1st International Conference on Recent Trends in Engineering & Technology, Mar-2012
Special Issue of International Journal of electronics, Communication & Soft Computing Science & Engineering, ISSN: 2277-9477

AUDIO STEGANOGRAPHY USING LSB

BANKAR PRIYANKA R. KATARIYA VRUSHABH R. PATIL KOMAL K. SHASHIKANT M. PINGLE

SANGHAVI MAHESH R.

Abstract-In this paper, Audio Steganography is an application to embed a data file in audio data. Steganography is technique used to transmit hidden information by modifying a covered file in an imperceptible manner. The transmission must be possible in spite of subsequent imperceptible (attacks) of the modified signal. We propose a novel approach of submission technique of audio Steganography. Using genetic algorithm, message bits are embedded into multiple and higher LSB layer values, resulting in increased robustness. The robustness specially would be increased against those international attacks which try to reveal the hidden message and also some unintentional attacks like noise addition as well.

A genetic algorithm (GA) is search heuristic that mimics the process of natural evolution. This heuristic is routinely used to generate useful solutions to optimization and search problem.

Index terms- Embedding, Genetic Algorithm (GA), LSB, Steganography.

I. INTRODUCTION

In the current internet community, secure data is limited due to its attack made on data communication. So more robust methods are chosen to so that they ensure secured data transfer. Steganography and watermarking are the fast developing area of information hiding. Steganography is changing a multimedia file in such way that you can't see some added data with naked eye. As Human Auditory System (HAS)[2] is more sensitive than Human Visual System (HVS)[1]. One of the solutions which came to the rescue is the audio Steganography. The two primary criteria for successful embedding of a convert message are that the stego signal resulting from embedding is perceptually indistinguishable from the host audio signal and the embedded message is recovered correctly at receiver.

There are numerous methods used to hide information inside picture, audio and video file. LSB (Least Significant Byte) coding is one of the earliest techniques in information hiding and watermarking area of digital sound. The main advantage of LSB coding algorithm is very high channel bit rate and low computational complexity of the algorithm.

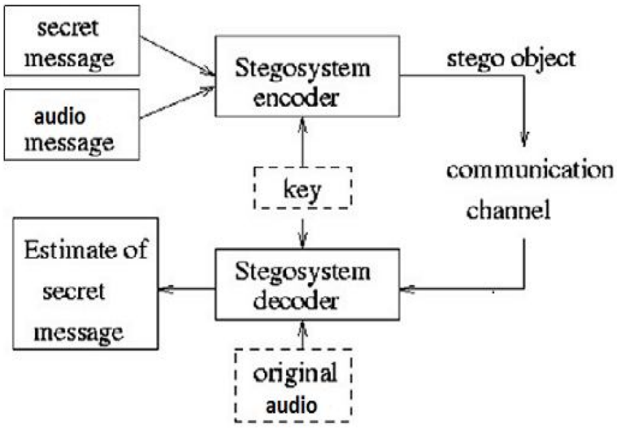

Fig 1: Audio steganography with cryptography

II. EXISTING SYSTEM

In the modern age so many techniques have been designed which works with concerned multimedia object. So in this regard various software tools are also available. Different existing software tools are surveyed. These tools are categorized as open source, shareware and commercial. The existing systems for audio steganography are restricted for some selected audio file formats. Message length is restricted to 500 characters.

III. PROPOSED SOLUTION

To provide more security the original data file is encrypted first before embedding. And second purpose of this system is to increase robustness in case of security. In this system we initially encrypt the message using asymmetric public-key algorithm (RSA) and then encrypted message bits are inserted at random higher LSB layer position of the host audio.

We have original audio sample and inserting message bit in different LSB layer positions we get some new samples. Sometimes it can happen that for more than one LSB layer we get the same difference between original audio sample and new audio samples. In this case we will choose the higher LSB layer.

IV. ALGORITHM FOR AUDIO STEGANOGRAPHY USING LSB

1. Start // Select one of the option following.
2. Hide Data.
   Recover Data.
3. Stop.

A. Hide Data

1. Read both text as well as audio file from user.

2. Perform RSA encryption on text file to convert plaintext to cipher text.
3. Embed cipher text into audio file by using GA based LSB coding algorithm.
4. Attach public key, private key and LSB layer value to stego file.

RSA Encryption

1. Read file.
2. Generate two random prime numbers P and Q.
   n:= P*Q // new variable
   phi:=(P-1)*(Q-1) // new variable
3. find e such that
   1 < e < phi and gcd (e,phi) ==1
   Where e and phi are always coprime.
   Calculate 'd' // new variable
   Such that e*d=1 mod phi
   d= e^{-1} mod phi
4. Generate public and private keys.
   Public key = (n,e) //Which is used for encryption.
   Private key = (n,d) //Which is passed to receiver for decryption.
5. Encryption
   Consider an example that 'm' is being encrypted in 'c' like this.
   C = m^e mod n
   = m^e mod n.
   Repeat this step for all character. Store each cipher character in ciphertext file (T').

GA Based LSB Coding

1. Convert encrypted message to byte streams.
2. Read an audio file byte-wise. Convert little Indian notation to integer array (16 bits sample).
3. Generate n (2-16) number of chromosomes of 16 genes by inserting a message bit into 16 bits audio sample in n (2-16) random positions.
4. Generate LSB layer value
5. Read both the files audio as well as text bit wise
6. Divide audio file in stream of 16 bits
7. Embed each bit of text in stream of bits on 'i' position as shown below
   if position = 1, then no action is taken
   if position = 2 to 16
   if 0 bit is to be embedded if data bit is for position i
   if data bit on i-1 position to 1 position are 0's, perform crossover operation with 1...11 (i-1 no's) bit string
   if data bit on i+1 position is 0, perform mutation operation on i+1 position and crossover operation for i-1 to 1 with 0…00(i-1 no's) bit string
   if data bit on i+1 and i-1 to 0 are 1 no action is taken if 0 bit is to be embedded
   if data bit is 0 then no action is taken if 1 bit is to be embedded
   if data bit is 1 then no action is taken if 1 bit is to be embedded
   if data bit is 0 then
   if layer is 1, then no action is taken if layer = 2 to 16
   if i-1 to 0 position are holding 1
   crossover operation for i-1 to 1 with 0…00(i-1 no's) bit string
   if i+1 position holding 1 and i-1 to 1 position holding 0, perform mutation operation on i+1 position and crossover operation for i-1 to 1 with 1…11(i-1 no's) bit string

B. Recover Data

1. Read stego file from user with specified destination where user wants to generate new file.
2. Extract cipher text from stego file with public and private key using LSB layer value.
3. Convert cipher text into plain text with the help of public and private key by using RSA decryption algorithm.

GA Based LSB Coding Extraction

1. Read the stego audio file byte-wise (16 bits sample).
2. By getting the location number (LSB layer value) of the hidden message bit's into the stego audio sample, extract message bit from the stego audio file
3. To get 8 bits of the message data and random location number from audio data, choose 16 (16 bits) stego-audio data.
4. Get the message byte streams for all the random positions
5. Convert message byte stream to a message text file (T')

RSA Decryption

1. Read cipher character 'c' from cipher text file 'T''
2. Read private key = (n, d)
3. Apply formula for each 'c' to generate 'm'
   m = c ^ d mod n
   = c^d mod n.
4. Store all 'm' in target text file (T).

V. ADVANTAGES

1. In this proposed system text is embedded in audio same technique can be used to hide audio in another audio with some little changes for successful implementation.
2. This system supports three file formats '.aiff' for MAC OS, '.wav' for windows and '.AU' for Unix.
3. As compared to existing systems this system will provide user to increase text file up to 1000 character.
4. More often in today's security advancement, we sometime come across certain cases in which combination of cryptography and steganography are used to achieve data.

VI. CONCLUSION

This ew GA approach is proposed to resolve problem of substitution technique for audio steganography. Problem is having less robustness against attacks which try to expose the hidden data. An intelligent algorithm will try to embed the message bits in the deeper layers of samples and other bits will be altered to decrease the error. Using this proposed

GA, message bits could be embedded into multiple and deeper layers to achieve higher capacity and robustness.

In this paper, we concentrate on the method of data hiding such way that observer would not suspect it is there at all. Again if someone knows that data is in the audio it is very difficult to extract data from the host audio.

VII. ACKNOWLEDGMENT

This work is part of academic project of last year computer engineering under the University of Pune. Our thanks to project guide and other professors for their valuable suggestion and support.

VIII. REFERENCES

[1] Krishna Bhowal, Anindya Jyoti Pal, Geetam S. Tomar, P.P.Sarkar, “*Audio Steganography using GA*”,2010 International Conference on Computational Intelligence and Communication Network

[2] Nedeijko Cvejic, “ALGORITHMS FOR AUDIO WATERMARKING AND STEGANOGRAPHY” *Oulu University Library OAI repository test (finland)* publication year 2004

[3] Zamani M., Manaf A. A., Ahmad R.B., Zeki A. M. and Abdullah S., “A Genetic-Algorithm-Based Approach for Audio Steganography”, World Academy of Science, Engineering and Technology 54, 2009

[4] Cvejic N. and Seppnen T.”Increasing the Capacity of LSB Based Audio Steganography”, Proc. 5th IEEE International Workshop on Multimedia Signal Processing , St. Thomas,Dec 2002, pp. 336-338

[5] Lee.Y.K. And Chen L.H. “High Capacity Image Steganographic Model”, IEEE proceedings vision, Image And Signal Processing, 2000, 288-294.

[6] Westfeld A. And Pitzzmann A.,”Attack on Steganographic System”,Lecture Notes in Computer Science, Springer –Verlag, Berlin 2000,pp. 61-75.

[7] Sridevi R, Damodaram A, Narasimham SVL, “Efficient method of audio steganography by modified LSB algorithm and strong encryption key with enhanced security” Journal of Theoretical and Applied Information Technology © 2005 - 2009 JATIT.

[8] petitcolas, R.J. Anderson, and M.G. Kuhn, “Information Hiding—A Survey,” *Proc. IEEE*, 1999, pp. 1062–1078

[9] Cvejic N. Seppanen, T., “Increasing robustness of LSB audio steganography using a novel embedding method” Oulu Group, Oulu Univ., Finland.

[10] Bassia P. et al., “Robust audio watermarking in the time domain,” IEEE. Trans. Multimedia, 2001, pp. 232–241.

[11] “MP3STEGO: HIDING TEXT IN MP3 FILES” *The SANS Institute InfoSec Reading Room*.

[12] C. Parthasarathy and Dr. S.K.Srivatsa, **“**INCREASED ROBUSTNESS OF LSB AUDIO STEGANOGRAPHY BY REDUCED DISTORTION LSB CODING**”** *Journal of Theoretical and Applied Information Technology*.

AUTHOR’S PROFILE

Miss. Bankar Priyanka R, BE Computer, SNJB’s Late. Sau. KBJ COE, Chandwad, Nasik.
Priyabankar555@gmail.com

Mr. Katariya Vrushabh R, BE Computer, SNJB’s Late. Sau. KBJ COE, Chandwad, Nasik.
Vrushabh43@gmail.com

Miss. Patil Komal K, BE Computer, SNJB’s Late. Sau. KBJ COE, Chandwad, Nasik.
Komal.shinde31@gmail.com

Mr. Pingle Shashikant M, BE Computer, SNJB’s Late. Sau. KBJ COE, Chandwad, Nasik.
Shashi.pingle@yahoo.co.in

Prof. Sanghavi Mahesh R. (ME CSE), Asst Prof, Head In Dept Of Computer Engineering, SNJB’s Late. Sau. KBJ COE, Chandwad, Nasik.
2nd University Ranker in ME-CSE.
Sanghavi.mahesh@gmail.com