IOSR Journal of Electronics and Communication Engineering (IOSRJECE)
ISSN: 2278-2834 Volume 2, Issue 3 (July-Aug 2012), PP 01-04
www.iosrjournals.org

"Steganography for Text Messages Using Image"

[1]S.A. Khandekar, [2]Mrs.MR.Dixit
[1] Maharashtra Academy Of Engineering, Pune-412105 M.S. India.
[2]KIT College of Engineering Gokulshirgaon, Kolhapur M. S. India.

Abstract: *The rise of the Internet and multimedia techniques in the mid-1998s has prompted increasing interest in hiding data in digital media. Early research concentrated on watermarking to protect copyrighted multimedia products (such as images, audio, video, and text).Data embedding has also been found to be useful in covert communication, or Steganography. The goal was and still is to convey messages under cover, concealing the very existence of information exchange. There have been a number of Steganography embedding techniques proposed over the past few years.*

Key words*: Steganography, Discrete cosine transforms (DCT), JPEG, Quantization, Embedding, Extraction.*

I. Introduction

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message; this is in contrast to cryptography, where the existence of the message is clear, but the meaning is obscured.

Steganography literally means "covered writing" and is the art of hiding the very existence of a message. In today's digital world, invisible ink and paper have been replaced by much more versatile and practical covers for hiding messages – digital documents, images, video, and audio files. As long as an electronic document contains perceptually irrelevant or redundant information, it can be used as a "cover" for hiding secret messages.

The possible cover carriers are innocent looking carriers (images, audio, video, text, or some other digitally representative code) which will hold the hidden information. A message is the information to be hidden , anything that can be embedded into a bit stream. Together the cover carrier and the embedded message create a stegano-carrier. Hiding information may require a stegano key which is additional secret information, such as a password, required for embedding the information. For example, when a secret message is hidden within a cover image, the resulting product is a stegano-image. In this paper we discuss about present theory and practices in section I and section II discussed about the proposed method.

II. Present theories and Practices

1. Smith and Comiskey presented several spread spectrum data-hiding methods in [6]. These techniques utilize the message data to modulate a carrier signal, which is then combined with the cover image in sections of nonoverlapping blocks. The message is extracted via cross correlation between the steganoimage and the regenerated carrier; hence, cover image escrow is not necessary. A thresholding operation is then performed on the resulting cross correlation to determine the binary value of the embedded data bits.

2. A data-hiding scheme using the statistical properties of dithered imagery is proposed by Tanaka *et al.* [12]. With this method, the dot patterns of the ordered dither pixels are controlled by the information bits to be concealed. This system accommodates 2 kB of hidden information for a bit level 256x 256 image, yielding a payload of data or information hiding ratio of one information bit to four cover image bits. An information-hiding ratio of 1 : 6 is obtained for trilevel images of the same size.
The method has high payload but is restricted to dithered images and is not resistant to errors in the steganoimage

3. Davern and Scott presented an approach to image steganography utilizing fractal image compression operations [4].An information bit is embedded into the steganoimage by transforming one similar block into an approximation for another. The data are decoded using a visual key that specifies the position of the range and domain regions containing the message. Unfortunately, the amount of data that can be hidden using the method is small and susceptible to bit errors. Additionally, the search for similar blocks in the encoder, and the decoder comparison process, are both computationally expensive operations.

4. Turner [13] proposed a method for inserting an identification string into a digital audio signal by substituting the "insignificant" bits of randomly selected audio samples with the bits of an identification code. Bits are deemed "insignificant" if their alteration is inaudible. Such a system is also appropriate for two-dimensional (2-D) data such as images, as discussed.

Unfortunately, Turner's method may easily be circumvented. For example, if it is known that the algorithm only affects the least significant two bits of a word, then it is possible to randomly flip *all* such bits, thereby destroying any existing identification code.

III. Proposed Methodology and scope of the work:

In our Steganography system we are embedding text (file format: .txt) data in an image (file format: JPEG,BMP) in frequency domain, using a Steganographic algorithm and providing a key parameters namely, *shared secrete password* .The resultant image, called *Stego Image* is strictly in JPEG/ BMP format. Using same password and proposed decoder, we are extracting the embedded data storing it in proper form i.e. in .txt , a text format.

Steganography in spatial domain, targets specific locations in the image. But when intensity information is modified, then Steganography in the spatial domain is less resilient to common image processing operations. This is because embedded data becomes undetectable. So there is necessity of frequency domain Steganography.

In this section we are including the overview of our system modules.

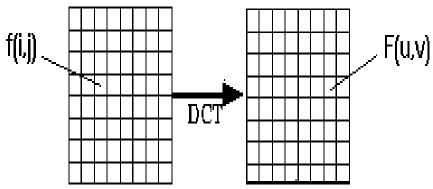
Our system is divided into two modules:

1. Embedding
2. Extraction

EMBEDDING is actually the hiding secret message into the cover image .It works in following modules;

DCT (Discrete Cosine Transform) & Quantization:

The DCT is used in JPEG and other compression methods. The transform itself doesn't actually compress the image. Rather, it converts the pixel values from the ***spatial domain*** to the ***frequency domain***.



The general equation for a 2D (*N* by *M* image) DCT is defined by the following equation:

$$F(u,v)=\left(\frac{2}{N}\right)^{\frac{1}{2}}\left(\frac{2}{M}\right)^{\frac{1}{2}}\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}A(i)A(j).\cos\left[\frac{\pi.u}{2.N}(2i+1)\right]$$

$$.\cos\left[\frac{\pi.v}{2.M}(2j+1)\right].f(i,j)$$

and the corresponding ***inverse*** 2D DCT transform is simple $F^{-1}(u\ ,v)$, i.e.:

where

$A(\xi)=1/\sqrt{2}$ for $\xi = 0$

otherwise

This sub-module includes following steps-

1. Take the cover image.
2. Get the RGB representation of it .For Every component divide cover image into 8X8 pixel block.
3. Apply 2D-DCT on each block obtain AC & DC coefficients.
4. Quantize the coefficients.

Embedding algorithm:

It includes following steps

The user-specified password as stego_key is used to allow for embedding message bits.

1. Skip the zero and DC coefficients.
2. Embed message bits using LSB of randomly selected quantized coefficient..

IV. 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.

DCT and Quantization:-

The DCT issued in JPEG and other compression methods. The transform doesn't actually compress the image but, it converts the pixel values from spatial domain to frequency domain. Then using specified quantization table quantizes the coefficient.

EXTRACTION is the process of extracting a secret message from stegano image using password. It includes the following steps.

1. Take the stego (embedded) image
2. Accept the shared secret password.
3. Use proposed encoder to decode the coefficient.
4. Using password as stegano_key collect back the randomly selected quantized DCT coefficient.
5. Then, we extract the embedded message bits.

V. Results

Our proposed method gives very promising result.

FOR EMBEDDING:

Requirement: Image file format Bit map image , JPEG image. The text message that is to be embed into cover image.

Expected results: After embedding process , the cover image and stego image must looking exactly same.

Result:1) Stego image and cover image are looking same after embedding a message.

2) PSNR of the image is above 80 dB.

FOR EXTRACTING:

Requirement: Extracted data from the stego image should match with original data.

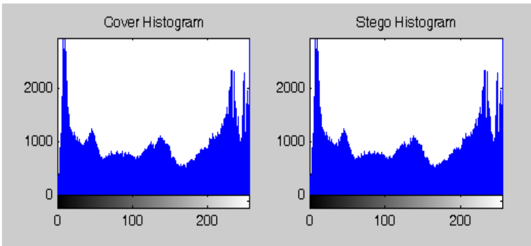
Expected results: There should not be any data loss after extraction of secrete data.

Result: Extracted data file is exactly similar in size and contents as the original file.

1)Cover image

Stego image

Histogram (PSNR = 95.94 dB)



Data can be embed in any image with high PSNR.

Name of Image	**Flower.jpg**				
No.of charac. Embeded	5	10	15	20	25
No.of charc.extracted	5	10	15	20	25

VI. Conclusion

Secret messages are embedded in the high frequency sub-band resulted from Discrete Cosine Transformation and quantization. Coefficients in the low frequency sub-band are preserved unaltered to maintain the image quality.

Even if the maximum numbers of characters (50 characters) are embedded in an image, still PSNR remains above satisfactory threshold level i.e. above 30 db.

As the size of the image increases the amount of information to be embed is also increases.

References:

[1] .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.

[2] I.J. Cox, J. Killian, T. Leighton and T .Shamoon, "Secure spread spectrum watermarking for images ,audio and video" in Proc. IEEE Int .Conf. Image Processing, Lausanne,Switzerland,Sept.2000,vol.111,pp.243-246.

[3] F.Johnsonand S. Jajodia, "exploring Steganography: seeing the unseen" IEEE computer magzinne,pp26-34 FEB1998

[4] P. Davern and M. Scott," Fractal based image steganography" ,in Information Hiding ,First International Workshop ,Lecture Notes in computer science M.D.Swanson,B.Zhu8 and

[5] A.H. Tewfik," Robust data hiding for images "in Proc. IEEE digital Signal procesising Workshop, Loen,Norway,Sept 1996 pp 37-40.

[6] I.J. Cox, S.roy and S .L Hingorani," Dyanamic histogram warping of images pairs for constant image brightness," in IEEE Int .Conf. Image Processing.

[7] S. Dumitrescu, X.WU and Z.Wang ," Detection of LSB Steganography via sample pair analysis ",IEEE transction on Signal processing,vol.51,no.7,july 2003,pp.1995-2007

[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*.

[10] J. Brassil, S. Low, N. Maxemchuk, and L.O'Gorman, "Electronic marking and identification techniques to discourage document copying," in *Proc. Infocom'94*, pp. 1278–1287.

[11] K. Tanaka, Y. Nakamura, and K. Matsui, "Embedding secret information into a dithered multi-level image," in *Proc. IEEE Military Communication sConf.*, Monterey, CA,1990,pp. 216–220

[12] L. F. Turner, "Digital data security system," Patent IPN WO 89/08915, 1989.

S.A. Khandekar born on 25th September 1976 at Kolhapur town in Maharashtra state. He has obtained his degree in Electronics engineering from KITCOE, Shivaji University, Kolhapur in 2000.He is presently working as a Sr.Lecturer in Electronics department , MAE College of engineering, Pune, Maharashtra state. His total experience in teaching is 11 years. His areas of interest are microprocessor and microcontrollers, computer network and programming languages.

Mrs. Manasi R. Dixit obtained her degree in Electrical engg. From Walchand college of engg. Sangali, Shivaji university and her ME (Electrical) degree from Walchand College of Engineering (WCE) Sangli. . She has a teaching experience of 26 years most of which is at KITCOE, Kolhapur. Presently she is working as a Associate Professor in the Electronics department at K.I.T. College of Engineering, Kolhapur. She has guided no. of undergraduates and postgraduate students. She is a life member of ISTE.