ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 10, April 2013

Secure Visual Cryptography Technique for Color Images Using RSA Algorithm

Manika Sharma, Rekha Saraswat

Abstract*— Visual Cryptography is a special technique which is used to send the images securely over the network. Visual cryptography is a cryptographic technique which allows visual information to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. Simple Visual Cryptographic technique is insecure. This cryptographic technique involves dividing the secret image into n shares and a certain number of shares (m) are sent over the network. The decryption process involves stacking of the shares to get the secret image. In the current work, we have proposed a cryptographic technique for color images where we are using color error diffusion with XOR operation. The shares are developed using Random number. The key generated for decryption process is sent securely over the network using RSA algorithm. This approach produces less distorted image and the size of the decrypted images is same as the original image.

***Index Terms*—Dithering, Random Number, RSA, Visual Cryptography.**

I. INTRODUCTION

In this Era, where sharing of information have become indispensable and is part of most of the activities being performed on internet. With the growth of Internet the need for secure sharing of images has become extremely important. There are basically two important components in cryptography, data hiding and secure transfer of data. Visual Cryptography is an emerging scheme which is proving to be efficient for both issues of secure image sharing. This technique is based on Human Visual System and hence do not include complex mathematical computations. The basic model of visual cryptography was given by Naor and Shamir for Binary images [1]. In this scheme the secret image is divided into n number of shares out of which the certain number of shares (m) is sent over the network to the required destination, any m-1 number of shares will not be able to reveal the secret image. Pixel is the smallest unit of an image .Here a 32-bit pixel of a digital image is taken and is divided into Red, Green, Blue, and Alpha each of 8 bit. Hence four channel images are produced where alpha part depicts the level of transparency.[5]

In 1998, the lattice based (k, n) VCS scheme for gray level and color image was proposed by H. Koga and H. Yamamoto. As per this method the pixels are treated as elements of finite lattice and the superimposing of pixels is done as an operation on the finite lattice. In this scheme, (k,n) VCS for color images is described with c colors as a collection of c subsets in nth Cartesian product of the finite lattice.[10] Chin-Chen Chang proposed spatial-domain image encrypting schemes. Here two secret shares are embedded into two gray level images. To decode the hidden messages, enveloping images can be superimposed [8].

Liguo Fang recommended a (2, n) scheme based on balancing the performance between pixel expansion and contrast. [9] Xiaoping and Tan suggested Threshold visual secret sharing schemes which mixed XOR and OR operation and was based on binary linear error correcting code. In literature survey, we found that the disadvantage of these schemes is that only single set of secret messages can be embedded, so for sharing large amount of secret messages several shares should be generated and the key must be sent securely. The other issues are the problem of expansion in the size of decrypted image and the quality of the decrypted image. [10]

In this approach, the secret image is first divided into channel images and color error diffusion technique is applied for dithering to improve the quality of image. This technique produces better results as compared to other dithering techniques. In this paper Section II describes the overall encryption process. Section III describes the key generation and the secure sending of the key to the destination. Section IV defines the overall decryption phase. The analysis of the approach is given in section V and finally the conclusion is given in Section VI.

II. ENCRYPTION PROCESS

The overall process of encryption phase consists of several steps which are explained as follows. In this scheme a secret image is divided into four channel images namely red channel, green channel, blue channel and alpha channel. On each of the channel images color error diffusion technique is applied. The respective channel images are divided into n number of shares, with any m number of shares the secret can be perfectly reconstructed and even the complete knowledge of m-1 shares reveals no information about the original image. [7] [2]

Error diffusion is a type of half toning in which the quantization residual is distributed to neighboring pixels that have not yet been processed. The simplest form of the algorithm scans the image one row at a time and one pixel at a time. The current pixel is compared to a half-gray value [3]. If it is above the value a white pixel is generated in the resulting image. If the pixel is below the half way brightness, a black pixel is generated. The generated pixel is either full bright or full black, so there is an error in the image. The error is then added to the next pixel in the image and the process repeats.

The shares obtained after color error diffusion are enveloped in the innocent covers using invisible digital watermarking [6]. After this step the encrypted image is produced. Now the last step of the encryption is performed. The key is generated, which consist information about the number of shares and the information about the envelop images. The overall process is explained in the Fig I.

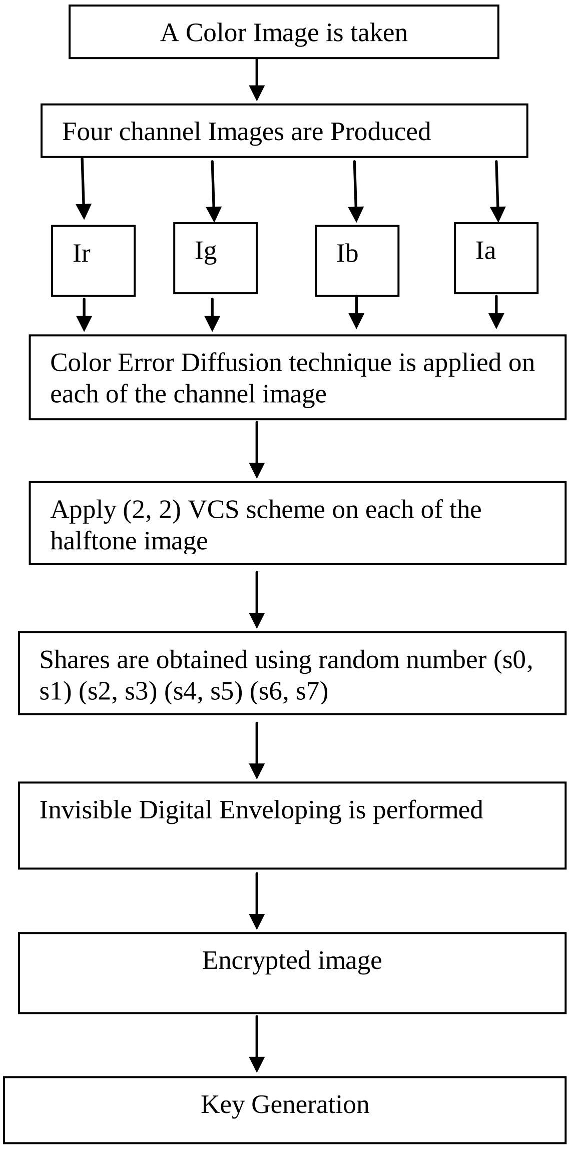
A Color Image is taken
Four channel Images are Produced
Ir
Ig
Ib
Ia
Color Error Diffusion technique is applied on each of the channel image
Apply (2, 2) VCS scheme on each of the halftone image
Shares are obtained using random number (s0, s1) (s2, s3) (s4, s5) (s6, s7)
Invisible Digital Enveloping is performed
Encrypted image
Key Generation

Fig 1. Encryption Process.

III. KEY GENERATION

The key generation is important step after the encryption phase because the decryption phase is based on the key. The key contains information about the following attributes [3].

- The number of shares used in the encryption process.
- The envelop images used as the innocent covers for the shares in the encryption phase.

The concept of key sharing is added to enhance the security of the encrypted image. The key has to be sent over the network in secure manner so that it is not accessible to the hacker. One of the appropriate ways to send the key securely is to use RSA algorithm. This way omits the need for a courier to deliver keys to recipients. RSA is an algorithm for public key cryptography that is based on factoring large numbers.

IV. DECRYTION PROCESS

The decryption process is the reverse process of the encryption process. In the decryption process the shares are stacked together and the 2×2 block is sub sampled in such a way that it is converted into a single pixel and the size of the decrypted image is same as the original image. [12]

- Firstly, it involves the retrieval of the key at the receiving side and getting all the information about the number of shares and envelops images.
- Once the key is retrieved, we identify the enveloped images and remove the watermark from the shares .[6]
- The shares are stacked together using XOR operation which produces better quality of image.[2]
- The channel images thus obtained are superimposed to get the original image.[7]

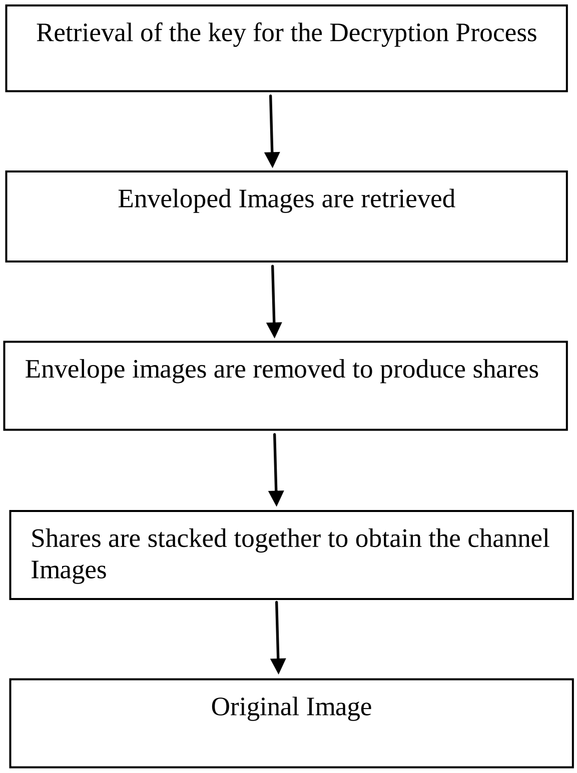
Retrieval of the key for the Decryption Process
Enveloped Images are retrieved
Envelope images are removed to produce shares
Shares are stacked together to obtain the channel Images
Original Image

Fig 2. Decryption Process

V. ANALYSIS OF THE PROPOSED APPROACH

With the addition of the digital enveloping, the security of the image sharing process has enhanced and hence the shares can be sent through same network channel or different channels. The use of Random number makes the encryption process easy. Table I. represents the computational value for decrypted images for Picture Quality evaluation using different dithering techniques (see Table I). The parameters such as Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Normalized Cross correlation (NC) are calculated between original color image and decrypted color image using following equations [11].

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 10, April 2013

Figure 4 shows the comparison of the PSNR value through a line graph. Figure 5 shows the comparison of the MSE values of the secret image. Figure 6 shows comparison of the normalized correlation of the original image using a line graph

MEAN SQUARE ERROR (MSE): The MSE is defined as the difference between the pixel value of the decrypted image and the original image.[7]

$$\text{MSE}=\frac{\sum_{I=1}^{n}\sum_{j=1}^{m}(I-\text{I}')^{2}}{3\text{MN}}$$

Where M and N is the width and height of the image. I is the pixel value of the original image and I' is the pixel value of the decrypted image.

PEAK SIGNAL TO NOISE RATIO (PSNR): It is the ratio between the maximum possible power of a signal and the power of corrupting noise. PSNR is usually expressed [7]

$$\text{PSNR} = \log\,(2^{n}\text{-}1) / \text{MSE}$$

Where n is the number of shares and MSE is the Mean Square Error.

NORMALISED CORRELATION (NC): It is defined as the measure of the similarity representation between the original image and decrypted image. [5]

$$\text{NC}=\frac{\text{I} \times \text{I}'}{\text{I}^{2}}$$

I is the pixel value of the original image and I' is the pixel value of the decrypted image.

TABLE I.

Picture quality evaluation	Floyd and Steinberg dithering	Adaptive order dithering	Color error diffusion using XOR
PSNR	24	25.25	27.17
MSE	180.90	190	125
NC	.26	.28	.50

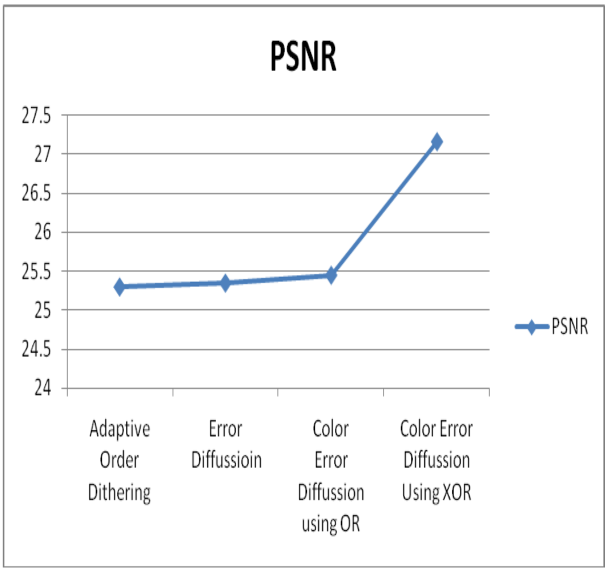

Fig 3. Comparison of Peak signal to noise ratio (PSNR) values

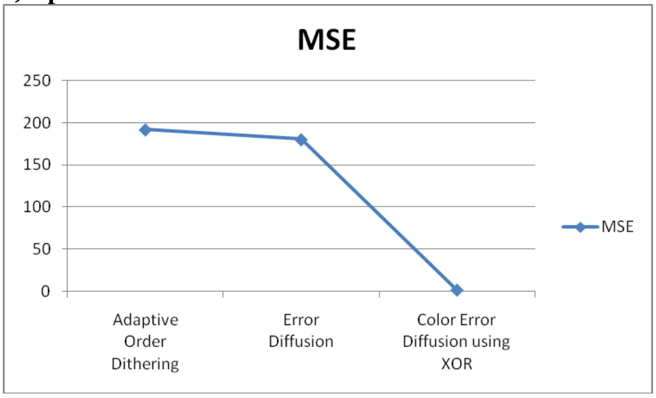

Fig 4 . Comparison of Mean Square Error (MSE) values

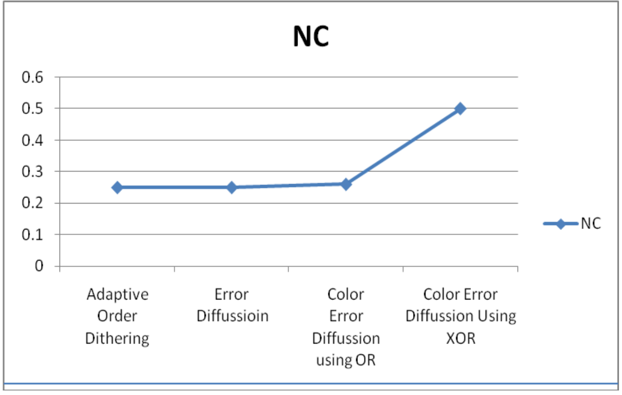

Fig 5. Comparison of Normalized Correlation (NC) values

VI. CONCLUSION AND FUTURE WORK

In this paper, the assumption is that the original image is produced from the three channel images R, G, B. Hence the quality of the original image depends on the quality of the channel images. Here, a Visual Cryptography scheme is proposed in which the quality of the decrypted image is improved as Color Error diffusion technique is used. To add more security to the secret sharing of the image Invisible Digital Watermarking is used which protects the secret image from the hacker. For the decryption process a key is used which includes the Number of share required to decrypt the secret image and the envelop images which are used in the encryption process. The key is sent through the network using RSA algorithm which is a secure method of sending key over the network.

Further, work can be done to improve the secure sharing of the key over the network. There is scope to automate the process of encryption for saving time and improve the quality of the shares.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptology-Eurocrypt'94, 1995.

[2] P. Ranjan, "Principles of Multimedia", Tata McGraw Hill, 2006.

[3] John F Koegel Buford, Multimedia Systems, Addison Wesley, 2000.

[4] M. Naor, A. Shamir, Visual cryptography, Advances in Cryptology, Euro crypt 94, Lecture Notes in Computer Science, Vol. 950, pp. 1-12, 1995.

[5] Naskar P., Chaudhuri A, Chaudhuri Atal, Image Secret Sharing using a Novel Secret Sharing Technique with Steganography, IEEE CASCOM, Jadavpur University, 2010.

[6] Hartung F., Kuttter M., "Multimedia Watermarking Techniques", IEEE, 1999.

[7] C.N. Yang, C.S. Laih, New colored visual secret sharing Scheme, Design, codes and cryptography, vol. 20, pp.325-335, 2000.

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

[9] H. Arafat Ali, Qualitative Spatial Image Data Hiding for Secure Data Transmission, ICGST, GVIP Journal, Volume 7, Issue 2, August,pp-35-43 2007.

[10] H. Koga, H. Yamamoto, Proposal of a lattice based visual secret sharing scheme for color and gray-scale images, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 1998.

[11] R. Floyd and L. Steinberg, An adaptive algorithm for spatial gray scale, Proceedings of the S.I.D. 17, 2(Second Quarter), 75-77, 1976.

[12] G. Atenies, C. Blundo, A.De Santis, D.R. Stinson, Visual Cryptography for general access structures, Information computation, 129, pp.86-106.