Audio Steganography using RSA Algorithm and Genetic based Substitution method to Enhance Security

Gaurav Singh,Kuldeep Tiwari,Shubhangi Singh

Abstract-Audio Steganography is a technique used to transmit hidden information by modifying an audio signal is an imperceptible manner.It is a method that ensures secured data transfer between parties normally in internet community.In this paper we present an approach for resolving the problem related to the substitution technique of audio steganography.In first level of security we use RSA algorithm to encrypt message,In the next level,encrypted message is to be encoded in to audio data for this we used genetic algorithm based substitution method.the basic idea behind this paper is to enhance the security and robustness.

Keywords-Audio steganography,genetic algorithm,Substitution method,RSA algorithm,HAS,HVS

1 Introduction

Steganography is the study of techniques for hiding the existence of a secondary message in the presence of aprimary message. The primary message is referred to asthe carrier signal or carrier message; the secondary message is referred to as the payload signal or payload message.Steganography itself offers mechanisms for providing confidentiality and deniability; it should be noted that both requirements can also be satisfied solely through cryptographic means [1]. Steganographic algorithms can be characterized by a number of defining properties. Three of them, which are most important for audio steganographic algorithms, are defined below.

Transparency evaluates the audible distortion due to signal modifications like message embedding or attacking. In most of the applications, the steganography algorithm has to insert additional data without affecting the perceptual quality of the audio host signal. The fidelity of the steganography algorithm is usually defined as a perceptual similarity between the original and stego audio sequence. However, the quality of the stego audio is usually degraded, either intentionally by an adversary or unintentionally in the transmission process, before a person perceives it. In that case, it is more adequate to define the fidelity of a steganography algorithm as a perceptual similarity between the stego audio and the original host audio at the point at which they are presented to a consumer.

In order to meet fidelity constraint of the embedded information, the perceptual distortion introduced due to embedding should be below the masking threshold estimated based on the HAS/HVS and the host media.[1]

Capacity of an information hiding scheme refers to the amount of information that a data hiding scheme can successfully embed without introducing perceptual distortion in the marked media. In the case of audio, it evaluates the amount of possible embedding information into the audio signal. The embedding capacity is the all included embedding capacity (not the payload) and can be measured in percent (%), bits per second or frame and bits per mega byte or kilo byte audio signal. In the other words, the bit rate of the message is the number of the embedded bits within a unit of time and is usually given in bits per second (bps). Some audio steganography applications, such as copy control, require the insertion of a serial number or author ID, with the average bit rate of up to 0.5 bps. For a broadcast monitoring watermark, the bit rate is higher, caused by the necessity of the embedding of an ID signature of a commercial within the first second at the start of the broadcast clip, with an average bit rate up to 15 bps. In some envisioned applications, e.g. hiding speech in audio or compressed audio stream in audio, algorithms have to be able to embed message with the bit rate that is a significant fraction of the host audio bit rate, up to 150 kbps [3].

Robustness measures the ability of embedded data or watermark to withstand against intentional and unintentional attacks. Unintentional attacks generally include common data manipulations such as lossy compression, digital-to-analog conversion, re-sampling, re-quantization, etc. whereas intentional attacks cover a broad range of media degradations which include addition white and colored noise, rescaling, rotation (for image and video steganography schemes), resizing, cropping, random chopping, and filtering attacks [2]. Also, the robustness of the algorithm is defined as an ability of the data detector to extract the embedded message after common signal processing manipulations. Applications usually require robustness in the presence of a predefined set of signal processing modifications, so that message can be reliably extracted at the detection side. For example, in radio broadcast monitoring, embedded message need only

to survive distortions caused by the transmission process, including dynamic compression and low pass filtering, because the data detection is done directly from the broadcast signal. On the other hand, in some algorithms robustness is completely undesirable and those algorithms are labeled fragile audio steganography algorithms [1].

II. WHY STILL SUBSTITUTION TECHNIQUES OF AUDIO STEGANOGRAPHY

The steganographic algorithms were primarily developedfor digital images and video sequences; interest and researchin audio steganography started slightly later. In the past fewyears, several algorithms for the embedding and extraction of message in audio sequences have been presented. All of the developed algorithms take advantage of the perceptual properties of the HAS in order to add a message into a host signal in a perceptually transparent manner. Embedding additional information into audio sequences is a more tedious task than that of images, due to dynamic supremacy of the HAS over human visual system.
On the other hand, many attacks that are malicious against image steganography algorithms (e.g. geometrical distortions, spatial scaling, etc.) cannot be implemented against audio steganography schemes. Consequently, embedding information into audio seems more secure due to less steganalysis techniques for attacking to audio. Furthermore, Natural sensitivity and difficulty of working on audio caused there are not algorithms and techniques as mush as exist for image. Therefore, regarding nowadays audio files are available anywhere, working on audio and improvement in related techniques is needed. The theory of substitution technique is that simply replacing either a bit or a few bits in each sample will not be noticeable to the human eye or ear depending on the type of file. This method has high embedding capacity (41,000 bps) but it is the least robust. It exploits the absolute threshold of hearing but is susceptible to attacks.
The obvious advantage of the substitution technique, the reason for choosing this technique, is a very high capacity for hiding a message; the use of only one LSB of the host audio
sample gives a capacity of 44.1 kbps. Obviously, the capacity of substitution techniques is not comparable with the capacity of other more robust techniques like spread spectrum
technique that is highly robust but has a negligible embedding capacity (4 bps) [4].

III. THE REMAINED PROBLEMS OF SUBSTITUTION TECHNIQUES OF AUDIO STEGANOGRAPHY

Like all multimedia data hiding techniques, audio steganography has to satisfy three basic requirements. They are perceptual transparency, capacity of hidden data and robustness. Noticeably, the main problem of audio substitution steganography algorithm is considerably low robustness. There are two types of attacks to steganography and therefore there are two type of robustness. One type of attacks tries to reveal the hidden message and another type tries to
destroy the hidden message. Substitution techniques are vulnerable against both types of attacks. The adversary who tries to reveal the hidden message must understand which bits are modified. Since substitution techniques usually modify the bits of lower layers in the samples - LSBs, it is easy to reveal the hidden message if the low transparency causes suspicious. Also, these attacks can be categorized in another way: Intentional attacks and unintentional attacks. Unintentional
attacks like transition distortions could destroy the hidden message if is embedded in the bits of lower layers in the samples -LSBs.
As a result, this paper briefly addresses following problems of substitution techniques of audio steganography:
1) Having low robustness against attacks which try to reveal the hidden message.
2) Having low robustness against distortions with high average power.

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 RSA algorithm 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 usingRSA encryption algorithm. And then applying proposed Substitution 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].

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

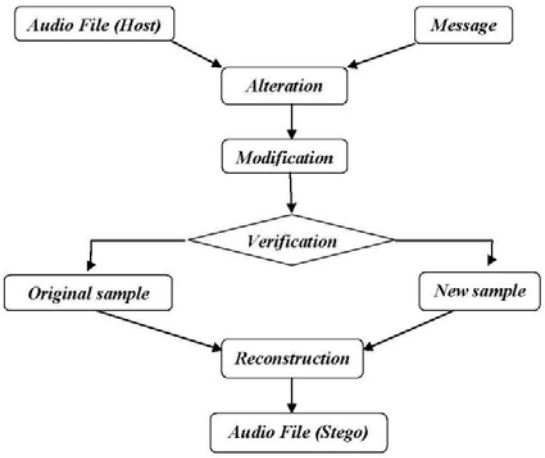
In fact this stage is quality controller. What the algorithm could do has been done, and now the outcome must be verified. If the difference between original sample and new sample is acceptable and reasonable, the new sample will be accepted; otherwise it will be rejected and original sample will be 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 Conclusion-A new approach is proposed to resolve two problems of substitution technique of audio steganography. First problem is having low robustness against attacks which try to reveal the hidden message and second one is having low robustness against distortions with high average power. An intelligent algorithm 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.
Using the proposed genetic algorithm, message bits could be embedded into multiple, vague and deeper layers to achieve higher capacity and robustness.

6 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 Ahmad3, 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 York, pp.1279–1282.

Author Details :

Gaurav Singh(1),Kuldeep Tiwari(2),Shubhangi Singh(3)

(1) Galgotia University,Greater Noida

Gauravsinghraghav0072@gmail.com

(2) Galgotia University,Greater Noida

Kuldeep22tiwari@gmail.com

(3) Galgotia University,Greater Noida

Shubhangi.singh1508@gmail.com