VISUAL CRYPTOGRAPHY FOR COLOR IMAGES

[1]Amarjeetsingh Thakur, [2]Veeresh Hiremath, [3]Uday Nadiger

[1,2,3] Asst.Prof., ECE Dept., S.G.Balekundri Institute of Technology, Karnataka (India)

ABSTRACT

Visual cryptography is a secret sharing scheme for encrypting a secret image, it is a perfectly secure way that allows secret sharing without any cryptographic computation, which is termed as Visual Cryptography Scheme (VCS). In this paper secret image is divided into shares (printed on transparencies), and each share holds some information. At the receiver, this shares are merged to obtain the secret information which is revealed without any complex computation. The proposed algorithm is for color host image, divided into three color planes Red, Green, Blue and merged with secret image which is binarized and divided into shares. The decoding requires aligning the result obtained by merging color host image and shares, so as to obtain the secret image.

Keywords: Color plane, Encryption, Secret sharing, Shares, Visual Cryptography.

I INTRODUCTION

Visual cryptography was originally proposed for the problem of secret sharing. Secret sharing is one of the early problems to be considered in cryptography. In a (k, n)-threshold problem, a secret is divided into n pieces. With any k of the n pieces, the secret can be perfectly reconstructed, while even complete knowledge of k-1 pieces reveals absolutely no information about the secret. Visual cryptography illustrated a new paradigm to solve the (k,n) problem. It was originally proposed by Naor and Shamir [1].

The original scheme generates n images (known as shares) based on the secret message (the original image) which can be printed on n transparencies. The original message can then be recovered if any k or more than k of the transparencies are stacked together, but no information about the original image can be gained if fewer than threshold number of k transparencies are stacked. Visual cryptography is a unique technique in the sense that the encrypted messages can be decrypted directly by the human. [1,2]

To encrypt a ($K_1 \times K_2$) binary image using visual cryptography, each binary pixel r(i,j) (i.e. r(i,j)=1 for white and r(i,j)= 0 for black) is handled separately via an encryption function FEnc(·) to produce a ($m_1 \times m_2$) block of black and white pixels in each of the n shares. Thus, a ($K_1 \times K_2$) input binary image is encrypted into (n) binary shares S_1, S_2, . . , Sn each one with resolution of ($m_1K_1 \times m_2K_2$) pixels. Since the arrangement of the pixels varies from block to block, it is impossible to recover the useful information without accessing a predefined number of shares [2,3].

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 [4].

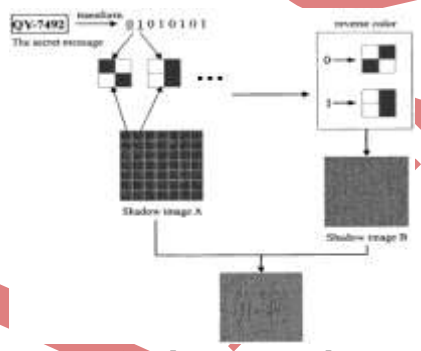

Figure 1: Visual cryptography system

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 [5].

III HALFTONE VISUAL CRYPTOGRAPHY

The shares were of poor quality that was generated in [6] and the suspicion of data encryption increases, again. To increase the quality of the meaningful shares Zhou et al [7] proposed a new technique based on halftone visual cryptography. In halftone visual cryptography as shown in Fig 2, a pixel, which is secret as well as binary, is encoded into an array of sub pixels in each share, mentioned to as halftone cells. Visually satisfying halftone shares

can get by the use of halftone cells of proper size. This method helps in maintaining the security and the contrast.

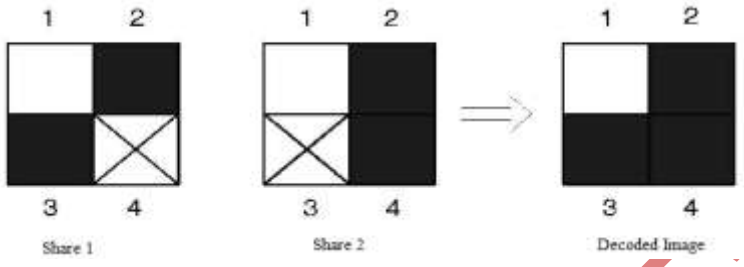

Figure 2: Halftone Visual Cryptography Scheme (2 out of 2)

IV PROPOSED ALGORITHM

Step1: Secret color image.

Step2: Perform half toning in each plane (R,G,B) separately.

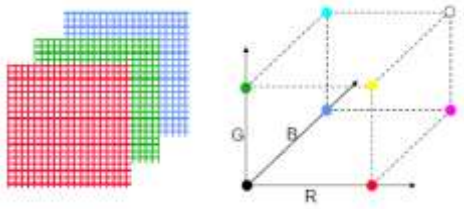

Figure 3: Halftoning Process

Step3: Encrypt the color space.

Step4: Half tone 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).

   $s_{ij} = I(ii,jj);$

2. Do the pixel reversal.

   $s_{ij1} = 255\text{-}s_{ij};$

3. Read each pixel and convert to shares.

4. Reduce s_{ij}.

5. Repeat step no. 2.

6. Take difference of two random generator with original pixel.

7. Repeat step no. 2.

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

V 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 4.

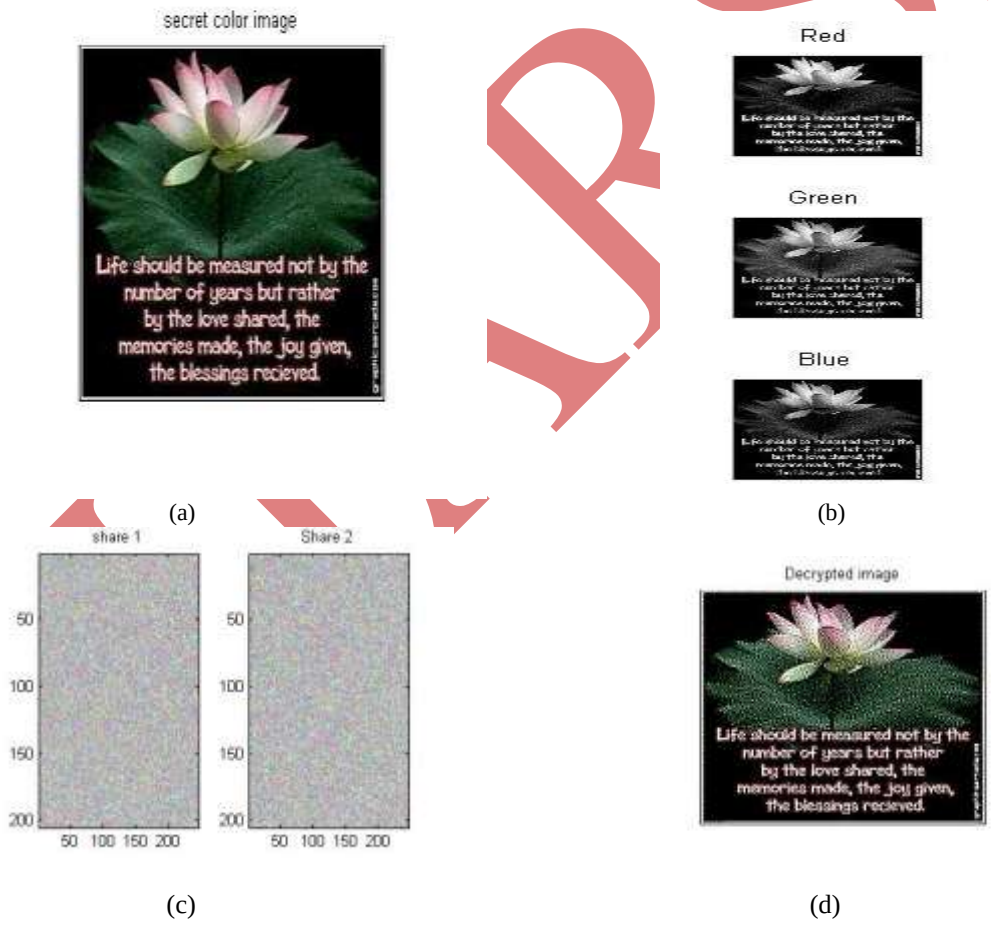

Figure 4: Color visual cryptography results (a) Secret color image (b) RGB primitive colors (c) Share 1 and share 2 (d) Decrypted image

VI CONCLUSION

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] Moni Naor and Adi Shamir. Visual Cryptography. Eurocrypt 94, 1994.

[2] Jim Cai, A Short Survey On Visual Cryptography Schemes, 2008.

[3] K.Y. Chen, W.P. Wu, and C.S. Laih. On the (2,2) visual multi-secret sharing schemes, 2008.

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

[5] 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) .

[6] Nakajima, M. and Yamaguchi, Y., "Extended visual cryptography for natural images", Journal of WSCG. v10 i2. 303-310.

[7] Zhi Zhou, Gonzalo R. Arce and Giovanni Di Crescenzo, "Halftone Visual Cryptography", IEEE Transactios On Image Processing, Vol. 15, No. 8, August 2006.