ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 11, September 2015

National Conference on Emerging Trends in Computing, Communication & Control Engineering [NCET 2K15]

On 4th September, 2015

Organized by

Department of CSE, ECE & EEE, Magna College of Engineering, Chennai-600055, India.

Audio Steganography Using AES Algorithm

Mahalakshmi.S[1], Selvarani. R[2], Thilagam .J[3], N.Tharminie[4]

UG Student, Department of Computer Science and Engineering, Magna College of Engineering, Chennai, India[1,2,3]

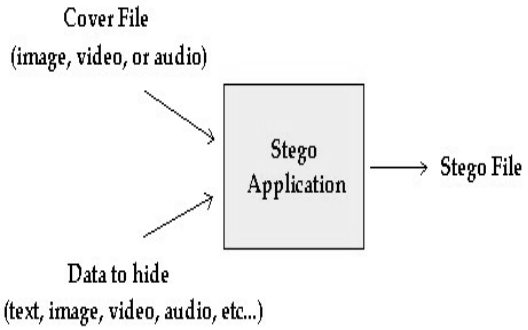
Associate Professor, Department of Computer Science and Engineering, Magna College of Engineering, Chennai, India[4]

ABSTRACT: In this paper, Steganography is performed on audio files using Advanced Encryption Standard(AES) to overcome the disadvantages in Data Encryption Standard(DES). . When performing data hiding on audio, first the data is encrypted by password based encryption using AES algorithm to generate the cipher text. Now the cipher text is kept hidden in the audio file using low bit encoding method. When extracting the data from audio first cipher text is separated from audio then the plain text is generated by decrypting the cipher text.

I. INTRODUCTION

Steganography has been used on a message, the viewer would not be able to tell that the message contains a hidden message within it. The data to be concealed is compressed and hidden within another file. The hidden message may be placed inside the white space of text messages or the dark areas of a photographic image, or within the unused portions of a audio file format. The first item needed for Steganography is called a carrier or a container. This can be a text file, graphic file or sound file which will host the message that is desired to be hidden.

II. STEGO APPLICATION



The steganography application hides different types of data within a cover file. 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.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 11, September 2015

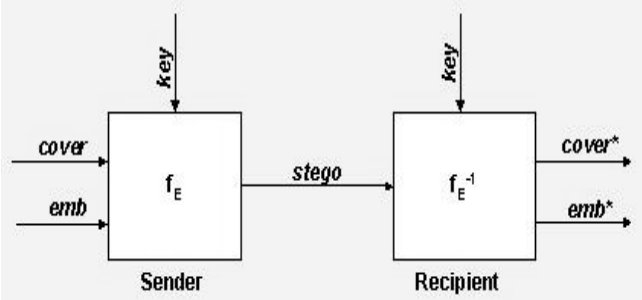
National Conference on Emerging Trends in Computing, Communication & Control Engineering [NCET 2K15]

On 4th September, 2015

Organized by

Department of CSE, ECE & EEE, Magna College of Engineering, Chennai-600055, India.

III. A GENERIC STEGANOGRAPHY SYSTEM



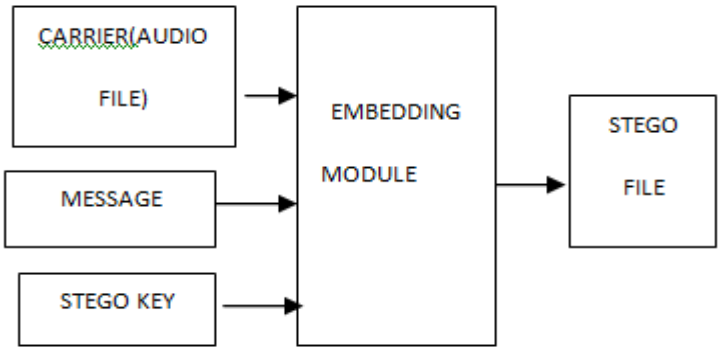
- **Emb**: The message to be embedded.
- **Cover**: The data in which emb will be embedded.
- **Stego**: A modified version of cover that contains the embedded message emb.
- **Key**: Additional secret data that is needed for the embedding and extracting processes and must be known to both, the sender and the recipient.
- **fE**: A steganographic function that has cover, emb and key as parameters and produces stego as output.
- **FE-1:** A steganographic function that has stego and key as parameters and produces emb as output. FE-1 is the inverse function of fE in the sense that the result of the extracting process fE-1 is identical to the input E of the embedding process fE.

The embedding process fE embeds the secret message E in the cover data C. The exact position (S) where E will be embedded is dependence on the key K. The result of the embedding function is slightly modified version of C: the stego data C'. After the recipient has received C' he starts the extracting process fE-1 with the stego data C' and the key K as parameters. If the key that is supplied by the recipient is the same as the key used by the sender to embed the secret message and if the stego data the recipient uses as input is the same data the sender has produces (i.e., it has not been modified by an adversary), then the extracting function will produce the original secret message E.

IV. AUDIO STEGANOGRAPHY

Audio Steganography is secured which is designed to send data is a effective method using this technique. In this application we will embed one audio file in to another audio file using a secured manner. This method makes user to send data securely which is called steganography and cryptography.

BASIC AUDIO STEGANOGRAPHIC MODEL



- The basic model of Audio steganography consists of Carrier (Audio file), Message and Password.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 11, September 2015

National Conference on Emerging Trends in Computing, Communication & Control Engineering [NCET 2K15]

On 4th September, 2015

Organized by

Department of CSE, ECE & EEE, Magna College of Engineering, Chennai-600055, India.

- Carrier is also known as a cover-file, which conceals the secret information.
- 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.

The information hiding process consists of following two steps

i. Identification of redundant bits in a cover-file. Redundant bits are those bits that can be modified without corrupting the quality or destroying the integrity of the cover-file.

ii. To embed the secret information in the cover file, the redundant bits in the cover file is replaced by the bits of the secret information .

V. AUDIO STEGANOGRAPHIC METHODS

- There have been many techniques for hiding information or messages in audio in such a manner that the alterations made to the audio file are perceptually indiscemible.
- LSB CODING
- PHASE CODING
- SPREAD SPECTRUM
- ECHO HIDING

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.
- 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.

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, you can set the

LSB of each byte like this:

- 1001001**0**
- 0101001**1**
- 1001101**1**
- 1101001**0**
- 1000101**0**
- 0000000**1**
- 0111001**0**
- 0010101**1**

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.

PHASE CODING

- The phase coding technique works by replacing the phase of an initial audio segment with a reference phase that represents the secret information.
- Phase coding is explained in the following procedure:

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 11, September 2015

National Conference on Emerging Trends in Computing, Communication & Control Engineering [NCET 2K15]

On 4th September, 2015

Organized by

Department of CSE, ECE & EEE, Magna College of Engineering, Chennai-600055, India.

a. Divide an original sound signal into smaller segments such that lengths are of the same size as the size of the message to be encoded.

b. Matrix of the phases is created by applying Discrete Fourier Transform (DFT).

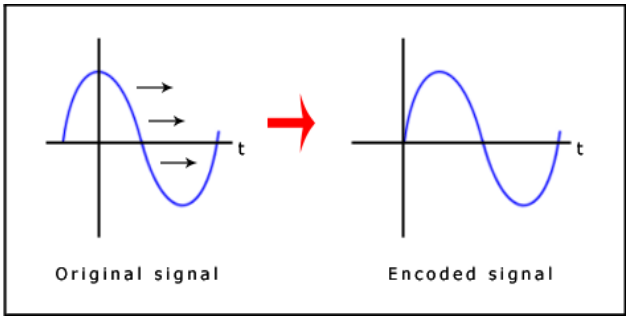
c. Calculate the Phase differences between adjacent segments.

d. Phase shifts between adjacent segments are easily detectable. It means, we can change the absolute phases of the segments but the relative phase differences between adjacent segments must be preserved. So the secret information is inserted only in the phase vector of the first signal segment as follows:

$$\text{phase\_new} = \begin{cases} \prod/2 \text{ if message bit } = 0 \\ -\prod/2 \text{ if message bit } = 1 \end{cases}$$

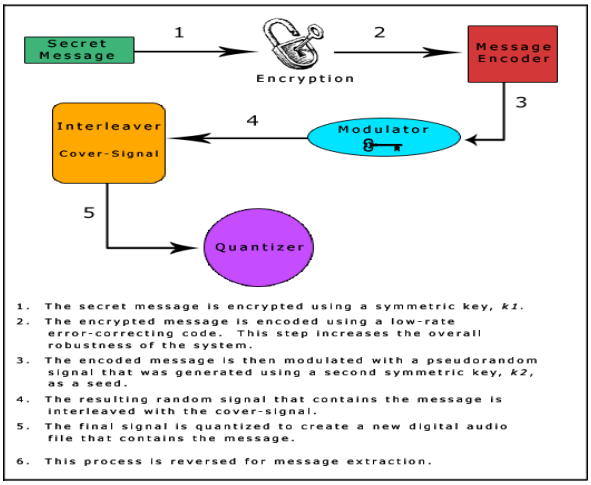
e. Using the new phase of the first segment a new phase matrix is created and the original phase differences.

f. The sound signal is reconstructed by applying the inverse Discrete Fourier Transform using the new phase matrix and original magnitude matrix and then concatenating the sound segments back together.



SPREAD SPECTRUM

- In audio steganography, the basic spread spectrum (SS) method attempts to spread secret information across the frequency spectrum of the audio signal.
- The Spread Spectrum method is capable of contributing a better performance in some areas compared to phase coding techniquein that it offers a moderate data transmission rate and high level of robustness against removal techniques.



ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 11, September 2015

National Conference on Emerging Trends in Computing, Communication & Control Engineering [NCET 2K15]

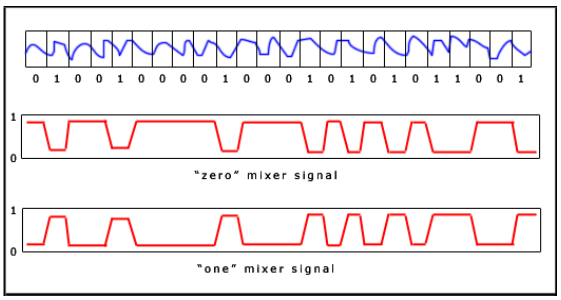
On 4th September, 2015

Organized by

Department of CSE, ECE & EEE, Magna College of Engineering, Chennai-600055, India.

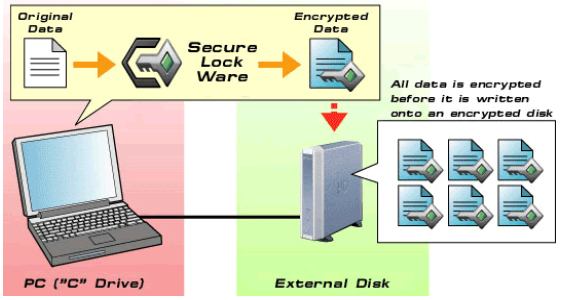
ECHO HIDING

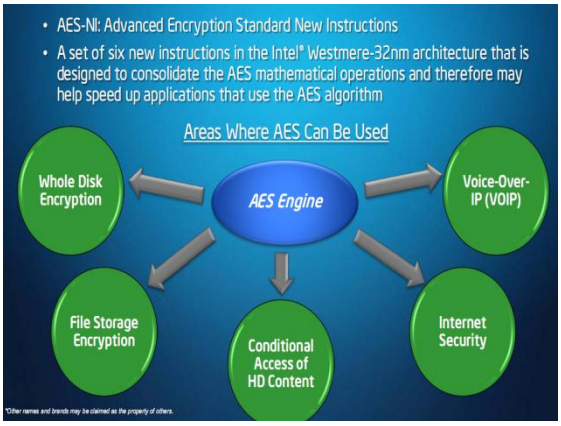
- Echo hiding technique embeds secret information in a sound file by introducing an echo into the discrete signal.
- Echo hiding has advantages of providing a high data transmission rate and superior robustness when compared to other methods.
- Only one bit of secret information could be encoded if only one echo was produced from the original signal.
- Hence, before the encoding process begins the original signal is broken down into blocks.
- Once the encoding process is done, the blocks are concatenated back together to create the final signal.



VI. PROPOSED WORK

AES is a new cryptographic algorithm that can be used to protect electronic data. Specifically, AES is an iterative, symmetric-key block cipher that can use keys of 128, 192, and 256 bits, and encrypts and decrypts data in blocks of 128 bits(16 bytes). Unlike public-key ciphers, which use a pair of keys, symmetric key ciphers use the same key to encrypt and decrypt data. Encrypted data returned by block ciphers have the same number of bits that the input data had. Iterative ciphers use a loop structure that repeatedly performs permutations and substitutions of input data.





ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 11, September 2015

National Conference on Emerging Trends in Computing, Communication & Control Engineering [NCET 2K15]

On 4th September, 2015

Organized by

Department of CSE, ECE & EEE, Magna College of Engineering, Chennai-600055, India.

VII. AUDIO STEGANOGRAPHIC APPLICATIONS

- Audio data hiding can be used anytime you want to hide data.
- There are many reasons to hide data but most important is to prevent unauthorized persons from becoming aware of the existence of a message.
- In the business world Audio data hiding can be used to hide a secret chemical formula or plans for a new invention.
- Audio data hiding can also be used in the non commercial sector to hide information that someone wants to keep private.
- It can also be used in forensic applications for inserting hidden data into audio files for the authentication of spoken words and other sounds, and in the music business for the monitoring of the songs over broadcast radio.

VIII. CONCLUSION

The new AES will certainly become the de facto standard for encrypting all forms of electronic information, replacing DES.

AES-encrypted data is unbreakable in the sense that no known cryptanalysis attack can decrypt the AES cipher text without using a brute-force search through all possible 256-bit keys.

Security is no longer an afterthought in anyone's software design and development process. AES is an important advance and using and understanding, it will greatly increase the reliability and safety of your software systems.

ADVANTAGES OF AES

- AES is more secure.
- AES supports larger key sizes.
- AES is faster in both hardware and software.
- AES's 128-bit block size makes it less open to 3DES with its 64-bit block size.
- AES is required by the latest U.S. and international standards.

REFERENCES

[1] W. Bender, W. Butera, D. Gruhl, R. Hwang, F. J. Paiz, S. Pogreb, “Techniques for data hiding”, IBM Systems Journal, Volume 39 , Issue 3-4, July 2000, pp. 547 – 568.

[2] Samir Kumar Bandyopadhyay, Debnath Bhattacharyya, Poulami Das, Debashis Ganguly and Swarnendu Mukherjee, “A tutorial review on Steganography”, International Conference on Contemporary Computing (IC3-2008), Noida, India, August 7-9, 2008, pp. 105-114.

[3] Robert Krenn, “Steganography and steganalysis”, An Article, January 2004.

[4] Nedeljko Cvejic, Tapio Seppben “Increasing the capacity of LSB-based audio steganography ” FIN- 90014 University of Oulu, Finland ,2002.

[5] Sajad Shirali-Shahreza M.T. Manzuri-Shalmani “High capacity error free wavelet domain speech steganography" ICASSP 2008.

[6] Neil F.Johnson, Z.Duric and S.Jajodia. “Information Hiding Steganography and Watermarking-Attacks and Countermeasures”,Kluwer Academic Publishers, 2001

[7] AES page available via http://www.nist.gov/CryptoToolkit. 4

[8] Computer Security Objects Register (CSOR): http://csrc.nist.gov/csor/.

[9] J. Daemen and V. Rijmen, AES Proposal: Rijndael, AES Algorithm Submission, September 3, 1999.

[10] J. Daemen and V. Rijmen, The block cipher Rijndael, Smart Card research and Applications, LNCS 1820, Springer-Verlag, pp. 288-296.