International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in; editorijoer@gmail.com

Vol.7., Issue.4, 2019
July-Aug

REVIEW ARTICLE

ISSN: 2321-7758

REVIEW ON HIDING ENCRYPTED MESSAGES USING TRANSFORMATION TECHNIQUES IN IMAGE

RANJANA KUMARI
M.Tech Scholar, Department of EC
Mittal Institute of Technology, Bhopal, India
https://doi.org/10.33329/ijoer.74.25

ABSTRACT
Information security, Steganography is a vast field of computing world that develops numerous intelligent systems for secret communication. Image steganography is the most popular dimension due to its frequency on the internet in this field. The goal of this research work is to provide high level of security, maximum embedding capacity, efficiency and reliability for secret communication using image processing and steganography techniques. Steganography is the practice of concealing the communication existence by hiding the traveled message in cover media. This research work is to study Discrete Cosine Transform (DCT), Fast Fourier Transform (FFT) or Wavelet Transform based steganography for hiding secret bits sequentially in Least Significant Bits (LSBs). Likewise, it is analyzed and concluded that low and middle frequencies to analyze their performance using PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error). The findings indicate that the middle frequency has the larger hiding capacity and relatively better PSNR and MSE.
Keywords: Digital Image, Spatial Domain, Image Transforms, DWT, DCT

I. Introduction

Information security [1] in today's world is a sense of declaration against threats, means that important information must be secured and there risks of attacks as well as controls must be balanced. Information security actually starts with the emergence of first main frame computer. But with the introduction of information security many viruses and code breakers were also developed that breaks the security channel and damage the important information.

Information security is further divided into three dimensions that are:

Figure 1: Information Security

Watermarking: Watermarking is a recognizable image pattern that may be darker or lighter in tone, indicates the copy rights of particular documents.

Cryptography: Cryptography comes from a Greek word meaning hidden or secret writing for secure communication in the presence of third parties or Un-authorized persons.

Steganography: Steganography is a combination of two words. "Stegano" means covered and "graphic" means writing. Steganography [2] is an art of hiding the existence of the message in order to draw attention to the secret message so that third parties or illegal people cannot recognize the message. Steganography is used in antiquity, just as messages with invisible inks are written on the body while messages on envelopes in stamped areas are sent in a different way. Modern methods of steganography are called digital steganography.

II. Types of Steganography

Steganography [3] is further divided into five different dimensions that are as follows:

Text steganography: Text steganography contains a simple text, it can be letters or numbers.

Image steganography: Image steganography is the most common form of steganography. It is most often used in different places to hide text in images, audio in images and video in images.

Audio steganography: Audio steganography s another dimension of the audio format. It can be in any other format where the information is hidden and transmitted by an intelligible edition of the audio file.

Video steganography: Video steganography consists in hiding secret information in the video. The video is also a safe medium because the video frequency changes every second and the color of the video changes at any time and cannot be seen with the naked eye.

Protocol steganography: Protocol steganography ntegrates information using network control protocols such as HTTP, FTP, TCP, SSH, UDP and so on. Secret information is integrated with Voice over IP.

III. Techniques of Steganography

Over the last decades, several steganographic algorithms have been used to insure data security [4]. These techniques consist of two domains, which are: spatial domain techniques and frequency domain techniques are shown in Figure 2.

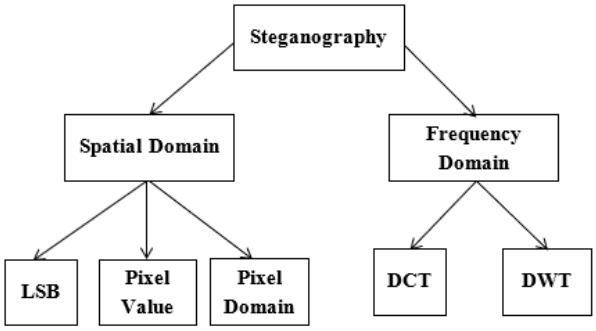


Figure 2: Steganographic Techniques

A. Spatial domain techniques

The message bits are encoded directly by these techniques causing few changes in the intensities of the sample hardly result in perceptual variations to the cover. They offer a fine concealment while giving a big ability of the embedded data and simple investigation [5]. As a result, these techniques are considerably utilized in steganographic applications. They offer great capacity but cannot stand up to simple modifications and are easy to recognize.

The LSB substitution technique is a common spatial domain technique used to incorporate LSB confidential data of pixel values into a vector. Since LSBs are masked when distorted, they can be easily modified and wasted by filtering, compressing or transforming the inaccurate format or dimensions. If an image is the hidden message, the LSBs of the title image are replaced by MSB bits (the most significant bits) of the masked image if there is no apparent confusion in the statistical property of the title image [6]. Mainly these techniques have different types of transformations:

Type 1: store 1 byte of hidden image in 1 byte of cover image.

Type 2: store 1 byte of hidden image in 2 bytes of cover image.

Type 3: store 1 byte of hidden image in 4 bytes of cover image.

Type 4: store 1 byte of hidden image in 8 bytes of cover image.

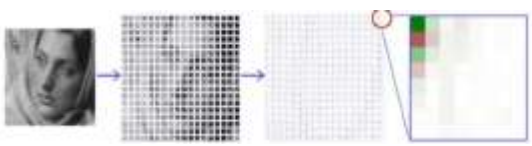
B. Frequency or transform domain techniques

The transformation of the spatial domain into the frequency domain is applied to an image in which the properties of HVS (human visual system) cannot detect very subtle changes in visual representation. In the field of transformation, the secret message is found in other robust regions and covers the entire image [7]. Therefore, it is more difficult to recognize than the visual domain.

C. Discrete cosine transform (DCT)

DCT is the algorithm most commonly used in image steganography as a standard for JPEG image format and image compression. It is an orthogonal transformation that uses some basic functions with characteristics such as low bit error rate, high compression ratio, perfect effect of synthetic computational complexity and perfect integration of data. It splits the image into frequency bands (low, medium and high), making it easier to select the band in which hidden data must be incorporated [8]. DCT is used by many non-analytical applications such as image processing and signal processing such as video conferencing. Data is entered in non-important bits of DCT coefficients. During this period, any change to the coefficient affects all the pixels in the block. Steps involved in DCT, shown in Figure 3:

- Group the cover image into 8 ×8 blocks of pixels.
- Transform every block of pixels into 64-DCT coefficients using the forward 2D_DCT transformation.
- Quantization is applied by all block values divided by a coefficient of quantization.
- Encode coefficients using very common entropy coders to reduce the size further, e.g. the Huffman Coding, Run Length Encoding algorithm.



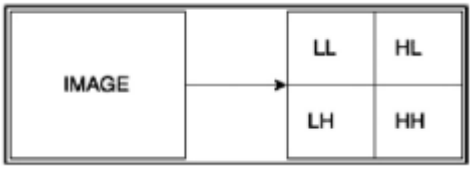


Figure 3: DCT transformation

D. Discrete wavelet transform (DWT)

It is utilized to convert the signals in time domain to frequency domain. After transformation, it will produce coefficients set arranged in a manner which allows the signal spectral analysis and the signal spectrum attitude in time. DWT is a technology of cutting edge in the image compression area. Wavelet algorithms provide fundamental enhancements in the quality of images at a large ratio of compression. DWT is calculated by consecutive low and high pass filters. Image signals decompose it into four sub-bands After 2-D DWT. One of the simplest and, most commonly used filters is Haar Wavelet Filters. Hiding in DWT do- main is more flexible and surpasses DCT with respect to compression survival, but its disadvantage is the capacity is limited [9,10].

E. Discrete fourier transform (DFT)

FT (Fourier Transform) and inverse FT used in transforming from time domain to frequency domain and vice versa. The computation of FT numerically requires discretization, numerical integration, and Finite time duration. This is an approximation of the real value and it is called discrete Fourier transformation (DFT) [11, 12]. Where DFT divides the images to cos and sin constituents of different frequency. Each pixel in the spatial domain is transformed to the frequency domain and decomposed into real part and imaginary part. Therefore, the number of frequencies needed to represent an image perfectly is the same number of pixels in the spatial domain. So the image has the same size in the Fourier domain and the spatial domain.

Main objectives of this research work are:

- To create well-built, competent and off course strong technique to prevent from Steganalysis.

- Increase in the PSNR (peak signal to noise ratio) of the Stego-image, minimize the distortion in the image.

IV. Related Work

Chang et al. [4] uggested that a new steganographic algorithm was JPEG dependent using the central frequency of the quantized DCT coefficients that had previously been modified to mask confidential data. The results showed that the proposed approach has a greater capacity than Jpeg–Jsteg, and whereas, preserving the acceptable quality of stegoimage.

Bhargava et al. [5] explained that the tattooing techniques of images can be subdivided into the idea of a spatial domain type of domain, a transformation domain or a wavelet system. This article aims to provide a detailed overview of all watermark techniques, with particular attention to the types of image watermarks and their applications in today's world.

Raja et al. [7] used an LSB algorithm to incorporate a hidden image into the carrier image and then the DCT algorithm was applied for compression. Finally, reverse procedures are performed at the end to extract the embedded image.

Brabin et al. [8] proposed a steganography technique based on QET (Quantization Error Table) for JPEG images. The system incorporates the confidential data into the DCT coefficients selected based on the quantization error which represents the difference between the de-quantized DCT block and the original DCT block. After quantization, the DCT coefficients that have been transformed to zero are selected to incorporate the confidential data. The number of bits to be masked in the selected DCT coefficients is calculated based on the QET value. This method increases the compactability in each DCT block, but has the disadvantage of requiring the master image, the target image, the quantization factor and the modified quantization table for the extraction process.

Kaur and Kochhar [9] presented a comparative analysis to demonstrate the effectiveness of the proposed algorithms (LSB and DCT). The result shows that DCT is the best security algorithm.

Saejung et al. [10] studied steganography algorithms based on wavelet and DCT transformation. They discovered that the DCT algorithm provides a better PSNR than the wavelet transformation.

Kaushal, A. and Chaudhary, V. [11] proposed a steganographic algorithm using the Fourier transform at discrete fractions (DFrFT). A study of steganography with comparison algorithms in the spatial and frequency domain according to the DCT, the DFT (discrete Fourier transform) and the DFrFT. They recommended the use of steganography based on frequency domain algorithms (DCT, DFT, DFrFT).

Bansal and Chhikara [12] have studied an improved steganographic technique based on the DCT, called the screen algorithm, which uses the quantized DCT coefficients to incorporate the data hidden in the image. The proposed steganography algorithm can provide a high capacity and effectively improve security.

Sahar A. El_Rahman [14] proposed a DCT-based steganography tool to hide confidential information on a nuclear reactor using the sequential method of medium frequency integration [13]. The results show that the proposed instrument offers a relatively high integration capacity without visual distortion in the resulting image, while improving security and maintaining the accuracy of hidden data.

It is important to understand how digital steganography works and to ensure that the cover image / image is large enough to support byte manipulation. The basics of data integration are based on three different facts. These three elements are capacity, security and robustness. Capacity is the amount of data that can be hidden in the cover audio. Security is the interceptor's ability to decrypt data hidden in the audio coverage. After all, robustness means the amount of manipulation audio coverage can handle before a change occurs. Steganography is very similar to cryptography because the recipient must know the secret called a secret key. In order for the steganography to remain

secure, the original and unchanged cover sound must be kept secret. It would be easy to locate the hidden data in an audio file if you have the original sound next to the steganography cover sound. The compression ratio, the low PSNR ratio and High mean squared error are some more different issues in steganography.

V. Conclusion

Data is the heart of computer communication and during the year many methods were developed to achieve the goal of hiding data with steganography. The trick is to incorporate the hidden object into a much larger object so that the human eye does not notice the change. The image steganographic algorithms are presented for embedding secret messages in images. This paper presents the review on different steganography techniques used in existing work that lead to design more robust steganographic algorithm.

References

[1] Anderson R , Petitcolas F . On the limits of steganography. IEEE J Selected Areas Commun 1998;16(4):474–81.

[2] Artz D . Digital steganography: hiding data within data. IEEE Internet Comput J 2001;5(3):75–80.

[3] Acharya UR , Acharya D , Bhat P , Niranjan U . Compact storage of medical images with patient information. IEEE Trans Inf Technol Biomed 2001;5(4):320–3.

[4] Chang CC , Chen ST , Chung ZL . A steganographic method based upon JPEG and quantization table modification. J Inf Sci 2002;141:123–38 .

[5] Bhargava, G., & Jhapate, A., “A Study on Digital Watermarking Techniques”, INTERNATIONAL JOURNAL ONLINE OF SCIENCE, 4(3), 5, 2018. [accessed 2019 Jan 12]. Retrieved from http://ijoscience.com/ojsscience/index.php/ojsscience/article/view/130 .

[6] Provos N , Honeyman P . Hide and seek: an introduction to steganography. IEEE Secur Privacy 2003;1(3):32–44.

[7] Raja KB , Chowdary CR , Venugopal KR , Patnaik LM . A secure image steganography using LSB, DCT and compression techniques on raw images. In: 3rd international conference on intelligent sensing and information processing; 2005. p. 171–6.

[8] Brabin DRD , Sadasivam V . QET based steganography techniques for JPEG image. In: International conference of control, automation, communication and energy conservation; 2009. p. 1–5.

[9] Kaur G , Kochhar A . A steganography implementation based on LSB & DCT. Int J Sci Emerg Technol Latest Trends 2012;4(1):35–41.

[10] Saejung S , Oondee A , Preechasuk J , Chantrapornchai C . On the comparison of digital image steganography algorithm based on DCT and wavelet. Int Comput Sci Eng Conf (ICSEC) 2013:328–33.

[11] Kaushal A , Chaudhary V . Secured image steganography using different transform domain. Int J Comput Appl 2013;77(2):24–8.

[12] Bansal D , Chhikara R . An improved DCT based steganography technique. Int J Comput Appl 2014;102(14):46–9.

[13] A El_Rahman S. A comprehensive image steganography tool using LSB scheme. Int J Image Graph Sig Process (IJIGSP) 2015;7(6):10–18.

[14] Sahar A. El_Rahman, “A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information”, Elsevier, 2016.