

Visual Cryptography using Half-toned Colored Images

Afshan Mohammadi¹, Dr. Jalesh Kumar²

¹M. tech. 4th SEM, Department of CSE, J.N.N College of Engineering, Shivamogga, Karnataka, India

²Associate Professor, Department of CSE, J.N.N College of Engineering, Shivamogga, Karnataka, India

Abstract – As the increase of information transmission over the internet is increasing across World Wide Web, protection of the private as well as public information or data to be transmitted has become a challenging task. Over the years, encryption technique included many steps with different calculations to help avoid the unauthorized access to data transmitted over the internet communication inverse process of the encryption technique is decryption in which the original secret information could be retrieved, hence both the encryption and decryption process required their own algorithms to be completed. Thus, this shows that both the encryption as well as the decryption is not only time consuming but also resource consuming too. But the visual cryptography (VC) provides an effective way for the solution of this problem by including fewer steps and lesser complexity. In VC the main focus is on the encryption were as the decryption is a simple procedure to be taken out. As there will be an algorithm needed just for encryption of picture or information decryption could perform by human vision system. In the proposed method, the encryption algorithm uses an 16 standard color code format is taken which helps in generation of shares from original picture as well as halftoning to picture is done by using XOR operation and decryption could be performed by just stacking the shares and with human vision without any extra needed efforts.

Key Words: Visual Cryptography, XOR based scheme, RGB 16 color code model, and halftoning to picture, human vision.

1. INTRODUCTION

Visual cryptography as the name itself suggests that, it adds a visual dimension to the entire security workspace. It encrypts the visual information, as it works on the informative images, encrypts it that appears to be series of the randomized pixels and decrypts by using the simple XOR operation. This reduces the total time and cost for the maintaining and developing information security.

In order to hide messages, VC doesn't include the substitution of any character with an encrypted character. Though in terms of defining, it only encrypts the visual information this can be extended to suit all the types. i.e., any information whether a set of bits, character, numeric or combination of these could be produced visually as an image before being subjected to the VC. This image is then encrypted by the algorithms to deceive the perpetrator and secure the messages.

An important use of the visual cryptography is that its use in the digital watermarking to authenticate the document originality. This included the private secret document embedded with a copyright share, which is not visible to naked eyes. But when overlapped with the corresponding share reveals the copyright information. And thus the authenticity of the document is maintained.

Visual cryptography can also be used in the protection of the biometric template in which the complex computation is not required for the decryption [1] and the other use of this is that it could be used for the encryption of the color image were at first it used the black and white or 8 bit color code format now the 16 standard color code format can be used for the encryption of the data or the image.

2. LITERATURE SURVEY

A. Halftone Visual Cryptography

As described by Zhi Zhou et al. in [2] VC already suggest that, surreptitious binary picture is encrypted to shares indiscriminate binary patterns. If shares stacked together then encrypted image can be reproduced this can be done only when the overlapping of the proper shares is done. Thus halftoning is the technique or method of converting the high bit pixels into a lower bit format. The halftoned image is generated by the methods like the blue noise half-toning, or pixel reversal. The technique underlying the two out of two halftone illustration threshold proposal extended top the cryptography, where furtive binary photo's hidden in halftone shares.

B. Secret Sharing Scheme for the Protection of Digital Image

Sushanta Biswas et al. in [3] discussed about work focuses on to the major algorithms related to secret sharing system. At first base on polynomial interpolation it describes the secret sharing scheme. Technique develops $k-1$ degree polynomial function to compute shares using secret image, where the minimum digit meant of shares be generate by clandestine image is represented by k . it also describes (r, n) scheme, where original image can obtained if slightest r or more "n" shares obtained; hence $r-1$ shares cannot be used to retrieve the original image.

It requires the polynomial function and the k coefficients of the polynomial to share the secret pixel so that the image share extent compact $1/k^{\text{th}}$ of clandestine image [3]. It then requires $k/$ further shares to re-enact secret photo.

Drawback of this method is that the original image is not completely retrieved. Another Secret sharing technique was proposed where a secret image was having the pixel value greater than 250 is divided into two even though this technique completely recovers the secret image but it produces the expandable shares. VSS is another format based on k, n verge concept but it suffers from two drawbacks: pixel extension plus low down image superiority.

C. An extended VC scheme without pixel expansion for halftoned images

H.M. Heys et al. in [4] detailed about basic (2, 2) plan of VC, consequential share and improved image after stacking these shares contains four time added pixels compared actual image to be inventive. This is resolved by dividing the pixels by using the block-wise approach. This method has the two algorithms for its working: the simple block replacement (SBR) algorithm and the balanced block replacement (BBR) algorithm [4]. The results showed that the SBR produced the darker images when compared with BBR, which produced images that has more resemblance to the actual image.

D. Comparatively study on visual cryptography

Samip Patel et al. in [5] gave description about Visual cryptography has been implemented with many variations based on quantity needed of image that's kept secret, expansion of pixel, mode deciphering etc. This summarizes TABLE 1.

TABLE- 1: COMPARISON OF DIFFERENT VC TECHNIQUES

TECHNIQUES	ADVANTAGES	DISADVANTAGES
Traditional VC	Gives safety for binary Images	Not capable of generating meaningful shares of an image
Progressive VC	No pixel expansion is done	No complete assurance on correct restoration of original pixel
Random Grid VC	No pixel expansion	Lesser visual quality
Multiple Secret Sharing VC (version 1)	Image encrypts 2 mystery images amid 2 shares. Revolving angle is 90°	Size of share is 4 times larger than main mystery image.
Multiple Secret Sharing VC (version 1)	Revolving angle vary	Expansion of image pixel is greater here
Extended VC	Meaningful shares are developed	Contrast loss occur

3. PREVIOUSLY IMPLEMENTED SCHEME

The previously implemented scheme was Hou's color visual SSS [6], Hou anticipated three tint visual cryptography method which used same technique to decay secret color image to 3 detach pictures were colored correspondingly as cyan,magenta,yellow. Later halftoning was made beneficiary to translate 3 shaded pictures present in image that is halftoned. As a final point, once all 3 halftone image that's colored were obtained they were stacked together to obtain the final single halftoned image. The color halftoned image used the 8 diverse ensign to display: CMYRGBW.

For each of pixel of halftoned shaded photo, subsequent procedure followed. Foremost according share ONE, 4 blocks build and then 4 pixels as CMYW be permuted indiscriminately. Then for share 2 generation the numbers of blocks are calculated regarding to color proportion of 4 pixels.

In favor of exemplar if pixel one pixel halftoned color picture is G, then pixels color percentage would be form 100 percent, 0 percent, and 100 percent for CMY correspondingly. The incarnation of pixels of block share 1: cyan, magenta, yellow and white. This information is referred to produce the block of share2, where permutation of pixels YMCW processing of entire pixels is completed, two shares will be formed. every one block two shares be composed of cyan,magenta,yellow and white. Sensitive image could be reconstructed visualized only when two shares related to undisclosed figure are stacked mutually and clandestine icon be revealed. This resulted in reduce the pixel extension but limitation of this proposed scheme was that it reduced quality of representation or degrades quality of icon.

4. PROPOSED SCHEME

Proposed work, image with 256 colors is converted into a 16 standard RGB color code format.Hence will generate shares lacking compromise of pledge. Floyd Steinberg algorithm that uses error diffusion technique worn influence 256 shaded image into 16 standard shade cipher image and also anticipated method uses XOR based operation for the decomposition of the image into 4 shares and then the decryption can be performed by stacking these shares.

The steps included in to the proposed methodology are as given below:

A. VC for Shaded Images

In this proposed method RGB color code format if taken for the purpose of data allocation. Algorithm is meant to manipulate 256 shade code picture into small code figure is Floyd-Steinberg algorithm. It achieve dithering process by diffusion technique, along with to create share it considers the nearest neighbor pixel, as in the CMY model the 8 color codes were used.

But in this proposed method the 16 color code format is used, without the degradation of superiority of secret figure. Halftoning performed with the help of error diffusion method.

B. The Floyd- Steinberg-Dithering Algorithm

Floyd-Steinberg-Dithering algorithm, used as image manipulation tool, this uses the error diffusion technique for the decomposition of the secret image [7]. Once an RGB image is selected as an input image then the halftoning of the secret image is done by using the error diffusion technique, which basically uses the idea of totaling residual error to quantization pixel towards pixels those are neighboring. Dithering also means the same thing, where the noise is intentionally applied that is used in the randomization of quantized error, and also prevents the color banding.

The working of the dither by using the error diffusion technique to generate the halftone image: in support of every point in icon first it finds nearest shade on hand, and it calculates dissimilarity among image color and nearest hue available. If the error values are present then the error is moved to the neighboring pixel that has not yet been visited, so that the quantization error could be removed from the current pixel of halftoned figure and first pixel of halftone image could neither approximated or nearly matches the first pixel of the original image. The process is continued until each and every pixel of the halftone image could at least resemble with the original image after randomizing the quantization error and then the halftone image would be obtained.

A Floyd- Steinberg-Dithering Algorithm

I = Input figure

Output Image = null

For i = 1 toward m **do**

For j = 1 toward n **do**

Output Image [i, j] = NearestColor accessible (I [i, j])

Err= I [i, j] - Output Image [i, j]

I [i, j+1] += err x (7/16)

I [i+1, j-1] += err x (3/16)

I [i+1, j] += err x (5/16)

I [i+1, j+1] += err x (1/16)

End for

End

C. Procedure for creation of shares

This part uses above a algorithm necessary for share generation process in shade cod model. In earlier process additive and subtractive models were used for the halftoning. Later the CMY model used the 8 color code format. The proposed work use RGB basic hue code format used for establishment of shares and stacking images and generate 16 standard hue code formats.

5. RESULTS

A. Experimental Outcome

The segment present simulation outcome illustrates performance of proposed scheme. Anticipated work be implementing using MATLAB R2015 under Windows environment. Outer Matlab imagery could also be three types i.e. black& white, greyscale and highlighted. Within Matlab however, there's four sorts of imagery To carry out the experiment 2 color images are taken and are served as the test images and different combinations are tested for these 2 images, as in below Figure 1.

Original Image	Halftoned Image	4 Shares generated during Encryption	Decrypted Image	Combination of shares used
				Share 1, share 2, share 3, share 4
				Share 2 and share 4
				Share 1 and share 2
				Share 1, share 2, share 3





Figure -1: Experimental result for different combination of images

B. Performance Analysis

The quality of the generated shares can be demonstrated by considering the various performance metrics that are included in this section. The performance metrics included are the PSNR, specificity, sensitivity, and accuracy of image.

Among which peak signal noise ratio is one of mainly important parameter that is to be considered. PSNR computes ratio of max doable signals to that of noise that affect image deception. Below table gives the PSNR value of the images before the encryption and after the decryption.

TABLE -2: PSNR values for the images before encryption and after decryption

IMAGE	ORIGINAL IMAGE PSNR	DECRYPTED IMAGE PSNR
	22.2466	22.2888
	22.1101	22.1804
	22.2146	22.3301
	22.1003	22.1877

[2] Zhi Zhou, Member, IEEE, Gonzalo R. Acre, Fellow, IEEE and Giovanni Di Crescenzo, "Halftone Visual Cryptography", IEEE Transactions on Image Processing, Vol. 15, NO.8, August 2006.

[3] Amitava Nag, Sushanta Biswas, Debasree Sarkar and Partha Pratim Sarkar "Secret Sharing Scheme for protection of digital images", Egyptian Informatics Journal, Volume 15, Issue 3, November 2014, Page.no 201- 209.

[4] N. Askari, H.M. Heys, and C.R. Moloney "An Extended Visual Cryptography Scheme without Pixel Expansion for halftone Images", 2013

[5] Prashant B Swadas, Samip Patel, Dhruvi Darji, "A Comparative Study on Visual Cryptography", IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 pISSN: 2321- 7308, Volume 03, Issue 01, January 2014, Page.no 182-185.

[6] Y. C. Hou, "Visual Cryptography for color images", pattern Recognition, Vol. 36, pp. 119- 1629, 2003.

[7] M. Karolin, T. Meyyappan, "RGB Based Secret Sharing Scheme in Color Visual Cryptography", Int. Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 7, pp. 151-155, 2015.

6. CONCLUSIONS

The Visual cryptography provides one of protected way in the direction of broadcast images on internet, as there is always an fear of losing the sensitive information when transmitted over internet. Hence, the visual cryptography provides the security for the secret image as it gives no clue to the hacker concerning secret image. The image is divided into worthless shares, even if the hacker gets over one of the share is of no use unless all the shares are stacked together.

The proposed method uses diffusion technique. Spaced out from offered methods, proposed method facility for hued code models. The PSNR analysis carried out indicates that the model is working satisfactorily.

REFERENCES

[1] Askari, Nazanin, Moloney, Cecilia, Heys, Howard M. "Application of visual cryptography to biometric authentication", NECEC 2011.