ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

An Efficient Single Share Generation Scheme in Visual Cryptography

S.Sharmila[1] and Dr.T.Meyyapan[2]

[1]*M.Phil Research Scholar,* [2]*Professor*

Department of Computer Science and Engineering, Alagappa University,

Karaikudi-600 003, Tamilnadu, India.

[1]sharmila916@gmail.com, [2]meyyappant@alagappauniversity.ac.in

***Abstract*— Current trend of security technology is well growth in key apprehension. One of the well-known technologies is secure image transmission, through which the user can achieve the precise level of protection. Visual cryptography (VC), a modern cryptographic technique, used to transfer the image through the internet in a secluded manner. The basic concept of VC method is the given image is divided into two or more segments named as "shares". Again, when all the shares are arranged together the original image will be showed. The application level usage of image distribution using existing techniques such as gray level images, black and white images, and color images. It is considered as an unsafe method, because the hackers and their activities can affect any network administrator on the internet. Hence, the image share distribution should be more secure. This paper proposed a single share construction method for the color image visual cryptography. The image brightness is improved in 2×2 VC method to use Floyd-Steinberg dithering method instead of customary halftone technique. This method includes, the shares generation using the 2×2 VC method, then the LSB technique is preferred to insert the shares, from one another using symmetric key and finally get single share. The implemented experimental results lead a platform for single share construction.**

***Keywords*— Visual Cryptography, Hou's Method, Floyd – Steinberg Dithering Method, LSB Algorithm, Halftone technique.**

I. INTRODUCTION

Data transfer is the foremost responsibility of nowadays network. Hence, security of the data remains an important concern in data transfer. Cryptographic algorithms, results as the resolution to the above concerned problem. Moreover, the textual contents were more easily secured by using the cryptographic algorithms. Visual cryptography, means secure the data that is in image format. It is very useful for sharing the images through the internet for transmission between sender and receiver. By using this technique the decryption method is eliminated, which in turn saves time. In the process of visual cryptography, secret image split into two scrambled images called shares and by stacking these shares, the original image will reveal. In Visual cryptography, no computation of the decryption is required [2]. The scheme proposed by Naor and Shamir in 1994 [1] uses the (2x2) VC scheme in binary image. The basic VC scheme states as below in practical manner. Usually the input will be provided as text in this method. Hsien-Chu Wu [4], have proposed a new color VC scheme which generates meaningful shares by using the halftone technique, secret coding table and cover coding table. The secret image decrypted by stacking the two meaningful shares together. In their approach, they also extend a single pixel into a 2×4 block. However, the size of the share remains the same as the 2×2 pixel expansion case. Hence, by this way, providing a considerable part of the storage space can be saved, and more importantly, the shares do not at random noise format. Arun Ross [5], proposed visual cryptography for imparting privacy to biometric templates. In the case of fingerprints and Iris, the templates are decomposed into two noise-like images using (2,2) Visual Cryptography Scheme, and the spatial arrangement of the pixels in these images varies from block to block, it is impossible to recover the original template without accessing both the shares. The XOR operator is employed to superimpose the two noisy images and to recover the complete original template. Gwo-Chin Tai [3] proposed a novel public robust digital watermarking scheme based on visual cryptography. In this scheme, a binary logo is used to represent the ownership of the host image. The logo used to generate a private sharing image and a public sharing image by visual cryptography algorithms. The public sharing image will act as the watermark image, embedded within the host image. An error correction-coding scheme, then applied to protect the watermark. The extended algorithm and public share image can be open to the public users, but the provider of the image, to whom the private key resides, is the authorized user to retrieve the ownership logo.

II. RELATED WORK

Hou *et.al.* [6] proposed VC scheme for gray level images and color images which is based on halftone technique & color decomposition method. Color decomposition is used to decompose color image into three primary colors C,M and Y and Halftone technique is used to transfer from gray level to binary images. This method retains the advantage of traditional visual cryptography, namely, decrypting secret images by human eyes without any cryptography computation.

Zhongmin Wang *et al.* [7] have proposed Halftone Visual Cryptography based Error Diffusion. In this method, the secret image is concurrently embedded into binary valued shares while these shares are halftoned by error diffusion. Here, not

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

only error diffusion has low in complexity but also halftone shares are good in quality. Image is recovered when all these qualified shares are stacked together.

N. Askari *et al.* [8] have proposed method for Halftone Images by an extended visual cryptography scheme without pixel expansion in which the size of the share images and the recovered image is the same as for the original halftone secret image. The resulting scheme maintains the perfect security of the original extended visual cryptography approach.

Shankar.K *et al.* [9] have proposed method in which the pixel values are taken from RGB matrix and these values are divide by 2 to create basic matrices. Then, randomly generated the key matrix and perform XOR which means key matrix values are XOR with basic matrices values to create shares. After shares creation, it gets an encrypted form of shares by applying AES algorithm. By this method, not only provide security but also reduces fake shares.

The method proposed by Xuehu Yan *et al.* [10] in which an HVCS with minimum ABPs, through embedding prefixed in parallel and separated maximally SIPs into meaningful shares in the halftoned processing of the cover images by error diffusion. The proposed scheme has best in visual quality and also has advantages when compared to related meaningful VCS. In this scheme, cannot reveal any visual information of the cover images from the reconstructed secret image. The security of the proposed HVCS is ensured by the security of the underlying VC.

III. Proposed Method

The proposed single share construction visual cryptography method is used to transmit the image over the network as securely and confidentially. The image is transferred as shares and all shares are stacked together to get back the original image. The proposed method is used to create the shares from their pixel values. The pixel values of the color image (RGB image) are extracted from the original image. The extracted pixels values are used to create the single share using LSB embedded method. Finally the single share is compared with the original image for evaluating their performance by using the peak signal noise ratio (PSNR) value, and Mean square error (MSE).

A. *Floyd-Steinberg dithering Algorithm*

In 1976, Robert W. Floyd and Louis Steinberg developed an image dithering algorithm called Floyd-Steinberg dithering Algorithm. There are several dithering algorithms available, but Floyd-Steinberg dithering algorithm is most popular because, it minimizes the visual artifacts through an error-diffusion process. Dithering is a technique used to limit the color palette in images. Color error diffusion means convert an RGB image into a binary image simply stated as RGB pixel value from 0 to 255.

-	**#**	**7/16**
3/16	**5/16**	**1/16**

Fig.1 Dithering Procedure

Dithering procedure is expanded as follows. Scan each pixel in the RGB image (P_{ij}). Find closest color available in that image (C_{ij}). Calculate difference between the pixel of (P_{ij}) and (C_{ij}) called quantization error. Next, divide these error values and distributed over the neighbor pixels with following condition, Here – denotes already error should be quantized and # means current pixel is processed, 7/16 of error to the right neighbor, 3/16 to the bottom left, 5/16 to bottom,1/16 to bottom right neighbor. Continue every pixel of the image to be quantized and get a 24bit color image.

B. *LSB algorithm*

Most of the image stenographic techniques are in Least Significant Bit embedding. Because it is very flexible for secret, data to be stored in cover image also to degrade the original image to very less value. The magic of the LSB technique is when hiding the information within the image, the users cannot find the information in the secret image. This process is looping when decomposition of least significant bit of each pixel replaced with secret message bits until message end. Hence, the message will hide evenly in the second to least significant as well as in the least significant bit then too.

C. *Single Share construction Method*

The proposed encoding method contains four steps. First step is to convert a secret image into halftone image using Floyd-Steinberg dithering algorithm. Next separates the each color component R, G and B from dithered image. After expands each pixel into six (2x2) blocks, that means three dithered pixel into 2. Each dithered first pixel is combined into creating share 1 and second pixels are combined into creating share 2. When the entire pixel in the secret image is encoded, then obtaining two shares of the secret image. Once 2X2 VC method completed in dithered image we get share1 and share 2. Finally to construct a single share using LSB algorithm using stego key. The stego key is used to encrypt the secret image from cover image. Finally, we get a single share. The decoding process is reverse process of encoding. After stacking the share1 and share 2 the secret image can be decrypted.

1) *Block diagram*

Figure 1 shows the block diagram of the proposed method of the visual cryptography and its each block are explained in the following.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

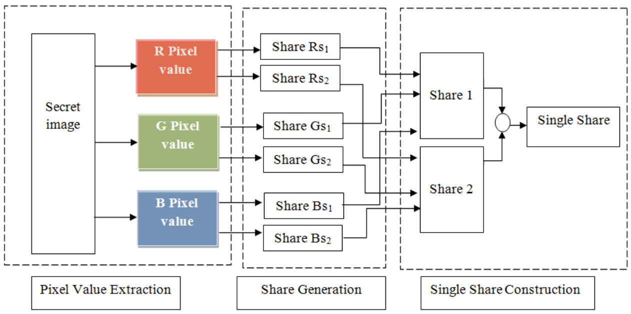


Fig.2 Block diagram of proposed method

Step 1: A 24-bit color secret image P_{ij} dithered into 3bit RGB image P_{Dij} using Floyd-Steinberg dithering algorithm.

Step 2: Convert the RGB image into three dithered image R_{Dij}, G_{Dij} , B_{Dij} .

Step 3: Each pixel of R_{Dij}, G_{Dij}, B_{Dij}, and Expanded into 2 x 2 blocks according to the Naor and Shamir basic method. After expanding pixel to obtain the six 2x2 blocks like R_{D1ij}, G_{D1ij}, B_{1Dij} and R_{D2ij}, G_{D2ij}, B_{D2ij}.

Step 4: According to 2X2 VC Method combine the R_{D1ij}, G_{D1ij} , B_{D1ij} to create, share 1 and R_{D2ij}, G_{D2ij} , B_{D3ij} to create share2. The process executed until every pixel is composed.

2) Single Share construction Algorithm: Encoding

Step 5: After shares created to start the embedding from share 1 to share 2 or share2 to share1 using LSB algorithm with the help of stego key. Once the embedding process completed, obtain the single share for the secret image.

3) Single Share construction Algorithm: Decoding

Step 1: Read the single share and compute LSB of each pixel using stego key.

Step 2: Extracting share 1 and share 2.

Step 3: After stacking the share 1 and share 2, the secret image can be decrypted.

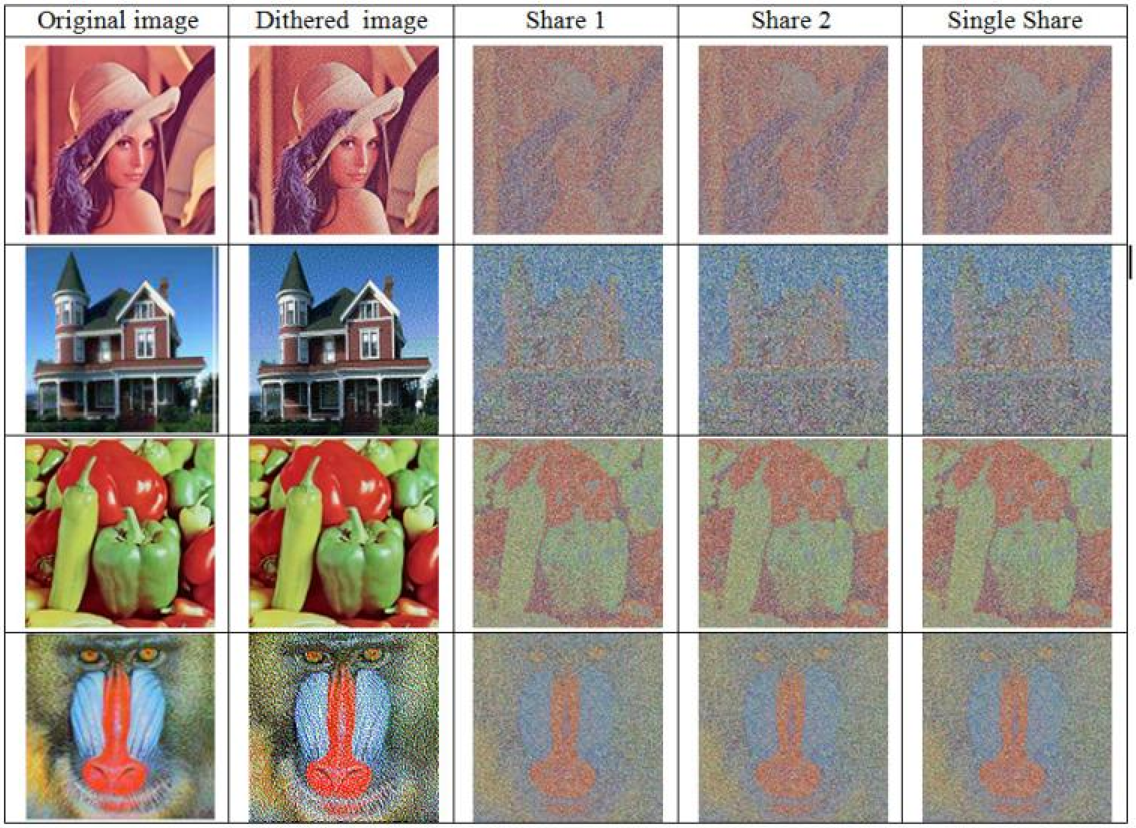
IV. Results and Discussions

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 core i5 processor and 4GB RAM.

The table 1 shows the Original image, and its shares. The shares are created based on the above single share construction method. Analysing our method to tested four-color images of size 512 x 512 to generate the single share. In this process stego-image is generated using LSB algorithm, which carried out to enhance the security of hidden data.

TABLE I
Experimental Results of the different image

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016



For the performance analysis of the single share construction to be implemented on four images house, peppers, Lena, and Baboon. The overall performance of the proposed method is analysed by using the peak signal noise to ratio value and mean square error. In table 2, the row 1, 2, 3 and 4 demonstrates the analysis results of the original images. Through images, the proposed strategy is connected with the image and output images are indicated by their PSNR values. The PSNR value indicates quality of the resultant image is better or worse. As per PSNR understanding stegnography and compression, PSNR high is better quality, but Image Encryption process PSNR low is better quality. Here, the PSNR qualities are 10.4288, 8.7139, 9.9212 and 10.7707 very Low PSNR indicates shares are very strongly encrypted.

TABLE II
PERFORMANCE ANALYSIS OF DIFFERENT IMAGES

Image Name	**PSNR**	**MSE**
Lena	10.4288	0.1048
House	8.7139	0.1104
Peppers	9.9212	0.1006
Baboon	10.7707	0.0989

.

V. CONCLUSIONS

The Major drawback of the existing visual cryptography is very low security of shares. To overcome the existing problem the proposed method constructs a single share mechanism that is useful to protect the shares. Our single share approach provides double layer security to the VC scheme. The strength of the algorithm is to confuse the human perception it is image encryption method. Finally, experimental results demonstrate the how to create a single share in VC scheme and difficulty of exposing the identity of the secret image in different real time applications. Our method provides the combination of VC scheme and Steganography to increase the computation complexity to some extent, but it provides high security to share.

REFERENCES

[1] M. Naor, A. Shamir, in: A. De Santis (Ed.), Visual Cryptography, Advances in Cryptology: Eurpocrypt'94, Lecture Notes in Computer Science, Vol. 950, Springer, Berlin, 1995, pp. 1–12.

[2] Chang-Chou Lin, Wen-Hsiang Tsai, "Visual cryptography for graylevel images by dithering techniques", Pattern Recognition Letters 24 (2003) 349–358, Elsevier Science.

[3] Gwo-Chin Tai, Long-Wen Chang, "Visual Cryptography for Digital Watermarking in Still Images", Springer -Advances in Multimedia

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

Information Processing - PCM 2004 Lecture Notes in Computer Science Volume 3332, 2005, pp 50-57.

[4] Hsien-Chu Wu, Hao-Cheng Wang and Rui-Wen Yu, "Color Visual Cryptography Scheme Using Meaningful Shares", in Conf. Rec. 2008 IEEE Int. Conf. Intelligent Systems Design and Applications, pp. 173 - 178.

[5] Arun Ross and Asem Othman, "Visual Cryptography for Biometric Privacy" IEEE Trans. INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 1, MARCH 2011.

[6] Young-Chang Hou, "Visual cryptography for color images", Pattern Recognition 36 (2003) 1619 -1629, Pattern Recognition Society. Published by Elsevier Science Ltd.

[7] Wang, Zhongmin, Gonzalo R. Arce, and Giovanni Di Crescenzo. "Halftone visual cryptography via error diffusion." Information Forensics and Security, IEEE Transactions on 4.3 (2009): 383-396.

[8] Askari, Nazanin, Howard M. Heys, and Cecilia R. Moloney. "An extended visual cryptography scheme without pixel expansion for halftone images." Electrical and Computer Engineering (CCECE), 2013 26th Annual IEEE Canadian Conference on. IEEE, 2013.

[9] Shankar, K., and P. Eswaran. "Sharing a Secret Image with Encapsulated Shares in Visual Cryptography." Procedia Computer Science 70 (2015): 462-468.

[10] Yan, Xuehu, et al. "Halftone visual cryptography with minimum auxiliary black pixels and uniform image quality." Digital Signal Processing 38 (2015): 53-65