International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.4, No.8, August 2015 DOI:10.15693/ijaist/2015.v4i8.52-55

Image Transfer Using Visual Cryptography and Symmetric Cryptography Method

Prasanna Kumar H.R[#1]
#Research Scholar
Department of Computer Science and Engineering
NMAM Institute of Technology
Karnataka, India, 574110

Niranjan N Chiplunkar[*2]
**Professor*
Department of Computer Science and Engineering
NMAM Institute of Technology
Karnataka, India, 574110

Abstract- **Cryptography is a technique used to keep the message secret. Now a day's one of the major challenge is transfer of data securely through the secure communication channel. Symmetric cryptography and Asymmetric cryptography are the two major types of cryptographic algorithms are used to encrypt the secret message, so that the receiver can decrypt it using suitable cryptographic algorithm. Visual cryptography is a technique, in which the secret image is initially partitioned into different meaningful or meaningless shares. Only after combining the required number of shares using some particular method, the receiver can obtain original image. Each individual shares does not disclose any information about the secret. To transfer the secret, which is in the form of image, the visual cryptography technique is more suitable. Different algorithms already proposed in visual cryptography by considering the security level. To enhance the security level multi layer security approach is suitable. Instead of using only Symmetric or Asymmetric methods, Visual cryptography technique is also considered along with these two techniques. The proposed method increases the level of security, so that the intruders cannot get the secret image. In this paper, a visual secret sharing scheme is used so that the secret image can hide into share images with pixel expansion. An extra confidential image is embedded in the share images. Share images are encrypted using DES algorithm. Extra confidential image is also used for check the validity of reconstructed secret image. At the receiver side, receiver has to decrypt two shares and stack them to get secret image.**

Index terms -Floyd-Steinberg Dithering, Visual Cryptography, DES Algorithm.

I. INTRODUCTION

In Cryptography, original plain text is converted into coded message called cipher text. The technique used to convert plain text into cipher text is called encryption. The receiver gets the original plain text message from cipher text using decryption technique. The encryption and decryption can perform by the use of secret key.In symmetric method,single key is used for both encryption and decryption. In asymmetric method two keys are used, one for encryption and one for decryption. In asymmetric method one key is made as public and the other is kept as secret. In stream cipher, single unit of data is converted into cipher text at a time. In block cipher a block of data is converted into cipher text at a time. The secret key used is independent of plain text. For different secret key, the encryption algorithm produces different cipher text for the same plain text. DES, AES are examples for Symmetric algorithms, while RSA is asymmetric algorithm.

Visual cryptography which is proposed by Naor and Shamir [1] in 1995. The secret image is divided into different shares and individual shares do not reveal any information about the secret. Different methods are proposed in Visual cryptography. In (2, 2) method, the secret image is divided into two shares and both the shares are required to get the original image. In (2, n) method, the secret image is divided in to n number of shares and any two shares are enough to obtain the original image. In (k, n) method, the secret image is divided into n number of shares and any k shares are used to get back the original image. In this method any k-1 shares does not give any hint about the secret.

Existing System: Der-Chyuan Lou et al [2] proposed a method, in which additional confidential image is embedded in share images. Secret image is also hidden in share images. Extra confidential image can get by keeping the first share constant and the other share is shifted for some units. In [3], author proposed Visual cryptography method for hiding confidential data. In [4], authors proposed a method in which shifting coefficient technique is used.

II. PROPOSED SYSTEM

In proposed system Floyds-Steinberg Dithering technique is used for half toning. In this method, extra confidential image is embeds into two meaningless share images. These share images are encrypted using symmetric algorithm DES. The two shares are sent to the receiver. The share images are first decrypted and stack both the image to get the secret image, at receiver side. By keeping first share image constantly and by shifting the second share image, extra confidential image is revealed. Fig.1 and Fig.2 shows the embedding and Extraction Phase of the proposed system.

In embedding phase, two images are taken as input. One secret image and the other one is extra confidential image. Apply Floyd-Steinberg algorithm to get the half toned images. For the half toned images, Visual Cryptography technique is applied to get two shares. Apply the symmetric algorithm DES separately for two shares and send these encrypted shares to the receiver.

At the receiver end, decrypt two shares using DES algorithm to get two shares. To get the secret image, stack two share images. Extra confidential image can get by using shifting coefficient technique. Extra confidential image is used for authentication purpose.

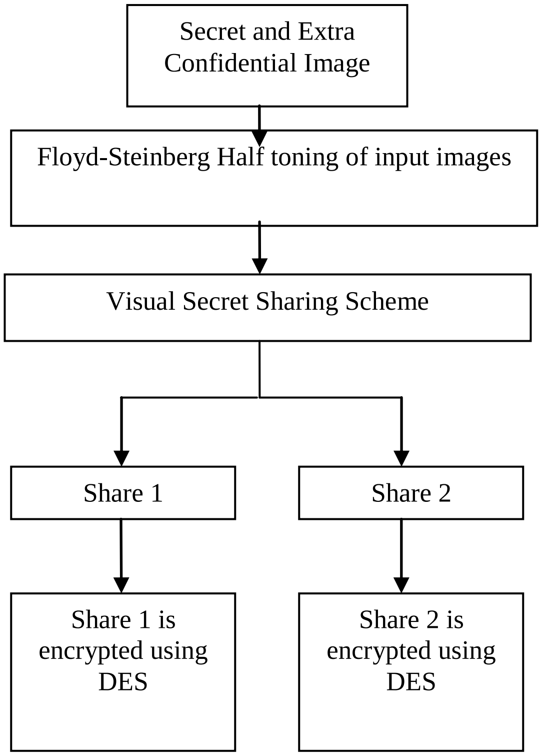

Secret and Extra Confidential Image
Floyd-Steinberg Half toning of input images
Visual Secret Sharing Scheme
Share 1
Share 2
Share 1 is encrypted using DES
Share 2 is encrypted using DES

Fig 1: Embedding Phase

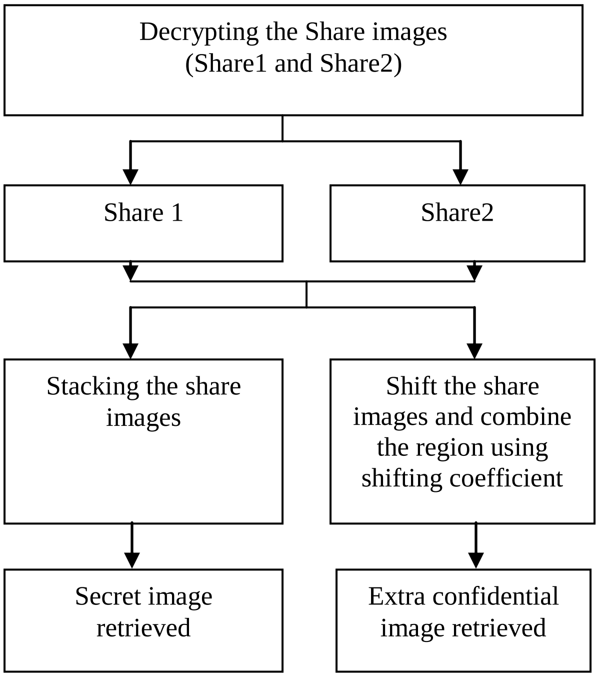

Decrypting the Share images (Share1 and Share2)
Share 1
Share2
Stacking the share images
Shift the share images and combine the region using shifting coefficient
Secret image retrieved
Extra confidential image retrieved

Fig 2:Extracting Phase

A. Floyds-Steinberg Dithering

Digital half toning represents the variety of grayscale with the density of black pixels. The denser of black pixels in a region represents lower degree of grayscale. On the contrary, the sparser of black pixels in a region represents higher degree of grayscale. The Floyd–Steinberg dithering process can be described by the following equations:

$$u_{ij} = x_{ij} + \sum(h_{kl} \times e_{i-k,j-l})$$

$$Q(u_{ij}) = \begin{cases} 255\ (white - pixel - color),\ uij \geq 128 \\ 0\ (black - pixel - color),\ uij < 128 \end{cases}$$

$$e_{ij} = \begin{cases} uij - 255,\ uij \geq 128 \\ uij,\ uij < 128 \end{cases}$$

Where$e_{i,j}$ is the quantified error at location (i, j), $Q_{(ui,j)}$ is used to determine a pixel value to be 0 or 255, $u_{i,j}$ is a state variable, and h is the error diffusion kernel.

For example, Fig. 4a is the input grayscale image. The value of the first pixel is 159, so we set its halftone value to be 255. Then we compute the error 159 - 255 = -96 and distribute the error to its neighbourhood.

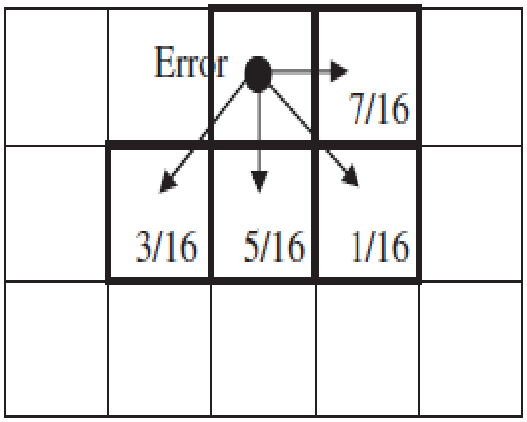
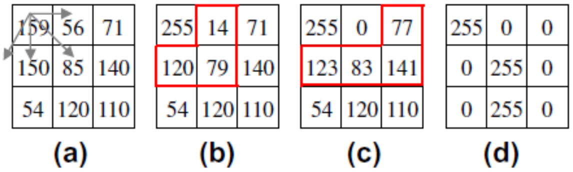


Fig. 3.Floyd–Steinberg diffusion matrix of distributing the error fractions to four neighbouring pixels.



159	56	71
150	85	140
54	120	110

(a)

255	14	71
120	79	140
54	120	110

(b)

255	0	77
123	83	141
54	120	110

(c)

255	0	0
0	255	0
0	255	0

(d)

Fig. 4. (a) Grayscale image; (b) result after processing the first pixel; (c) result after processing the first two pixels; (d) result after processing all the pixels.

B. DES Algorithm

Data Encryption Standard (DES), adopted in 1977[5] by the National Bureau of Standards, now the National Institute of Standards and Technology (NIST), as Federal Information Processing Standard 46(FIPS PUB 46). The algorithm is designed to encipher and decipher blocks of data consisting of 64-bits under control of a 64-bit key of which 56-bits are randomly generated and used directly by the algorithm. Its output is 64-bit block ciphertext. Decryption takes 64-bit cipher text along with 56-bit key and produces 64-bit output of plaintext. The encryption process takes 16 rounds in which a round function, defined in terms the S-boxes, is applied over various subkeys of 56-bit input key, which are generated according to a well defined scheme. The diagram in Fig. 5 shows the flowchart of Single Round of DES algorithm.

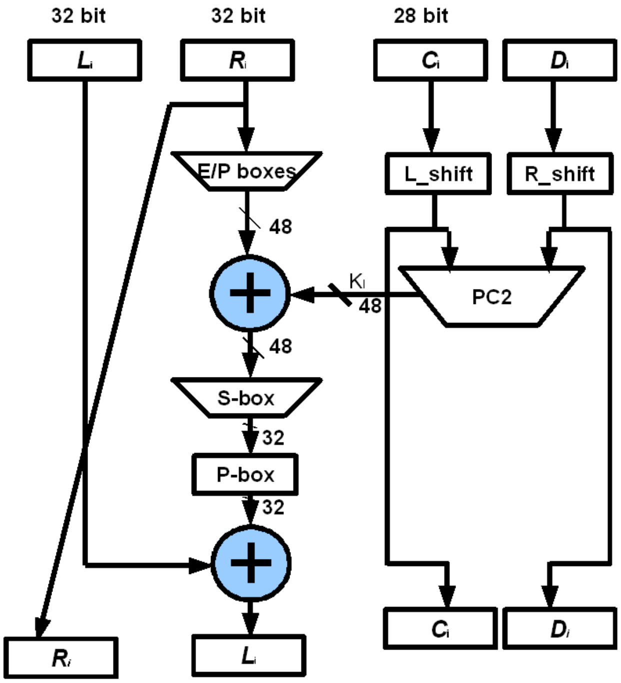


Fig 5: Data Encryption Standard Flowchart

III. RESULTS

In this paper, we used 256x256 gray image namely Lena(Secret Image) and 256×128gray image namely cameraman(Extra Confidential Image).These images are transformed into halftone images by error-diffusiontechnique. These half toned images are used to generate share images and which should be encrypted using DES algorithm. On the extraction Phase ,first we performed DES decryption on share images then on overlap we get secret image and on keeping one share fixed and other shifting we get the extra confidential image.

Fig 6: Secret image

Fig 7: Extra Confidential image

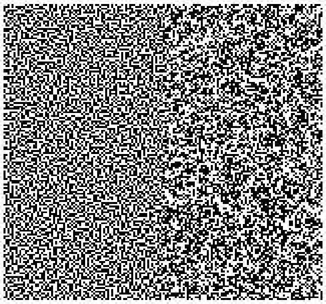


Fig 8 : Share image1

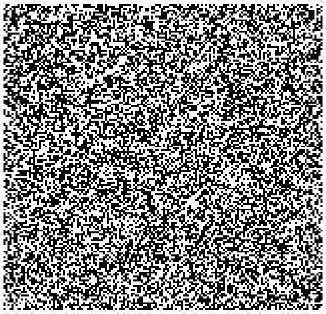


Fig 9: Share image2

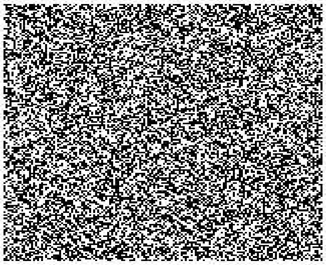


Fig 10: Share1 after DES encryption

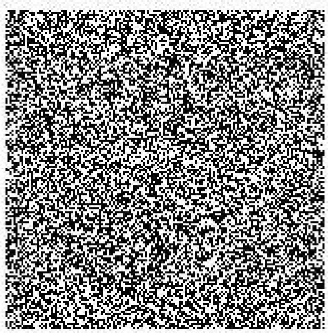


Fig 11: Share2 after DES encryption

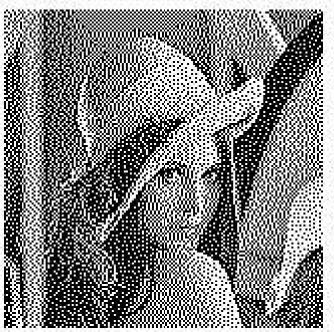


Fig 12: Secret image after decryption

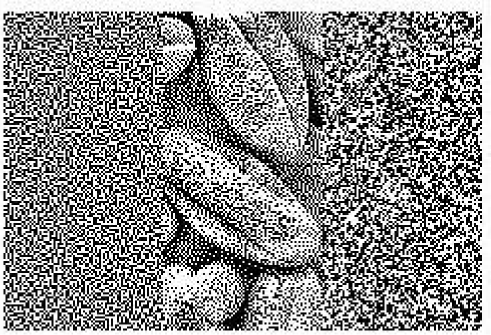


Fig13: Extra Confidential image after decryption

IV. Conclusion

In this paper, we study the effect of DES in image ciphering which provides second layer of protection to visual secret sharing scheme. To transfer the secret image both Symmetric algorithm and Visual cryptography techniques are used. The proposed method increases the security level. Extra confidential image is used to achieve the authentication purpose.

References

[1] M. Naor, A. Shamir, "Visual Cryptography", in Proceedings of Eurocrypt 1994. Lecture notes in Computer Science.1994, Vol.950,pp. 1-12.

[2] Der-Chyuan Lou, Hong-Hao Chen, Hsein-Chu Wu, Chwei-Shyong Tsai, " A Novel authenticable color visual secret sharing scheme using non expanded meaningful shares", Elsevier on displays, Vol.32, pp.118-134,2011

[3] W.P. Fang, J.C. Lin, " Visual Cryptography with extra ability of hiding confidential data", Journal of Electronic Imaging 15 (2) (2006) 0230201-0230207.

[4] John Justin M, Manimurugan S, Alagendran B, " Secure color visual secret sharing scheme using shifting coefficient with no pixel expansion", IJCSIT, Vol.3(2),2012,3793-3800

[5] Stallings W, Cryptography and Network Security, (Prentice Hall, New Jersey, 2003)

Authors Profile

Prasanna Kumar H.R, working as Associate Professor at PESITM, Shimoga, India. He is Persuing his Ph.D in the area of Cryptography. He has 17 years of Teaching experience

Dr. Niranjan N. Chiplunkar currently working as Principal, NMAM Institute of Technology, Nitte, INDIA. His areas of Interest are CAD for VLSI, Image Processing, Network Security, and Wireless and Sensor Networks. He presented more than 60 papers in Conferences and published many papers in National and International Journals. He Authored two text books on VLSI-CAD and Microprocessor. He is a member of professional societies like IEEE, ISTE, IE and CSI. He has visited countries like USA, Japan, China, Thailand, Sri Lanka, Malaysia, and UAE on different official assignment.