Steganography for Hiding Two Different Kinds Of Text Message In An Image.

R. Kiruthika

Abstract: Information security is a critical issue in this digitalized world. Steganography is the art of hiding the fact that communication is taking place, by hiding information in another media. Data embedding has also been found to be useful in concealed communication, or Steganography. The goal was and still is to convey messages under cover, concealing the very existence of information exchange. There have been many steganographic techniques available for hiding message in image having its own strength and weakness. The chosen media for this system are Jpeg images. This paper will focus on hiding the text message in the Least Significant Bit of the different blocks of a Jpeg image. We discuss results obtained from evaluating available steganographic techniques and compare the different methods according to the susceptibility.

Keywords: Steganography, LSB, Embedding, Extraction

I. Introduction

Steganography is the art and science of writing hidden messages in such a way that no one apart from the recipient knows the existence of the message [1]. The earliest methods include cave drawings, smoke signals, and drums. As more and more communication is conducted electronically, new needs, issues and opportunities are born. We want to keep the message secret. A common solution to this problem is encryption and decryption. Steganalysis is processed to detect of the presence of Steganography. In this method the secret message is embedded into the image. The three parameters of the hidden process is named as [2]

- Embedding time.
- Extraction time.
- Offset from the original text.

All steganographic methods concept is to achieve the minimal amount of time for text embedding and extraction for the execution to reduce the probability of error. However, the image will not be changed and looks like the original after embedding the text.

II. Steganography and Cryptography

In cryptography, the system is broken when the attacker can read the secret message. Breaking a steganographic has two stages:

1. The attacker can detect that Steganography has been used.
2. Additionally, he is able to read the embedded message.

III. Types of Steganography

Steganography can be classified into various types, depending upon the cover medium used. Cover medium may be text, image, audio or video file. So Steganography can be said occur in three major types:

i) Text Steganography

ii) Image Steganography

iii) Audio / Video Steganography

IV. Hiding Information in JPEG Images

JPEG images are commonly used for the text Steganography in most of the current research. The JPEG image format customized a discrete cosine transform (DCT) to successive two 8x8 blocks of pixel of the image. The hidden message was embedded into the least significant bits of the two blocks of the image of the quantized DCT coefficients [4]. Recently, many different Steganography techniques proposed a method to hide text in JPEG image. A number of techniques are classified steganographic system is the best way to secure short message in the image. In our system, first our cover image was divided into two blocks of pixel and in each blocks of pixel a text message was embedded in the least significant bits of the blocks and image was merged after hiding the text to get the original cover image.

R.Kiruthika is working as an Assistant Professor in Department of Master of Computer Applications of KLNCE, Tamil Nadu. Email: kirthi_kirthi2@yahoo.com

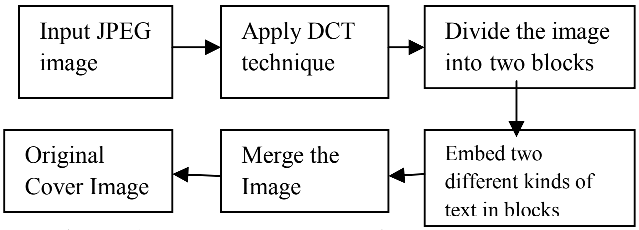
Input JPEG image
Apply DCT technique
Divide the image into two blocks
Embed two different kinds of text in blocks
Merge the Image
Original Cover Image

Figure 1:- Proposed Embedding Model

Steganography in spatial domain, targets specific locations in the image. But when intensity information is modified, then the embedded data becomes undetectable. So there is necessity of frequency domain Steganography. Our proposed system was divided into two modules:

1. Embedding
2. Extraction

V. Embedding Phase

Originally it was believed that text message embedding using Steganography would not be possible to use with JPEG images, for the time being they use lossy compression which results in parts of the image data being changed. The theory behind this method is analyzed was shown that the techniques can be used to hide text in images. Steganographic technique based on Lena image is proposed to apply in this system. The Lena image which was divided into two blocks was shown in the Figure 2.

Figure 2:- Original Cover Image

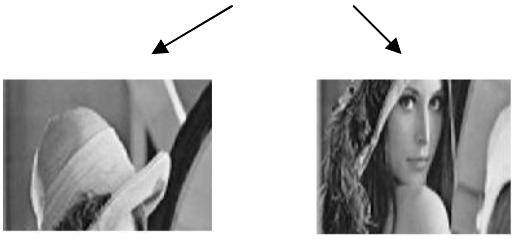

Figure 3:- Two blocks of Cover Image

In our Steganography system we are embedding text (file format: .txt) data in an image (file format: JPEG) using a Steganographic algorithm. The resultant image, called Stego Image which is strictly in JPEG format. Using the same technique, we are extracting the embedded data storing it in proper form i.e. in .txt, a text format.

VI. Embedding Algorithm.

1. Take the cover image.
2. Divide the original cover image into two blocks of image using split and merge algorithm.
3. Apply DCT algorithm.
4. Embed two different kinds of text messages in two blocks of image.
5. Merge the two blocks of image to get the original image.

VII. Compression

The method is basically the source encoding that reduces the number of bits required to represent an image. The image can be reconstructed perfectly from compressed data. In our system DCT is used as a compression method. The transform doesn't actually compress the image but it converts the pixel value from spatial domain to frequency domain.

VIII. Extraction

The process of extracting a secret message from Stego image includes the following steps:

1. Take the Stego image.
2. Use proposed encoder to decode the image.
3. Again the Stego image was divided into two blocks of image to extract the data.
4. Using secret key identified the region and extracts the embedded message bits.

Original image

Stego image

IX. Results

Our proposed system gives very promising result.

FOR EMBEDDING:

Requirement: Image file format: JPEG image. Two different text messages that are to be embedded into cover image.

Expected Result: The two different kinds of text message should be properly embedded in the LSB of first and second blocks of the original image. After embedding process, the cover image and the Stego image must look exactly the same.

Name of the Image	Lena.jpg
No. of character embedded in the first block of image	15
No. of character extracted from the first block of image	15
No. of character embedded in the second block of image	12
No. of character extracted from the second block of image.	12

X. Conclusion

Steganography has its place in the security. On its own, it won't serve much but when used as a layer of cryptography; it would lead to a greater security. Secret messages are embedded in the least significant bit of the two blocks of image. How many characters are embedded and extracted from each block of the image was discussed in this paper. After the embedding process, the cover image and the Stego image are looking exactly the same. Experimental results show that the proposed system is successful not only in achieving by embedding the different kinds of text in an image but also obtaining a Stego image of satisfactory quality.

References

[1]. Andreas Westfeld and Andreas Pfitzmann. Attacks on Steganographic Systems 1999. In Proceedings of Information Hiding - Third International Workshop. Springer Verlag, September 1999.

[2]. Evaluation of various LSB based methods of image Steganography on GIF file format – Namita Tiwari, International Journal of Computer Applications, September 2010

[3]. Johnson, N.F. & Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal, February 1998.

[4]. Lee Yeuan-kuen et al, "An Advanced Least-Significant- Bit Embedding Scheme for Steganographic Encoding", 5414/2009: pp. 349-360, 2009.

[5]. Johnson, N.F. Jajodia, S.& Duric, Z., 2001. Information hiding: steganography and watermarking – attacks and countermeasures. Kluwer academic publishers.

[6]. Li Zhi,Sui Ai Fen, "Detection of Random LSB Image Steganography"IEEE pp2113-2117,2004

[7]. J. R. Smith and B. O. Comisky, "Modulation and information hiding in images," in *Information Hiding, First International Workshop, Lectu e Notesin Computer Science,* R. Anderson, Ed. Berlin, Germany:Springer-Verlag, 1996, vol. 1174, pp. 207–226.

[8]. F. A.P. Petitcola s, R.J. Anderson and M.G.Kuhn,"Information Hiding –A Survey", Proceeding of the IEEE, vol.87,no.7,pp.1062-1078,july 1999

[9]. G. Caronni, "Assuring ownership rights for digital images," in *Proc .Reliable IT Systems, VIS'95*.