Multi Level Encryption Scheme for Transferring Secret image

Prasanna Kumar H.R
Research Scholar,
Department of Computer Science and Engineering
NMAMIT, Nitte
Karnataka, INDIA
hrpbhat@gmail.com

Niranjan N. Chiplunkar
Professor,
Department of Computer Science and Engineering
NMAMIT, Nitte
Karnataka, INDIA
niranjanchiplunkar@rediffmail.com

Abstract— As the rapid development of Internet Technology, Security and Privacy of data being transmitted has become the major issue. Transfer of data securely and reliably has become one of the challenges. Security issues should be considering because hackers may utilize weak link over communication network to steal information. Cryptography is the technique used to keep the message secure. Many images transmitted via Internet containing secret information but not secure. Encryption technique which prevents unauthorized access of data. Visual Cryptography technique introduced by Naor and Shamir, in which secret image is divided into number of shares. No information about secret image is revealed from individual share. Decryption can be done by overlaying one share above the other share. In this paper the idea is to increase the security level as the basic model of Visual Cryptography is not an efficient tool to hide the information. The secret image is encrypted using Arnold's Transformation technique in the first level. In the second level create two shares from encrypted image using basic (2, 2) Visual Cryptography technique. To increase the security level, instead of sending these shares to receiver, third level security is adopted. In third level security, shares are embedded in two host images using Chang and Yu's method. Generated shares are embedded into respective host images so that the attacker cannot suspect the secret image in it. On the receiver end, shares are extracted from camouflage image and then stacked to get the encrypted image. Encrypted image is decrypted using Inverse Arnold Transformation.

Keywords-*Visual Cryptography, Arnolds Transformation, Secret Sharing,*

*****

I. Introduction

Naor and Shamir [1] introduced Visual Cryptography method. It is a cryptographic method in which secret image is divided into different meaningless share images. Decryption can be done by overlapping share images. No computation is required at receiver end in basic Visual Cryptography method. Decryption can be done by Human Visual system. The secret image can be recovered by stacking two shares. In (2, 2) scheme the secret message is hidden in two shares and both are needed for a successful decryption of the message as shown in figure 1. In (2, n) scheme the secret image is encrypted into n shares and recovers the secret image when two or more shares are overlaid. In (n, n) scheme the secret image is encrypted into n shares and all the n shares are required to recover the secret image. If any n-1 shares will not produce any hint about the secret image. In (k, n) scheme the secret message is encoded into n shares but only *k* shares are required for decryption where *k*<=*n*. If *k*-1 shares are stacked, no information about the secret message is obtained. Naor and Shamir applied the idea of visual cryptography only on black and white images.

Verheul and Tilborg introduced a scheme that can be applied on colored images. Later more advanced visual cryptography scheme is introduced where a color image is hidden into multiple meaningful host images. Hwang proposed a new visual cryptography scheme which improved the visual effect of the shares. Hwang's scheme is very useful when we need to manage a lot of transparencies; but it can only be used in black and white images.

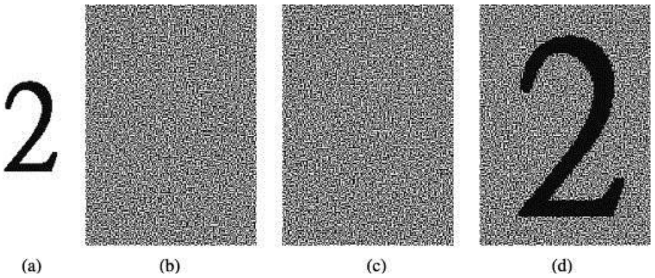

Fig -1: (2, 2) VCS

A. Existing System:

In 2002 Chang et al. [2] proposed a new secret color image sharing scheme based on modified Visual Cryptography. This approach uses meaningful shares (cover images) to hide the colored secret image that results in camouflage images. In the recovery process shares are extracted from the camouflage images and these shares are stacked together to recover the secret image. The recovery process is lossless.

B. Proposed System:

In the existing system the secret image will be revealed if the attackers get all the shares. In this proposed system the idea is to increase the levels of security as the basic model of Visual Cryptography is not an efficient tool to hide the information. In this system, we utilize Arnold's cat matrix to enhance the security of this scheme by means of pixel scrambling. The secret image is encrypted using modified 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.

II. RELATED TOPICS

A. Arnold's Transformation

Arnold transform is also known as Arnold's cat map, is a kind of image scrambling method. This transformation changes pixel position of the image from (x, y) to (x', y') without changing the pixel value. The original image repeats itself after certain number of iteration. The number of iterations taken is known as the Arnold's period which depends on the image size. The generalized form of Arnold's cat map can be given by the transformation,

$\Gamma : T2 \rightarrow T2$ such that:

$$\begin{pmatrix}x'\\y'\end{pmatrix}=\begin{pmatrix}2&1\\1&1\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}(mod\ N)$$

Where x, y ϵ {0, 1, 2 … N −1} and N is the size of a digital image.

B. Basic Visual Cryptography Scheme

Naor and Shamir proposed scheme, where binary image is encoded into two shares, share1 and share2. In the Figure 2, each pixel is broken into two sub pixels. Let B indicate black pixel and W indicate white pixel. When we stack both the shares we get following combinations**.** For black pixel BW+WB=BB or WB+BW=BB and for white pixel BW+BW=BW or WB+WB=WB. Similarly second approach where each pixel is broken into four sub pixels. There are six different encryption rules both white as well as black pixel. By using any one of the rule, encryption is done by splitting the white (or black) pixel into two shares. Decryption can be done by simply overlapping of two shares, which retrieve the secret image as a result.

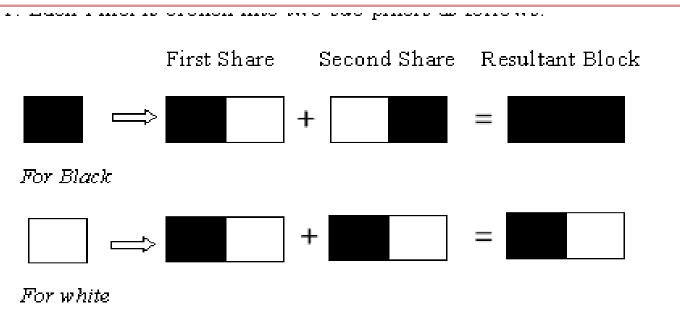

Fig 2-Basic (2,2) scheme

III. STRUCTURE OF THE PROPOSED SCHEME

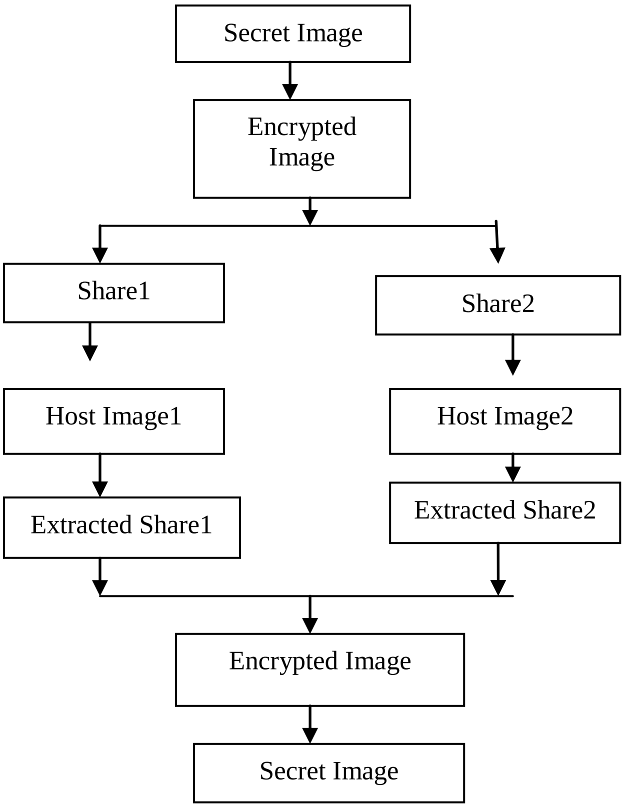

Fig -3. Proposed system

In this proposed system we take three images of same size, one secret image and two cover images. On the sender side secret image is encrypted using modified 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. The encrypted image is decrypted using inverse Arnold transformation to get the original image. Fig 3 shows the structure of proposed scheme.

IV. RESULTS

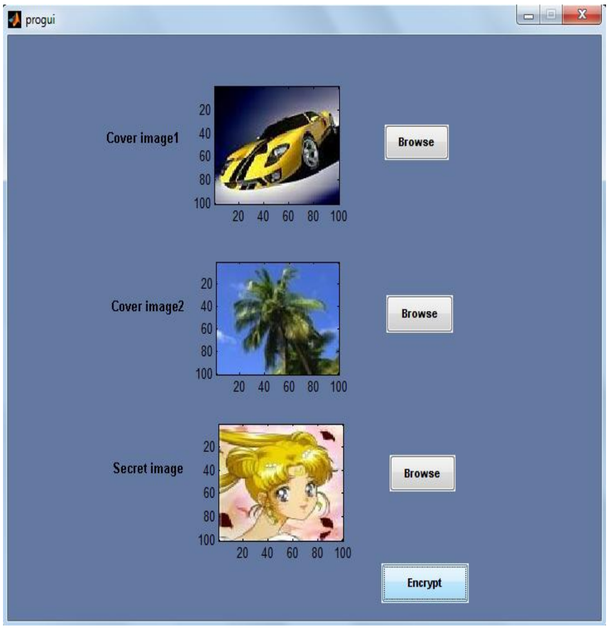

Fig 4-GUI for sharing scheme

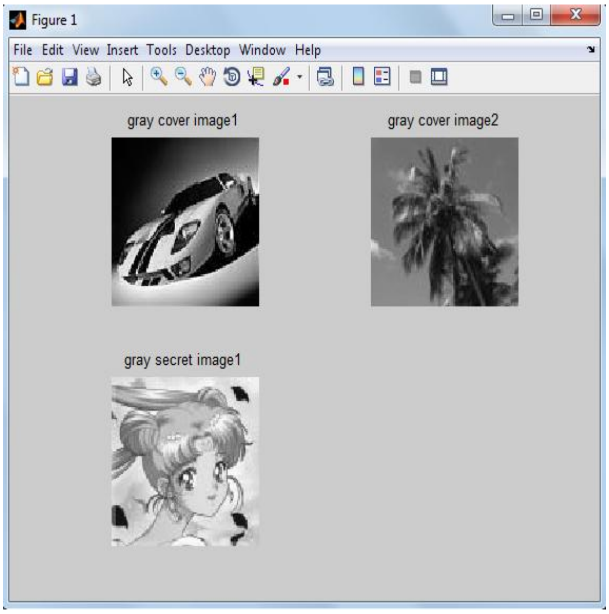

Fig-5: Grayscale images

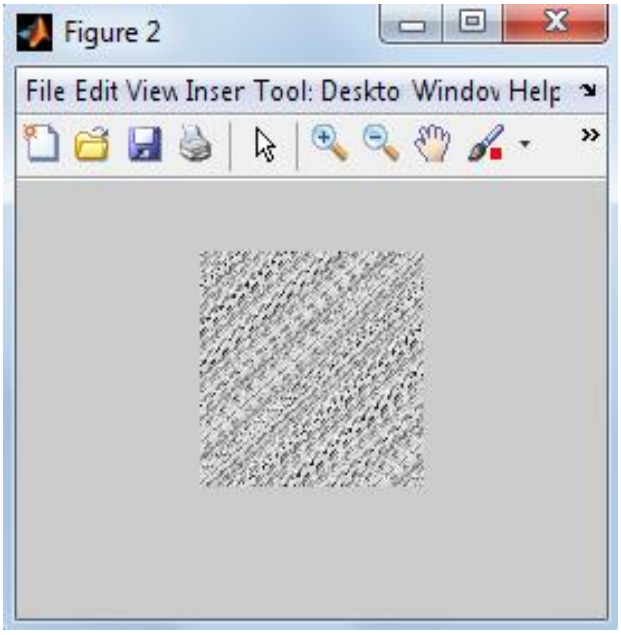

Fig-6: Encrypted Image

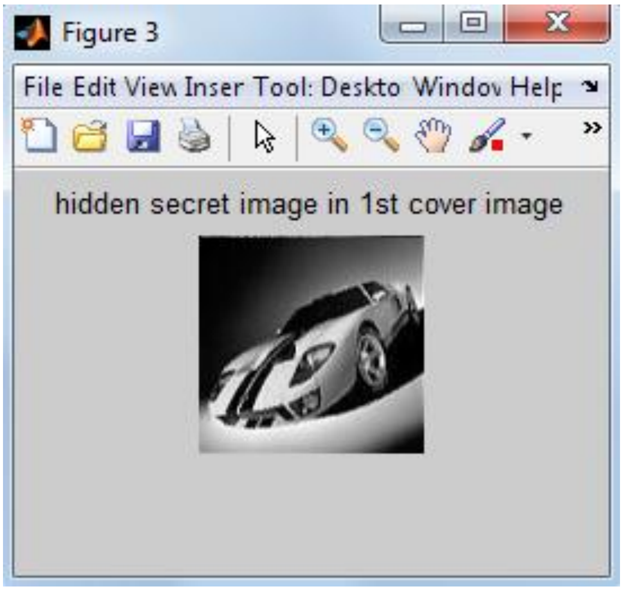
Figure 3
File Edit View Inser Tool: Deskto Windov Help
hidden secret image in 1st cover image

Fig-7: Hidden encrypted secret image in first cover image

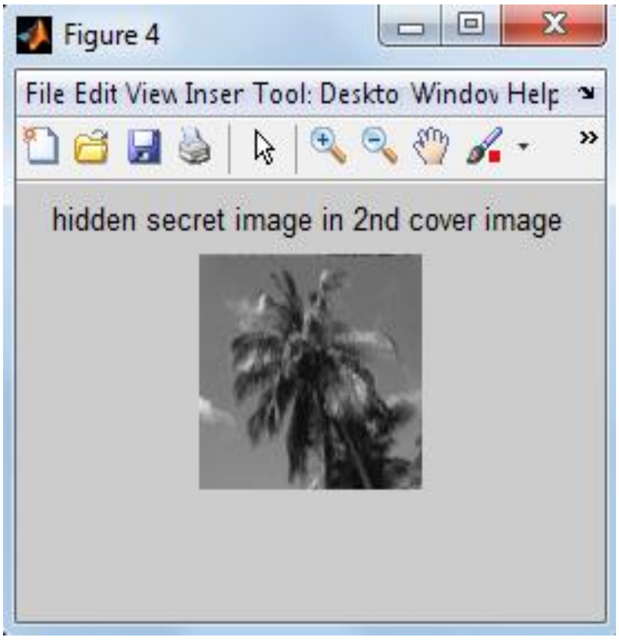
Figure 4
File Edit View Inser Tool: Deskto Windov Help
hidden secret image in 2nd cover image

Fig-8: Hidden encrypted secret image in second cover image

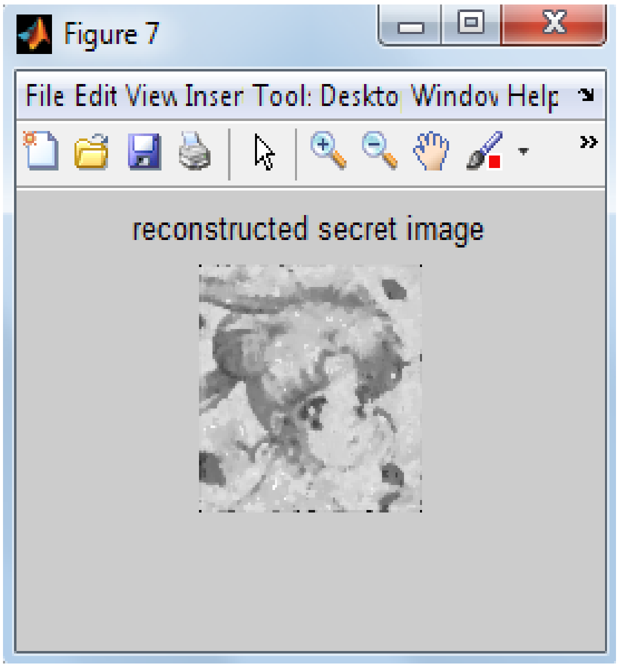
Figure 7
File Edit View Inser Tool: Deskto Windov Help
reconstructed secret image

Fig-9: Reconstructed image

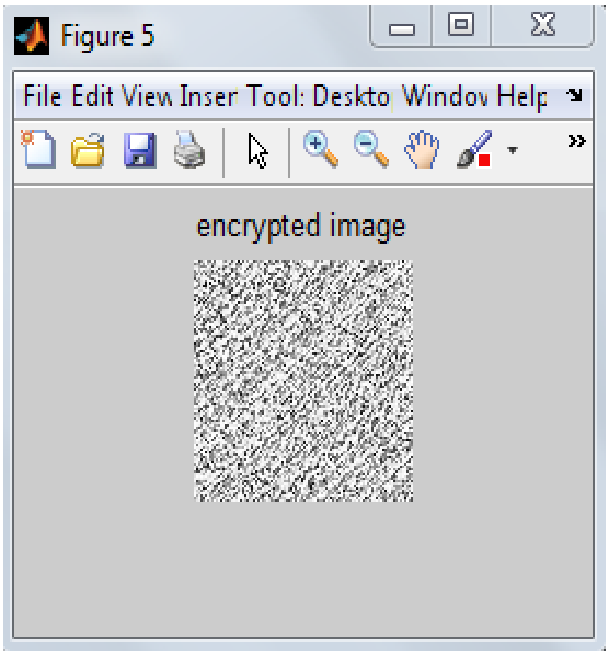

Fig-9: Extracted Encrypted image

V. CONCLUSIONS

This paper presented a new approach for securely transferring the data image. The proposed system uses three levels of security which contains, Arnolds Transformation, (2, 2) Visual Cryptography method and Embedding phase. This paper provides a more secure way of image sharing as the image is encrypted using modified Arnold transformation before hiding into multiple cover images.

ACKNOWLEDGMENT

The authors would like to thank Neethi M, NMAMIT, Nitte for her contribution for this paper.

REFERENCES

[1] M. Naor and A. Shamir, “ Visual Cryptography”, in Proceedings of Euro crypt 1994, Lecture notes in Computer Science, 1994, Vol.950, pp. 1-12

[2] Chang C.C and Yu. T.X., “ Sharing a Secret Gray Image in Multiple Images”, in the proceedings of International Symposium on Cyber Worlds: Theories and Practice, Tokyo, Japan.

[3] R. Youmaran, A. Adler, A. Miri, “ An Improved Visual Cryptography Scheme for Secret Hiding”, in the proceedings of 23rd Biennial Symposium on Communications, 2006, pp. 340-343

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

[5] 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

[6] Chiiaranjan Pradhan, Vilakshan Saxena, Ajay Kumar Bisoi, " Imperceptible Watermarking Technique using Arnold's Transformation and Cross Chaos Map in DCT Domain", International Journal of Computer Applications, Volume 55-No.15, October 2012

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

[8] C. Yang and C. Laih., " New Colored Visual Secret Sharing Schemes", Designs, Codes and Cryptography, 20:325-335,2000Reference 4

.