Minimum distortion secured binary image steganography

Priyanka SambhajiDahiwal[1], Mrs. GyankamalJ.Chhajed[2]

[1]P. G. Student, [2]Assistant Professor
Department of Computer Engineering, VPKBIET, Baramati

***Abstract*: To transfer any information secure network is used. In critical data confidentiality is important. This proposed work is a steganography technique and provides the approach of security with the combination of data compression technique to improve stegnographic capacity. In this project, a binary image steganographic scheme that aims to minimize the embedding distortion on the texture is presented. The complement of binary image is taken first then image need to be rotated. After rotation mirroring process is used. The flipping distortion score of pixel is calculated on measuring the flipping distortion of corresponding pixels. A steganographic scheme will be developed on the basis of measurement. In this scheme, the scrambled binary image is divided into number of blocks is called superpixels. Then syndrome-trellis code is used to minimize the designed embedding distortion. This scheme will prove to be secure without degradation in image quality and affecting embeddingcapacity.**

***Keywords:* Binary image, flipping distortion, encryption.**

I. INTRODUCTION

In day to day life security is more important. Data hiding techniques have number of varieties like digital media applications, copy control, etc. data encryption is increase confidentiality of document but in steganography embeds the data or message string with an image. Image can hide the data. Hiding data in a binary image is difficult because pixel can be easily detected by human visual system to avoid this problem we divide the image into number of blocks. In image Steganography, if minimize the flipping distortion of pixel then it is not identify by HVM. Basically two keys are used for data hiding, first is public key which used by sender for encryption and second is private key which is use in server side. In this domain, on basis of distortion score value of pixel message bits are commonly encrypted. In this paper binary image can take only two values 0 and 1. 0 values for white pixel and 1for black pixel. In paper [2] new techniques are used to embed data in text, binary image, figures and signs. To embed a significant amount of data without causing noticeable artifacts manipulation method is used. In [3] paper Presented a novel steganography scheme capable of concealing a large amount of data in a binary image. The proposed scheme has the following features: it uses a secret key and a weight matrix to protect the hidden data, it uses a weight matrix to increase the data-hiding ratio, and it uses an XOR operator to increase the security.

II. LITERATURESURVEY

In paper [5] a method for data hiding in binary images was proposed and it can used morphological transformation to convert binary images. To get the details of coefficients in images and the location of the pixels used location map. Therefore flipping of edge pixel is shifting vertically and horizontally.
In [2] Author defines the techniques for large datasets. Author Represent steganographic scheme which is used for large amount of binary image data. This scheme used for secret key and weight matrix for protect the data. In this paper author used XOR operator to increase the security.
In paper [3] Propose a new technique for embedding binary images .It include binary images, including scanned text, figures, and signatures etc. in this technique manipulates the pixels into fixed block size to embed the specific amount of data.
In research paper [4] proposes a new method for binary image authentication to improve security of message string. A technique of this author is novel blind data hiding method. In this paper, the focus is on data hiding for binary images in lower level for the purpose of image authentication.
In paper [5] author can define a new method to achieve blind watermark extraction, to determine the data hiding locations. Author use the details of coefficient in binary image. The details of coefficient are can store on location map of binary image.

III. PROPOSEDMETHODOLOGY

1. Embedding Process

System architecture is represented by following block diagram.

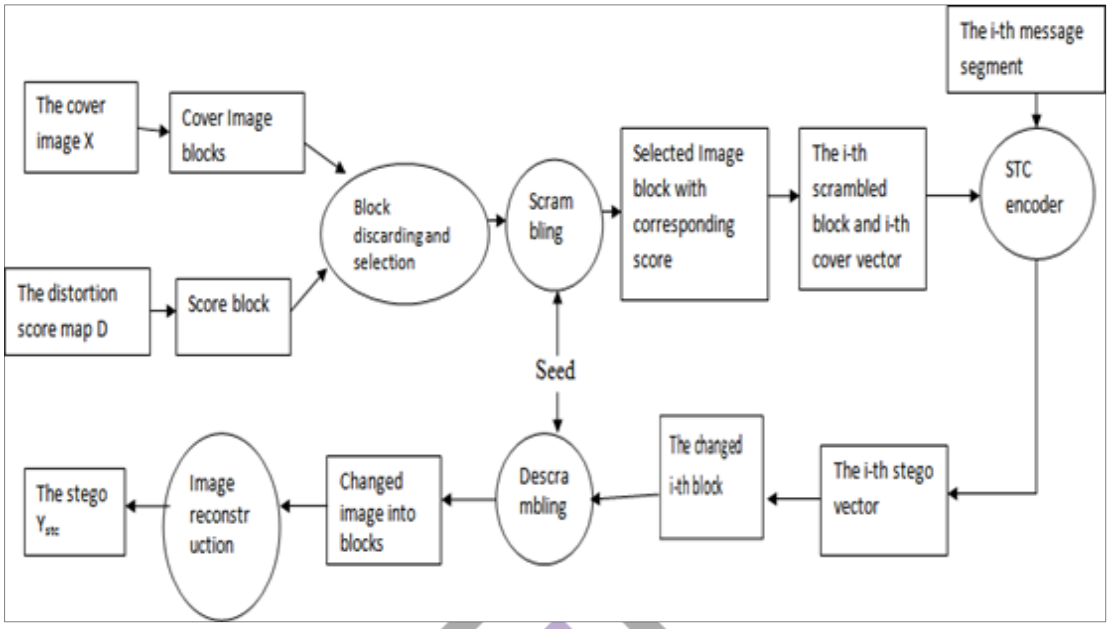

Fig 3.1 Embedding block diagram [1]

A. Input Process:

1) The cover image is a input of embedding procedure. Here X is denoted as binary image.
2) The cover image divides into non-overlapped blocks
3) In Distortion score block map, calculate Distortion score of each pixel. In Stegnographic scheme should only change the pixels with the lowest distortion scores.
4) In score block, select the pixel block which is having lowest distortion score.
5) In block discarding and selection phase, blocks are selected based on distortion score.

B. Scrambling:

1) When the cover image is divided into non-overlapped block. Then in scrambling process the flippable pixels distributed more uniform region contain in an image and then the density of flippable pixel is decreases.
2) Then scrambled pixel still corresponds to distortion score at same location.
3) Then each selected pixel is called superpixel. Then calculate Parity of number of black pixel and it is calculated by using following formula:

$$J_{i,j} = \left(\sum_{i'=i}^{i+lj-1} \sum_{j'=j}^{j+lj-1} I_{i',j'}\right) mod 2$$

Here $J_{i,}$ is calculated parity of black pixel.

C. STC encoder:

The message is embedding using STC application.
One message segment is embedding using STC application.

2. ***Extracting Process:***

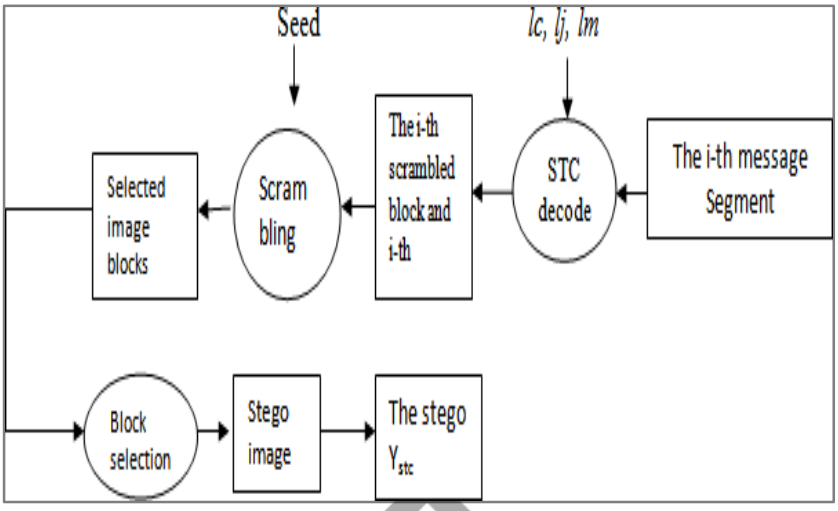

Fig 3.2 .Extracting Process[1]

1) In Extraction process first divide image into non-overlapped blocks. Then select all non-uniform block.
2) Then scrambling process is performing on blocks.
3) STC decoder is used for extracting message segment.

2.1 Algorithm

A) Embedding Algorithm

Take binary image I and then convert into non-overlapped block.

1) Calculate the distortion score of binary image I.
2) Divide binary image I into non-overlapped blocks. Then divide the binary message **m** into non-overlapped message segments.
3) Select all non uniform blocks in binary image I and change all image blocks in binary image.
4) Select all the non uniform blocks in I and the Corresponded. Distortion score blocks in D. here D is distortion score.
5) Consider all the selected blocks in I as an ensemble binary image and all the selected blocks in D as an ensemble D then
   Scramble binary image I and D with the same scrambling seed so that each scrambled pixel still corresponds to the correct Distortion score at the same location.
6) Then image block divide into super pixels. The block select whose value and distortion score D is calculated.
7) Then use this superpixel as cover vector to embed message segment by applying STC encoder.
8) For each superpixel whose value needs to be changed, flip the pixel with the lowest distortion score in it.
9) Repeat Steps 5, 6 and 7 until all the message segments have been embedded.
10) Descramble the embedded image blocks.

B) Extracting Procedure

In extraction Procedure, user can be use private key to see the hidden message.

To extract message following steps are used:

1) Divide binary image into non-overlapped blocks and Select all the non uniform blocks.
2) Scramble the selected stego image blocks via the same scrambling described in Step 4 of the embedding procedure.
3) For the stego block, form the superpixel vector by using the same process in Step 5 of the embedding procedure. Use it as the stego vector to extract the message segment m by applying
STC decoder.
4) Repeat Step 3 until all the message segments have been extracted.

IV. RESULT AND DISCUSSIONS

The PSNR will be used to demonstrate the advantage of the proposed scheme on the embedding efficiency, which is gained from employed embedding strategy. The MSE is a measure of the quality of an estimator and it is always non-negative, and values closer to zero are better.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]\,2$$

$$\text{PSNR} = 10.\log_{10}\frac{MAX_1^2}{MSE}$$

V. CONCLUSION

This work exploits the texture of binary images and proposed a minimum distortion secured binary image steganography. In this work binary image processing is done. In image process first take complement of binary image then rotate texture pattern of image and then mirroring- invariant local texture pattern. The proposed flipping distortion measurement is set with the weighted sum of crmiLTP changes, where the weight is empirically assigned according to the discrimination power of the crmiLTP histogram.

REFERENCES

[1] Bingwen Feng, Wei Lu, and Wei Sun," Secure Binary Image Steganography Based on Minimizing the Distortionon the Texture", vol. 10, no. 2, february2015

[2] Q. G. Mei, E. K. Wong, and N. D. Memon, "Data hiding in binary text documents," *Proc. SPIE*, vol. 4314, pp.369–375, Aug.2001.

[3] Y.-C. Tseng, Y.-Y. Chen, and H.-K. Pan, "A secure data hiding scheme for binary images," *IEEE Trans.Commun.*,vol.50,no.8,pp.1227–1231,Aug.2002.

[4] M. Wu and B. Liu, "Data hiding in binary image for authentication and annotation," *IEEE Trans. Multimedia*, vol.6,no.4,pp.528–538,Aug.2004.

[5] H. Yang and A. C. Kot, "Pattern-based data hiding for binary image authentication by connectivity-preserving," *IEEE Trans.Multimedia*, vol. 9, no. 3, pp. 475–486, Apr.2007.

[6] H. Yang, A. C. Kot, and S. Rahardja, "Orthogonal data embedding for binary images in morphological transform domain - A high-capacity approach," *IEEE Trans. Multimedia*,vol.10,no.3,pp.339–351,Apr.2008.

[7] M. Guo and H. Zhang, "High capacity data hiding for binary image authentication," in *Proc. Int. Conf. Pattern Recognit.*,Aug.2010,pp.1441–1444.

[8] H. Cao and A. C. Kot, "On establishing edge adaptive grid for bilevel image data hiding," *IEEE Trans. Inf. Forensics Security*,vol.8,no.9,pp.1508–1518,Sep.2013.

[9] T. Filler, J. Judas, and J. J. Fridrich, "Minimizing additive distortion in steganography using syndrome-trellis codes," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 920– 935,Sep.2011.

[10] T. Pevný, T. Filler, and P. Bas, "Using high-dimensional image models to perform highlyundetectablesteganography," in *Information Hiding* (Lecture Notes in Computer Science), R. Böhme, P. W. L. Fong, and R. Safavi-Naini, Eds.,vol. 6387. New York, NY, USA: Springer-Verlag,Oct.2010,pp.161–177.

[11] V. Holub and J. Fridrich, "Designing steganographic distortion using directional filters," in *Proc. IEEE Int.WorkshopInf.ForensicsSecurity*,Dec.2012,pp.234–239.

[12] F. Huang, W. Luo, J. Huang, and Y. Q. Shi, "Distortion function designing for JPEG steganography with uncompressed side-image," in *Proc. 1st ACM Workshop Inf. HidingMultimediaSecurity*,2013,pp.69–76.

[13] N. Provos, "Defending against statistical steganalysis,"in*Proc. 10th Conf. USENIX Security Symp.*, 2001, pp.323–335.