



IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 Issue: VII Month of publication: DOI:

www.ijraset.com

July 2019

Call: 🛇 08813907089 🕴 E-mail ID: ijraset@gmail.com



Binary Image Steganography using Flipping Distortion Technique

Ms. Priyanka S. Dahiwal¹, Mrs Gyankamal Chhajed², Dr Devendrasingh Thakore³ ¹Student, ²Professor, VPKBIET, Baramati Maharashtra, India ³Bharath Vidyapeeth (Deemed to be University) College of Engineering, Pune.

Abstract: In binary image steganography many methods are used. The flipping distortion of the pixel is important to hide the message in image. The binary steganography image is divided into 3X3 blocks. Binary image encrypted with a private key. In this method non-overlapped blocks is take and scan image from top left corner. To decrypt the message string user need private key. Some techniques like minimizing flipping distortion are used securely data transfer.

In steganographic scheme divide the scrambled image into superpixels and generate cover image.

I.

In this method, the image divided into blocks of order 3 X 3. Each block is divided diagonally and the number of black and white pixel in both the upper and lower halves of the block is determined. After that connectivity and smoothness test is performed on each 3X3 block to decide whether block is embeddable or not. For extraction the hidden data bits, reverse process is applied on the image. Hence original image is not use for extraction.

Keywords: Data hiding, encryption, Image processing.

INTRODUCTION

The digital binary images are widely used in the applications including legal documents, digital books, maps, and architectural and electronic drawings and in business applications. The unauthorized use of a signature, such as copying it onto an unauthorized payment, is becoming a serious concern. In addition, a variety of important documents, such as social security records, insurance information, and financial documents, have also been digitized and stored. Because of the ease to copy and edit digital images, annotation and authentication of binary images as well as detection of tampering are very important. For images in which the pixels take value from only a few possibilities, hiding data without causing visible artifacts becomes more difficult. In particular, flipping white or black pixels that are not on the boundary is likely to introduce visible artifacts in binary images. As these digital media are getting widely used, their security related issues are becoming of primary concern. Hence many digital watermarking techniques have been proposed and very few data hiding techniques are available for binary images, In the spatial domain, flipping pixel values in a binary image used to embed message bits. In binary image black pixel is identify by 1 and white is identify by 0. As a result, distortions on binary images are easily detected even by human eyes. To avoid this problem some selected part of image is take for data hiding. For embedding message in image noisy area is selected. Many techniques /methods are used for detect the suitable pixel. selected pixel is called super pixel .scrambling process very important to find outs super pixel. Some schemes traced the boundary to find more suitable pixels for embedding message bits, whereas the others divided the cover image into overlapped/non-overlapped blocks and found the best flipping location in each block.

Some techniques are used for detecting location of pixel. In paper [3] assessed the flipping distortion according to the smoothness and connectivity in a 3×3 window. Yang and Kot [4] defined a connectivity-preserving criterion for 3×3 patterns to determine the flippability.

II. LITERATURE SURVEY

In all measuring techniques, it calculate distortion according to human visual system (HVS)[1]. That's why yielded stego images are use because it has good visual qualities and it is not easily detected by human eyes. To secure steganography. Image should be in statistic and minimize the embedding impact. Noting that binary images naturally represent the texture [1][3], In paper [1] texture model to measure the embedding distortion. In image processing there are three types of approaches describing the texture geometry-based, statistic-based, and model-based approach. In the proposed measurement, the first and second types are combined to describe the texture with respect to both spatial structure and statistical distribution [1]. Bingwen Feng, Wei Lu, Wei Sun describes new technique for data hiding. The steps are:

- 1) Extract the local texture pattern (LTP) as the texture primary.
- 2) The histogram of LTPs is then employed to describe the texture distribution.
- 3) The LTP is motivated by the concept of the local binary pattern (LBP) the complement, rotation, and mirroring-invariant local



International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177 Volume 7 Issue VII, July 2019- Available at www.ijraset.com

Wu *et al.* propose to employ the visual distortion table to assess the "flippability" of a pixel [1]–[3]. To equal embedding capacity of image shuffling technique is used. Normally large blocks are take for shuffling because in each block at least one pixel to flip. In paper [3], center pixels are flip, some patterns create distortion as a hole in straight line. Pairs of edge patterns which are dual to each other are employed to trace the contour to find suitable locations for data hiding in [4]. A secret key and a weight matrix are used to protect the hidden data in Image. The randomness in choosing the embedding locations creates poor visual effects despite the large capacity. Further improvements on visual quality are made by choosing the edge pixels [1].





Fig. Decoding Process



International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177 Volume 7 Issue VII, July 2019- Available at www.ijraset.com

In system architecture 2 procedure is important these are:

- A. Embedding Procedure
- 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 Steganographic 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 Process
- 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:

$\mathbf{J}_{\mathbf{i},\mathbf{j}} = \left(\sum_{i'=i}^{i+lj-1} \sum_{j'=1}^{j+lj-1} Ii'j' \right) mod2$

Here, is calculated parity of black pixel. The hidden data can be extracted without using the original unmarked image. It can also be extracted after high quality printing and scanning with the help of a few registration marks. This scheme achieves enhanced efficiency by embedding same number of bits in each block.

C. Embedding Process

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 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.

D. Extracting Process

In extraction Procedure, user can 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.

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

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

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)



ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177 Volume 7 Issue VII, July 2019- Available at www.ijraset.com

Decode Now

IV.	RESULT
Minimum Distortion Secure binary image stegnography	Image Partitioning
Select Image CubierclastDewisastNew Image Encyptorrinputation.pg	
Encryption Process Encoding Decoding	Apply SVD
	-
🕼 Encrypted Image	Steganography Eile 9999 my name is priyanka
Hide Data Decrypt Image	priyankadahiwal9@gmail.com
	Encode Now
Steganography Eile 9999	Steganography
my name is priyanka Success! i The Image was encoded Successfully!	

9999

priyankadahiwal9@gmail.com

Encode Now





ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177 Volume 7 Issue VII, July 2019- Available at www.ijraset.com

Steganography		🚺 🛃 Steganography
Eile		Eile
Success!	I 1	9999 my name is priyanka
Encode Now		Encode Now

A. Result Analysis

Sr.no	Image	Size	No. of embeddable	MSE	MSE									
			block					MSE						
1	Baboon	200X200	255	2.6902	2.6902	2.5875	2.4902					2.6648		
2	Leena	255X255	249	2.5875				1.7569		1.7109	1,1939		1.6337	1.949
3	Leena1	256X256	221	2.4902					0.6355					
4	Cartoon1	169X257	255	1.7569										
5	D1	177X285	255	0.6355	200	255	256	257	285	204	255	225	260	276
6	Danger	247X204	241	1.7109	XOO	55X	56X	X69	77X	47X	55X	25X	94X	83X
7	cat	255X255	225	1.1939	0	N	0	1	-	Ň	N	2	1	1
8	hero	225X225	255	2.6648	Baboon	Leena	Leena1	Cartoon	1 D1	Danger	cat	hero	Image4	Image8
9	Image4	194X260	255	1.6337										
10	Image8	183X276	245	1.9490	1	2	3	4	5	6	7	8	9	10





International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177

Volume 7 Issue VII, July 2019- Available at www.ijraset.com

V. CONCLUSION

This work exploits texture of binary image and study all methods of data hiding. This work is related to data hiding. In this paper flipping distortion technique is used for minimize the distortion between pixels and select the pixel which is good to flip. Spatial domain techniques are best for some factors like visual quality. Capacity and computational complexity are common factors for both spatial and transform domain which depend on the corresponding methods.

REFERENCES

- Bingwen Feng, Wei Lu, Wei Sun, Secure Binary Image Steganography Based on Minimizing The Distortion on The Texture, Volume: 10, Issue: 2, pp.243 255 Feb. 2015
- [2] Q. G. Mei, E. K. Wong, and N. D. Memon, Data hiding in binary text documents, Proc. SPIE, vol. 4314, pp. 369375, 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. 12271231, 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. 528538, 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. 475486, Apr. 2007.
- [6] H. Yang, A. C. Kot, and S. Rahardja, Orthogonal data embedding for binary images in morphological transform domainA high-capacity approach, IEEE Trans. Multimedia, vol. 10, no. 3, pp. 339351, 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. 14411444.
- [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. 15081518, 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. 920935, Sep. 2011.
- [10] T. Pevn, T. Filler, and P. Bas, Using high-dimensional image models to perform highly undetectable steganography, in Information Hiding (Lecture Notes in Computer Science), R. Bhme, P. W. L. Fong, and R. Safavi-Naini, Eds., vol. 6387. New York, NY, USA: SpringerVerlag, Oct. 2010, pp. 161177.
- [11] V. Holub and J. Fridrich, Designing steganographic distortion using directional filters, in Proc. IEEE Int. Workshop Inf. Forensics Security, Dec. 2012, pp. 234239.











45.98



IMPACT FACTOR: 7.129







INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 🕓 (24*7 Support on Whatsapp)