 ISSN: 2321-8169
1371 – 1373

Data Hiding in Color Image for Visual Information Security

Mr. Prashant M. Pattanshetti [#1], Prof. Dhanashree P. Kutre [*2]

Department of Electronics and Communication Engineering
Maratha Mandal's Engineering college, Belgaum, Karnataka, India
[1]*prashant.athany@gmail.com*
[2] *dhanashree_ece@mmec.edu.in*

Abstract— Visual Cryptography is a special encryption technique to hide information in image in such a way that it can be decrypted by the human vision if the correct key image is used. Visual Cryptography uses two transparent images one image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the image. Both transparent images and layers are required to reveal the information. The beauty of the Visual secret sharing scheme is its decryption process i.e. to decrypt the secret using Human Visual System (HVS) without any computation

Keywords— *Visual Cryptography, Encryption, Decryption, Halftone image, Pixel, Shares.*

*****

I. INTRODUCTION

Visual Cryptography is proposed in 1994 by Naor and Shamir who introduced a simple but perfectly secure way that allows secret sharing without any cryptographic computation, which they termed as Visual Cryptography Scheme (VCS). The simplest Visual Cryptography Scheme is given by the idea of A secret image consists of a black and white pixels where each pixel is treated independently [1].

VC technique is for binary images where α the secret image is, γ is a randomly generated share while β is the other share such that:

$$\alpha_i + \beta_{i=} \gamma_i, \quad i=0,1,2,.....,n$$

Thus without β and γ, α cannot be deduced at all [2].This scheme provides perfect security with simplicity [3].Visual cryptography possesses these characteristics:

- Perfect security
- Decryption without the aid of a computing device
- Robustness against lossy compression and distortion due to its attribute [3].

In a k-out-of-n scheme of VC, a secret binary image is cryptographically encoded into n shares of random binary patterns, The n shares are Xeroxed onto n transparencies, respectively, and distributed among n participants, one for each participant. No participant knows the share given to another participant. Any k or more participants can visually reveal the secret image by superimposing any k transparencies together. The secret cannot be decoded by any k-1 or fewer participants [4].There are many algorithms to encrypt the image in another image, but a few of them have been in visual cryptography for color image. In this paper, the different approach have been produced for the visual cryptography for color image, the proposed algorithm splits a secret image into two shares based on three primitive color components.

II. VISUAL CRYPTOGRAPHY MODEL

A printed page of cipher text and a printed transparency (which serve as a secret key). The original clear text is revealed by placing the transparency with the key over the page with the cipher, even though each one of them is indistinguishable from random noise. The model for visual secret sharing is as follows. There is a secret picture to be shared among n participants. The picture is divided into n transparencies (shares) such that if any m transparencies are placed together, the picture becomes visible. If fewer than m transparencies are placed together, nothing can be seen. Such a scheme is constructed by viewing the secret picture as a set of black and white pixels and handling each pixel separately [5].

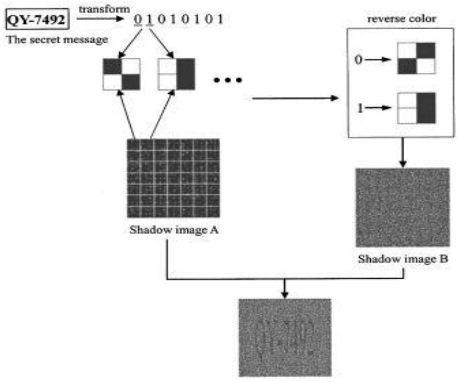


Figure 1: Visual cryptography system

In visual cryptography system the pixels of the image to be encrypted can be applied to the image in different manner. There is a set of n participants (image), and the secret image is divided and encoded into n shadow images called shares. Each participant is encrypted by one share, k out of n participants are needed to combine shares and see secret image, sometime k-1 of shares can not reveal information about secret image. The technology makes use of the human vision system to perform the OR logical operation on the superimposed pixels of the shares. When the pixels are small enough and packed in high density, the human vision system will average out the colors of surrounding pixels and produce a smoothed mental image in a human's mind [6].

 ISSN: 2321-8169
1371 – 1373

III. PROPOSED ALGORITHM

Step1: Secret color image.

Figure 2: secret color image

Step2: The secret color image as shown in Fig.1 is decomposed into three planes namely, red, green, blue, RGB. Fig.2 shows the three primitive color components of secret color image, where each image has 256 levels of the corresponding primitive color, and each pixel represented by 24 bits.

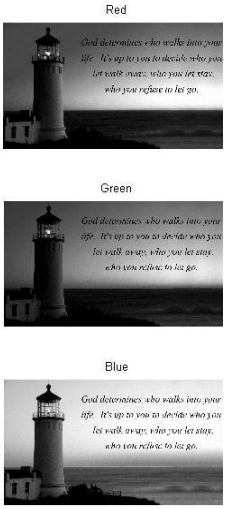


Figure 3: Primitive color (R, G, and B) component

Step3: Encrypt the color space

Step4: Half tone image

Figure 4: Halftone image

Step5: Two shares will be generated by the following method.

Method:

1. Read the pixel value with respect to ii(number of rows of secret image) and jj(number of columns of secret image).
   sij = I(ii,jj);
2. Pixel reversal.
   sij1 = 255-sij;
3. Read each pixel and convert to shares.
4. Reduce sij.
5. Pixel reversal.
6. Take difference of two random generator with original pixel.
7. Pixel reversal.

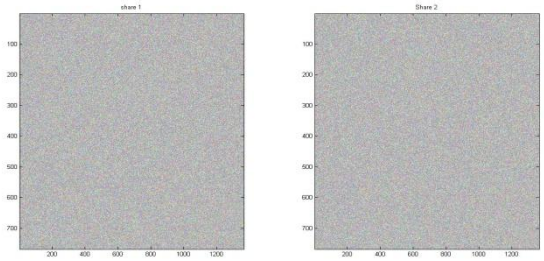


Fig. 5: Share1 and Share 2

Step 6: After mixing share1 and share 2 with three planes of RGB we obtain decrypted image.

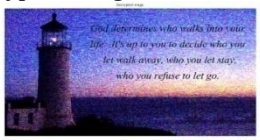
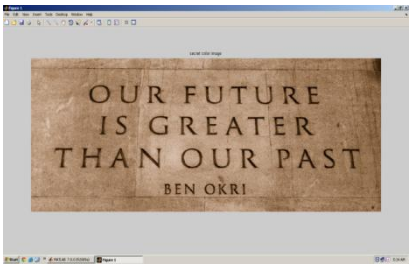


Fig. 6: Decrypted image

Step7: Size of the decrypted image is same as secret image.

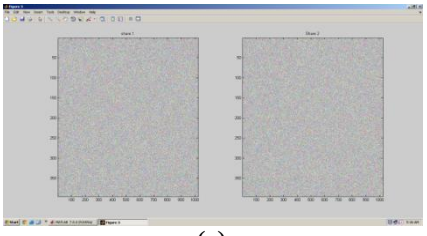
IV. EXPERIMENTAL RESULTS

In this paper, we first consider host image to be color image and transformed the color image into Red, Green and Blue components. Share 1 and share 2 generated. Finally, shares are combined to decrypt the image. It is not possible to decrypt the image if any one share is missing. The algorithm was implemented in MATLAB. The simulation results of the algorithm's performance on secret image are seen in Figure 6.



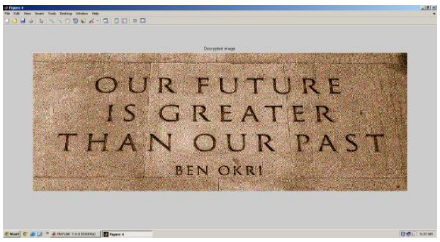
(a)

(b)



(c)

 ISSN: 2321-8169
1371 – 1373



(d)

Fig.6 Color visual cryptography results (a) Secret color image (b) RGB primitive colors (c) Share 1 and share 2 (d) Decrypted image

V. CONCLUSIONS

Visual cryptography exploits human eyes to decrypt secret image with no computation required. This paper exploits the techniques of Halftone technology. The proposed scheme revealed good security due its randomness. Both original and retrieved image having same sizes are the results of the proposed scheme.

Acknowledgment

We thank immensely our management for extending their support in providing us infrastructure and allowing us to utilize them in the successful completion of our research paper.

REFERENCES

[1] JIM CAI 2003. *A Short Survey on Visual Cryptography Schemes* ,www.wisdom.weizmann.ac.il/naor/PUZZLES/Visual.html.

[2] A. Shamir, ”How to share a secret,” Communications of the ACM,vol.22,no. 11, pp. 612-613,Nov 1979.

[3] W.Q.Y,J. Duo and M. Kankanhalli, ”Visual cryptography for print and scan applications ,” in Proc. IEEE Int. Symp. Circuits Syst.,2004, pp.572-575.

[4] InKoo Kang, Gonzalo R.Arce, and Heung-Kyu Lee ”Color Extended Visual Cryptography Using Error Diffusion ” IEEE TRANSACTIONS ON IMAGES PROCESSING, VOL. 20, NO.1,JANUARY 2011.

[5] Talal Mousa Alkharobi, Aleem Khalid 2003. New Algorithm For Halftone Image Visual Cryptography, Alvi King Fahd University of Pet. & Min. Dhahran.

[6] Bert W. Leung, Felix Y. Ng, and Duncan S. Wong, 2007. On the Security of a Visual Cryptography Scheme for Color Images, (RGC Ref. No. CityU 122107) .