Abstract — A wide range of steganography techniques has been described in this paper. Beside the evaluation of embedding parameters for the existing techniques, two problems - weaknesses- of substitution techniques are investigated which if they could be solved, the large capacity and strength of substitution techniques would be practical. Furthermore, a novel, principled approach to resolve the problems is presented. Using the proposed genetic algorithm, message bits are embedded into multiple, vague and higher LSB layers, resulting in increased robustness.

Index Terms — audio steganography, substitution techniques, genetic algorithm, LSB technique, data hiding, watermarking

I. INTRODUCTION

Steganography is the study of 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 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 [6].

Steganography and watermarking describe methods to embed information transparently into a carrier signal. Steganography is a method that establishes a covered information channel in point-to-point connections, whereas watermarking does not necessarily hide the fact of secret transmission of information from third persons. Besides preservation of the carrier signal quality, watermarking generally has the additional requirement of robustness against manipulations intended to remove the embedded information from the marked carrier object. This makes watermarking appropriate for applications where the knowledge of a hidden message leads to a potential danger of manipulation. However, even knowledge of an existing hidden message should not be sufficient for the removal of the message without knowledge of additional parameters such as secret keys [2].

Steganographic algorithms can be characterized by a number of defining properties. Three of them, which are most important for audio Steganographic algorithms are introduced below.

Transparency evaluates the audible distortion due to signal modifications like message embedding or attacking. 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 [13].

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 [9].

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 [13].

II. WHY STILL SUBSTITUTION TECHNIQUES OF AUDIO STEGANOGRAPHY

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) [2].

III. THE REMAINED PROBLEMS OF SUBSTITUTION TECHNIQUES OF AUDIO STEGANOGRAPHY

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:

- Having low robustness against attacks which try to reveal the hidden message
- Having low robustness against distortions with high average power

A. First Problem

One type of robustness that is very critical for security is withstand against the attacks which try to reveal or extract the hidden message. This paper is to improve this type of robustness. With an intelligent algorithm we hope to reach a more robust substitution technique, as such, extracting the hidden message become inaccessible to adversary. 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.

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 [1] that the human auditory system (HAS) is highly sensitive to the AWGN. This fact limits the number of bits that can be imperceptibly modified during message embedding [3]. 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.

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.

IV. THE SOLUTION

Accordingly, there are two following solutions for mentioned problems:

1. The solution for first problem: Making more difficult discovering which bites 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 we try to satisfy “other bits alteration to decrease the amount of the error” of second solution, if we 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.

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.
V. GENETIC ALGORITHM APPROACH

As Figure 1 shows, there are four main steps in this algorithm that are explained below.

Figure 1. Approach Diagram

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 we 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 that we expect 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: 00111111 = 47
Target layer is 5, and message bit is 1
Without adjusting: 00111111 = 63 (difference is 16)
After adjusting: 00111000 = 48 (difference will be 1 for 1 bit embedding)
Sample bits are: 00100111 = 39
Target layers are 4 & 5, and message bits are 11
Without adjusting: 00111111 = 63 (difference is 24)
After adjusting: 00011111 = 31 (difference will be 8 for 2 bits embedding)

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.

CONCLUSIONS

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.

ACKNOWLEDGEMENTS

This work is part of a project supported by the Ministry of Science, Technology and Innovation of Malaysia whose title is “Development of Digital Audio Information Hiding Systems For High-Embedding-Capacity Applications” (01-01-06-SF0524).

REFERENCES