ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Review on: Enhancing the Security of Multilevel Audio Steganography Using AES

[I]Nitasha, [II]Nidhi Sood
[I,II]Dept. of Computer Science, Bahra University, Waknaghat, distt Solan, India

Abstract

Steganography is an art and a science of communicating in a way; which hides the existence of the communication. It is also called as "covered writing", because it uses a "cover" of a message for sending any important secret message. Audio steganography is the art and science of hiding digital data such as text messages, documents and binary files into audio files such as WAV, MP3, and RM files. Here, defined the multilevel audio steganography where four different steganographic methods have been used instead of using one steganographic method. Multi-Level Steganography has advantage of difficult decoding and sending two or more secret message through a single cover object. This paper defines a method for audio steganography using LSB coding, parity coding, and phase coding and Spread Spectrum technique in multi-level steganography. The techniques: LSB, Parity coding, Phase coding and Spread Spectrum are being used and to make this more secured, here AES is used to enhance the security, so that data will become more securable, this is related to networks for providing high security. It performing hidden communication and extend its use on network steganography. In this paper the first level where LSB technique is being used and in second level parity coding and third level Phase Coding and in forth level spread spectrum [1, 8]. This method has provided an effective way to achieve higher security, increased undetectability and the maintained consistency in the clarity of digital audio signal.

Keywords

Audio Steganography, Information security, Data hiding, multilevel steganography, Stego object, Decoy object, AES.

I. Introduction

Steganography is the art and science of writing hidden information in such a way that no one; apart from the sender and intended recipient; suspects the existence of the message; a form of security through obscurity. And Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics; sound; text; HTML; or even floppy disks) with bits of different, invisible information. Therefore this hidden information can be plain text; cipher text; or even images.

Steganography is an art and a science of communicating in a way; which hides the existence of the communication. It is also called as "covered writing", because it uses a "cover" of a message for sending any important secret message. And Steganography serves as a means for private; secure and sometimes malicious communication. Steganography is a powerful tool which increases security in data transferring and archiving. Steganography is the practice of hiding information "in plain sight". Therefore this technique relies on a message being encoded and hidden in a transport layer in such a way as to make the existence of the message unknown to an observer. Importantly, the transport layer - the carrier file - is not secret and can therefore be viewed by observers from whom the secret message itself should be concealed. Therefore power of steganography is in hiding the secret message by obscurity; hiding its existence in a non-secret file. And in that sense; steganography is different from cryptography; which involves making the content of the secret message unreadable while not preventing non-intended observers from learning about its existence [1,2,3,4]. Because the success of the technique depends entirely on the ability to hide the message such that an observer would not suspect it is there at all; the greatest effort must go into ensuring that the message is invisible unless one knows what to look for. Therefore the way in which this is done will differ for the specific media that are used to hide the information. And in each case; the value of a steganography approach can be measured by how much information can be concealed in a carrier before it becomes detectable; each technique can thus be thought of in terms of its capacity for information hiding.

In the steganography scenario, the secret data is first concealed within another object which is called "cover object", to form "stego object" and then this new object can be transmitted or saved. Using different techniques, we can send secret data in the form of an image, a music file or even a video file by embedding it into the carrier, forming a stego signal. At the receiver's end, the secret data can be recovered from the stego signal using different algorithms. **Multilevel Audio Steganography** is defined as the steganography, where we use two or more than two techniques that are known as multilevel audio steganography [11].

II. Audio Steganography & Methods Of Hiding

Audio steganography is the art and science of hiding digital data such as text messages, documents and binary files into audio files such as WAV, MP3, and RM files. The output audio file is called the carrier file and is the only intermediate to be sent to the receiver. Imperceptibility is the property of steganography and it refers to the fact that no one apart from the original sender and the intended receiver can suspect the presence of secret data into the carrier file being communicated. Steganography can be achieved by means of three types of techniques: injection; substitution; and generation [9].

A. Injection

The injection technique implants the data to hide in the insignificant part of the carrier file, which is normally ignored by operating systems and software applications. Therefore for example; most computer files comprise what so called an end-of-file marker or EOF for short, which indicates that no more data can be read from a data source. Example is the PDF file which ends with an EOF indicating to the reader application that no more pages are to be fetched and that the file has ended. Steganography by injection exploits the EOF section and injects secret data after the EOF marker which eventually has no side effect on the carrier file and is often disregarded by the execution environment.

B. Substitution

The substitution technique substitutes the insignificant bits in the carrier file with the bits of the data to hide. And insignificant bits are those bits that can be modified without damaging the quality or destroying the integrity of the carrier file. This technique takes advantage of the limited capabilities of the Human Auditory System (HAS) which cannot recognize two sounds that are slightly not alike.

C. Generation

The generation technique reads the data to hide and generates out of them a new set of data. It is a dynamic method of creating a carrier file based on the information contained in the data to hide [4].

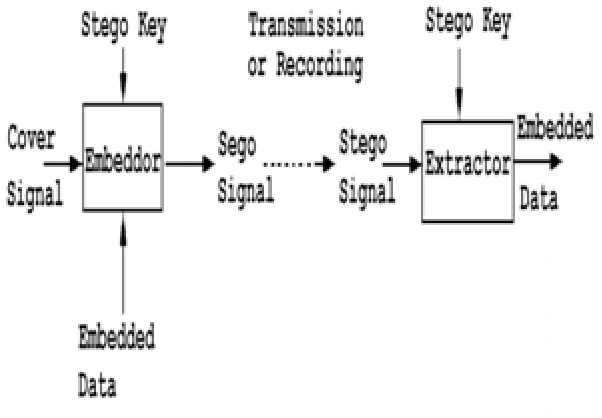

Figure 1: Generation Technique

Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media; such as digital images. And these methods range from rather simple algorithms that insert information in the form of signal noise to more powerful methods that exploit sophisticated signal processing techniques to hide information.

III. Techniques of Audio Steganography

The list of techniques that are commonly used for audio steganography are listed and discussed below:

1. LSB
2. Parity coding
3. Phase coding
4. Spread spectrum
5. Echo hiding

A. LSB

Using the least-significant bit is possible; as modifications will usually not create audible changes to the sounds. It is possible to encode messages using frequencies that are inaudible to the human ear. Any frequencies above 20.000 Hz; messages can be hidden inside sound files and will not be detected by human checks [8].

B. Parity Coding

Instead of breaking a signal down into individual samples; the parity coding method breaks a signal down into separate regions of samples and encodes each bit from the secret message in a sample region's parity bit. And if the parity bit of a selected region does not match the secret bit to be encoded; the process flips the LSB of one of the samples in the region. The sender has more of a choice in encoding the secret bit; and the signal can be changed in a more unobtrusive fashion.

C. Phase Coding

Phase coding addresses the disadvantages of the noise inducing methods of audio steganography. Therefore phase coding relies on the fact that the phase components of sound are not as perceptible to the human ear as noise is. The technique encodes the message bits as phase shifts in the phase spectrum of a digital signal; achieving an inaudible encoding in terms of signal-to-perceived noise ratio.

D. Spread Spectrum

In audio steganography, the basic spread spectrum (SS) method attempts to spread secret information across the audio signal's frequency spectrum as much as possible. And this is analogous to a system using an implementation of the LSB coding that randomly spreads the message bits over the entire sound file. Unlike LSB coding; the SS method spreads the secret message over the sound file's frequency spectrum; using a code that is independent of the actual signal. And as a result; the final signal occupies a bandwidth in excess of what is actually required for transmission.

E. Echo Hiding

In this technique, the secret data are embedded into the audio signals as a short acoustic echo. In fact, an echo is a replication of sound, however, received by the listener sometime after the original sound. As the echo is audible, its amplitude must be decreased so that it becomes imperceptible. Therefore in order to hide data; bits whose values are 0 are represented by an echo delayed 1ms; bits whose values are 1 are represented by an echo delayed 2ms. The limitation of echo hiding technique is the low hiding capacity as it would be computationally intensive to insert echo for every bit to hide [7, 8, 10].

IV. AES

In early 1997 NIST announced that they were looking for a successor to DES and they solicited input from the cryptographic community. Because of the amount of interest this sparked, NIST decided to issue a call for new algorithms in the fall of 1997 and to hold a competition to decide on the best candidate for the standard. Submissions ran well into 1998 and in all 15 algorithms were entered into the competition. After a public debate and two conferences organised by NIST in which the competing algorithms were analysed both for security as well as for performance a shortlist of 5 candidates was selected. Another round of cryptanalysis followed which ended with another conference in April 2000. On October 2nd 2000 NIST announced that the Rijndael algorithm – designed by Belgian cryptographers Joan Daemen and Vincent Rijmen – had won the competition and would become AES. The AES algorithm is a block cipher with a block size of 128 bits (16 bytes). It supports key lengths of 128, 192 and 256 bits. AES has been thoroughly screened by the cryptographic community and no significant attacks have been found to date. NIST currently believes AES to be secure beyond 2030 [19]. Contrary to its predecessor DES – which was specifically designed for sensitive but not for secret information – AES has been approved for use in encrypting official material marked 'SECRET' with 128-, 192- and 256-bit keys and for use in encrypting official material marked 'TOP SECRET' with 192- and 256-bit keys by the United States'

Committee on National Security Systems (CNSS) [5].

Like DES, AES is a symmetric block cipher. Therefore this means that it uses the same key for both encryption and decryption. However, AES is quite different from DES in a number of ways. Therefore algorithm Rijndael allows for a variety of block and key sizes and not just the 64 and 56 bits of DES' block and key size. And block and key can in fact be chosen independently from 128,160,192,224,256 bits and need not be the same. The AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128,192,256 bits. Depending on which version is used; the name of the standard is modified to AES-128; AES-192 or AES- 256 respectively. And as well as these differences AES differs from DES in that it is not a feistel structure. Therefore recall that in a feistel structure; half of the data block is used to modify the other half of the data block and then the halves are swapped. And in this case the entire data block is processed in parallel during each round using substitutions and permutations [5,7].

A number of AES parameters depend on the key length. E.g., if the key size used is 128 then the number of rounds is 10 whereas it is 12 and 14 for 192 and 256 bits respectively. The present the most common key size likely to be used is the 128 bit key. This description of the AES algorithm therefore describes this particular implementation.

Therefore Rijndael was designed to have the following characteristics:

- Resistance against all known attacks.
- And Speed and code compactness on a wide range of platforms.
- Design Simplicity.

V. Advantage of Stegnography

A. Audio based Steganography has the potential conceal more information:

1. Audio files are generally larger than images
2. Our hearing can be easily fooled
3. Slight changes in amplitude can store vast amounts of information

B. The flexibility of audio Steganography is makes it very potentially powerful:

1. The methods discussed provide users with a large amount of choice and makes the technology more accessible to everyone. And a party that wishes to communicate can rank the importance of factors such as data transmission rate; bandwidth; robustness; and noise audibility and then select the method that best fits their specifications.

C. Another aspect of audio Steganography that makes it so attractive is its ability to combine with existing cryptography technologies.

1. Users no longer have to rely on one method alone. Therefore not only can information be encrypted; it can be hidden altogether.

D. Many sources and types make statistical analysis more difficult:

1. Greater amounts of information can be embedded without audible degradation

E. Security:

1. Many attacks that are malicious against image Steganography algorithms (e.g. geometrical distortions, spatial scaling; etc) cannot be implemented against audio Steganography schemes. Embedding information into audio seems more secure due to less steganalysis techniques for attacking to audio.

2. As emphasis placed on the areas of copyright protection; privacy protection; and surveillance increases; Steganography will continue to grow in importance as a protection mechanism.

3. Audio Steganography in particular addresses key issues brought about by the MP3 format; P2P software; and the need for a secure broadcasting scheme that can maintain the secrecy of the transmitted information; even when passing through insecure channels [2, 3, and 11].

VI. Conclusion

This paper proposed an audio steganography technique for hiding text data into digital audio files based on four different techniques to select the carrier audio samples into which bits of the secret data are to be hidden. In this paper four secret messages can be hidden. It is concluded that message is hidden securely and there is no change in size format and description of the message in the files. This proposed system will not change the size of the file even after encoding and also suitable for any type of audio file format. An effective audio steganography 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. At last to increase the data security, here using AES.

VII. Acknowledgment

Thanks to my Guide and family member who always support, help and guide me during my dissertation. Special thanks to my father who always support my innovative ideas.

References

[1] *Ashwini Mane, GajananGalshetwar, AmuthaJeyakumar: "Data Hiding Technique: Audio SteganographyusingLsb Technique", Vol. 2, Issue 3, May-Jun 2012.*

[2] *Youssef Bassil: "A Two Intermediates Audio Steganography Technique", VOL. 3, NO.11 Nov, 2012*

[3] *Frączek, W., Mazurczyk, W., Szczypiorski, K. (2010) Stream Control Transmission Protocol Steganography. In Proc. of Second International Workshop on Network Steganography (IWNS 2010) co-located with The 2010 International Conference on Multimedia Information Networking and Security (MINES 2010), Nanjing, China, and November 4-6, 2010.*

[4] *Frączek, W., Mazurczyk, W., Szczypiorski, K. (2011) Multi-Level Steganography Applied to Networks. In Proc. of: Third International Workshop on Network Steganography (IWNS 2011) co-located with The 2011 International Conference on Telecommunication Systems, Modeling and Analysis (ICTSM2011), Prague, Czech Republic, 27-28 May 2011.*

[5] *Zameer Fatima and Tarun Khanna: "Audio Steganography Using AES Algorithm", Proceedings of the 5th National Conference; INDIACom-2011.*

[6] *MazdakZamani , Azizah A. Manaf , and Rabiah B. Ahmad: "Knots of Substitution Techniques of Audio Steganography", 2009 International Conference on Computer Engineering*

and Applications IPCSIT vol.2 (2011) © (2011) IACSIT Press, Singapore.

[7] Youssef Bassil LACSC – Lebanese Association for Computational Sciences Registered under No. 957, 2011,

[8] Multi-Level Stenographic Algorithm for Audio Steganography using LSB Modification and Parity Encoding Technique by Prof. Samir Kumar Bandyopadhyay1 and Barnali Gupta .Volume 1, Issue 2, July – August 2012

[9] Audio Steganography: A Survey on Recent Approaches World Applied Programming, Vol (2), No (3), March 2012. 202-205 ISSN: 2222-2510 ©2011 WAP journal.

[10] Efficient method of audio steganography byModified lsb algorithm and strong encryption Key with enhanced security1r sridevi, 2dr. A damodaram, 3dr. Svl.narasimhame

[11] A Secure Audio SteganographymApproachhttp ://irep.iium.edu.my/467/ 1/A _SECURE_AUDIO_ STEGANOGRAPHY_approach.pdf [12]Volume 4, Issue 1, January 2014 Multi-Level Steganographic Algorithm for Audio Steganography using LSB, Parity Coding and Phase Coding Technique Kamalpreet Kaur DeepankarVerma Student Assistant Professor M.tech, Department of CSE M.tech, Department of CSE RBIEBT, Kharar(Pb)-India RBIEBT, Kharar(Pb)-India