IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 4, Ver. V (Jul – Aug. 2014), PP 31-38
www.iosrjournals.org

Secured Genetic Algorithm based image hiding technique with location number compression

Krishna Bhowal[1], D. Sarkar[2], S. Biswas[3], P. P. Sarkar[4]
[1,2,3,4]Dept. Of E.T.S (USIC), University of Kalyani, Kolkata, India

Abstract: *Data hiding involves hiding of information in a cover media to obtain the indistinguishable media, in such a way that the cover media is supposed not to have any embedded image for its unintended recipients. Steganography and Watermarking are main parts of the fast developing area of information hiding. This paper is based on Steganography, Watermarking and Cryptography where the system ensures secured image transfer between the source and destination. Encrypted image bits are embedded into higher and random LSB layers, resulting in increased robustness against noise addition. On the other hand, multi-objective Genetic Algorithm operators are used to reduce distortion. The basic idea of this paper is to improve security. For this improvement image embedding position numbers are converted to optimized Arrays and these Arrays are embedded into the Audio file. Performance based on imperceptibility, security and hiding capacity has been evaluated and discussed.*

Keywords: *Watermarking, Steganography, Artificial intelligence, Cryptography, Genetic algorithm.*

I. Introduction

Steganography, Watermarking and Fingerprinting are branches of information hiding. Basic requirement of steganography imposes that the presence of hidden information within the stego-cover media should be undetectable. There should be no perceptible difference between the watermarked and original signal, and the watermark should be difficult to remove or alter without damaging the host signal. In a computer-based data hiding techniques in audio, secret images are hidden in digital audio signal so that they can be extracted at the receiving end with the help of a secret key and not merely to obscure its presence. The secret image is embedded by slightly altering binary sequence of audio signals. Multimedia data hiding techniques have developed a strong basis of growing number of applications like copyright protection, authentication, tamper detection, covert communications etc. Embedding secret images in digital sound is usually a more challenging task than embedding images in other media.

The pure data hiding techniques, secret key data hiding techniques and public key data hiding techniques are the three common data hiding techniques. In pure data hiding techniques, no secret key is required to exchange prior to communication / exchange. However, the method has a drawback of being less secured since the parties rely on the assumption that no other party is aware of this secret image.

Exchange of a secret key is required in secret key data hiding technique prior to exchange / communication. Secret key data hiding technique hides the secret image inside a cover image by using a secret key. The secret image can be accessed by parties who know the secret key. The advantage of this process is that even if it is intercepted; only parties who know the secret key can extract the secret image.

Public key data hiding technique is based on the concepts of public key cryptography. Public key data hiding technique uses a public key and a private key to secure the exchange/communication between the parties. In public key data hiding technique, the sender uses the public key during the encoding process and uses only the private key, which has a direct mathematical relationship with the public key to decipher the secret image. It has multiple levels of security, which makes it difficult for opponent to access the secret image.

Data hiding technique exploits the psychoacoustical masking phenomenon of the human auditory system. Auditory masking property renders a weak tone imperceptible in the presence of a strong tone in its temporal neighborhood. This property of inaudibility of weaker sounds is used in different ways for embedding information and these properties have led researchers to explore the utilization of audio signals as carriers to hide information. The hidden information is imperceptible if a listener is unable to distinguish between host audio and watermarked-audio signal.

Data hiding techniques can be characterized by a number of defining properties. Some important properties are defined below.

Transparency evaluates the audible distortion due to signal modifications like image 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. 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 cover media.

Robustness measures the ability of embedded data to withstand against intentional and unintentional attacks. Basic Data hiding process has been shown in Fig. 1.

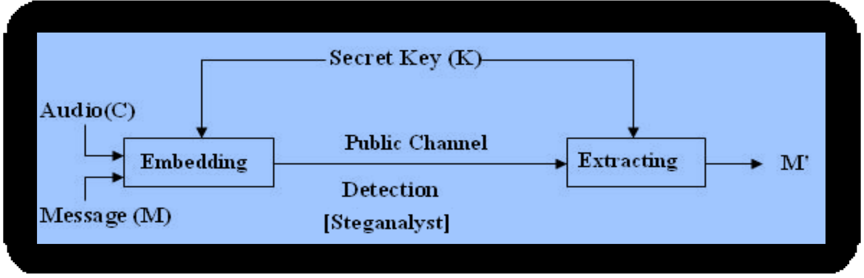


Fig. 1 Basic data hiding process

LSB coding is one of the earliest techniques studied in the information hiding area of digital audio. The main advantage of the LSB coding method is a very high channel bit rate and a low computational complexity of the algorithm, while the main disadvantage is considerably low robustness against signal processing modifications. Since substitution techniques usually modify the bits of lower LSB-layers in the samples, it is easy to reveal the hidden image if the low transparency causes suspicious. In order to conceal secret information successfully, a variety of methods for embedding information in digital audio have been introduced [1-17].

As we know LSB-layer's bits in samples are more suspicious, so embedding the image bits other than LSB-layers could be helpful to decrease the perceptibility and to increase the robustness. The basic idea of this research work is to provide a novel method to hide the secret data from intruders at high random LSB layers. Then the secret data will be sent to the destination in safer and secure manner. The quality of sounds depends on the length of the image and size of the audio which are selected by the users. Even though it shows changes in bit level deviations in the frequency chart, as a whole we cannot determine the change in the audio. Here the technical challenge is to provide transparency and robustness which are conflicting requirements. The perceptibility and extraction of hidden information of the proposed algorithm is more challenging as well, because there is a significant number of bits flipped in a number in bit layers. On the other hand, image retrieval from random higher LSB layers is still one of the major drawbacks of the modified LSB methods. In this paper, the hidden information location numbers have been compressed to extract the hidden information location numbers from the receiver end.

The remainder of the paper is organized as follows: section 2 discusses related works done by different researchers. Section 3 explains proposed work. Section 4 discusses experimental results. Section 5 highlights advantages of our approach. Section 6 concludes the paper presented here.

II. Related Works

Being a simple method, a very high level of security is not achieved in LSB insertion method. To improve security, modifications are done to the existing LSB method by different researchers. Apart from security, certain other parameters like complexity, computational load, SNR, Bit Error Rate, efficiency, etc are also considered for data hiding techniques.

Parity coding and XORing methods have been used with LSB methods by some of the researchers. On the other hand, to improve security against distortion and noise of LSB method, some of the papers have increased the depth of the embedding layer from 4th to 6th and 8th LSB layer without affecting the perceptual transparency of the stego audio signal. In [1] and [2], only bits at the sixth position of each 16 bits sample of the original host signal are replaced with bits from the image. To minimize the embedding error, the other bits have been flipped in order to have a new sample that is closer to the original one. On the other hand, [3] has shifted the LSB embedding to the eighth bit and has avoided hiding in silent periods or near silent points in the host signal. The fact that the embedding occurs in the eighth bit will slightly increased the robustness of this method compare to the conventional LSB methods. However, the hiding capacity will be decreased since some of the samples are to be left unchanged to preserve the audio perceptual quality of the audio signal. In addition, the easiness of image retrieval is still one of the major drawbacks of the LSB and its variant, knowing by fact that embedded bits are at sixth or eighth position from the stego audio signal. To solve this problem, location numbers have been minimized by using Huffman Coding in this paper so that we can easily extract hidden information embedded in different random LSB positions from the receiving end.

III. Proposed Works

In this paper, different security issues for our steganographic process have been discussed and measured. We take care about the position number of the image bits embedded in the host audio. It is very important for the receiver as without knowing the image bit position numbers it is not possible to extract the original image.

Initially asymmetric algorithm (RSA) has been applied to encrypt the image and then proposed LSB algorithm has been applied and encrypted image bits have been embedded to the audio bit stream (16 bit sample) at random in higher LSB layer positions (increase the robustness) to get a collection of chromosomes. Now Genetic Algorithm operators have been used to get the next generation chromosomes. Next, the best chromosome has been selected 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. Sometimes it can happen that for more than one LSB layer, we get the same deviation between original audio sample and stego audio samples. In this case, higher LSB layer has been chosen. Here higher LSB layer has been given higher preference in case of layer selection.

Encrypted image bit positions are the very import information for the receiving parties, because receiving of image is possible only by knowing the position numbers of the image bits in the stego audio file. On the other hand, if intruders want to know the hidden image in the stego-audio file, they will try to know the location numbers of the image bit in the stego-audio file. To ensure the secured transmission, first, optimized arrays of location numbers has been created using Huffman coding and optimized arrays have been embedded into the Audio file.

Now to get the encrypted image from receiving end, first, extract the position numbers from optimized arrays. Decode encrypted image bits using Modified LSB decoding and get the encrypted image. Finally, apply private key of RSA algorithm to extract the original image from encrypted image.

3.1 Step to generate Watermarked-audio file

a. Convert plain image to encrypted image using RSA algorithm.

b . Convert encrypted image to linear byte streams.

c. Read an audio file byte-wise.

d. Generate n (2–16) number of chromosomes of 16 genes by inserting an encrypted image bit into 16 bits audio sample at n (2–16) random positions.

e. To generate better next generation population, following GA operator based insertion algorithm has been used:

Let ‘pos’ is the insertion position of the audio data,
Let $\mathrm{fm}\ (\mathrm{pos})$ be mutation operation on ‘pos’ position,
$\mathrm{fc1}\ (\mathrm{start}, \mathrm{end})$ be crossover operation from ‘start’ to ‘end’ by 1 and
$\mathrm{fc0}\ (\mathrm{start}, \mathrm{end})$ be crossover operation from ‘start’ to ‘end’ by 0.

```
if pos = 1, then no action is taken
if pos = 2 to 15 then do the following
if image bit is 0 and audio bit is 1 for pos = i
        if audio bits on 1 to (i-1) positions are holding 0’s, then perform $\mathrm{fc1}\ (1, \mathrm{i} - 1)$ operation.
        if audio bits on 1 to (i-1) positions are holding 1’s and on (i+1) position holding 0, then performs $\mathrm{fc0}\ (1, \mathrm{i} - 1)$ and $\mathrm{fm}\ (\mathrm{i} + 1)$ operations.
if image bit is 1 and audio bit is 0 for pos = i
        if audio bits on 1 to (i-1) positions are holding 1’s, then perform $\mathrm{fc0}\ (1, \mathrm{i} - 1)$ operation.
        if audio bits on 1 to (i-1) positions are holding 0’s and on (i+1) position holding 1, then performs $\mathrm{fc1}\ (1, \mathrm{i} - 1)$ and $\mathrm{fm}\ (\mathrm{i} + 1)$ operations.
        if audio bit on (i+1) and (i-1) positions are holding 0/1 and 1/0 respectively, no action is taken.
        If audio bit and image bit is same, then no action is taken as there will be no deviation between two samples.
```

f. Now select the best chromosome, where best one is the chromosome which has the minimum difference with the original 16 bit audio sample.

g. Here fitness value is the position number for which we get the best chromosome.

Again, the position number, best chromosome and distortion are closely related, because whenever we will choose the best chromosome, it will reduce the distortion.

h. Fitness value is representing two things here:

(i) Position number which is very important at the receiving end to extract the image.

(ii) Distortion which again very important regarding security (distortion can convinced hacker to hack the image).

So, multi-objective GA is used here

i. Use modified LSB algorithm to embed image bits into audio sample bytes and stores the positions into temporary array.

j. Position numbers has been compressed using Huffman coding and embedded them in to audio file.

Example of Huffman Coding:
We know that to store a image character, we need 8 locations of the 8 16-bit samples.
Fixed-Length versus Variable-Length Prefix Codes (Huffman code) for 8 locations numbers

Location Numbers	15	14	13	2
Frequency	3	2	2	1
Fixed-length code	1111	1110	1101	0010
Prefix code	1	01	001	000

To store 8 of these location numbers,
(1) The fixed-length code requires 8 x 4 = 32 bits,
(2) The prefix code uses only 3 x 1 + 2 x 2 + 2 x 3 + 1 x 3 = 16 bits a 50% saving.
k. Write stego audio byte stream to an audio file.

3.2 Extracting hidden image

At the time of inserting image bits into audio sample, we optimize the deviation between cover data and stego-data, so stego-audio is more or less equal to the original audio. So, to extract the hidden image we need to know only the position number of hidden image bits.
a. Read the stego audio file byte-wise.
b. Extract position numbers from compressed arrays using Huffman decoding algorithm.
e. Decrypt encrypted image by private key of RSA algorithm to get plain image.
f. Write the extracted image to a text file.
g. Write the audio byte stream to an audio file.

IV. Experimental Results

The attacks to a data hiding technique mainly include passive attack, active attack, and extracting attack. A passive attacker only wants to detect the existence of the embedded image, while an active attacker wants to destroy the embedded image. The purpose of an extracting attacker is to obtain the image hidden in the stego-object. So there are three kinds of security measures for different attackers respectively, i.e., detectability, robustness and difficulty of extraction. Usually the problem of steganography only concerns the detectability so in many literatures delectability is referred to the security of a stegosystem [5]. The problem of Watermarking concerns the detectability and robustness both. In this section we discussed and measured the security of our data hiding process and some experimental results, two examples: Example 1 describes how the best sample is selected, Example 2 describes how to reduce the distortion using GA operators.

4.1 Audio Quality Evaluation

From Table 1 and Fig. 2, it is clear that statistical signal change (signal amplitude) due to bit flipping is very negligible compare to the original signal.

Table 1: Deviation of digital audio payload (%):

0.000	0.015	0.000	0.018	0.000	0.003	0.000	0.003	0.000	0.000
0.000	0.000	0.013	0.009	0.000	0.006	0.025	0.009	0.000	0.012
0.000	0.006	0.006	0.006	0.003	0.021	0.000	0.006	0.003	0.003
0.000	0.000	0.012	0.009	0.000	0.012	0.012	0.012	0.000	0.006
0.000	0.006	0.000	0.006	0.000	0.000	0.000	0.009	0.006	0.021
0.000	0.009	0.000	0.009	0.000	0.006	0.000	0.009	0.000	0.006
0.000	0.009	0.006	0.003	0.000	0.003	0.000	0.009	0.000	0.006
0.000	0.006	0.009	0.015	0.000	0.006	0.000	0.006	0.000	0.003
0.000	0.000	0.000	0.009	0.000	0.006	0.000	0.003	0.000	0.000
0.000	0.003	0.000	0.006	0.003	0.006	0.000	0.003	0.000	0.015
0.000	0.003	0.006	0.006	0.006	0.003	0.000	0.003	0.000	0.018
0.003	0.000	0.000	0.009	0.000	0.006	0.006	0.006	0.000	0.006

Proposed LSB data hiding algorithm is tested on 5 audio sequences from different music styles (classic, jazz, country, pop, rock). The audio experts were selected so that they can represent a broad range of music genres, i.e. audio clips with different dynamic and spectral characteristics. All music pieces have been embedded by image using the proposed and standard LSB algorithm. Clips were 44.1 kHz sampled mono audio files, represented by 16 bits per sample. Duration of the samples ranged from 10 to 15 seconds.

4.2 Audio quality measures

Here we give brief descriptions of the quality measures used. The original signal (the cover audio) is denoted x(i), i = 1 to N while the distorted signal (the watermarked-audio) as y(i), i = 1 to N.

Segmental Signal-to-Noise Ratio (SNRseg): SNRseg is defined as the average of the SNR values over short segments on equation no. (1):

$$\mathrm{SNRseg} = \frac{10}{M}\sum_{m=0}^{M-1}\log_{10}\sum_{i=Nm}^{Nm+N-1}\left(\frac{x^2(i)}{\left(x(i)-y(i)\right)^2}\right) \ldots\ldots(1)$$

where x(i) is the original audio signal, y(i) is the distorted audio signal. The length of segments is typically 15 to 20 ms for speech. The SNRseg is applied for frames which have energy above a specified threshold in order to avoid silence regions.

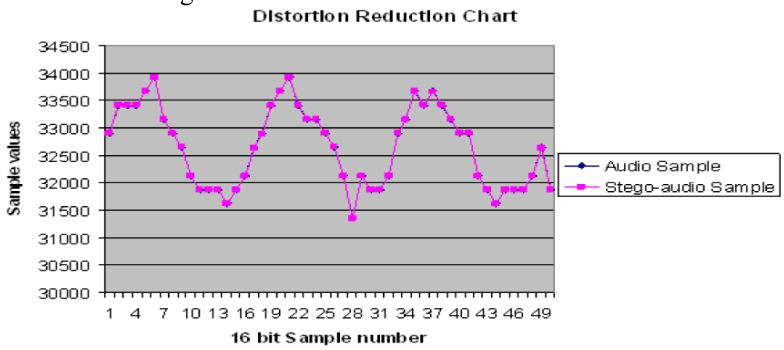


Fig. 2 Minimum deviation between host & Stego-audio samples

Signal-to-Noise Ratio (SNR), is a special case of SNRseg, when M=1 and one segment encompasses the whole record. The SNR is very sensitive to the time alignment of the original and distorted audio signal [6]. The SNR is measured as equation no. (2) and Table 2 showing the experimental result for 5 categories of audio file.

$$\mathrm{SNR} = 10\log_{10}\frac{\sum_{i=1}^{N}x^2(i)}{\sum_{i=1}^{N}\left(x(i)-y(i)\right)^2} \ldots\ldots(2)$$

Table 2: SNR values and Capacities of the proposed data hiding algorithm for different audio signals

	Music Genre	Sample Size (Bits)	SNR (dB)		Capacity (%)	
			PM	SW	PM	SW
1	classic	16	83.42	33 to 76	12.5	2 -34
2	jazz	16	82.67	32 to 81	12.5	2 -34
3	country	16	82.94	31 to 80	12.5	2 -34
4	pop	16	83.15	38 to 82	12.5	2 -34
5	rock	16	83.27	39 to 78	12.5	2 -34

PM→ Proposed Method SW→ Similar Works ([1], [2]. [3])

4.3 Correlation-Based Measures

The similarity between two digital audio samples can also be quantified in terms of the correlation function [6-8]. These ensure measurement of the similarity between two audios, hence in this sense they are complementary to the difference-based measures: Some correlation based measures are given in equation no. (3), (4) and (5).

Structural content:

$$C1 = \frac{1}{K}\sum_{k=1}^{K}\frac{\sum_{i=0}^{N-1}x(i)^2}{\sum_{i=0}^{N-1}y(i)^2} \ldots\ldots(3)$$

Normalized cross-correlation measure:

$$C1 = \frac{1}{K}\sum_{k=1}^{K}\frac{\sum_{i=0}^{N-1}x(i)*y(i)}{\sum_{i=0}^{N-1}x(i)^2} \ldots\ldots(4)$$

Czenakowski distance (CZD): A metric that is useful for comparing vectors with strictly non-negative components, like in the case of audio samples, is given by the Czenakowski distance:

$$C = \frac{1}{N}\sum_{i=0}^{N-1}\left(1-\frac{2*\min(x(i),y(i))}{x(i)+y(i)}\right) \ldots\ldots(5)$$

The Czenakowski coefficient (also called the percentage of similarity) measures the similarity among different samples, communities, and quadrates.

Obviously as the difference between two audio samples tends towards zero $\boldsymbol{\varepsilon} = \mathbf{x}(\mathbf{n}) - \mathbf{y}(\mathbf{n}) \rightarrow \mathbf{0}$, all the correlation-based measures tend towards 1, while as $\boldsymbol{\varepsilon}^2 \rightarrow \mathbf{G}^2$ they tend towards 0.

Recall also that distance measures and correlation measure are complementary, so that under certain conditions, minimizing distance measures is tantamount to maximizing the correlation measure. Table 3 is explaining the experimental result for CZD.

Table 3: Music genre, Sample size and CZD values

	Music Genre	**Sample Size (Bits)**	**CZD**
1	classic	16	0.00001888249326
2	jazz	16	0.00002231742249
3	country	16	0.00002079240629
4	pop	16	0.00001666038440
5	rock	16	0.00001739731132

Experimental results show that the two audio clips (original audio sequence and embedded-audio signal) cannot be discriminated by people. Results of subjective tests showed that perceptual quality of watermarked-audio, if embedding is done using the proposed algorithm, is higher in comparison to standard LSB embedding method. This confirms that described algorithm succeeds in increasing the depth of the embedding layer and also randomizing the bit layer without affecting the perceptual transparency of the watermarked-audio signal.

Therefore, significant improvement in robustness against signal processing manipulation can be obtained, as the hidden bits can be embedded higher LSB layers deeper than in the standard LSB method. The proposed algorithm flips bits in more than one bit layers of the watermarked-audio during the embedding procedure. This property may increase the resistance against Steganalysis that identifies the used LSB layer by analyzing the noise properties of each bit layer.

4.4 Capacity and Detection probability:

The capacity depends on the embedding function, and may also depend on properties of the cover. For example, least-significant-bit (LSB) replacement with one bit per sample in an eight-bit audio achieves a net capacity of 12.5%, or slightly less if one takes into account that each audio is stored with header information which is not available for embedding. If the sample size is 16-bit then net capacity will be 6.25% or slightly less. It is intuitively clear, often demonstrated and theoretically studied that longer secret images require more embedding changes and thus are statistically better detectable than smaller ones. Hence, capacity and embedding rate are related to security.

The purpose of information hiding is to hide the existence of a secret image and also increasing robustness. Therefore, the security of a data hiding technique is judged by the impossibility of detecting the image content and extracting the hidden image after detection. However, sometimes, Cryptography also is used to increase the level of security.

4.4.1 Detection Probability (Embedding location number-wise):

We used 8 16-bit samples to embed 8 image-bits. The opponent has to detect 8 bits to get a character.

Probability to detect an embedded bit position = $\frac{1}{16}$

Probability to detect 8 embedded bit positions =$\frac{1}{16}X\frac{1}{16}X\frac{1}{16}X\frac{1}{16}X\frac{1}{16}X\frac{1}{16}X\frac{1}{16}X\frac{1}{16} = \frac{1}{16^8}$

If the length of a image is N characters, then the probability to extract whole image =

$\frac{1}{16}X\frac{1}{16}X \ldots.X\frac{1}{16}$ upto $8 * \mathrm{N}$ terms $= \frac{1}{16^{\mathrm{N}*8}}$

In this work, an encrypted-image-character has been converted to 8-bit stream, so the total probability is lesser.

4.4.2 Decoding Probability (bit (0/1)-wise):

Probability to decode an embedded bit = $\frac{1}{2}$

Probability to decode 8 embedded bits =$\frac{1}{2}X\frac{1}{2}X\frac{1}{2}X\frac{1}{2}X\frac{1}{2}X\frac{1}{2}X\frac{1}{2}X\frac{1}{2} = \frac{1}{2^8}$

If the length of image is N characters, then the probability to extract whole encrypted image = $\frac{1}{2}X\frac{1}{2}X \ldots.X\frac{1}{2}$ upto $8 * \mathrm{N}$ terms $= \frac{1}{2^{\mathrm{N}*8}}$. Again, image has been encrypted by RSA algorithm, so it is very difficult to extract the original image.

Fig. 3 show histogram of the number of modified bit layers in a 10 sec audio sample (116892x16 bits in total) for the proposed LSB algorithm. It is clear that number of flipped bits per bit layers is distributed over all bit layers in the proposed algorithm. In the case of standard LSB algorithm, LSB data hiding techniques can easily detect the bit layer where the data hiding was performed. It is a much more challenging task in the case of the proposed algorithm, because there are a significant number of bits flipped in 16 bit layers and the adversary cannot identify exactly which bit layer is used for the data hiding.

4.5 Examples

Example 1 GA based approach in image hiding, explained in Table 4,
Original Audio sample = 1000000110000010
Image bit = 1
Fitness value = 16, because for the highest position number 16 we got the best quality individual or chromosome.

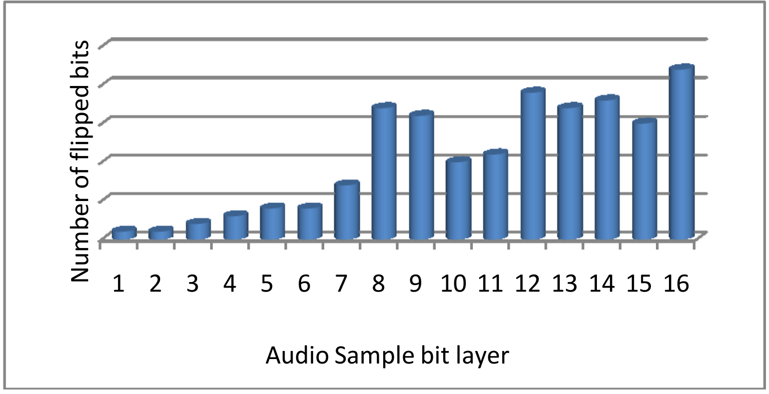
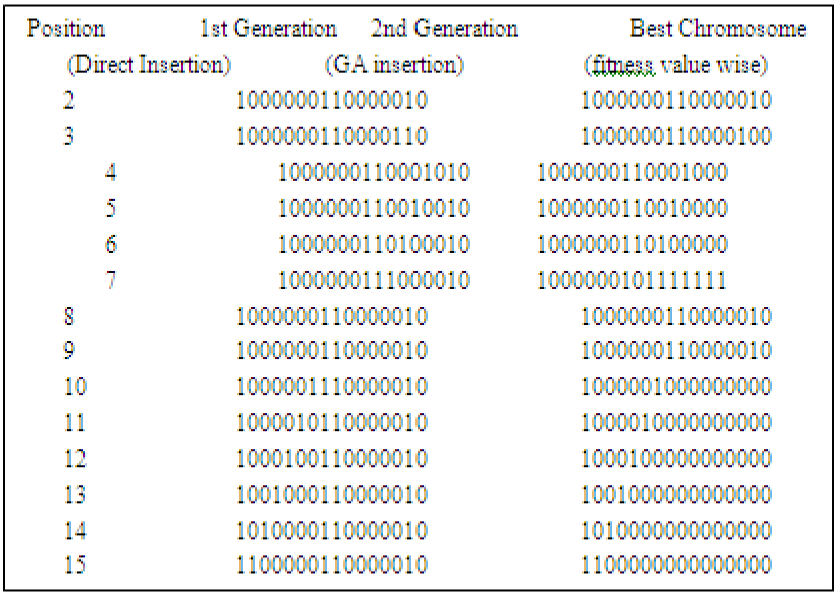


Fig. 3 Number of flipped bits per bit layer for the proposed algorithm

Table 4 GA based image hiding



Position	1st Generation (Direct Insertion)	2nd Generation (GA insertion)	Best Chromosome (fitness value wise)
2	1000000110000010		1000000110000010
3	1000000110000110		1000000110000100
4	1000000110001010		1000000110001000
5	1000000110010010		1000000110010000
6	1000000110100010		1000000110100000
7	1000000111000010		1000000101111111
8	1000000110000010		1000000110000010
9	1000000110000010		1000000110000010
10	1000001110000010		1000001000000000
11	1000010110000010		1000010000000000
12	1000100110000010		1000100000000000
13	1001000110000010		1001000000000000
14	1010000110000010		1010000000000000
15	1100000110000010		1100000000000000

Example 2 GA based insertion algorithm
Audio Sample 0..00101111$_2$ = 47$_{10}$, LSB layer 4, image bit 0, Output 0..00100111$_2$ = 39$_{10}$, After applying GA operators it is 0..00110000$_2$ = 48$_{10}$ which is more closer to 47$_{10}$.
Audio Sample 0..00111010$_2$ = 58$_{10}$, LSB layer 4, image bit 0, Output 0..00110010$_2$ = 50$_{10}$, After applying GA operators it is 0..00110111$_2$ = 56$_{10}$.
Audio Sample 0..00001000$_2$ = 8$_{10}$, LSB layer 3, image bit 1, Output 0..00001100$_2$ = 12$_{10}$, After applying GA operators it is 0..00000111$_2$ = 7$_{10}$.
Audio Sample 0..00110111$_2$ = 55$_{10}$, LSB layer 4, image bit 1, Output 0.00111111$_2$ = 63$_{10}$, After applying GA operator it is 0.00111000$_2$ = 56$_{10}$.

V. Advantages Of Our Approach

- Embedded image bits position numbers has been converted to optimized arrays to make it secure.
- Described 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 watermarked audio signal.

- That is, two-way robustness (to know the actual position of the image bit) are there, First, insertion positions are randomly chosen, Second, LSB layers are most of the time are high layers.
- Image bit embedding that causes negligible embedding distortion of the host audio, since optimization is done using GA operators.
- In addition, listening tests showed that perceptual quality of watermarked-audio is higher in the case of the proposed method than in the standard LSB method [1-17].

VI. Conclusion

This paper presents a bit-modification algorithm for modified LSB data hiding technique where image bit positions has been converted to optimized arrays and arrays has been inserted into the audio file. The key idea of the algorithm is to embed the image bit which will cause negligible embedding distortion of the host audio. Listening test shows 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 audio signal. The detection and extraction of hidden information of the proposed algorithm is more challenging as well, because there is a significant number of bits flipped in a number in bit layers. On the other hand, position numbers transmission problem has been resolved by converting them in optimized arrays and it makes system more undetectable.

References

[1] N. Cvejic, T. Seppanen, "Increasing Robustness of LSB Audio Steganography Using a Novel Embedding Method", Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC04), 2004, vol. 2, pp. 533-540

[2] N. Cvejic, and T. Seppnen, "Reduced distortion bit-modification for LSB audio steganography", Journal of Universal Computer Science, January 2005, 11(1), pp. 56-65.

[3] Mohamed A. Ahmed, Miss Laiha Mat Kiah, B.B. Zaidan and A.A. Zaidan, "A Novel Embedding Method to Increase Capacity and Robustness of Low-bit Encoding Audio Steganography Technique Using Noise Gate Software Logic Algorithm", Journal of Applied Sciences, 2010, 10(4), pp. 59-64.

[4] K Bhowal, D Bhattacharyya, A J Pal, Tai-Hoon Kim, "A GA based audio steganography with enhanced security" Telecommunication Systems Journal, Springer, April 2013, 52(4), pp 2197-2204.

[5] Fridrich, Jessica and others. "Steganalysis of LSB Encoding in Color Images." Proceedings of the IEEE International Conference on Multimedia, New York: IEEE Press, 2000, pp-1279-1282

[6] Quackenbush, S. R., T. P. Barnwell III, and M. A. Clements, "Objective Measures of Speech Quality", book, Prentice Hall, 1988, Englewood Cliffs.

[7] Avcıbaş, İ., Sankur B., and Sayood K., "Statistical evaluation of image quality metrics", Journal of Electronic Imaging , April 2002, 11(2), 206– 223.

[8] A. M. Eskiciog˘lu and P. S. Fisher, "Image quality measures and their performance," IEEE Trans. Commun. 1995, 43(12), pp-2959–2965

[9] W. Bender, D. Gruhl, N. Morimoto and A. Lu, "Techniques for data hiding", IBM Systems Journal, Vol. 35, Nos. 3 & 4, pp. 313-336, 1996.

[10] Y.-C. Tseng, Y.-Y. Chen and H.-K. Pan: A secure data hiding scheme for binary images, IEEE Trans. Commun., 2002 , 50(8), pp. 1227-1231.

[11] Houda Jouhari, EL Mamoun Souidi, "A Novel Embedding Scheme based on Walsh Hadamard Transform" Journal of Theoretical and Applied Information Technology, 15th October 2011. 32(1), pp- 55- 60

[12] Md. Shafakhatullah Khan, V.Vijaya Bhasker, V. Shiva Nagaraju "An Optimized Method for Concealing Data using Audio Steganography" International Journal of Computer Applications, November 2011, 33(4), pp - 25-30

[13] Cvejic N. and Seppä̈nen 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.

[14] Pal S.K., Saxena P. K. and Mutto S.K. "The Future of Audio Steganography". Pacific Rim Workshop on Digital Steganography, 2002, Japan.

[15] K. Gopalan "Audio Steganography using bit modification ", proc. IEEE Int. conf acoustics, speech, and signal processing, April 2003,Vol 2, pp 421-424.

[16] M. D. Swanson, M. Kobayashi and A. H. Tewfik, "Multimedia data-embedding and watermarking technologies", Proc. IEEE, June 1998, Vol. 86, pp. 1064-1087,.

[17] Z. Mazdak,A. M. Azizah,B. A. Rabiah,M.Z.Akram and A.Shahidan, "A Genetic-Algorithm-Based Approach for Audio Steganography", World Academy of Science, Engineering and Technology 2009, 54.

[18] Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, Ton Kalker, "Digital Watermarking and Steganography" 2nd edition, Morgan Kaufmann Publishers Inc. San Francisco, CA, USA ©2008, pp-425 - 490

[19] Bohme, R "Advanced Statistical Steganalysis, Principles of Modern Steganography and Steganalysis" ISBN: 978-3-642-14312-0, 2010

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