International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04 | Apr-2016 www.irjet.net p-ISSN: 2395-0072

AUGMENTATION OF SECURITY AND EMBED THE CAPACITY THROUGH HUFFMAN CODING IN STEGANOGRAPHY

SMT. ARPITA S H [1], SONALI P [2], RAJESHWARI S [3], RANJEETA M[4], SHEEGOURI[5]

[1]ASSISTANT PROFESSOR DEPT OF ECE KLS VDRIT HALIYAL, KARNATAKA, INDIA
[2345]STUDENT DEPT OF ECE KLS VDRIT HALIYAL

Abstract - *In this work to enhance the data security and embedding capacity we incorporated Static Huffman coding algorithm in digital image Steganography. Data is compressed by Static Huffman compression technique and then embedded in digital image using LSB technique and Watermarking. The security is enhanced providing a three layer protection. Primarily by Static Huffman compression technique. At the second stage security is provided by LSB Watermarking technique and at last y using a secret key.*

Key Words: **Steganography, Huffman coding, Stego image.**

1.INTRODUCTION

The present work shows that in steganography the embedding of compressed data is done through static Huffman coding. The native meaning of word "steganography" is hidden writing and is originated from the Greek language. Steganography is the art and science of hiding communication; a steganographic system thus embeds hidden content in unremarkable cover media. The basic advantage of steganography is to keep the unwanted persons or intruders away from the actual fact and this technique is successful since they are not able to see the hidden message and only cover is visible.

In ancient times, Greek soldiers engraved their message on the wood and pasted it with wax to hide it and messages were hidden on the back of wax writing tables, written on the stomachs of rabbits, or tattooed on the scalp of slaves.

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. Modern steganography uses the opportunity of hiding information into digital multimedia files and also at the network packet level.

The most common method employed in steganography is the LSB substitution method in which two or three bits are replaced by the bits of the secret message so that distortion is not visible by human eyes but they are unable to give high embedding capacity and because of the same pattern, steganalysis techniques can detect them.

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. Modern steganography uses the opportunity of hiding information into digital multimedia files and also at the network packet level.

2. Related Work

The popular concept in steganography is to hide the secret message in digital images by changing the

least significant bits of the pixels. Deepshikha Chopra and et al.[] explained about Image Watermarking using Least Significant Bit (LSB) algorithm for embedding the message/logo into the image and also its different security issues have been explained. Rosziati Ibrahim and et al. [] proposed a SIS (Steganography Imaging System) here the secret message was converted into binary codes and then embedded two bits in each pixel. Xin Liao and et al.[] explained a novel steganographic method based on four-pixel differencing and modified least significant bit (LSB) substitution to improve the embedding capacity and provide imperceptibility. The average difference value of a four-pixel block is exploited to classify the block as a smooth area or as an edge area. Secret data are hidden into each pixel by the k-bit modified LSB substitution method, where k is decided by the level which the average difference value falls into. Readjustment will be executed to guarantee the same level that the average difference value belongs to before and after embedding, and to minimize the perceptual distortion. By proving that the readjusting procedure works, a theoretical proof is given to justify the method succeeded in embedding and extracting.

2.1 Huffman Coding

The aim of data compression is to represent an information source (e.g. a data file, a speech signal, an image, or a video signal) as accurately as possible as using the fewest number of bits. There are two compression techniques commonly used

1. Lossless compression
2. Lossy compression

Huffman encoding is an algorithm or lossless data compression that represents data in fewer bits than otherwise needed. Huffman coding needs to prepare a code word table that contains the information of mapping data between real data and the code words for encoding. There are two types of Huffman coding methods: static Huffman is coding and adaptive Huffman coding. Static Huffman coding uses a known code word table for encoding. While, Adaptive Huffman coding uses an encoding tree which is adaptively constructed and maintained at sender as well as receiver side. Here we use static Huffman coding in our algorithm.

Huffman coding is based on frequency of occurrence of a data item. The principle is to use a lower number of bits to encode the data that occurs more frequently []. The average length of a Huffman code depends on the statistical frequency with which the source produces each symbol from its alphabet. A Huffman code dictionary [], which associates each data symbol with a codeword, has the property that no code-word in the dictionary is a prefix of any other codeword in the dictionary [20]. The basis for this coding is a code tree according to Huffman, which assigns short code words to symbols frequently used and long code words to symbols rarely used.

2. RESULT

Result Images

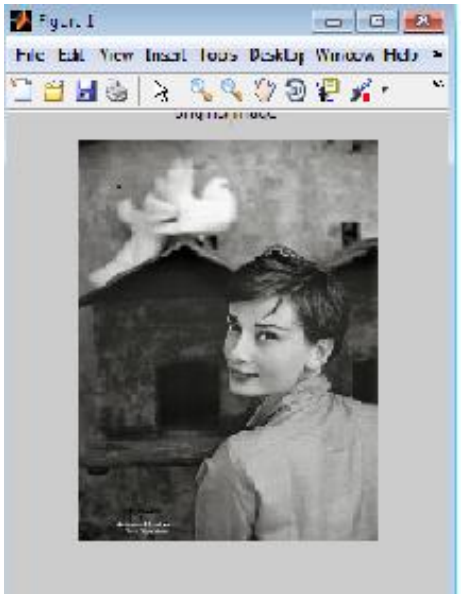

Fig -1: Cover Image

Fig 1 represents an input cover image which is a gray scale image with JPEG extension. This image is used as one of the input in LSB Embedding process where all its pixel values are extracted

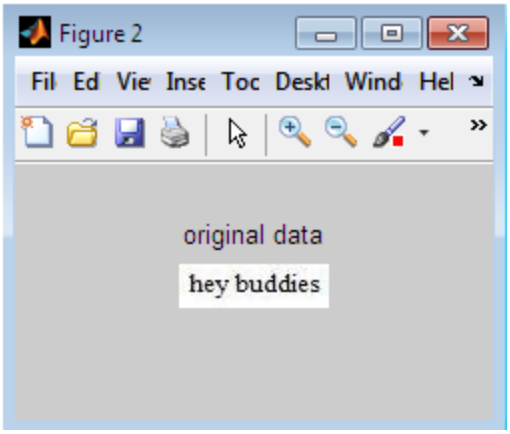

Fig -2 : Original Data

Fig 2 indicates the secret data, in order to reduce the size of the secret data we compress it using Static Huffman coding.

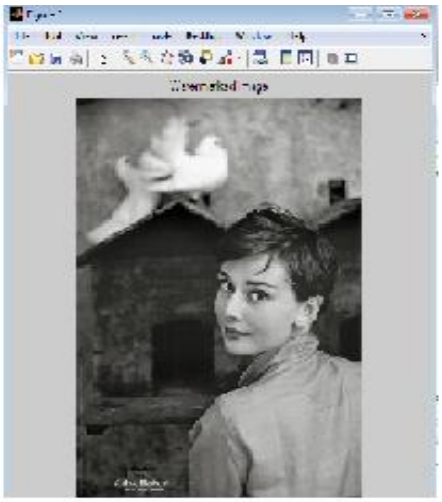

Fig -3 : Stego Image

After compressing the secret data and embedding it into the least significant bits of the cover image using LSB based Watermarking technique we obtain a Watermarked Image as shown in Fig 3.

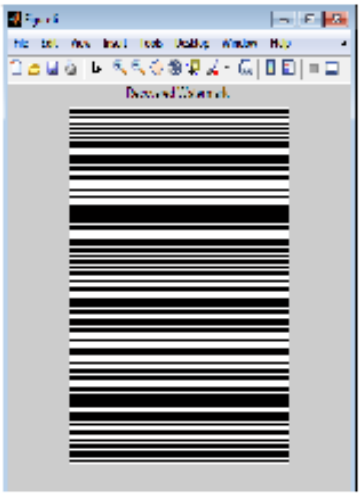

Fig -4: Recovered Watermark Image

In the process of extraction of secret data, we pass our watermarked image through the reverse LSB Watermarking technique, its output is the secret data which is as shown in the Fig 4. It also consists of some noise.

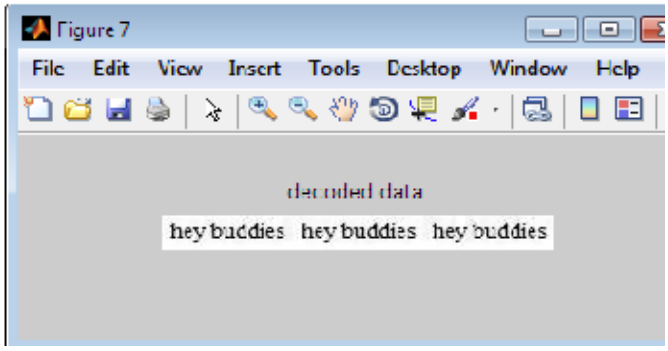

Fig -5: Output Decoded Data

3. CONCLUSIONS

In this paper, we aim to hide the very existence of the secret data in the cover image. It is successfully achieved using LSB Watermarking technique, which is one of the Steganographic techniques. Also we provide the security for the secret data, which is successfully achieved by providing a three layer security which includes Huffman Compression at the first stage, followed by a secret key usage at the second stage and at the third stage LSB watermarking technique is used.

REFERENCES

[1] D. Kornack and P. Rakic, "Cell Proliferation without Neurogenesis in Adult Primate Neocortex," Science, vol. 294, Dec. 2001, pp. 2127-2130, doi:10.1126/science.1065467.

[2] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[3] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[4] K. Elissa, "Title of paper if known," unpublished.

BIOGRAPHIES

SMT. ARPITA S H

ASSISTANT PROFESSOR DEPT OF ECE KLS VDRIT HALIYAL, KARNATAKA, INDIA

Shrigouri N

STUDENT DEPT OF ECE KLS VDRIT HALIYAL

Sonali A Patwardhan

STUDENT DEPT OF ECE KLS VDRIT HALIYAL

Ranjeeta Mujumdar

STUDENT DEPT OF ECE KLS VDRIT HALIYAL

Rajeshwari N Shelawadi

STUDENT DEPT OF ECE KLS VDRIT HALIYAL