# A New Visual Cryptography Scheme for Color Images

B.SaiChandana , S.Anuradha

Department of Computer Science and Engineering
GITAM University, Visakhapatnam
Email: bschandana@yahoo.co.in,ganuharsh@gmail.com

## Abstract

Visual cryptography is a method for protecting image-based secrets that has a computation-free decoding process. In this paper, we proposed a visual cryptographic system which can be used to hide the original image information from an intruder or an unwanted user. The images can be in any standard format. The encrypted image is sent to the destination through the network and then the image is decrypted. We used symmetric key cryptography. Experimental results indicate the proposed method is a simple, practical and effective cryptographic system.

**Key Words**: Image sharing, Visual cryptography, Image processing.

## I. Introduction

Visual cryptography [1] is a cryptographic technique which allows visual information (pictures, text, etc) to be encrypted in such a way that the decryption can be performed by the human visual system without the aid of computers. As network technology has been 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 image in any standard format, so that the encrypted image when perceived by the naked eye or intercepted by any person with malicious intentions during the time of transmission of the image is unable to decipher the image.

Firstly an image and key is fed into cryptosystem. The encryption algorithm produces a cipher image which is sent into receiver through a communication channel. When the cipher image reaches the destination, the receiver enters the key and the original image is decrypted. Figure 1 shows the block diagram of the cryptosystem. The key we used is the symmetric key with minimum size of 47 bits. Two important factors are used to determine the efficiency of any cryptographic scheme [2], namely: 1) the quality of the reconstructed image and 2) the resizing factor ("fac"). Any loss of information during the reconstruction phase leads to reduction in the quality of the recovered image. On the other hand resizing factor refers to enlarging or reducing the original image. To enlarge an image, specify resizing factor greater than 1. To reduce an image, specify resizing factor between 0 and 1.For bandwidth constrained communication channels it is desirable to keep resizing factor ("fac") as small as possible. For color images, reducing resizing factor is of paramount importance since they occupy more space and consume more band width compared to grayscale and binary images.

This paper is organized as follows: Section II describes the theoretical formulations, Section III describes the mathematical function, Section IV describes the encryption algorithm, Section V describes the decryption algorithm, Section VI gives the experimental results and finally Section VII gives the conclusion.

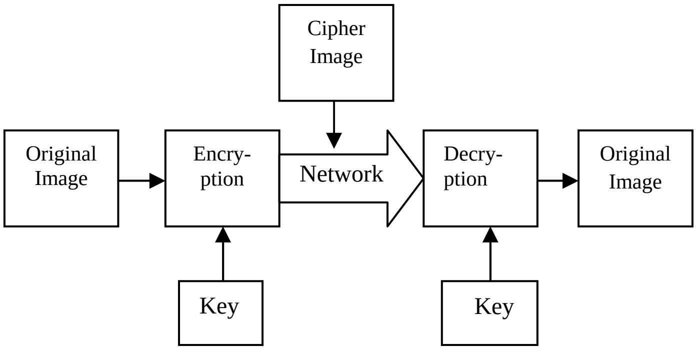


Figure 1: Block diagram of our Cryptosystem

## II. Theoretical Formulations

A color image is usually represented in the RGB color space [3,4] , because most of the computer input and output devices use this color system. Each vector consists of three components, which are the intensity values in the Red, Green and Blue channel. The combination of these values delivers one particular color. A change in the intensity value will change the information stored in the picture. So by performing some changes in intensity values we can encrypt the image and doing the reverse in decryption. If the changes are performed separately on Red, Green and Blue layers, we can have more robust visual cryptographic system. This is because of the fact that when an intruder goes for complete analysis of the image will try to know these basic intensity values. These intensity values will help him to generate the original image. So if the encryption is done at this basic level then it will be hard to break the system. All the changes in the intensity values are performed using a mathematical function.

## III. Mathematical Function

The function used in this cryptosystem should have a bijective mapping i.e. the function should have one-one and onto mapping. This indicates the inverse of the function exists. Hence the original information of the image can be retrieved back during decryption without any error. The function is given as

g(u)= abs(1/log(tan((exp(k) * cos(exp(1)) * sin(exp(U))))))

here ‘k’ and’ l’ are the keys and ‘U’ is the gcd of the two keys which are used for encryption.

## IV. Encryption Algorithm

Step 1: Ask for the image and the keys X1 and Y1 and the resizing factor “fac”.

Step 2: Generate the function g( ) which will contain the values generated from a function in an array.

Step 3: Find the absolute value of the function g( ). Here U=gcd(X1,Y1).

Step 4: Pass it through a low pass filter.

Step 5: Resize the image using bi-cubic interpolation and get the RGB layer in a separate matrix with the factor “fac”.

Step 6: Multiply the pixel values with the absolute values calculated.

Step 7: Flip the new formed Red matrix upside-down.

Step 8: Flip the new formed Green matrix left-side right.
Step 9: Rotate the Blue matrix by twice of the “fac”.

Step 10: Generate the image again save it in .bmp format. (The image is saved in .bmp format because actual values of the pixel are retained and the number of pixels is also the same which is in contrast with the other compressed images like jpeg, gif, etc.)

Step 11: Send the image with the resizing factor to the receiver.

## V. Decryption Algorithm

Decryption is just the reverse process of encryption. The aim of decryption is to make the encrypted information readable again (i.e. to make it unencrypted).

Step 1: Receive the image and ask for the key and resizing factor.

Step 2: Break the received image into Red Green and Blue parts/layers.

Step 3: Flip the new formed Red matrix upside-down.

Step 4: Flip the new formed Green matrix left-side right.

Step 5: Rotate the Blue matrix by twice of the “fac”.

Step 6: Generate the function depending upon the keys. Here U=gcd(X1,Y1).

Step 7: Find the absolute value of function and pass it through low pass filter.

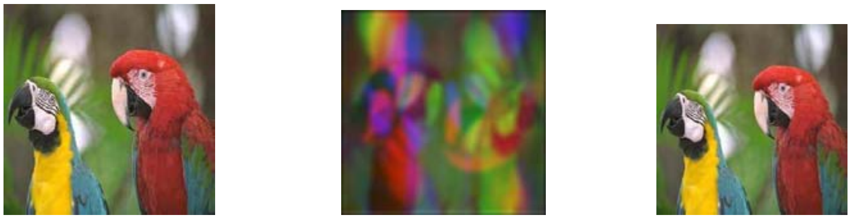
Step 8: Divide the pixel values of the received image with the absolute value of the function.

Step 9: Form the image.

Step 10: Resize the image by multiplying its rows and column with the “fac” using bi-cubic interpolation.

## VI. Experimental Results

This section presents the simulation results illustrating the performance of the proposed cryptosystem. The test image employed here is the true color image “parrot” with 290×290 pixels. The key size is of 47 bits. The encryption and decryption algorithm are implemented in MATLAB 7.0 [5,6] in core2duo of 2.66 GHz machine. The decryption algorithm takes 40 seconds to get executed. Now if an intruder goes for the exhaustive search for the keys then it will take around $2.2*10^{22}$ years to get the keys. This is the long time for secret information to lose its secrecy. Hence the proposed system is a strong one. If the key length is increased the system will become more secure. The results for our system are shown in figure 2 and in figure 3.

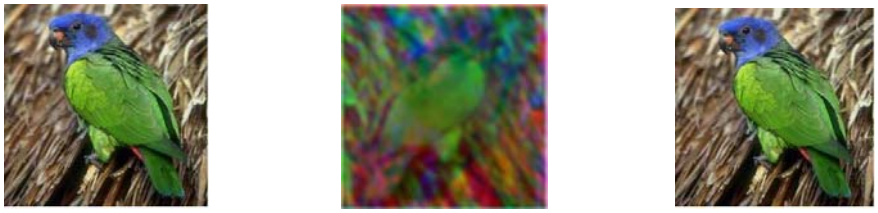


a) Original image

b) Encrypted image

c) Decrypted image

Figure 2: Encryption and Decryption process



a)Original image b) Encrypted image c) Decrypted image

Figure 3: Encryption and Decryption Process

As stated earlier, the efficiency of any cryptosystem depends on the quality of the reconstructed image. We used the Structural Similarity (SSIM) index [7] for measuring the quality between two images. The SSIM index can be viewed as a quality measure of one of the images being compared provided the other image is regarded as of perfect quality.  The quality measures are calculated between the original image and the encrypted/decrypted image. Table 1 shows the quality measures of the images in figure 2 and in figure 3.

Table 1: SSIM index

| Image | SSIM Index ( for figure 2) | SSIM Index ( for figure 3) |
|---|---|---|
| Original Image | 1 | 1 |
| Encrypted Image | 0.0004 | 0.0003 |
| Decrypted image | 0.98 | 0.99 |

## VII. Conclusion

In this paper, we have presented a new visual cryptographic system which can be used to hide the original image information from an intruder or an unwanted user. The advantages of the proposed method are its resizing factor and its capability of perfect reconstruction of the secret image. This work is an attempt to make a secured transfer of valuable images between two trusted parties. The confidentiality is maintained and the authentication can be checked by digital signatures. The proposed method can be considered as a good candidate for secure visual data transmission in systems with limited bandwidth. This work is highly applicable in military field.

## VIII. References

[1] M.Naor and A Shamir, “Visual Cryptography”, Proceeding of Eurocrypt 94 Lecture Notes in Computer Science, LNCS963,Berlin: Springer, 1994, pp1-11.

[2] Mohsen Heidarinejad, Amirhossein Alamdar Yazdi and Konstantious N.Plataniotis, “ Algebraic visual cryptography scheme for color images”, ieee transactions 2008.

[3] K. Jain, “Fundamentals of Digital Image Processing”. Englewood Cliffs, NJ: Prentice-Hall, 1989.

[4] Ian T. Young, Jan J. Gerbrands, Lucas J. VanionVliet, “ fundamentals of image processing “ paperbook.

[5] Gilat, Amos (2004). MATLAB: An introducComputingtion with applications 2nd edition. John Wiley and Sons.

[6] Quarteroni, Alifo; Fausto Saleri(2006). Scientific with MATLAB and Octave. Springer.

[7] Z. Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600-612, Apr. 2004.