Security Enhancement in Audio Steganography by Encryption Algorithm

Anil R. Deshpande
PG Student Department of Computer Science, Khurana Sawant Institute of Engineering & Technology, Hingoli, Maharashtra, India.

N.N. Kant
Professor, Department of Electronics and Telecommunication Engineering,
Khurana Sawant Institute Of Engineering & Technology, Hingoli, Maharashtra, India.

Abstract – Steganography is considered as method to protect the digital information. Present work explore steganography for audio signals ensures secure data transfer between the source and destination in terms of audio file of different formats and the application of encryption algorithm is use at the first level of security, which is very complex to break. In the second level it uses algorithm to encode the message into audio signals. It also uses the encryption key for encoding and decoding the hidden data. The idea is to provide a good and efficient method for hiding the data from hackers and send it to the destination in a safer manner through audio signals. Though it is well modulated program, it has been limited to certain restrictions. The quality of sound depends on the size of the audio which the user selects and length of the message.

Index Terms – Steganography, LSB, Cover Data, Stego File, Text Embedding on Audio, RSA

1. INTRODUCTION

Steganography is a Greek ancient art of hiding information. Steganography is the scientific technique of hiding messages [1, 25] in such a way that no one, suspects the existence of the message [12]. Steganography is carried out using [15-19, 24, 26] audio (.wav, mp3 digital format) and other media (Images, video Clips) files are used for hiding the messages. steganography enables the user to transmit information masked inside a file in plain view. The hidden data is both difficult to detect and when combined with known encryption algorithms, equally difficult to decipher. In audio steganography method, secret messages are embedded in digital sound[6]. The secret message is embedded by slightly altering the binary sequence of a sound samples. Known as stago file after the message embedding. Embedding secret messages in digital sound is usually a more difficult process. In steganography, only the sender and the receiver know the existence of the message, whereas in cryptography [14,20, 26] the existence of the encrypted message is visible to the world [5, 23,26]. By combining steganography and cryptography, one can achieve better security [7]. The existing system of audio steganography poses restrictions on the choosing of audio files. User can select only a particular file format to hide the secret data. It complexity arises when more messages are to be encoded. The disadvantages of existing system are:

1.Selection of audio formats is restricted.
2. Lack in good user interface.
3.Consume much time to encode and decode.
4.Non-Provision of sending the file to the destination.
5.User needs to understand better to know the operations.

These are the disadvantages in the existing system which can be tried to be overcome by the propose system.

The propose system which is based on steganography for audio signals ensures secure data transfer between the source and destination in terms of audio file of different formats. Encryption algorithm will be use.

It is a method of hiding the message in the audio file of any formats. It provides an easy way of implementation of mechanisms when compared with audio steganography. Apart from the encoding and decoding in audio steganography, it contains extra layers of encryption and decryption. The four layers are:

- Encoding
- Encryption (Password Protection)
- Decryption
- Decoding

In this, Encryption algorithm is use to encode the message into audio file. Encryption algorithm is use to encrypt the message before encoding for further security purpose. The idea behind this is to provide a good, efficient method for hiding the data from hackers and sent to the destination in safe manner. Though it is well modulated software it has been limited to certain restrictions. The proposed system tries to overcome the restrictions made on the existing systems. It provides good looking environment to user. It also provides the user to give secret key for encryption. The length of message is more than the existing system. It cannot detect the lack in quality of sound. The encryption key can be any

combination of characters, symbols, and numbers. The key which is used for encoding is also used for decoding.

The recent papers [21] considered a RSA (PRime) based encryption technique to be applied together with a GA based audio steganography. It is also well-known that the RSA method is the most useful asymmetric key cryptographic system evolved till date. In this respect, it was found challenging to implement the RSA cryptography to work as a wrapper on an audio stago file Moreover, the present paper is more comprehensive in natures than the earlier reported similar contributions.

Rest of the paper is organized as the next section presents the design methodology of the proposed technique for enhancing the security. The section 1 presents the detailed design the proposed system the section 2 presents the implementation of the developed system. The paper is ended with a section on presenting conclusions and scope of future work.

1. Detailed design

Detailed design of new system based on Encryption Algorithm consist of following steps

- Data Encryption Standard (DES) Algorithm for Encryption
- Modes of Operation
- Algorithm for Hiding Data in File

1.1 Data Encryption Standard (DES) Algorithm

In 1972, the National Institute of Standards and Technology decided that a strong cryptographic algorithm was needed to protect non-classified information. The algorithm was required to be cheap, widely available, and very secure. NIST envisioned something that would be available to the general public and could be used in a wide variety of applications. So they asked for public proposals for such an algorithm. In 1974 IBM submitted the Lucifer algorithm, which appeared to meet most of NIST's design requirements.

NIST enlisted the help of the National Security Agency to evaluate the security of Lucifer. At the time many people distrusted the NSA due to their extremely secretive activities, so there was initially a certain degree of skepticism regarding the analysis of Lucifer. One of the greatest worries was that the key length, originally 128 bits, was reduced to just 56 bits, weakening it significantly. The NSA was also accused of changing the algorithm to plant a "back door" in it that would allow agents to decrypt any information without having to know the encryption key. But these fears proved unjustified and no such back door has ever been found.

The modified Lucifer algorithm was adopted by NIST as a federal standard on November 23, 1976. Its name was changed to the Data Encryption Standard (DES). The algorithm specification was published in January 1977, and with the official backing of the government it became a very widely employed algorithm in a short amount of time.

Over time various shortcut attacks were found that could significantly reduce the amount of time needed to find a DES key by brute force. And as computers became progressively faster and more powerful, it was recognized that a 56-bit key was simply not large enough for high security applications. As a result of these serious flaws, NIST abandoned their official endorsement of DES in 1997 and began work on a replacement, to be called the Advanced Encryption Standard (AES). Despite the growing concerns about its vulnerability, DES is still widely used by financial services and other industries worldwide to protect sensitive on-line applications.

To highlight the need for stronger security than a 56-bit key can offer, RSA Data Security has been sponsoring a series of DES cracking contests since early 1997. In 1998 the Electronic Frontier Foundation won the RSA DES Challenge II-2 contest by breaking DES in less than 3 days. EFF used a specially developed computer called the DES Cracker, which was developed for under $250,000. The encryption chip that powered the DES Cracker was capable of processing 88 billion keys per second. More recently, in early 1999, Distributed. Net used the DES Cracker and a worldwide network of nearly 100,000 PCs to win the RSA DES Challenge III in a record breaking 22 hours and 15 minutes. The DES Cracker and PCs combined were testing 245 billion keys per second when the correct key was found. In addition, it has been shown that for a cost of one million dollars a dedicated hardware device can be built that can search all possible DES keys in about 3.5 hours. This just serves to illustrate that any organization with moderate resources can break through DES with very little effort these days.

DES encrypts and decrypts data in 64-bit blocks, using a 64-bit key. It takes a 64-bit block of plaintext as input and outputs a 64-bit block of cipher text. Since it always operates on blocks of equal size and it uses both permutations and substitutions in the algorithm, DES is both a block cipher and a product cipher.

DES has 16 rounds, meaning the main algorithm is repeated 16 times to produce the cipher text. It has been found that the number of rounds is exponentially proportional to the amount of time required to find a key using a brute-force attack. So as the number of rounds increases, the security of the algorithm increases exponentially.

1.2 Modes of Operation

1.2.1 ECB (Electronic Code Book)

This is the regular DES algorithm. Data is divided into 64-bit blocks and each block is encrypted one at a time. Separate encryptions with different blocks are totally independent of each other. This means that if data is transmitted over a

network or phone line, transmission errors will only affect the block containing the error. It also means, however, that the blocks can be rearranged, thus scrambling a file beyond recognition, and this action would go undetected. ECB is the weakest of the various modes because no additional security measures are implemented besides the basic DES algorithm. However, ECB is the fastest and easiest to implement, making it the most common mode of DES seen in commercial applications. This is the mode of operation used by Private Encryptor.

1.2.2 CBC (Cipher Block Chaining)

In this mode of operation, each block of ECB encrypted ciphertext is XORed with the next plaintext block to be encrypted, thus making all the blocks dependent on all the previous blocks. This means that in order to find the plaintext of a particular block, you need to know the ciphertext, the key, and the ciphertext for the previous block. The first block to be encrypted has no previous ciphertext, so the plaintext is XORed with a 64-bit number called the Initialization Vector, or IV for short. So if data is transmitted over a network or phone line and there is a transmission error (adding or deleting bits), the error will be carried forward to all subsequent blocks since each block is dependent upon the last. If the bits are just modified in transit (as is the more common case) the error will only affect all of the bits in the changed block, and the corresponding bits in the following block. The error doesn't propagate any further.

Proposed Algorithm for Encryption
/*
** This program provides the following cryptographic functionalities
* 1. Encryption using DES
* 2. Decryption using DES
* 3. Generate a DES key
*/
Step 1. Generate a DES key using KeyGenerator
Step 2. Create a Cipher by specifying the following parameters
a. Algorithm name - here it is DES
b. Mode - here it is CBC
c. Padding - PKCS5Padding
Step 3. Initialize the Cipher for Encryption
Step 4. Encrypt the Data
1. Declare / Initialize the Data. Here the data is of type String
2. Convert the Input Text to Bytes
3. Encrypt the bytes using
Step 5. Decrypt the Data
1. Initialize the Cipher for Decryption
2. Decrypt the cipher bytes

1.3 Hiding Data in File

Encoding secret messages in audio is the most challenging technique to use when dealing with steganography. This is because the human auditory system has such a dynamic range that it can listen over. To put this in perspective, the perceives over a range of power greater than one million to one and a range of frequencies greater than one thousand to one making it extremely hard to add or remove data from the original data structure. The only weakness comes at trying to differentiate sounds (loud sounds drown out and quiet sounds) and this is what must be exploited to encode secret messages in audio without being detected.There are two concepts to consider before choosing an encoding technique for audio. They are the digital format of the audio and the transmission medium of the audio. There are three main digital audio formats typically in use. They are Sample Quantization, Temporal Sampling Rate and Perceptual Sampling. Sample Quantization which is a 16-bit linear sampling architecture used by popular audio formats. Temporal Sampling Rate uses selectable frequencies (in the KHz) to sample the audio. Generally, the higher the sampling rate is, the higher the usable data space gets. The last audio format is Perceptual Sampling. This format changes the statistics of the audio drastically by encoding only the parts the listener perceives, thus maintaining the sound but changing the signal. This format is used by the most popular digital audio on the Internet today is MP3. Transmission medium must also be considered when encoding secret messages in audio. W. Bender introduces four possible transmission mediums:

Digital end to end - from machine to machine without modification.Increased/decreased resampling - the sample rate is modified but remains digital.Analog and resampled - signal is changed to analog and resampled at a different rate. Over the air - signal is transmitted into radio frequencies and resampled from a microphone.

There are three more popular encoding methods for hiding data inside of audio. They are low low-bit encoding, phase phase-coding and spread spectrum. low-bit encoding embeds secret data into the least significant bit of the audio file. This method is easy to incorporate but is very susceptible to data loss due to channel noise and resampling. Phase coding substitutes the phase of an initial audio segment with a reference phase that represents the hidden data. This can be thought of as sort of an encryption for the audio signal by using what is known as Discrete Fourier Transform (DFT), which is nothing more than a transformation algorithm for the audio signal.

Spread spectrum encodes the audio over almost the entire frequency spectrum. It then transmits the audio over different frequencies which will vary depending on what spread spectrum method is used. Direct Sequence Spread Spectrum (DSSS) is one such method that spreads the signal by

multiplying the source signal by some pseudo random sequence. The sampling rate is then used as the chip rate for the audio signal communication. Spread spectrum encoding techniques are the most secure means by which to send hidden messages in audio, but it can introduce random noise to the audio thus creating the chance of data loss.

Proposed Algorithm for Data Hiding

Input: Audio file and message
Output: Audio file with hidden message
while data left to embed do
get next byte coefficient from message
if message $\neq 0$ and message $\neq 1$ then
get next LSB from message
replace file LSB with message LSB
end if
insert message into file
end while

2. IMPLEMENTATION

For developing the proposed system Java 1.4 or above is needed and it requires Microsoft-XP Operating System with standard PC (with minimum hardwareconfiguration available in present time)

Input:
Audio file along with the message to hide
Process:
User select options such as encryption and password protection. After selecting the option the message is hidden in audio file.
Output:
Audio file along with the hidden message

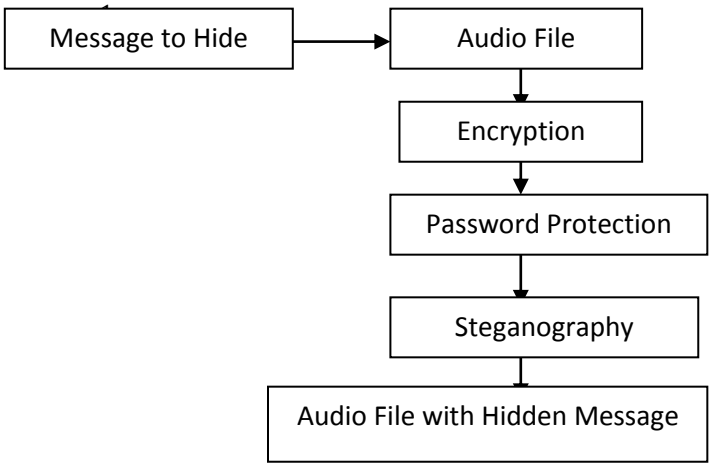

Figure 1 Flow chart for inserting message in audio file

Following are the steps performed to hide data in audio file:

Step 1: User selects the audio file
Step 2: Select the message or file to hide.
Step 3: Select the data should to be encrypted while hiding.
Step 4: Select the password for audio file.
Step 5: Audio file with hidden message

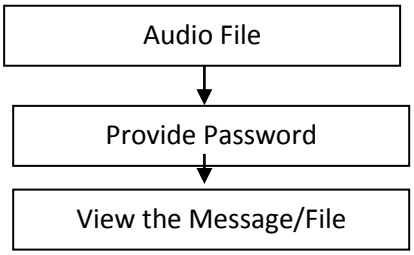

Figure 2: Flow cart for retrieving hidden message from audio file

Step 1: User selects the audio file
Step 2: Provide the password provided at the time of hiding
Step 3: View the hidden message or choose the location o save file.

3. INVESTIGATION AND SYSTEM EVALUATION

Here we will have first try to investigate whether the proposed DSE based encryption mechanism works suitably in the audio steganography framework presented in this paper. The second question is that if it works, then how efficiently it will be working. The develop software GUI interfaces in JAVA which on the other hand will prove the implementation feasibility of the proposed audio stago-encryption framework. The interfaces also included some buttons for other cryptographic operations in the consider encryption as well as decryption system.

4. CONCLUSION AND SCOPE FOR FUTURE WORK

Steganography is the technique for hiding the existence of a secondary message in presence of primary message. The most common use of steganography is to hide a message or file inside another file. This paper, which is an attempt to develop compact and efficient tool for steganography, serves the needs of compiling and running the program with minimum hardware, software and memory. The develop system tries to provide a good interface between user and system. The package tries to provide such facilities to the user which makes his job very easy.

The secure environment is provided to the customer and every measure is being taken to keep the customer information safe. System is very handy and requires minimum investments. There are number of ways that this paper could be extended. Its performance can be upgraded to higher levels in practical conditions. There are also other weighting algorithms like spread spectrum, echo data hiding etc., and those can be implemented. Instead of having common secret key to encode and decode, a public–private key pairs will be introduced.

Also other encryption algorithm such as triple DES, AES and RSA can be used to enhance the security of hidden data. The compression algorithm can be used to reduce the size of the hidden data. this research recommends the incorporation of higher level of security mechanism besides data hiding through steganography. More experiments enhancing the limit of encrypted string length for various other types of audio files can augment the above claims but do not appear to bring any new conceptual insights.

REFERENCES

[1] Gopalan K. Audio steganography using bit modification. Proc. of IEEE Int. Conf. Acoustics, Speech, and Signal Processing, 2003. Vol. 2, pp. 421-424.

[2] NazariS,Eftekhari-MoghadamAM, andMoin MS. A novel image steganography scheme based on morphological associative memory and permutation schema. 2014, Security and Communication Networks, 2014, Early View, DOI:10.1002/sec.962.

[3] Chang CC, Chen TS &Hsia HS. An Effective Image Steganographic Scheme Based on Wavelet Transform and Pattern-Based Modification. IEEE Proceedings of the 2003 International Conference on Computer Networks and Mobile Computing, 2003.

[4] Chen B,WomellGW.Quantization index modulation: a class of provably good methods for digital watermarking and information embedding", IEEE Transactions on Information Theory, 2001, Vol. 47, No. 4, pp. 1423-1443.

[5] Chen B.Design and analysis of digital watermarking, information embedding, and data hiding systems. Ph.D. dissertation, 2000, MIT, Cambridge, MA.

[6] AminMM, SallehM, Ibrahim S, M. KatminR,ShamsuddinMZI. Information Hiding using Steganography, 2003,Proceedings of 4thIEEE National Conference on Telecommunication Technology, Shah Alam, Malaysia.

[7] ZollnerJ, FederrathH, KlimantH, et al. Modelling the Security of Steganographic Systems.In 2ndWorkshop on Information Hiding, Portland, April 1998, pp. 345-355.

[8] Johnson NF, KatzenbeisserS. A Survey of Steganographic Techniques. In Information Hiding: Techniques for Steganography and Digital Watermarking. 2000, Boston, Artech House, pp. 43-78.

[9] YardimciY, Cetin AE,AnsariR. Data hiding in speech using phase coding. ESCA. Eurospeech97, Sept. 1997, pp. 1679- 1682, Greece.

[10] BennettK. Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text.2004, Purdue University, CERIAS Tech. Report 2004-13.

[11] MatsuokaH. Spread Spectrum Audio Steganography using Sub–band Phase Shifting. Proceedings of the 2006 IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP'06)

[12] KatzenbeisserS,Fabien AP, eds. Information Hiding Techniques for Steganography and Digital Watermarking. 2000, Boston: Artech House.

[13] ParthasarathyC,SrivatsaSK. Increased Robustness of LSB Audio Steganography by Reduced Distortion LSB Coding.2009, Journal of Theoretical & Applied Information Technology, Vol 7, No 1, pp 80-86.

[14] Stallings W. Cryptography and Network.2010, PHI, India.

[15] GargR, GulatiT.Comparison of LSB & MSB Based Steganography in Gray-Scale Images. International Journal of Engineering Research & Technology (IJERT), 2012, Vol. 1, Issue 8.

[16] GhongeM, DhawaleA, TongeA.Review of Steganography Techniques. International Journal of Advent Research in Computer & Electronics (IJARCE), 2014, Vol.1, No.1.

[17] RohitT, Sharma B, and MalhotraS. A robust substitution technique to implement audio steganography. Proc. of IEEE International Conference on Optimization, Reliabilty, and Information Technology (ICROIT), 2014, pp. 290-293.

[18] PawarSS, KakdeV. Review on Steganography for Hiding Data. International Journal of Computer Science and Mobile Computing, 2014, Vol.3 Issue.4, pp. 225-229.

[19] AshwiniP, BhagyashreeP, AshwiniR, NagargojeYR, Khan MA. Image and Audio Based Secure Encryption and Decryption. International Journal of Advanced Research in Computer and Communication Engineering, 2014, Vol. 3, Issue 3.

[20] PandeA, MohapatraP,ZambrenoJ. Securing Multimedia Content Using Joint Compression and Encryption. IEEE MultiMedia, 2013, Vol.:20, Issue: 4, pp. 50–61.

[21] SaurabhJ, AmbhaikarA. Audio Steganography using RPrime RSA and GA Based LSB Algorithm to Enhance Security. International Journal of Science and Research (IJSR), 2012, Vol 1 Issue 2.

[22] PadmashreeG, VenugopalaPS.Audio Stegnography and Cryptography: Using LSB algorithm at 4th and 5th LSB layers. International Journal of Engineering and Innovative Technology (IJEIT),2012, Vol. 2, Issue 4.

[23] Pooyan M, Delforouzi A. LSB-based Audio Steganography Method Based on Lifting Wavelet Transform. IEEE International Symposium on Signal Processing and Information Technology, 2007.

[24] Mazurczyk W. Lost Audio Packets Steganography: The First Practical Evaluation. Security and Communication Networks,2012, Vol 5(12), pp. 1394–1403.

[25] Sachin S. Agrawal "Secured Audio Signals Using Enhanced Steganography", International Journal on Computer Engineering and Information Technology (IJCEIT), Volume No. 14, No 19, pp. 44-49, Scientific Engineering Research Corporation, ISSN 0972-2034

[26] Adeel Javed, Atanu Das. Security Enhancement in Audio Steganography by RSA Algorithm. International Journal of Electronics & Communication Technology IJECT, 2015, Vol.:20, Issue: 1, pp. 139–142.