Volume 6, Issue 5, May 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Analytical Study of L.S.B & D.C.T Algorithm in Audio-Video Steganography

[1]Anupama Kaushik, [2]Nikhil Sharma, [3]Kirti Lakra, [4]Anshul Dabas, [5]Yagnish Dahiya
[1]Assistant Professor, [2, 3, 4, 5] Student of B.Tech (I.T.)
[1, 2, 3, 4, 5] Maharaja Surajmal Institute of Technology, Janakpuri, New Delhi, India

Abstract-- Steganography is the technique of hiding private or sensitive information within something that appears to be nothing out of the usual. In this paper audio-video steganography which is the combination of Audio steganography and Image steganography. In this paper our aim is to hide secret information behind audio and image of video file. As we know that video is the combination of many still frames of images and audio. We can select any frame of video and audio for hiding our secret data. In this research , we focus on the Least Significant Bit (LSB) technique in hiding messages in audio and Discrete Cosine Transform(DCT) in video. In this paper Least Significant Bit (LSB) based spatial domain technique and Sub band Discrete Cosine Transform (DCT) domain techniques are being analysed. Although LSB is best, but sub band DCT domain algorithm is more robust and secure as compared to LSB based technique.

Keywords-- Steganography, LSB, information hiding, DCT.

I. INTRODUCTION

In today's information technology era, the rise of the internet is one of the most important fact of information technology and communication due to this the security of the data and the information has raise concerned. So, great measures should be taken to protect the data and information[1]. One of the reasons that intruders can be successful is that most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of steganography. Steganography is a technique of hiding information in digital media. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists[1]. Plainly visible encrypted messages no matter how unbreakable will arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message. The primary objective of steganography is to avoid drawing attention to the transmission of hidden information. If suspicion is raised, then this objective that has been planned to achieve the security of the secret message because if the hackers noted any change in the sent message then this observer will try to know the hidden information inside the message[1].

Steganography is a Greek word which means concealed writing. The word "steganos" means "covered " and "graphial " means "writing" . Thus, steganography is not only the art of hiding data but also hiding the fact of transmission of secret data. Steganography hides the secret data in another file in such a way that only the recipient knows the existence of message. In ancient time, the data was protected by hiding it on the back of wax, writing tables, and stomach of rabbits or on the scalp of the slaves. But today's most of the people transmit the data in the form of text, images, video, and audio over the medium. In order to safely transmission of confidential data, the multimedia objects like audio, video, images are used as a cover sources to hide the data[2]. In the basic steganographic process, the secret message is hidden into a cover object. The cover object can be any of text, image, audio, video etc. A secret key is also used and the secret message is embedded into the cover object using the secret key. This new message obtained is called stego message. The stego message is transmitted over the public channel. The receiver gets the message and retrieves the message using the stego key which is same as used by the sender. In this way security is achieved by hiding the existence of the message[2].

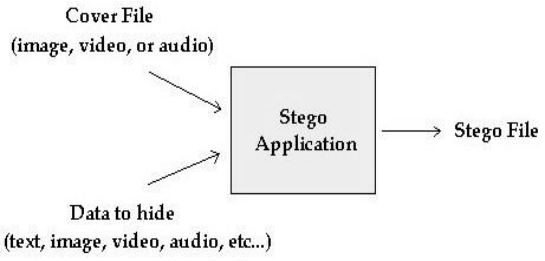

Fig 1: Steganography Application Scenario

The resulting stego also contains hidden information, although it is virtually identical to the cover file. What Steganography essentially does is exploit human perception; human senses are not trained to look for files that have information hidden inside of them, although there are programs available that can do what is called Steganalysis (Detecting use of Steganography.) [2]

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 [3].
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 [3].
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 [3].
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 (e.g., 8.667 to 9) which is used to hide the data in each of the images in the video, which is unnoticeable by the human eye. H.264, Mp4, MPEG, AVI are the formats used by video steganography[3].
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[3].

II. STEGANOGRAPHY REVIEW

In this review on Steganography is carried out and presented in detail. Communication has become inevitable in everybody's routine life. Be it e-mails, text, or photo or audio, video, they get communicated in millions among billions. There are many categories of information such as business, research, finance, etc. This information is traded between the countries and states for various purposes which require secure communication. Information security is the only solution which can give us secure information and help us to have a secure communication. Information security plays a pivotal role to keep the information safe. Among the prominent definitions for information security, the most vital of them is information security which is about veracity, discretion and data availability. Though several successful methods exist, they are still in research to boost up their performance. Undoubtedly, information security is a soul of exchange of data. Steganography. In their work new steganography technique is proposed in which multiple RGB images are embedded into single RGB image using DWT steganographic technique. The cover image is divided into 3 colors *i.e.* Red, Green and Blue color space. These three color spaces are utilized to hide secret information. Experimental results obtained using this system has good robustness[4].

We have gone through some papers and find out that utilization of both steganographic and cryptographic techniques in order to gain extra layer of security to the hidden data. This proposed a security scheme in which steganography is used along with cryptography to provide better security to embedded data. In their method first data is encrypted then it is embedded into cover image using steganographic method. Proposed algorithm transforms any kind of message into text with the help of manipulation tables, and then carries out hill cipher methods to it and finally hides the data into red, blue, and green pixels of the cover image[4].

Ishwarjot Singh ,J.P Raina from proposed a very innovative system that will combine the steganography and cryptography into one system. There will be no separate computations for steganography and cryptography. Hence this system needs lesser computations than existing methods, while maintain the higher security levels. Core of this system is LSB matching technique and Boolean function in stream ciphers. For steganography gray scale images are utilized and Boolean functions are applied for cryptographic purpose and to control the pseudo-random increment and decrement of LSBs. Experimental results shows that this system is very much safer from steganalysis attacks[4].

In 2014, there are three researches being reviewed, the first research is the survey of various audio steganography techniques, which is described by the comparison of various data security techniques followed by the comparison of various steganography techniques. The second research presents a different image steganography technique that takes two secret keys to randomize the bit hiding process. The paper proposes that the use of two secret keys will maintain the high data hiding capacity. The third research focuses on bitmap image format to implement LSB steganography method. The paper also proposes the use of AES algorithm to ensure two layer security of the message[4]

From the three consecutive years (2012-2014), the most preferred choice of the researchers is image Steganography techniques. There are four main categories that used in steganography that are image, audio, sound and protocol . Out of ten researchers, seven is proposing new techniques or methods in image steganography. Image files usually are comply with the requirements of creating a stego image but researchers are also focussing on other methods like audio, video, etc to hide the secret data[4].

III. PROPOSED WORK

Audio Steganography-

Audio Steganography involve hiding data in audio file. It basically hide the data in WAV, AU and MP3 sound files.

Methods used are i) Low Bit Encoding ii) Phase Coding iii) Spread Spectrum.

The basic model of Audio steganography consists of Carrier (Audio file), Message and Password. Carrier is also known as a cover-file, which conceals the secret information[5].

Basically, the model for steganography is shown in Fig 2. Message is the data that the sender wishes to remain it confidential. Message can be plain text, image, audio or any type of file. Password is known as a stego-key, which ensures that only the recipient who knows the corresponding decoding key will be able to extract the message from a cover-file. The cover-file with the secret information is known as a stego-file.

Advantages or applicability as we discuss below[5].

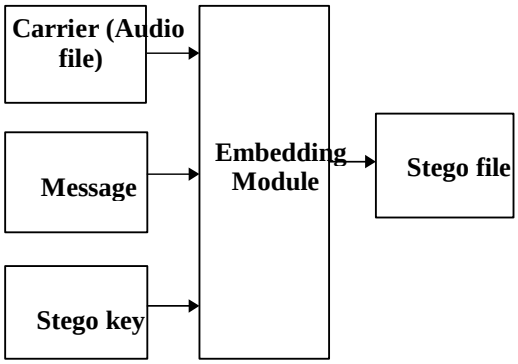

Fig 2: Audio Steganography process

Audio steganographic method:

Technique used for audio steganography in this research is LSB (Least Significant Bit) Coding.

Least Significant Bit (LSB) Coding:

A very popular methodology is the LSB (Least Significant Bit) algorithm, which replaces the least significant bit in some bytes of the cover file to hide a sequence of bytes containing the hidden data. That's usually an effective technique in cases where the LSB substitution doesn't cause significant quality degradation, such as in 24-bit bitmaps[6].

In computing, the least significant bit (LSB) is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. The LSB is sometimes referred to as the right-most bit, due to the convention in positional notation of writing less significant digit further to the right. It is analogous to the least significant digit of a decimal integer, which is the digit in the ones (right-most) position[6].

1	0	0	1	0	1	0	1

Fig 3: Binary representation of decimal 149

The binary representation of decimal 149, with the LSB highlighted. The MSB in an 8-bit binary number represents a value of 128 decimal. The LSB represents a value of 1. For example, to hide the letter "a" (ASCII code 97, which is 01100001) inside eight bytes of a cover[6], you can set the LSB of each byte like this:

10010010
00101011
10011011
11010010
10001010
00000010
01110010
00101011

The application decoding the cover reads the eight Least Significant Bits of those bytes to recreate the hidden byte—that is 0110001—the letter "a." As you may realize, using this technique let you hide a byte every eight bytes of the cover. Note that there's a fifty percent chance that the bit you're replacing is the same as its replacement, in other words, half the time, the bit doesn't change, which helps to minimize quality degradation[6].

Steps to hide secret information using LSB are:

a. Covert the audio file into bit stream.
b. Convert each character in the secret information into bit stream.
c. Replace the LSB bit of audio file with the LSB bit of character in the secret information[6].

Video steganography-

Video Steganography is a technique to hide any kind of files into a carrying Video file. The use of the video based Steganography can be more eligible than other multimedia files, because of its size and memory requirements. The least significant bit (LSB) insertion is an important approach for embedding information in a carrier file. Least significant bit (LSB) insertion technique operates on LSB bit of the media file to hide the information bit. In this project, a data hiding scheme will be developed to hide the information in specific frames of the video and in specific location of the frame by LSB substitution using polynomial equationof an image, it can be done in such a way that the human eye will not notice

the anomalies. Since masking uses visible aspects of the image, it is more robust than LSB modification with respect to compression, cropping and different kinds of image processing. The information is not hidden at the "noise" level but is inside the visible part of the image, which makes it more suitable than LSB modifications in case a lossy compression algorithm like JPEG is being used[7].

Video steganographic method:

Technique used for video steganography in this research is DCT (Discrete Cosine Transform).

Discrete Cosine Transform (DCT) method -

DCT coefficients are used for JPEG compression . It separates the image into different parts of importance. It transforms a signal or image from the spatial domain to the frequency domain. It separates the image into high, middle and low frequency components. In low frequency sub band, much of the signal energy lies at low frequency which contains most

important visual parts of the image, while in high frequency sub band, high frequency components of the image are usually removed through compression and noise attacks . So the secret message is embedded by modifying the coefficients of the middle frequency sub band, so that the visibility of the image is not affected [8].

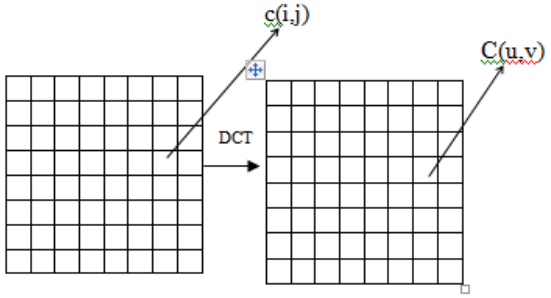

Fig 4: Discrete Cosine Transform of an Image

Signal energy lies at low frequency in image; it appears in the upper left corner of the DCT. Compression can be achieved since the lower right values represent higher frequencies, and generally small enough to be neglected with little visible distortion[8].

DCT is used in steganography as- Image is broken into 8×8 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[8].

IV. PERFORMANCE AND RESULT

The analysis of LSB based and DCT based steganography has been done on basis of parameters like PSNR,MSE(Mean Square Error), Processing time, security. PSNR computes the peak signal to noise ratio, in decibels, between two images. This ratio is used as a quality measurement between two images. If PSNR ratio is high then images are best of quality[9].

Table 1 Parameters Analysis of Both Steganograph Methods

Features	**LSB**	**DCT**
Invisibility	Low	High
Payload capacity	High	Medium
Robustness against statistical attacks	Low	High
Robustness against image manipulation	Low	Medium
Independent of file format	Low	Medium
PSNR	High	Medium
M SE	Less	Medium

In this paper analysis of LSB & 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 background 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[9].

V. FUTURE SCOPE

In this modern era of technology, with the increase in the need of secure and robust communication, the Information and technology sector looks towards the future research in the field of Steganography, as cryptography alone cannot provide a secure communication. Some future researches may include[10]:

1. Developing a system by combining the benefits of both cryptography and steganography
2. Developing an environment which should be platform independent.
3. Considering different media other than images, video i.e. the traditional media
4. Use of best algorithms to achieve a secure and a robust communication[10].

VI. CONCLUSION

The paper presented above gives a understanding of cryptography and steganography concepts, along with it the paper gives a review of the research and developments in the field of steganography through the various steganography techniques. The paper also provides the suggestion regarding the future researches in the field of steganography[10].

REFERENCES

[1] T. Morkel J.H.P. Eloff and M.S. Olivier "*An Overview Of Image Steganography*".
[2] https://en.wikipedia.org/wiki/Steganography
[3] http://www.ijettjournal.org/volume-11/number-8/IJETT-V11 P276.pdf
[4] Ishwarjot Singh ,J.P Raina," *Advance Scheme for Secret Data Hiding System using Hop field & LSB*" International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 7–July 2013.
[5] http://airccse.org/journal/jma/3311ijma08.pdf
[6] http://repository.um.edu.my/401/5/Chapter_2_.pdf
[7] http://www.ijcsit.com/docs/Volume%205/vol5issue01/ijcsit 2014050167.pdf
[8] https://globaljournals.org/GJCST_Volume10/gjcst_vol10_ issue_1_paper8.pdf
[9] http://www.ijsett.com/images/Paper(4)35-41.pdf
[10] Swati malik, Ajit "*Securing Data by Using cryptography with Steganography*" International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 5, May 2013.

