An Improved Visual Cryptography Scheme for Colour Images

Asha Bhadran R

M,Tech, Computer Science and Engineering, Lourdes Matha College of Science and Technology,Thiruvananthapuram ,Kerala, India

---***---

Abstract - ***With the growth of digital media, it is becoming more prevalent to find a method to protect the security of that media. An effective method for securely transmitting images is found in the field of Visual Cryptography (VC). Visual cryptography scheme is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes, and images etc) to be encrypted in such a way that the decryption can be performed by the human visual system(HVS), without the aid of computers. The shares are safe because separately they reveal nothing about the secret image. A distinctive property of visual cryptography scheme is that one can visually decode the secret image by superimposing shares .By taking advantage of this property, third person can easily retrieve the secret image if shares are passing in sequence over the network. This paper presents a visual cryptographic technique for color images in which the generated shares are again encrypted. For this XOR operation is used and this will provide double security for the secret document. Thus secret shares are not available in their actual form for any alteration by the adversaries who try to create fake shares. The proposed scheme also uses the concept of halftoning.***

KeyWords : *Visual Cryptography , Halftoning ,*

Information Security.

1. INTRODUCTION

In today's information age, information sharing and transfer has increased exponentially. The threat of an intruder accessing secret information has been an ever existing concern for the data communication experts. With the rapid advancement of network topology, multimedia information is transmitted over the Internet conveniently. Various confidential data such as military maps and commercial identification are transmitted over the Internet. While using secret images, security issues should be taken into consideration because hackers may utilize weak link over public network to steal information that they want. To deal with security problems of secret images, we should develop some secure appropriate algorithm by which we can secure our data on internet. With this system visual information (pictures) can be secure over the internet with the help of Visual Cryptography.

This scheme enhances the security of VC shares through the encryption of shares using image encryption algorithm, which provides the strong security to the transfer of secret information in form of images, printed text and hand written material.

Visual Cryptography (VC) is a special encryption technique used to encrypt images in such a way that it can be decrypted by the human visual system if the correct key images are used. The technique was proposed by Moni Naor and Adi Shamir in 1994. According to them Visual Cryptography is a method of encrypting a secret image into shares such that stacking a sufficient number of shares reveals the secret image. Shares are binary images usually presented in transparencies. Unlike conventional cryptographic methods, VC needs no complicated computation for recovering the secret image. The act of decryption is to simply stack shares and view the secret image that appears on the stacked shares. Visual Cryptographic technique is being used for secretly transfer of images in army, hand written documents, financial documents, text images, internet- voting etc.

VC shares exist in their actual form during the transmission over network. However, directly third person cannot guess the secret information with any single share, but there is a possibility of retrieval if hackers are able to collect all the shares passing in sequence over the network. Thus to get rid of this problem, we need to enhance the security of shares. For the same purpose we have to encrypt the shares generated using Visual Cryptography so that even if hackers are able to get all the shares but they cannot retrieve the original secret without the access of key.

2. RELATED WORK

Basic (2,2)Visual Cryptography Scheme : Naor & Shamir [4] implemented a (2, 2) visual cryptography. In this type of visual cryptography scheme, the secret image is divided into exactly two shares-share1 and share2. To reveal the original image, these two shares are required to be stacked together. If pixel is white one of the above two rows of table from fig 2.1 is chosen to generate share1 and share2 , likewise if pixel is black one of the below two rows table of fig 1 is chosen to generate Share1 and Share2. Here each share of pixel p is encoded into two white and two black pixels. Each share alone gives no hint about the pixel p. That is share will not provide any information whether it is white or black. Secret image is shown only when both shares of images are overlaid or superimposed.

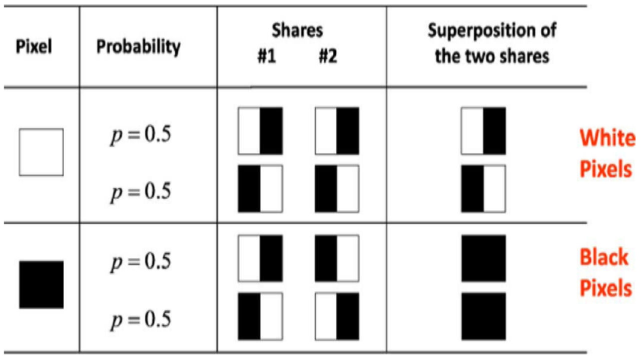


Figure 2.1 : Construction of (2,2) VC scheme

Shyamalendu Kandar & Arnab Maiti [2] has proposed a technique of k-n secret sharing on color images. At the time of dividing an image into n number of shares, they have used random number generator. Minimum k numbers of shares are sufficient to reconstruct the image. If k numbers of shares are taken then the remaining shares are (n–k). In an image if certain position of a pixel is 1, then in (n–k) +1 number of shares in that position of that pixel there will be 1. In the remaining shares in that position of the pixel there will be 0. A random number generator is used to identify those (n–k) +1 number of shares. Secret is not properly hidden and it is easy to guess the contents in all three shares. If intruder is able to get the information about randomness, secret image can be retrieved.

Kulvinder Kaur, Vineeta Khemchandani [1] presents an approach for encrypting visual cryptographically generated image shares using Public Key Encryption. RSA algorithm is used for providing the double security of secret document. Thus secret share are not available in their actual form for any alteration by the adversaries who try to create fake shares.

3.EXISTING SYSTEM

The existing scheme generates the VC shares using basic Visual Cryptography model and then encrypt both shares using RSA algorithm of Public Key Cryptography so that the secret shares will be more secure and shares are protected from the malicious users who may alter the bit sequences to create the fake shares. During the decryption phase, secret shares are extracted by RSA decryption algorithm & stacked to reveal the secret image. Existing methodology is shown in figure 3.1.

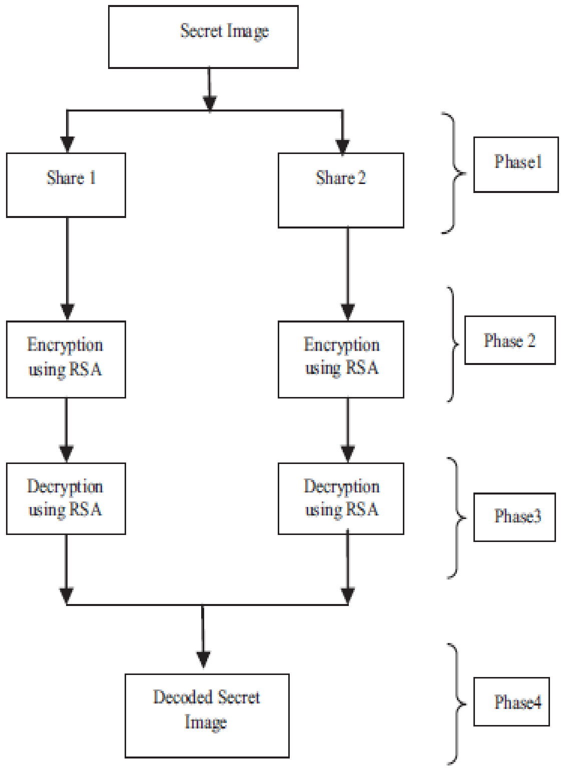


Fig- 3.1 : Existing system methodology

3.1. Limitations of existing system

Existing scheme have the following limitations:

- Existing scheme is only valid for binary images.
- Encrypted image requisite large bandwidth over network.
- Takes more time for the encryption of the shares using RSA algorithm.
- RSA algorithm requires complex computation.

4. PROPOSED SYSTEM

The proposed system consists of 5 modules.

Image Conversion: In this module, a color input image is taken as the input image. Then the input secret image is divided into three channel images namely red channel, green channel and alpha channel. And on each of the channel images halftoning is applied.

A halftone image is made up of a series of dots rather than a continuous tone. These dots can be different sizes, different colors, and sometimes even different shapes. Larger dots are used to represent darker, more dense areas of the image, while smaller dots are used for lighter areas. Color halftoning generates a halftone pattern for each of these inks. When these patterns are printed over each other, the human viewer will observe a color that depends on the amounts of the color inks.

Share Generation : In this phase Visual Cryptography Encryption is implemented. It consists of generation of shares from secret image using VC (2, 2) scheme. To encode a secret employing a (2,2) VC scheme the original image is divided into two shares such that each black pixel in the original image is replaced with a non-overlapping block of subpixels .and a white pixel is shared into two identical blocks of subpixels. The result of this module is the generation of six shares of secret image (2 shares from each channel image).

Share Encryption : Shares are encrypted with a simple image encryption algorithm which uses the help of bitxor operation.
The procedure is as follows:

```
1.Generate the key.
2.For each pixel in the input share,
   Fkey(:,ind) = key((1+(ind-1)*n) : (((ind-1)*n)+n));
3. for ind1 = 1  to  length of input share
4    for ind2 = 1 to breadth of input share
 5 perform     outImage(ind1,ind2) =
bitxor(Img(ind1,ind2),Fkey(ind1,ind2));
 6 ImageOut(:,:,ind) = outImage(:,:,1);
```

Share Decryption : Share decryption requires the same key that is used to encrypt the share.Share decryption also uses the same algorithm which is used for share encryption except that the encrypted share is given as the input.

Visual Cryptographic Decryption : In this phase ,Visual Cryptographic decryption will be performed.We can decrypt the original image by applying binary XOR operation on both decrypted shares of each channel image and finally concatenate all these to obtain the original image.
The methodology of the proposed system is shown in the figure 4.1 and 4.2.

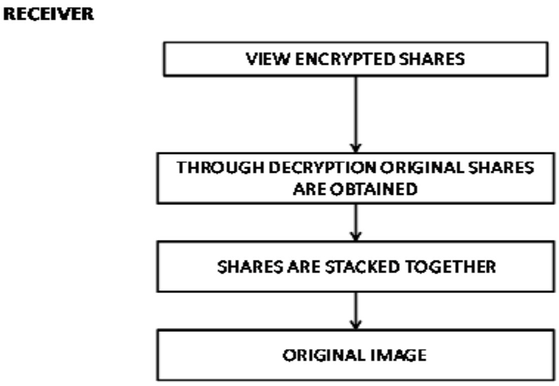

RECEIVER
VIEW ENCRYPTED SHARES
THROUGH DECRYPTION ORIGINAL SHARES ARE OBTAINED
SHARES ARE STACKED TOGETHER
ORIGINAL IMAGE

Fig- 4.2 : Decryption Process

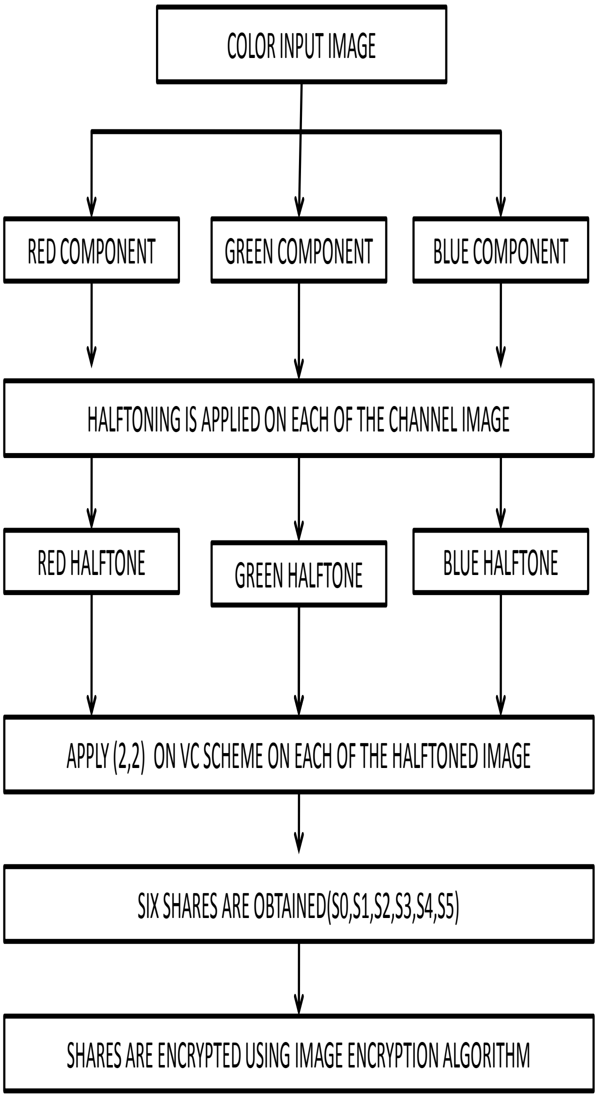
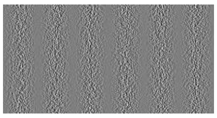

COLOR INPUT IMAGE
RED COMPONENT
GREEN COMPONENT
BLUE COMPONENT
HALFTONING IS APPLIED ON EACH OF THE CHANNEL IMAGE
RED HALFTONE
GREEN HALFTONE
BLUE HALFTONE
APPLY (2,2) ON VC SCHEME ON EACH OF THE HALFTONED IMAGE
SIX SHARES ARE OBTAINED(S0,S1,S2,S3,S4,S5)
SHARES ARE ENCRYPTED USING IMAGE ENCRYPTION ALGORITHM

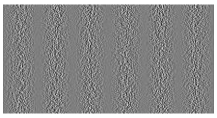
Fig- 4.1: Encryption process

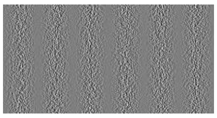
5.EVALUATION OF RESULTS

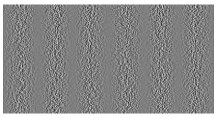
Proposed scheme has been implemented in MATLAB 7(R2010a) . To run this scheme minimum hardware configuration is required with no extra specifications. The experiments have been run in Windows 8 .
To test the performance of this scheme number of experiments has been conducted with varying image sizes, types but every time secret color image is retrieved and the time taken to encrypt the shares is less than that of existing system.
Results of some experiments are shown in the following figures:

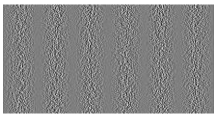
(a)Original image

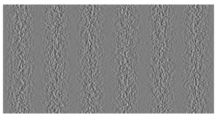

(b1)Share 1

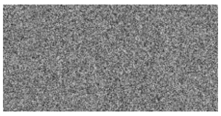

(b2)Share 2

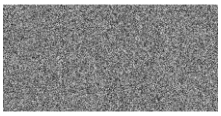

(b3)Share 3

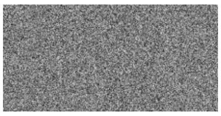

(b4)Share 4

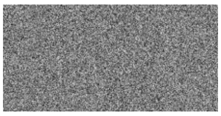

(b5)Share 5

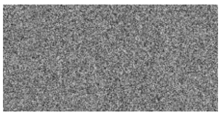

(b6)Share 6

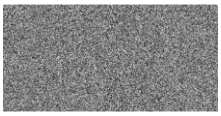

(c1)Encrypted share 1

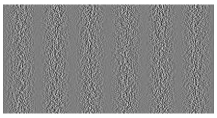

(c2)Encrypted share2

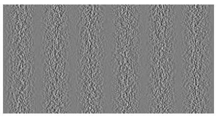

(c3)Encrypted share3

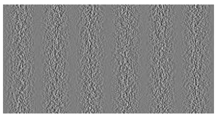

(c4)Encrypted share4

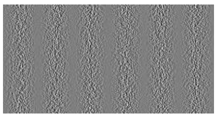

(c5)Encrypted share5

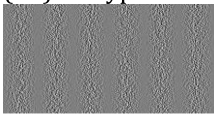

(c6)Encrypted share6

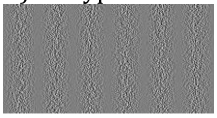

(d1)Decrypted share1


(d2)Decrypted share2


(d2)Decrypted share3


(d3)Decrypted share4


(d5)Decrypted share5


(d6)Decrypted share6

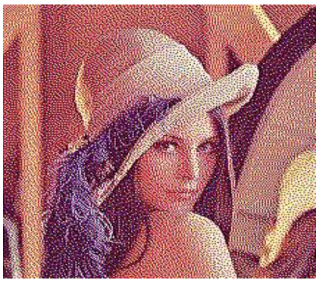

(e)Retrieved image

Fig – 5.1:Results of proposed scheme

The comparisons of the existing and proposed works as shown in the Table1

Table -1: Comparison

Algorithm	Complexity	Security	No.of share gene-rated	Image retrieved if color image is given as input
Naor & Shamir (Basic 2×2)	Medium	Increase	2	Binary
Kaur & Khemc-Handani's Scheme	More complex	Increase	2	Binary
Proposed	Medium	Increase	6	Color halftone

Chart -1 shows the size of decrypted images for the existing and proposed schemes.

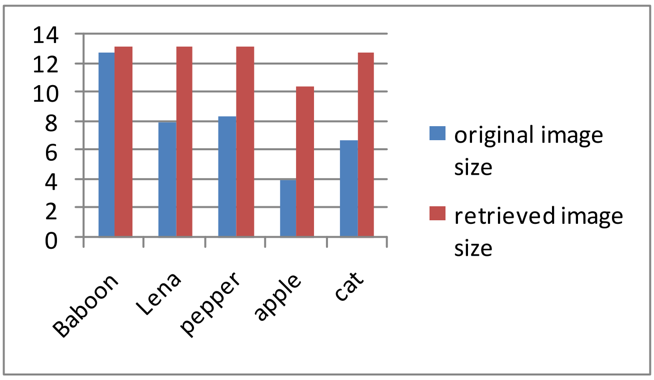


Chart -1 :Comparison based size of decrypted images.

Fig-5.2 shows that the entropy value of the proposed scheme is higher than the existing scheme which means the proposed scheme is better than the existing schemes .

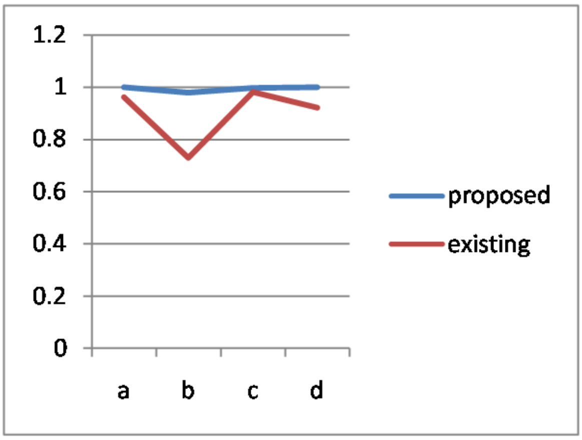


Fig-5.2:Comparison based on entropy value.

6. CONCLUSIONS

With the rapid evolution of digital media, it is becoming vital to find a method to protect the security of that media. An effective method for securely transmitting images is found in the field of Visual Cryptography. In my work visual cryptography shares are again encrypted using image encryption algorithm for providing the double security of secret document.Existing schemes are valid only to binary and gray-level images. But in my work when a color image is given as input, the retrieved image was color halftone image.

Advantages :

- Color images are retrieved.
- Complexity is less.
- Double security.

7.FUTURE WORK

It has been observed that there are many possible enhancements and extensions exist as the visual quality & size of revealed image. The major areas of future scope are:

- Inorder to improve the quality of decrypted images, inverse halftoning can be applied.
- Size of images.

REFERENCES

[1] Kulvinder Kaur,Vineetha Khemchandani,*Securing Visual Cryptographic Shares Using Public Key Encryption*,3rd IEEE International Advance computing conference,2013

[2] Shyamalendu Kandar , Arnab Maiti," K-N secret sharing visual cryptography scheme for color image using Random number",vol 3,no.3,Mar 2011.

[3] InKoo Kang, Member, IEEE, Gonzalo R. Arce, Fellow, IEEE, and Heung-Kyu Lee, Member, IEEE, "Color Extended Visual Cryptography Using Error Diffusion", IEEE Transactions on image processing, vol. 20, no. 1, january 2011.

[4] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT, 1994, pp. 1–12.

[5] A. Houmansadr and S. Ghaemmaghami, "A novel video watermarking method using visual cryptography," in Proc. IEEE Int. Conf. Eng. Intell. Syst., 2006, pp. 1–5

[6] Manika Sharma, Rekha Saraswat ,*Secure Visual Cryptography Technique for Color Images Using RSA Algorithm,* International Journal of Engineering and Innovative Technology , Volume 2, Issue 10, April 2013

[7] Young-Chang Hou. Visual cryptography for color images. Pattern Recognition, 36:1619-1629, August 2002.

[8] Jim Cai, "A Short Survey On Visual Cryptography Schemes", 2004 http:// www.cs.toronto.edu/~jcai/paper.pdf.

[9] Ching-Nung Yang ,Tse-Slih Chen,"Colored Visual Cryptography Scheme based additive color mixing",Pattern Recognition,vol. 41,pp.3114-3129,2008.

BIOGRAPHIES

Asha Bhadran received her BTech degree in Information Technology in 2012 from Kerala University. Currently, she is pursuing M.Tech in Computer Science and Engineering from Kerala University.