International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Volume 1 Issue 10 (November 2014) www.ijirae.com

Robust Audio Steganography Technique using AES algorithm and MD5 hash.

Kamal Pradhan
Dept. of Computer Science, SUIIT

Chinmaya Bhoi
Dept. of ECE, SUIIT

Abstract—***Data transmission in public communication system is prone to the interception and improper manipulation by eavesdropper. Audio Steganography is the procedure of hiding the existence of secret information by zipping it into another medium such as audio file. This paper explores the innovative audio Steganography technique in a practical way in order to conceal the preferred information. The proposed system uses LSB (least significant bit) technique for embedding text into an audio file. The text is encrypted using AES (Advanced encryption standard) encryption function and md5 hash function which is used for verifying data integrity of the audio file. The performance of this system is evaluated through a more secure process based on robustness, security and data hiding capacity.***

Keywords— ***Advanced encryption system, steganography, modulation, Human Auditory System***

I. INTRODUCTION

Advanced ICT and communication technology helps a large amount of the information for electronic storage and transmission. The growing awareness of Internet use among the mass and the abundant availability of public and private digital data have driven industry professionals and researchers to focus upon the data protection. Data hiding techniques have been developed for a strong basis for Steganography area with an addition of applications like digital rights management, secret communications etc. Steganography is the scientifically acknowledged art of invisible communication [4]. It is accomplished through hiding information within the media files that is also hiding the presence of the communicated information [12]. The word Steganography comes from the Greek words “stegos” meaning “cover”, and “grafia” meaning “writing” defining it as “covered writing” [1].Basically, audio steganography is a type of digital steganography which merges digital data into digital audio files such as WAV, MP3, and WMA files [19] [9] [14]. Audio steganography takes advantage of the Human Auditory System (HAS) which cannot hear the slight variation of audio frequencies at the high frequency side of the audible spectrum [3] [16], and thus, audio steganography can exploit and use this type of frequencies to hide secret data without damaging the quality of the audio file or changing its size [8].

This paper focuses on a novel randomized steganography algorithm for hiding digital data into uncompressed audio files [6]. The digital message is converted into cipher text through the process of encryption algorithm. Here we use AES (Advanced Encryption Standard) algorithm for the encryption process. The encrypted data is then stored in the carrier audio file inside the LSBs of the randomly selected audio samples [7] [5] [2] [10]. A hash is generated using md5 hash function which is sent to the receiver for verifying the data integrity of the audio file. As the proposed algorithm is randomized its main advantage being irrecoverable in a sense that it is difficult for any third party apart from the original communicating parties to detect the presence of the secret data into the carrier audio file. The recovery of the sent data is completely in the hands of the proprietor.

II. SYSTEM ARCHITECTURE

Modern steganography refers to hiding information in digital picture files and audio files [20]. It works by replacing bits of unused data in regular digital files with bits of invisible information. To embed hidden information into audio requires two files - the cover audio file that will hold the hidden data and the secret message file [17]. A message may be plain text, cipher text (or another audio). When combined, the cover audio and the hidden message make a stego audio [15]. A stego-key or password may be used to hide and decode the message. Special software is needed for steganography. This paper looks at two programs that will hide text within the audio files.

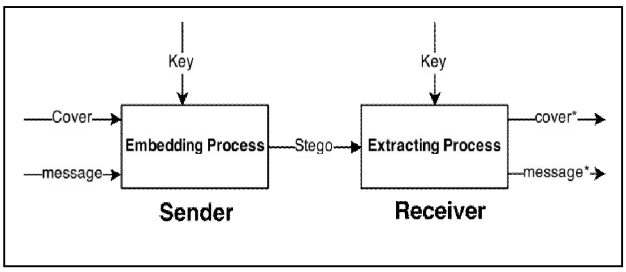


Fig. 1. Basic Steganography Technique

The proposed system architecture for audio steganography is given in fig 4 (a) and 4 (b). The system uses WAV file as cover medium and message in text format and a secret key for embedding process. During extraction process the secret key is used to extract message from stego WAV file [18]. During the embedding and extraction process the message and cover audio goes through AES encryption algorithm and MD5 hash function. The system components of the proposed system are mentioned in the sections:

II. (A) WAVEFORM AUDIO FILE FORMAT (WAV) FILE FORMAT

Waveform Audio File Format (WAV) file format was jointly developed by IBM and Microsoft for storing sound in files. It is a subset of Microsoft's Resource Interchange File Format (RIFF) bit stream format for storing data in chunks and sub chunks. Each chunk has a type, represented by a four-character tag. This chunk type comes first in the file, followed by the size of the chunk, then the contents of the chunk. A WAV file can contain both compressed and uncompressed audio but the most common WAV audio format is uncompressed audio in the linear pulse code modulation (LPCM) format. The table below shows the canonical wave file format [16].

Endianness	*File offset*	*Field Name*	*Field Size*	*Description*
Big	*0*	*ChunkID*	*4*	*Contains the letters "RIFF" in ASCII form.*
Little	*4*	*ChunkSize*	*4*	*This is the size of the entire file in bytes.*
Big	*8*	*Format*	*4*	*Contains the letters "WAVE".*
Big	*12*	*Subchunk1ID*	*4*	*Contains the letters "fmt".*
Little	*16*	*Subchunk1Size*	*4*	*This is the size of the rest of the Subchunk.*
Little	*20*	*AudioFormat*	*2*	*PCM = 1 (i.e. Linear quantization).*
Little	*22*	*NumChannels*	*2*	*Mono = 1, Stereo = 2, etc.*
Little	*24*	*SampleRate*	*4*	*8000, 44100, etc.*
Little	*28*	*ByteRate*	*4*	*SampleRate * NumChannels * BitsPerSample/8.*
Little	*32*	*BlockAlign*	*2*	*NumChannels * BitsPerSample/8*
Little	*34*	*BitsPerSample*	*2*	*8 bits = 8, 16 bits = 16, etc.*
Big	*36*	*Subchunk2ID*	*4*	*Contains the letters "data".*
Little	*40*	*Subchunk2Size*	*4*	*This is the number of bytes in the data.*
Little	*44*	*Data**	*Subchunk2size*	*The actual sound data.*

Table 1. WAV File Format

III. (B) ADVANCED ENCRYPTION STANDARD (AES),

Advanced Encryption Standard (AES), is based on the Rijndael cipher, a symmetric 128-bit block data encryption technique that has been developed by Belgian cryptographers Joan Daemen and Vincent Rijmen [23]. The Advanced Encryption Standard (AES), the symmetric block cipher ratified as a standard by National Institute of Standards and Technology of the United States (NIST). This has been chosen using a process lasting from 1997 to 2000 that was markedly more open and transparent than its predecessor, the aging Data Encryption Standard (DES) [23]. AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware. AES allows for three different key lengths: 128, 192, or 256 bits. Encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. All these rounds are identical for the keys except the last round.

International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Volume 1 Issue 10 (November 2014) www.ijirae.com

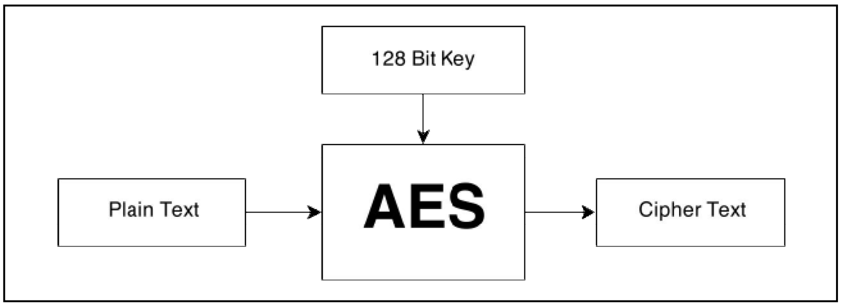


Fig. 2. AES Encryption Technique

II. (C) MD5 MESSAGE-DIGEST ALGORITHM

In 1999 Ron Rivest designed the MD5 message-digest algorithm to replace an earlier hash function, MD4. The MD5 algorithm is a widely used cryptographic hash function producing a 128-bit hash value, typically expressed in a text format as a 32 digit hexadecimal number. MD5 has been in a wide variety of cryptographic applications, and is also commonly used to verify data integrity [21]. The idea behind this algorithm is to take up a random data (text or binary) as an input and generate a fixed size "hash value" as the output. The input data can be of any size or length, but the output "hash value" size is always fixed. Here is an example of MD5 Hash function at work:

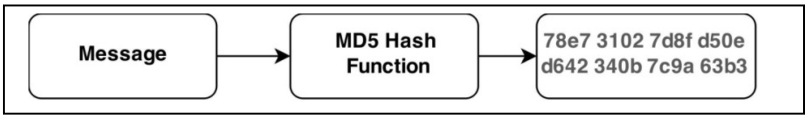


Fig. 3. MD5 Hash Function Block Diagram

II. (D) THE EMBEDDING AND DECODING ALGORITHM

Embedding Algorithm

- *The proposed system uses least significant method to embed data inside the cover audio. Initially the message, secret key and cover audio are taken as input at the sender's side.*
- *The message is encrypted using AES algorithm using 128 bit key.*
- *The encrypted message is embedded inside the cover audio using LSB technique.*
- *After embedding the hash code of the samples of cover audio is produced using MD5 hash algorithm.*
- *The hash code is embedded inside the cover audio and the stego audio is produced.*
- *The stego audio file is sent to receiver.*

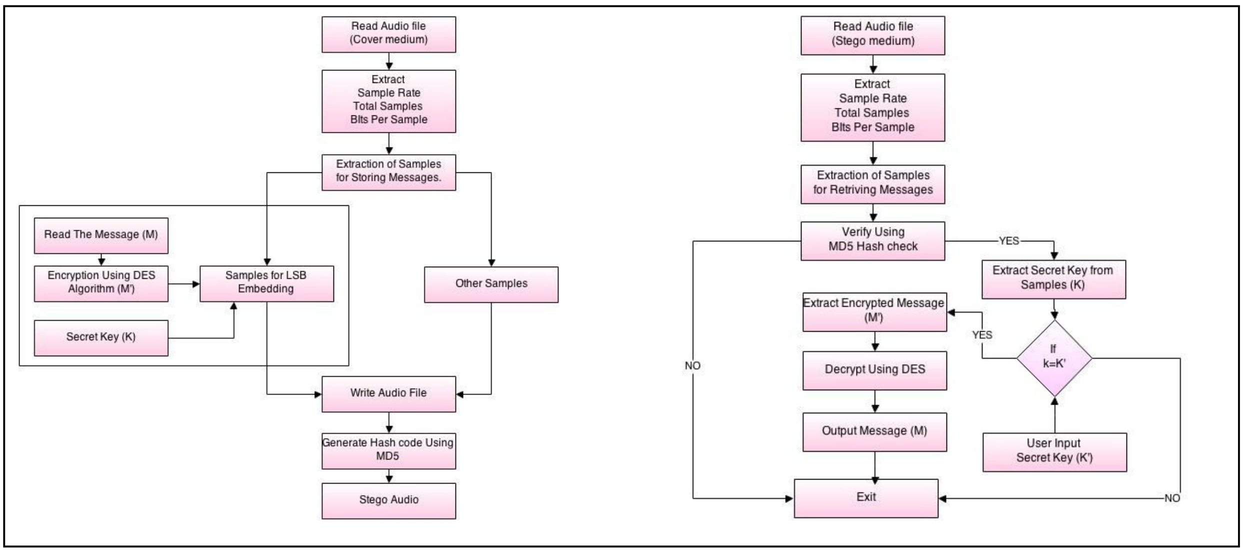


Fig. 4(a) Flowchart of embedding algorithm *Fig. 4(b) Flowchart of decoding algorithm*

Decoding Algorithm

- *The receiver then extracts the samples and hash code embedded inside the stego audio.*
- *The hash code of stego samples is generated and compared with the extracted hash code.*
- *The integrity of the audio samples is verified, if both the codes match. Otherwise the data is corrupted or intercepted.*
- *Finally the encrypted message is extracted from the audio samples using the stego key.*
- *The encrypted message is then converted to plain text using AES algorithm.*

III. PERFORMANCE EVALUATION
IV.

The efficiency of all Steganography algorithms has to comply with some basic requirements. The requirements are Invisibility, Payload capacity, Robustness against statistical attacks and independent of file format. In this algorithm we have used wav audio file format [11]. The Peak Signal Noise Ratio (PSNR), Payload capacity of wav audio format is calculated and compared using different message [13]. Finally the histograms of cover audio and stego audio are compared. We have carried out the experiment and implemented the above algorithm using MATLAB R2012b with two different in wav audio files (a) Test1.wav and Test2.wav.

We then test the algorithm using the PSNR (Peak signal-to-noise ratio). PSNR is a standard measurement used in Steganography technique in order to test the quality of the stego audios. The higher the value of PSNR, the higher quality the stego audio will have. The PSNR can be calculated as follows:

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

The PSNR is defined as:

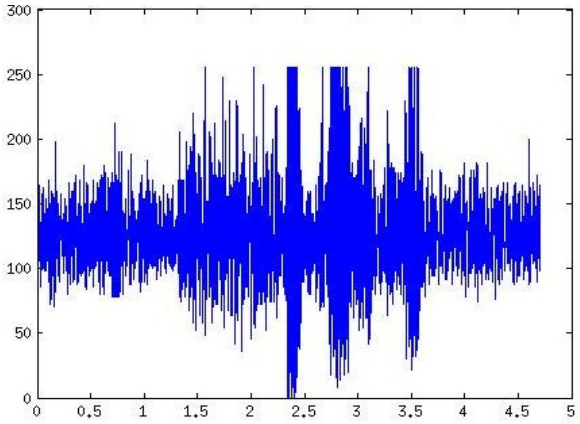
$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) = 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$

I represent the sample value of cover audio and k represents the sample value of stego audio. In equation 2 MAX represents the maximum possible sample value of the audio; if the audio samples are represented using 8 bits per sample then the MAX value is 255. We compare the stego audio with cover audio to calculate the PSNR value.

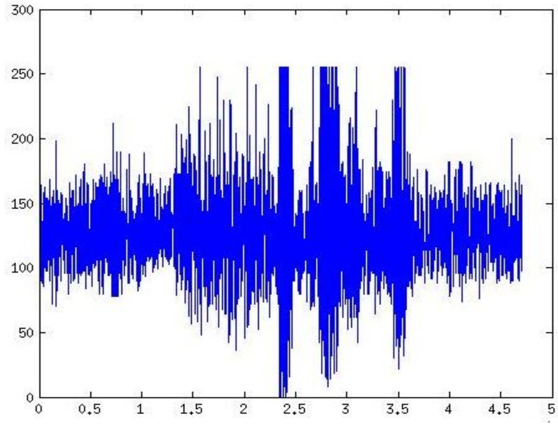
FILENAME	COMPRESSION METHOD	SAMPLERATE	TOTAL SAMPLES	DURATION	BITS PER SAMPLE	MESSAGE SIZE (KB)	PSNR (db)
Test1.wav	Uncompressed	22050	47048	2.1337	8	40	56.44
Test2.wav	Uncompressed	22050	68956	3.1273	8	200	49.39

Table 2.WAV File Details

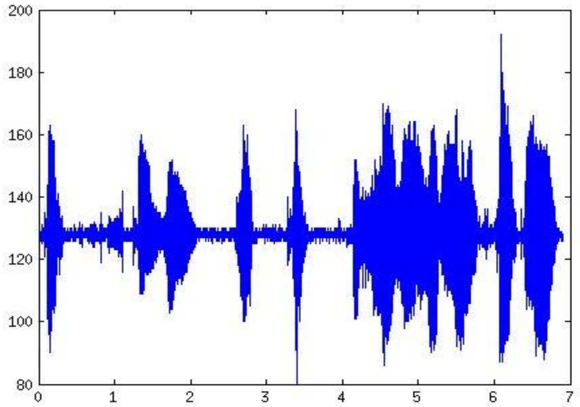
Fig 2 and 3 show the histogram plots of the cover and stego audio for the two wav files. One more important thing to note from the histograms is that, our algorithm preserves the general shapes of the histograms. This feature of our algorithm makes it difficult to detect whether any data is hidden or not in the transmitted Audio.



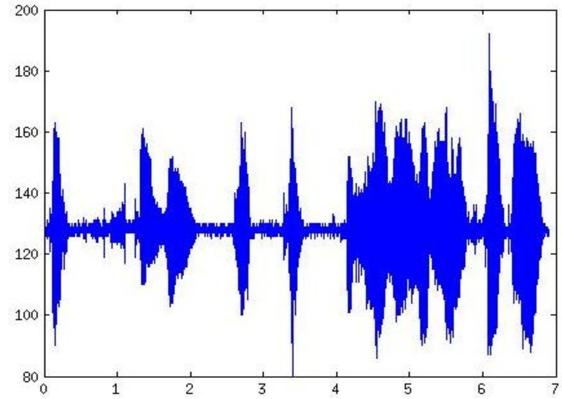
Test1 .wav



Test1.wav



Test 2.wav



Test2.wav

Fig. 5(a) Histogram of cover audio file.

Fig. 5(b) Histogram of Stego audio file.

V. CONCLUSION

The proposed framework for hide messages with incurring minimal auditory degradation. The embedded message can be recovered successfully without any errors. The proposed method can be employed for applications that require high-volume volume robustness against certain non-malicious attacks. In order robustly hide large volumes of data in audio without causing significant perceptual degradation, hiding techniques must adapt to local characteristics within a audio.

VI. REFERENCES

[1] S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood,MA, 2000.

[2] Prof. Samir Kumar, Bandyopadhyay Barnali and Gupta Banik, " LSB Modification and Phase Encoding Technique of Audio Steganography Revisited",International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 4, June 2012(IJRCCE) ISSN : 2278 – 1021.

[3] Masoud Nosrati, Ronak Karimi and Mehdi Hariri,"Audio Steganography: A Survey on Recent Approaches", World Applied Programming, Vol (2), No (3), March 2012. 202-205 ISSN: 2222-2510©2011 WAP journal.www.waprogramming.com.

[4] A. A. Zaidan, B. B. Zaidan, O. Hamdan Alanazi, Abdullah Gani, Omar Zakaria and Gazi Mahabubul Alam, " Novel approach for high (secure and rate) data hidden within triplex space for executable file", Scientific Research and Essays Vol. 5(15), pp. 1965-1977, 4 August, 2010 ISSN 1992-2248 ©2010 Academic Journals

[5] Nedeljko Cvejic and Tapio SeppÄanen, "Increasing Robustness of LSB Audio Steganography by Reduced Distortion LSB Coding".

[6] Youssef Bassil, "A TWO INTERMEDIATES AUDIO STEGANOGRAPHY TECHNIQUE", Journal of Emerging Trends in Computing and Information Sciences (CIS), ISSN: 2079-8407, Vol. 3, No.11, November 2012 http://www.cisjournal.org/journalofcomputing/archive/vol3no11/vol3no11_3.pdf.

[7] Ankit Chadha, Neha Satam, Rakshak Sood and Dattatray Bade, "An Efficient Method for Image and Audio Steganography using Least Significant Bit (LSB) Substitution",International Journal of Computer Applications (0975 – 8887) Volume 77– No.13, September 2013.

[8] Fatiha Djebbar, Beghdad Ayad, Karim Abed Meraim and Habib Hamam,"Comparative study of digital audio steganography techniques", Djebbar et al. EURASIP Journal on Audio, Speech, andMusic Processing 2012, 2012:25 http://asmp.eurasipjournals.com/content/2012/1/25.

[9] Jayaram P, Ranganatha H R and Anupama H S,"INFORMATION HIDING USING AUDIO STEGANOGRAPHY – A SURVEY", The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011.

[10] Jassim Mohmmed Ahmed and Zulkarnain Md Ali,"Information Hiding using LSB technique", IJCSNS International 18 Journal of Computer Science and Network Security, VOL.11 No.4, April 2011.

[11] Andreas Westfeld, "F5—A Steganographic Algorithm High Capacity Despite Better Steganalysis".

[12] Chuo-Ling Chang and Bernd Girod ,"Direction-Adaptive Discrete Wavelet Transform for Image Compression", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 16, NO. 5, MAY 2007.

[13] kamal Pradhan , gourav gohil , "Securing web communication using three layer image shielding" ICDCIT 2014(International Conferance on Distributed Computing an Internet Technology).

[14] S.S. Divya, M. Ram Mohan Reddy," HIDING TEXT IN AUDIO USING MULTIPLE LSB STEGANOGRAPHY AND PROVIDE SECURITY USING CRYPTOGRAPHY", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 1, ISSUE 6, JULY 2012 ISSN 2277-8616.

[15] Gunjan Nehru and Puja Dhar, "A Detailed look of Audio Steganography Techniques using LSB and Genetic Algorithm Approach", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012 ISSN (Online): 1694-0814 www.IJCSI.org.

[16] Lovey Rana, Saikat Banerjee, "Dual Layer Randomization in Audio Steganography Using Random Byte Position Encoding", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 8, February 2013 ISSN: 2277-3754 ISO 9001:2008 Certified

[17] M.Baritha Beguma and Y.Venkataramani, "LSB Based Audio Steganography Based On Text Compression", International Conference on Communication Technology and System Design 2011.

[18] Linu Babu , Jais John S , Parameshachari B D,Muruganantham C and H S DivakaraMurthy ,"Steganographic Method for Data Hiding in Audio Signals with LSB & DCT ", IJCSMC, Vol. 2, Issue. 8, August 2013, pg.54 – 62 .

[19] Anamika Sharma and Pushpinder Singh, "Semantic Analyzer for Audio Steganography" , International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 1, January 2014 (IJARCCE).

[20] Md. Rafiqul Islam, A.W. Naji, A.A.Zaidan and B.B.Zaidan, "New System for Secure Cover File of Hidden Data in the Image Page within Executable File Using Statistical Steganography Techniques" , (IJCSIS) International Journal of Computer Science and Information Security, Vol.7 No.1, 2009.

[21] Mark ciampa, "CompTIA Security+ 2008 in Depth" Cengage Learning, 2009, ISBN 1598639137, 9781598639131

[22] Joan Daemen and Vincent Rijmen, The Design of Rijndael, AES - The Advanced Encryption Standard, Springer-Verlag 2002 (238 pp.)

[23] FIPS PUB 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, U.S. Department of Commerce, November 2001.

