A New Secret Coloured Image Encryption and Decryption Scheme based on (2, 2) Visual Cryptography Scheme (VCS)

Harinandan Tunga
Computer Science & Engineering Department
RCC Institute of Information Technology
Kolkata, India

ABSTRACT
Cryptography is an art and science of achieving security by encoding the message to make them non-readable. Extended Visual Cryptography is a type of cryptography which encodes a number of images in the way that when the images on transparencies are stacked together, the hidden message appears without a trace of original images. The decryption is done directly by the human visual system(HVS) with no special cryptographic calculations. We present a system which takes three pictures as an input and generates two images which correspond to two of the three input pictures. The third picture is reconstructed by printing the two output images onto transparencies and stacking them together. Generally, visual cryptography suffers from the deterioration of the image quality. This paper also describes the method to improve the quality of the output images.

Index Terms
Visual Cryptography, Human Visual System (HVS), Extended Visual Cryptography, Secret sharing , Pixel expansion

1. INTRODUCTION
Visual cryptography is a image hiding technique introduced by Naor and Shamir[1].As network has greatly advanced, much information is transmitted via the Internet conveniently and rapidly. At the same time, the security issue is a crucial problem in the transmission process. For example, the information may be intercepted from transmission process. This method aims to build a cryptosystem that would be able to encrypt any colour image in standard format, so that the encrypted images when perceived by the naked eye or intercepted by any person with malicious intensions during the time of transmision is unable to decipher the image.

In a VCS, there is a secret image which is encrypted into n share images. The secret image is called the original secret image for clarity, and the share images are the encrypted images (and are called the transparencies if they are printed out). When a qualified set of share images (transparencies) are stacked together properly, it creates an image which is almost same as the original image; this image is called the recovered secret image.

The (k,n) visual cryptography scheme (VCS) introduced in 1994 by[1],allowed a dealer to encode a secret image into n shares. The secret image would be visible if and only if any k shares ($k \leq n$) are stacked together, whereas any set of less than k shares do not reveal any information about the secret image. Naor and Shamir applied this idea on black and white images only. Few years later, Verheul and Tilborg [2] developed a scheme that can be applied on colored images.The inconvenient with these new schemes is that they use meaningless shares to hide the secret and the quality of the recovered plaintext is bad. More advanced schemes based on visual cryptography were introduced in [3,4,5,],where a colored image is hidden into multiple meaningful cover images.

Chang et al. [3] introduced in 2000 a new colored secret sharing and hiding scheme based on Visual Cryptography schemes (VCS) where the traditional stacking operation of subpixels and rows interrelations is modified. This new technique does not require transparencies stacking and hence, it is more convenient to use in real applications. However, it requires the use and storage of a Color Index Table (CIT) in order to losselessly recover the secret image. CIT requires space for storage and time to lookup the table. Also, if number of colors c increases in the secret image, CIT becomes bigger and the pixel expansion factor becomes significant which results in severe loss of resolution in the camouflage images. Chang and Yu introduced in [?] an advanced scheme for hiding a colored image into multiple images that does not require a CIT.This technique achieves a lossless recovery of the secret image but the generated shares (camouflage images) contain excessive noise.

Two important factors are used to determine the efficiency of any Visual Cryptography scheme, namely: 1) the quality of the reconstructed image and 2) the pixel expansion factor (m). Any loss of information during the reconstruction phase leads to the reduction in the quality of the recovered image. On the other hand pixel expansion m refers to the number of sub-pixels in the generated shares that represent a pixel of the original input image. It represents the loss in resolution from the original image to the shared ones.

2. DEVELOPMENT
2.1 RGB Color Image
The RGB color model is the most common way to encode color in computing. A color in the RGB color model is described by indicating how much of each of the red, green, and blue is included. The color is expressed as an RGB triplet (*r*,*g*,*b*), each component of which can vary from zero to a defined maximum value. If all the components are at zero the result is black; if all are at maximum, the result is the brightest representable white. The red, green and blue use 8 bits each, which have integer values from 0 to 255.This makes 256 * 256 * 256 = 16777216 possible colors.

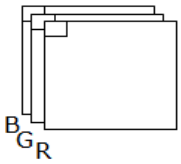


Fig.1 RGB image representation

2.2 Hiding Algorithm

Assume that a color image (r,g,b) constitute a secret to be hidden. Each color can be represented as a 3-byte sequence where each byte consists of an 8- bit binary vector. The main idea is to expand each byte of the colored pixel into m subpixels and embed them into n shares.This scheme uses m=9 as an expansion factor.The resulting structure of each byte in a pixel can be represented by an nx9 Boolean matrix S = [Sij] where ($1 \le i \le n$, $1 \le j \le 9$) and Sij =1, if and only if, the jth subpixel in the ith share has a non-white color.To recover the color of the original secret pixel, an "XOR" operation on the stacked rows of the n shares is performed.

For a 2 out of 2 scheme, the construction can be described as a collection of 2x9 Boolean matrices S.If a byte, out of the 3-bytes of a pixel, with value $k_p=(k_1k_2...k_8)$ needs to be shared then the following condition needs to be satisfied:

$$k_p = S_{1i} \bigoplus S_{2i} \quad (1)$$

where $1 \le i \ge 9$

2.3 Encryption Method

1. Take a colored secret image I_{HL} of size HxL and choose any two arbitrary cover images O^1_{HL} and O^2_{HL} of size HxL.
2. The secret image and the two cover images are decomposed into three planes under additive model, namely, red, green, blue (RGB) where each image has 256 levels of the corresponding primitive color, and each pixel is represented by three bytes.Converting to (R, G, B), where R, G, B {0- 255}.
3. Scan through each planes of I_{HL} and convert each pixel I to a 9-bit binary string denoted as $k=(k_1k_2k_3k_4k_5k_6k_7k_8k_9)_2$. (The MSB is to be padded with the value 0).
4. For j=1 to 9 do
   If (k_j==1) then
   Generate a random value 'r' (either 0 or 1)
   If (r==0) then
   $S_{j,1}$=0
   $S_{j,2}$=1
   Else
   $S_{j,1}$=1
   $S_{j,2}$=0
   Else
   $S_{j,1}$=0
   $S_{j,2}$=0
5. Scan through O^1 and for each pixel of color k^1_p , arrange the row "i" in S as a 3x3 block B^1_p and fill the subpixels valued "1" with the color k^1_p, if and only if k^1_p is a non-white color.
6. Do the same for O^2 and construct B^2_p. The resulting blocks B^1_p and B^2_p are the subpixels of the P^{th} pixel after the expansion.
7. After processing all the pixels in all the three planes of I_{HL}, two shares, namely share 1 and share 2 , for each of the three planes of the secret image are generated. Performing an OR operation on the share 1 for each of the primitive color planes(R,G,B) ,the Camouflage Image 1 is produced. Similarly Camouflage Image 2 is produced.

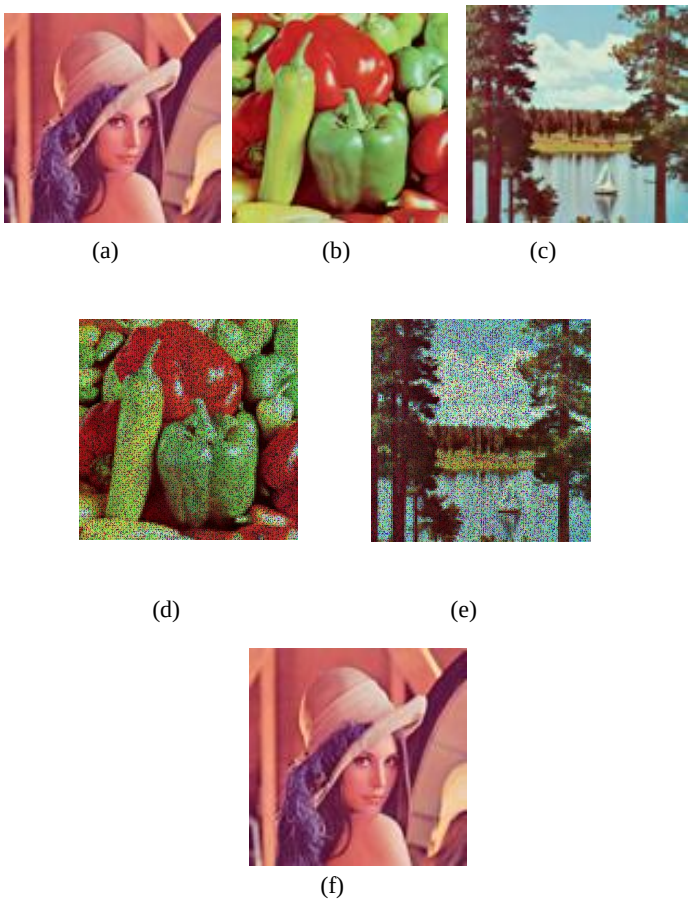
2.4 Decryption Method

The Camouflage images O1* and O2* are required for the recovery process. The camouflage images are 9 times bigger than I_{HxL} due to the expansion factor of sub-pixels.

1. The Camouflage images are decomposed into the three primitive color planes(R,G,B).
2. Extract the first 3x3 blocks V^1 and V^2 from the planes of both the camouflage images O1* and O2* respectively.
3. Rearrange V^1 and V^2 in a 2x9 matrix format S_R.
4. Input S_R to the F(_) corresponding to equation (1) to obtain $(k_1k_2\ldots k_9)$.
5. Recover K_p , the first pixel in the respective color plane of I_{HxL} by converting $(k_1k_2\ldots k_9)$ to decimal value.
6. Repeat the same for all 3x3 blocks in O^{1*} and O^{2*} and construct I_{HxL} for all the three color planes.
7. Three decrypted planes corresponding to the three primitive colors are generated. Performing an OR operation on the three planes, the original image is recovered losslessly.

3. RESULTS

This paper was simulated and run on Matlab. A 100x100 secret image (Fig. a: lena) is hidden into two 100x100 cover images (Fig. b:fruits and Fig. c:lake).The camouflage images(Fig. d and Fig. e) produced are meaningful and contains less noise.The recovery of the secret image is lossless, as it is evident from fig.



(a) (b) (c)

(d) (e)

(f)

Fig. 4: (a) Secret Image , (b) Cover Image#1 , (c) Cover Image#2 , (d) Camouflage Image#1, (e) Camouflage Image#2, (f) Decrypted Image

Three pictures (Fig. a, Fig. b and Fig. c) as an input and generates two images (Fig. d and Fig. e) which correspond to two of the three input pictures. The third picture is reconstructed by printing the two output images onto transparencies and stacking them together.

4. REFERENCES

[1] M. Naor and A. Shamir, Visual cryptography. Advances in Cryptology EUROCRYPT '94. Lecture Notes in Computer Science, (950):1–12, 1995)

[2] E. Verheul, H. V. Tilborg.,"Constructions and properties of k out of n visual secret sharing schemes", Designs, Codes and Cryptography, 11(2), pp. 179–196, 1997.

[3] Chang, C. C. and Yu. T. X., Sharing a Secret Gray Image in Multiple Images, in the Proceedings of International Symposium on Cyber Worlds: Theories and Practice, Tokyo, Japan, Nov. 2002, pp.230-237

[4] C. Chang, C. Tsai, and T. Chen, A new scheme for sharing secret color images in computer network. In the Proceedings of International Conference on Parallel and Distributed Systems, pages 21–27, July 2000)

[5] C. Yang and C. Laih., New colored visual secret sharing schemes. Designs, Codes and Cryptography, 20:325–335,2000.

[6] A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping by Musheer Ahmad and M. Shamsher Alam.

[7] "Design and Implementation of a Novel Authentication Algorithm for Fool-Proof Lock-Key System Based On Visual Secret Sharing Scheme", by Harinandan Tunga, and Soumen Mukherjee, IJCSI Vol.9 Issue 3, No 1, May 2012, ISSN (Online): 1694-0814. www.ijcsi.org.

[8] Atul, Kahate, Cryptography and Network Security, (Second Edition 2008).