Methods for Providing High Security to Transfer Secret Image

Prasanna Kumar H.R, Niranjan N Chiplunkar

Abstract—Privacy and security of data being transmitted has become the major issue. Now a day's one of the major challenge is transfer of data securely through the secure communication channel. Many images transmitted via Internet containing secret information but not secure. In Visual cryptography technique, the secret image is initially partitioned into different shares. The shares may be meaningful or meaningless. The receiver can get the original image only after combining specified number of shares. Here each individual image does not give 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. Multi layer security approach is used to increase the security level. Along with Symmetric and asymmetric algorithm, Visual Cryptography method is also considered for more security. 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. In another method, the secret image is encrypted using Arnold's transformation in the first step. Two shares are created using basic (2, 2) method in the second step. In the third level of security, shares are embedded in two host images. On the receiver end, shares are extracted from camouflage image and then stacked to get the encrypted image. Encrypted image is decrypted using Arnold's Inverse Transformation These two proposed methods definitely increase the level of security.

Index Terms—**Fl**oyd-Steinberg Dithering, Visual Cryptography, DES Algorithm**, S**ecret sharing; Arnold Transformation.

1 Introduction

To keep the confidential message secret, Cryptography technique is used. In Cryptography, original plain text is converted into coded message called cipher text. Encryption is the process of converting plain text into cipher text. The receiver can get the secret message using decryption technique by the use of 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 was introduced by Naor and Shamir in 1995 [1]. It is a new cryptographic scheme where the cipher text is decoded by the human visual system. Hence, there is no need of any complex cryptographic computation for decryption. The idea is to split a secret image such as text, handwriting, picture, etc… into two random shares (printed on transparencies) which separately reveals no information about the secret image other than the size of the secret image. When shares are stacked together the secret image can be recovered.. 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.

2 Proposed Sytem

i. 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

- *Prasanna Kumar H.R, Reaearch Scholar, Dept. of CS&E NMAMIT, Nitte Karnataka, India, 574110, hrpbhat@gmail.com*
- *Niranjan N Chiplunkar, Professor, NMAM Institute of Technology, Karnataka, India, 574110, niranjanchiplunkar@rediffmail.com.*

separately for two shares and send these encrypted shares to the receiver.

At the receiver end, decrypt 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.

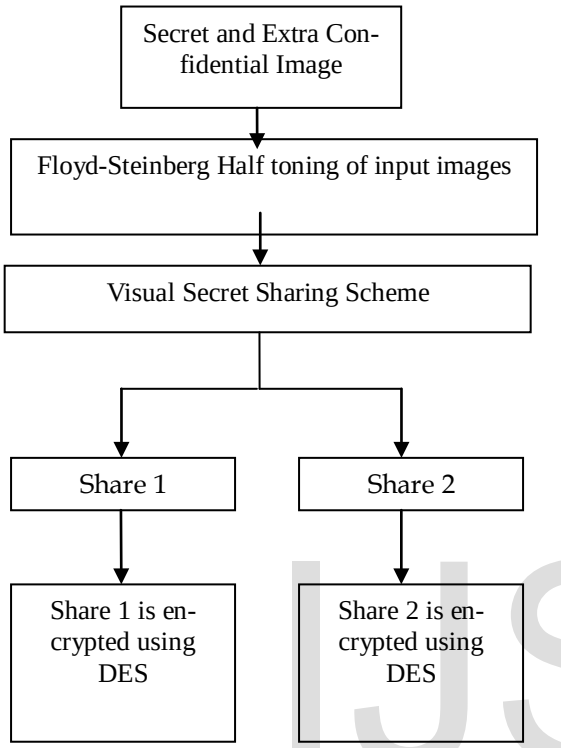

Fig 1: Embedding Phase

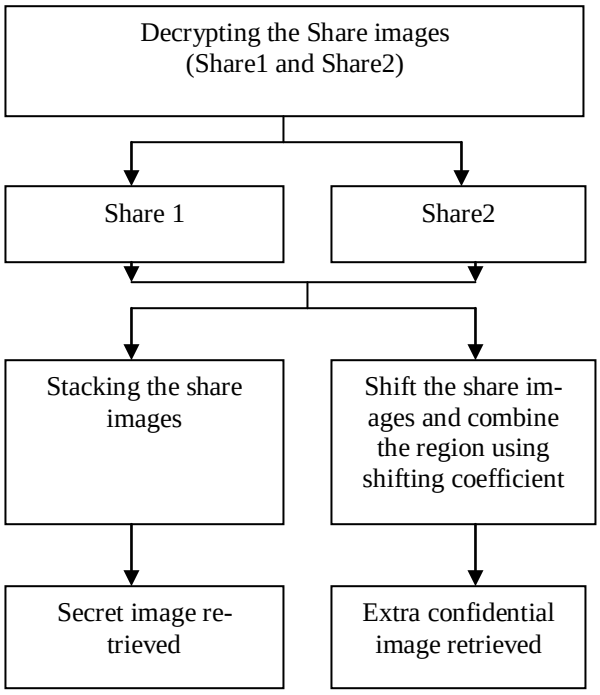

Fig 2: Extracting Phase

A. Floyds-Steinberg Dithering

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

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

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

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

Where ei,j is the quantified error at location (i, j), Q(ui,j) is used to determine a pixel value to be 0 or 255, ui,j is a state variable, and h is the error diffusion kernel.

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 cipher text. 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 sub keys of 56-bit input key, which are generated according to a well defined scheme.

ii. In the second method, the secret image is encrypted using Arnold transformation and the scrambled image is encrypted using visual cryptography. The generated shares are embedded into respective host images so that the attacker cannot suspect the secret image in it. On the receiver end the shares are extracted from camouflage images and are stacked to get the encrypted image. Later the encrypted image is decrypted using inverse Arnold transformation to get the original image.

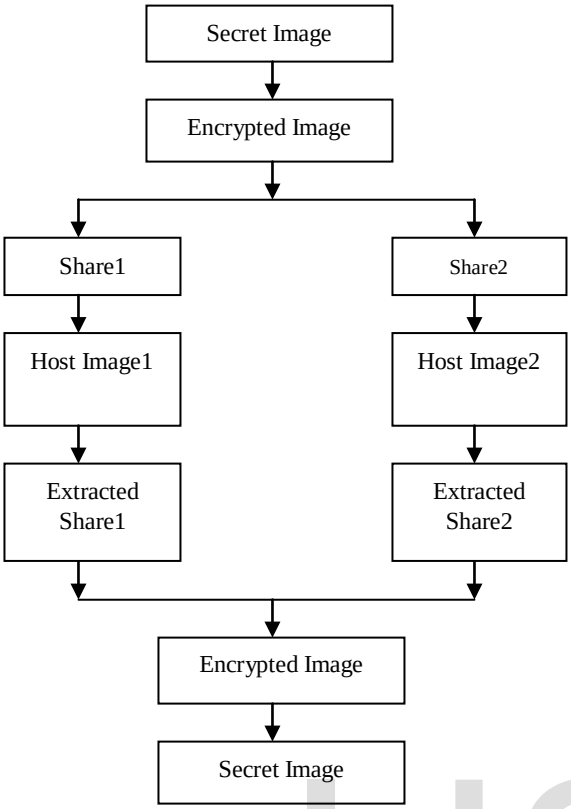

Fig. 3: Flow diagram of proposed method

3 RESULTS

In this paper, we used 256 x 256 gray image namely Lena (Secret Image) and 256×128 gray image namely cameraman (Extra Confidential Image). These images are transformed into halftone images by Error-diffusion technique. 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 overlapping two shares, we get secret image and on keeping one share fixed and other shifting we get the extra confidential image.

Fig 4: Secret image

Fig 5: Extra Confidential image

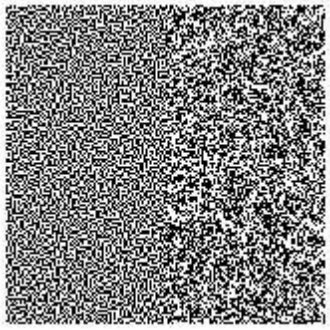

Fig 6 : Share image1

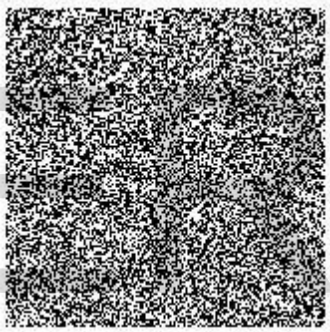

Fig 7: Share image2

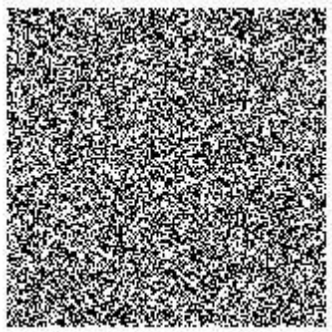

Fig 8: Share1 after DES encryption

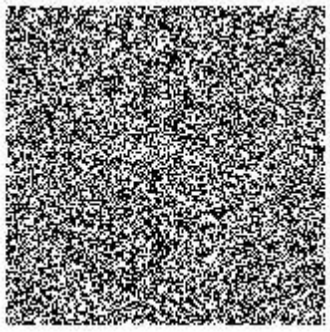

Fig 9: Share2 after DES encryption

Fig 10: Secret image after decryption

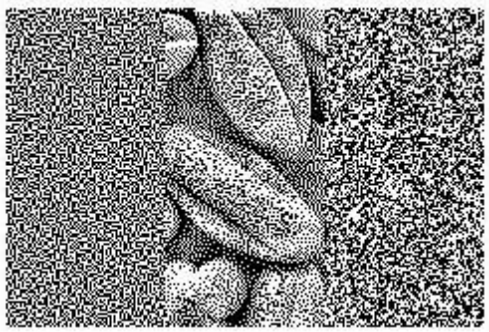

Fig11: Extra Confidential image after decryption

In the second method, A secret image of size 100x100 is encrypted using Arnold transformation technique and the encrypted image is hidden in two cover images. Recovery process is lossless. Shares are stacked to get the encrypted image. Inverse Arnold transform is applied to obtain the secret image.

Fig: 12: Cover image1

Fig:13: Cover image2

Fig: 14: Secret image

Fig:15: Encrypted images

Fig: 16: Reconstructed image

4 Conclusion

In the first method, we studied 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.

In the second method, a technique is used for securely transferring the data image. This method provides a more secure way of image sharing as the image is encrypted using Arnold transformation before hiding into multiple cover images. This scheme also prevents the cheating attacks by embedding the shares onto Host Images.

5 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)

[6] Feng Liu and Chuankun Wu," Embedded Extended Visual Cryptography Schemes", IEEE transactions on information forensics and security, vol. 6, no. 2, June 2011

[7] Mr. Rohith S, Mr. Vinay G "A Novel Two Stage Binary Image Security System Using (2,2) Visual Cryptography Scheme" in proceedings of International Journal Of Computational Engineering Research, ISSN: 2250–3005.

[8] R.Youmaran, A. Adler, A. Miri ,"An Improved Visual Cryptography Scheme For Secret Hiding",IEEE transaction 2006.

[9] B.Padhmavathi, P.Nirmal Kumar, M.A.DoraiRangaswamy, "A Novel Scheme for Mutual Authentication and Cheating Prevention in Visual Cryptography using Image Processing", ACEEE Int. J. on Signal & Image Processing, Vol. 01, No. 03, Dec 2010.

[10] ChittaranjanPradhan, VilakshanSaxena, Ajay Kumar Bisoi, "Imperceptible Watermarking Technique using Arnold's Transform and Cross Chaos Map in DCT Domain", International Journal of Computer Applications, Volume 55– No.15, October 2012

[11] C. Yang and C. Laih., New colored visual secretsharing schemes. Designs, Codes and Cryptography,20:325–335,2000.