ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, *Vol 8(1), 17–22, January 2015* DOI : 10.17485/ijst/2015/v8i1/52396

Secure Data Transfer through Audio Signal with LSA

R. Valarmathi[1*] and G. M. Kadhar Nawaz[2]

[1]Bharathiar University, Coimbatore, Tamilnadu, India; India; valarmathigk@yahoo.com
[2]Department of MCA, Sona College of Technology, Salem-5, Tamilnadu, India

Abstract

Today's large demand of internet applications requires data to be transmitted in a secure manner. Data transmission in public communication system is not secure because of interception and improper manipulation by eavesdropper. So the attractive solution for this problem is steganography. Steganography is the scheme of hiding the existence of secret information by concealing it into another medium such as image, video or audio. Cryptography is used to encrypt the data so that it is unreadable by a third party. So to add another layer of protection we can encrypt the key of the hidden message. This paper proposes a new algorithm to hide the data in Audio signal and it uses Linear Subsequence Algorithm (LSA) which increases data protection.

Keywords: Cryptography, Encryption, Linear Subsequence Algorithm (LSA), Steganography

1. Introduction

By development of computer and the expansion of its use in different areas of life and work, the issue of security of information has gained special significance[16]. One of concerns in the area of information security is the concept of hidden exchange of information. For this purpose, various methods including cryptography, steganography, coding and so on have been used[27,14]. Steganography is one of the methods which have attracted more attention during the recent years.

Steganography is the study of embedding and hiding messages in a medium called a covertext. Steganography is related to cryptography and is just about as old[1]. It was used by the Ancient Greeks to hide information about troop movements by tattooing the information on someone's head and then letting the person grow out their hair. Simply put, steganography is as old as dirt[16].

Most steganography jobs have been performed on images, video clips, text, music and sound. It has also been implemented on such varying systems as computers and mobile phones[17].

Nowadays, however, information security has been improved considerably with the other mentioned methods. The steganography method, in addition to application in cover exchange of information, is also used in such other fields as copyright protection, preventing e-document forging, etc[11].

There are three important parameters in designing steganography methods: perceptual transparency, robustness and hiding capacity[7]. While robustness is usually the most important factor for applications like copyright protection and watermarking, hiding capacity is more important for steganography applications because the goal of steganography algorithms is to transfer information[17].

Among the methods of steganography, the most common one is to use images for applying steganography. In these methods, features such as pixels of image are changed in order to hide the information so as not to be identifiable by human users and the changes applied on the image are not tangible[17].

In audio steganography, the weaknesses of Human Auditory System (HAS) is used to hide information in the audio. Because the human auditory system has more precision than Human Visual System (HVS), audio steganography is more challenging than image steganography[17].

2. Steganographic Techniques

The steganographic techniques are broadly classified into spatial domain, transform domain, spread spectrum, statistical methods, distortion and cover generation

*Author for correspondence

techniques. Spatial domain techniques are also called as substitution techniques. In substitution technique the secret message bits is encoded in the insignificant parts of the cover image. Since there are only minor changes in the image the sender assumes the attacker will not notice the changes in the original image. But it is vulnerable to signal processing attacks and also it loses the total information for loss compression techniques[24].

The Transform domain techniques[24] hides the information in significant bits of the cover image hence it is robust to the techniques like compression and cropping. Most common transform domain techniques are discrete cosine transform and wavelet transforms. A trade off exists between the amount of secret information to be embedded and the robustness obtained. Spread spectrum deals either cover image as noise or tries to add pseudo random noise to the cover image.

The next is statistical technique[24] also called as model based technique which modifies the statistical characteristic of the cover image in addition it preserves them in embedding process. This modification can be perceived by humans by identifying the luminance variation. This technique is vulnerable to rotating, cropping, scaling attacks and also all the watermarking attacks.

The Distortion technique[24] requires the knowledge of the cover image in the decoding process. In practice it is not efficient method because the secret message can be extracted if the original cover image is available to the attacker. In earlier days most text based hiding methods were distortion type. The last technique is cover generation; in this the digital cover is generated only for the purpose of being a cover for secret message transfer. Regular expressions and mimic functions are used to generate a cover.

More number of Audio Steganography works has been done using the above methods. This paper uses Cross Bit Manipulation for improving the performance of the proposed work.

3. Audio Steganography

In a computer-based audio steganography system, secret messages are embedded in digital sound. The secret message is embedded by slightly altering the binary sequence of a sound file. Existing audio steganography software can embed messages in WAV, AU, and even MP3 sound files[4].

Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media, such as digital images[4]. In order to conceal secret messages successfully, a variety of methods for embedding information in digital audio have been introduced. 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[4].

3.1 Related Work

Relevant work has been done on this subject. Many have designed system which increase the capacity of the steganography approach and few has increased security. Sheelu proposed a system that enhances the data hiding capacity in Audio Steganography using LSB method. She uses last 4 LSB's instead of a single LSB to enhance the data hiding capacity of carrier file[20]. S. S. Divya, M. Ram Mohan Reddy proposed two novel approaches of substitution technique of audio steganography that improves the capacity of cover audio for embedding additional data[8]. Bhagyashri A. Patil, Vrishali A. Chakkarwar proposed a method of audio steganographic system that provides a unique platform to hide the secret information in audio file though the information is in text, image or in an audio format[5]. P. Ramesh Yadav, V. Usha Shree, K. Padmapriya proposed a steganographic method of embedding textual information in an audio file[15]. Taruna, Dr. Dinesh Singh proposed technique which keyless randomization is provided to insert secret information in multiple and variable LSB's[23].

Tanmaiy G. Verma, Zohaib Hasan, Dr. Girish Verma proposes the system introduces double layer protection along with a new run time inter-leveling based audio steganography technique[22]. Nagaseshu K., Srinivasa Rao V., Hima Deepthi V. proposed technique that alters the data of lower bit in a cover object to embed textual information[12]. R. Sridevi, Dr. A. Damodaram, Dr. Svl. Narasimham proposed the system which is based on audio Steganography and cryptography, ensures secure data transfer between the source and destination[21]. R. M. Goudar, Prashant N. Patil, Aniket G. Meshram, Sanyog M. Yewale, Abhay V. Fegade presents the a system, which uses features of both cryptography as well as steganography, where TCP/IP header is used as a steganographic carrier to hide encrypted data[10].

R. Venkateswaran, V. Sundaram proposes a new model ISS-IHAS - Embedding Text in Audio Signal that embeds the text like the existing system but with strong encryption that gains the full advantages of cryptography[26]. K. Geetha, P. Vanitha Muthu propose a new model ETAS - Embedding Text in Audio Signal that embeds the text like the existing system but with encryption that gains

the full advantages of cryptography[9]. K. Sakthisudhan, P. Prabhu, P. Thangaraj proposed a system which is simulated and their corresponding waveforms prove the effectiveness of the method[18]. K. P. Adhiya, Swati A. Patil proposed a Steganographic method for embedding textual information in WAV audio[2].

Neil Jenkins, Jean Everson Martina proposes new methods which have looked at the use of audio as a carrier for hidden data[13]. Budda Lavanya, Vittapu Sravan kuma proposed the technique, first the audio file is sampled and then an appropriate bit of each alternate sample is altered to embed the cryptography of textual information (secret information)[6]. B. Santhi, G. Radhika and S. Ruthra Reka dio steganography proposed the simple method for audio steganography that slightly modify the LSB technique[19]. M. Vara Lakshmi, Sundaradasu Suresh presents audio steganography algorithms like Substitution methods. By using these methods they provide more security using cryptographic methods developed in substitution techniques[25]. Ary Mazharuddin Shiddiqi, Tirta Priambadha, Baskoro Adi Pratomo is aimed to implement a method of Steganography and cryptography in a chat application[3]. Ziyad Tariq Mustafa Al-Ta'i, presents multilayer new covert audio cryptography as a developed model in order to get more secrecy[29].

4. Proposed Work

Proposed work consists of sender and receiver side. In the sender side, the text file which has to be embedded into an audio file is encrypted using Linear Subsequence Algorithm (LSA). The encrypted file obtained is then embedded in an audio file using Cross Bit Manipulation Algorithm (CBMA). The resultant audio file contains the secret message. Before embedding the text file into an audio file, carry bits of both the file are compared and if it matches then only the embedding process can be done.

In the receiver side, the embedded audio file is received and the receiver can extract the secret message. The secret file content can be extracted and displayed. Then original text file content can be extracted and displayed using CBMA and LSA respectively.

The following gives about the CBMA and LSA Algorithms:

4.1 Cross Bit Manipulation

The cross bit table instruction permutes bits using the audio, a general permutation audio. The audio consists of the concatenation of a butterfly audio and an inverse butterfly audio. The structure of the, where n = 8. The n-bit audios consist of lg(n) stages and thus the full audio has 2 X lg(n) – 1 stages (one stage is eliminated due to the equivalence of the first and last stages of the two subaudios)[28].

Each stage is composed of n/2 2-input switches, each of which is constructed using two 2:1 bit. In the this stage (I starting from 1), the input bits are $n/2^i$ positions apart for the butterfly audio and 2^{i-1} positions apart for the inverse audio. A switch either passes through or swaps its inputs based on the value of a control bit. Thus n/2 control bits are required per stage[28].

The cross instruction permutes bits using two stages of the audio. One of the two input operands holds the data to be permuted while the other input operand is used to hold the control bits for two stages (the other stages are configured to pass through the bits). An additional sub-opcode is used to indicate which two stages are used. lg(n) cross instructions are required for any arbitrary permutation of n bits[28].

The CBMA works as follows for Embedding: 1. Get Input from Embedded Stenography File. 2. Convert embedded file into ASCII Value. 3. Write binary Value (bu) get through the algorithm. 4. Calculate Carry. 5. Set Carry as Secrectbit. 6. Move right most cross bit in carry and skip addition if bit is zero. 7. Continue until if Embedded files all ASCII values rearranged. 8. Write sb into the Encrypted file Format 9. goto step 5 until Cross Table is Empty. 10. Increment the count by 1. 11. Goto Step 2. 12. Write sb into output secret file. The reverse process has been done for the De-Embedding to get the secret message in the receiver side.

4.2 Linear Subsequence Algorithm (LSA) for Encryption

Step 1: Get user input.
Step 2: Assign user input = vector D[K].
Step 3: ASCII Value Calculation for D[K]:
 For (i = 0; D[i] <=D[k].length; i++)
 ASCII value for D[i] = A[i];
 Repeat 2 And 3 until loop exit.
Step 4: Getting input increment value = I.
Step 5: Getting input iteration value = IT.
Step 6: Getting input operator = O.
Step 7: For (j = 0; j++)
 Init Temp = 0; Temp = A[j] + I;
 If (Temp > 255) Then

Vector P[j] = (Temp – 255);
Else P[j] = Temp;
Repeat 7 until IT times exit.
Step 8: Finding Alphabet for ASCII value in P[j]
For (x = 0; P[x] <=P[j].length; x++)
Alphabet value for P[x] = vector alp[i];
Repeat 8 until loop exit.
Step 9: Output Encrypted Value.

4.3 Linear Subsequence Algorithm (LSA) for Decryption

Step 1: Get user input.
Step 2: Assign input: vector D1 [k].
Step 3: Finding ASCII value for alphabet D1 [k]
For (y = 0; D1[y] <=D1 [k].length; y++)
Alphabet value for D1[y] = vector AS[y];
Repeat 3until loop exit.
Step 4: Getting input increment value = I1.
Step 5: Getting input iteration value = IT1.
Step 6: Getting input operator = O1.
Step 7: For (z = 0; z++)
Init Temp1 = 0; Temp1 = A1 [z] – I1;
If (Temp1 < 0) then Vector P1 [z] = (A1 [z] + 255);
Else P1[z] = Temp1;
Repeat 7 until IT times exit.
Step 8: Output Decrypted Value.

5. Analysis of the Proposed Work

The proposed technique has been implemented and tested. A number of cases have been tested and the system successfully hides the encrypted text file in an Audio file without much more deviation from the original Audio file. The following gives the analysis of the proposed work.

5.1 System Throughput Estimation

The Secret audio files processing, the chart is been evaluated for File Transferring Rate, and Stream Throughput value. The throughput to find out how many Streams gets to File Transfer. The First Stream file transfer rate obtains 0 to 1500, The second Stream file transfer rate obtains 1500 to 3000, The Third Stream file transfer rate obtains 3000 to 3500, The Fourth Stream file transfer rate obtains 3500 to 5000, The fifth Stream file transfer rate obtains 5000 to 5275, The six Stream file transfer rate obtains 5275 to 6725, The Last Stream file transfer rate obtains 6725 to 8000.

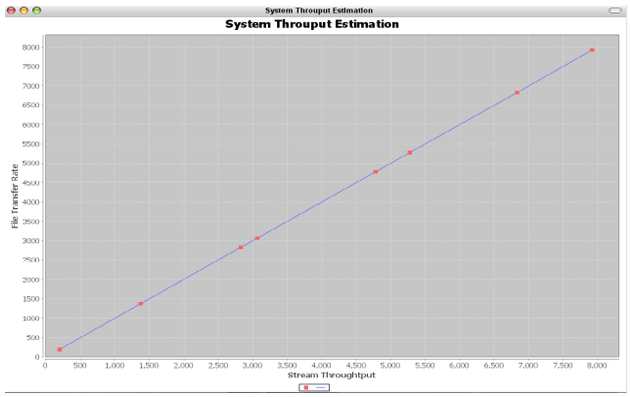

Figure 1. System Throughput Estimation.

5.2 Audio Classification based on the Algorithm

Table 1. Audio Classification

SI. No	Audio Stenography Application	Benign Process			Suspicious Process		
		Detect	Trace	Restrict	Detect	Trace	Restrict
1	Communicate with remote Host ATM	$Label_{executable}$	✓	✓			Deny
2	Create Cloud Computing executable File	$Label_{executable}$		✓			Deny
3	Bank Record Modify register for start up	$Label_{executable}$		✓			Deny
4	Copy the Important Application and files	$Label_{executable}$	✓	✓			Deny
5	Obtain System Information		✓	✓			Deny
6	Inject into other Process		✓	✓			Deny
7	Modify Executable file			✓			Deny
8	Create or modify OS series			✓			Deny
9	Change security setting			✓			Deny
10	Hiding the Network clients			✓			

Continued

Table 1. (*Continued*)

Sl. No	Audio Stenography Application	Benign Process			Suspicious Process		
		Detect	Trace	Restrict	Detect	Trace	Restrict
11	Destroying Army Anti Secret services		✓	✓			Deny
12	Modifying system configuration file			✓			Deny
13	Logging the keystrokes and Mouse clicks			✓			Deny
14	Modifying the register for Uninstallation			✓			Deny
15	Create Windows hooks			✓		$Label_{process}$	Deny
16	Install all Modifying software for Driver Corruption			✓		$Label_{process}$	Deny

6. Conclusion

The proposed system successfully embeds encrypted secret text file in an Audio file. The quality of the retrieved data is not affected by the proposed embedding scheme as can be seen from the zero bit error. The experimental results show the better performance of the proposed system and it shows the desired features of Audio steganography technique.

7. Acknowledgement

My sincere thanks to Dr. G. M. Kadhar Nawaz M.C.A., Ph.D., Director& Professor, Department of MCA, Sona College of Technology, Salem-5 for supporting and encouraging to do this research work and I extend my thanks to my friends who are in this circle and also the peer review committee members.

8. References

1. Billiam A. An Introduction to Steganography and its uses. 2014. Available from: http://null-byte.wonderhowto.com/how-to/introduction-steganography-its-uses-0155310/
2. Swati AKP, Patil A. Hiding Text in Audio Using LSB Based Steganography. Inform Tech Knowl Manag. 2012; 2(3). ISSN 2224-5758 (Paper) ISSN 2224-896X (Online).
3. Shiddiqi AM, Priambadha T, Pratomo BA. Echo Data Hiding Steganography and RSA Cryptography On Audio Media. Industri. 11(1):1–9.
4. Audio steg: methods - Snotmonkey.com, Available form: http://www.snotmonkey.com/work/school/405/methods.html, 2005.
5. Patil BA, Chakkarwar VA. Review of an Improved Audio Steganographic Technique over LSB through Random Based Approach. IOSR-JCE. 2013 Jan-Feb; 9(1):30–4. e-ISSN: 2278-0661, p-ISSN: 2278-8727.
6. Lavanya B, Kumar VS. Combination of Cyphertext and Audio Steganography Technique for Secrete Communication. International Journal of Emerging Technology and Advanced Engineering. 2012 Dec; 2(12). (ISSN 2250-2459, ISO 9001:2008 Certified Journal) Avaliable: www.ijetae.com.
7. Cvejic N, Seppanen T. A wavelet domain LSB insertion algorithm for high capacity audio steganography. Proceedings of 10th IEEE digital Signal Processing Workshop; 2002.
8. Divya SS. Reddy RMM. Hiding Text In Audio Using Multiple LSB Steganography And Provide Security Using Cryptography. Int J Adv Comput Sci Tech Research. 2012 Jul; 1(6).
9. Geetha K, Muthu VP. Implementation of ETAS (Embedding Text in Audio Signal) Model to Ensure Secrecy. IJCSE. 2010; 2(4):1308–13.
10. Goudar RM, Patil PN, Meshram AG, Yewale SM, Fegade AV. Secure Data Transmission by using Steganography. Information and Knowledge Management. 2012; 2(1).
11. Hartung, Girod B. Copyright Protection in Video Delivery Networks by Watermarking of Pre-Compressed Video. Proceedings of European Conference on Multimedia Applications; 1997.
12. Nagaseshu K, Rao SV, Deepthi HV. A Novel Approach for Embedding Text in Audio to Ensure Secrecy. IJCSIT. 2011; 2(4):1592–4.
13. Jenkins N, Martina JE. Steganography in Audio. Avaliable: http://petitcolas.net/fabien/steganography/mp3stego/, p. 269–78.
14. Singh PK. Steganography. 2009. Avaliable: http://www.academia.edu.
15. Yadav RP, Shree UV, Padmapriya K. Hiding Data in Audio Using Audio Steganography. International Journal of Computer Applications in Engineering Sciences. 2011 Jun; 1(2).
16. Salah S. Text Steganography in SMS. 2008. Avaliable: http://www.academia.edu.
17. Shirali-Shahreza S, Manzuri-Shalmani MT. Adaptive Wavelet Domain Audio Steganography with High Capacity

and Low Error Rate. IEEE International Conference on Information and Emerging Technologies; 2007.
18. Sakthisudhan K, Prabhu P, Thangaraj P. Secure Audio Steganography for Hiding Secret information. International Conference on Recent Trends in Computational Methods, Communication and Controls; 2012.
19. Santhi B, Radhika G, Reka RS. Information Security using Audio Steganography - A Survey. Res J Appl Sci Eng Tech. 2012; 4(14):2255–8.
20. Sheelu. Enhancement of Data Hiding Capacity in Audio Steganography. IOSR-JCE. 2013 Jul-Aug; 13(3): 30–5. e-ISSN: 2278-0661, p-ISSN: 2278-8727.
21. Sridevi R, Damodaram A, Narasimham Svl. Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key with Enhanced Security. J Theor Appl Inform Tech. 768–71.
22. Verma TG, Hasan Z, Verma G. A Double Layer Protection Transmission Technique Using Cryptography and Steganography. IJARCET. 2013 Oct; 2(10):2761–3.
23. Taruna, Singh D. Message Guided Random Audio Steganography Using Modified LSB Technique. International Journal of Computers & Technology. 2014 Jan; 12(5): 3464–8.
24. Vanmathi C, Prabu S. A Survey of State of the Art techniques of Steganography. IJET. 2013.
25. Lakshmi VM, Suresh S. Hybrid Steganography Using Multimedia (Image, Audio, Video) Concepts Based On Invariant Substitution Techniques. International Journal for Development of Computer Science & Technology. 2013 June-July; 1(4).
26. Venkateswaran R, Sundaram V. Implementation of ISS - IHAS (Information Security System - Information Hiding in Audio Signal) model. IJACSA. 2011; 2(6).
27. Vijayalakshmi V, Mahalakshmi, Thamizharasan. Data Encryption hiding technique in Non-Standard cover files. International Journal of Advanced Research in Computer Science and Technology. 2014.
28. Hilewitz Y. Advanced Bit Manipulation Instructions: Architecture, Implementation and Applications. 2008.
29. Al-Ta'i ZTM. Development of Multilayer New Covert Audio Cryptographic Model. International Journal of Machine Learning and Computing. 2011 Jun; 1(2).