IMAGE AND WAVE STEGANOGRAPHY

Ashwin P Ajith[1], Chaitanya Bachhav[2], Dipyaman Paul[3], L. Sai Kiran Reddy[4], Jishnu Ghosh[5], Caroline El Fiorenza[6]

[1]*Computer Science & Engineering, SRM Institute of Technology, Ramapuram, Chennai, India*

[2]*Computer Science & Engineering, SRM Institute of Technology, Ramapuram, Chennai, India*

[3]*Computer Science & Engineering, SRM Institute of Technology, Ramapuram, Chennai, India*

[4]*Computer Science & Engineering, SRM Institute of Technology, Ramapuram, Chennai, India*

[5]*Computer Science & Engineering, SRM Institute of Technology, Ramapuram, Chennai, India*

[6]*Computer Science & Engineering, SRM Institute of Technology, Ramapuram, Chennai, India*

Abstract

It is said that in this age of information technology privacy is a myth, however, the field of information security is also developing. The science of using codes and semantics to protect information exists since time immemorial. Steganography deals with hiding sensitive information (not just encrypting). In this project we'll hide data in images and audio waves, by encoding it in the RGB values of the image and by manipulating certain parts of the audio wave such that the data reaches the receiver without any loss. We'll be using the SH-1 algorithm which implements secure hashing to generate the encoding bits, so as to hide the data in the wave-form. The information/data goes through the compression and encryption processes and then is encoded in the carrier image. At the receiver's end the cover image is input, once confirmed that it is a steg-image the data can be retrieved.

Keywords - *Steganography;Security; Encryption; Hiding Data; SHA-1; Python; PIL*

I. INTRODUCTION

Steganography is a special branch of information hiding where a secret message is embedded in a cover image based on a shared stego key, resulting in a stego image. In contrast to steganography, steganalysis aims to detect or extract the hidden data in those stego images. The steganographic algorithm is considered to be broken if an attacker can decide whether or not a given image is a stego image, based on steganalysis with a higher probability of detection instead of just random guessing. Steganography requires a carrier object, secret data and an embedding algorithm. It also requires an encryption algorithm and a secret key in some cases, increasing the security levels of steganography. Applications of steganography includes secure transmission of top-secret documents between national and international governments, captioning, tamper-proofing, securing online banking, voting systems, and time-stamping. Watermarking and cryptography are two closely related areas to steganography. The main theme of steganography and cryptography is same, i.e., to obscure the secret information, but the corresponding techniques used in both areas are different. The procedure of steganography and watermarking are similar, carrying different purposes. Steganography deals with the embedding of secret data while watermarking is concerned with copyright protection of digital data. There is a very slight difference between Steganography and Cryptography. People often think that these two terms are the same or have the same meaning. But that's not the case. Cryptography on one hand is collection of techniques used to ensure secure transmission of data over a channel. Steganography on the other hand is the hiding of a secret message within an ordinary message, such as an image or various other media, 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.

II. LITERATURE SURVEY

Mr. A. Balasubramani et al. [1] has shed some light on Steganography. In the paper he has briefly explained about Steganography and the difference between Steganography and Cryptography.

Ruchika Patel et al. [2] has explained the watermarking technique and how it is used to make sure that the hidden message stays secret.

T.Santanam et al. [3] has explained various steganography techniques. He has also explained all the three techniques i.e, Pure Steganography, Secret key steganography and Secret key steganography.

Suresh Gawande et al. [4] has gone through different Steganography methods. The methods which he has discussed are Substitute method, Spread Spectrum and Audio Steganography.

Palwinder Singh et al. [5] tells us about Audio Steganography.It's a way of hiding information in plain sight is by using audio waves as cover. This type of information hiding is known as audio steganography.

Qilin Qi et al. [6] has discussed about various known countermeasures against Staganography. He has discussed mostly all of the techniques to find out hidden data in images, audio and video files.

III. SYSTEM ARCHITECTURE

Fig. 1: Data Hiding

Least Significant Bits is perhaps the simplest steganographic method. It is most commonly known as LSB. In this the secret data is hidden inside a cover image. With this method, the least significant bits of the carrier image pixels are replaced with the secret data bits. Payload capacity of the LSB varies depending on the number of LSBs used for message embedding, but it also results in noticeable changes in the carrier or cover image. A pixel is the unit of an image and each pixel is a combination of three basic colors, Red, Green and Blue(RGB). Each RGB combination in each pixel decides the color of that pixel. In LSB the least significant bit is replaced by the bits, which contain the secret information. Since the bit replaced is of least significance, so replacing it with another bit doesn't affect the image that much. But we still have to make sure that we shouldn't add too much information in the cover image or anyone will be able to distinguish between a normal image and it's stego-image. Another way of hiding information in plain sight is by using audio waves as cover. This type of information hiding is known as audio steganography. In audio steganography, secret message is embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio file. There are several methods are available for audio steganography. We are going to have a brief introduction on some of them. LSB Coding Sampling technique followed by Quantization converts analog audio signal to digital binary sequence. In this technique LSB of binary sequence of each sample of digitized audio file is replaced with binary equivalent of secret message. This LSB technique is the same one which is used to store secret information in images or cover texts. Phase Coding Human Auditory System (HAS) can't recognize the phase change in audio signal as easy it can recognize noise in the signal. The phase coding method exploits this fact. This technique encodes the secret message bits as phase shifts in the phase spectrum of a digital signal, achieving an inaudible encoding in terms of signal-to- noise ratio. Spread Spectrum There are two approaches are used in this technique: the direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS).

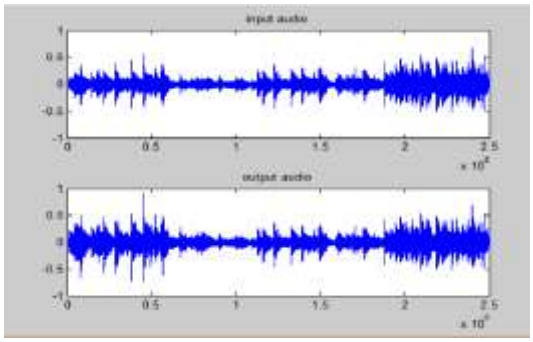

Fig. 2: Audio Steganography by Direct Sequence Spread Spectrum

IV. CONCLUSION

In this paper different steganographic articles were studied and were categorized into different techniques. As many new application areas are identified like internet banking, mobile communication security, cloud security etc., the insight into the steganographic principles will definitely guide us to identify new areas and to improve its applications in the already existing application areas also. As more and more powerful computers are being built everyday, the chances of a secret message getting decrypted is also increasing with the launch of more powerful computers. That's why more and more people are researching on the ways in which they can hide information in images, audios, videos, etc. More and more covers and ways are being found everyday in order to hide these secret messages.

V. FUTURE WORKS

With the rapid increase in movie files exchanged over the Internet (YouTube, etc.) a huge haystack to hide or exchange covert information exists today, and the size of this haystack is predicted to increase exponentially over the next decade. Clearly this provides a new method for pedophiles to exchange their content through innocuous sharing of benign looking digital media, and criminals, or worse, to continually exchange large amounts of clandestine information.

VI.ACKNOWLEDGMENT

The authors would like to thank Ms.Caroline El Fiorenza for the constant encouragement, timely support and guidance which helped us in successfully completing our proposal.

VII.REFERENCES

[1] Mr. A. Balasubramani, Dr. Chdv. Subba Rao, "Sliced Images and Encryption Techniques in Steganography Using Multi Threading For Fast Retrieval", International Journal of Applied Engineering Research, Volume 11, Issue No. 9, November-2016.

[2] Ruchika Patel, Parth Bhatt, "A Review Paper on Digital Watermarking and its Techniques", International Journal of Computer Applications, Volume 110, Issue No. 1, January-2015.

[3]C.P.Sumathi,T.Santanam,G.Umamaheswari,"A Study of Various Steganographic Techniques Used for Information Hiding", International Journal of Computer Science & Engineering Survey, Volume 4, Issue No. 6, December 2013.

[4] Rakhi, Suresh Gawande, "A REVIEW ON STEGANOGRAPHY METHODS",International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Volume 2, Issue No. 10, October 2013.

[5]Palwinder Singh, "A Comparative Study of Audio Steganography Techniques",International Research Journal of Engineering and Technology, Volume 3, Issue No. 4, April-2016.

[6] Qilin Qin, "A Study on Countermeasures against Steganography: an Active Warden Approach", Theses, Dissertations, & Student Research in Computer Electronics & Engineering. 25., December-2013.