RESEARCH PAPER | Engineering | Volume : 6 | Issue : 3 | March 2016 | ISSN - 2249-555X | IF : 3.919 | IC Value : 74.50

A Secret Color Image Transmission In Secured Way Using Steganography

KEYWORDS: Image processing, secret share, Peak Signal to Noise Ratio

Mandar Jatkar	Preeti Gophane
Asst Prof, Vivekanand Education Society's Institute of Technology Chembur Mumbai	Asst Prof, Vivekanand Education Society's Institute of Technology Chembur Mumbai

ABSTRACT *Image processing is one of the most developing and interesting topic in recent Technologies. Stegnographic images is mainly used for the purpose of information hiding in various fields. Secret sharing is a method of distributing a secret among a group of participants. Each participant is allocated with a share of the secret. Secret shares are generated with the help of reversible polynomial function and the participant's numerical key. The secret image and the cover image is embedded together to construct a stego image. The reversible image sharing process is used to reconstruct the secret image and cover image. Peak signal to noise ratio is applied to analyze the quality of the stego images.*

I. INTRODUCTION

Security is an important issue in information technology. It is an important issue which is ruling the internet world today. Confidentiality, security, authentication are main issues in security. Sensitive and important data can be shared secretly using visual secret sharing method. The secrets are encrypted and are shared to different participants. The participant's shares are decrypted to reconstruct the secret. In (t, n) scheme t shares are needed to reconstruct the original secret. Single participant share is not valid, only when t shares are combined the original secret is reconstructed.

Blakley and shamir developed (t, n) threshold scheme, where a dealer encrypts and divide the secret into n number of shadows. This scheme is proposed in the year 1979. The dealer then distributes the shadows to the authorized participants. Any t out of n, authorized participants can co-operate to reveal the secret data with their corresponding shadows.

Visual secret sharing developed by shamir[1] from the (t, n)– threshold concept. Secret image is encoded into random images named as shadows, during transmission the shadows are transmitted instead of secret.

Lin and Tsai [10] and Wu, Y.S., Thien, C.C., Lin [11]suggested a secret sharing method that produces shadows based on t-1 polynomial. These shadows are embedded with in a cover image to hide the secret. However the secret images are constructed using the above secret sharing method will have distortions because of truncations of gray pixels values that are greater than 250.

Pei-Yu Lin et al. [14] introduced a method which produces a lossless secret message and the original image from the distorted stego images. It uses the (t, n) threshold secret sharing system introduced by Blakley [2] and Shamir [3]. Retrieving original image is especially important in the fields like medical, military. This approach preserves the fidelity of the cover image. They tested the algorithm with different types of images to estimate the quality of the stego-image. They achieved a better PSNR. Smaller the value of m the better is the quality of the stego image, but this reduces the capacity of the secret data to be embedded.

Novel image secret sharing for color image is proposed in our paper which possesses reversible characteristics as [13]. Authorized participants are allowed to reconstruct the secret and the original cover from the stego using the reversibility scheme [13]. This reversible scheme can be used for medical image processing, artistic images and military images where the secret is retrieved without any distortion.

II. PROPOSED WORK

Overview of this paper consists of the following modules:-e

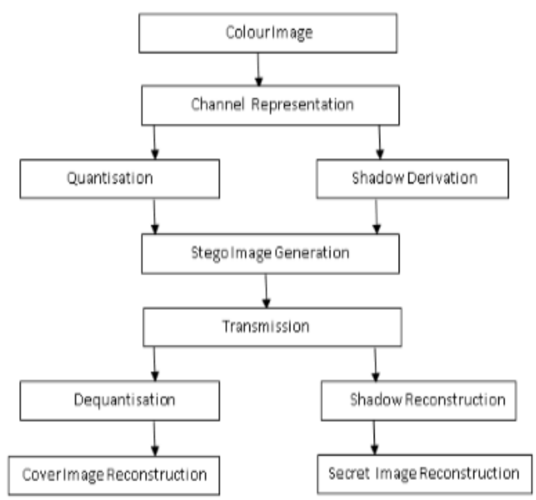


Figure 1 : Block Diagram

1. Channel Representation: Colour images are used as secret and as cover image. In colour image each pixel is in the form of 3 channels red, green and blue. The pixel value of each channel is between 0-255.
2. Shadow Derivation: Secret sharing is a process of shadow generation. The secret color image pixels are converted into m-ary notational system with the help of the prime number m that is nothing but modulo operation of each pixel of secret color image. Let c1, c2, ct-1, d are co-efficient of invertible polynomial function F(x), p be the pixel value of cover color image. The output of m-ary notational system will be c1,

c2……ct-1 digits. With the help of the prime number, d will be calculated for every pixel of each channel of cover color image, where d=p mod m. The output of invertible polynomial function will be encrypted with the help of the participant's numerical key. Each participant generates their shadows with their appropriate numerical key value.

3. Quantization Process: Quantization process Q=(p/m)*m is done to preserve the cover image pixel value in order to retain the actual quality of cover image during reconstruction. Quantized pixel value is calculated with the help of two operations division and multiplication. Divide the cover image pixel by the prime number m and take the floor value, perform multiplication by prime number on the floor value which gives the quantized value of cover image pixel.
4. Stego Image Generation: The cover image is used to hide the generated shadow images. By embedding the pixels of shadow image into cover image ,we get the stego images. The quantization value got from cover image is added to the pixel from shadow image to get the stego image.
5. Shadow Reconstruction: Each authorized participant will have a stego image and a key. Let sp be the stego image pixel value and y be the pixel value of shadow. With the help of prime number m, the shadows will be reconstructed where y = sp mod m. Likewise n shadows are reconstructed from n stego images. Shadows can be reconstructed from the stego images.
6. Secret Image Reconstruction: Secrets can be reconstructed only with minimum of t shadows, less than t is of no use. The Lagrange's formula is formed by using participant's numerical key and shadow value. The Lagrange's formula is given below.

$$f(x) = \sum_{i=1}^{k} (\text{yj lj(x)})$$

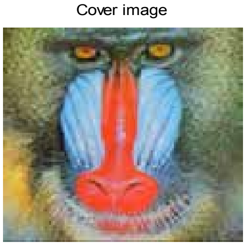
Where yj is shadow value, lj is calculated using participant's numerical key.

7. Cover Image Reconstruction: Quantization operation Q= (sp/m)*m will be used to get back the color cover image without loss. Quantization operation is performed on the stego image, which will generate a quantized value. This quantized value is added with the last digit of Lagrange's interpolation equation, the result of which reconstructs the cover image pixel.

III. SIMULATION RESULTS

Few color test images are taken as cover image. The experimental platform was programmed in Matlab version 9.

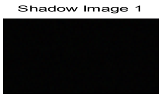
Cover image



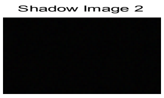
Secret Image

The original secret color image is hidden inside the cover image.

Shadow Image 1



Shadow Image 2



Shadow Image 3

Shadows generated using polynomial function

Stegno Image 1

Stegno Image 2

Stegno Image 3

The three shadows of the secret color image will be hidden into the cover image to generates a stego image

Reconstructed Secret Image

Reconstructed Cover Image

Secret image is extracted from the stego. Cover image is also reconstructed from the stego image.

The distortions present in the stego image are calculated using Peak to Signal Noise Ratio (PSNR).

PSNR=10 X 10 LOG $_{10}$ (255^2 / MSE color)

MSEcolor - Mean Square Error between the original cover color image and the stego color image. For a cover image of size H x W, the MSEcolor is given as below,

MSE color = (1/ HXW) $\sum_{i=1}^{H} \square \sum_{,-1} \frac{R+G+B}{3}$

Where R, G, B are calculated as

$R = (R\,x_{ij} - R\,y_{ij})^2$

$G = (G\,x_{ij} - G\,y_{ij})^2$

$B = (B\,x_{ij} - B\,y_{ij})^2$

Rxij and Ryij - Pixel values of the Red component in the original cover color image and the stego color image, respectively.

Gxij and Gyij - Pixel values of the Green Component in the original cover color image and the stego color image, respectively.

Bxij and Byij - Pixel values of the Blue component in the original cover color image and the stego color image, respectively.

Table 1 : Comparison with various Prime numbers.

Prime Number(m)	PSNR(dB) (Lena)
3	47.8601
5	45.1602
7	41.8735
11	38.2424
13	36.6608
17	34.2382
19	33.4348

23	31.8863
29	30.8001

A higher PSNR value means that the quality of the stego color image is similar to that of original color cover image. PSNR value less than 35 dB means that some of the important signal characteristics are lost. PSNR value less than 30 dB is an unacceptable quality. Good quality is implied by PSNR value greater than 35 dB.

Table 2 : Comparison with various methods.

Other Methods	Drawbacks	Advancement of Proposed Paper
LSB Substitution	Large cover image needed, not bother about the cover image quality	Same size of cover image is enough, Cover image quality is maintained by Quantization process
Small shadow technique(compression)	Lossy is possible	Lossy is not possible
(2,n) Secret Sharing	More Security is needed	It follows (t, n) threshold Sharing Scheme. No use of t-1 shadows.
(n, n) Secret Sharing	All shadows should combine to retrieve the secret	

IV. CONCLUSION

In the existing methods, the reconstructed shadows are meaningless and the distortions are large. The proposed reversible image sharing approach for color image reveals the secret image without loss and preserves the cover image. The generated shadows are meaningful with better PSNR value compared with the previous methods.

REFERENCES:

[1] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptograhy: EUROCRYPT'94, LNCS, vol. 950, pp. 1–12, 1995.
[2] Blakley, G.R., l979. " Safeguarding cryptographic keys". In: Proc. AFIPS National Computer Conf., vol. 48, pp. 3l3–3l7.
[3] Chang, C.C., Hwang, R.J., l997. Efficient cheater identification method for threshold schemes. IEE Proc. – Comput. Digital Techn. l44 (l), 23– 27
[4] Beimel, A., Chor, B., l998. Secret sharing with public reconstruction. IEEE Trans. Inform. Theory 44 (5), l887– l896.
[5] Wang, R.Z., Su, C.H., 2006. Secret image sharing with smaller shadow images Pattern Recognition Lett. 27(6),55l–555.
[6] Wang, D., Zhang, L., Ma, N., Li, X., 2007. Two secret sharing schemes based on Boolean operations. Pattern Recognition 40 (l0), 2776–2785
[7] Chen, T.H., Tsao, K.H., 2009. Visual secret sharing by random grids revisited. Pattern Recognition 42 (9), 2203– 22l7.
[8] Chang, C.C., Lin, C.C., Lin, C.H., Chen, Y.H., 2008. A novel secret image sharing schemin color images using small shadow images. Inform. Sci. l78 (ll), 2433–2447