Review Paper on LSB and DCT Technique of Image Steganography

Deepti Pandey[1] R.K.Bharti[2]

[1]M.E Student

[1,2]Department of Computer Science and Engineering

[1,2]Bipin Tripathi Kumaon Institute of Technology, Dwarahat, Almora, Uttarakhand

Abstract— Steganography is a technique of hiding the secret information between two parties that communication is taking place. Many different cover file formats can be used to hide the secret data, but digital images are the most popular because of their frequency on the Internet. For hiding the important information behind an images, there exists a large variety of steganographic techniques some are more complex and all of techniques have respective strong and weak points. The least significant-bit (LSB) based insertion techniques are very popular for steganography in spatial domain. On the other hand, DCT (Discrete Cosine Transform) based technique insertion of secret information in carrier depends on the DCT coefficients.

Key words: LSB, DCT, Steganography, Cryptography

I. Introduction

In today, the rise of the internet, the most important factor of sharing information and communication between two parties has been the security of information. the previous times data has been hidden in some ways or other and with the increase of security, Steganography has come into place. Steganography plays an important role in information security.

Steganography is the art of cover a hidden data in such a way that no one apart from the intended recipient knows of the existence of the data . Due to growing the need for security of data image steganography is gaining popularity . The main aim of steganography is to send secret data between sender and receiver to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data . However Steganography is used at a more complex level as detection is dependent on recognizing the secret data .

A. *Cryptography:*

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data-origin authentication. Cryptography protects the information by transforming it into an incomprehensible format. It is useful to achieve private transmission over a public network. Also, the original text, or plaintext, is transformed into a coded alike called cipher text via any encryption algorithm. Only those who hold a secret key can decipher (decrypt) the cipher text into plaintext.

Cryptography system can be classified into

– Symmetric key system
– Asymmetric key system
  - Symmetric key system: In symmetric key system uses the same key for both encryption and decryption. symmetric key system also known as private key crypto system.
  - Asymmetric key system: In asymmetric key system uses the different key for encryption and decryption.this type of crypto systems, there is no need for exchanging keys,this is eliminating the key distribution problem such type of systems can provide digital signatures.

B. *Different Kinds of Stegnography:*

Steganography, from Greek steganos, or "covered," and graphie, or "writing" is the hiding of a secret message within an ordinary message and the extraction of it at its destination. Steganography takes cryptography a step farther by hiding an encrypted message so that no one suspects it exists. Ideally, anyone scanning your data will fail to know it contains encrypted data.

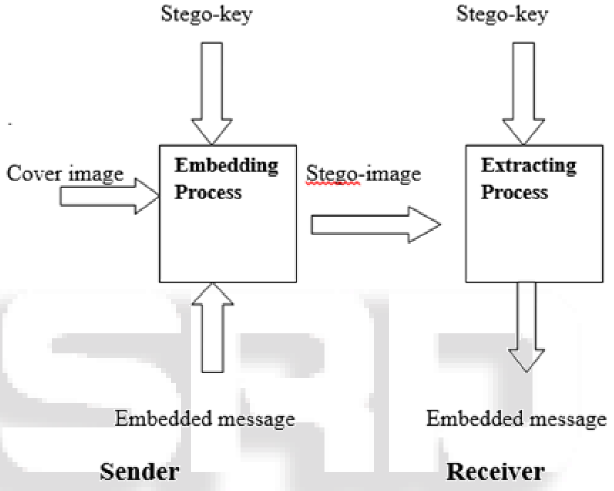

Fig. 1: Basic Steganography Model

The various types of steganography is following

– Image Steganography
– Audio Steganography
– Text Steganography
– Video Steganography
  - Image Steganography: In Image Steganography, it is an art of hidden writing behind an image even knowing by the unintended recipient that messege exists.
  - Audio Steganography: In Audio Steganography, we can hide secret data in audio file.
  - Text Steganography: If we can hide secret data in a text file, it is called as Text Steganography.
  - Video Steganography: if we hide secret data behind a video, it is called Video Steganography.

II. Difference between Steganography and Cryptography

Steganography	Cryptography
Steganography deals with composing hidden messages so that only the sender and the receiver know that the message even exists.	Cryptography is the study of hiding information and it is used when communicating over an untrusted medium such as internet, where information needs to be

	protected from other third parties.
Steganography does not alter the structure of secret message.	Cryptography alter the structure of secret message.
Little known technology	Common technology

Table 1:

Steganography Techniques: There are various types of hiding techniques to hide the secure data

- LSB Technique
- DCT Technique

A. LSB Technique:

1) Introduction:

Least significant bits (LSB) insertion is a simple approach of image steganography to embedding the secret information behind an image file. LSB technique is based on spatial domain. In spatial domain technique are based on direct manipulation of pixel in an image. The simplest steganographic techniques embed the bits of the message directly into least significant bit of the cover-image in a deterministic sequence. Modulating the least significant bit does not result in human-perceptible difference because the amplitude of the change is small.

2) Least Significant Bit Insertion:

In today, One of the most common techniques used in steganography is called least significant bit(LSB) insertion. In this method is exactly sounds like; the least significant bits of the cover-image are altered so that they form the embedded information.

The following example shows how the letter A can be hidden in the first eight bytes of three pixels in a 24- bit image.

Pixels: (00100111 11101001 11001000)(00100111 11001000 11101001)(11001000 00100111
11101001)

A: 01000001

Result: (00100110 11101001 11001000)(00100110 11001000 11101000)(11001000 00100111
11101001)

The three underlined bits are the only three bits that were actually altered. LSB insertion requires on average that only half the bits in an image be changed. Since the 8-bit letter A only requires eight bytes to hide it in, the ninth byte of the three pixels can be used to begin hiding the next character of the hidden message.

3) Advantages of LSB:

- The advantages of LSB are its simplicity to embed the bits of the message directly into theLSB plane of cover-image and many techniques use these methods .
- Modulating the LSB does not result in a human-perceptible difference because the amplitude of the change is small.Therefore, to the human eye, the resulting stego-image will look identical to the cover-image.This allows high perceptual transparency of LSB.

B. DCT Technique (Discrete Cosine Transform):

The Discrete Cosine Transform (DCT) algorithm is well known and commonly used for image compression. DCT converts the pixels in an image, into sets of spatial frequencies. It has been chosen because it is the best approximation of the Karhunen_loeve transform that provides the best compression ratio. The DCT work by separating images into the parts of different frequencies. During a step called Quantization, where parts of compression actually occur, the less important frequencies are discarded, hence the use of the lossy. Then the most important frequencies that remain are used retrieve the image in decomposition process. As a result, reconstructed image is distorted.

The Discrete Cosine Transform (DCT) transforms the image from spatial domain to frequency domain. DCT coefficients are obtained for the given carrier image. The secret data is embedded in the carrier image for DCT coefficients lower than the threshold value. To avoid visual distortion, embedding of secret information is avoided for DCT coefficient value 0.

1) Advantages of DCT Technique:

Compared to other input dependent transforms, DCT has many advantages :

1) It has been implemented in single integrated circuit.
2) It has the ability to pack most information in fewest coefficients.
3) It minimizes the block like appearance called blocking artifact that results when boundaries between sub-images become visible.

III. Conclusion

This Paper gives the review of two Steganography techniques,. Both has many advantages of image steganography. we can say that DCT technique is more better than the LSB insertion method. DCT provide the better security and the hacker does not detect the important data easily.

References

[1] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain "A New Approach for LSB Based Image Steganography using Secret Key", International Conference on Computer and Information Technology (ICCIT),Pages No. 286 – 291, 22-24 Dec., 2011.

[2] Swati Tiwari, R. P. Mahajan, "A Secure Image Based Steganographic Model Using RSA Algorithm and LSB Insertion", International Journal of Electronics Communication and Computer Engineering (IJECCE), Vol. 3, Issue No. 1, 2012.

[3] Wang C, Zhang W J. Adaptive reduction of blocking artifacts in DCT domain for highly compressed images[J] . IEEE Transactions on Consumer Electronics, 2004, 50 (2) : 647-654.

[4] Mamta Juneja, Parvinder Singh Sandhu, "Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption", International Conference on Advances in Recent Technologies in Communication and Computing, Pages No. 302 –305, 27-28 Oct.2014.