ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 9, March 2013

Enhanced Data Hiding Model in Audio to Ensure Secrecy

Navnath S. Narwade, Vikas Bhagasara, Mahesh Kanthali, Rushikesh Pailwar

Abstract: ***Data hiding was done using plain text, still images, video and IP datagram for a long period time. Recently audio steganography is area of focus. This paper presents a novel method of secret data to be hidden in audio using cryptography and steganography combined together. The security of this method is enhanced by using of an encryption method prior to the data embedding step. First data is mathematically encrypted, then RSA encryption is applied on it. Resultant data is embedded in audio. The perceptual quality of the host audio signal was not to be degraded while embedding. The proposed method supports different formats of wav audio such as 16 bit and 8 bit .wav audio, mono and stereo .wav audio irrespective of its sampling frequency22 kHz or 44 kHz. The entire proposed model was simulated and experimental results show that proposed method has high imperceptibility, large payload, high audio quality and full recovery.***

Keywords: **Steganography, Cryptographers algorithm, Cover object, Covert data, Stego-object, Embed, Extraction, LSB, Wav audio.**

I. INTRODUCTION

Steganography is a powerful tool which increases security in data transferring and archiving [4, 5, 11]. In the steganography scenario the covert 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. It causes the existence of the covert data and even its transmission become hidden [4,5]. Steganography is often confused with cryptography because the two are similar in the way that they both are used to protect confidential information. The difference between the two is in the appearance in the processed output; the output of steganography operation is not apparently visible but in cryptography the output is scrambled so that it can draw attention [8]. Steganalysis is process to detect of presence of steganography [11]. A steganographic method of embedding textual information in an audio file is presented in this paper. In the proposed technique, first the audio file is sampled and then an appropriate bit of each alternate sample is altered to embed the textual information. ETAS model - Embedding Text in Audio Signal that embeds the text like the existing system but with encryption that gains the full advantages of cryptography. In this method for digital audio steganography where data is encrypted using DES (Data Encryption Standard) algorithm and embedded into the host audio signal using LSB algorithm [3]. Today's large demand of internet applications requires data to be transmitted in a secure manner so audio steganography is the scheme of hiding the existence of secret information by concealing it into another medium such as audio file [5]. For a digital data hiding system to be effective and practical, it should exhibit the following characteristics [1].

1) Imperceptibility: Embedding this extra data must not degrade human perception about the object. Namely, the covert data should be ''inaudible'' in stego digital music. Evaluation of imperceptibility is usually based on an objective measure of quality, called signal-to-noise ratio (SNR), or a subjective test with specified procedures.

2) Security: The data hiding procedure should rely on secret keys, not the algorithm's secrecy, to ensure security, so that pirates cannot detect or remove secure data by statistical analysis from a set of audio signals. The algorithm should be published and an unauthorized user, who may even know the exact data hiding algorithm, cannot detect the presence of hidden data, unless he/she has access to the secret keys that control this data-embedding procedure.

3) Data Payload: The data payload refers to the number of bits that are embedded into original audio within a unit of time. It is measured by bps (bit per second). The objective of a steganographic algorithm is to increase payload as much as possible.

4) Real-time processing: Covert data should be rapidly embedded into the host signals without much delay, so that integrated streaming/data hiding functionality in the delivery of audio over a network can be enabled. Also, a web crawler should support fast data extraction/detection.

II. MATHEMATICAL ANALYSIS OF RSA MODEL

RSA is the most widely used public key algorithm. It is named after its creators-Rivest,Shamir and Adleman.RSA principle is simple that it is easy to multiply two prime numbers but it is very difficult to factor the product and get them back.

RSAAlgorithm is as follows:-

1. Take two very large prime no.A & B of equal length and obtain their product (N)

   $$N = A*B$$

2. Subtract 1 from A as well as B and take product (T)

   $$T = (A-1)\,(B-1)$$

3. Choose the public key (E) which is a randomly chosen no. such that it has no common factor with T.

4. Obtain the private key(D) as follows

   $$D = E^{-1} \bmod T$$

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 9, March 2013

5. The rule for encryption of a block of message M into cipher text(C) is as follows:

$$C=M^E \bmod N$$

6. Message M is raised to power of E (public key) & then divided by N. Remainder of this division is sent as cipher text C.

7. Received message C at the receiver is decrypted as follows:

$$M =C^D \bmod N$$

III. PROPOSED MODEL

In proposed model, the message is first encrypted and then embedded in the carrier. Embedding of encrypted data is done in every alternate byte's lower nibble of audio carrier. The system has following four steps:

1. Encryption
2. Embedding
3. Extraction
4. Decryption

1. Encryption: First Mathematical encryption and then RSA encryption algorithm is used to enhance the security further.
2. Embedding: The process of hiding the message in the audio file. Lower nibble of each alternate sample of audio file is embedded by encrypted message bits.

Figure 1 shows total encryption and embedding block diagram. In encryption part mathematical and RSA encryption method is used. In embedding part lower nibble of each alternate sample of data part is embedded.

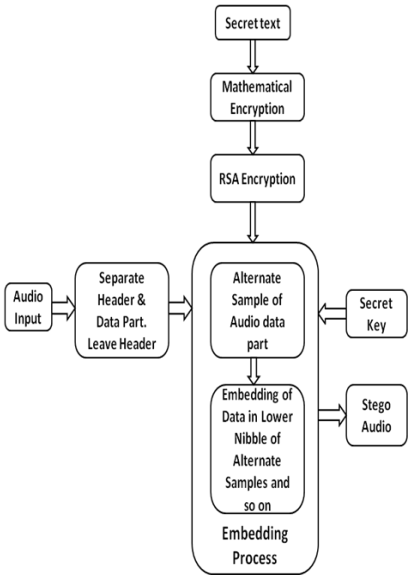

Fig 1.Block Diagram of Encryption & Embedding

3. Extraction: is a process of retrieving the message from the lower nibble bits of alternate sample of audio file are taken in one queue.
4. Decryption: Decryption is simply the inverse of encryption, RSA decryption and mathematical decryption done on extracted bits in queue.

Figure 2 shows total extraction and decryption block diagram. In extraction part lower nibble of each alternate sample of data part is extract in one queue and decryption done on it. In decryption part RSA and mathematical decryption method is used.

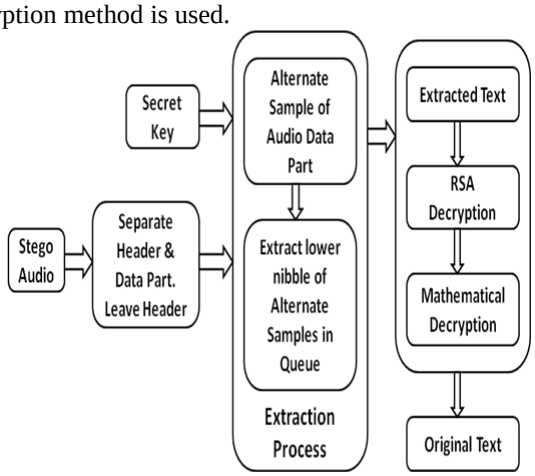

Fig 2. Block Diagram of Extraction & Decryption

IV. ALGORITHM

Multiple bits of each sample of the file have been modified to insert text data in it. The degradation of the host audio file after modification of the bits has also been observed. But after going through all the modification it has been observed that lower nibble (4bit of LSB) change gave result as per Human Auditory System requirement. The human auditory system (HAS) perceives sounds over a range of power greater than 10^9:1 and a range of frequencies greater than 10^3:1[1].Thus, data can be embedded according to the following algorithm.

A. Algorithm* (For Encrypt-Embed of Data*):

- Separate the header section and data section of the audio file. Leave header part.
- Data section is used for embedding. Start from a suitable position of the data bytes. (The present start byte was 51st sample for our experimental results).
- Apply mathematical encryption on secret message
- Apply RSA encryption on output of mathematical encryption.
- Edit the lower nibble with the data which is output of RSA encryption have to be embedded by embedding secret key.
- Modify the lower nibble of every alternate sample henceforth to embed the RSA encrypted output.

***B.* Algorithm (For Extract-Decrypt of Data):**

The data retrieving algorithm at the receiver's end follows the same logic as the embedding algorithm.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 9, March 2013

- Separate the header section and data section of the audio file. Leave first 50 bytes.
- Start extraction from the 51st byte and store the lower nibble in a queue by using extraction secret key.
- Check every alternate sample and store the lower nibble in the previous queue with a left shift of the previous bit.
- Convert the binary values to decimal to get the ASCII values of the secret message.
- Take extracted text from ASCII value.
- Apply RSA decryption on extracted text.
- Apply Mathematical decryption on RSA decrypted output and original secret message is recovered.

V.EXPERIMENTALRESULTS& VALIDATION

An audio file with ".wav" extension has been selected as cover file. Modification of bits should not degrade sound quality. WAV files have two basic parts, the header and the data. The header is situated in the first 44 bytes of the wav file. Except the first 44 bytes, the rest of the bytes of the file are all about the data. No change can be done in header section because a minimal change in the header section leads to a corrupted audio file. Data section is used for embedding. Start from a suitable position 51st sample of the data bytes. The Lower nibble value of the 51st sample should be modified. If the binary value of the corresponding sample is "01110100" then lower nibble should be modified. Suppose Original message is"Prithvi Missile". Suppose 1stRSA encrypted value is"A", the sender has to embed its ASCII "01000001" in 51st and 53th sample as shown in Table I.

Table I: Samples of Audio File with Binary Values Before and After Embedding

Sample No.	Binary values of corresponding sample	RSA encrypt value to be embedded	Binary values after modification
51	01110100	0100	01110100
53	01011110	0001	01010001

When it comes to the point of data retrieving at the receiver's end, the retrieving algorithm has to be followed:
First, change the audio message into binary format that has come from the source as stego-object. Leave first 50 bytes with no change in them. Start from 51st bit, Take the lower nibble, and store it in a queue. Check every alternate sample to collect the whole data embedded. Like 53rd, 55th and 57th and so on. Store the lower nibble of the alternate samples in the queue with left shift of previous bit. Convert the binary values to decimal to get back the ASCII from which the message can be retrieved by using RSA decryption and Mathematical decryption. The whole retrieval process can be depicted with the following Table II more thoroughly:

Table II: Extraction of data from audio File

Sample No.	Binary values with embedded secret data	Bits that are stored in the queue
51	01110100	0100
53	01010001	01000001

Figure 3 shows graph of original audio which is used as host file. Figure 4 shows graph of audio after embedding and figure 5 shows graph of recovered audio after extraction. Graph of original audio, embedded audio and recovered audio is nearly same. These graphs are plotted Sample Numbers versus amplitude. The simulation was carried out in MATLAB R2008a software.
Table III shows Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR) of embedded and recovered audio obtained during simulation. Following wav audio formats were selected for experiments.
1)8-bit wav audio
2)16-bit wav audio
3)22 kHz sampling frequency wav audio
4)44 kHz sampling frequency wav audio
5) Mono wav audio
6) Stereo wav audio
It is clear from the Table III that stereo audio can embed more data than mono audio. Recovered audio have less PSNR than embedded audio.

Table III: Validation Parameter of audios

Audio	Parameter	8-bit	16-bit	22khz 16-bit	44khz 16-bit	Mono 16-bit	Stereo 16-bit
Embedded	MSE	5.81914e-006	5.88369e-006	1.16372e-005	5.88369e-006	4.56073e-005	5.88369e-006
	PSNR(dB)	52.3514	52.3035	49.3415	52.3035	43.4097	52.3035
Recovered	MSE	1.50557e-005	1.50597e-005	3.16717e-005	1.50597e-005	8.45737e-005	1.50597e-005
	PSNR(dB)	48.223	48.2218	44.9933	48.2218	40.7276	48.2218

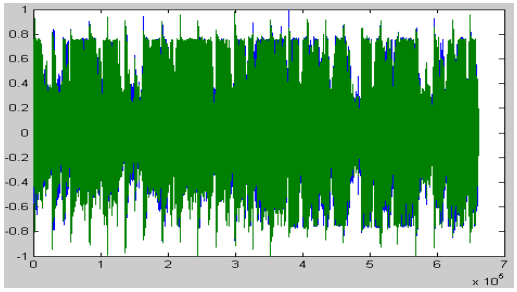

Fig 3.Original Audio

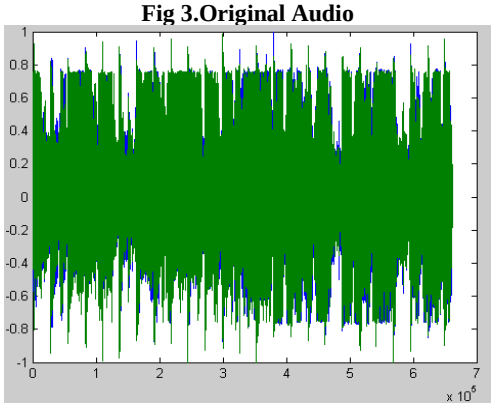

Fig4. Embedded Audio

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 9, March 2013

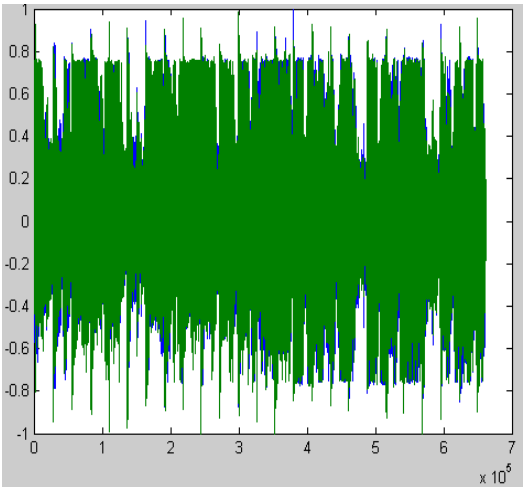

Fig 5. Recovered Audio

Fig 6 Is Original Message and Figure 7 Is Recovered Message. These Two Messages Are 100% Similar.

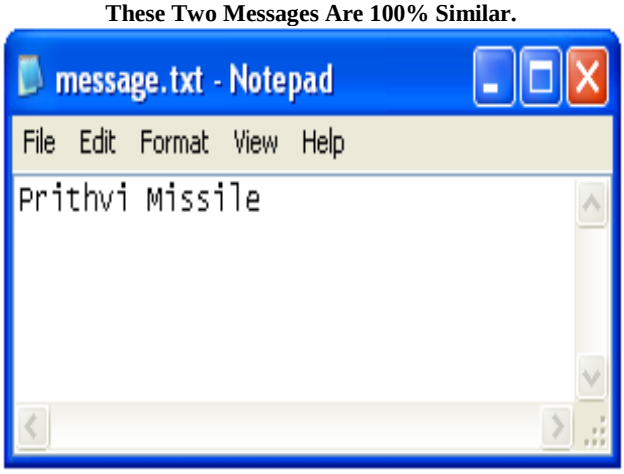

Fig 6.Original text message

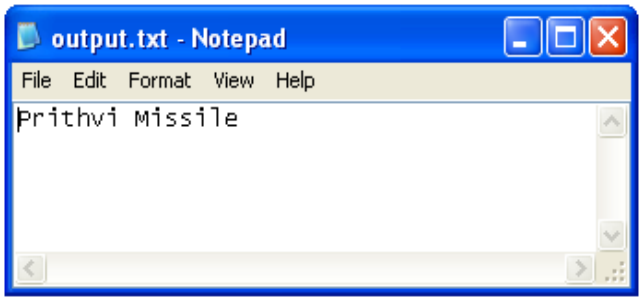

Fig7. Recovered message

VI. CONCLUSION

In this paper we have introduced a good, efficient &robust method of imperceptible audio data hiding. The wav audio can be of either 8 bit or 16 bit, either mono or stereo, either of 22 kHz or44 kHz sampling frequency. This proposed system will not change the size of the file even after encoding. Thus we conclude that audio data hiding techniques can be used for a number of purposes other than covert communication or deniable data storage, information tracing and finger printing, tamper detection. 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 corporate world. This work is more suitable for automatic control of robotic systems used in military and defense applications that can listen to a radio signal and then act accordingly as per the instructions received. By embedding the secret password in the audio signal the robot can be activated only if the predefined password matches with the incoming password that reaches the robot through audio signal. It can then start functioning as per the instructions received in the form of audio signal.

VII.FUTURE SCOPE

There are a number of ways that this project can be extended. Its performance can be upgraded to higher levels by using a better algorithm for encoding and decoding. The future work on this project will be to improve the compression ratio of the audio to the text. This project can be extended to a level such that it can be used for the different types of audio formats like .mp3, .mp4, etc., in the future.

REFERENCES

[1] Basu, P. N.; Bhowmik T., "On Embedding of Text in Audio– A case of Steganography", International Conference on Recent Trends in Information, Telecommunication and Computing, 2010.

[2] Poulami Dutta, Debnath Bhattacharyya and Tai-hoon Kim,"Data Hiding in Audio Signal: A Review",International Journal of Database Theory and Application Vol. 2, No. 2, June 2009.

[3] Zameer Fatima and Tarun Khanna , "Audio Steganography Using DES Algorithm", Proceedings of the 5th National Conference: Computing For Nation Development, March 10 – 11, 2011 Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi ISSN 0973-7529 ISBN 978-93-80544-00-7.

[4] K.P.Adhiya & Swati A. Patil, -"Hiding Text in Audio Using LSB Based Steganography", Information and Knowledge Management www.iiste.orgISSN 2224-5758 (Paper) ISSN 2224-896X (Online) Vol 2, No.3, 2012.

[5] Jayaram, Ranganatha, Anupama, -"Information Hiding Using Audio Steganography – A Survey", The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011.

[6] Bandyopadhay S. K.; Datta B.; Dutta K., "Information Hiding in Higher LSB Layer in an Audio Image", International Journal of Advanced Research in Computer Science, Vol. 2, No. 3, 2011.

[7] William Stalings,"Cryptography and Network Security", Prentice Hall of India Private Limited, New Delhi.

[8] K.Sakthisudhan, P.Prabhu and P.Thangaraj"Secure Audio Steganography for Hiding SecretInformation"ICON3C 2012,Proceedings published in International Journal of Computer Applications® (IJCA).

[9] Samir Kumar Bandyopadhyay and Biswajita Datta "Higher LSB Layer Based Audio Steganography Technique" IJECT Vol. 2, Issue 4, OCT. - DEC. 2011 ISSN: 2230-7109 (Online) | ISSN: 2230-9543.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 9, March 2013

[10] Swati Malviya, Manish Saxena and Dr. Anubhuti Khare "Audio Steganography by Different Methods", International Journal of Emerging Technology and Advanced Engineering , www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 7, July 2012).

[11] Robert Krenn, "Steganography and Steganalysis," An article, January 2004. http://www.krenn.nl/univ/cry/steg/article.pdf

[12] http://en.wikipedia.org/wiki/Steganography.

AUTHORS

Mr. Navnath S. Narawade is a research scholar at Electronics and Telecommunication Engg department at Sant Gadgebaba Amravati University, Amravati. He received the M.E(Electronics and Telecommunication Engg) in 2005 from Govt. College of Engg, Pune under University of Pune, B.E.(Electronics) from Walchand College of Engg, Sangli under Shivaji University ,Kolhapur. His research interests are focused on image and signal processing, particularly in robust reversible watermarking.

Mr.Vikas Bhagasara is UG Engg. Studentin Final Year BE (Electronic & Telecommunication). He is doing research on Digital Image processing and Embedded Design in Marathwada Mitra Mandal'sInstitute of Technology, Pune.

Mr. Mahesh Kanthali is UG Engg. Studentin Final Year BE (Electronic & Telecommunication). He is doing research on Digital Image processing and Embedded Design In Marathwada Mitra Mandal's Institute of Technology, Pune.

Mr.Rushikesh Pailwar is UG Engg. Student in Final Year BE (Electronic & Telecommunication). He is doing research on Digital Image processing and Embedded Design in Marathwada Mitra Mandal's Institute of Technology, Pune.