Secure Binary Image Steganography Based on Huffman Coding

S Saravanan

PG Research Scholar

Mr. K Kishore KumarM.E Professor **Mr. NRajKumar M.E Assistant Associate Professor**

Vel Tech Dr.RR & Dr.SR Technical University

Abstract— **In insecure communication, data hiding techniques have an important role to protect secret information from unauthorized access. Steganography is a hiding technique that hides the secret information inside the digital medium in undetectable manner. In this paper, an secure binary steganography method based on huffman coding is proposed. First extract the complement, rotation, and mirroring-invariant local texture patterns (crmiLTPs) from the binary image first. The weighted sum of crmiLTP changes when flipping one pixel is then employed to measure the flipping distortion corresponding to that pixel.The steganographic scheme generates the cover vector by dividing the scrambled image into superpixels. The secret message is hided in cover image using Huffman coding. Experimental results have demostated that the proposed steganographic scheme can achieve statistical security without degrading the image quality or the embedding capacity.**

Keywords- Binary Image, Steganography, data hiding, huffman coding

I.Introduction

Over the last few decades, security of dataexchanged over the network has become a major concern. Twomajor techniques have existed to achieve the same, namelycryptography and steganography. Cryptography alters thestructure of the text itself whereas steganography hides the textbehind some other digitally representative media, thustransmitting it unsuspectingly. In the last decade many advances have been made inthe area of digital media, and much concern has arisenregarding steganography for digital media. Steganography [1]is a singular method of information hiding techniques. Itembeds messages into a host medium in order to conceal secretmessages so as not to arouse suspicion by an eavesdropper [2].A typical steganographic application includes covert communicationsbetween two parties whose existence is unknown toa possible attacker and whose success depends on detectingthe existence of this communication [3]. In general, the hostmedium used in steganography includes meaningful digitalmedia such as digital image, text, audio, video, 3D model [4],etc. A large number of image steganographic algorithms havebeen investigated with the increasing popularity and use ofdigital images [5], [6].

The motivation behind developing image Steganography methods according to its use in various organizations to communicate between its members, as well as, it can be used for communication between members of the military or intelligence operatives or agents of companies to hide secret messages or in the field of espionage. The main goal of using the Steganography is to avoid drawing attention to the transmission of hidden information. If suspicion is raised, then this goal that has been planned to achieve the security of the secret messages, because if the hackers noted any change in the sentmessage then this observer will try to know the hidden information inside the message.

The main terminologies used in the Steganography systems are: the cover message, secret message, secret key and embedding algorithm. The cover message is the carrier of the message suchas image, video, audio, text, or some other digital media. The secret message isthe information which is needed to be hidden in the suitable digital media. The secret key is usually used to embed the message depending on the hiding algorithms. The embedding algorithm is the way or the idea that usually use to embed the secret information in the cover message.

There are two types of domains in which the data can be hidden. In spatial domain, directly the pixel value is modified while in transform domain candidate pixels are determined based on the coefficient calculations. Transform domain techniques are more robust against attacks as compared to the transform domain techniques.

In recent years, many data hiding methods have been developed for binary images, which can be used to authenticate digitally stored handwritings, CAD graphs, signatures, and so on. Stego images obtained by these schemes have also been reported to achieve considerable visual qualities. However, these methods ignore the security against steganalyzers. The high undetectability of the secret messages can reduce the suspicion from attackers and thus enhance the security. To this end, we focus on designing a secure binary image data hiding scheme (or more strictly speaking, a steganographic scheme) by improving the undetectability while preserving the stego image quality and embedding capacity.

In this paper, a spatial domain-based binary image steganographic scheme is proposed. In the embedding phase, huffman encoding is employed to hide the secret message. the proposed steganographic scheme presents a significant performance compared with state-of-theart works.The reminder of this paper is organized as follows: Section II gives the related work of steganography. In Section III, the proposed steganographic scheme is presented. Comparison experiments among different distortion measurements and among different steganographic schemes are reported in Section IV. Finally, Section V concludes the paper.

II. Related Work

M. Guo et al [7] proposed a data hiding scheme for binary images, which includes the document type images, scanned figures text and signatures. In this data hiding scheme, embedding efficiency and the placement of embedding changes are perform simultaneously. Take M×N image block, the upper bound of the amount of bits that can be embedded of the scheme is nlog2((M×N)/ n +1) by changing n pixels. This scheme is used for embed more amount of data, as well as it maintain a better quality of image, and it has the wider applications. This data hiding scheme embed more amount of data and it will not affected the quality of the image.

H. Cao et al [8] proposed, a method for authenticating binary host images using an edge – adaptive data hiding method. Uses a simple binary image to show that EAG (edge-adaptive grid) selects good data carrying pixel locations (DCPL) efficiently in "L- shaped" patterns rather than block – based methods.

K. L. Chiew [9]proposed, a new multi-class steganalysis for binary image. This method can identify the type of steganographic technique used by examining on the given binary image. It is also capable of differentiating an image with hidden message from the one without hidden message.

Q. Mei et al.[10] propose a data hiding mechanism for document images. A pattern table is constructed containing 100 pairs of boundary patterns composed of Add and Delete patterns. 8-connected boundary following algorithm is used to get the outer boundary of a connected component and is divided into 5 pixel long segments. These are matched with the patterns in pattern table and accordingly data is embedded. For extraction same procedure is followed. This method has a good data hiding capacity but this technique is not robust to printing and scanning and hence is useful only in steganography and authentication applications.

Wu et al.[11] assign the flippability scores and give a particular rank to each pixel which is determined by observing the smoothness and the connectivity dynamically. Scores are given between the range from 0 to 1. 0 indicates no flipping. Smoothness is determined from transitions in horizontal, vertical and diagonal directions while the connectivity is determined from number of black and white clusters. Shuffling is applied to achieve the even distribution of flappable pixels in each block. Odd-even feature is imposed for extraction purpose. As odd-even feature is not compulsory in this method the number of flippable blocks get increased and hence the capacity

Guorong Xuan et al . [12], proposed a reversible data hiding method for binary images using run-length (RL) histogram modification. The binary image is scanned from left to right and from top to bottom to form a sequence of alternative black RL and white RL. Combining one black RL and its immediate next white RL, one RL couple is formed, thus generating a sequence of RL couples. In this scheme there is a threshold, T1, which is defined as such a sum of the black and white RLs within one RL couple that those RL couples, whose sum of black and white RLs is short than T1, will not be used for data embedding. The reason of doing so is to eliminate isolated white pixels (white RL being 1), which may defeat reversibility, i.e., the original image cannot be received exactly. Advantage of this method is that it can be applied to all types of binary images like text, graph, halftone, non-halftone etc. This method has good visual quality and data hiding capacity.

K Suresh Babu et al. [13] proposed Steganographic model Authentication of Secret Information in Image Steganographythat can verify the reliability of the information being transmitted to the receiver. The method can verify whether the attacker has tried to edit, delete or forge thesecret information in the stego-image. The method can verify whether each row has been modified or forged by the attacker.

S.Arivazhagan1 et al. [14] The work deals with Image steganalysis which focuses firstin identifying the employed steganographic algorithm and this information is used in deciphering any hidden data in cover images. In this work the stego images are decomposed into its approximation and detail sub bands and from the decomposed sub bands, co-occurrence and statistical features are derived. This leads to detection of steganographic algorithm

III Proposed Work

This section describe the proposed work of secure binary image steganography using Huffman Coding. The work contains two phase: Data Embedding and Data Extraction.

A. Huffman Coding

Huffman encoding is a variable length lossless compression technique and applied to any entity which represented in digital form. First secret image is encoded using Huffman coding and then resulting Huffman codes are embedded into cover image. Huffman codes are optimal codes that map one symbol of cover image to one code word. Huffmantable (HT) represents binary codes of each symbol of cover image. The Huffman table used at encoder and decoder side must be same. Thus the Huffman table is required for decoding process along with stego image. Huffman encoding is mainly used for the following three characteristics:

Lossless Compression: It ensures the preservation of actual data while compressing it.

IJSER

ISSN 2229-5518

*Increase the Security:*Huffman encoded bit stream does not discloses anything because to extract the exact meaning, the Huffman table is required.

Authentication: It provides authentication, as if any single bit changes in the Huffman coded bit stream, Huffman table will not be able to decode the data.

B. Data Embedding

The block diagram of embedding procedure is shown in Figure 1. Given a lw × lh size binary image **X**, we first divide **X** into non-overlapped blocks of size $l' \times l'$ where $l' = lC \times lJ$, where $lJ \times lJ$ is the size of the superpixel and $lC \times lC$ is the length of the cover vector.

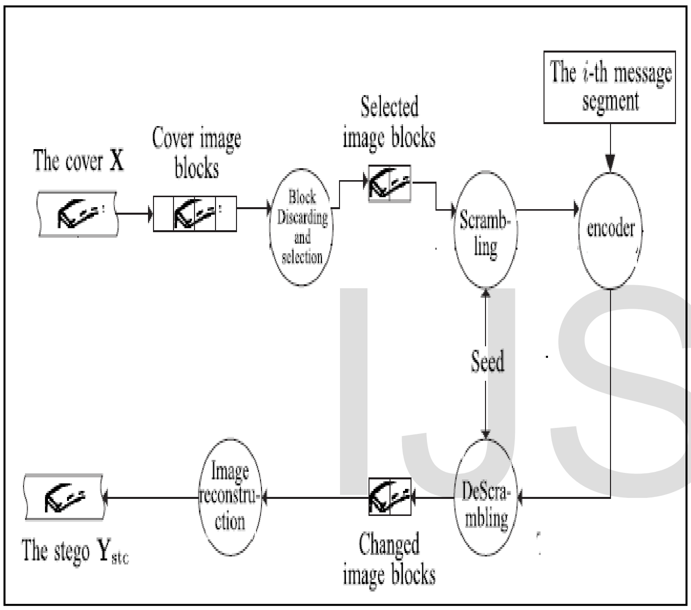

Figure 1 Data Embedding Block Diagram

The embedding procedure contains the following steps:

1. Divide **X** into non-overlapped blocks of size $l' \times l'$ where $l' = lC \times lJ$. Divide the binary message **m** into non-overlapped message segments of length lm;

2. Remove all uniform blocks (i.e all the pixels in the block is white ot black). Select all the nonuniform blocks in X.

3. Consider all the selected blocks in **X** as an ensemble **X**'. Scramble **X'** with the same scrambling seed.

4. for each selected image block the huffman coding is applied to hide the i^{th} secret message.

5. Repeat Steps 4 until all the message segments have been embedded;

6. Descramble the embedded image blocks;

7. Successively replace each nonuniform block in the cover image with the corresponded stego block to obtain the stego image **Y**stc.

C. Data Extraction

The block diagram of extraction procedure is shown in Figure 2.

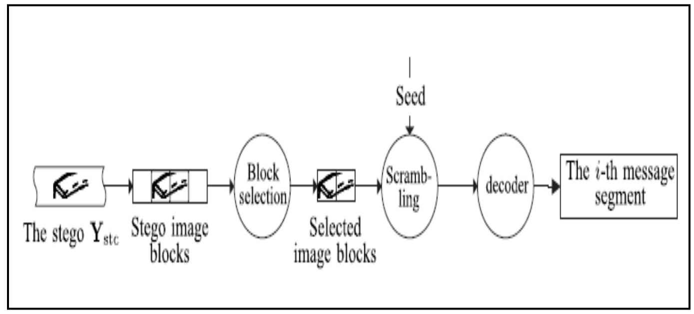

Figure 2 Data Extraction Block Diagram

The extraction of the embedded message contains the following Step:

1. Divide **Y**stc into non-overlapped blocks of size $l' \times l'$ where $l' = lC \times lJ$. Select all the nonuniform blocks;

2. Scramble the selected stego image blocks via the same scrambling described in Step 3 of the embedding procedure;

3. For each stego Block apply Huffman decoding

4. Repeat Step 3 until all the message segments have been extracted.

IV Exprimental Result

The experiments consist of "cartoon", "CAD", "texture", "mask", "handwriting", and "document" images. Most of them are acquired directly from the Google images. All the images are cropped into 256 × 256 pixels in order to discard the large blank regions. Test images are given in Fig. 3. The employed image sources cover a wide range of contents: the "texture" images look noisiest, whereas the "mask" images look smoothest.

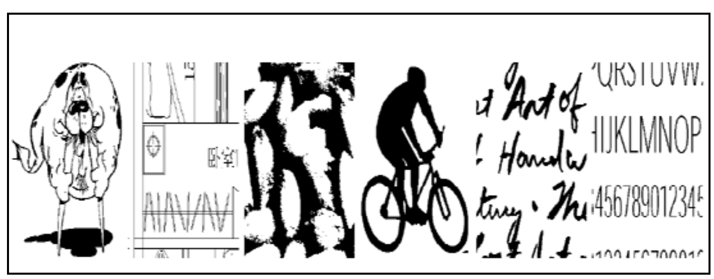

Figure 3 Sample Test Image

There are two error metrics are used to compare the differences between original image and stego image. The two

IJSER

metrics are Mean Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR)

Mean Squared Error (MSE)

MSE is the mean of the cumulative squared error between the stego and original image. Given a noise free m*n image (Original Image) and its noise approximation K (Stenography image), MSE is defined as:

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

A lower value for MSE means lesser error. So it is a target to find an image stenography scheme having a lower MSE. That will be recognized as a better stenography.

Peak Signal to Noise Ratio (PSNR)

It is a measure of the peak error. It is usually expressed in terms of the logarithmic decibel scale. PSNR is most commonly used to measure the quality of stenography image. The Signal in this case is the original data, and the noise is the error introduced by stenography. PSNR is an approximation to human perception of stenography quality. Here, MAX_I is the maximum possible pixel value of the image. When the pixels are represented using 24 bits per sample, then MAX_I =16777215(2^{24}).

$$PSNR = 10 \log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

$$= 20 \log_{10}(MAX_I) - 10 \log_{10}(MSE)$$

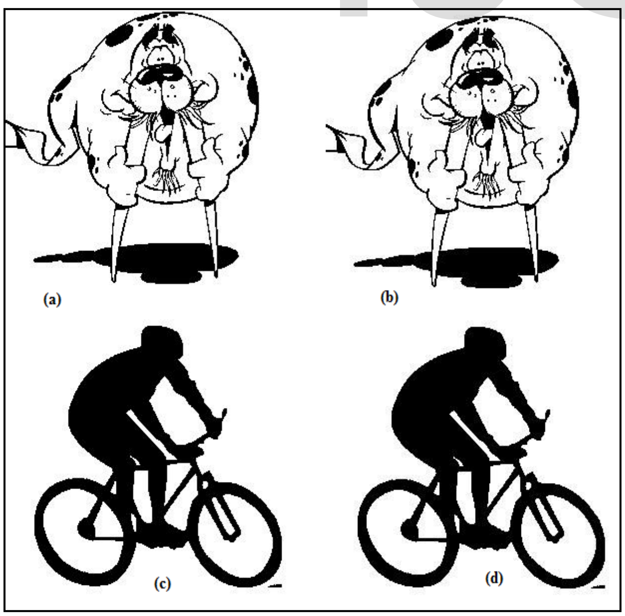

Figure 4 (a) and (c) Original Image, (b) and (d) stego image

Table 1PSNR and MSE value

Image Name	PSNR	MSE
Cartoon	33.07	32.0
CAD	35.12	20.0
Texture	32.11	40.0
Mask	34.12	20.0
Handwritten	33.35	30.0
Document Image	34.51	23

Fig 4. Shows the original and stego images of cartoon and CAD.

Table 1 shows the PSNR and MSE value of Stego Image

V Conclusion

In this paper, we exploit the texture property of binary images and propose a secure binary image steganographic scheme using Huffman Coding. Huffman encoding provides high embedded capacity and Security. The algorithm improves the security and the quality of the stego image. Result shows that the proposed method is better in compare to other existing methods. According to the results, the stego images are almost identical to the cover images and it seems very difficult to differentiate them. Experiments on the constructed imagedataset have shown that the proposed steganographic schemecan yield more secure stego images with better, at least similar,image qualities when the same length of message bits areembedded.

IJSER

REFERENCE

[1] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *Computer*, vol. 31, no. 2, pp. 26–34, 1998.

[2] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," *IEEE Security Privacy*, vol. 1, no. 3, pp. 32–44, May/Jun. 2003.

[3] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hidinga survey," *Proc. IEEE*, vol. 87, no. 7, pp. 1062–1078, Jul. 1999.

[4] Y.-M. Cheng and C.-M. Wang, "A high-capacity steganographic approach for 3D polygonal meshes," *Vis. Comput.*, vol. 22, nos. 9–11, pp. 845–855, 2006.

[5] S.-C. Liu and W.-H. Tsai, "Line-based cubism-like image—A new type of art image and its application to lossless data hiding," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 5, pp. 1448–1458, Oct. 2012.

[6] I.-C. Dragoi and D. Coltuc, "Local-prediction-based difference expansion reversible watermarking," *IEEE Trans. Image Process.*, vol. 23, no. 4, pp. 1779–1790, Apr. 2014.

ISSN 2229-5518
[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] K. L. Chiew and J. Pieprzyk, "Binary image steganographic techniques classification based on multi-class steganalysis," in Information Security, Practice and Experience. Berlin, Germany: Springer-Verlag, 2010, pp. 341–358.

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

[11] M. Wu and B. Liu,"Data hiding in binary images for authentication and annotation,"IEEE Trans. Multimedia, vol. 6, no. 4, pp. 528–538, Aug. 2000

[12] Guorong Xuan, Yun Q. Shi, Peiqi Chai, Xuefeng Tong, Jianzhong Teng, Jue Li," Reversible Binary Image Data Hiding By Run-Length Histogram Modification", IEEE, 2008

[13] K SureshBabu et. al., "Authentication of Secret Information in Image Steganography", pp. 1-6, Nov. 2008, IEEE .

[14] S.Arivazhagan,W.Sylvia Lilly Jebarani,, M.Shanmugaraj,"An Efficient Method for the Detection of Employed Steganographic Algorithm using Discrete Wavelet Transform",Second International conference on Computing, Communication and Networking Technologies, pp.1-6, 2010

IJSER

IJSER © 2016
http://www.ijser.org