Novel Approach for Color Extended Visual Cryptography Using Error Diffusion

Dr.D.Vasumathi[1] M.Surya Prakash Rao[2] M.Upendra Kumar[3] Dr.Y.Ramadevi[4] Dr.R.Rajeswara Rao[5]

1 Associate Professor CSE JNTUH College of Engineering Hyderabad A.P. India
2 M.Tech CN and IS Student MGIT A.P. Hyderabad India
3 Associate Professor CSE MGIT A.P. Hyderabad India
4 Professor CSE CBIT Hyderabad A.P. India
5 Professor CSE MGIT Hyderabad A.P. India

Abstract - **Visual cryptography, an emerging cryptography technology, uses the characteristics of human vision to decrypt encrypted images. Cryptography is the study of mathematical techniques related aspects of Information Security such as confidentiality, data security, entity authentication and data origin authentication, but it is not the only means of providing information security, rather one of the techniques. Visual cryptography is a new technique which provides information security which uses simple algorithm unlike the complex, computationally intensive algorithms used in other techniques like traditional cryptography. Previous methods in the literature show good results for black and white or gray scale VC schemes, however, they are not sufficient to be applied directly to color shares due to different color structures. Some methods for color visual cryptography are not satisfactory in terms of producing either meaningless shares or meaningful shares with low visual quality, leading to suspicion of encryption. Color visual cryptography (VC) encrypts a color secret message into color halftone image shares. This project introduces the concept of visual information pixel (VIP) synchronization and error diffusion to attain a color visual cryptography encryption method that produces meaningful color shares with high visual quality. VIP synchronization retains the positions of pixels carrying visual information of original images throughout the color channels and error diffusion generates shares pleasant to human eyes. Comparisons with previous approaches show the superior performance of the new method.**

***Index Terms*—Color meaningful shares, digital halftoning, error diffusion, secret sharing, visual cryptography (VC).**

1. INTRODUCTION

Cryptography is the practice and study of hiding information. In today's environment, cryptography is considered a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security, and engineering. Cryptography is used in technologically advanced applications, including areas such as the security of ATM cards, computer passwords, Security in electronic voting, Security in ATM transactions and electronic commerce, which all depend on cryptography.

Visual Cryptography 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 human visual system, without the aid of computers. It uses a simple algorithm unlike the complex.

Visual cryptography technique (for black and white images) is introduced by Naor and Shamir. Any visual secret information (pictures, text, etc) is considered as image and encryption is performed using simple algorithm to generate n copies of shares depending on type of access structure schemes. The simplest 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 random dots without revealing the secret information.

Basic visual cryptography is expansion of pixels. First Continuous image (Gray scale) is converted into halftone image (Binary) using any halftone technique as error diffusion, thresholding, ordered dithering, etc.

1.1. *Problem Specification*

A color Visual cryptography encryption method which leads to meaningful shares and is free of the previously mentioned limitations is introduced. The method is simple and efficient. It relies on two fundamental principles used in the generation of shares, namely, error diffusion and VIP synchronization. Error diffusion is a simple but efficient algorithm for image halftone generation. Error diffusion generates shares pleasant to human eyes. The quantization error at each pixel is filtered and fed to 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 images to human vision.

Synchronization of the VIPs across the color channels improves visual contrast of shares. In color VC schemes, the colors of encrypted pixels and the contrast can be degraded due to random matrix permutation. Random matrix permutations are key security features in VC schemes. In grayscale VC schemes, it does not affect the visual quality; however, in color schemes, independent execution of random matrix permutation for each color channel can cause color distortion by placing VIPs at random positions in sub pixels which finally degrades the visual quality. VIP synchronization prevents the color and contrast of original images from degradation even with matrix permutation. VIP synchronization retains the positions of pixels carrying visual information of original images throughout the color channels.

1.2. Applications of Visual Cryptography

Today the growth in the information technology, especially in computer networks such as Internet, Mobile communication, and Digital Multimedia applications such as Digital camera, handset video etc. has opened new opportunities in scientific and commercial applications. But this progress has also led to many serious problems such as hacking, duplications and malevolent usage of digital information.

Being a type of secret sharing scheme, visual cryptography can be used in a number of applications including access control. For instance, a bank vault must be opened every day by three tellers, but for security purposes, it is desirable not to entrust any single individual with the combination.

1.3. Extended VC

Generally, a (k,n)-EVC scheme takes a secret image and n original images as input and produces n encrypted shares with approximation of original images that satisfy the following three conditions:

- any k out of n shares can recover the secret image;
- any less than k shares cannot obtain any information of the secret image;
- all the shares are meaningful images; encrypted shares and the recovered secret image are colored.

Denote $S_c^{c_1,c_2,....,c_n}$ as the collection of matrices from which the dealer chooses a matrix to encrypt, where $c, c_1, \ldots, c_n \in \{0,1\}$. For , is the bit of the pixel on the ith original image and c is the bit of the secret message. For a black and white (k,n)-EVC scheme, we have to construct 2^n pairs of such collection $\left(S_0^{c_1,\ldots,c_n}, S_1^{c_1,\ldots,c_n}\right)$, one for each possible combination of white and black pixels in the n original images. Here we give a definition of the black and white EVC scheme.

Definition 2: A family of 2n^2 pairs of collection of $n\,X\,m^!$ binary matrices $\left\{S_0^{c_1,..,c_n}, S_1^{c_1,..,c_n}\right\}$, constitute a black and white (k,n)-EVC scheme if there exist values $\alpha\,F\,(>0), \alpha s\,(>0)$, and h satisfying the following.

2. LITERATURE REVIEW

With the rapid advancement of network technology, multimedia information is transmitted over the Internet conveniently. Various confidential data such as military maps and commercial identifications are transmitted over the Internet. While using secret images, security issues should be taken into consideration because hackers may utilize weak link over communication network to steal information that they want .To deal with the security problems of secret images, various image secret sharing schemes have been developed.

It is now common to transfer multimedia data 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.

2.1 Black And White VC Schemes

Naor and Shamir's proposed encoding scheme to share a binary image into two shares Share1 and Share2. If pixel is white one of the above two rows of Fig. 2.1 is chosen to generate Share1 and Share2. Similarly if pixel is black one of the below two rows of Fig.2.1 is chosen to generate Share1 and Share2. Here each share pixel p is encoded into two white and two black pixels each share alone gives no clue about the pixel p whether it is white or black. Secret image is shown only when both shares are superimposed.

Stacking shares represents OR operation to human visual system. OR operation is lossy recovery. If XOR operation is applied instead of OR then we can get lossless restore of the original image. But, XOR operation requires computation. The physical stacking process can only simulate the OR operation. The drawbacks of this scheme are:

1. It is for black and white images.
2. Need more storage capacity as shares are four times the original image.
3. It is time consuming as single pixel encoding at each run.

Many advanced schemes were introduced when a colored image is encrypted. A multi-pixel non-expanded scheme for color images introduced which can encode more than one pixel for each run resulting same size of shares as secret image. The scheme achieves high efficiency for encoding and this works well for general access structure for chromatic images without pixel expansion but it generates meaningless shares. The disadvantage of the above schemes is that only one set of confidential messages can be embedded, so to share large amounts of confidential messages several shares have to be generated.

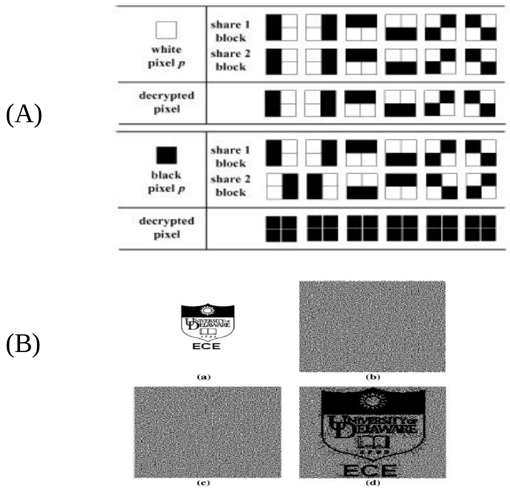


Fig. 2.1(A). Construction of (2, 2) VC scheme: a secret pixel is encoded into four subpixels in each of two shares. The decrypted pixel is obtained by superimposing the blocks in shares one and two. Fig. 2.2(B) Example of 2-out-of-2 scheme. The secret image is encoded into two shares showing random patterns. The decoded image shows the secret image with 50% contrast loss. (a) Binary secret image. (b) Encrypted share 1. (c) Encrypted share 2. (d) Decrypted secret message.

2.2. Color Visual Cryptography Schemes

Sharing a secret color image and also to generate the meaningful share to transmit secret color image Chang and Tsai anticipated color visual cryptography scheme. For a secret color image two significant color images are selected as cover images which are the same size as the secret color image. Then according to a predefined Color Index Table, the secret color image will be hidden into two camouflage images. One disadvantage of this scheme is that extra space is required to accumulate the Color Index Table. In this scheme also number of subpixels is in proportional to the number of colors in the secret image as in Verheul and Van Tilborg Yang and Laih schemes. When more colors are there in the secret image the larger the size of shares will become. To overcome this limitation Chin-Chen Chang et al developed a secret color image sharing scheme based on modified visual cryptography. This scheme provides a more efficient way to hide a gray image in different shares. In this scheme size of the shares is fixed; it does not vary when the number of colors appearing in the secret image differs. Scheme does not require any predefined Color Index Table. Though pixel expansion is a fixed in this scheme is not suitable for true color secret image. To share true-color image Lukac and Plataniotis introduced bit-level based scheme by operating directly on S-bit planes of a secret image.

To illustrate basic principles of VC scheme, consider a simple (2, 2)-VC scheme in Fig. 2.1(A). Each pixel from a secret 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 a set of four subpixels, two of them black and two white. Thus, the subpixel set gives no clue as to the original value of. When two subpixels originating from two white are superimposed, the decrypted subpixels have two white and two black pixels. On the other hand, a decrypted subpixel having four black pixels indicates that the subpixel came from two black pixels. Fig.2.2(B) shows an example of a simple (2, 2)-VC scheme with a set of subpixels shown in Fig. 2.1. Fig. 2.2.(a) shows a secret binary message, Fig. 2.2(b) and (c) depict encrypted shares for two participants. Superimposing these two shares leads to the output secret message as shown in Fig. 2.2(d). The decoded image is clearly identified, although some contrast loss is observed.

3. VISUAL CRYPTOGRAPHY AND ERROR DIFFUSION

Error-diffusion scheme that produces higher quality results. The error filter employed in the error diffusion also affects the share quality. An error filter with longer weight leads to high contrast of encryption shares. The algorithm is faster than the universally used Floyd-Steinberg algorithm, while maintaining its original simplicity. The efficiency of our algorithm is based on a deliberately restricted choice of the distribution coefficients. Its pleasing nearly artifact-free behavior is due to the off-line minimization process applied to the basic algorithm's parameters (distribution coefficients). This minimization brings the Fourier spectra of the selected key intensity levels as close as possible to the corresponding "blue noise" spectra. The continuity of the algorithm's behavior across the full range of intensity levels is achieved thanks to smooth interpolation between the distribution coefficients corresponding to key levels. This algorithm is applicable in a wide range of computer graphics applications, where a color quantization algorithm with good visual properties is needed.

3.1. Fundamentals of VC

Generally, a(k,n) -VC scheme encrypts a secret message into shares to be distributed to n participants. Each share shows noise-like random black and white patterns and does not reveal any information of the secret image by itself. In a k -out-of n scheme, access to more than k shares allows one to recover the secret image by stacking them together, but access to less than shares is not sufficient for decryption. A black and white (k,n) -VC scheme consists of two collections of n x m binary matrices S_0 and S_1, having elements denoted by 1 for a black pixel and 0 for a white pixel. To encrypt a white (black) pixel, a dealer randomly chooses one of the matrices in $S_0(S_1)$

and distributes its rows to the n participants. More precisely, a formal definition of the black and white –(k,n)-VC scheme is given next.

Based upon the principle of VC, extended VC has been proposed whose shares take meaningful images rather than random noise-like patterns to avoid suspicion.

The same algorithms may be applied to each of the red, green, and blue (or cyan, magenta, yellow, black) channels of a color image to achieve a color effect on printers such as color laser printers that can only print single color values.

For example, if there is a small error in the green channel that cannot be represented, and another small error in the red channel in the same case, the properly weighted sum of these two errors may be used to adjust a perceptible lightness error, that can be represented in a balanced way between all three color channels (according to their respective statistical contribution to the lightness), even if this produces a larger error for the hue when converting the green channel. This error will be diffused in the neighboring pixels.

3.2. *Error Diffusion*

Error diffusion techniques are used in most halftoning transformations to convert a multiple-level color image into a two level color image. The simple and attractive concept of this technique is the diffusion of errors to neighboring pixels; thus, image luminance is not lost.

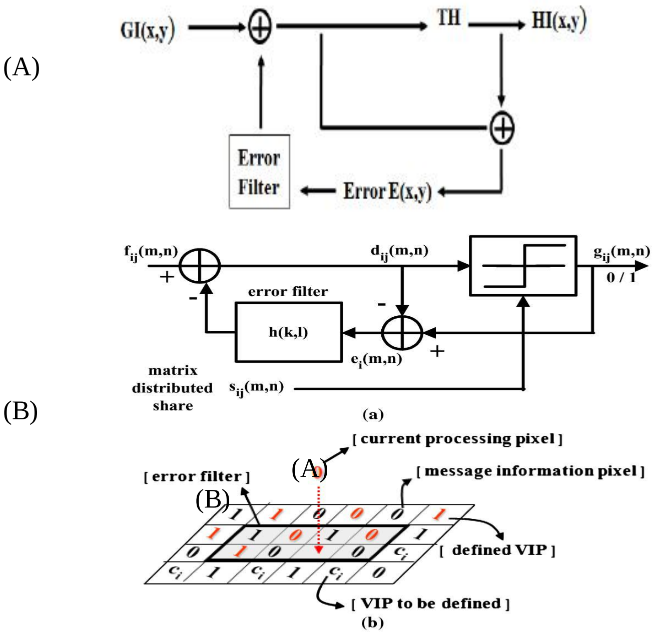


Fig. 3.1(A). Flowchart of error diffusion architecture. Fig. 3.2(B). (a) Block diagram of error diffusion with share encryption. If $s_{ij}(m,n)$ is a VIP, $g_{ij}(m,n)$ is determined by the output of the thresholding quantization. Otherwise, $g_{ij}(m,n)$ is prefixed. (b) Visualization of error diffusion with VIP. Digits in black are prefixed value and that in red are defined value by error diffusion. c_i s are VIPs to be defined.

4. COLOR VC ENCRYPTION BASED UPON PIXEL SYNCHRONIZATION AND ERROR DIFFUSION

We describe the encryption method for color meaningful shares with a VIP synchronization and error diffusion. First, we describe the VC matrix derivation method for VIP synchronization from a set of standard VC matrices. We then introduce an error diffusion process to produce the final shares. The halftone process is independently applied to each cyan (C), magenta (M), and yellow (Y) color channel so each has only one bit per pixel to reveal colors of original images. A secret message is halftoned ahead of the encryption stage.

4.1 *Color Visual Cryptography*

In computer systems, Application Interfaces (APIs) provided by most image processing software as well as the Windows operating system are based on the RGB model. This is mainly because they use monitors as the primary output media. Monitors themselves generate color images by sending out RGB light into human’s retina. In true color systems, R, G, B are each represented by 8 bits, and therefore each single color of R, G, B can represent 0–255 variations of scale, resulting in 16.77 million possible colors. When using (R, G, B) to describe a color pixel, (0; 0; 0) represents full black and (255; 255; 255) represents full white.

Because most color printers use C, M, Y inks to display color, a color image must be processed by the color-decomposed procedure before printing. Color decomposition mainly is to separate C, M, and Y colors from colors within every pixel of the image. These three components form three monochromatic images. (Because colored ink is expensive and the mechanical tolerances may cause the three inks to be printed slightly out of register, the black edges will suffer colored tinges. So, some printers add the black ink when printing black color, resulting in four separate color images.) These monochromatic images are like gray-level images in which every pixel has its own color level and has to be transformed into a halftone image before printing. The three monochromatic halftone images will be (cyan, white), (magenta, white) and (yellow, white) binary images, respectively. After stacking these images, all kinds of the colors in the original image can be displayed.

A. Method 1

In first method uses the procedure illustrated into transform a color secret image into three C, M, and Y halftone images. Then, every pixel of the halftone images is expanded into a 2×2 block to which a color is assigned according to the model. Every block of the sharing images therefore includes two transparent (white) pixels and two color pixels so that the entropy reaches its maximum to conceal the content of the secret image. Furthermore, we design a half black-and-white mask to shade unexpected colors on the stacked sharing images so that only the expected colors show up.

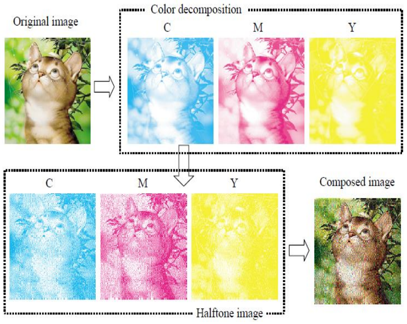
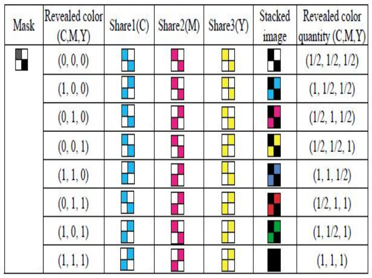


Fig. 4.1. Color image printing.



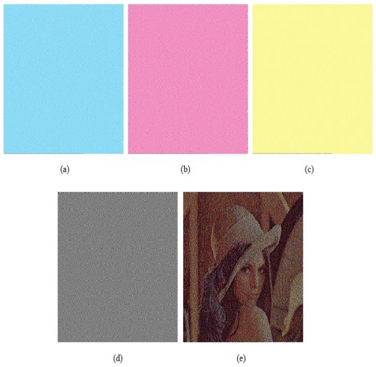
Mask	Revealed color (C,M,Y)	Share1(C)	Share2(M)	Share3(Y)	Stacked image	Revealed color quantity (C,M,Y)
▦	(0, 0, 0)	▦	▦	▦	▦	(1/2, 1/2, 1/2)
	(1, 0, 0)	▦	▦	▦	▦	(1, 1/2, 1/2)
	(0, 1, 0)	▦	▦	▦	▦	(1/2, 1, 1/2)
	(0, 0, 1)	▦	▦	▦	▦	(1/2, 1/2, 1)
	(1, 1, 0)	▦	▦	▦	▦	(1, 1, 1/2)
	(0, 1, 1)	▦	▦	▦	▦	(1/2, 1, 1)
	(1, 0, 1)	▦	▦	▦	▦	(1, 1/2, 1)
	(1, 1, 1)	▦	▦	▦	■	(1, 1, 1)

Fig. 4.2. Scheme 1 of color cryptography.

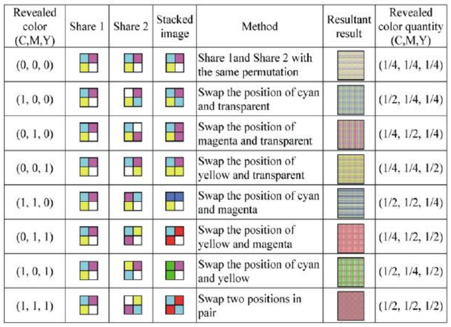
B. Method 2

Although there are only 8 different resultant colors in the stacked image based on Method 1, it is still difficult for us to find out that Fig. 4.3(e) is actually not a continuous-tone image. This is because human eyes cannot identify color pixels that are too tiny, so the nearby color pixels tend to be mixed up by human eyes, thus forming an average color. Because the halftone and color-decomposition techniques can be used to display various colors, another scheme for color visual cryptography can be constructed. The second method expands every pixel of a halftone image into a 2×2 block on two sharing images and fills the block with cyan, magenta, yellow and transparent, respectively. Using these four colors, two stacked images can generate various colors with different permutations. Take Fig. 4.4(B) for example. The distributions of colors in Shares 1 and 2 of the first row are the same. Human eyes will mix up and equalize the elect of the four stacked pixels (cyan, magenta, yellow and transparent) and see a white-like color. In terms of color intensity, cyan, magenta, and yellow each occupies a quarter of the block, i.e., (14; 14; 14). Shares 1 and 2 of the second row exchange the positions of cyan and transparent to reveal two cyan pixels, one magenta pixel, and one yellow pixel within the four pixels after stacking. Therefore, the color intensity is (12; 14; 14), showing a cyan-liked color. To obtain a composed image, we can follow the instruction in Fig. 4.4(B) to select a distribution of colors for the blocks in Shares 1 and 2 and generate two sharing transparencies. After stacking the two sharing transparencies, we can get a stacked image with color intensity ranging from (14; 14; 14) to (12; 12 ;12).

(A)



(B)



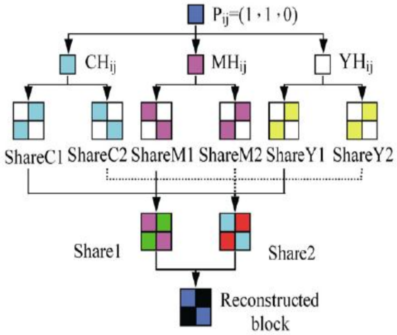
Revealed color (C,M,Y)	Share 1	Share 2	Stacked image	Method	Resultant result	Revealed color quantity (C,M,Y)
(0, 0, 0)	▦	▦	▦	Share 1and Share 2 with the same permutation	▦	(1/4, 1/4, 1/4)
(1, 0, 0)	▦	▦	▦	Swap the position of cyan and transparent	▦	(1/2, 1/4, 1/4)
(0, 1, 0)	▦	▦	▦	Swap the position of magenta and transparent	▦	(1/4, 1/2, 1/4)
(0, 0, 1)	▦	▦	▦	Swap the position of yellow and transparent	▦	(1/4, 1/4, 1/2)
(1, 1, 0)	▦	▦	▦	Swap the position of cyan and magenta	▦	(1/2, 1/2, 1/4)
(0, 1, 1)	▦	▦	▦	Swap the position of yellow and magenta	▦	(1/4, 1/2, 1/2)
(1, 0, 1)	▦	▦	▦	Swap the position of cyan and yellow	▦	(1/2, 1/4, 1/2)
(1, 1, 1)	▦	▦	▦	Swap two positions in pair	▦	(1/2, 1/2, 1/2)

Fig. 4.3(A). Four separating shared transparencies and result of stacking: (a) Share 1(C), (b) Share 2(M), (c) Share 3(Y), (d) Mask, and (e) stacked image. Fig. 4.4(B). Scheme 2 for color visual cryptography.

C. Method 3

In order to alleviate the inconvenience of Method 1, which needs four sharing images, and the loss of image contrast under Method 2, we construct a third method. This method needs only two sharing image and does not sacrifice too much contrast for color visual cryptography. It transforms a color secret image into three halftone images C, M, and Y and exploits the technique of gray-level visual cryptography to generate six temporary sharing images C1, C2, M1, M2, Y1, and Y2. Each of these sharing images will have two white pixels and two color pixels in every 2×2 block; i.e. all the color quantities are 24. The method then combines C1, M1, and Y1 to form a colored halftone Share 1 and C2, M2, Y2 to form Share 2. So, for each block in Share 1 and Share 2, the color intensity is (12; 12; 12). After stacking Shares 1 and 2, the range of color intensity is between (12; 12; 12) to (1; 1; 1). Fig. 4.5 shows how to decompose a blue pixel (1; 1; 0) into two sharing blocks and how to reconstruct the blue-liked block.

(A)



(B)

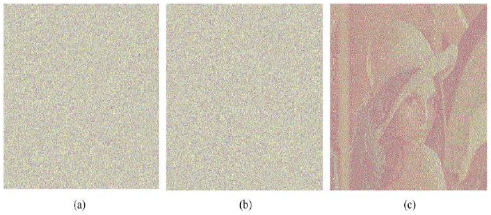


Fig. 4.5(A). Color pixel decomposition and reconstruction. Fig. 4.6(B). Two sharing transparencies and stacked elect: (a) Share 1, (b) Share 2, and (c) stacked image.

4.2. Visual Quality of Shares

VIPs are assigned freely to carry the visual information of original images in each subpixels m. Visual quality of the encrypted shares and of the decrypted share, denoted as Q_e and Q_d, respectively, mostly depends upon the size of pixel expansion m, and λ, the number of VIPs and γ, the number of 1 s in each m. The Q_e and Q_d are represented as

$$Q_e = \frac{\lambda}{m} \qquad \text{and}$$

$$Q_d(=\alpha) = \frac{w(s_1^{c_1,\dots,c_n}) - w(s_0^{c_1,\dots,c_n})}{m}$$

$$= 1 - \frac{\gamma + \lambda}{m}$$

We assume that the $w(s_1^{c_1,\dots,c_n})$ in Q_d is m, meaning all elements of the "OR"-ed row vector of the matrix are 1. The Q_d has the same value as contrast difference in the Algorithm.

4.3. Peak Signal-To-Noise Ratio (PSNR)

The phrase Peak Signal-to-Noise Ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale.

The PSNR is most commonly used as a measure of quality of reconstruction of lossy compression codecs (e.g., for image compression). The signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codecs it is used as an *approximation* to human perception of reconstruction quality, therefore in some cases one reconstruction may appear to be closer to the original than another, even though it has a lower PSNR (a higher PSNR would normally indicate that the reconstruction is of higher quality). One has to be extremely careful with the range of validity of this metric; it is only conclusively valid when it is used to compare results from the same codec (or codec type) and same content.

It is most easily defined via the mean squared error (MSE) which for two *m*×*n* monochrome images *I* and *K* where one of the images is considered a noisy approximation of the other is defined as:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left[I(i,j) - K(i,j)\right]^2$$

The PSNR is defined as:

$$PSNR = 10.\log_{10}\left(\frac{MAX_1^2}{MSE}\right)$$

$$= 20.\log_{10}\left(\frac{MAX_1}{\sqrt{MSE}}\right)$$

$$= 20.\log_{10}(MAX_1) - 10.\log_{10}(MSE)$$

Here, MAX_I is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255. More generally, when samples are represented using linear PCM with *B* bits per sample, MAX_I is 2^B-1. For color images with three RGB values per pixel, the definition of PSNR is the same except the MSE is the sum over all squared value differences divided by image size and by three. Alternately, for color images the image is converted to a different color space and PSNR is reported against each channel of that color space.

Typical values for the PSNR in lossy image and video compression are between 30 and 50 dB, where higher is better. Acceptable values for wireless transmission quality loss are considered to be about 20 dB to 25 dB. When the two images are identical, the MSE will be zero. For this value the PSNR is undefined (see Division by zero).

Algorithm of Visual Cryptograph using Error Diffusion

1. Transform the color image into three halftone images: C, M, and Y.
2. For each pixel Pij of the composed image, do the following:

   (a) According to the traditional method of black-and white visual cryptography, expand Cij, Mij and Yij into 2x2 blocks, C1ij ; C2ij ;M1ij ;M2ij and Y1ij , Y2ij .

   (b) Combine the blocks C1ij ;M1ij and Y1ij and fill the combined block corresponding to Pij in Share 1.

   (c) Combine the blocks C2ij ;M2ij and Y2ij and fill the combined block corresponding to Pij in Share 2.
3. Repeat Step 2 until every pixel of the composed image is decomposed, hence obtaining two visual cryptography transparencies to share the secret image.

4. After stacking the two sharing images, the secret image can be decrypted by human eyes.

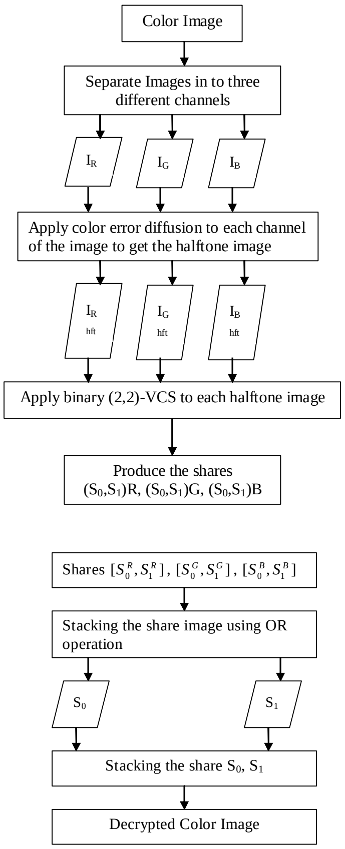
4.4. Encryption

In the encryption algorithm the shares are generated from the color image. The color image is decomposed into R, G, B channels. From these channels the Shares are created using following steps: *Color Halftone:* The color image "I" is decomposed into IR, IG and IB channels. Then apply the halftone for each channel to get

$I_{hlf}^{R}, I_{hlf}^{G}, I_{hlf}^{B}$ halftone images

[I] – split – to – RGB → $[I_R, I_G, I_B]$ $[I_R, I_G, I_B]$ – halftone → $I_{hlf}^{R}, I_{hlf}^{G}, I_{hlf}^{B}$

The color error diffusion is used for dithering technique. It reduces the color sets that render the halftone image and chooses the color from sets by which the desires color may be rendered and whose brightness variation is minimal. The Error diffusion technique is a dispersed dot dither method. In this method for each point in the image we find the closest color available and calculate the difference between the value in the image and the color two basic ways tp scam the image are with a normal left-to-right and top-to-bottom raster, or with an alternative left-to-right and right-to-left raster. This algorithm scans through all pixels in the original image normally starting from the pixel left and then goes through all pixels from left to right and up and down. The value of each pixel in I is compared with a threshold. Normally, the value of threshold is 0.5 in the non-modified error diffusion. Depending on whether the pixel value is bigger or smaller than the threshold a 1 (black dot) or a 0 (white dot) is set at the corresponding position in Ihft. The error is then diffused to a number of non-processed pixels. The diffusion of error is decided by an error filter. *Creation of Shares:* This method produces separate shares for red, green and blue.


Color Image
Separate Images in to three different channels
I_R
I_G
I_B
Apply color error diffusion to each channel of the image to get the halftone image
I_R hft
I_G hft
I_B hft
Apply binary (2,2)-VCS to each halftone image
Produce the shares $(S_0,S_1)R$, $(S_0,S_1)G$, $(S_0,S_1)B$
Shares $[S_0^R,S_1^R]$, $[S_0^G,S_1^G]$, $[S_0^B,S_1^B]$
Stacking the share image using OR operation
S_0
S_1
Stacking the share S_0, S_1
Decrypted Color Image

(A)

(B)

Fig. 4.7(A) Flow chart for Encryption. Fig.4.8(B) Flow chart for Decryption

$$I_{hlf}^{R}\,(2,2)VCS \rightarrow [S_0^R, S_1^R]$$

$$I_{hlf}^{G}\,(2,2)VCS \rightarrow [S_0^G, S_1^G]$$

$$I_{hlf}^{B}\,(2,2)VCS \rightarrow [S_0^B, S_1^B]$$

where $[S_0^R, S_1^R]$ are shares of red channel, $[S_0^G, S_1^G]$ are shares of green channel and $[S_0^B, S_1^B]$ are the shares of blue channel respectively.

4.5. 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.

1) *Stacking of Shares:* The stacking (OR) operation is performed to recover the image of each channel.

$[S_{0R}, S_{0G}, S_{0B}] \rightarrow$ stacking $\rightarrow S_0$ $[S_{1R}, S_{1G}, S_{1B}] \rightarrow$ stacking $\rightarrow S_1$

2) *Recovering the Image:* The secret color image is recovered by performing the stacking (OR) operation between the shares S0, S1

$[S_0, S_1]$ Stacking →Recovered secret image

4.6. Security of Our Scheme

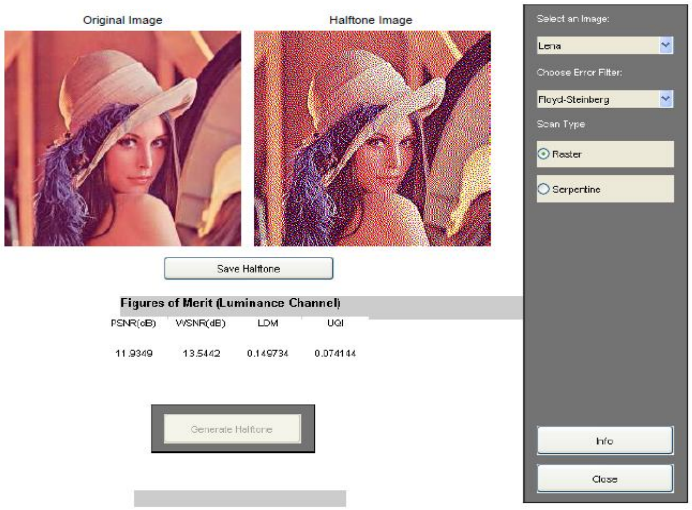
In our scheme, each row of basis matrices S_0 and S_1 has the same number of 1s, 0s regardless of the original image pixel color and the message pixel color is. That means each of the encrypted share has the same amount of information about the original images and the secret message. Further more in some cases without legitimate number of participants, k they have false information about the secret message because the VIP is decided during the error diffusion step. The hamming weight of $S_1[i]$, $W(S_1[i])$, should be greater than $W(S_0[i])$ in the decrypted share, but decryption with less than k shares can cause $W(S_1[i]) \leq W(S_0[i])$ which leads false decrypted information.

Only with proper number of shares the correct contrast difference is achieved. Unlike standard EVCS, the robustness of our proposed scheme to cheating comes from that fact that it is impossible to differentiate VIPs and other pixels in the encrypted shares and it is hard to know the actual VIP values which were decided during the error diffusion.

5. RESULTS

5.1 Results

A. Error diffusion with floyd Stenberg :



Select an Image: Lena

Choose Error Filter: Floyd-Steinberg

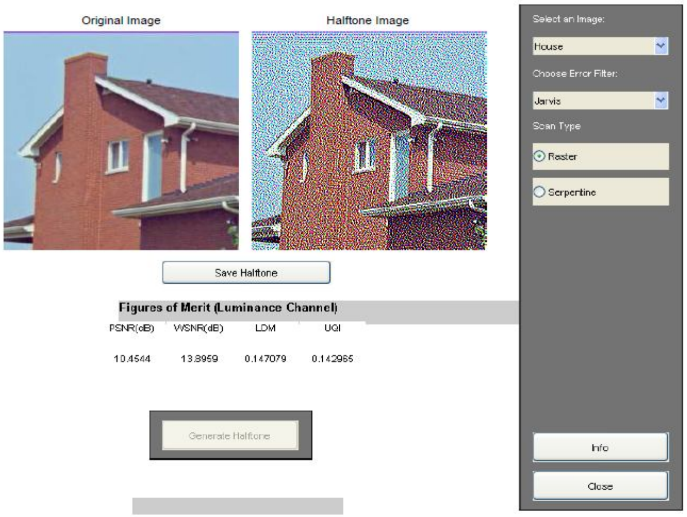
Scan Type: ● Raster ○ Serpentine

Figures of Merit (Luminance Channel)

PSNR(dB)	WSNR(dB)	LDM	UQI
11.9349	13.5442	0.149734	0.074144

Fig 5.1 error diffusion with floyd Stenberg

B. Error diffusion with Jarvis:



Select an Image: House

Choose Error Filter: Jarvis

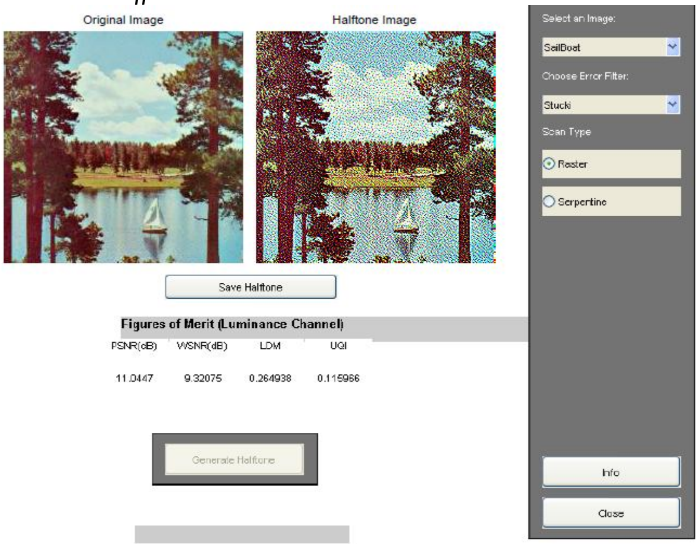
Scan Type: ● Raster ○ Serpentine

Figures of Merit (Luminance Channel)

PSNR(dB)	WSNR(dB)	LDM	UQI
10.4544	13.8959	0.147079	0.142965

Fig 5.2 error diffusion with jarvis

C. Error diffusion with Stucki :



Select an Image: SailBoat

Choose Error Filter: Stucki

Scan Type: ● Raster ○ Serpentine

Figures of Merit (Luminance Channel)

PSNR(dB)	WSNR(dB)	LDM	UQI
11.0447	9.32075	0.264938	0.115966

Fig 5.3 error diffusion with Stcuki

Table.1. Different Values of error diffusion with PSNR value

Image	**Class**	**PSNR**
Lena	Floyd-Steinberg	11.934
Lena	Jarvis	11.746
Lena	Stucki	11.796
House	Floyd-Steinberg	10.589
House	Jarvis	10.454
House	Stucki	10.528
Sailboat	Floyd-Steinberg	11.235
Sailboat	Jarvis	10.973
Sailboat	Stucki	11.044

5.2 CONCLUSION

The concept of VIP synchronisation and error diffusion to attain a color visual cryptography encryption method that produces meaningful color shares with visual quality is introduced. VIP synchronize the positions of pixels that carry visual information of original images across the color channels so as to retain the original pixel values the same before and after encryption. Error diffusion is used to construct the shares such that the noise introduced by the preset pixels are diffused away to neighbors when encrypted shares are generated. It is obvious that there is a tradeoff between contrast of encryption shares and the decryption share. However, we can recognize the colorful secret messages having even low contrast. Either VIP synchronization or error diffusion can be broadly used in many VC schemes for color images.

References:

[1] Naor and Adi Shamir, “Visual Cryptography”, advances in cryptology– Eurocrypt, pp 1-12,1995.

[2] C.C. Wu, L.H. Chen, “A Study On Visual Cryptography”, Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.

[3] H.-C. Hsu, T.-S. Chen, Y.-H. Lin, “The Ring Shadow Image Technology Of Visual Cryptography By Applying Diverse Rotating Angles To Hide The Secret Sharing”, in Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control, Taipei, Taiwan, pp. 996–1001, March 2004.

[4] S. J. Shyu, S. Y. Huanga,Y. K. Lee, R. Z. Wang, and K. Chen, “Sharing multiple secrets in visual cryptography”, Pattern Recognition, Vol. 40, Issue 12, pp. 3633 - 3651, 2007.

[5] Liguo Fang, BinYu, “Research On Pixel Expansion Of (2,n) Visual Threshold Scheme”, 1st International Symposium on Pervasive Computing and Applications ,pp. 856-860, IEEE.

[6] Mustafa Ulutas, Rıfat Yazıcı, Vasif V. Nabiyev, Güzin Ulutas, (2,2)- “Secret Sharing Scheme With Improved Share Randomness”, 978-1-4244-2881-6/08, IEEE, 2008.

[7] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, “Multiple-Image Encryption By Rotating Random Grids”, Eighth International Conference on Intelligent Systems Design and Applications, pp. 252-256 , 2008.

[8] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, “Multi-Secrets Visual Secret Sharing”, Proceedings of APCC2008, IEICE, 2008.

[9] Zhengxin Fu, Bin Yu, “Research On Rotation Visual Cryptography Scheme”, International Symposium on Information Engineering and Electronic Commerce, pp 533-536, 2009.

[10] E. Verheul and H. V. Tilborg, ”Constructions And Properties Of K Out Of N Visual Secret Sharing Schemes.” Designs, Codes and Cryptography, 11(2) , pp.179–196, 1997.

[11] C. Chang, C. Tsai, and T. Chen. “A New Scheme For Sharing Secret Color Images In Computer Network”, Proceedings of International Conference on Parallel and Distributed Systems, pp. 21–27, July 2000.

[12] Chin-Chen Chang , Tai-Xing Yu , “Sharing A Secret Gray Image In Multiple Images”, Proceedings of the First International Symposium on Cyber Worlds (CW.02), 2002.

[13] R. Lukac, K.N. Plataniotis, “Bit-Level Based Secret Sharing For Image Encryption”, Pattern Recognition 38 (5), pp. 767–772, 2005.

[14] error diffusion from, cryptography , psnr calculation, by http://en.wikipedia.org/wiki/Error_diffusion

[15] R.Youmaran, A. Adler, A. Miri , “An Improved Visual Cryptography Scheme For Secret Hiding”, 23rd Biennial Symposium on Communications, pp. 340-343, 2006.

[16] S.J. Shyu, “Efficient Visual Secret Sharing Scheme For Color Images”, Pattern Recognition 39 (5) ,pp. 866–880, 2006.