Advanced Research in Electrical and Electronic Engineering
p-ISSN: 2349-5804; e-ISSN: 2349-5812 Volume 5, Issue 2 April-June, 2018, pp. 162-164

http://www.krishisanskriti.org/Publication.html

Survey on an Audio Steganography using DWT and Triple DES Techniques

Chethan M.D.[1], Anitha Devi M.D.[2] and Dr. M.Z. Kurian[3]

[1]M Tech student, Digital Electronics, Dept. of ECE, SSIT, Tumakuru, India
[2]Assistant Professor, Dept. of ECE, SSIT, Tumakuru, India
[3]HOD Dept. of ECE, SSIT, Tumakuru, India
E-mail: [1]chethanmd.cit@gmail.com, [2]anumdssit@gmail.com, [3]mzkurianvc@yahoo.com

Abstract—*Information hiding is a general term of embedding messages in the content. The term hiding refers to either producing the data to be hidden or making the existence of secret information unnoticeable. Different techniques are used to hide the information, in that audio steganography is the one. Audio Steganography using DWT and triple DES is a technique used to transmit hidden information by modifying an audio signal in an imperceptible manner. It is the science of hiding some secret text or audio information in a host message. The host message before steganography and stego message after steganography have the same characteristics. This paper provides an up-to-date critical survey on different techniques used along with audio steganography. In the process of system development literature reviews conducted to understand the theory, methods and technologies associated with the audio steganography that have been developed.*

Keywords*: Audio steganography, DWT, Triple DES.*

1. INTRODUCTION

When two entities are communicating, security is one of the major concerns. Data needs to be concealed when it is transmitted over the network to protect it from intruders. When it comes to ensuring data confidentiality [1], one can use either cryptography or steganography. In the approach presented in this paper, a steganography is proposed. This ascertains greater security of the secret information. Audio steganography is a technique in which the secret data is embedded into the cover audio, with the secret message invisible to unauthorized users. There are three requirements for any steganography system - perceptual transparency, hiding capacity and robustness [2]. After embedding the message, the stegno audio is obtained. At the receiver's end the hidden data can be extracted from the stegno signal using the reverse algorithm.

2. LITERATURE SURVEY

All authors in [1] have proposed a two level data security comprising of text cryptography and image steganography. The secret text is encrypted using Blowfish algorithm followed by embedding it into an image using LSB encoding. The carrier image can be then transmitted over the network. In [2], authors have suggested an algorithm in which the data is first subjected to encryption using Data Encryption Standard (DES). The encrypted message is then passed to embedding phase. In embedding phase the encrypted message will embedded into the cover medium which is either image or audio or video resulting in a stego medium. The embedded stego medium contains the encrypted text message which is extracted at the receiver side. The extracted text is decrypted using decryption module.

Authors in [3] have put forward an algorithm in which the secret data is first encrypted using AES algorithm. This encrypted data is then embedded into an audio file. The authors then encrypt the audio file using Spread Spectrum technique before transmitting it over the network.

In [4], authors have proposed two methods of hiding data into an audio signal using LSB coding. One is considering parity of the digitized samples of cover audio in which the parity of the samples are checked before data embedding. The other approach is considering the XOR operation. This method performs XOR operation on the LSBs and then depending on the result of XOR operation and the message bit to be embedded, the LSB of the sample is modified or kept unchanged.

S Poongodi .[5], Proposed a technique used to hide data inside an image for high security. The data is hidden in such a way that the exact or original data is not visible. The hidden data can be retrieved as when required. The scheme of RDH technique is achieved through color image instead of gray scale image to improving the capacity to hidden data. Initially for more privacy protection content owner encrypt the original image using encryption key. Then, compress the LSB bits to create sparse space for accommodating hidden data using data hiding key. By using both the keys the receiver can extract hidden data and recover the original image without any error. If the receiver has only the data hiding key or only encryption key such that the receiver can get only hidden data or only decrypted image.

Amitava Nag and Sushant Biswas [6] Developed a novel technique for image steganography based on DWT. Where DWT is used to transform original image from spatial domain to frequency domain. First 2-D DWT is performed on a gray level cover image of size M × N and Huffman encoding is performed on the secret message/ image before embedding. Then, each bit of Huffman code of secret message/image is embedded in the high frequency coefficients resulted from DWT. Image quality is to be improved by preserving the wavelet coefficients in the low frequency sub-band. Their experimental results show that the algorithm has a high capacity and a good invisibility.

Zhiecheng Ni, Yun-Qing Shi et.al [7], Suggested a reversible data hiding (RDH) scheme for gray scale cover images with highly sensitive cover content. Their work exploits least complexity in computation by incorporating histogram shifting method to embed secret bits in confused cover, where cover confusion has been implemented using logistic map fuction. So to achieve high capacity or configurable embedding rates, they implemented multilevel peak point embedding mechanism is used while embedding the secret bits, confused cover with embedded data alone or marked stego cover generated using any transposition algorithm for confusion are applied to several statistical, plain text and brute force attacks. Hence they introduced data embedding in confused cover followed by successive multi-level encryption scheme in association with Arnold cat map function and chaotic systems.

Pye Pye Augn and Tun Min Naing [8] proposed technique used with the combination of cryptography and steganography, it enhanced with new secure feature for generating a new security system. Cryptography and steganography are two popular ways for secure data transmission in which the former distort a message so it cannot be understood and another hides a message so it cannot be seen in cryptography, in this work they suggested to use AES algorithm to encrypt secret message and then these are separated keys: one of which is used to hide in cover image. In steganography, a part of encrypted message as a key is used to hide in discrete cosine transform (DCT) of an image which is highly secured. This kind of system is to be introduced in application such as transferring secret data that can be authentication of various fields.

Vignesh kumar [9], Developed a Digital steganography, which explains the art and science of writing hidden messages in such a way that, apart from the sender and intended recipient no one suspects the existence of the message a form of security through the state of being known. The main two scheme used for image steganography are spatial domain embedding and transform domain embedding. The main aim of using wavelet transform is to transform original image from spatial domain to frequency domain. But here integer wavelet transform is performed on a gray level cover image and in turn embeds the message bit stream into the LSBs of Integer wavelet coefficients of the image. The main purpose of this is to improving embedding capacity and brings down the distortion occurring to the stego image. The implementation of wavelet transforms that map integer to integer in the area of image steganography allowed the embedded message to be recovered without loss. Then the proposed algorithm holds the bit stream in the LSB bits of the transform coefficients. It does not affect the integrality of the embedded coefficients. The experimental results show that the algorithm has a high capacity and good invisibility.

Harsh Prayagi and Tushar Srivatava [10], proposed a Steganography technique which plays the important role in information security. Since the rise of the internet one of the most important factors on information technology and communication has been the security of information. Many different file formats can be used but digital images are the most popular because of their frequency on the internet. For hiding secret information in images, there exist a large variety of steganography techniques some are more complex than other and all of them have respective strong and weak points. Steganography is the art and science of writing the hidden messages in such a way that no one, apart from the sender and intended recipient, suspect the existence of message, a form of security through obscurity. Generally, messages will appears to be something else: images, articles, shopping lists or some other convert Ext and classically, the hidden message may be in invisible ink between the visible lines of private letter. Steganography is the science that involves communicating secret data in an appropriate multimedia carrier e.g. image, audio and video files. Steganography is the art of hiding the fact that communication is taking place by hiding information in other file formats can be used, but digital images are the most popular because of their frequency on the internet. For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. So we prepare this application to make the information hiding simpler and user friendly. The user has two tab options- encrypt and decrypt. If the user select encrypt, application gives the screen to select image file, information file and option to save the image file. If the user select decrypt, application gives the screen to select only the image file and ask path where user wants to save the secret file. This paper has two methods- Encryption and Decryption. In encryption the secret information is hiding in with any type of image file. Decrypt is getting the secret information from image file.

H. Golpira and H. Danyali [11] proposed a reversible blind watermarking for medical images based on wavelet histogram shifting. In this work medical image such as MRI is used as host signal. A two dimensional wavelet transform is applied to the image. Then, the histogram of the high frequency subbands is determined. Next, two thresholds are selected, the first is in the beginning and the other is in the last portion of the histogram. For each threshold a zero point is created by shifting the left histogram part of the first threshold to the left,

and shifting the right histogram part of the second threshold to the right. The locations of the thresholds and the zero points are used for inserting the binary watermark data. This algorithm performs well for MRI images but not for ECG host signals. Moreover, the capacity of these algorithms is low. Moreover, no encryption key is involved in its watermarking process.

Researchers have challenged countless issues that related to reliability, confidentiality, availability, security, precision and the rest. Researchers have proposed several methods to solve these problems. Digital watermarking is one of the keys of these problems. In this technique, secret information will hide inside the host signal operating confidential key. Subsequently, stego signal is received. Stego signal is transmitted to the receiver via internet. This process is called encoding. The receiver is extracted that secret information from the signal using same secret key. This process called decoding. There are numerous procedures for procuring patient confidential information. Steganography technique is widely used for securing the information. In steganography, original information hides inside the alternative cover (images, video, and audio) and forms the embed message. The embedded message delivers to the authorized person via internet and authorized person extracts the actual information from alternative cover. Steganography technique is based on encryption and decryption process but it is not enough to secure patient information. We have implemented a new technique, which is established on wavelet transforms.

3. CONCLUSION

As discussed earlier, security of information over the internet is becoming a major concern. In this paper, the authors made an effort to know the different techniques to safeguard information from intruders using an amalgamated approach of audio steganography using DWT and Triple DES. The secret data is first encrypted which is embedded into an audio file and then this audio file is encrypted before being transmitted over the network. This ensures that even if the audio file is intercepted by an unauthorized person, the person doesn't discover the secret information.

REFERENCES

[1] Komal Patel, Sumit Utareja, Hitesh Gupta, “Information Hiding using Least Significant Bit Steganography and Blowfish Algorithm”, International Journal of Computer Applications (0975 – 8887) Volume 63– No.13, February 2013

[2] V. Lokeswara Reddy, A Subramanyam , P Chenna Reddy, “A Novel Approach for Hiding Encrypted Data in Image, Audio and Video using Steganography”, International Journal of Computer Applications (0975 – 8887) Volume 69– No.15, May 2013

[3] Md. Shafakhatullah Khan, V.Vijaya Bhasker, V. Shiva Nagaraju, “An Optimized Method for Concealing Data using Audio Steganography”, International Journal of Computer Applications (0975 – 8887) Volume 33– No.4, November 2011

[4] H.B.Kekre, Archana Athawale, Swarnalata Rao, Uttara Athawale, “Information Hiding in Audio Signals”, International Journal of Computer Applications (0975 – 8887) Volume 7– No.9, October 2010

[5] Navjot kaur and Usvir kaur, “An audio watermarking using Arnold transformation with discrete wavelet transform (DWT) and discrete cosine transform (DCT).”*et al/ International journal of computer science engineering* vol. 2,no 06, Nov 2013 .

[6] K. Malasri and L. Wang, “Addressing security in medical sensor networks,” in *proc*. 1st *ACM SIGMOBILE Int workshop syst. Netw. Supp. Healthcare Assist. Living Environ*.,2007,p.12.

[7] H. wang, D. Peng, W. Wang, H. Sharif, H. chen, and A. Khoynezhad, “Resource- aware secure ECG healthcare monitoring through body sensor networks,” *IEEE Wireless Commun., vol. 17,no. 1,pp.* 12-19, Feb. 2010.

[8] Ayman and Ibrahim Khalil, “Wavelet-Based ECG steganography for protecting patient confidential information in point-of-care system,” *IEEE Transactions on biomedical Engineering, Vol. 60, No. 12, December 2013*

[9] Dr PrenaMahajan and Abhishek Suchdeva, “A study of encryption algorithm AES, DES, AND TDES FOR security,” *Global Journal of Computer Science and Technology Network, web and security* volume 13, issue 15 version 1.0 year 2013.

[10] Ganesh, G. Balasubhramanian, S.K, Jena, Pradhan,” Simulation results for wavelet approximation,” RGPA, no. 16, May 2012.

[7] H. Golpira and H. Danyali, “Reversible blind watermarking for medical images based on wavelet histogram shifting,” in *IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), 2009*.

[14] Unik Lokhande, A. K. Gulve, “Steganography using Cryptography and Pseudo Random Numbers”, International Journal of Computer Applications (0975 – 8887) Volume 96– No.19, June 2014

[17] D R Stinson, “Cryptography Theory and Practice”, 3rd Edition [18] William Stallings,” Cryptography and Network Security”, 5th Edition