**IOSR Journal of Engineering (IOSRJEN)** **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 07, Issue 10 (October. 2017), ||V1|| PP 12-16

# A Novel Technology For Identification Of Terrorist Information Transmitted Through In Social Media (WhatsApp)

Nishtha Pateriya [#1], Dr. Tripti Arjariya [*2]
[#]*M-Tech, Bhabha Group of Institute Bhopal,* [*]*HOD of (CSE), Bhabha Group of Institute Bhopal, (M.P.) India*
*Corresponding Author: Nishtha Pateriya*

**Abstract:** A new era where terrorist use Audio File steganographysocial media. In this research paper region-adaptive steganography algorithm which will be used for the novel technic to detect steganography attacks. We propose the major advantages of the proposed steganography detection technique is Spread Spectrum. A combination of Echo Hiding discrete wavelet transform and least significant bit (LSB) coding technique is also a steganography embedded technique on different regions of the host Audio File. In addition, there is a novel use the Echo Hiding discrete wavelet transform and least significant bit (LSB) coding technique steganography technique as a means to detect if certain types of attack have occurred in audio file media using WhatsApp. The severity of these attacks can be adjusted by modify their corresponding parameter values and easily transmitted in WhatsApp or other social media. In this paper a new algorithm proposed for detection hidden data from the original Audio Filetransmitted through WhatsApp and **has**little relation with secret message file. It was providing more security to the information.

**Keywords**-Echo Hiding discrete wavelet transform and least significant bit (LSB) coding technique, Audio Filesteganography, Audio Fileencryption, Linear Classifier,Message Encryption

---

Date of Submission: 26-09-2017 Date of acceptance: 18-10-2017

---

## I. INTRODUCTION

An audio steganography technique can be classified into two groups based on the domain of operation. One type is time domain technique and the other is transformation based method. The time domain techniques include methods where the embedding is performed without any transformation. Steganography is employed on the original samples of the audio signal. One of the examples of time domain steganography technique is the least significant bit (LSB) method. In LSB method the watermark is embedded into the least significant bits of the host signal. As against these techniques, the transformation based steganography methods perform steganography in the transformation domain. Few transformation techniques that can be used are discrete cosine transform and discrete wavelet transform. In transformation based approaches the embedding is done on the samples of the host signal after they are transformed. Using of transformation based techniques provides additional information about the signal. In general, the time domain techniques provide least robustness as a simple low pass filtering can remove the watermark. Hence time domain techniques are not sensible for the applications such as copyright protection and airline traffic monitoring; however, it can be used in applications like proving ownership and medical applications [1].

**Figure 1.** Binary model for audio data and text data architect

Steganalysis is the discovery of the existence of hidden information; therefore,like cryptography and cryptanalysis, the goal of Steganalysis is to discover hiddeninformation and to break the security of its carriers [2].

Types of attacks used by the steganalystStego-only attack: Only the stego-object is available for analysis. For example,only the stego-carrier and hidden information are available.

Known cover attack: The original cover-object is compared with the stego-objectand pattern differences are detected. For example, the original image andthe image containing the hidden information are available and can be compared.

However, one of the mostsignificant problems, which affect the commerce ofdigital media, is how to protect copyright andownership. Digital steganography, one of the popularapproaches considered as a tool for providing thecopyright protection, is a technique based on embeddinga specific mark or signature into the digital products.While several steganography algorithms have beenproposed [3], transform domain schemes, such asdiscrete wavelet transform (DWT) based steganographyhave shown more advantages and provide higherperformance than others.As one of the most popular and viable techniques in protecting copyrights in digital media, steganography technology has received enormous level of attention of researchers and practitioners alike. Unfortunately, due to the same reason, steganography technology also attracted the attentions of hackers, criminals alike who are interested in breaking the steganography's in order to crack the protection system. The result, there is a constant challenge on the researchers to keep improving the robustness of the steganography technique while at the same time maintaining its transparency as to not intruding any legitimate use of the media. Progress in this area has been steady as can be seen from a healthy number of publications in the field and the sheer number of institutes around the world that deal with the issue [4]. In the more specific field of digital Audio Filesteganography, one of the most notable techniques is region-based Audio Filesteganography [5]. The paper described a method for embedding and detecting chaotic steganography's in large Audio Files. An adaptive clustering technique is employed in order to derive a robust region representation of the original Audio File. The robust regions are approximated by ellipsoids, whose bounding rectangles are chosen as the embedded area for the steganography. The drawback of this technique is due to limited number of suitable regions for storing the steganography the steganography storing capacity can be low.

Most first generation digital steganography algorithm embedded the steganography into the timedomain samples or transform domain to transform coefficients, but this leads to a poor robustnessof time domain algorithms to the signal processing like compression, noise and filtering, transformdomain steganography uses the idea of audio masking effect and spreads spectrum technology toimprove the robustness, simultaneous reduces the performance of anti-synchronization attack.In the field of digital audio steganography, the idea is to use the stable feature points of the audio to mark the embedded position of the steganography, and use the stable performance of these feature points anti-synchronized attacks to improve the ability of the steganography anti-synchronization attack. Feature points should have the feature such as stability, more uniform distribution and the ability to accommodate the steganography [6].

## II. RELATED WORK

In this Research paper [7] here they with the emergence of steganography, the counter technology, namely Steganalysis has also emerged. Steganalysis is used to detect or extract the hidden message from the carriers. It is a set of techniques: visual or statistical by which it is possible to check for the existence of steganography content in cover object. Steganalysis could be passive or active. Passive Steganalysis simply aims to identify the presence or absence of secret message whereas Active Steganalysis attempts to estimate the message length, secret key, message bits, etc. Current Steganalysis techniques emphasize on the design of the classifier based on the training set of cover objects and stego objects obtained from a variety of different embedding algorithms. The inherent features of natural Audio File get violated when an Audio File undergoes some embedding process; classification is done on the basis of the some of these features. The extraction of sensitive features and design of good classifier are the principal tasks for Steganalysis.

Digital Audio Files are easy to manipulate and modify for ordinary people [9]. This makes it more and more difficult for a viewer to check the authenticity of a given digital Audio File. Copy-move forgery is a specific type of Audio File tampering where a part of the Audio File is copied and pasted on another part generally to conceal unwanted portions of the Audio File. This research work present an improved algorithm based on Discrete Wavelet Transform (DWT) and Discrete Cosine Transform Quantization Coefficients Decomposition (DCT-QCD) to detect such cloning forgery. The proposed scheme accurately detects such specific Audio File manipulations as long as the copied region is not rotated or scaled and copied area pasted as far as possible in specific position from original portion.

For efficiently verifying the integrity of Audio Files cannot, therefore, is overemphasized in this digital era. The primary task of a copy-move Audio File forgery detection algorithm is to determine if a given Audio File contains cloned regions without prior knowledge of their shape and location. An obvious approach is to

exhaustively compare every possible pair of regions. However, such an approach is exponentially complex. The drawback with schemes based on steganography is that the water mark must be embedded right during the Audio File formation to avoid the possibility of steganography an already forged Audio File. This is practically difficult as most digital cameras and other Audio File acquisition devices do not have instantaneous steganography facilities.

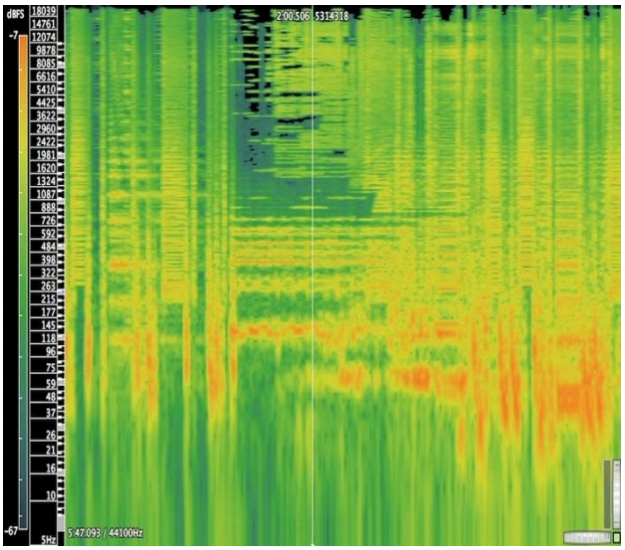

**Figure 2.** Basic Audio Signal Spectrum sample for steganography model

In this research paper [10], Steganalysis is the art and science of detecting the embedded message in a multimedia document, this document may be text, Audio File, audio or video. Many studies focus on review the Steganalysis algorithm based on steganography and Steganalysis classification. This paper will review the Audio File Steganalysis techniques based on Audio File type format classification, from Audio File format point of view, focusing on the main and the most commonly used format JPEG, BMP, GIF and PNG.

## III. PROPOSED ALGORTHM

The proposed steganography attack detection scheme requires the certain threshold of original Audio Files and steganographyAudio File.

Steganography is an information hiding technique where secret message is embedded into unsuspicious cover signal. An effective audio stenographic scheme should possess the following three characteristics: Inaudibility of distortion (Perceptual Transparency), Data Rate (Capacity) and Robustness. These characteristics (requirements) are called the magic triangle for data hiding.

**Algorithm:**
**Input:** Audio File, Data in text format
**Output:** Extracted data f found

*Step: 1. Taken original Audio File which is send by host through WhatsApp $HA_i$and $TA_i$.*
*Step: 2. Converting $HA_i$ and $TA_i$in to binary.*
*Step: 3. Identify any extra binary value $HA_i$ and $TA_i$.*
*Step: 4. If $HIB_i$ and $TIB_i$ had any value then.*
*Step: 5. Calculating SNR and Time of $HA_i$ and $TA_i$..*
*Step: 6. Generating Spectrum file of both files.*
*Step: 7. Matching SNR of $HA_i$ and $TA_i$.*
*Step: 8. If match = true*
*Step: 9. File free from attack*
*Step: 10. Else*
*Step: 11. File had some hidden data*
*Step: 12. Extract Hidden data*

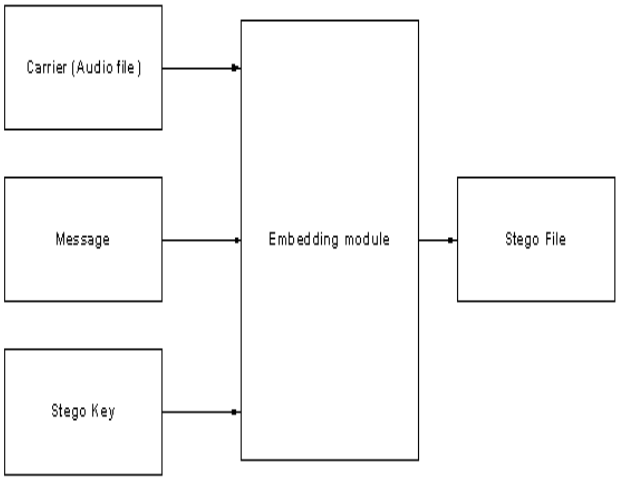


**Figure 3**. Basic Audio steganography model

In the proposed algorithm have presented a high capacity and high stego-signal quality audio steganography scheme based on samples comparison in Echo Hiding discrete wavelet transform and least significant bit (LSB) coding technique of a segment are compared with pre-determined threshold value T and based on comparison bits are embedded. The strength of our algorithm is depend on the segment size and their strength are enabled the algorithm to achieve very high embedding capacity for different data type that can reach up to 25% from the input audio file size with lest of 35 dB SNR for the output stego signal.

Our Proposed Algorithm is able to detect any type of attack if applied in steganographyAudio File. And improves the speed of detection, and also test the robustness of the Audio Files.

## IV. CONCLUSION

We have proposed in this Research paper a combination of Echo Hiding discrete wavelet transform and least significant bit (LSB) coding technique is also a steganography embedded technique on different regions of the host Audio Fileapproach. To improve the reliability of the LSB, DWT and Echo Hiding based steganography detection in WhatsApp, this paper introduces the new solution based Audio Filesteganography detection method that is used to recover the geometrically distorted Audio File before detecting the steganography. It can be implemented by the blind based LSB, DWT and Echo Hiding based steganography scheme. Our a combination of Echo Hiding discrete wavelet transform and least significant bit (LSB) coding technique is also a steganography embedded technique on different regions of the host Audio Filesteganography technique is realized by using two steganographyAudio Files, each with a strong High Frequency or Low Frequency components. Non overlapping regions of these steganographyAudio Files are inserted into the host Audio File using a combination of Audio File segmentation.The experimental results will performed and analyze of different Audio Files file is implemented in Matlab tool.

## REFERENCE

[1] Mazdak, Z., A.M. Azizah, B.A. Rabiah, M.Z. Akram and A., Shahidan" A Secure audio steganography approach", World Acad. Sci. Eng., Technol., 52: 360-363, 2009.

[2] Deborah Radcliff "Computer World" URL: http://www.computerworld.com/securitytopics/security/story/0,10801,71726,00.html

[3] G. Voyatzis, N. Nikolaidis and I. Pitas, "Digital steganography: An overview", EUSIPCO, vol. 1, pp. 9-12, 1998.

[4] Petitcolas, F.A.P., Anderson, R.J., Kuhn, M.G., Information Hiding—A survey, Proceeding of the IEEE, Special Issue on Protection of Multimedia Content, 1062-1078, July 1999.

[5] A. Nikolaidis and I. Pitas, "Region-based Audio File steganography," Audio File Processing, IEEE Transactions on, vol. 10, no. 11, pp. 1726-1740, 2001.

[6] H. X. Wang Overview of content based adaptive audio steganography. Journal of Southwest Jiao tong University. 44(3), 2009, 430-437 (in Chinese).

[7] Archana O. Vyas , Dr. Sanjay V. Dudul , " Study of Image Steganalysis Techniques", International Journal of Advanced Research in Computer Science, Volume 6, No. 8, Nov-Dec 2015 ISSN No. 0976-5697.

[8] Satishkumar Chavan, Rohan Shah, Roshan Poojary, Jaisel Jose and Gloria George,"A Novel Robust Color Steganography Scheme for Color steganography Audio Files in Frequency Domain", International Conference on Advances in Recent Technologies in Communication and Computing IEEE 2010.

[9] Mehdi Ghorbani, Mohammad Firouzmand, Ahmad Faraahi, "DWT-DCT (QCD) Based Copy-move Image Forgery Detection", IEEE 2011.

[10] Sherif M. Badr, Gouda I. Salama, Gamal M. I. Selim, Ashgan H. Khalil, "A Review on Steganalysis Techniques: From Image Format Point of View", International Journal of Computer Applications (0975 – 8887) Volume 102– No.4, September 2014.

Nishtha Pateriya . "A Novel Technology For Identification Of Terrorist Information Transmitted Through In Social Media (WhatsApp)." IOSR Journal of Engineering (IOSRJEN), vol. 7, no. 10, 2017, pp. 12–16.