International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 4, Issue 6, November - December 2015 ISSN 2278-6856

Image Steganography for data hiding Using Huffman code, Zigzag and OPAP

Ketaki Bhaskar, Mitali Bakale, Priyanka Chaure, Priti Shirke

Savitibai phule pune university, Karamveer Kakasaheb Wagh Institute of Engineering and Education Research
Department of Computer Engineering Nashik, India

Abstract

For *the purpose of security, Data hiding process embeds data into digital media. Digital image is one of the best media to stores data. It provides large capacity for hiding secrets information which results into the stego-image imperceptible to human vision, a novel Steganographic approach based on data hiding method such that pixel-value differencing. In existing approach different techniques are used such as LSB substitution method, hamming, pixel indicator based method etc. In LSB, there are constraints on image size. In proposed system, Huffman, zigzag and OPAP methods are used to overcome the limitation of the size and provide both high embedding capacity and outstanding imperceptibility for the stego-image. The text data can be embedded into the cover image. Huffman code is to compression the secret messages before sending it to the receiver. Zigzag scanning to select the pixels that will secret messages is hidden. To enhance the quality of the stego-images optimal pixel adjustment process (OPAP) is used. It also minimizes embedding error. The aim is to provide better security with high embedding capacity and a better stego-image quality than the existing system.*

Keywords: Digital image, Steganography, Zigzag scanning, Huffman method, OPAP.

1. INTRODUCTION

The Steganography is the practice of concealing a file, message, image, or video within another file message, image, or video. The word Steganography combines the Greek words “Steganos” meaning covered, protected and concealed and “Graphien” meaning writing. Generally, the hidden messages are appears to be something else: shopping lists, articles etc. the hidden messages may be in visible ink between the visible lines of private letter.

The most of the people send the secret data over the internet but internet is not more secure, there can be happen data leakage that’s why data can be lost. Therefore it is a challenge to send a data secretly up to the destination. Data hiding is basically process of embeds data into digital media for the purpose of security. For data hiding various techniques are used like a cryptography and Steganography.

The cryptography is method of storing and transmitting data in particular form so that only those for whom it is intended can read and process it. Cryptography is most often associated with scrambling plaintext into cipher text (the process called encryption), the back again (called decryption). The cryptography has some limitations like takes a long time to figure out the code and if you were to send a code to another person in past, it will take long to get o that person.

In Now a days, data hiding is very important issue computing world. The data hiding can be done by the concept of Steganography. Steganography can be defined as concealing information in ways that prevent the detection of hidden messages. The Steganography can implemented using of different kind of techniques like Least significant bit(LSB), Zigzag scanner, Huffman method, OPAP(Optimal pixel adjustment process) etc. To divert the attention of hackers the transmission of secret data should be using some other alternate method. Steganography is the field that gives a meaningful way of secure data being transmitted through an open channel without the attention of eavesdroppers.

Steganography in images can be normally done in two domains: They are, Spatial and Transform domain. The proposed system involves work in the spatial domain. First the cover image is divided into four blocks and each block is further subdivided into three planes(R, G, B).At each subdivided block pixel indicators are used. There are two types of pixel indicators used (i) Default, (ii) User Defined. Based on the indicators used in each subdivided blocks the secret data can be embedded into the LSB of cover image. The embedding process is done in Zigzag manner and the resulting image is called stego-image. The goal of the proposed system is to achieve better PSNR than the existing systems.

2. LITETATURE REVIEW

Existing approaches:

2.1 Image Steganography using LSB and LSB+ Huffman code:

In this existing, approach, the embedding information into cover of the media such as text,image, audio, and video. This existing approach uses two techniques for the Steganography (text into image) Least Significant Bit (LSB) and Least Significant Bit with Huffman code (LSB+HUFF). It uses the zigzag scanning for the two methods to increase the security, and compares the results using Peak Signal to Noise Ratio (PSNR). All images used here is a gray scale Images. But disadvantages are of this approach its having the image size restriction and here is used only gray scale image.

2.2 ZIG-ZAG PVD – A Nontraditional Approach :

Image hiding is method in which a secret text is hidden in a cover image thereby forming a stego image. In this existing approach, data hiding is performed by taking difference value of three and two neighboring pixels by adapting Zigzag traversing scheme (ZZTS). This method enhances security and the quality of image in spite of high capacity of concealed information. Error correction mechanism using hamming code is applied to ensure reliable secret communication. The effectiveness of the proposed stego system has been estimated by computing Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Mean Structural similarity index (MSSIM) and Bits per color Pixel. It does not give better quality of image. So that is the limitation of this approach.

2. 3 Analysis of data hiding using Digital Image Signal Processing :

Digital image is one of the best media to store hidden data. It provides large capacity for hiding secret information which results into stego-image indiscernible to human vision, that novel Steganographic approach based on data hiding method such as pixel-value differencing. This method provides both high embedding capacity and outstanding indiscernible for the stego-image. In this approach, different image processing techniques are described for data hiding related to pixel value differencing. Pixel Value Differencing based techniques is carried out to produce modified data hiding method. Hamming is an error correcting method which is useful to hide some information where lost bit are detected and corrected. OPAP is used to minimize embedding error thus quality of stego-image is improved without disturbing secret data. Zigzag method enhances security and quality of image. In modified method Hamming, OPAP and Zigzag methods are combined. In adaptive method image is divided into blocks and then data will be hidden. Objective of the proposed work is to increase the stego – image quality as well as increase capacity of secret data.

2.4 Image Steganography using Zigzag, Huffman code and OPAP :

Data hiding process embeds data into digital media for the purpose of security. Digital image is one of the best media to accumulate the data. It provides large capacity for hiding secret information which results into stego-image indiscernible to human vision, a novel Steganographic approach based on data hiding method such as pixel-value differencing. In existing approach different techniques are used such as LSB substitution method, hamming, pixel indicator based method etc. In LSB, there are constraints on image size. In proposed system, Huffman, a zigzag and OPAP method are used to overcome the limitation of the size and provides both high embedding capacity and outstanding indiscernible for the stego-image. The text data can be embedded into the cover image. Huffman code is to compression the secret messages before sending it to the receiver. Zigzag scanning to select the pixels that will secret message is hidden. To enhance the quality of the stego-images optimal pixel adjustment process (OPAP) is used. It also minimizes embedding error. The aim is to provide better security with high embedding capacity and a better stego-image quality than the existing system.

3.PROPOSED METHOD

In proposed system, the combinations of Huffman, a Zigzag and OPAP method are used to image Steganography. The following figure shows the block diagram of proposed system. Also here described all algorithm one by one as follows:

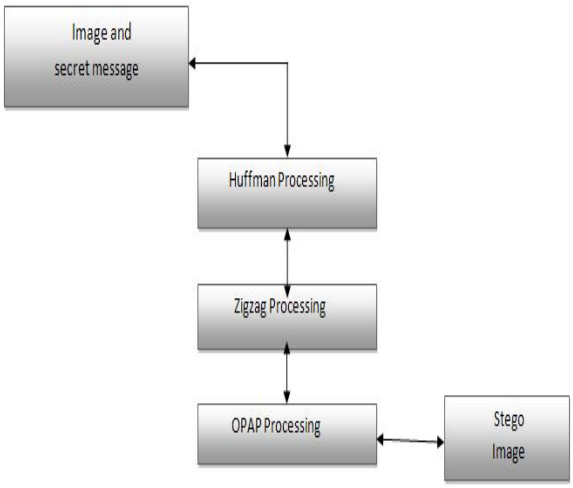

Figure 1. Block diagram

In above figure 1 shows the processing of image steganography. Basically in above figure shows that, firstly cover image and secret text will be accept after on that image Huffman algorithm will be applied and it will provide the quick tree generation then output of Huffman algorithm will provide to Zigzag algorithm as a input then zigzag algorithm scan the coefficients of image scan by zigzag manner. After that output of zigzag algorithm will provide to OPAP algorithm as a input then OPAP will do the minimize the error and after all processing will create the stego image. And its will all about the encryption processing we can also decrypt the image by reverse processing.

3.1 Huffman code

This is the first phase of Steganography to convert the image into Zigzag method. The algorithm is described by david Huffman assigns every symbol to a leaf node of a binary code tree. These nodes are weighted by the number occurrences of the corresponding symbol called frequency or cost.

The tree structure results from combining the nodes step-by-step until all of them are embedded in a root tree. The algorithm always combines the two nodes providing the lowest frequency in the bottom up procedure. The new

interior nodes get the sum of frequencies of both child nodes.In following figure, the branches of the tree represent the binary values 0 and 1 according to the rules for common prefix-free code trees. The path from the root tree to the corresponding leaf node defines the particular code word. Basically the Huffman code is used for data compression and optimization using the frequencies of Binary tree. The output of Huffman code method gives the input to the Zigzag method. This phase basically first apply on cover image.

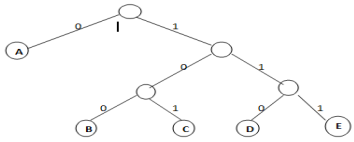

Figure 2. Huffman tree

3.2 Zigzag method

This is the second phase of Steganography and it accepts the input from the Huffman code. Zigzag algorithm is used for scanning in Zigzag manner. The coefficient scanning plays an important role in block-based image and video coding standards, such as JPEG, MPEG etc. in this coding standards method, the Zigzag method is used for image or frame coding. The Zigzag method scans the coefficients of image.

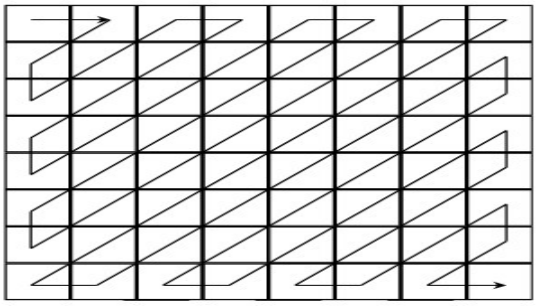

Figure 3. Zigzag scanning

This method enhances security and the quality of image instead of high capacity of concealed information. Zigzag PVD uses the difference of each pair of pixels to determine the number of message bits that can be embedded into that pair of pixel. It starts at the upper-left corner of the Cover image and scans the image in a Zigzag manner.

3.3 OPAP:

The OPAP stands for optimal pixel adjustment process. This OPAP algorithm is help for minimization error. The OPAP take output of Zigzag phase as input. And the output of OPAP will be Stego image.

4. CONCLUSION

In a proposed method, we saw the concept of Steganography and how it is used to data hiding to an image. Here we used the combinational method like a Huffman code, Zigzag and OPAP. The contributions of the proposed method are summarized as follows: the cover image accept the text image then applied on Huffman code to tree generation and compression after that whatever the output of Huffman code gave to input as Zigzag method for scanning then output of Zigzag method gave to input as OPAP for minimize the error after that finally we got stego image and this process for encrypt the stego image also we done decryption of stego image into cover image by going reverse order.

5. FUTURE SCOPE

In previous method Steganography just used for only hide the image but future scope of this proposed method is that doing the Steganography on also videos that's why the security will be increase more in the computing world.

REFERENCES

[1] "Image Steganography using the LSB and LSB+ Huffman code", Wa'el Ibrahim A. Aqaba university college, Aqaba-Jordan

[2] "Zigzag pixel indicator based on the secret of data hiding method" ,P. Mahimah, Mrs. R. Kulakarni, Anna university, Chennai, India

[3] "A Steganographic method based upon JPEG and quantization table modification", National Chung cheng university, Taiwan

[4] "Highly secured and randomized images Steganographic algorithm", Dr. R. Sridevi, JNTUH, Hyderabad

[5] "Pixel Values of Differencing a Steganographic method: A Survey", Jagruti salunke and sumedha sirsikar, university of pune

[6] ZIG-ZAG PVD – A Nontraditional Approach", M.padma Dr. Y. Venkataramani, Trichy

[7] Lip Yee Por, Delina Beh,Tan Fong Ang and Sim Ying Ong "An Enhanced Mechanism for Image Steganography Using Sequential Color Cycle Algorithm" The International Arab Journal of Information Technology, 2013

[8] Adem Orsdemir, H. Oktay Altun, Gaurav Sharma and Mark F. Bocko, "steganalysis aware steganography: statistical indistinguishability despite high distortion", SPIE-IS&T, Vol. 6819, 2008, pp.1 -9.

[9] Ahmad T. Al-Taani and Abdullah M. AL-Issa, "A Novel Steganographic Method for the Gray-Level Images", International Journal of Computer, Information, Systems Science and Engineering 3:1 2009

[10] *[10]* Alvaro Martín, Guillermo Sapiro and Gadiel Seroussi, "Is

[11] Image Steganography Natural", IEEE Transactions on the Image Processing, Vol.14, 2005, pp. 2040-2050