Visual Cryptographic Scheme for Color Images using Threshold Level Determination

Ms. K. Chitra
Research Scholar
Department of Banking Technology
School of Management, Pondicherry University, India-605014

Dr. V. Prasanna Venkatesan
Professor
Department of Banking Technology
School of Management, Pondicherry University, India-605014

Abstract

Visual cryptography is one of the cryptographic techniques which divide the original image (or) data into 'n' number of shares. Each share contains a part of original information, for the reconstruction process 'k' number of shares is required to reconstruct the data. Here we propose the visual cryptographic scheme for color images using threshold level determination. If the threshold level is higher in particular pixel for the particular color that pixel gains the transparency value (white shares) and the remaining other colors having black pixel values. The proposed method satisfy the visual cryptographic properties such as there will be no pixel expansion, it requires only few shares to reconstruct the image, there will be no lose in the data share.

Keywords: Visual Cryptography, Dithering, Secret Sharing, Primitive Color Additive Model

I. INTRODUCTION

Now a days the transmission of digital data from one node to another node through the network is increasing. So, providing security for the nodes is a big challenge for the network. Visual cryptography is one of the cryptographic techniques which carried out the information in a secured manner. The word security in visual cryptography provides many ways of security like password transmission, hiding the secret information, steganography techniques, watermarking techniques, identification and authentication of owners.

But the above such techniques/methods does not provide such security like visual cryptography scheme provides because the main drawback of that technique is that the secret information which can be protected in single information carrier. If the information carrier is lost/ damaged/ destroyed we cannot reconstruct the original information. To overcome this problem, visual cryptography secret sharing scheme was introduced by Naor and Shamir. The secret information is split into two components/shares that two components/shares are required for reconstruction of the original information by superimposing a threshold number of shares.

In the visual cryptography scheme it does not required any computation for the decryption process because our human vision system has to perform the pixel- wise logical OR operation. Suppose, the pixels are small and also it having higher density then our human vision system will average out the colors around the particular pixels. For early days, the visual cryptography system mainly focuses on black and white secret images [2]-[9]. After that they move on to grey scale images, this images using dithering process (i.e. adding noise to the image/shares) which degrades the image quality[10]. Another issue in visual cryptography scheme is image size invariant (i.e. pixel expansion) which means that the original image size is twice less than that of the secret shares and also the retrieved image size, this also causes the reduction in image quality.

In this paper, we introduce a new visual cryptography scheme for color images. Which supports the images for 'n' number of colors and there will be no pixel expansion. If we can reconstruct the original image we required K-out-of-N shares and also it adjust no. of color levels in the secret shares. For the construction of visual cryptography scheme we are using probabilistic technique for achieving no pixel expansion. For the color level determination we use standard deviation to identify the colors. For separating the shares in color level determined image we use additive model with probability in shares.

II. RELATED WORK

Naor and Shamir introduce the concept of visual cryptography. This concept using many types of secret sharing schemes this all schemes are applied to any type of application and also any type of images. Here we taken some of the samples of VCS scheme are (k-n) secret shares that are embedded into the envelope images by LSB. This embedded LSB are retrieved from each of the pixel by OR operation from that they generate the original image [8-10]. Most of the papers they are taken the sample as two share images of (2, n, h, l) scheme that have been demonstrated with the minimum value of 'm' is given as $m=m_{min}(2, n, h, l)$ this new bound provide a slight variation of the ILP and also it find out the corresponding pixel value by $m_{mei}(2, n, h, l)$ and $m_{mee}(2, n, h, l)$ [1].

For constructing those imagers they are using threshold VCS for black and white images to color images using Boolean matrix. Here for the threshold calculation they generate histogram. In addition to that they tune the pixel value using the random pick of probability values [6-8].

III. PROPOSED SCHEME

The architecture design describes the overall flow of the system at the starting stage to the ending stage. The proposed scheme explains all the main process such as selection of secret image, automatic detection of color levels, generating given no. of shares and overlapping of shares.

In the sender side, first they have to choose the secret message/image in color after that the determination of color level is taken place. Depending upon the color level the binary information is created (e.g.) for a taken particular pixel the color component of that particular pixel having red color is more than that of the other two color components.

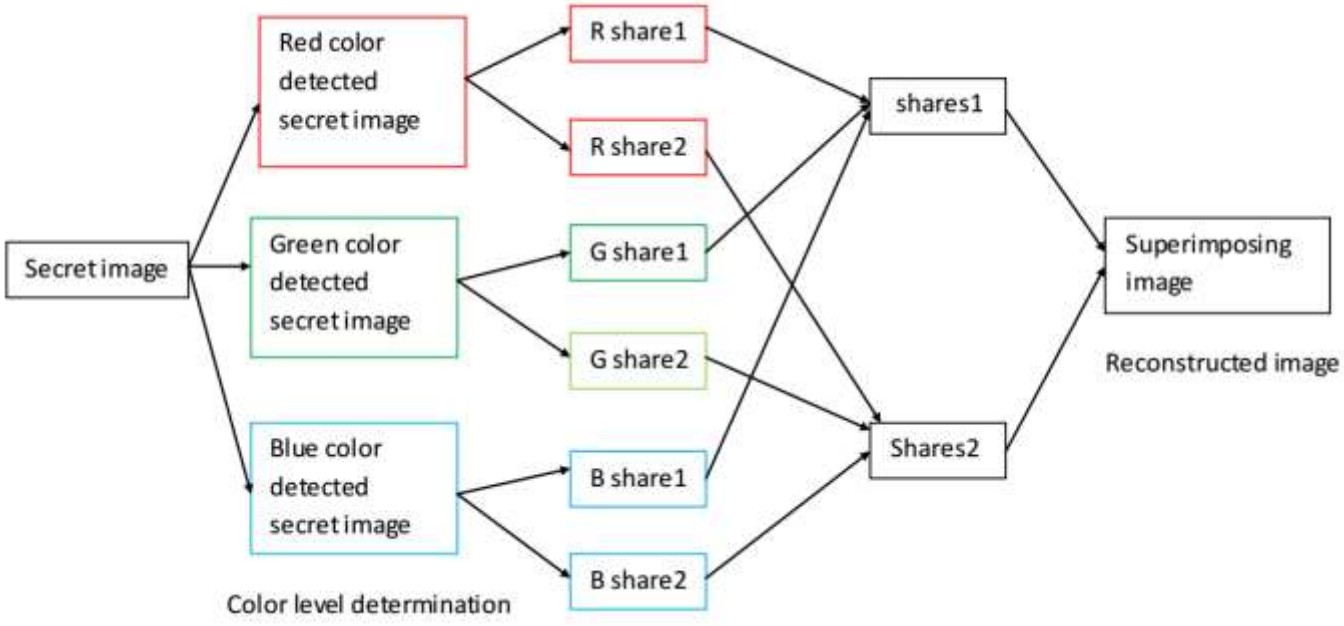

Fig. 1: Architectural Diagram for Proposed VCS

That red color is taken as the transparency color value 1 and the other two colors taken the value as 0. The same process is taken out for the end of last pixel. After the color level determination of the secret image, each color detected secret image is divided into two shares. After the segregation each color shares we have to grouping the share1 and share2 of all colors with the help of color multiplication algorithm. At the last by superimposing this share, finally we get retrieved image.

IV. EXPERIMENTAL RESULTS

In this section, the experimental results for each stage using the algorithm can be illustrated and the screen shots for the output retrieved can also be shown.

A. *Step1: Select A Secret Image*

The user has to select the secret image which has to be transmitted secretly. Here we taken the secret image as Lena.jpg with the matlab comment is given as,

```
secretImg = imread(strcat(Path,FileName));
```

The following comment is used to split the color component,

```
R = secretImg(:,:,1);
G = secretImg(:,:,2);
B = secretImg(:,:,3);
```

Find out the secret image size with these following comments,

```
[height, width, ~] = size(secretImg);
size_of_image = height * width;
```

Fig. 2:

B. *Step 2: Automatically Detect The Color Level*

For the given Lena.jpg color image, the color value is assigned for each color is determined with the help of standard deviation.

1) The color level assigned for red color is 32 and the standard deviation is 1805.60.
2) The color level assigned for green color is 32 and the standard deviation is 1275.10.
3) The color level assigned for blue color is 24 and the standard deviation is 2134.55.

Depending upon the deviation in the colors the standard deviation generates the color value. The above point shows the particular color values and their standard deviation. The below shown figure shows the decomposition of RGB color images.

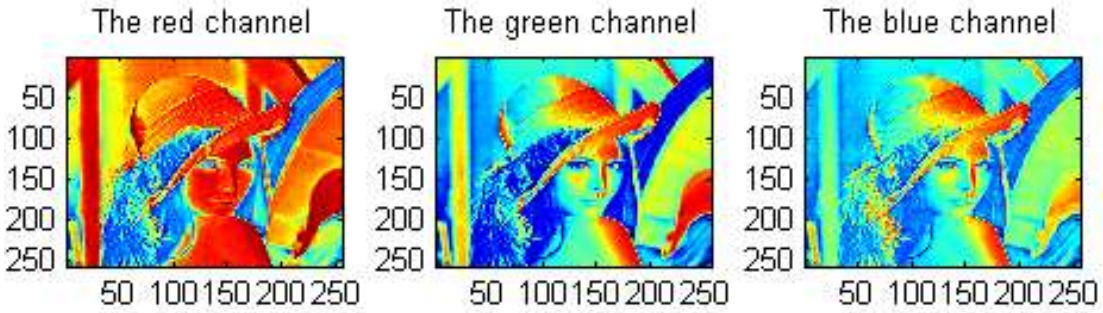

Fig. 3:

C. *Step 3: Generating Shares*

The following comment generates the 2-out –of-2 shares for each color secret image. For the generation of shares it carried out one color after another color.

```
[ rShare1, rShare2 ] = two_two_ShareGen ( secretImg, COLOR_LEVEL_RED, a, 1);
[ gShare1, gShare2 ] = two_two_ShareGen ( secretImg, COLOR_LEVEL_GREEN, g,2);
[ bShare1, bShare2 ] = two_two_ShareGen ( secretImg, COLOR_LEVEL_GREEN, b,3);
```

For each pixel, the random number is generated if that random number is less than 0.5 it takes the value as 0 (or) otherwise 255 for both that two shares. If the taken random number is greater than 0.5 then it takes the values as 0 for share1 and 255 for share2 (or) 0 for share2 and 255 for share1.

D. *Step 4: Overlapping shares:*

In this step, the grouping of shares is taken place with the help of OR operation. The share1 and share2 of each color is grouped separately. By using the following comments we group those shares.

```
rgbImage1 = cat(3, rShare1, gShare1, bShare1);
rgbImage2 = cat(3, rShare2, gShare2, bShare2);
result_share1 = rgbImage1;
result_share2 = rgbImage2;
```

By overlapping these two grouped shares we get the reconstructed image of Lena with the help of color multiplication.

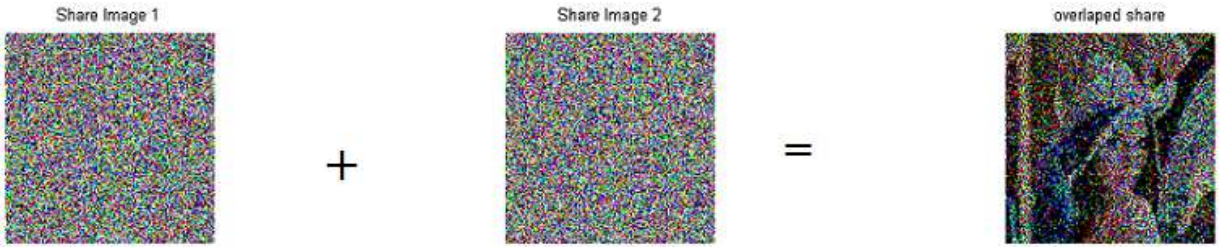

Fig. 4:

V. CONCLUSION

In this paper we use K-out-of-N secret sharing techniques for visual cryptography. Our original image is reconstructed from the three channel images R, G, B shares. For primitive color grouping we use color multiplication with additive model. Here the visual cryptographic scheme is proposed to provide more security to the original data. For the reconstruction process our human vision system has to perform the XOR operation. The main advantage of using this technique is 'k' number of shares is sufficient to reconstruct the original image; there will be no pixel expansion and also we did not require any complex mathematical model for decryption.

REFERENCES

[1] P. A. Eisen and D. R. Stinson, "Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels," in Des. Codes Cryptography, vol. 25, no. 1, pp. 15–61, 2002.
[2] Carlo Blundo, Paolo D'Arco and Douglas R.Stinson, "Contrast Optimal Threshold Visual Cryptography Schemes", in Society for Industrial and Applied Mathematics, 2003.
[3] Bin Yu, Xiaohui Xu and Liguo Fang, "Multi-secret Sharing Threshold Visual Cryptography Scheme," in 2007 International Conference on Computational Intelligence and Security Workshops.
[4] Fang Liguo and Yu Bin, "(2, n) Visual Threshold Scheme Based on Permutation", in Computer Engineering, 33(9): 157-159, 2007.
[5] Haibo Zhang, Xiaofei Wang, Wanhua Cao and Youpeng Huang, "Visual Cryptography for General Access Structure Using Pixel-block Aware Encoding," in Journal of computers, vol. 3, no. 12, December 2008.
[6] Xiaoyu Wu , Duncan S. Wong , and Qing Li, "Threshold Visual Cryptography Scheme for Color Images with No Pixel Expansion," in ISCSCT '09, vol. 26-28, pp.310-315 December 2009.
[7] T.-H. Chen and K.-H. Tsao, "Threshold visual secret sharing by random grids," in Journal of Systems and Software, vol. 84, no. 7, pp. 1197–1208, 2011.
[8] Shyamalendu Kandar and Bibhas Chandra Dhara, "k-n Secret Sharing Visual Cryptography Scheme on Color Image using Random Sequence", International Journal of Computer Applications (0975 – 8887) Volume 25– No.11, July 2011.
[9] Dimple Kapoor , Swati Keshari , Saurabh Kumar Gaur, "An Overview of Visual Cryptography", in International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 2, February 2014.
[10] Bharanivendhan and Amitha, "Visual Cryptography Schemes for Secret Image Sharing using GAS Algorithm," in International Journal of Computer Applications (0975 – 8887), Volume 92 – No.8, April 2014.