# Survey: Image Steganography using DCT Technique

**Janki Gajjar**[1]
[1]Student of M.E
[1]Department of Computer Science & Engineering
[1]Narayan Shastri Institute of Technology

*Abstract*— Steganography is defined as the study of invisible communication. Steganography usually deals with the ways of hiding the existence of the communicated data in such a way that it remains confidential. It maintains secrecy between two communicating parties. In image steganography, secrecy is achieved by embedding data into cover image and generating a stego-image. There are different types of steganography techniques each have their strengths and weaknesses. Using Steganography techniques on Stego image we can improve the security. For improving second level security we can also apply blowfish algorithm on stego image. so that the result in improvement of security in terms of execution can be achieved.

***Key words:*** Image Steganography, Cryptography, Application, DFT, DCT, DWT, DCT Algorithm

## I. INTRODUCTION

In today's world, the communication is the basic necessity of every growing area. Everyone wants the secrecy and safety of their communicating data. In our daily life, we use many secure pathways like internet or telephone for transferring and sharing information, but it's not safe at a certain level. In order to share the information in a concealed manner two techniques could be used. These mechanisms are cryptography and steganography. For decades people strove to develop innovative methods for secret communication. In such a way that non-participating persons are not able to detect the presence of this information by analyzing the information detection. The remainder of this introduction highlights briefly some historical facts and attacks on methods [2]. The major job of the field of steganography is the storing, thrashing, and embedding of surreptitious data in all types of digital data like audio, videos, images and text because they are vulnerable for various attack. Digital Steganography is the technique of securing digitized data by hiding it into another piece of data. Therefore, the need of hiding secret identification inside different types of digital data is required such that owner can prove copyright ownership; identify attempts to tamper with sensitive data and to embed annotations. The main task of the field of steganography is the storing, hiding, and embedding of secret data in all types of digital data [3].

### *A. Problem Statement:*

Digital Steganography is the skill that involves communicating surreptitious data in a proper multimedia carrier, which are image, audio, and video files. Under this statement, if the feature is observable, the point of attack is evident, thus the here goal is conceal to the continuation of the embedded data. In cryptography, the message is modified in an encrypted form with the help of encryption key which is known to sender and receiver only. The message cannot be accessed by anyone without using the encryption key. However, the transmission of encrypted message may easily arouse attacker's suspicion, and the encrypted message may thus be intercepted, attacked or decrypted violently. In order to overcome the shortcomings of cryptographic techniques, steganography techniques have been developed.

### *B. Motivation:*

Steganography has provided the privacy of information transmitters across the World Wide Web. The internet allows for effortless spreading of information over huge areas. This is both an approval and bother since people all over the world can view your information but so can everybody else. Encrypting data has been the most popular approach to protecting information but this protection can be broken with enough computational power. An alternate approach to encrypting data would be to hide it by making this information look like something else. These way only people would realize its true content. In particular, if the important data is hidden inside of an image then everyone but your people would view it as a picture. At the same time people could still retrieve the true information. The data security that it provides even if the hacker gets access to our multimedia data, then also he can't access the information, that is, the hacker has done the difficult part of hacking and getting access to the data but the actual data so still under his nose. Furthermore steganography does not allow the copy one to another.

### *C. Objectives:*

The main objective of the dissertation is to propose a new solution for in our daily routine, we use various secure or protected pathways like internet or telephone for transferring and sharing or transfer information, but it's not safe at a certain level sometimes it has break. In categorize to share or exchange the information in a secret manner two techniques could be used. These mechanisms are cryptography and steganography. We try to enhance the security and the robustness of the information against attacks and image steganography techniques.

### *D. Scope of Dissertation work:*

To, hide or protect the information, cryptography is providing the several level of security. Here we have used the image steganography for the hide the communication between to parties so that attacker can't see the communication as well as provide second level security to store the encrypted information behind the Image.

## II. IMAGE STEGANOGRAPHY

Steganography [1] is does not only hiding of the data but also hiding the information of transmission. Steganography hides the secret or confidential data in another file in such a way that only the receiver knows the existence of message. In past decades, the data or information message was protected by hiding it on the back of wax, writing tables, and

 

stomach of rabbits or on the scalp of the slaves. But now a day's many of the people transmit the data in various types of categories like; text, images, video, and audio over the medium. The secure transmission of confidential data, the multimedia object like audio, video, images are used as a cover sources to hide the data.

Here explain the five types of steganography:

1) Text Steganography:

It consists of hiding information inside the text files. In this method, the secret data is hidden behind every nth letter of every words of text message. Numbers of methods are available for hiding data in text file. These methods are i) Format Based Method; ii) Random and Statistical Method; iii) Linguistics Method [1].

2) Image Steganography:

Hiding the data by taking the cover object as image is referred as image steganography. In image steganography pixel intensities are used to hide the data. In digital steganography, images are widely used cover source because there are number of bits presents in digital representation of an image [1].

3) Audio Steganography:

It involves hiding data in audio files. This method hides the data in WAV, AU and MP3 sound files. There are different methods of audio steganography. These methods are i) Low Bit Encoding ii) Phase Coding iii) Spread Spectrum [1].

4) Video Steganography:

It is a technique of hiding any kind of files or data into digital video format. In this case video (combination of pictures) is used as carrier for hiding the data. Generally discrete cosine transform (DCT) alter the values which is used to hide the data in each of the images in the video, which is unnoticeable by the human eye. Mp4, MPEG, AVI are the formats used by video steganography [1] .

5) Network or Protocol Steganography:

It involves hiding the information by taking the network protocol such as TCP, UDP, ICMP, IP etc, as cover object. . In the OSI layer network model there exist covert channels where steganography can be used [1].

### *A. Steganography Terminology:*

Steganography consists of two provisions that is message and cover image. Message is the secret data that needs to hide and cover image is the carrier that hides the message in it [1].

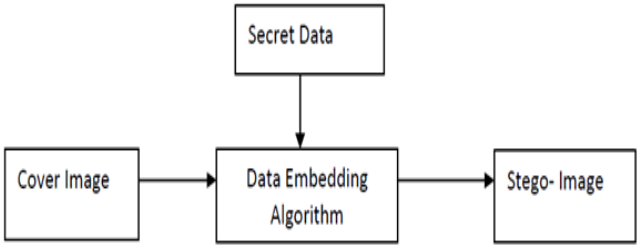


Fig. 2.1: Steganography Diagram

#### *1) Application of Steganography:*

- Confidential Communication and Secret Data Storing
- Protection of Data modification
- Access Control System for Digital Content Distribution
- E-Commerce ex. Online shopping
- Media ex. Encrypt the disk media
- Database Systems for password storage.
- Digital watermarking.

### *B. Image steganography Transformation:*

Based on the analyses of steganography tools' algorithms, we partition these tools into two categories [6]:

#### *1) Spatial Domain Based Steganography:*

Spatial steganography mostly includes LSB (Least Significant Bit) steganography least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image. The least significant bit of some or all of the bytes inside an image is changed to a bit of the secret message.

#### *2) 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.

In Transform domain, Pixel values are transformed and then processing is applied on the transform coefficients.

a) DFT: These Mathematical transform 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.

b) DCT: It transforms a signal from an image representation in to frequency representation by grouping pixels into 8*8 pixels block and transforming the pixel block in to 64 DCT.

c) DWT: Wavelets are special functions which are used as function for representing signals.

#### *3) Comparission between Straganography and Cryptography:*

Basically, the purpose of cryptography and steganography is to provide secret communication. Steganography is Hiding a secret message within a larger one in such a way that others cannot discern the presence or contents of the hidden message" and Cryptography is "The process or skill of communicating in, or deciphering secret writing or ciphers."

## III. DCT ALGORITHM

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 8×8 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.

Algorithm to retrieve text message

- Step 1: Read stego image
- Step 2: Stego image is broken into 8×8 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 quantizatio table.
- Step 6: Calculate LSB of each DCT coefficient.

*A. Comparison between Transformation Techniques:*

| Steganography Techniques | Cover Media | Embedding Techniques | Advantages |
|---|---|---|---|
| Image Hiding | Image | | |
| 1.LSB(Lea st Significant Bit) | | This method is used the least significant bit of every pixel in one image to hide the most significant bit of another | Simplest & easiest way of hiding information |
| 2.DCT (Discrete Cosine Transform) | | Embeds the information by altering the transformed DCT co-efficient | Hide data can be distributed more evenly over the whole image in such a way to make it robust |
| 3.DWT (Discrete Wavelet transform) | | This technique work by talking many wavelet to encode a whole image | Coefficient of wavelet are altered with the noise within tolerable level |

Table 3.1: Comparison between Transformation Techniques

## IV. Conclusion & Future Enhancement

During the reviewed and analysis of various papers on steganography techniques. I have observed that mainly of the steganography work is done in the past two years. In current environment, LSB is the most widely used technique for steganography. The various security and data hiding techniques are used to implement steganography using LSB, ISB, MLSB.

We can protect our information by hiding our communication using steganography. And for more security here we apply DCT transformation for best quality image.

In future, the work may be extended by including the image compression technique and implementation of blowfish with high speed and minimum energy consumption.

## References

[1] Dr. Fuhui Long, D. H. Fundamentals Of Content-Based Image Retrieval.
[2] Mehwish Rehman, M. I. (2012). Content Based Image Retrieval: Survey. World Applied Sciences Journal, 404-412
[3] SUJATHA, S. S. (Aug 2013). Survey Paper On Various Methods in Content Based Information Retrieval. Impact: International Journal of Research in Engineering & Technology (IMPACT: IJRET) ISSN 2321-8843, Vol. 1 (Issue 3), 109-120.
[4] Al, N. L. (2012). A Review of Image Classification Techniques in Content Based Image Retrieval. International Journal of Computer Science and Information Technologies, 5182 – 5184
[5] D.Jeyabharathi, D. S. (2013). Performance Analysis of Feature Extraction and Classification Techniques in CBIR. International Conference on Circuits, Power and Computing Technologies, 978-1-4673-4922-2.
[6] Nancy Goyal, N. S. (July 2014). A Review on Different Content Based Image Retrieval Techniques Using High Level Semantic Features. International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2 (Issue 7).
[7] Nidhi Singhai, P. S. (July 2010). A Survey On: Content Based Image Retrieval Systems.

 