National Conference on Advances in Computer Science and
Applications with International Journal of Computer Applications (NCACSA 2012)
Proceedings published in International Journal of Computer Applications® (IJCA)

Enhanced Version of StegGen: an Optimized Steganographic Tool based on GA

Murugeswari Kandavel[1], Deisy C[1],Ganesan Govindan[2],and Suganthi J[3]
[1] Department of Computer Applications,Thiagarajar College of Engineering 625105,Madurai,India
[2]K.L.N. College of Information Technology,Madurai,Tamilnadu,India
[3]Hindustan College of Engineering and Technology,Coimbatore India

ABSTRACT

Steganography is the act of hiding a message inside another message in such a way that can only be detected by its intended recipient. Naturally, there are security agents who would like to fight these data hiding systems by steganalysis, i.e. discovering covered messages and rendering them useless. There is currently no steganography system which can resist all steganalysis attacks. In this paper we propose an optimal GA evolutionary process to make an optimized steganographic encoding on an audio file in addition to Bitmap images. Our steganography step is based on our tool StegGen, which is designed using LSB color cycle scheme for images and now it enhanced for audio steganography using substitution techniques.

Keywords

Genetic Algorithm, substitution Techniques, Steganography, StegGen.

1. INTRODUCTION

Internet users frequently need to store, send, or receive private information. The most common way to do this is to transform the data into a different form. The resulting data can be understood only by those who know how to return it to its original form. This method of protecting information is known as encryption. A major drawback to encryption is that the existence of data is not hidden. Data that has been encrypted, although unreadable, still exists as data. If given enough time, someone could eventually decrypt the data. A solution to this problem is steganography [1]. The ancient art of hiding messages so that they are not detectable. No substitution or permutation was used. The hidden message is plain, but unsuspecting to the reader. Steganography's intent is to hide the existence of the message, while cryptography scrambles a message so that it cannot be understood. Using genetic algorithms that are based on the mechanism of natural genetics and the theory of evolution, we can design a general method to guide the steganography process to the best position for data hiding.

2. AUDIO STEGANOGRAPHY

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 human auditory system/human visual system (HAS/HVS) and the host media.[2]

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 [3]. 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 [2].

3. STEGGEN DESIGN

StegGen is proposed by us, an image steganography which based on leat significant bit (LSB) insertion method. The LSB is the lowest order bit in a binary value. This is an important concept in computer data storage and programming that applies to the order in which data are organized, stored or transmitted [5]. Usually, three bits from each pixel can be stored to hide an image in the LSBs of each byte of a 24-bit image. Consequently, LSB requires that only half of the bits in an image be changed [6] when data can be hidden in least and second least significant bits and yet the resulting stego-image which will be displayed is indistinguishable to the cover image to the HVS[7].

Our tool initially designed for only image steganography,now it enhanced for audio steganography.For hiding in an image we choose LSB Color cycle insertion method, now audio steganography is designed using LSB substitution techniques.Our tool screen shot is shown in figure 1[11].For hiding message in an audio,the idea proposed by Zamani et.al.[12] is conceived.That idea is discussed in the following sections.

Fig. 1: Screenshot of StegGen

4. WHY SUBSTITUTION TECHNIQUES?

The steganographic algorithms were primarily developed for digital images and video sequences; interest and research in audio steganography started slightly later. In the past few years, 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 much 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) [8].

5. PROBLEMS OF SUBSTITUTION TECHNIQUES

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, two problems are addressed:

1) Having low robustness against attacks which try to reveal the hidden message.

2) Having low robustness against distortions with high average power.

A. First Problem

One type of robustness that is very critical for security is withstanding against the attacks which try to reveal or extract the hidden message. To improve this type of robustness, an intelligent algorithm is used.

Certain way to withstand against these attacks is making more difficult discovering which bits are modified. Thus, the algorithm may not change some sample due to their situations.This selecting will improve the security of the method and robustness of the technique, because if somebody tries to discover the embedded message, he has to apply a specific algorithm to read some bits of samples. But if modified samples are secret, nobody can discover the message. It is remarkable that if we achieve float target bits, it will be novel.

As we know in samples LSBs are more suspicious, thus embedding in the bits other than LSBs could be helpful to increase the robustness. Furthermore, discovering which samples are modified should be uncharted. To reach to the level of ambiguity, the algorithm will not use a predefined procedure to modify the samples but will decide, according to the environment, in this case the host file; as such it will modify indistinct samples of audio files, depending on their values and bits status. Thus, some of the samples which algorithm determines they are suitable for modifying will modify and other samples may not change. This ambiguity in selecting samples will thus increase security and robustness of the algorithm.

B. Second Problem

A significant improvement in robustness against unintentional attacks -for example signal processing manipulation- will be obtained if an embedded message is able to resist distortions with high average power. To achieve this robustness the message could embed in deeper layers. But, selecting the layer and bits for hosting is critical because the random selection of the samples used for embedding introduces low power additive white Gaussian noise (AWGN). It is well known from psychoacoustics literature [9] that the HAS is highly sensitive to the AWGN. This fact limits the number of bits that can be imperceptibly modified during message embedding [8]. Embedding the message bits in deeper layers absolutely Causes bigger error and it will decrease the quality of transparency. Thus, the algorithm which embeds the message bits in deeper layers should modify other bits intelligently to decrease the amount of this error and reserve the transparency. Predictably, substitution techniques try to modify the bits of samples in accordance with a directive that is defined in algorithm. The target bits are definite, and the amount of resultant noise is not controlled. Of course, there are some better techniques that try to adjust the amount of resultant noise in substitution techniques. These improved algorithms alter other bits else than target bit in sample to decrease the amount of resultant noise. A key idea of the improved algorithm is message bit embedding that causes minimal embedding distortion of the host audio. It is clear that, if only one of 16 bits in a sample is fixed and equal to the message bit, the other bits can be flipped in order to minimize the embedding error. For example, if the original sample value was 0…010002=810, and the message bit was zero is to be embedded into 4th LSB layer, instead of value 0…000002=010 that the standard algorithm would produce, the proposed algorithm produces a sample that has value 0…001112=72, which is far closer to the original one.

However, the extraction algorithm remains the same; it simply retrieves the message bit by reading the bit value from the predefined layer in the stego audio sample. In the areas where the original and message bit do not match, the standard coding method produces a constant error with 8-Quantization Steps (QS) amplitude [10].

The improved method introduces a smaller error during message embedding. If the 4th LSB layer is used, the absolute error value ranges from 1 to 4 QS, while the standard method in the same conditions causes a fixed absolute error of 8 QS. What would be improved is a level of intelligence in those substitution algorithms which try to adjust the sample bits after modifying the target bits. The basic idea of the algorithm is embedding that cause minimal embedding distortion of the host audio. What is clear as much as intelligence the alteration algorithms have, the amount of resultant noise could be improved. Because the total noise will be less, when we are able to alter and adjust more samples.

6. THE SOLUTION

Accordingly, there are two following solutions for mentioned problems:

1) *The solution for first problem:* Making more difficult discovering which bits are embedded by modifying the bits else than LSBs in samples, and selecting the samples to modify privately-not all samples.

2) *The solution for second problem:* Embedding the message bits in deeper layers and other bits alteration to decrease the amount of the error.

To integrate these two solutions, "embedding the message bits in deeper layers" that is a part of second solution also can satisfy "modifying the bits else than LSBs in samples" of second solution. In addition, when try to satisfy "other bits alteration to decrease the amount of the error" of second solution, if ignore the samples which are not adjustable, also "selecting not all samples" of first solution will be satisfied.

Thus, 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. It is clear that the main part of this scenario is bit alteration that it should be done by intelligent algorithms which use either genetic algorithms or a symbolic AI system.

7. GENETIC ALGORITHM APPROACH

As Figure 2 shows, there are four main steps in this algorithm that are explained below.

A. Alteration

At the first step, message bits substitute with the target bits of samples. Target bits are those bits which place at the layer that want to alter. This is done by a simple substitution that does not need adjustability of result be measured.

B. Modification

In fact this step is the most important and essential part of algorithm. All results and achievements are depending on this step. Efficient and intelligent algorithms are useful here. In this stage algorithm tries to decrease the amount of error and improve the transparency. For doing this stage, two different algorithms will be used. One of them that is more simple likes to ordinary techniques, 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, with a more intelligent algorithm, I will try to modify and adjust more bits and samples than some previous algorithms. If we can decrease the difference of them, transparency will be improved. There are two example of adjusting for expected intelligent algorithm below.

Sample bits are: 001**0**1111 = 47
Target layer is 5, and message bit is 1
Without adjusting: 001**1**1111 = 63 (difference is 16)
After adjusting: 001**1**0000 = 48 (difference will be 1 for 1 bit embedding)

Sample bits are: 001**00**111 = 39
Target layers are 4&5, and message bits are 11
Without adjusting: 001**11**111 = 63 (difference is 24)
After adjusting: 000**11**111 = 31 (difference will be 8 for 2 bits embedding)

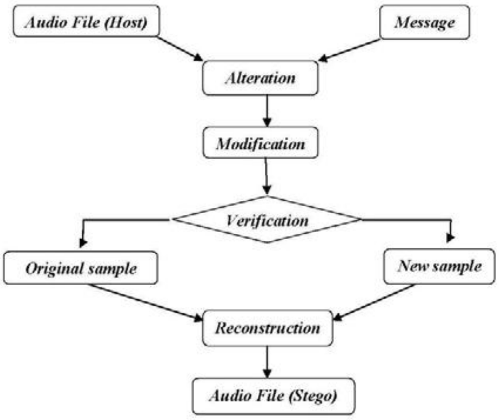

Fig. 2: Steps in the algorithm

Another one is a Genetic Algorithm 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 sampled. *Fitness* may be determined by a function which calculates the error. It is clear, 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.

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.

D. Reconstruction

The last step is new audio file (stego file) creation. 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 claim the algorithm does not alter all samples or predictable samples. That means whether which sample will be used and modified is depending on the status of samples (Environment) and the decision of intelligent algorithm.

8. CONCLUSION

Our idea is to develop an audio steganography tool, which is designed using LSB substitution technique. Even though substitution techniques are vulnerable, with the help of an innovative algorithm based on Genetic Algorithm, here we can achieve more transparency and robustness. Hence this algorithm is adopted and our tool StegGen is enhanced with audio steganography in addition to image steganography.

9. REFERENCES

[1] Sellars D.: An Introduction to Steganography, cs.uct.ac.za/courses/CS400W/NIS / papers99/ dsellars/stego.htm

[2] lMartín Alvaro, Sapiro Guillermo and Seroussi Gadiel : Is Image SteganographyNatural?,IEEE Transactions On Image Processing, Vol.14, No. 12, December, 2005.

[3] Cvejic N. and Seppänen T : Increasing the capacity of LSB based audiosteganography, Proc. 5th IEEE International Workshop on Multimedia Signal Processing, St. Thomas, VI, December 2002, pp. 336-338.

[4] Lee, Y. K. and Chen L. H. : High Capacity Image Steganographic Model, IEEEProceedings Vision, Image and Signal Processing, pp.288-294, 2000.

a. N. F. Johnson, S. Jajodia : Exploring Steganography: Seeing the Unseen, IEEE Computer, February 1998, pp.26-34.Julie K. Petersen : The Telecommunications Illustrated Dictionary, CRC Press, 2002,ISBN:084931173X

[5] Kefa Rabah, : Steganography – The Art of Hiding Data, Information Technology Journal 3 (3), 2004, pp. 245-269.

[6] Pal S.K., Saxena P. K. and Mutto S.K.: The Future of Audio Steganography, PacificRim Workshop on Digital Steganography, Japan, 2002.

[7] Westfeld A. and Pitzmann A. : Attacks on Steganographic Systems , Lecture Notes inComputer Science, vol. 1768, Springer-Verlag, Berlin, pp. 61-75, 2000.

[8] Fridrich, Jessica et.al., : Steganalysis of LSB Encoding in Color Images, Proceedingsof the IEEE International Conference on Multimedia. 1279–1282. New York: IEEE Press, 2000.

[9] G.Ganesan, K.Murugeswari et.al. : StegGen: A Steganographic Tool using LSBColor Cycle, proceedings of NCINM 2011.

[10] Mazdak Zamani and Azizah A. Manaf et. Al .: A Genetic-Algorithm-Based Approach for Audio Steganography , World Academy of Science, Engineering and Technology,2009