeed reduce the number of black subpixels effectively. The pixel expansion of this scheme is c×m, where c is the number of colors in the secret image, and m is the pixel expansion size of each color. At less pixel expansion, this scheme improves the visual quality of the revealed secret image. Afterwards, Shyu proposed an efficient c-color (k, n)-threshold visual secret sharing scheme [10] and has further improved the pixel expansion to maintain good visual quality of the revealed secret image. However, in spite of all the advancements both schemes have made, the shares produced by [11-12] are meaningless.

II. Related Work

We consider the problem of neighbor discovery at the physical and medium access layers. In many networks (especially static wired networks) lists of neighbors may be entered manually by a network administrator. We are concerned with situations where this is not easy to do, or when self-configuration is desired.

Neighbor discovery can be done in a centralized or a distributed way. In centralized methods, there is a central controller. All nodes report to the controller, which determines the positions of the nodes, computes their neighbors, and informs each node. Central control of neighbor discovery is expected to cost a lot of energy, particularly when the number of nodes is large. Distributed algorithms have no central controller.

1: **procedure** MATRICES CONSTRUCTION (S_0, S_1, λ)

2: **for** $i = 1, \cdots, n$ **do**

3: **for** $j = 1, \cdots, m$ **do**

4: (a): set $count = 0$

5: (b): if $S_0[i_j] = S_1[i_j] = 0$ is found, then $S_0[i_j] \leftarrow c_i$ and $S_1[i_j] \leftarrow c_i$ and $count = count + 1$.

6: goto (d) if $i < k$ or goto (e) if $i \geq k$.

7: (c): if $S_0[i_j] = S_1[i_j] = 0$ is not found, then switch element $S_0[i_{j1}]$ and $S_0[i_{j2}]$) $(j_1 \neq j_2)$ or

8: switch element $S_1[i_{j1}]$ and $S_1[i_{j2}]$) $(j_1 \neq j_2)$, and goto (b).

9: (d): if $count = \lambda$ and $i < k$, then goto (a) with i increased by 1.

10: (e): if $count = \lambda$ and $i \geq k$, then check if there exists an α satisfying:

$$W(S_1[i]) - W(S_0[i]) \geq \alpha \cdot m$$

A distributed algorithm of Zheng et al. is described in [7]. The algorithm is analyzed under the assumption that radios can simultaneously send and receive on the same channel. This is difficult to achieve in practice, and is unlikely to be the case for sensor networks. Additionally, because their algorithm is deterministic, there is a non-zero probability that a cluster of neighboring nodes, all within transmission range of each other, will systematically interfere with each other, making neighbor discovery impossible. A large part of the analysis in this paper is devoted to determining when nodes should transmit or receive, and to addressing interference.

Nakano and Olariu describe algorithms to initially assign numbers to completely identical nodes, and to elect leaders in wireless ad hoc networks in [8-9]. These problems bear some similarity to neighbor discovery, as they would also take place early in the life of a sensor network. Their algorithms assume the use of the global positioning system (GPS) to achieve synchronous operation.

In the distributed algorithm of Baker and Ephremides [10], all nodes participate in a two-round round-robin schedule. In each round each node is assigned a single slot to announce its identity and the identities of neighbors discovered so far. Nodes listen in the other slots, and can determine all their neighbors, and all their neighbors' neighbors, within two rounds, under the assumption that nodes receive messages from neighboring nodes without errors.

Asynchronous, multi-channel neighbor discovery algorithms have been developed by the Bluetooth research community [6-7]. But they address a case where channel set is fixed, while in CRN channel set can vary among nodes. Also in Bluetooth, neighbor discovery is asymmetric (master/slave configuration), but in CRN we consider a symmetric scenario. In fact, we have borrowed some ideas from Bluetooth neighbor discovery process when developing our algorithm.

if α exists, goto (a) with i increased by 1 until i reaches at n.

if α doest not exists, *undo* all changes of ith row and goto (c).

11: **end for**

12: **end for**

III. Proposed System

A. Encryption

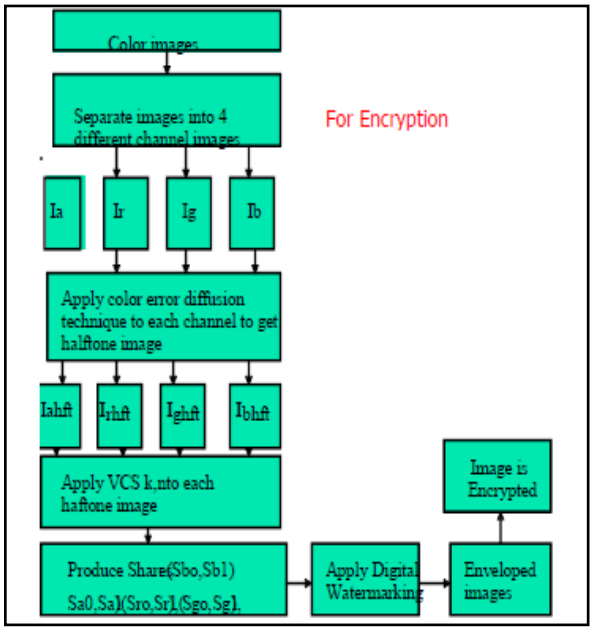

Fig. 1:

1. Color images to be sent as secret is taken as input.
2. Image is divided into channels like alpha channel, red channel,green channel,red channel. Alpha channels are masks through which you can display images. The alpha channel is an 8-bit channel, which means it has 256 levels of gray from 0 (black) to 255 (white). White acts as the visible area; black acts as the transparent area . The level of gray in between determines the level of visibility. For example, 50 percent gray allows for 50 percent visibility. The resulting image is called RGBA.

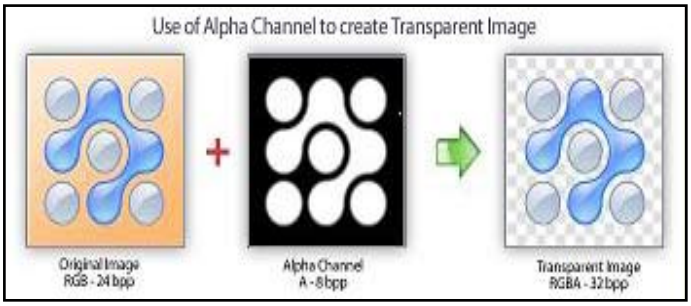

Fig. 2:

3. Then Color error diffusion dot dether technique is applied to these channels to obtain halftone images for example output of halftoning process looks like below image Original image

Original image halftone image

Fig. 3:

4. Each channel image is divided into multiple shares say n according to the input given by user earlier developed using VCS k,n scheme . In XOR based VCS scheme where the share images are superimposed using XOR operation which results in perfect reconstruction of both Black and white pixels.

Secret Image	Shares	OR	XOR
0 (White pixel)	$\begin{bmatrix}1&0\\1&0\end{bmatrix}$, $\begin{bmatrix}1&0\\1&0\end{bmatrix}$	$\begin{bmatrix}1&0\\1&0\end{bmatrix}$	$\begin{bmatrix}0&0\\0&0\end{bmatrix}$
1 (Black pixel)	$\begin{bmatrix}1&0\\1&0\end{bmatrix}$, $\begin{bmatrix}0&1\\0&1\end{bmatrix}$	$\begin{bmatrix}1&1\\1&1\end{bmatrix}$	$\begin{bmatrix}1&1\\1&1\end{bmatrix}$

Fig. 4:

Every secret pixel is turned into two shares, and each share belongs to the corresponding share image. In the decryption process the two corresponding shares are stacked together (using XOR operation) to recover the secret pixel. Two share of a white secret pixel are of the same while those of a black secret pixel are complementary as shown in fig. 3, 4 above. Similary, a white secret pixel is recovered by a share with the stacked result of half white sub-pixels and a black secret pixel is recovered by all black.

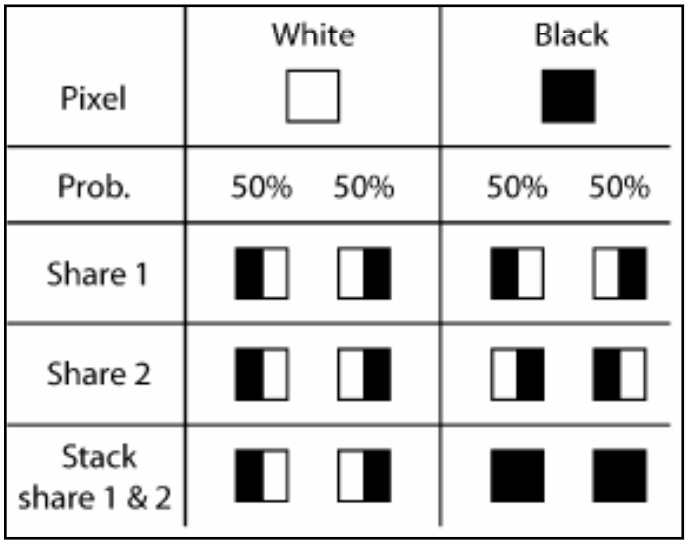

Fig. 5:

5. In this step each share is enveloped in to a different image using Digital Watermarking(LSB Replacement). That is,for n shares n enveloping images are required.

Fig. 6:

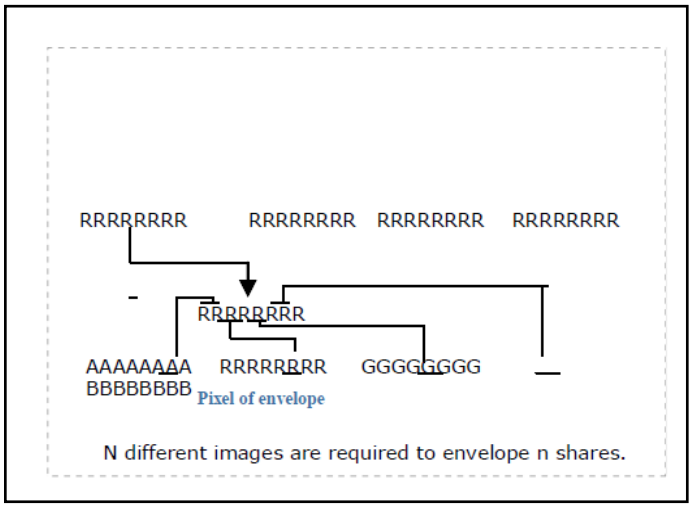

Fig. 7:

Each two bits of each pixel of share is replaced with last two bit of each pixel of eveloping image as shown above in figure,In this way all the pixels of a share is embedded into enveloping image,such that original is hided and enveloped image obtained looks similar to original image. In this way each 8 bit pixel of a share is embed into 32 bit pixel of envelope images. For enveloping n shares n different images are required

B. Decryption

In the decryption algorithm the color image channels are reconstructed by stacking the shares of channels.These color image channels are combined to get the secret color image.

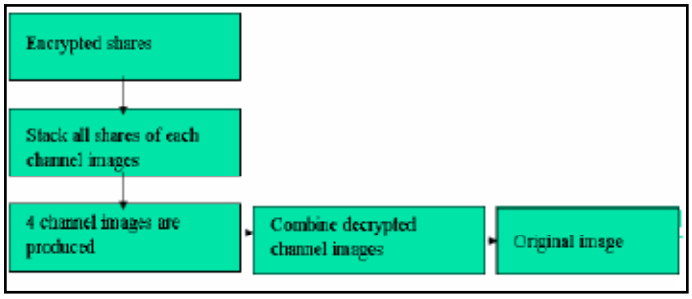

Fig. 8:

IV. Conclusion

The main focus is to improve the quality of the image by using digital halftoning with error diffusion in color VC.

In order to hide secrecy in images, the information divides secret images into multiple shares. At the same time security is also an important issue. So the Secret information can be retrieved by stacking any k number of decrypted shares. Hence research in VC is towards maintaining the contrast at the same time maintaining the security.

References

[1] Nagaraj V. Dharwadkar, B. B. Amberker, Sushil Raj Joshi,"Visual Cryptography for Color Image using Color Error Diffusion", IGCST –GVIP Journal, Vol. 10, issue 1. Feb 2010.

[2] M. Naor, A. Shamir,"Visual cryptography", Advances in Cryptology-Eurocrypt'94, 1995, pp. 1–12.

[3] Kandar Shyamalendu, Maiti Arnab,"K-N Secret Sharing Visual Cryptography Scheme For Color Image Using Random Number", International Journal of Engineering Science and Technology, Vol. 3, No. 3, 2011, pp. 1851-1857.

[4] Naskar P., Chaudhuri A, Chaudhuri Atal,"Image Secret Sharing using a Novel Secret Sharing Technique with Steganography", IEEE CASCOM, Jadavpur University, 2010, pp. 62-65.

[5] F. Liu1, C.K. Wu1, X.J. Lin,"Colour visual cryptography schemes", IET Information Security, July 2008.

[6] Kang InKoo el. at.,"Color Extended Visual Cryptography using Error Diffusion", IEEE 2010.

[7] SaiChandana B., Anuradha S.,"A New Visual Cryptography Scheme for Color Images", International Journal of Engineering Science and Technology, Vol. 2 (6), 2010.

[8] Li Bai,"A Reliable (k,n) Image Secret Sharing Scheme", IEEE, 2006.

[9] Mohsen Heidarinejad, Amirhossein Alamdar Yazdi, Konstantious N.Plataniotis,"Algebraic visual cryptography scheme for color images", IEEE transactions 2008.

[10] K. Jain,"Fundamentals of Digital Image Processing", Englewood Cliffs, NJ: Prentice-Hall, 1989.

[11] Z. Wang, A. C. Bovik, H. R. Sheikh, E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity", IEEE Transactions on Image Processing, Vol. 13, No. 4, pp. 600-612, Apr. 2004.

Mr. Kiran Kumar Kinthada is a student of Kakinada Institute of Engineering & Technology(KIET), korangi, Kakinada. Presently he is pursuing his M.Tech (C.S) from this college and he received his Master of Computer Applications (M.C.A) from VIGNAN'S INSTITUTE OF INFORMATIONTECHNOLOGY,JNTUK,KAKINADA, in the year 2009. His area of interest includes Computer Networks and Object oriented Programming languages in Computer Applications.

Mr.T.rajendra prasad,an efficient teacher, received MCA from ANDHRA UNIVERSITY in 2007 and, M.Tech (CSE) from JNTU Kakinada is working as an Assistant Professor in Department of C.S.E, Kakinada Institute of Engineering and Technology(KIET), korangi, Kakinada. He has 4 years of teaching experience. He has supported many students to publish many papers in both National & International Journals. His area of Interest includes Database Management Systems, Database design & administration. He trained the engineering graduates for "ORACLE CERTIFIED PROFESIONAL" certified process.