International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 16 (2017) pp. 5631-5636
© Research India Publications. http://www.ripublication.com

Strengthen the Security of Confidential Information Using Cryptographic Techniques

Prasanna Kumar H.R[1] and Dr. Niranjan N Chiplunkar[2]

[1]Associate Professor, Department of IS&E, PESITM, NH-206, Sagar Road, Shimoga-577204, Karnataka State, India.

[2]Principal, NMAMIT, Nitte, Udupi Distrct-577110, Karnataka State, India.

[1]Orcid: 0000-0001-9289-220X

Abstract

Secure transmission of confidential information is one of the major challenges. Several cryptographic methods have been proposed by the researchers to provide the security. In the conventional cryptographic method, symmetric or asymmetric algorithms are used to protect the confidential data. Visual cryptography is another method, used mainly for secure transmission of secret images. Applying conventional method or visual cryptographic method alone will not provide required security. We proposed two methods for protecting the confidential data, which uses both conventional method and visual c cryptography technique. In the first method, encrypt the secret image and then apply visual cryptography scheme to create the shares. Shares are then embedded in cover image and send it to the receiver. This method provides three level of security. In the second method, after applying the visual cryptography scheme, Data Encryption Standard is applied separately to two shares and encrypted shares are send to the receiver. This method provides both security and authentication. Along with secret image, one more confidential image is taken as input to provide authentication. The two proposed methods provide high security to transfer confidential image.

INTRODUCTION

Security aspect is the major concern, as the information technology is ruling the world [1]. Two important challenges while transmitting the data are security and reliability. Due to uncontrolled hacking, the images containing the confidential data which are transmitted through internet are not secure [2]. Maintaining the security and privacy of data becoming more important, while transmitting confidential data. Security becomes major and important issue, and the threat of accessing secret information by the unintended recipients has been major problem. The method, which overcomes the threat is cryptography, which is a mathematical technique used to convert plain text into unreadable form. Single key is used for both encryption and decryption in symmetric cipher, while two separate keys are used in asymmetric method of cryptography. The advantage of symmetric ciphers is that it is less complex and executes faster. Asymmetric cryptography is slower than symmetric method, but it is more secure than symmetric method [3]. High computation cost and managing the secret key are the two important limitations of traditional cryptographic method. Therefore to transfer secret image, several methods are proposed by the researchers.

There are mainly two approaches to transfer secret image. The first approach is conventional cryptographic method and it has an encryption algorithm and a key. The major issue of this method is key management. The strength of this method is that the best quality image can be recovered after decryption. In the second approach, secret image is divided into different shares and each individual share, does not reveal any information about the result. The strength of this method is that there is no key management but it has a drawback of degradation in the quality of recovered image.

A. Visual Cryptography

The visual cryptography technique, proposed by Naor and Shamir [4] provide a reliable and secure system for transferring secret images. Original image is divided into number of shares according to the available schemes of visual cryptography, and by overlapping the required number of shares, original confidential image can be revealed. The one of the advantage of visual cryptography system is that, any of the individual shares does not reveal any hint about the secret, as it looks like an image with noise.

In (2, 2) scheme of visual cryptography, secret image is considered as input and two shares are created. Only by overlapping these two shares, secret can be revealed. In (2, n) scheme; only two shares are enough to obtain the secret, out of ‘n’ shares. Similarly there exist (n, n) and (k, n) visual cryptography schemes. In the basic visual cryptography scheme, decryption algorithm is not required, as the human visual system can be able to decrypt the image. Visual cryptography method reduces the computation cost and a person without having the knowledge of cryptography can decrypt the secret. There is degradation in the quality of recovered image in visual cryptography method.

PROPOSED METHODS:

A. Multi level security scheme

In this method, secret image is encrypted using Arnold's cat map transformation technique. In the next step, basic visual cryptography method is applied to create the shares. Instead of sending the shares to receiver, one more level of security is applied, by embedding two shares into two cover images. At the receiver side, shares are extracted from host images and using decryption process of (2, 2) visual cryptography method, two shares are stacked to obtain the encrypted form of the original confidential image. In the next step, decrypt the image to get original confidential image. In this method, if the attacker gets all the shares, he cannot be able to get the secret. This method provides high security for the confidential image but there is some degradation in the quality of the recovered image.

B. Providing high security and Authentication:

The main drawback of basic visual cryptography method is that if any attacker gets all the shares, he can obtain the secret by just overlapping these shares. To avoid this, we proposed a method, which combines both visual cryptography scheme and conventional cryptography method.

In the proposed method, two images are considered as input. Both the images are half toned using Floyd's algorithm. In the next step, basic visual cryptography method is applied to obtain the shares. The two shares are encrypted separately using DES algorithm, which is one of the symmetric cryptographic methods. In this method, shifting coefficient value is considered as a secret key. At the receiver end, share image is decrypted using DES algorithm [5] and using basic (2, 2) visual cryptography scheme, secret image is obtained. The secret image is obtained by stacking the two shares. The confidential image is obtained by stacking the first share with the shifted second share. The shifting coefficient value is required to get the confidential image. Confidential image is considered to verify the authenticity of the sender. The proposed method provides both security and authentication.

METHODOLOGY

A. Algorithm for Multi level security scheme:

The encryption process consists of following steps:

Step 1: Input confidential image as an input

Step 2: Encrypt the input image using Arnold's Transformation technique

Step 3: Visual Cryptography method is applied to scrambled image, to obtain two shares

Step 4: Embed two shares in separate host images

Step 5: Two host images containing the encrypted shares are send to the receiver

The following steps are used during decryption process:

Step 1: Extract two shares from the host images, where extracted shares are in encrypted form

Step 2: Two shares are stacked using visual cryptography method to obtain encrypted image

Step 3: Apply Inverse Arnold's transformation technique to obtain original confidential image.

B. Algorithm for providing high security and authentication technique:

The various steps involved in encryption process:

Step 1: Secret image and confidential image are the input for the method

Step 2: Half tone both the images using Floyd's Steinberg method. Obtain the shifting coefficient value during this step and consider the shifting coefficient value as a key.

Step 3: Apply visual cryptography method to create two shares

Step 4: Each individual shares are encrypted using DES algorithm

Step 4: Encrypted shares are send to the receiver

The various steps involved during decryption process:

Step 1: Decrypt two share images using DES algorithm

Step 2: Stack the two shares to get encrypted image, using basic visual cryptography technique.

Step 3: Shift the second share using shifting coefficient value, used as a key

Step 4: Confidential image can be obtained by stacking first share and shifted second share.

RESULT AND DISCUSSION

In the multi level security scheme, the cover images and a secret image [6] of size 100x100 are taken as an input as shown in figure 1, and converted to grayscale as shown in figure 2. A secret image is encoded using modified Arnold transformation method as shown in figure 3. The encrypted image is hidden using two cover images, as shown in the figure 4 and figure 5. Encrypted images are obtained by stacking the shares and Inverse Arnold transform is applied to recover the secret image as shown in figure 6.

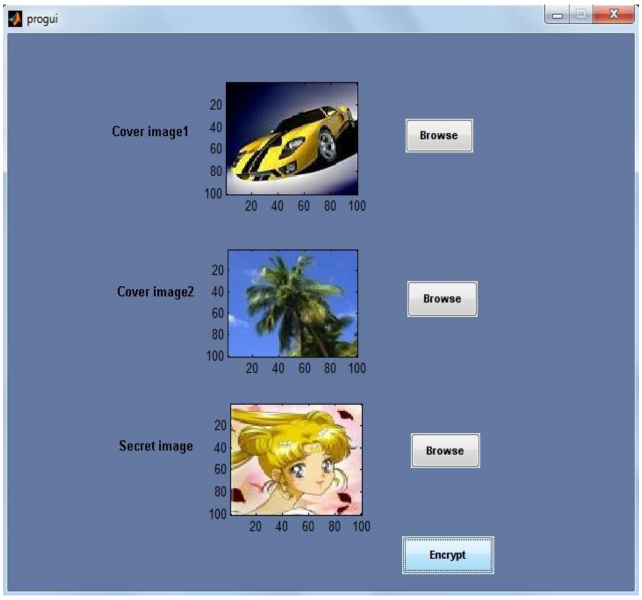

Figure 1: Two cover images and secret image

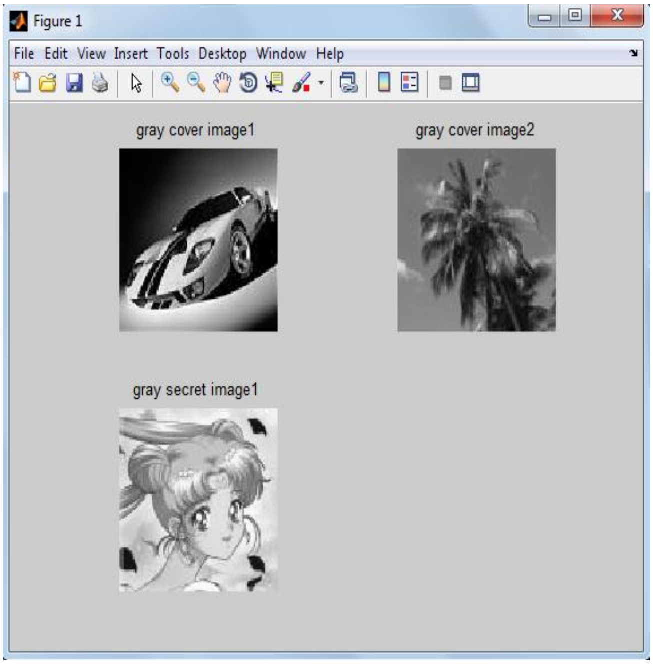

Figure 2: Grayscale images

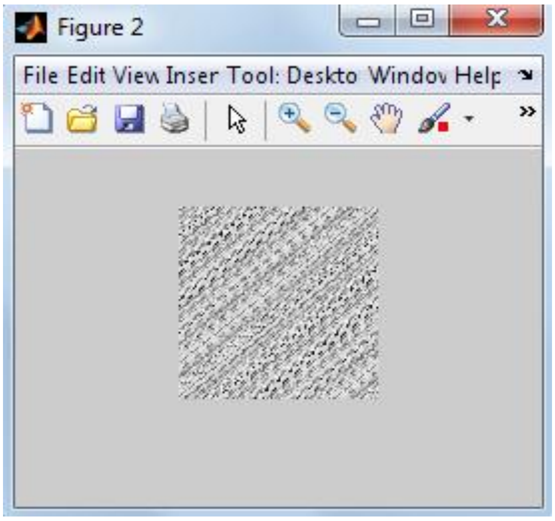

Figure 3: Encrypted secret image

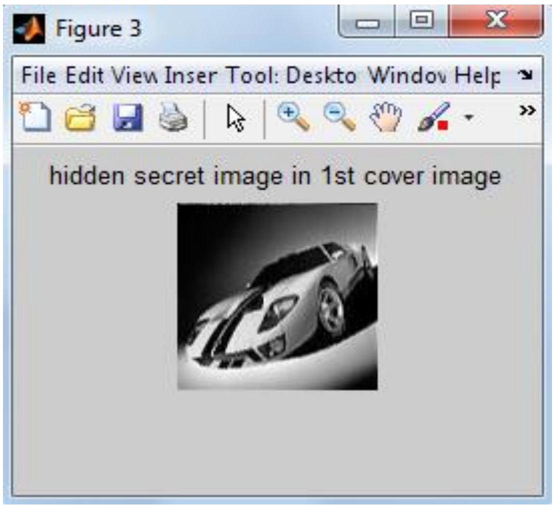
Figure 3
File Edit View Inser Tool: Deskto Windov Help
hidden secret image in 1st cover image

Figure 4: First share hidden in cover image

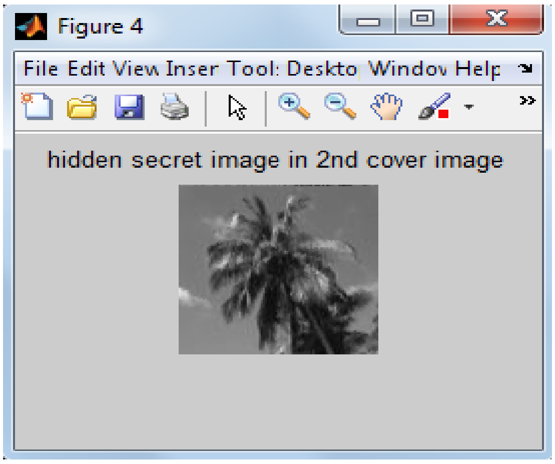
Figure 4
File Edit View Inser Tool: Deskto Windov Help
hidden secret image in 2nd cover image

Figure 5: Second share hidden in cover image

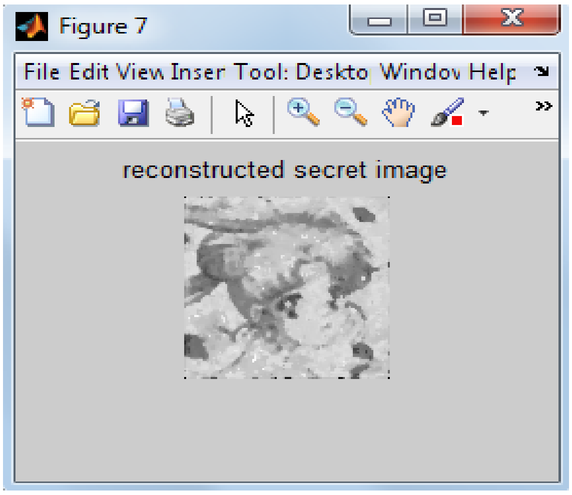
Figure 7
File Edit View Inser Tool: Deskto Windov Help
reconstructed secret image

Figure 6: Recovered image

PSNR Calculation

Peak Signal-to-Noise Ratio is used as a quality measurment between the compressed and original image. The higher the value of PSNR indicates better quality of the reconstructed or compressed image. In the proposed method, PSNR is used to measure the quality [7] of the recovered secret image and camouflage image.

A PSNR of 22.46dB and 32.54dB are obtained for two camouflage image respectively.

Correlation Coefficient

The quality of the encryption technique in crypto system is measured using correlation coefficient. Any image crypto system is called good, if encryption algorithm must be powerful to hide all attributes of a secret and the encrypted image must be highly uncorrelated and totally random. If the original plaintext image is completely different from the encrypted image then the corresponding correlation coeffcient [8] is very low or which is close to zero. On the other hand, if the correlation coefficient is one then two images are in perfect correlation and the two images are identical. Encryption process completely fails [9] if the correlation coefficient is one because the secret image is same as encrypted image.

According to the proposed system the correlation coefficients between the encrypted and original image is -0.015. The result shows that encrypted image is totally random and highly uncorrelated.

In the second method, the proposed system is implemented and evaluated to show the efficiency of the method. Based on the parameters like visual testing, value of the correlation coefficient and number of pixel change rate performance of the method is evaluated.

Figure 7 shows 160 X 160 gray secret image and figure 8 shows 160 X 80 confidential image. These images are transformed into halftone images by Floyds Steinberg's dithering technique. Shares are created from these halftone images and later apply DES algorithm for the shares. At the receiver side, first apply DES decryption then overlap two shares to get secret image. Confidential image can be obtained by keeping one share constant and other share by shifting. Figure 9 and Figure 10 are the share images after DES encryption. Figure 11 and Figure 12 are the retrieved Secret and confidential Image.

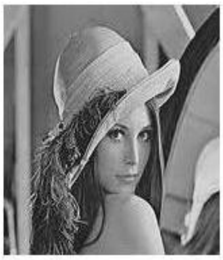

Figure 7: Input secret image

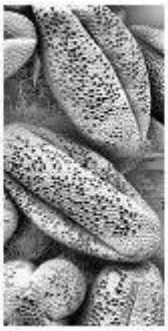

Figure 8: Input confidential image

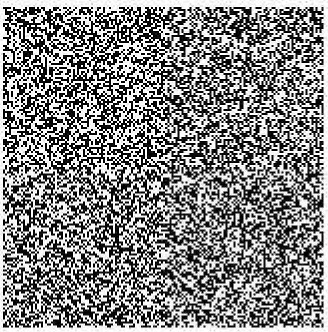

Figure 9: Share 1 after DES encryption

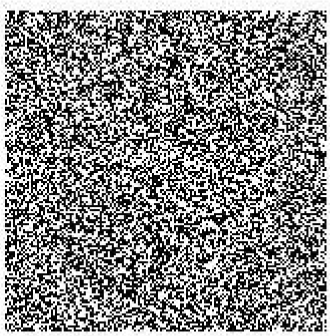

Figure 10: Share 2 after DES encryption

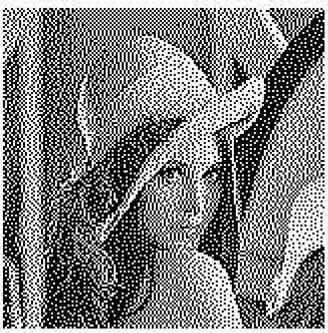

Figure 11: Recovered secret image

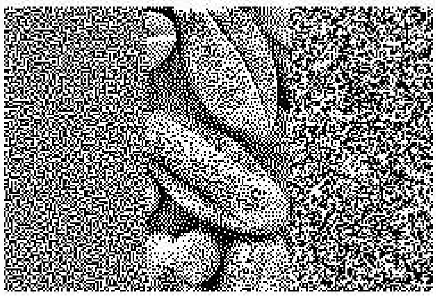

Figure 12: Recovered confidential image

Correlation Coefficient of cipher and plain images:

According the proposed system the horizontal correlation coefficients [10] is 0.8564 for Secret image (Lena) and -0.0322 for DES encrypted image. In case of Secret image, the estimation of horizontal correlation coefficient is 0.8564 which is close to 1 (maximum correlation) though for DES encrypted image the horizontal connection is - 0.0322, which implies that scrambled image is uncorrelated.

Number of Pixel Change Rate (NPCR):

In some cryptographic algorithm, if one bit changes in plaintext cause the cipher text change in an unpredictable manner. This desirable property of cryptographic algorithm is called diffusion. A diffusion characteristic of an image encryption shows that output pixels of the cipher text image depends on input pixels of the plaintext image in a complex way. Small change in plaintext cause the significant change in corresponding cipher text is the desirable property of cryptographic algorithm. To check this property, NPCR measure is used and it calculates the percentage by considering the ratio between numbers of different pixels to the total number of pixels in the image. For Lena image, the value obtained is 49.40 as NPCR.

CONCLUSION:

In the first proposed scheme, secret image is encoded using Arnold's transformation method before hiding the secret into cover images, to provide more security for confidential image. The proposed scheme prevents the cheating attacks because the shares are embedded into host images. Since there is a high correlation between camouflage image and original host image, camouflage images look less susceptible of containing secret information.

In the second proposed method, visual secret sharing method [11] is applied to create two meaningless share images without pixel expansion. In this approach, confidential data is embedded for authentication. To encrypt and decrypt the share images, shifting coefficient is used as a key. Extra confidential image cannot be recovered without shifting coefficient key. The proposed system provides high security and provide authentication. By encrypting the share image using DES it provides second layer of security to the secret image. The two proposed method, provides high security for the transmission of confidential image.

REFERENCES:

[1] Neelima Guntupalli, P.D. Ratna Raju, Suresh Cheekaty, "An Introduction to Different Types of Visual Cryptography Schemes", International Journal of Science and Advanced Technology, Vol. 1, No. 7, September 2011

[2] John Justin M, Manimurugan S, Alagendran B, " Secure Color Visual Secret Sharing Scheme Using Shifting Coefficient with No Pixel Expansion", International Journal of Computer Science and Information Technologies, Vol. 3(2), pp. 3793-3800, 2012

[3] J. Ramya, B. Parvathavarthini, "An Extensive review on Visual Cryptography Schemes", Proceedings of the IEEE International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), pp. 223-228, 2014

[4] Moni Naor, Adi Shamir, "Visual cryptography",

Advances in Cryptography, Eurocrypt'94, Lecture notes in Computer Science, Springer-Verlag, Vol. 950, pp. 1-12, 1995

[5] William Stallings, "Cryptography and Network Security", 5th Edition, Prentice Hall

[6] J. Ida Christy and V. Seenivasagam, "Feed Forward Networks in Color Extended Visual Cryptography to Generate Meaningful Shares", International Journal of Security and its Applications, Volume 9, No.1, pp. 165-178, 2015

[7] Bin Yan, Ya-Fei Wang, Ling-Yun Song, Hong-Mei Yang " Size invariant extended visual cryptography with embedded watermark based on error diffusion", Multimedia Tools and Applications, Volume 75, Issue 18, pp. 11157-11180, September 2016

[8] Prabir Kr. Naskar, AtalChaudhuri, "A secure Symmetric Image Encryption based on Bit wise Operation", International Journal of Image Graphics and Signal Processing, Volume 6, Issue 2, pp. 30-38, 2014

[9] Song, Xian-Hua, shen Wang, Ahmed A. Abd El-Latif and Xia-Mu Niu, "Quantum image encryption based on restricted geometric and color transformations", Quantum information Processing, 2014

[10] Song, Xian-Hua, shen Wang, Ahmed A. Abd El-Latif and Xia-Mu Niu, "Quantum image encryption based on restricted geometric and color transformations", Quantum information Processing, 2014

[11] Der-Chyuan Lou, Hong-HaoChen, Hsien-Chu Wu, Chwei-Shyong Tsai, "A novel authenticatable color visual secret sharing scheme using non-expanded meaningful shares", Displays, Volume 32, Issue 3, pp. 118-134, July 2011