International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

A Steganography Implementation based on LSB and DCT

Sujit Patil[1], Shrikant Joshi[2]

[1]Vishwakarma Institute of Information Technology, Pune – 411048, Maharashtra, India

[2]Professor, Vishwakarma Institute of Information Technology, Pune – 411048, Maharashtra, India

Abstract: ***In recent years, Steganography and Steganalysis are two important areas of research that involve a number of applications. These two areas of research are important especially when reliable and secure information exchange is required. Steganography is an art of embedding information in a cover image without causing statistically significant variations to the cover image. Steganalysis is the technology that attempts to defeat Steganography by detecting the hidden information and extracting. In this paper a comparative analysis is made to demonstrate the effectiveness of the proposed methods. The effectiveness of the proposed methods has been estimated by computing Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR), Processing time, security. The analysis shows that the BER and PSNR is improved in the LSB Method but security sake DCT is the best method.***

Keywords: Steganography, Discrete Cosine Transform (DCT), LSB (Least Significant bit)

1. Introduction

An important aspect of the modern way of life is communication. Many devices present today have the ability to transmit various information between them using different ways of communication, like insecure public networks, different types of wireless networks and the most used: the Internet. In some cases it is needed to keep the information travelling through different kinds of channels secret. Mainly there are two ways of concealing information: cryptography and steganography. Cryptographys main aspect is that the information is somehow distorted, scrambled by the sender using normally an encryption key also known only by the intended receiver who decrypts the message. The problem with cryptography is that a user intercepting the message, although he cannot decrypt it, he might detect that there is encrypted, secret information .On the other hand steganography is able even to hide this aspect making sure that even the fact that there is secret information, is concealed. Steganographys main aspect is that it is embedding the secret message into another message. The basic structure of Steganography is made up of three components: the carrier, the message, and the key.

Most of the steganography techniques; which hide the data directly in the pixels of the image, use the Least Significant Bit (LSB) embedding method. By using random factors and secret keys the security of steganography can be increased, but by considering the statistical characteristics of these images, most of these techniques will be fractured. However the least significant bits of the pixels looks random, practically they dont have random properties and represent some characteristics of the image .Evaluation on the properties of the image before and after steganography process, can indicate the changes in these least significant bits. As a result the application of steganography technique in spatial domain is not safe enough against the recent developing attacks. In the next section a brief introduction to the steganography in frequency domain is presented.

2. Literature Survey

The term steganography illustrates the art and science of hidden communication. By using steganography there is a chance to send messages so that nobody can detect the existence of the message. The message is embedded by weakening some characteristics of another media, which is called cover. Final output has equal properties to cover media, and also it includes our secret information. This new object is transmitted. If somebody is able to interpret this transmitted package, the secret message can be distinguished. While this transmitted package is really similar to cover media, detection of any embedded information is very difficult. For implementation of the steganography system, two algorithms are needed to be designed: one for hiding data and the other to extract this successfully. The main subject in embedding algorithm is to hide the secret message within the cover media without attracting any attention. The extraction algorithm has a simpler process and can be achieved by inversing the steps of embedding algorithm. All of the steganography steps can be shown graphically in Fig.1

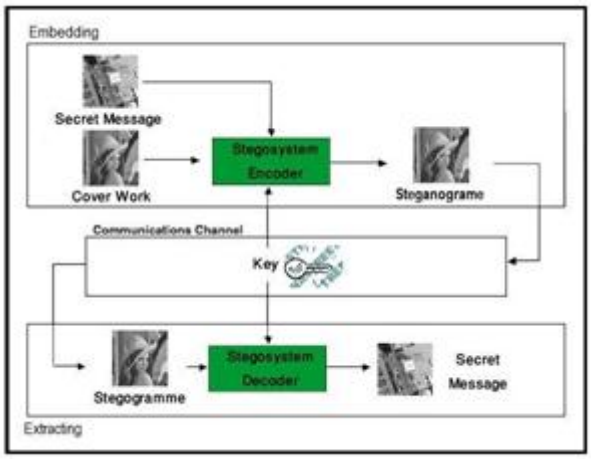

Figure 1: Steganography steps in a graphical view

The secret message usually is a text file or another image file which contains the secret information. This file is sent to the

encoder unit in the first step. The encoder must be designed and implemented with high precision, to hide the secret message with a few distortion and changes in the cover image. Encoder unit usually needs a key to increase the security level of hiding method; this key is used in the extraction phase too. Without using this key, the message will be available without any impediment, if someone guesses the embedding or extraction algorithm.

Output of the encoder unit is called steganograme which should be close enough, to cover media. Then this image and the key, which is used in embedding phase, are transmitted via a communication channel. In the next step this package are applied to decoder unit. Output of the decoder unit is delivered in the receiver side. The output of extraction unit is just an estimate of secret message, because during transition through the communication channel, the steganograme is exposed to different types of noises, which can change the values of some bits.

The application of steganographic technique can be broadly classified as operating in two different domains, such as spatial domain and frequency domain. In spatial domain, the embedding and hiding process are mostly carried out by bitwise manipulation.

For example, manipulating the LSB in one of the color components in an image. While, the frequency domain includes those which involve manipulation of transformed image such as Discrete Cosine Transformation (DCT) and wavelet transformation. Such manipulation includes changing the value of the quantized DCT coefficients.

3. Image Steganography Techniques

Based on the analyses of steganography tools algorithms, we partition these tools into two categories: (1). Spatial domain based steganography (2) Transform domain based steganography.

A. Spatial Domain Based Steganography

Spatial steganography mainly includes LSB (Least Significant Bit) steganography Least significant bit (LSB) insertion is a com-mon, simple approach to embedding information in a cover image

The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message.

Pixel: (10101111 11101001 10101000) (10100111 01011000 11101001) (11011000 10000111 01011001)

Secret message: 01000001

Result: (10101110 11101001 10101000) (10100110 01011000 11101000) (11011000 10000111 01011001)

B. Transform Domain Based Steganography

Basically there are many kinds of power level transforms that exist to transfer an image to its frequency domain, some of which are Discrete Cosine Transform, KL Transform and Wavelet Transform.

C. The Discrete Cosine Transform (DCT)

This method is used, but similar transforms are for example the Discrete Fourier Transform (DFT). These mathematical transforms convert the pixels in such a way as to give the effect of spreading the location of the pixel values over part of the image [5]. The DCT transforms a signal from an image representation into a frequency representation, by grouping the pixels into 8 8 pixel blocks and transforming the pixel blocks into 64 DCT.

DCT is used in steganography as- Image is broken into 88 blocks of pixels. Working from left to right, top to bottom, the DCT is applied to each block. Each block is compressed through quantization table to scale the DCT coefficients and message is embedded in DCT coefficients.

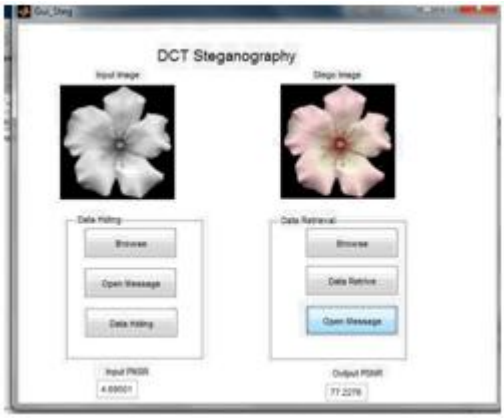

Figure 2: DCT Steganography

Figure 3: LSB Steganography

4. Model

A. Definitions

(i) Cover image: It is defined as the original image into which the required information is embedded. It is also termed as carrier image. The information should be embedded in such a manner that there are no significant changes in the statistical properties of the cover image.

(ii) Stegoimage: It is an unified image obtained by the combination of the payload and cover image.

(iii) Perceptibility: It describes the ability of a third party (not the intended recipient) to visually detect the presence of hidden information in the stego image. The embedding algorithm is imperceptible when used on a particular image if

an innocent third party, interested in the content of the cover image, is unaware of the existence of the payload. Essentially this requires that the embedding process not degrade the visual quality of the cover image.

(iv) Robustness: It characterizes the ability of the payload to survive the embedding and extraction process, even in the face of manipulations of the stego image such as filtering, cropping, rotating and compression. (v)Security: It is inability of adversary to detect hidden images accessible only to the authorized user. The quality factor can enhance the security of the image. A steganographic image is perfectly secure when statistical data of the cover and stego images are Identical.

B. Error Analysis

(i)Bit Error Rate: For the successful recovery of the hidden information the communication channel must be ideal but for the real communication channel, there will be error while retrieving hidden information and this is measured by BER. The cover image is represented as cov and stego image as steg in the given equation Where i is the pixel position.

(ii) Mean Square Error: It is defined as the square of error between cover image and the stego image. The distortion in the image can be measured using MSE.

$$MSE = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(X_{i,j} - Y_{i,j})^2}{MN}$$

(iii) Peak Signal to Noise Ratio: It is the ratio of the maximum signal to noise in the stego image.

$$PSNR = 10 \log \frac{255_2}{MSE}$$

5. Algorithms of Steganography

A. Lsb Based Steganography Algorithm to embed text message
Step 1: Read the cover image and text message which is to be hidden in the cover image.
Step2: convert the color image into grey image. Step 3: Convert text message in binary.
Step 4: Calculate LSB of each pixels of cover image.
Step 5: Replace LSB of cover image with each bit of secret message one by one.
Step 6: Write stego image

B. Lsb Based Steganography Algorithm to retrieve text message
Step 1: Read the stego image.
Step 2: Calculate LSB of each pixels of stego image.
Step 3: Retrieve bits and convert each 8 bit into character.

C. DCT Based Steganography Algorithm to embed text message
Step 1: Read cover image.
Step 2: Read secret message and convert it in binary.
Step 3: The cover image is broken into 88 block of pixels.
Step 4: Working from left to right, top to bottom subtract 128 in each block of pixels.
Step 5: DCT is applied to each block.
Step 6: Each block is compressed through quantization table.
Step 7: Calculate LSB of each DC coefficient and replace with each bit of secret message. Step 8: Write stego image

D. DCT Based Steganography Algorithm to retrieve text message
Step 1: Read stego image
Step 2: Stego image is broken into 88 block of pixels.
Step 3: Working from left to right, top to bottom subtract 128 in each block of pixels.
Step 4: DCT is applied to each block.
Step 5: Each block is compressed through quantization table. Step 6: Calculate LSB of each DC coefficient.

Figure 2 shows DCT Based Steganography Algorithm while Figure 3 shows LSB Based Steganography Algorithm.

6. Conclusion

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. It is therefore a book on magic. It is emerging in its peak because it does not attract anyone by itself. In this paper analysis of LSB and DCT methods has been successfully implemented and results are delivered. The MSE and PSNR of the methods are also compared and also this paper presented a back-ground discussion and implementation on the major algorithms of steganography deployed in digital imaging. From the results it is clear that as PSNR in LSB is the best but as we know that security is much more important in today's communication system. So security wise DCT is the best.

References

[1] S. N. Jacobsen, U. Madhow, B. S. Manjunath, and S. Chandrasekaran, "Robust Image-Adaptive Data Hiding Based on Erasure and Error Correction," IEEE Transactions on Image Processing, vol. 13, no. 12, pp. 1627-1639, Dec. 2004.
[2] R. C. Gonzalez and R. E. Woods, and S. L. Eddins, Digital Image Processing using MATLAB Second Edittion, Addison Publishing, 2004.
[3] P. Honeyman, Hide and Seek: An introduction to steganography, IEEE Security and Privacy Journal, 2003.
[4] K. L. Chiew, L. Jane, F. Sarah, and S. Juan, "Steganography: DCT Coefficients Reparation Technique in JPEG Image," International Journal of Digital Content Technology and its Applications, vol. 2, no. 2, 2008.
[5] N. Hideki, N. Michiharu, and K. Eiji, High-performance JPEG steganography using quantization index modulation in DCT domain, Pattern Recognition Letters, vol. 27, pp. 455461, 2006.
[6] C. C. Chen, "A reversible data hiding scheme using complementary embedding strategy," Information Sciences, pp. 30453058, 2010.
[7] Q. Liu, A. H. Sung, M. Qiao, Z. C. B. Ribeiro, "An improved approach to steganalysis of JPEG images," Information Sciences, vol. 180, 2010, pp. 16431655.

[8] C. L. Liu and S. R. Liao, "High-performance JPEG steganography using complementary embedding strategy," Pattern Recognition, viol. 41, 2008, pp. 2945 2955.
[9] W. Stallings, Cryptography and Network Security Principles and Practice, third ed, Pearson Education, New Jersey, 2003.
[10] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, Techniques for data hiding, IBM Syst. J., vol. 35, pp. 313336, 1996.
[11] D. Gruhl and W. Bender, Information hiding to foil the casual counterfeiter, in Proc. Information Hiding Workshop, Portland, OR, Apr. 1998.
[12] R. G. V. Schyndel, A. Z. Tirkel, and C. F. Osborne, A digital watermark, in Proc. IEEE Int. Conference on Image Processing, Austin, TX,1994, pp. 8689.
[13] N. Nikolaidis and I. Pitas, Copyright protection of images using robust digital signatures, in Proc. IEEE ICASSP96, 1996, pp. 21682171.
[14] M. D. Swanson, B. Zhu, and A. H. Tewfik, Robust data hiding for images, in Proc. IEEE Digital Signal Processing Workshop, Loen, Norway, Sept. 1996, pp. 3740.