Visual Cryptography for Color Images Using Error Diffusion

CH. KARUNA¹, P.USHA²

¹Asst Prof, Dept of ECE, KG Reddy College of Engineering and Technology, Moinabad, AP-India,
E-mail: karuna.chirragoni@gmail.com.

²Asst Prof, Dept of ECE, KG Reddy College of Engineering and Technology, Moinabad, AP-India,
E-mail: usha.bopparam@gmail.com.

Abstract: As a result of the rapid advancement of various kinds of Internet technologies, more information are transmitted to all parts of the world from everywhere through the Net. Protecting this data in a safe and secure way which does not impede the access of an authorized authority is an immensely difficult and very interesting problem. Visual cryptography(VC) plays a vital role in present days where security is required. Color visual cryptography encrypts a color secret message into n color halftone image shares. Halftone is the process of transforming an image with greater amplitude resolution to one with lesser amplitude resolution. Color VC scheme implemented in this dissertation encrypts informative color image in such a way that result of encryption is in the form of shares. Shares do not reflect any information directly, information is scrambled instead. Each share carries some information which in unreadable. This dissertation 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 high quality shares. In this Dissertation visual cryptography is implemented using MATLAB software. MATLAB code is written for encryption and decryption process.

Keywords: VC, VIP, Halftone, Error Diffusion, Encryption, Decryption, MATLAB, PSNR.

I. INTRODUCTION

Visual Cryptography (VC) is a type of secret sharing scheme introduced by Naor and Shamir in 1994. Visual cryptography provides a very powerful technique by which one secret can be distributed into two or more shares. The secret image can be recovered simply by stacking the shares together without any complex computation involved. The shares are very safe because separately they reveal nothing about the secret image. These meaningful shares will not arouse the attention of hackers. Secret Hiding can be achieved in two ways: Cryptography and Steganography. Cryptography and steganography are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence. These techniques have many applications in computer science and other related fields: they are used to protect e-mail messages, credit card information, corporate data, etc. More specifically, Steganography is the art and science of communicating in a way which hides the existence of the communication. A steganographic system thus embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper’s suspicion. On the other hand, cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.

II. CRYPTOGRAPHY FOR IMAGES

Cryptography is not only used to send the text but it can be extended to images called Visual Cryptography where the image is stored in different shared images. When all the shares are stacked together then only the hidden image is received.

A. Basic Principle of VC

Basic visual cryptography is expansion of pixels. Each pixel of the images is divided into smaller blocks. There are always the same number white and black blocks. If a pixel is divided into two parts, there are one white and one black block. If the pixel is divided into four equal parts, there are two white and two black blocks.

B. Gray-Level Visual Cryptography

To understand the principles of VC, consider the two out-of-two visual cryptography scheme where each pixel p of the Secret Image is encoded into a pair of sub pixels in each of the two shares. If p is white, one of the two columns tabulated under the white pixel in Fig.1 is selected. If p is black, one of the two columns tabulated under the black pixel is selected. In each case, the selection is performed by randomly flipping a fair coin such that each column has 50% probability to be chosen. Then, the first two pairs of sub pixels in the selected
column are assigned to share 1 and share 2, respectively. Since, in each share, p is encoded into a black–white or white–black pair of sub pixels with equal probabilities, independent of whether p is black or white, an individual share gives no clue as to the value of p. In addition, as each pixel is encrypted independently, no secret information can be gained by looking at groups of pixels in each share.

Fig. 1: Construction of a two-out-of-two VC scheme: a secret pixel can be encoded into two sub pixels in each of the two shares.

Consider the superposition of the two shares as shown in the last row of Fig. 1. If a pixel p is white, the superposition of the two shares always outputs one black and one white sub pixel, no matter which column of sub pixel pairs is chosen during encoding. If p is black, it yields two black sub pixels.

C. Visual Cryptography for Color Images

The additive and subtractive color models are widely used to describe the constitutions of colors as shown in fig 2. In the additive color model, the three primary colors are red, green, and blue (RGB), with desired colors being obtained by mixing different RGB channels. The more the colors are mixed, the more the brightness of the light. When mixing all red, green and blue channels with equal intensity, white color will result. The computer screen is a good example of the additive color model.

In the subtractive model, color is represented by applying the combination of colored lights reflected from the surface of an object. By mixing cyan, magenta and yellow pigments, a wide range of colors can be produced. The more the pigments are added, the lower the intensity of the light is and, thus, the darker the light is. This is the reason it is called the subtractive model. Cyan, magenta, and yellow are the three primitive colors of pigment which cannot be composed from other colors. The color printer is an application of the subtractive model. A natural color image can be divided into three color channels red, green and blue (cyan, magenta, and yellow, respectively) and each channel constitutes a grey-level image, where each pixel is represented by a 8-bit binary value. When using (R, G, B) to describe a color pixel, (0; 0; 0) represents full black and (255; 255; 255) represents full white. Because (R, G, B) and (C, M, Y) are complementary colors, in the true color model, (R, G, B) and (C, M, Y) possess the following relationships: C = 255–R, M = 255–G, Y = 255–B; Thus, in the (C, M, Y) representation, (0; 0; 0) represents full white and (255; 255; 255) represents full black.

III. COLOR VISUAL CRYPTOGRAPHY

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 presented in Fig. 3. Every block of the sharing images therefore includes two white pixels and two color pixels. If pixel Pij of the composed image is (0; 0; 0), the distribution of the color pixels in the three sharing images is as the fifth row in Fig. 3. After stacked by the mask image, all the color pixels on the three sharing images are shaded by black pixels and only the white pixels can reveal, thus showing a white-like color. If pixel Pij is (1; 1; 0), only the C and M components are revealed, with the Y component being covered by the black mask. The distribution of the color pixels in the three sharing images is as the eighth row in Fig. 3. The eight combinations of the three primary colors of the composed image under this method are shown in above figure.

Fig. 3: Scheme of Color Cryptography.

images is as the fifth row in Fig. 3, thus showing a blue-like (cyan plus magenta) color. If pixel Pij is (1; 1; 1), the C, M, and Y parts can all be revealed, thus showing a black color. The distribution of the color pixels in the three sharing images is as the eighth row in Fig. 3. The eight combinations of the three primary colors of the composed image under this method are shown in above figure.
The first row in Fig. 3 shows that black color occupies half of the $2\times2$ block in the composed image. Since black can be seen as the composition of $C$, $M$, and $Y$, which means that $C$, $M$, and $Y$ occupy half of the whole block respectively, the densities of $C$, $M$, and $Y$ components within a $2\times2$ block are all $1/2$. If the distribution of color pixels in the composed image is as the fifth row in Fig. 3, only $C$ and $M$ are revealed with $Y$ being covered by the black mask. Since black can be seen as the composition of $C$, $M$, and $Y$, $C$ and $M$ can appear in all four blocks of a $2\times2$ block in the composed image, but yellow only appears in two. So the color intensity of $C$, $M$ and $Y$ can be denoted as $(1; 1; 1/2)$. If the distribution of color pixels in the composed image is as the eighth row in Fig. 3, four blocks are all black and the color intensity $(C, M, Y)$ can be denoted as $(1; 1; 1)$. White pixels in a stacked image are no longer pure white $(0; 0; 0)$, but are half black-and-white $(1/2; 1/2; 1/2)$ instead. The colors in a stacked image are no longer distributed between $(0; 0; 0)$ and $(1; 1; 1)$, but are distributed between $(1/2; 1/2; 1/2)$ and $(1; 1; 1)$. This result is similar to the contrast loss occurred in black-and-white visual cryptography.

IV. HALFTONE PROCESS

A general idea of the dissertation is described and block diagram as shown in fig 4. In this dissertation input is a secret image of size $128\times128$ pixels and four cover images of size $256\times256$. The images can be of any standard format. The secret image and four images must be halftoned ahead of encryption process. The error diffusion algorithm is considered to halftone an image. For encrypting the secret image two random binary matrices $S_0$ and $S_1$ is considered. The size of these matrices is same as that of cover images. After encryption these cover images are called share images. The receiver decrypts the secret image from the four share images. PSNR of original secret image and reconstructed image is calculated for different halftone techniques. Halftoning is the process of transforming an image with greater amplitude resolution to one with lesser amplitude resolution. The goal of halftoning is to produce an image that resembles, as closely as possible, the original image. The digital halftoning is achieved by making use of the threshold mask. For each pixel, the halftoned binary pixel is determined as black if the original grayscale pixel is greater than or equal to the mask value and is determined as white vice versa. This has been practiced for over a hundred years in the printing industry; the solution for displaying continuous-tone images with only black or white dots. The halftone techniques are:

- Threshold
- Ordered Dithering
- Error Diffusion

A. Threshold

The simplest method of converting a grayscale image to a binary image is by threshold, i.e. a two-level (one-bit) quantization. Let $f(i, j)$ be a grayscale image, and $b(i, j)$ be the corresponding binary image based on simple thresholding. For a given threshold $T$, the binary image is computed as

$$b(i, j) = \begin{cases} 255 & \text{if } f(i, j) > T \\ 0 & \text{else} \end{cases}$$

(1)

Fig 5 illustrates the conversion to a binary image by thresholding, using $T = 127$.

B. Ordered Dithering

Ordered dithering uses a fixed matrix of thresholds. The matrix is a $k\times k$ square containing a permutation of the integers $0\ldotsk^2-1$; $k^2$ must also be the number of grey levels. Common Bayer threshold matrices used are of size $8 \times 8$. For each matrix value a threshold is calculated as $k\times255/64$, where $k$ is the matrix value and 64 is the number of elements in the matrix. Ordered dithering consists of comparing blocks of the original image to a grid of thresholds called a dither pattern as shown in fig 6. The algorithm is simple: tile the image with the threshold matrix. At each pixel, if its value is greater than the threshold at that point, output a white
pixel; otherwise output a black pixel. The whole array looks like:

\[
\begin{bmatrix}
0 & 32 & 8 & 40 & 2 & 34 & 10 & 42 \\
16 & 48 & 24 & 58 & 18 & 50 & 26 & 58 \\
4 & 36 & 12 & 44 & 6 & 38 & 14 & 46 \\
20 & 52 & 28 & 60 & 22 & 54 & 30 & 62 \\
1 & 33 & 9 & 41 & 3 & 35 & 11 & 43 \\
17 & 49 & 25 & 57 & 19 & 51 & 27 & 59 \\
5 & 37 & 13 & 45 & 7 & 39 & 15 & 47 \\
21 & 53 & 29 & 61 & 23 & 55 & 31 & 63
\end{bmatrix}
\]

Fig.6: Result of Ordered Dithering Halftone.

### C. Error Diffusion

Error diffusion techniques are used in most halftoning transformations to convert a multiple-level color image into a two level color image. Error diffusion is a simple and efficient way to halftone a grayscale image. Error diffusion produces halftone images of much higher quality than other halftone techniques. The simple concept of this technique is the diffusion of errors to neighboring pixels. The quantization error at each pixel is filtered and fed into a set of future inputs. Unlike other halftone methods, error diffusion is classified as an area operation, because what the algorithm does at one location influences what happens at other locations. An illustration of the algorithm is shown in Fig.7 (a), assuming that the input signal varies from \( g=0 \) to \( g=1 \), the threshold block simply sets the output to 0 for values less than \( 1/2 \) and to 1 for values greater than or equal to \( 1/2 \). The binary output signal is subtracted from the prethreshold signal to form an error. This error is “diffused” into yet to be considered input values as governed by the error filter. The signal consisting of past error values is passed through this filter to produce a correction factor to be added to future input values. This algorithm was first introduced by Floyd and Steinberg, who also proposed the error filter shown in Fig.7 (b). The algorithm processes pixels in a raster order, so that only nonzero filter elements are those in front of and below the current pixel. As with all error filters, the elements must sum to one.

![Error Diffusion Diagram](image)

Fig.7: (a) The Error diffusion algorithm, (b) The error filter identified by the Floyd and Steinberg.

where "_" denotes a pixel in the current row which has already been processed, and '#' denotes the pixel currently being processed.

### V. ALGORITHM

#### A. Encryption Process

To encode secret pixels, the secret information pixels are distributed as homogeneously as possible. In each cover image 4096 secret image pixels can be hidden. VIPs are pixels on the encrypted shares that have color values of the original images. This algorithm generates a set of random binary matrices \( S_0 \) and \( S_1 \) which are of size of cover image. In this method, secret pixels are hidden using ex-or operation. \( x_{(p,q)} \) represents the secret image pixel:

- for the color channel \( C \) of the secret message \( x_{(p,q)} \)
  - for \( p = 1:n:256 \)
  - for \( q = 1:m:256 \)
    - (a): if the bit \( x_{(p,q,c)}==0 \) then
      \[ \text{share}_i\_\text{img}_{(p,q,c)} = \text{xor} (S_{0(p,q)}, x_{(p,q,c)}) \]
    - (b): if the bit \( x_{(p,q,c)}==1 \) then
      \[ \text{share}_i\_\text{img}_{(p,q,c)} = \text{xor} (S_{1(p,q)}, x_{(p,q,c)}) \]
  - end for
  - end for
- Repeat above process for color channel \( G \) and \( B \)
- Repeat above process for all cover images.
C represents the RGB color channel of the secret image. \(p\) and \(q\) represents the rows and columns of the cover images. \(m\) and \(n\) represents after how many rows and columns a secret image pixel can be encrypted in each cover image. If the secret image pixel value is zero select \(S_0\) matrix and perform ex-or operation of secret image pixel and \(S_0\) matrix at position \((p,q)\), else perform ex-or of secret image pixel and \(S_1\) matrix at position \((p,q)\) and place it in first share image at position \((p,q)\). Repeat the process for all the color channels and all cover images.

B. Decryption Process

At the receiver side all the shares are collected and using the VC matrices \(S_0\), \(S_1\) the information is extracted from the meaningful shares and thus forms the reconstructed secret image. \(i\) and \(j\) represents rows and columns of the share images. \(n\) and \(m\) represents after how many rows and columns a secret image pixel should be extracted from share images and the value is same as in encryption process. If the share image value is equal to \(S_0\) matrix value at position \((i,j)\) then perform ex-or operation of the share image and \(S_0\) matrix value else perform ex-or of the share image and \(S_1\) matrix and place it in a variable. Perform same process for all color channels and all the share images.

- for the color channel \(C\) of the share image
- for \(i=1:n\) : 256
- for \(j=1:m\) : 256
  a) if \(\text{share}_\text{img}(i,j,c)=S_{0(i,j)}\) then
    \(\text{si}_\text{img}=\text{xor(share}_\text{img}(i,j,c),S_{0(i,j)})\)
  b) else
    \(\text{si}_\text{img}=\text{xor(share}_\text{img}(i,j,c),S_{1(i,j)})\)
- end for
- end for
- Repeat above process for channel G and B
- end for
- Repeat above process for all share images.

C. Peak Signal-to-Noise Ratio (PSNR)

The Peak Signal-to-Noise Ratio block computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and a compressed image. 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. The higher the PSNR, the better the quality of the compressed or reconstructed image. PSNR is most easily defined via the mean squared error (MSE) which is the average squared difference between a reference image and a distorted image. It is computed pixel-by-pixel by adding up the squared differences of all the pixels and dividing by the total pixel count. For images \(A = \{a_1 .. a_M\}\) and \(B = \{b_1 .. b_M\}\), where \(M\) is the number of pixels:

\[
MSE(A, B) = \frac{1}{M} \sum_{i=1}^{M} (a_i - b_i)^2
\]

(2)

For images \(A = \{a_1 .. a_M\}\), \(B = \{b_1 .. b_M\}\), and \(MAX\) equal to the maximum possible pixel value, PSNR is calculated using the following equation:

\[
PSNR(A, B) = 10 \log_{10}\left(\frac{MAX^2}{MSE(A, B)}\right)
\]

(3)

In this dissertation, PSNR between original secret image and reconstructed image is calculated.

VI. RESULTS AND DISCUSSIONS

A. Results for Visual Cryptography for Color Images using Error Diffusion

The actual secret image which represents the confidential information that is to be sent in a secure way to the destination. Image size is 128x128 pixels.

Fig.7: Secret Image.

These are the four colored images (fig 8) which plays the key role for the secure transmission of information. These are called the cover images in to which the secret image (fig 7) is to be encrypted. Image size is of 256x256 pixels. In this two images are natural images.

Fig.8: the halftone of the four cover images.
These are the halftone images of the secret image (fig 9) and four cover images using error diffusion algorithm. Halftoning tries to reproduce full range of gray/color while preserving quality and spatial resolution. The filter used in this algorithm is Floyd Steinberg error filter. After halftoning the memory size is reduced to half.

Fig. 9: Halftone Secret Image.

Fig. 10: the four share images that is obtained after the secret image.

Fig. 11: the reconstructed Secret image obtained from four share images.

Fig. 12: Reconstructed Secret Image.

PSNR = 22.5946 db

B. Results for Visual Cryptography for Color Images using Ordered Dithering

The actual secret image which represents the confidential information that is to be sent in a secure way to the destination. Image (fig 13) size is 128×128 pixels.

Fig. 13: Secret Image.

These are the halftone images (fig 14 and 15) of secret image and four cover images using ordered dithering technique. A bayer threshold matrix of size 8×8 is considered.

Fig. 14: Halftone Secret Image.

This is the reconstructed Secret image obtained from four share images (fig 16) and the image size is 128×128 pixels. PSNR of original secret image and reconstructed image is calculated (fig 17).
C. Results for Visual Cryptography for Color Images using Threshold

The actual secret image which represents the confidential information that is to be sent in a secure way to the destination. Image fig 18 size is 128×128 pixels.

Fig. 18: Secret Image.

These are the halftone images of secret image (fig 19 and 20) and four cover images using threshold. Threshold is calculated as average of all the pixel values. If the pixel value is greater than threshold it is set to one else zero.

Fig. 19: Halftone Secret Image.

Fig. 20: halftone Images of Secret Image.

This is the reconstructed Secret image obtained from four share images (fig 21) and the image size is 128×128 pixels. PSNR of original secret image and reconstructed image is calculated (fig 22).
VII. CONCLUSION AND FUTURE SCOPE

Visual Cryptography provides one of the secure ways to transfer images on the Internet. In this dissertation a \((n, n)\) secret image sharing scheme is considered. The input images can be of any standard format. The same algorithm has been applied to different halftone techniques and from the results it is observed that Visual Cryptography using Error Diffusion provides better visual quality shares. Halftone reduces the memory capacity of the images by half. The scheme proposed generates high quality of meaningful color shares as well as the colorful decrypted shares. It is obvious that there is a tradeoff between contrast of encryption shares and the decryption share; however, the color secret image can be recognized in even low contrast levels. PSNR of original and reconstructed images is calculated for all the three methods and it is observed that mathematically PSNR is high for threshold technique, but visually the quality of shares and reconstructed image is better for error diffusion technique.

VIII. REFERENCES


