Audio Steganography using RPrime RSA and GA Based LSB Algorithm to Enhance Security

Juhi Saurabh[1], Asha Ambhaikar [2]

[1]Rungta College of Engineering and Technology
Kohka Kurud Road, Bhilai
juhi.saurabh@gmail.com

[2]Rungta College of Engineering and Technology
Kohka Kurud Road, Bhilai
asha31.a@rediffmail.com

Abstract: ***Audio Steganography is a technique used to transmit hidden information by modifying an audio signal in an imperceptible manner. It is a method that ensures secured data transfer between parties normally in internet community [2]. Here we present a novel approach for resolving the problems related to the substitution technique of audio steganography. In the first level of security, we use an improved RSA encryption algorithm (RPrime RSA) to encrypt message, which is very complex to break. In the next level, the encrypted message is to be encoded into audio data for this we use a more powerful GA (Genetic Algorithm) based Least Significant Bit) Algorithm. In order to increase the robustness against intentional attacks in which the hackers always try to reveal the hidden message as well as some unintentional attacks such as noise addition, the encrypted message bits are embedded into random LSB layers. Here in order to reduce distortion, GA operators are used. The basic idea behind this paper is maintained randomness in message bit insertion into audio data for hiding the data from hackers and to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safer manner [5].***

Keywords: Audio Steganography, LSB, GA, HAS, HVS, RSA.

1. Introduction

Steganography is the art and science to hide data in a cover media such as text, audio, image, video, etc [7]. The term steganography in Greek literally means, “Covered Writing” [15]. Steganography is the main part of the fast developing area of information hiding [14]. Steganography provides techniques for hiding the existence of a secondary message in the presence of a primary message. The primary message is referred to as the carrier signal or carrier message, the carrier signal can be text, audio, image, video, etc.; the secondary message is referred to as the payload signal or payload message [1]. The message is being hidden in such a way that the existence of secondary message is unknown to the observer and the carrier signal is modified in an imperceptible manner [13].

There are various different steganographic methods for hiding the secret message. The fundamental requirement for a steganographic method is imperceptibility which means that the secret messages should not be discernible to the human eye. There are two other requirements, one is to maximize the embedding capacity, and the other is security [8]. Among different Steganography types, one technique is using audio files as stego-media. In a computer-based audio steganography system, digital sound is used for hiding secret message. By slightly altering the binary sequence of a sound file the secret message is embedded into the audio signal [3].

In the past few years, several algorithms have been presented for the embedding and extraction of message in audio sequences. All of the developed algorithms take advantage of the perceptual properties of the human auditory system (HAS) in order to add a message into a host signal in a perceptually transparent manner. Hiding additional information into audio sequences is a more tedious task than that of images [1], as Human Auditory System (HAS) is more sensitive than Human Visual System (HVS).

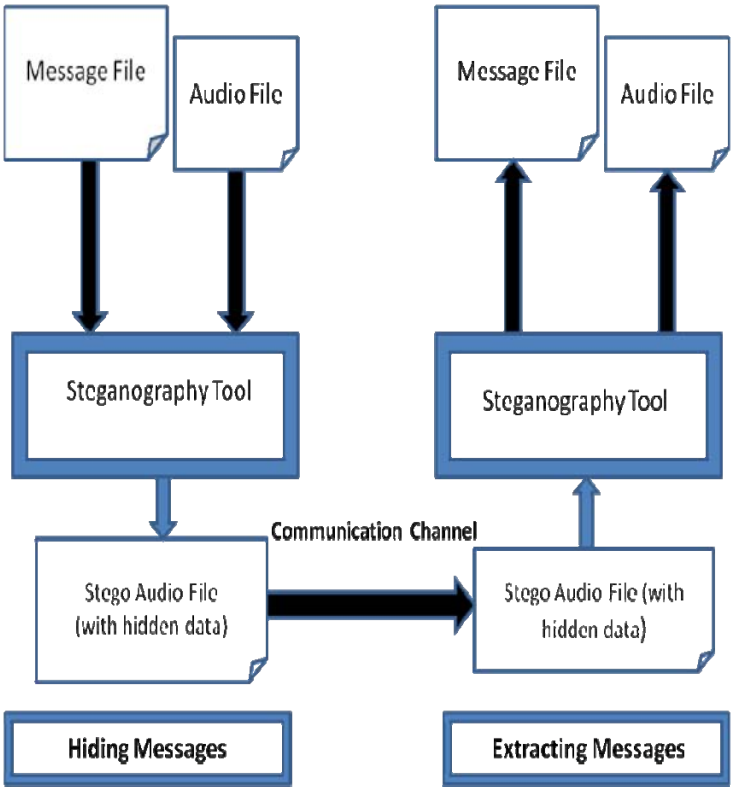

Figure 1: AUDIO STEGANOGRAPHY PROCESS

The methods proposed in this paper combine the techniques of audio steganography and cryptography, in order to make the message more secure. In this paper, cover medium is an audio and the secret message used is text. In all application scenarios mentioned above, multimedia steganography techniques have to satisfy two basic requirements. The first requirement is perceptual transparency, i.e. cover object

(object not containing any additional data) and stego object (object containing secret message) must be perceptually imperceptible. The second constraint is high data rate of the embedded data. All the stego-applications, besides requiring a high bit rate of the embedded data, have need of algorithms that detect and decode hidden bits without access to the original multimedia sequence [6].
In this paper we take a text file as a text message, using RPrime RSA encryption algorithm encrypt the text message and store the encrypted text message into another file "encrypt.txt". Now read the audio .wav file byte wise, and convert the encrypted text file into byte. Then applying proposed LSB algorithm, embed message bits to the audio bit steam in random positions (to increase the robustness) to get the stego-audio, here Genetic Algorithm operators are used to minimize the bit level deviation occurred between host audio and stego-audio. Now to get the original message apply reverse LSB method and RPrime RSA decryption process on stego-audio.

2. Related Work

Different methods are already used to hide message into audio file, i.e., in Audio Steganography. Initially, simple LSB, then modified LSB method were used [2]. Some of the authors tried to increase the LSB layer to increase the robustness against attack. It always increases the distortion in host audio.
In this paper we initially encrypt the message using asymmetric algorithm (RPrime RSA) and then encrypted message bits are inserted at random higher LSB layer position of the host audio. This helps in increasing the robustness.

3. Methodology

In this paper, first, we encrypt text message using RPrime RSA encryption algorithm. And then applying proposed LSB algorithm, embed message bits to the audio bit stream (16 bit sample) in random and higher LSB layer positions (increase the robustness) to get a collection of chromosomes. Now Genetic Algorithm operators are used to get the next generation chromosomes. Next select the best chromosome according to the best fitness value. Fitness value is a value of LSB position for which we get a chromosome with the minimum deviation comparing to the original host audio sample. Here higher LSB layer is given higher preference in case of layer selection. 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 [2].
In this paper, an intelligent algorithm is used to embed the message bits in the deeper layers of samples and alter other bits to decrease the error and if alteration is not possible for any sample it will ignore them, which helps in achieving higher capacity which refers to the amount of information that a data hiding scheme can successfully embed without introducing perceptual distortion in the marked media and robustness which measures the ability of embedded data or watermark to withstand against intentional and unintentional attacks [9].

3.1 GENETIC ALGORITHM APPROACH

In the genetic algorithms, the parameters are represented by an encoded binary string, called the "chromosome". And the elements in the binary strings, or the "genes", are adjusted to minimize or maximize the fitness value. The fitness function generates the fitness value of chromosomes, which is composed of multiple variables to be optimized by GA operators and also helps in calculating error [10].
There are four main steps in this algorithm:-

a. Alteration

The first step is alteration. The alteration step in the genetic algorithm refines the good solution from the current generation to produce the next generation of candidate solutions. In this step, the message bits are replaced with the target bits of samples. Target bits are those bits which are placed at the layer that we want to alter. This is done by a simple substitution that does not need adjustability of result be measured [4].

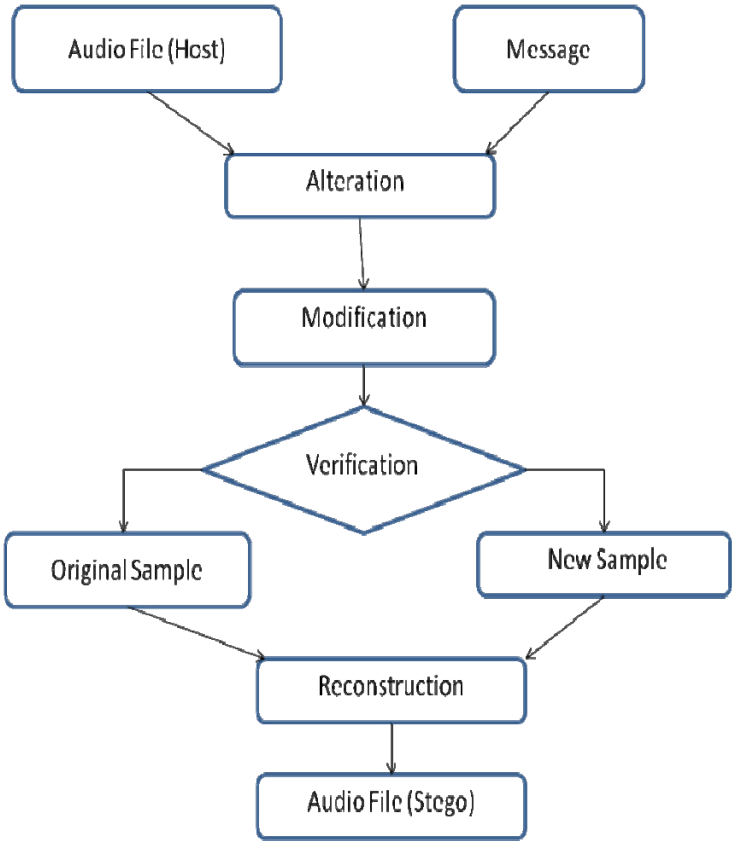

Figure 2: Genetic Approach Diagram

b. Modification

This step is the most important and essential part of algorithm. All results and achievements that we expect are depending on this step. In this stage two different efficient and intelligent algorithms will be used that will try to decrease the amount of error and improve the transparency. Transparency evaluates the audible distortion due to signal modifications like message embedding or attacking. One of them is a simple and ordinary technique, but in aspect of perspicacity will be more efficient to modify the bits of samples better. Since transparency is simply the difference

between original sample and modified sample, hence by using a more intelligent algorithm, more bits and samples are modified and adjusted as compared to the previous algorithms. If the used algorithm is able to decrease the difference of them, transparency will be improved.
Another one is a Genetic Algorithm in which the sample is like a *chromosome* and each bit of sample is like a *gene*. First *generation* or first *parents* consist of original sample and altered sample. *Fitness* may be determined by a function which calculates the error. The most transparent sample pattern should be measured fittest. It must be considered that in *crossover* and *mutation* the place of target bit should not be changed [11]. **Crossover** may be regarded as artificial mating in which chromosomes from two individuals are combined to create the chromosome for the next generation. It is also called recombination. Crossover only rearranges existing characteristics to give new combinations. **Mutation** is a random adjustment in the genetic composition.

c. Verification
In fact this stage is quality controller. What the algorithm could do has been done, and now the outcome must be verified. If the difference between original sample and new sample is acceptable and reasonable, the new sample will be accepted; otherwise it will be rejected and original sample will be used in reconstructing the new audio file instead of that [4].

d. Reconstruction
The last step is the creation of new audio file (stego file). This is done sample by sample. There are two states at the input of this step. Either modified sample is input or the original sample that is the same with host audio file. It is why we can say that the algorithm does not alter all samples or predictable samples. That means depending on the status of samples (Environment) and the decision of intelligent algorithm; which sample will be used and modified is decided [12].

4. Expected Outcome

Proposed Audio Steganography algorithm will be used for five audio sequences from different music styles (classical, pop, jazz, techno, rock). All music pieces will be watermarked using the proposed and GA based LSB watermarking algorithm.
The hackers will not be able to discriminate the two audio clips (original audio sequence and watermarked audio signal). Results of subjective tests will show that if the proposed algorithm is used for embedding then the perceptual quality of watermarked audio will be higher in comparison to standard LSB embedding method. This will confirm that the described algorithm has succeeded in increasing the depth of the embedding layer and also in randomizing the bit layer without affecting the perceptual transparency of the watermarked audio signal.
Therefore, there will be a significant improvement in robustness against signal processing manipulation, as the hidden bits can be embedded higher LSB layers deeper than in the standard LSB method.

5. Advantages of our approach

• The used algorithm succeeds in not only increasing the depth of the embedding layer but also layer is chosen randomly without affecting the perceptual transparency of the stego audio signal.
• Since optimization is done using Genetic Algorithm operators, there is message bit embedding that causes minimal embedding distortion of the host audio.
• There is a two-way robustness (to know the actual position of the message bit) are there, First, insertion positions are randomly chosen, Second, LSB layer are most of the time is high layer.
• Listening tests showed that in case of proposed method the perceptual quality of watermarked audio is higher than in case of the standard LSB method.
• Since there is a significant number of bits flipped in a number in bit layers and the adversary cannot identify exactly which bit layer is used for the data hiding, hence the steganalysis of the proposed algorithm is more challenging.
• The proposed algorithm obtains significantly lower bit error rates as compared to the standard algorithm.

6. Conclusion and Future Work

In this paper, an intelligent algorithm is used that will try to embed the message bits in the deeper layers of samples and alter other bits to decrease the error and if alteration is not possible for any samples it will ignore them. To achieve higher capacity and robustness, the message bits are embedded into multiple, vague and deeper layers by using the proposed genetic algorithm [11]. By using this method of data hiding the observer will not be able to suspect that the data is there at all. Again, if someone knows that data is in the audio, it is very difficult to extract the data from the host audio. The key idea of the algorithm is random and higher LSB layer bit embedding keeping minimal embedding distortion of the host audio. Listening tests showed that described algorithm succeeds in increasing the depth of the embedding layer from lower to higher random LSB layers without affecting the perceptual transparency of the stego audio signal. Since the proposed algorithm obtains significantly lower bit error rates as compared to the standard algorithm, hence the improvement in robustness in presence of additive noise is obvious. Our work can be further extended to a new level where one can use the proposed algorithm for hiding image.

References

1. Zamani, M., Manaf, A.A., Ahmad, R.B., Zeki, A.M., & Abdullah, S. (2009) A genetic-algorithm-based approach for audio steganography. World Academy of Science, Engineering and Technology, 54.

2. Krishna Bhowal, Anindya Jyoti Pal, Geetam S. Tomar, P. P. Sarkar, “Audio Steganography using GA”, IEEE Proceedings, 2010.

3. Krishna Bhowal, Debnath Bhattacharyya, Anindya Jyoti Pal, Tai-Hoon Kim, “A GA based audio steganography with enhanced security”, Springer Science, Business Media, LLC 2011.

4. Mazdak Zamani, Hamed Taherdoost, Azizah A. Manaf, Rabiah B. Ahmad, and Akram M. Zeki, “Robust Audio Steganography via Genetic Algorithm”, IEEE, 2009.

5. Sridevi, R., Damodaram, A., & Narasimham, S. V. L. 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.

6. Cvejic N. and Seppänen T. ”Increasing the capacity of LSB based audio steganography”, Proc. 5th IEEE International Workshop on Multimedia Signal Processing, St. Thomas, VI, December 2002, pp. 336-338.

7. Elham Ghasemi, Jamshid Shanbehzadeh, Nima Fassihi, “High Capacity Image Steganography usingWavelet Transform and Genetic Algorithm”, Proceedings of the International MultiConference of Engineers and Computer Scientists Vol. 1, 2011.

8. Lee, Y. K., & Chen, L. H. (2000). High capacity image steganographic model. In IEEE proceedings vision, image and signal processing (pp. 288–294).

9. Pal S.K., Saxena P. K. and Mutto S.K. “The Future of Audio Steganography”. Pacific Rim Workshop on Digital Steganography, Japan, 2002.

10. C. S. Shieh, H. C. Huang, F. H. Wang and J. S. Pan, ‘Genetic Watermarking Based on Transform-Domain Techniques’, Pattern Recognition, vol. 37, no. 3, pp. 555-565, 2004.

11. Mazdak Zamani, Azizah Bt Abdul Manaf, Rabiah Bt Ahmad*3*, Farhang Jaryani, Hamed Taherdoost, Saman Shojae Chaeikar, and Hossein Rouhani Zeidanloo, “A Novel Approach for Genetic Audio Watermarking”, Journal of Information Assurance and Security 5, 2010,102-111.

12. Mazdak Zamani, Azizah Bt Abdul Manaf, Hossein Rouhani Zeidanloo and Saman Shojae Chaeikar, “Genetic substitution-based audio steganography for high capacity applications”, Int. J. Internet Technology and Secured Transactions, Vol. 3, No. 1, 2011,97-110.

13. Westfeld A. and Pitzmann A. "Attacks on Steganographic Systems". Lecture Notes in Computer Science, vol. 1768, Springer-Verlag, Berlin, pp. 61-75, 2000.

14. Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding—a survey. Proceedings of IEEE, 87(7), 1062–1078.

15. Fridrich, J. et al. (2000) ‘Steganalysis of LSB encoding in color images’, Proceedings of the IEEE International Conference on Multimedia and Expo, IEEE Press, New York, pp.1279–1282.

Juhi Saurabh: Received the B.E. degree in Computer Science Engineering from M.P. Christian College of Engineering and Technology, Bhilai, in 2008, and pursuing M.Tech. in Software Engineering from Rungta College of Engineering and Technology, Bhilai, in 2011. Her current research interest is in audio steganography using RPrime RSA and GA based LSB algorithm to enhance security.

Asha Ambhaikar: Received B.E from Nagpur University, Nagpur, India, in Electronics Engineering in the year 2000 and later did her M.Tech in Information Technology Allahabad Deemed University, India. Recently she has submitted her Ph.D. in C.S.V.T.U, Bhilai. Currently she is working as an Associate Professor in Rungta College of Engineering & Technology (Department of Computer Science and Engineering), Bhilai, India. She has published more than 20 research papers in reputed national and international journals & conferences. Her area of interest includes, Computer Networking, Data warehousing and mining, Cloud Computing, Image processing, Distributed system and Information systems and Security.