International Journal of Research Studies in Science, Engineering and Technology
Volume 2, Issue 5, May 2015, PP 33-39
ISSN 2349-4751 (Print) & ISSN 2349-476X (Online)

Hidden Text into Audio Files

Adel A. Sewisy

Faculty of computers and Information
Department of computer Science
Assuit University, Egypt
sewisy@aun.edu.eg., dr.adelsewisy@yahoo.com

Romany F. Mansour

Faculty of Science
Department of computer Science
N.V., Assuit University, Egypt
romanyf@aun.edu.eg

S. Z. Rida

Faculty of Science
Department of Mathematics
South Valley University, Egypt
szagloul@yahoo.com

Amal A. Mohammed

Faculty of Science
Department of Mathematics
South Valley University, Egypt
amalrashed2011@hotmail.com

Abstract: *Steganography entails concealed data that is inside data set. For example, a text message that is in an image or an audio file or video file can be referred to as stenography. This paper features a new technique that is suggested by the scholars. The technique suggests that the text message is encoded through the use of Huffman coding method and entrenched into audio file when applying the LSB algorithm. The result is put into a novel audio file. Thereafter, the result is compared and precisely composed through the use of various values that include, PSNR (peak signal to noise ratio) and SNR (signal to noise ratio) thus making it possible identify the frequency of audio file prior and after entrenched text message. Trials indicate that the suggested method is comparatively effective for Embedded Encrypted Text into Audio files.*

Keywords: *Steganography, Information Hiding, Cryptography, Data Encryption, Huffman coding, LSB.*

1. INTRODUCTION

Steganography entails the art of writing concealed messages in such a manner that only the sender and the intended receiver are aware of the presence of the message. After the unprecedented technological advancement that has taken place over the years and in particular with the era of internet technology that is now commonly used for communication, it can be explained that there is a need to ensure that measures are put in place so that information that is sent from one party to another is secure. Indeed, such an approach would entail encryption and concealing of messages inside an image file, audio file or both types of files.

Concealing information can be discussed as an approach of restricting private information in an image file or audio, video and executable files in order to ensure that it becomes impossible for a person to have access to the message unless he/she is either the sender or the receiver. The program can modify the shape of the data indoctrination as well as the delivery of content format and not raise any suspicions.

The key benefit of concealing information through the use of various approaches is that it does not give any hints of there been a hidden message in case the message is accessed by a third party. Unlike encoded message, the message in this case will be used as a technique of inviting the focus of the third party.

Even though the steganography method has different applications that are useful, it can at times be applied for other illegal activities. For instance, drug dealers, terrorists and other criminals can use the technique in order to ensure that their communication is not accessed by third parties thus implying that it can help enhance the activities that are carried out by the criminals.

All of the above are some of the main reasons as to why development wider writing concealed compared techniques of encryption, since writing is encoded or distorted resulting to the administrator been required to implement different strategies in order to ensure that they get access to the original information and attempt to break the code, while writing concealed does not raise doubt when a

regular viewer, might pass by undetected with no suggestion of any information been concealed in the file that is included.

The suggested method integrates the cryptography and steganography concepts and as a result establishes a high level security which thwarts attackers from discovering the existence of the concealed message. In the initial level, the concealed message is encoded by application of Huffman coding Algorithm. In the succeeding level, the encoded text is concealed in the audio file through the use of least significant Bit.

The other sections of this paper are; Section 2 which contains a short review of related works, Section 3 that features steganography method while the general algorithm for the suggested method is provided in Section 4. The trials and examination of the outcomes are presented in Section 5 while conclusion is presented in section 6.

2. RELATED PAST WORKS

There are numerous past studies that have focused in the subject of steganography and compression of data. Nevertheless, it can be noted that only a small percentage of such studies have covered on the subject of hide data compressed , due to the fact that file cover is typically much larger than the message that is to be concealed implying that there is no need for data compression. Thus, it can be noted that there is a need for a research that focuses in data procession and minimization of size through the application of algorithm in order to ensure that the data can be reduced while the security of the data is increased.

R. Kaur [1] applied the multilevel procedure in audio steganography which entrenched three messages in audio file, in level 1 conceal message by making use of LSB technique, in level 2 conceal message 2 in audio file from level 1 applying parity bit coding method, in level three conceal message 3 in resulted audio file from level 3 applying frequency hopping spread spectrum coding technique and compute PSNR and MSE at every level and scheme the audio file figure at each level.

K.U. Singh [2] highlighted various audio steganography methods like temporal domain method and Transform Domain Technique (e.g, Discrete Wavelet transform, Spread Spectrum, Tone insertion, Phase coding) and then compared between these methods from strength and weakness. F. A. Sabir [3] applied both of cryptography and steganography methods and encoded text using DES (Data Encryption Standard) and concealed it in wav file using time and frequency domain technique and examined the cover audio file into its frequency elements through the use of Haar filter. He then computed the value of SNR (Signal to Noise Ratio) which affirmed that the concealing in frequency domain is ideal than concealing in time domain.

T. Sandhya[4] suggested technique based on integration of audio steganography and cryptography that is based on dual density double tree complex wavelet Transform with blowfish encryption. It implements most influential procedure in the initial level of security which is very intricate to disrupt. In the subsequent level, it applies a changed LSB procedure to encrypt the message into audio thus ensures superior security.

Taruna[5] applied a keyless randomization that is provided to supplement undisclosed information in numerous and variable LSBs. Cover signal is transformed into binary format and then with the suggested algorithm, binary cover signal is categorized into blocks of size 8x8 that have 16 bits per sub block, and then examining each sub block's first two MSBs to establish how many LSBs will be applied during attachment of secret data bits. PSNR values indicate that there is no obvious variance between cover audio signal and stego audio signal. R. Valarmathi [6] applied most authoritative algorithm in the initial level of security, which is very intricate to break. In the succeeding level it applies a modified LSB procedure to encrypt the message into audio. This system enhances better security.

A. Chadha [7] technique is dependent on Least Significant Bit (LSB) management and attachment of terminated noise as undisclosed key in the message. This technique is used in data concealing in images. For data concealing in audio, Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) were all applied.

N. Kaul [8] found that an audio message can be entrenched in an image through the use of LSB (Least Significant Bit) technique as well as the wavelet conversion. To conceal a speech in an image is

puzzling since the scope of speech is greater than the size of an image. Number of bits in 1kb of speech is almost equal to an image.

Burate D. J [9], suggested a new method to conceal text in speech in an environment that has no noise. We chose to operate in the digital field and conceal the text information within speech signal using audio steganography method. Indeed, our technique enhances the hiding data rate. We better reserve the uniqueness of the speech carrier by engaging an entrenching instead of a replacement operation on the undisclosed text. To intensify security, steganography has to be combined with cryptography. Nevertheless, our technique does not use any of the cryptography methods as it applies coding approach.

3. LSB AND HUFFMAN ALGORITHMS

Least significant Bit (LSB) algorithm is the most basic and knowledgeable technique in steganography and attaches one bit or more of hidden message and is substituted by the LSB of the audio file. Data entrenched into audio file in the time domain by LSB which designated a set of sampled audio file (the cover) that selected as undisclosed key. The process is applied by substituting LSBs of sampled audio file by the bits of undisclosed message and the re-claim process in the opposite order.

Huffman code is established by a fixed-length encrypting data into adjustable length. Huffman algorithm commences according to the list of data that is arranged by descendent likelihood of their presence in the file to be encrypted. Thereafter, the tree is established with the code in each sheet. This procedure is undertaken in numerous procedures at each step. Data are designated with smaller frequencies and added to the higher part of the tree followed by removal of the incomplete frequencies. The younger ones are selected from the list and substituted by secondary values in order to show two of the initial values. By doing that, the list is minimized to a single value secondary. Therefore, the procedure will last getting only one value. Finally, the set c ode for each sheet is contingent on the path from the root node to the icons in the menu, as presented in Fig. 1, which entails the flowchart of the algorithm for Huffman coding.

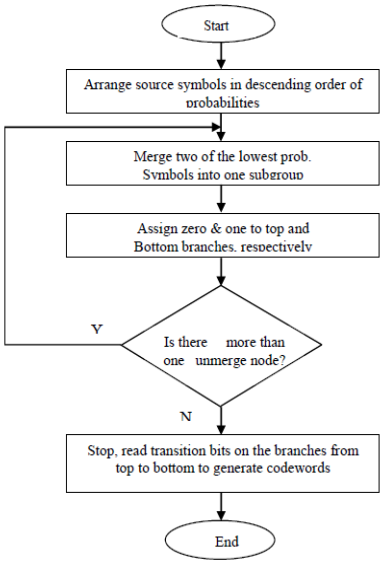

Fig1. *Huffman Algorithm*

4. THE SUGGESTED METHOD

The suggested method integrates the cryptography and steganography to acquire a high level security and avert attackers from establishing the existence of the undisclosed message. In the initial level, the confidential message is encoded using Huffman coding Algorithm. In the succeeding level the encoded text is concealed in the audio file using slightest significant bit. The subsequent steps exemplify the entrenched process:

- Evaluate the audio file(.wav) , establish the length of file, find out the number of samples
- Compute the key for keeping the data by

$$\text{key} = \frac{\text{number of samples}}{\text{sample rate}}$$

- Transform the cover audio file to binary.
- Read undisclosed message and change it to binary.
- Encode the entered undisclosed message using Huffman coding algorithm.
- Substitute the least important bit of each cover position by the bit of encoded undisclosed message.
- Generate a new audio file that comprises of embedded text into audio file

To obtain the encoded message from the cover audio file at the recipient's side, the succeeding steps should be used:

- Read the entrenched audio file(stego), establish the length of file, number of sample
- Transform stego file into Binary.
- Compute the key for keeping data into audio file

$$key = \frac{number\ of\ sampls}{sample\ rate}$$

- Apply Key to obtain the value that has frequency of letters and symbol of text
- Decrypt the undisclosed message using Huffman code to get the initial text
- Save the symbols in new text file

5. TRIAL RESULTS

We use the suggested procedure on various sound files (wav), and various text file. The outcome depends on the Signal to Noise Ratio (SNR), Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), and the frequency of wav file prior and after entrenched text file. The subsequent equations compute SNR, PSNR, MSE correspondingly:

$$SNR = 10log_{10}\left(\frac{\sum_{i=1}^{N} f(i)^2}{\sum_{i=1}^{N} (f(i)-g(i))^2}\right),$$

$$PSNR = 10log_{10}\left[\frac{\max\ value\ (f(i),g(i))^2}{abs\,(f(i)-g(i))^2}\right],$$

$$\text{MSE} = \frac{1}{\text{M}}\sum(\text{f(i)} - \text{g(i)})^2$$

Where:

N is the size of audio

f is the samples with index number in the original audio file

g is the samples with index number in the stego audio file

Table1. *The Text File Samples*

Name	Size(char)	Data Type
Text1	5	Text
Text2	50	Text
Text3	100	Text
Text4	500	Text
Text5	1000	Text
Text 6	1500	Text

Table2.*The Audio File Samples*

Name	Size(KB)	Length	Type	Sample rate	# of bits
Originalrekam	521	267003	wav	22050	16
Bombom	768	78632	wav	11025	8
FunkGuitar1	1239	638690	wav	44100	16

Table3. *The SNR MES and PSNR values for different audio files and different text file after steganography process.*

Name	Text file	SNR	MSE	PSNR
FunkGuitar1.wav	Text1	23.5332	5.3125e-005	70.3512
	Text2	11.8409	7.8438e-004	58.6590
	Text 3	8.7705	0.00016	55.5885
	Text4	1.7748	0.00080	48.5929
	Text5	-1.1970	0.0158	45.6211
	Text6	-2.9444	0.0236	43.8737
Bombom	Text 1	31.1941	4.321e0005	73.7467
	Text 2	19.5024	6.3805e-004	62.0544
	Text3	16.4320	0.010304	58.980
	Text4	9.436	0.0065	51.9883
	Text5	6.4645	0.0128	49.0165
	Text6	4.717	0.0192	47.2691
Initialrekam	Text 1	11.6836	1.3492	38.6993
	Text 2	0.0020	-0.0087	27.0070
	Text3	-3.0791	-0.0087	23.9366
	Text4	-10.0740	0.0191	16.9409
	Text 5	-13.0466	0.0401	13.9691
	Text 6	12.2217	0.0600	12.2217

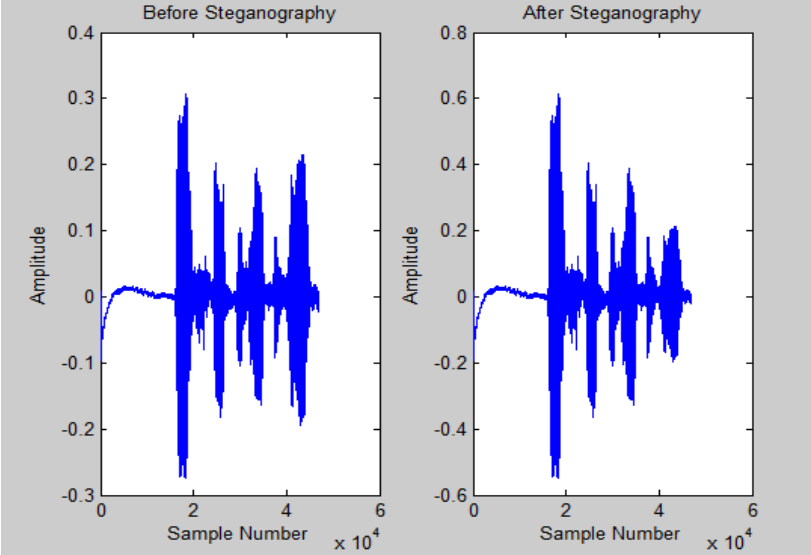

Fig1. *Audio file orginal.wav before and after embedded Text file*

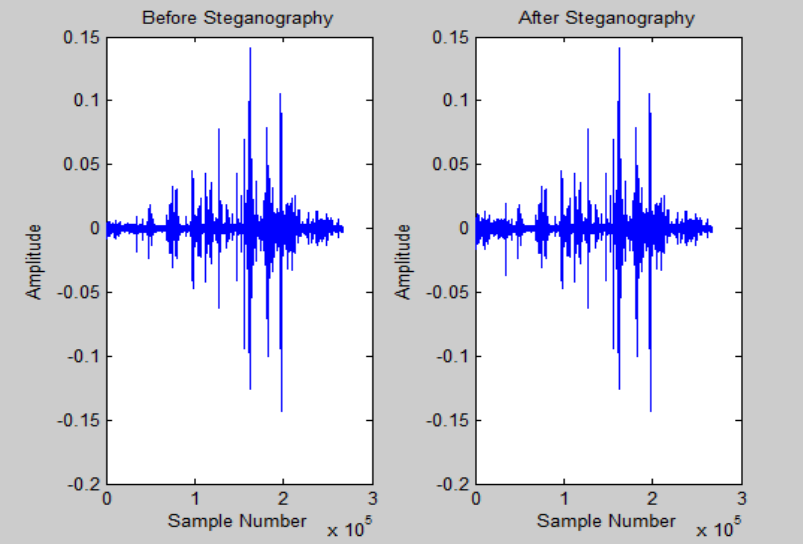

Fig2. *Audio file Originalrekam.wav before and after embedded Text file*

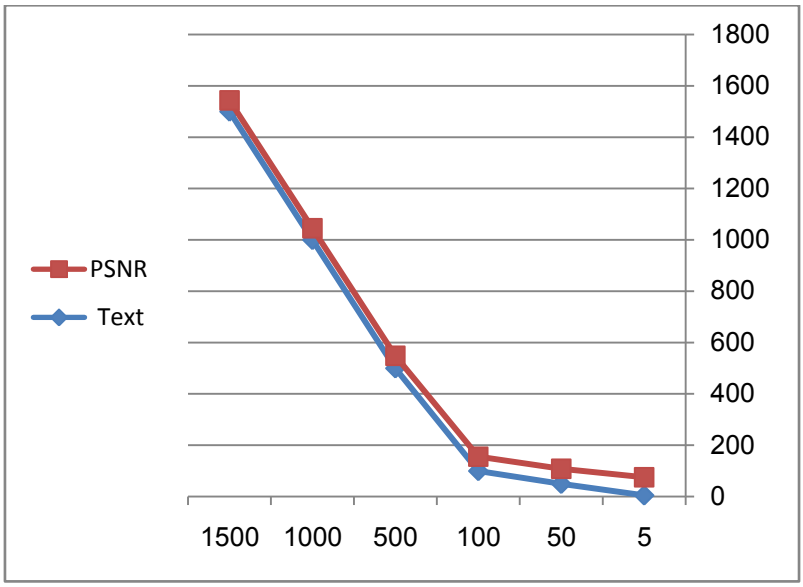

Fig3. *Correlations between text size and PSNR*

The suggested technique is used on various Text file size as depicted in Table 1 and various wav audio file with various size and various audio file with 16 bits per samples and 8 bits per samples as illustrated in table 2.

Fig. 2 depicts the initial audio signal file and audio file after concealed encrypted text file into it. Figure 2 also shows another initial audio signal file and audio file after hide encoded text file into it. Fig. 3 depicts the relation amongst Text size and PSNR which specifies that the value of PSNR reduces as the text size expands.

In the suggested technique, various measures such as PSNR (Peak Signal to noise Ratio), MSE (Mean Square Error), SNR (Signal to noise ratio), are used. From the outcome of the calculations, it can be noted that the noise rate reduced as the size of the file data to be concealed in the audio file increased. In the suggested algorithm, it can be noted that the algorithm retains the reliability of the conveyed data that has high retrieval rate, high precise rate and low error rate as can be proved from the Mean Square error (MSE) values.

Even if the results indicate that the audio file capability upsurges to conceal more data without affecting the clearness of the audio file signal, the benefit of this technique is that it is not complex and data can be easily retrieved with no errors.

6. CONCLUSION

This paper, feature a new technique that is suggest. To begin with, the text message is encoded using Huffman coding method and entrenched into audio file using LSB algorithm. The result is then put into a new audio file and thereafter contrasted through the use of various values that include; PSNR (peak signal to noise ratio), and SNR (signal to noise ratio). The frequency of audio file prior and after entrenched text message is schemed. Trials indicate that the suggested method is comparatively effective in Embedded Encrypted Text into Audio files.

REFERENCES

[1] R. Kaur, Jagriti, H.Singh and R.Kumar, Multilevel Technique to improve PSNR and MSE in Audio Stegsnography. International Journal of Computer Applications, Vol.103, No.5, 1-4, (2014).

[2] K.U. Singh, A Survey on Audio Steganography Approaches. International Journal of Computer Applications, Vol.95, No.14, 7-14, (2014).

[3] F. A. Sabir, Hiding Encrypted Data in Audio Wave File. International Journal of Computer Applications, International Journal of Computer Applications, Vol.91, No.4, 6-9, (2014).

[4] T. Sandhya, A Novel Audio Steganography Scheme using Double Density lauD Tree Complex Wavelet Transform Secured with Modified Blow Fish Encryption. International Journal of Emerging Technology and Advanced Engineering, Vol.3, No.1, 63-72,(2014).

[5] Taruna and Dinesh, "Message Guided Random Audio Steganography using deifidoM LSB Technique", International Journal of Computers & Technology, Vol.86, No.7, 3464-3469, (2014).

[6] R. Valarmathi, M.SC. and M. Phil, A Novel Approach for Audiography- A noitanibmoC of Audio Steganography and Cryptography. International Journal of Emerging Technology and Advanced Engineering, Vol.4, No.1, 55-61, (2014).

[7] A. Chadha, N. Satam and R .Sood, An Efficient Method for Image and Audio Steganography using Least Significant Bit (LSB) Substitution. *International Journal of Computer Applications*, Vol.77, No. 13, 37-45, (2013).

[8] N. Kaul and N. Bajaj, Audio in Image Steganography based on Wavelet Transform. International Journal of Computer Applications, Vol.79,3,7.oN -10,(2013).

[9] Burate D. J, Performance Improving LSB Audio Steganography *Technique.* , Vol.4, No.1, 67-75, (2013)