

RGB Based Secret Sharing Scheme in Color Visual Cryptography

M.Karolin¹, Dr.T.Meyyapan²

Research Scholar, Department of Computer Science and Engg, Alagappa University, Karaikudi, India¹

Professor, Department of Computer Science and Engg, Alagappa University, Karaikudi, India²

Abstract: Information hiding in the communication spectrum became a critical task. The Visual Cryptography is a type of cryptography that allows the image to be divided into multiple numbers of shares called transparent shares and then transmission of images. The intruder hence cannot understand the distorted image and thus the data communication becomes secured. In existing methods works for color images with 8 colors and even few of them without halftone techniques. In this paper, the authors propose a method for images with 256 colors which are converted to 16 standard RGB colors format. It generates shares without compromising the resolution. The Floyd – Steinberg dithering algorithm is used to manipulate the 256 color code image to reduce it to 16 standard colors code image. The proposed method employs (2, 2) XOR-Based visual cryptography method is also used to generate shares. Decryption procedure enables secret image sharing and stacking. Although, the proposed method converts the 256 color image to 16 color code format for the share creation, the intensity of the original image is maintained. The resulting scheme gives the perfect security of the shares that are well encrypted and the visual quality of the stacked image is very good. The experimental results of the proposed method are compared with that of 8 color RGB share generation techniques.

Keywords: Visual cryptography, XOR, 16 standard color code image, Floyd – Steinberg dithering.

I. INTRODUCTION

The exploration in the internet era makes it difficult to keep the information to be confidential. The secrecy of the message should be protected both at the sender's storage as well as in the transmission medium. The network services are now open to almost everyone and that is why the probability of reaching confidential data from one computer to another computer or from one client to another client may not be safe at all. Many techniques such as the cryptography, Steganography were involved for the purpose. In cryptography, the information is completely converted to unintelligible format so that the intruder cannot hack them.

Visual Cryptography is the technique for encrypting, user defined image into multiple number of shares. The technique was proposed by Naor and Shamir in 1994 [2]. It works on the principle that , the secret image provided by the user transforms them into printable transparent shares and these shares can be distributed to clients through communication mediums. On the other end the receiver may regenerate the original image by stacking all transparent shares on each other[3]. The most notable feature of Visual Cryptography is that in this approach is that it can recover a secret image without any computation.

It exploits the human visual system to read the secret message from some overlapping shares, thus overcoming the disadvantage of complex computation required in the traditional cryptography [1].The threshold method involved in the visual cryptography makes the application easier and thus reduce its complexity. Visual Cryptography for color images basically divided into three approaches, namely larger pixel expansion, conversion of color images to black and white and utilizes binary representation of the color images [5]. Most of the visual

cryptography methods, process in black and white and the grayscale images. The color image encryption is placed in our paper. Many algorithms are involved in the color image encryption in visual cryptography. Rijmen and Preneel have proposed a visual cryptography approach for color images [4].

The approach of Rijmen and Preneel indeed can produce 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. Hence, the VC on RGB images concentrates on our proposed work. In VC decryption process is limited up to the human visual system. This makes the VC a good scheme for cryptography of images that holds low computation load requirement. VC scheme has been widely placed in many applications such as threshold cryptography, electronic cash, watermarking of images etc. The paper is structured as follows. Section 1 consists of basic information about visual cryptography, shares and secret images. Section 2 describes the literature review, related to the proposed methodology. Section 3 comprises of our proposed method for the color images in RGB format. Section 4 comes out with the experimental results. Section 5 concludes the work.

II. RELATED WORKS

Visual secret sharing for color images was introduced by Naor and Shamir based upon cover semi groups [2]. Rijimen presented a 2-out-of-2 VC scheme by applying the idea of color mixture. Stacking two transparencies with different colors gives new third color mixture. Hou et al. [6, 1] proposed a method to improve the drawback of using limited colors in shares. They used

the binary encoding to represent the sub pixels selected for each block and applied the AND/OR operation randomly to compute the binary code for the stacking sub pixels of every block in the cover images. The code ranges from 0 to 255, but it can be even larger depending on the expanding factor. Consequently, a secret image can be a 256 color or true-color one.

Pooja and Dr. Y.S. Lalitha [11] uses pseudo randomized authentication procedure for color image visual cryptography. They use the halftone images which represent the resultant image in the same size as the original secret image. An algorithm is presented in their work and experimentally verified. According to their results, the (2, 2) pseudo-randomized visual cryptography, which generates shares, based on pixel reversal, randomized reduction in original pixel and subtractions of the original pixel. The original secret image is divided so that it reveals the secret image after inverse operation of qualified shares. This scheme reveals reduced pixel expansion, required for retrieval of the secret image and no loss in contrast of the decrypted image.

Sougata Mandal, Sankar Das and Asoke Nath, [7] applied different data hiding algorithm based on visual cryptography. The authors of the paper tried to hide any color message/image in two or more shares. Their method is that, from one share it impossible to create the second share or to extract the hidden secret message from one share without having the other share(s). It may be used for reconstructing password or any kind of important message or image.

Joshi Jesalkumari.A and R.R.Sedamkar [8], explains the concept of modified VC for colored secret images. The intent of their work is to describe the performance of the XOR Based visual cryptography schemes and traditional VCS on the basis of quality of the reconstructed image and type of shares generated for colored images. From their experimental results, it is concluded that XOR based VC gives better visual quality. But the color combo involves CMY pattern and the grayscale images.

J. Tamilarasi, V. Vanitha, T. Renuka [9], describes the method for improving Image Quality in extended Visual Cryptography for Halftone images with no pixel expansion. The advantage of their method lies in the term that the secret and share image have the same size. It produces less noise in recovering image. By using their method, it recovers the image by stacking the shares using XOR operation. The gray scale image is taken for the purpose and is converted to its binary representation. To avoid expansion of the image preprocessing has taken place after the half toning process.

Anantha Kumar Kondra, Smt. U. V. Ratna Kumari [10], introduced a new solution that helps to identify the errors in the shares and to verify the authentication. The CRC algorithm and VC scheme with error diffusion method generates the quality of the shares, diffuses the error and provides security against the threats like modification of the message, fabrication, interception etc. The author develops an encryption method to construct color EVC scheme with VIP synchronization. It

synchronizes the positions of the 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. Cryptanalysis is also performed to show the security concern of the method.

III. VISUAL CRYPTOGRAPHY BASIC MODEL

Visual Cryptography is a type of cryptography in which images can be securely encrypted by dividing them in a distorted image called transparent shares and transmitted through physically by printing these shares on transparency sheets to the intended user. Visual Cryptography takes in many formats such as for grayscale images, black and white images and for the color images. The proposed method is done for the color visual cryptography. In the Gray scale model, to ensure the transparencies the white pixels of black-and-white images as transparent. Typically, the black-and-white visual cryptography decomposes every pixel in a secret image into a 2×2 block in the two transparencies according to the rules of the basic model. When a pixel is white, the method chooses one of the two combinations of white pixels to form the content of the block in the two transparencies; when a pixel is black, it chooses one of the other two combinations. Then, the characteristics of two stacked pixels are: black and black is black, white and black is black, and white and white is white. Therefore, when stacking two transparencies, the blocks corresponding to black pixels in the secret image are full black, and those corresponding to white pixels are half-black-and-half-white, which can be seen as 50% gray pixels. As for information security, there are six possible patterns from which every block in a transparency can randomly choose, so the secret image cannot be identified from a single transparency.

The gray-level images are transformed into halftone ones before printing, and the transformed Halftone images are black-and-white only; such an image format is very suitable for the traditional method to generate the shares of visual cryptography. For each black or white pixel in the halftone image, decompose it into a 2×2 block of the two transparencies according to the rules. If the pixel is white, randomly select one combination from the former two rows as the content of the blocks in Shares 1 and 2. If the pixel is black, randomly select one combination from the latter two rows as the content of the blocks in the two transparencies. Repeat until every pixel in the halftone image is decomposed, hence resulting in two transparencies of visual cryptography to share the secret image.

3.1 Proposed Methodology

A. Visual Cryptography for Color Images

In the proposed method, the RGB (Red, Green and Blue) color image is taken for the information sharing. The Floyd – Steinberg dithering algorithm is used to manipulate the 256 code image to low code image. It achieves the dithering using error diffusion, and takes the nearest neighbor pixel to create the share. The existing algorithms uses CMY color image format is converted into

eight color codes. In our proposed method, the RGB color code is separated into 16 standard color code formats without reduction of the resolution. The dithering algorithm is used instead of half toning the image. By dithering for every share separate array is created and manipulated. For the secret image sharing and then stacking the decryption is involved. By using the proposed method, the intensity of the original image is maintained as well as 16 shares can be created and used.

B. Floyd-Steinberg Dithering Algorithm

Floyd–Steinberg dithering is an image dithering algorithm, used by the image manipulation tools. It executes the dithering of image using error diffusion technique, which means it adds the residual quantization error of a pixel onto its neighboring pixels. Dither is an intentionally applied form of noise used to randomize quantization error, also preventing large-scale patterns such as color banding in an images. Dither is routinely used for processing both in audio as well as video data. The diffusion coefficient pixels have the property, that if the original pixel values are exactly halfway in between the nearest available colors, the dithered result is a checkerboard pattern.

This property is applied in the share creation process of visual cryptography. The working of the dithering algorithm is as follows: for each point in the image, first find the closest color available. Calculate the difference between the value in the image and the color in the image. Now divide up these error values and distribute them over the neighboring pixels which have not visited yet. When get to these later pixels, just add the errors distributed from the earlier ones, clip the values to the allowed range if needed, and then continue. The array structure thus formed without the noise level is used to construct the shares. The bit-depth transitions generated from the dithering algorithm increases the intensity of the image. The dithering is applied to the images with limited intensity resolutions.

C. Share Generation Process

This section consists of the algorithm for the share generation in the color models. In the existing methods the additive and the subtractive color models were used to halftone or to produce the continuous shares and the stacked images. Then using the CMY model around standard 8 color codes was generated. The proposed algorithm uses the basic RGB color code for share creation and for stack images and generates 16 color codes. The algorithm with standard 16 color code is as follows:

Steps for Share Generation

- *Step 1:* Consider the input secret image as the RGB (Red, Green, Blue) model color image.
- *Step 2:* The input image is now fed to the error diffusion process that uses Floyd – Steinberg algorithm to diffuse the image.
- *Step 3:* Repeat Step-2 until every pixel in the image is decomposed. The dithering process then computes the standard sixteen named color codes.

- *Step 4:* According to the traditional method of Naor and Shamir’s black and white VC Schemes, expand each pixel into 2 X 2 blocks arrays.
- *Step 5:* This step results in generation of two shares (transparencies) of the secret image.
- *Step 6:* Finally, the stacked image is produced by combining the two shares that are generated.

IV. RESULTS AND DISCUSSIONS

4.1 Experimental Results

This section presents the simulation results illustrating the performance of the proposed Method. The proposed work is implemented with Visual Studio 2010 and language user C# .NET FRAMEWORK 4.0 using windows 8- 64-bit operating system with core2duo of 2.66 GHz machine and 3GB RAM. Hence the proposed system is a strong one. To carry out the experiments, four 128x128 RGB Color images shown in Figure 2, “Lena”, “Jet”, and “Barbara” served as the test images.

4.2 Performance Analysis

The following section shows various performance metrics considered to demonstrate the quality of generated shares. The two main parameters considered is the PSNR (Peak Signal to Noise Ration) and MSE (Mean Square Error). The PSNR computes the ratio of maximum possible signals to that of the noise that affects the image fidelity depiction. The peak error is calculated using PSNR ratio in Decibels unit. MSE is the measure which represents the cumulative squared error between the original image and resultant image. a measure of the peak error.

$$MSE = \frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [C_1(i, j) - C_2(i, j)]^2$$

$$PSNR = 10 \log_{10} \left(\frac{M \times N \times 255^2}{MSE} \right)$$

TABLE I

PSNR AND MSE VALUES FOR VARIOUS TEST IMAGES
FONT SIZES FOR PAPERS

Images	PSNR	MSE
Lena	31.33	97
Jet	29.47	93
Girl	30.48	95

4.3 COMPARATIVE ANALYSIS

A. Visual Quality Comparison

Fig 2 shows the Original image, and its shares. The shares are created based on the above proposed algorithm contains standard 16 color code method along with error diffusion process. Apart from the existing methods, the proposed algorithm works for the color code models. The proposed method yields, perfect share generation as well as ends in good reconstruction of the images with their desired quality of the image.

















Colors	Color Name	Decimal Code	Colors	Color Name	Decimal Code
	White	RGB(255,255,255)		Silver	RGB(192,192,192)
	Black	RGB(0,0,0)		Gray	RGB(128,128,128)
	Red	RGB(255,0,0)		Maroon	RGB(128,0,0)
	Lime	RGB(0,255,0)		Olive	RGB(128,128,0)
	Blue	RGB(0,0,255)		Green	RGB(0,128,0)
	Cyan	RGB(0,255,255)		Purple	RGB(128,0,128)
	Magenta	RGB(255,0,255)		Teal	RGB(0,128,128)
	Yellow	RGB(255,255,0)		Navy	RGB(0,0,128)

Fig 1. Standard sixteen named color models




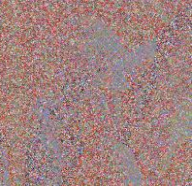
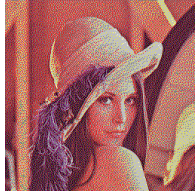


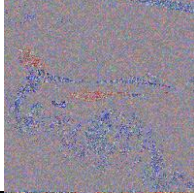
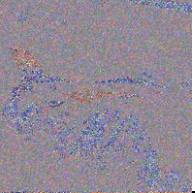

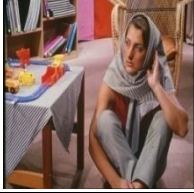

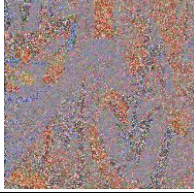
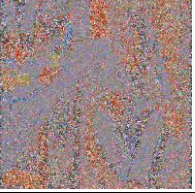

Original image	Dithered image	Share 1	Share 2	Stacked Image
				
				
				

Fig 2. Experimental Results for the Test Image









	Original image	Share 1	Share 2	Stacked Image
Proposed Method				
Existing Method				

Fig 3. Comparative Results of the proposed and Existing Methods

By implementation of the proposed algorithm, the user need not preprocess the image that degrades the visual quality. The stacked image from our proposed method is clear and the visual quality is thus enhanced. Hence, the security of the data is considerably increased. The following table shows a comparative analysis of the proposed method with existing method (8 color code).

B. Performance Based Comparison

The values in table 2 give the quality evaluation by using the performance metrics PSNR and MSE as the results. These results are analysed between various existing methods [12] such as the Floyd and Steinberg Dithering, Adaptive order dithering and color error diffusion using XOR. The results show that the proposed method ended with better PSNR values and Minimized Mean Square Error. The proposed algorithm gives good share generation with minimum error values proves it suits better for RGB color image share generation.

TABLE 2

COMPARATIVE ANALYSIS OF PSNR AND MSE VALUE BETWEEN VARIOUS EXISTING METHODS TO THE PROPOSED METHOD

Picture Quality Evaluation	Floyd and Steinberg Dithering	Adaptive Order Dithering	CED using XOR	Proposed Method
PSNR	24	25.25	27.17	31.33
MSE	180.90	190	125	97

V. CONCLUSION

Visual Cryptography provides one of the secure ways to transmit images on the Internet. In existing visual cryptography scenario, there exists very low security for shares created. Unlike most studies of visual cryptography, this paper exploits the techniques of dithering technology and color decomposition to construct 16 color code models from standard RGB. To overcome the limitations of existing techniques, the proposed method constructs a 16 color code mechanism which is more appropriate to protect the shares. The proposed method can be improved by civilizing the colors created and to produce clear resultant image. The algorithm strengthens the security by generating more number of colors to generate shares. The experimental results reveal that the proposed scheme ensures best reconstruction of images with desirable quality due to the tunable feature in the secret share creation step.

REFERENCES

[1] Young-Chang Hou, "Visual cryptography for color images", Journal of Pattern Recognition, Vol.36, pp.1619 – 1629, 2003.
 [2] M. Naor and A. Shamir, "Visual cryptography," Proceedings of Advances in Cryptology: Eurocrypt94, Lecture Notes in Computer Science, Vol. 950, pp. 1 - 12, 1995.
 [3] L. N. Pandey and Neeraj Shukla, "Visual Cryptography Schemes using Compressed Random Shares", in International Journal of

Advance Research in Computer Science and Management Studies, Volume 1, Issue 4, September 2013, pp:62 – 66.
 [4] V. Rijmen, B. Preneel, Efficient colorvisual encryption for shared colors of Benetton, Eurocrypt'96, Rump Session, Berlin, 1996.
 [5] Veena Hemke and Ranjana Shende, "Color Extended Optical Cryptography Using Random Shares For Visual Transferring Scheme", in IORD Journal of Science & Technology E-ISSN: 2348-0831 Volume 1, Issue VI, OCT 2014 PP 19-24.
 [6] Y.C. Hou, F. Lin, C.Y. Chang, Improvement and implementation of the secret color image sharing technique, Proceedings of the Fifth Conference on Information Management, Taipei, November 1999, pp. 592–597.
 [7] Sougata Mandal, Sankar Das and Asoke Nath, "Data Hiding and Retrieval using Visual Cryptography", in International Journal of Innovative Research in Advanced Engineering (IJIRAE), Volume 1, Issue 1, April 2014, pp:102 – 110.
 [8] Joshi Jesalkumari.A and R.R.Sedamkar, "Modified Visual Cryptography Scheme for Colored Secret Image Sharing", in International Journal of Computer Applications Technology and Research, Volume 2– Issue 3, 2013, pp: 350 – 356.
 [9] J. Tamilarasi, V. Vanitha, T. Renuka, "Improving Image Quality In Extended Visual Cryptography For Halftone Images With No Pixel Expansion", in International Journal of Scientific & Technology Research, Volume 3, Issue 4, April 2014, pp:126-131.
 [10] Anantha Kumar Kondra, Smt. U. V. Ratna Kumari, "An Improved (8, 8) Colour Visual Cryptography Scheme Using Floyd Error Diffusion", in International Journal of Engineering Research and Applications, Vol. 2, Issue 5, September- October 2012, pp.1090-1096.
 [11] Pooja and Dr.Lalitha Y. S, "Non Expanded Visual Cryptography for Color Images using Pseudo-Randomized Authentication", in International Journal of Engineering Research and Development, Volume 10, Issue 6 (June 2014), PP.01-08.
 [12] Manika Sharma and Rekha Saraswat, "Secure Visual Cryptography Technique for Color Images Using RSA Algorithm", in International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 10, April 2013.