A Secret Sharing Scheme for Secure Transmission of Color Images

Mayank Arya Chandra*
Mithlesh Kumari*
Kanika Talwar*

Abstract

Secret sharing is a very secure and efficient way through which we transmit a color image from one user to another user over a network. In this paper we give a method to generate a secret through multiple images. Based on secure image schemes, an effective and generalized scheme of color image hiding is proposed by means of numerical computations; we form a key and generate the secret image by using deformation (d) and formation (f) algorithms. In this paper we are going to present a new scheme for securing color images by hackers and intruders. It is a matrix computation scheme which uses the concept of secret sharing and key safeguarding. This paper proves that proposed scheme is more efficient and secure in terms of secret sharing as well as key safeguarding.

Keywords: Secret Sharing, Key Safeguarding, Security.

1. Introduction

In this computer era security require more attention there are several techniques used for data security like key safeguarding, encryption and other cryptography techniques. For security purposes text data is converted into image so, there is a major concern about security. Since text can be decoded and recognized by the system using brute force attack, but an image cannot be easily decoded and recognized by the any system. Image recognition is a very difficult task for any system.

Key safeguarding is a basic technique for data and image security but it can be broken easily by the brute force attack and another drawback of this technique is that if key is lost then data cannot be recovered. So we use secret image sharing technique in which we distribute the secret by forming the shares which are encrypted and secret image is reformed by qualified subsets of shares. We can say it is a more or less [p, q] threshold scheme where p is the number of shares produced and q is the number of qualified subsets of shares, where q p.

This method introduce by the Adi Shamir[1] and he was able to transmit a secure data over the network from one end to other. Harn and Lin [2] have given a technique for secret sharing scheme to solve the secret regeneration problem by extending

*Student, M.Tech (CSE), USIT, G.G.S.I.P. University, Delhi, India.

the lifespan of the shadows. Blundo, Santis and Naor[4] have proposed a Scheme for gray level images. Thein and Lin[5] have described a numerical processing based approach to share a protected image secretly where an image is permuted into random image and then shared images are generated using secret sharing. In the paper of the blakley[3], cryptographic approach takes lots of time for generating the share of the Image at the sender end and also take the lots of time for reconstructing the original image from the share at the receiver end. It means that it consumes a lot of time in encoding and decoding of the image.

The following paper and proposed scheme removes such type of problem. Paper consists following sections which are arranged as: The 2nd section describes proposed scheme, 3rd section describes the deformation and formation algorithms,4th section describes the experimental results, 5th section describes the conclusion and 6th section references.

2. Proposed Scheme

Here in this paper we proposed a new security scheme for color images which is based on key safeguarding as well as secret image sharing. Here we have taken an idea from matrix calculation for generating the key image using the secret color image and p securing images and reforming the secret color image using the key image and securing images.

Suppose we have to secure an image which should be retrieved by q securing images and a key. This is done by combining q pixels of secret image and q pixels value of securing images by equation given below to get the key for these pixels.

$$f(j) = \sum_{i=1}^{q} (a_{ji} + b_{i-1} * (j)^{q-i})$$

Where j= any +ve number 1, 2, 3…p
a_{ji} = pixel value of securing image j.
b_{i-1}= pixel value of secret image.
$F(j)$ = Key value

For reforming the secret image, subtract the q pixels of q securing images out of p value from key value. Apply this for all pixel values.

There are some mathematical computations done over here:
We taken p=5 and q=3 and by using eq. (1)

2.1 Deformation side

$F(1) = a_{11} + a_{12} + a_{13} + b_0 + b_1 + b_2$
$F(2) = a_{21} + a_{22} + a_{23} + 4*b_0 + 2*b_1 + b_2$
$F(3) = a_{31} + a_{32} + a_{33} + 9*b_0 + 3*b_1 + b_2$
$F(4) = a_{41} + a_{42} + a_{43} + 16*b_0 + 4*b_1 + b_2$
$F(5) = a_{51} + a_{52} + a_{53} + 25*b_0 + 5*b_1 + b_2$

2.2 Formation side

By using any three securing images and key image as j =1, 2, 3, the secret image is retrieved.
$b_0 + b_1 + b_2 = F(1) - a_{11} + a_{12} + a_{13}$
$4*b_0 + 2*b_1 + b_2 = F(2) - a_{21} + a_{22} + a_{23}$
$9*b_0 + 3*b_1 + b_2 = F(3) - a_{31} + a_{32} + a_{33}$

Find out the values of b0, b_1, b_2 which are the pixel values of secret image.

3. Proposed Algorithms

3.1 Deformation Algorithm

Step1: Choose secret and p securing images for generating the secure key.

Step2: Select q pixels from secret image and securing images and calculate the key value using eq. (1).

Step3: All keys stored in key image in two pixel values.

Step4: Apply step 2nd and 3rd for each and every pixel value.

3.2 Formation Algorithm

Step1: Select any q securing images and key image.

Step2: Retrieve the two pixel values of key image and q pixels values of securing image.

Step3: Subtract the q pixel values of securing image from key value of j^{th} securing image.

Step4: Apply step 3rd for each of the q securing images.

Step5: By using the above process, receive the secret q pixel values.

Step6: Combine the entire pixel secret image formed.

4. Experimental Results

Successfully we have received some experimental results which are mentioned here:
Fig. (1) is the secret image, Fig. (2)- (6) are the securing images, Fig. (7) is the key image and Fig (8) is the retrieved image using securing images and key image by above algorithms.

Fig. 1

Fig. 2

Fig. 5

Fig. 3

Fig. 6

Fig. 4

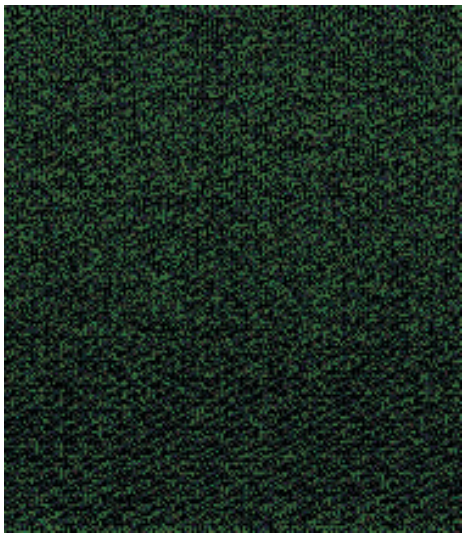

Fig. 7

Fig. 8

5. Conclusion

Successfully we have concluded that proposed scheme is more secure and efficient one because in this scheme secret image is developed using securing images which are also useful information having some meaning. So hacker may think that this is the secret image. The secret image is recovered without distortion. There is lot of scope for future work like use this scheme for multiple secret images and develop more security.

6. References

1. *A. Shamir, "How to Share a Secret," Communications of ACM," 1979.*
2. *G. R. Harn and H. Y. Lin, "An i-span Generalized Secret Sharing Scheme", In Proc.12th Annual International Cryptography conference, Aug 1992, California, USA.*
3. *G. R. Blakley, "Safeguarding cryptographic keys," I. Proc. of the National Computer Conference (NCC), AFIPS Conference Proceedings, vol. 48, pp. 313-317, 1979.*
4. *C. Blundo, A.D. Santis, M. Naor, "Visual Cryptography for grey level images," Information Processing Letters, vol. 75, pp. 255-259, 2000.*
5. *C. -C. Thien, J. -C. Lin, "Secret image sharing," Computers and Graphics, Vol. 26, pp.765-770, 2002.*
6. *M. Naor and A.Shamir, "Visual Cryptography," Advances in Cryptology: Eupocrypt' 94, Springer- Verlag, Berlin, pp. 1-12, 1995.*
7. *R. Brinkman, .M. Doumen, P.H. Hartel, and W.Jonker "Using secret sharing for searching in encrypted data," In W. Jonker and M. Petkovi c, editors, secure Data Management VLDB 2004 workshop, vol. LNCS 3178, pp. 18-27, Toronto Canada, Augest 2004.*
8. *C. C. Lin and W. H. Tsai, "Secret Image Sharing with Staganogarphy and authentication,"Journal of System and Software, vol.73,pp 405-411, 2004.*
9. *C. C. Lin and W. H. Tsai, "Secret Image Sharing Scheme," Journal of System and software ,vol.31, pp 267-272, 1997.*
10. *Chien-Chang Chen, Wen-Yin Fu, Chaur-Chin Chen,"A Geometry based Image Sharing Approach " Proc. IVCNZ (Image and Vision Computing, Newzeland), 28-29 Nov., 2005.*
11. *Hasimoto, K. Matsuo, A. Koike and Y. Minami, "Hierarchical Secret Image Sharing Method using JPEG 2000 Codestream Syntax, 13th European Signal Processing Conference(EUCIPCO 2005), Sept. 2005, Antalya, Turkey.*