A PRACTICAL APPROACH FOR EFFICIENT STEGANOGRAPHIC HIDING CAPACITY IN IMAGE USING MATLAB

Kanta[1], Kavita Khatkar [2]

[1]M.Tech, (CSE), JCDM College of Engineering, Sirsa, India

[2]Asst Professor (CSE), JCDM College of Engineering, Sirsa, India

ABSTRACT

The research work is about the study and implementation of steganography techniques and provides the approach of security with the combination Data Compression techniques to improve the Steganographic capacity. The transmission of information need to be secure over the network and confidentiality of information is main aspect for the critical information. This paper proposed the approach for security of information which includes the Data Compression Steps and steganography techniques for Data compression and hiding of data. This research work provides a new way of securing the information to avoid hassle in transmission over network high capacity data hiding techniques. This paper has been implemented the Huffman coding scheme with Steganographic method to hide the more data in smaller image and provides the more accuracy.

Keywords- Cryptography, Digital Media Images, Digital Signatures, Hidden Communication, Steganography

I. INTRODUCTION

1.1 Information Security and Steganography

Computer and network security have some requirements that should be addressed in order to get secure systems. Thus, in order to determine the performance of a security technology, three key concepts should be analyzed:
Confidentiality deals with protecting, detecting, and deterring the unauthorized disclosure of information". The main goal of cryptography is to garble a plaintext message in such a way that only the intended recipient can read it. This is precisely the goal of confidentiality.

a. Integrity deals with preventing, detecting, and deterring the unauthorized modification of information". An integrity attack is potentially more dangerous than a confidentiality attack. Cryptography addresses integrity by performing a digital signature check across information.
b. Availability relates to preventing, detecting, or deterring the denial of access to critical information". Cryptography can prevent confidentiality and integrity attacks, but it cannot prevent availability attacks.

   In addition to the three key concepts of security, two other security goals are critical relative to cryptography: authentication and non-repudiation.

a. Authentication: In most transactions you need to be able to authenticate or validate that the people you'redealing with are who they say they are.

b. Non-repudiation deals with the ability to prove in a court of law that someone sent something or signed something digitally. Without non repudiation, digital signatures and contracts would be useless.

1.2 Steganography

Steganography is the art of hiding information imperceptibly in a cover medium. The word "Steganography" is of Greek origin and means "covered or hidden writing". The main aim in steganography is to hide the very existence of the message in the cover medium. Steganography includes a vast array of methods of secret communication that conceal the very existence of hidden information. Traditional methods include use of invisible inks, microdots etc. Modern day steganographic techniques try to exploit the digital media images, audio files, video files etc.

1.3 Steganography differs from cryptography

- Steganography Hide the messages inside the Cover medium, many Carrier formats.
- Cryptography Encrypt the message before sending to the destination, no need of carrier/cover medium.

As mentioned, steganography deals with hiding of information in some cover source. On the other hand, Steganalysis is the art and science of detecting messages hidden using steganography; this is analogous to cryptanalysis applied to cryptography. The goal of steganalysis is to identify suspected packages, determine whether or not they have a payload encoded into them, and, if possible, recover that payload. Hence, the major challenges of effective steganography are

1.4 Security of Hidden Communication

In order to avoid raising the suspicions of eavesdroppers, while evading the meticulous screening of algorithmic detection, the hidden contents must be invisible both perceptually and statistically.

1.5 Size of Payload

Unlike watermarking, which needs to embed only a small amount of copyright information, steganography aims at hidden communication and therefore usually requires sufficient embedding capacity. Requirements for higher payload and secure communication are often contradictory.

The majority of today's Steganographic systems uses multimedia objects like image, audio, video etc as cover media because people often transmit digital pictures over email and other Internet communication.

1.6 Steganography Techniques

There are number of steganography techniques which are used for keep the information secure and confidential but the basic concept behind every technique is demonstrated as:

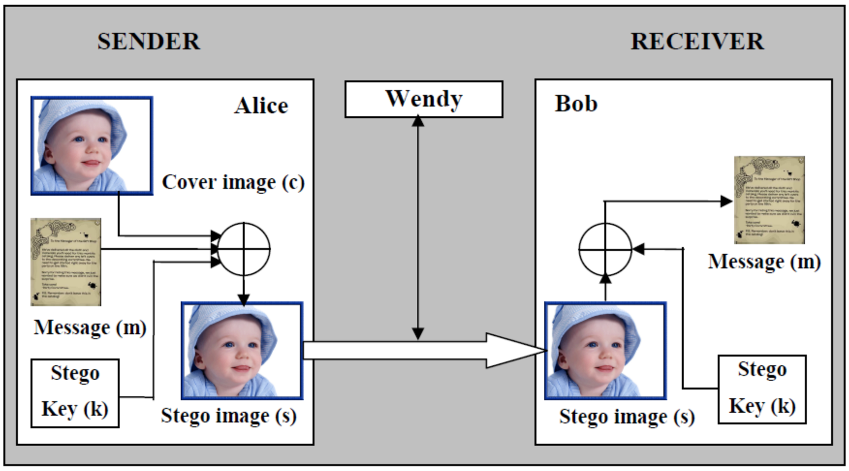


Figure 1: basic steganography principal

Encapsulate secret Message in Text File

Encapsulation means Encode the secret information in a text or text file for keep the information secure. The text file in which information has been hiding is small in size and decoding of information can be crack easily. There are some methods for accomplish the text based steganography.

i. **Line-shift encoding**

This (LSE) method shifts the each line of text in the order vertically or horizontally and as per measurement of existing Stationary line.

ii. **Word-shift encoding**

This (WSE) technique of Word-shift encoding is likely to be same as line-shift encoding but it has some changes which includes horizontal spaces between words to equate a value for the hidden message.

iii. **Feature Specific Encoding**

Feature specific encoding (FSE) involves encoding secret messages into formatted text by changing certain text attributes such as vertical/horizontal length of letters such as b, d, T, etc.

II. LITERATURE SURVEY

[1]Teng, C.Y. Shiau, Y.H. Chen, C.C. (2010), “A data hiding algorithm based on histogram re-quantization”, Publication Year: 2010 , Page(s): 1088 – 1091

Steganography, a technique of data hiding, is becoming more and more significant with expansion of the Internet communication. As a result, various steganographic algorithms have been proposed in recent years, for example, Ni et al. have carried out a lossless data-hiding algorithm based on the histogram modification. In order to reinforce more security and more data embedding capacity, this paper extends the Ni's algorithm with a random permutation and a histogram re-quantization. To begin with, applying a random permutation, the security is not easy to be broken by a brute-force attack. In addition, the embedding capacity is able to be strengthened approximately 3 times by adopting a histogram re-quantization. As to our approach, it is visually indistinguishable between a cover image and a stego image with a large embedding capacity.

[2]Christaline, J.A. Vaishali, D.(2011), "Image steganographic techniques with improved embedding capacity and robustness", IEEE, Publication Year: 2011 , Page(s): 97 – 101

Secured data transmission over computer networks can be achieved through steganography. In specific, Image Steganography entails the opportunity of hide any secret information into images. This paper presents the implementation of two image steganographic techniques in MATLAB. The first is a filter method to embed text information into image and new methods have been demonstrated to increase the information embedding capacity in the same domain. The second method is the wavelet transform method which proves to be more secured than any other method of image steganography.

[3]Parah, Shabir A. Sheikh, Javaid A. Bhat, G.M., "Data hiding in intermediate significant bit planes, a high capacity blind steganographic technique", Publication Year: 2012 , Page(s): 192 – 197.

The availability of relatively inexpensive digital products coupled with the promise of higher bandwidth and quality of service (QoS) for both wired and wireless communication networks have made it possible to create, replicate, transmit, and distribute digital data without any loss in quality. In such a scenario steganography has received huge attention from the research community round the globe, as it has been found useful for information security and under cover communication. Stegnography refers to covert communication for transfer of confidential information over a communication channel. This paper presents a high capacity stegnographic technique in which secret data is embedded in Intermediate Significant Bit planes of the cover image. The data to be embedded is broken down in blocks of relatively decreasing lengths and each block is embedded in the cover media under control of a highly secure key. This work shows attractive results with respect to imperceptibility and capacitywhen compared with a few reported techniques in addition to providing adequate data security.

[4]Feng, B. Lu, W. Sun, W., "Secure Binary Image Steganography Based on Minimizing The Distortion on The Texture", Publication Year: 2014 , Page(s): 1

Most state-of-the-art binary image steganographic techniques only consider the flipping distortion according to the human visual system (HVS), which will be not secure when they are attacked by steganalyzers. In this paper, a binary image steganographic scheme that aims to minimize the embedding distortion on the texture is presented. They 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. By testing on both simple binary images and the constructed image dataset, they show that the proposed measurement can well describe the distortions on both visual quality and statistics. Based on the proposed measurement, a practical steganographic scheme is developed. The steganographic scheme generates the cover vector by dividing the scrambled image into super pixels. Thereafter, the syndrome-trellis code (STC) is employed to minimize the designed embedding distortion. Experimental results have demonstrated that the proposed steganographic scheme can achieve statistical security without degrading the image quality or the embedding capacity.

[5]Sirsikar, S.Salunkhe, J., "Analysis of Data Hiding Using Digital Image Signal Processing", Publication Year: 2014 , Page(s): 134 – 139

Data hiding process embeds data into digital media for the purpose of security. Digital image is one of the best media to store data. It provides large capacity for hiding secret information which results into stego-image imperceptible to human vision, a novel steganographic approach based on data hiding method such as pixel-value differencing. This method provides both high embedding capacity and outstanding imperceptibility for the stego-image. In this paper, 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. Result analysis compared for BMP images only, with calculation of evaluation metrics i.e. MSE, PSNR and SSIM...

III. OBJECTIVES

1. To implement and analyze the improved steganographic capacity algorithms.
2. To measure the capacity of improved algorithm.

IV. PROBLEM FORMULATION AND METHODOLOGY

4.1 Need and significance

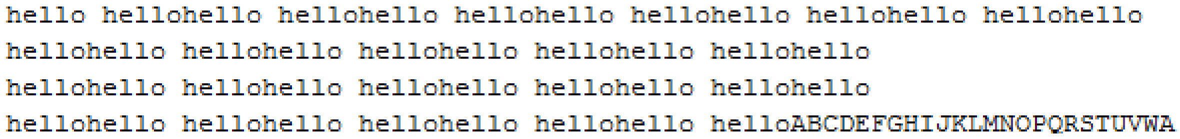
There has been a great concern about preserving the intellectual property rights of digital media such as text, image, audio, and video. Another concern regarded the ban of using encryption techniques on the Internet. This has significantly motivated the interest in information hiding techniques over the recent years. Additionally, the growing concern about the ease of copying, reproducing, and theft of digital works has motivated and increased the interest of publishing and broadcasting industries in watermarking and authentication techniques. Cryptography converts the secret information into a scrambled code in such a way that only the intended recipient, who has the decoding key, can read this secret message. Furthermore, a third party can tell that a secret message has been sent from one party to another but he/she cannot read this message. However, Steganography hides the very existence of this secret message. Thus, a third party cannot even know that a secret message has been embedded within a stego file or sent over a network. Using encryption, the size of the secret message is not an issue but it represents a significant challenge for steganography since the size of cover files (i.e. image) mostly restricts the steganographic capacity. Embedding a secret message in a cover image may change or modify some characteristics of this cover image and therefore attract the eavesdroppers' attention. Thus, the steganographic capacity and stego image imperceptibility are the most important aspects of image-based steganographic systems. Hiding more data within a given cover image makes the stego image more suspicious and therefore more detectable. Therefore, there is a kind of tradeoff between the steganographic capacity and the stego image imperceptibility

4.2 Research Methodology

1. To Understand the Various Concepts of Steganography.
2. To analyze the usefulness of Steganographic Capacity.
3. Study the Techniques for Improving Capacity.
4. Identify the problems in existing techniques and Methods.
5. Design an efficient technique to improve Capacity.
6. Develop the Algorithm in any programming language to demonstrate the real scenario.
7. Analyze the Results.

V. RESULTS & DISCUSSIONS

Figure 2: input data



```
hello hellohello hellohello hellohello hellohello hellohello hellohello
hellohello hellohello hellohello hellohello hellohello
hellohello hellohello hellohello hellohello hellohello
hellohello hellohello hellohello hellohello helloABCDEFGHIJKLMNOPQRSTUVWA
```

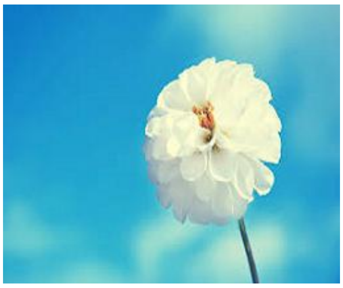
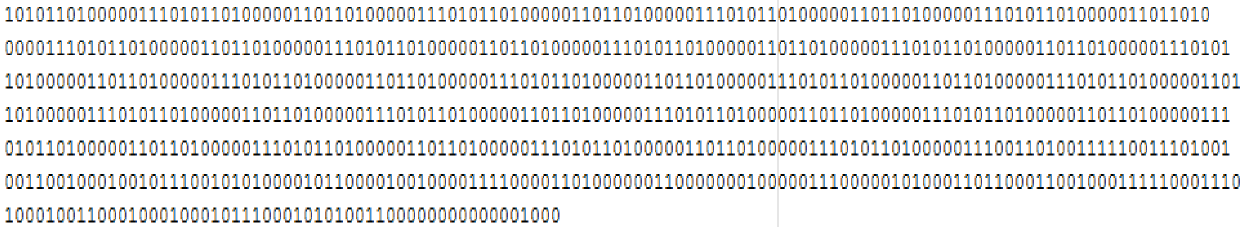
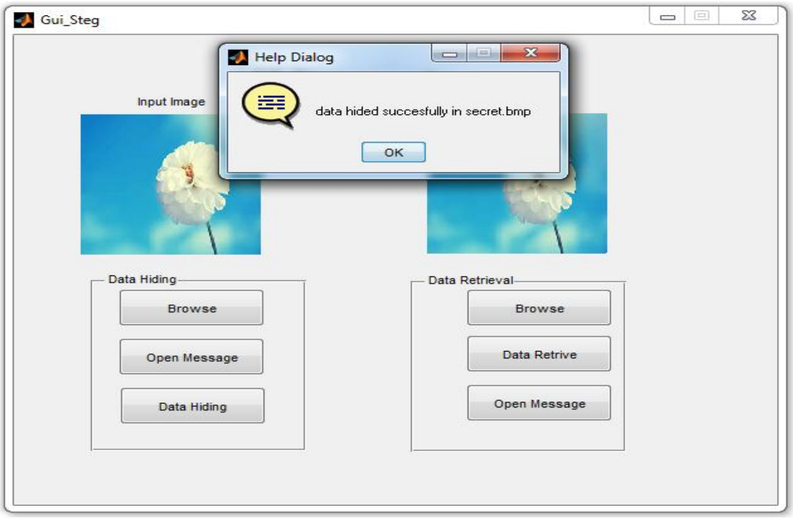


Figure 3: input image



```
10101101000000111010110100000011011010000001110101101000000110110100000011101011010000001101101000000111010110100000011011010
00000111010110100000011011010000001110101101000000110110100000011101011010000001101101000000111010110100000011011010000001110101
101000000110110100000011101011010000001101101000000111010110100000011011010000001110101101000000110110100000011101011010000001101
10100000011101011010000001101101000000111010110100000011011010000001110101101000000110110100000011101011010000001101101000000111
010110100000011011010000001110101101000000110110100000011101011010000001101101000000111010110100000011100110100111110011101001
00110010001001011100101010000010110000100100001111000011010000000110000000100000111000001010001101100011001000111110001110
1000100110001000100010111000101010011000000000000001000
```

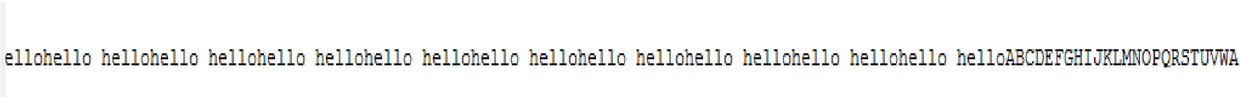
Figure 4: input data converted using huffman coding



data hided succesfully in secret.bmp

Figure5: Huffman coded data hiding in image

Figure6: secret image with data



```
ellohello hellohello hellohello hellohello hellohello hellohello hellohello hellohello hellohello helloABCDEFGHIJKLMNOPQRSTUVWA
```

Figure7: output after extraction and dehuff

VI. CONCLUSION

In this work we explored the existing image steganography techniques. We proposed an efficient image steganography technique. In image steganography, image is used as a carrier for transmission of the secret information or data. The image used can be either gray scale or color image. In this technique data is firstly preprocess using Huffman Coding. This preprocessing reduces the size of the data by a significantly great amount. This preprocessed data is then embedded into the LSBs of the pixels of the image depending upon the intensity of the pixel values. Our proposed algorithm is targeted to achieve very high image embedding capacity into the cover image and more security of the secret data.

REFERENCES

[1] Teng, C.Y. Shiau, Y.H. Chen, C.C. (2010), "A data hiding algorithm based on histogram re-quantization",Publication Year: 2010 , Page(s): 1088 – 1091

[2] Christaline, J.A. Vaishali, D.(2011), "Image steganographic techniques with improved embedding capacity and robustness", IEEE, Publication Year: 2011 , Page(s): 97 – 101

[3] Parah, Shabir A. Sheikh, Javaid A. Bhat, G.M., "Data hiding in intermediate significant bit planes, a highcapacity blind steganographic technique",Publication Year: 2012 , Page(s): 192 – 197.

[4] Feng, B. Lu, W. Sun, W., "Secure Binary Image Steganography Based on Minimizing The Distortion on The Texture", Publication Year: 2014 , Page(s): 1

[5] Sirsikar, S. Salunkhe, J., "Analysis of Data Hiding Using Digital Image Signal Processing",Publication Year: 2014 , Page(s): 134 – 139

[6] Asad, M. Gilani, J., "Khalid, A, "An enhanced least significant bit modification technique for audio steganography", Computer Networks and Information Technology (ICCNIT), 2011 International Conference, 2011 , Page(s): 143 - 147

[7] Shahadi, H.I. Jidin, R., "High capacity and inaudibility audio steganography scheme Information Assurance and Security (IAS)", 2011 Page(s): 104 - 109

[8] Balgurgi, P.P. Jagtap, S.K., "Intelligent processing: An approach of audio steganography", Communication, Information & Computing Technology (ICCICT), 2012, Page(s): 1 – 6

[9] Shah, P. Choudhari, P. Sivaraman, S.,"Adaptive Wavelet Packet Based Audio Steganography using Data History", Industrial and Information Systems, 2008. ICIIS 2008. IEEE, 2008, Page(s): 1 – 5

[10] Arvind Kumar , Km. Pooja (2010), "Steganography- A Data Hiding Technique".