ADVANCED LSB TECHNIQUE FOR AUDIO STENOGRAPHY

Mohammed Salem Atoum[1], Mohammad M Alnabhan[2] and Ahmad Habboush[3]

[1]Faculty of Science, Information Technology and Nursing,
Irbid National University, Irbid, Jordan
[2]Faculty of Information Technology, Mutah University
[3]Faculty of Information Technology, Jerash University

ABSTRACT

This work contributes to the multimedia security fields by given that more protected steganography technique which ensures message confidentiality and integrity. An Advanced Least Significant Bit (ALSB) technique is presented in order to meet audio steganography requirements, which are imperceptibility, capacity, and robustness. An extensive evaluation study was conducted measuring the performance of proposed NLSB algorithm. A set of factors were measured and used during evaluation, this includes; Peak Signal to Noise Ratio (PSNR) and Bit Error Rate. MP3 Audio files from five different audio generators were used during evaluation. Results indicated that ALSB outperforms standard Least Significant Bit (SLSB) technique. Moreover, ALSB can be embedding an utmost of 750 kb into MP3 file size less than 2 MB with 30db average achieving enhanced capacity capability.

KEYWORDS

MP3, LSB, Cryptography, Steganography.

1. INTRODUCTION

There is a continuous challenge in securing digital transmission between network nodes against any form of penetration and intrusion. Ensuring security of information requires considering three main components confidentially, integrity, and availability. This can be conducted through techniques, described as steganography and cryptography [1].

Cryptography is the process of encryption and decryption of a digital data. However, cryptography techniques are considered week or consume high resources. Steganography is mainly based on covering digital data in a safe digital carrier [2]. Steganography is utilized for hiding secret messages in ancient times [3]. According to [4], steganography can be described as a method of hiding secondary information (e.g. file or message) within primary information, known as the carrier or host, with no effect on the size of information and without causing any form of distortion. The information is embedded within a media expressed as a bit stream, stego signal or sequence [5].

Dhinaharan Nagamalai et al. (Eds) : CoSIT, SIGL, AIAPP, CYBI, CRIS, SEC, DMA - 2017
pp. 79– 86, 2017. © CS & IT-CSCP 2017 DOI : 10.5121/csit.2017.70409

Watermarking is another technique that is used to insert watermark into host cover to protect information such as copyright for hosts [6]. Steganography and watermarking usually embed information in host media in a transparent manner [7]. However, considering watermarking, the process requires compromising intentional attacks and preventing any cause of information destruction by insuring robustness and protecting signals quality [6]. Watermarking is the most suitable technique in scenarios where hidden information knowledge can result in information manipulations [7].

The strength of steganographic technique is based on saving the data in the carrier medium against attacks or alteration. Audio files are considered very suitable media providing different compression rates and allow performing steganography in MP3 format. Audio stenographic methods based on SLSB have gained continuous concern. However, this technique has limitations in security, capacity and imperceptibility. In addition, to date, embedding messages after audio compression has not been widely considered. Accordingly, this work investigates standard audio steganographic techniques and addresses its weaknesses and presents an Advanced Least Significant Bit (ALSB) technique in order to improve robustness and security of the standard LSB algorithm.

2. STANDARD LEAST SIGNIFICANT BIT

Standard Least significant bit (SLSB) algorithm is considered simplest steganographic method [8]. In SLSB, secret message and cover are converted to stream of bits. One or more bit of secret massage are used to replace cover LSB bits. Afterwards, bits stream are sent to the receiver which uses the same algorithm to extract the embded message [9]. SLSB uses least significant bits of the cover and utilizes sequential embedding. This result in clear suspicion secret message location within the cover files [10]. Hence, it is easier to detect and extract the secret message by the attacker [11]. In order to enhance the efficiency of SLSB algorithm security, a generator described as pseudorandom number (PN) is used [12]. However, the use of PN has incurred time limitations, because using PN requires more time to operate.

A few research works have been conducted in the area of MP3 audio steganography more specially while considering embedding after compression [11]. The cause might be the weakness of this technique in achieving a good well expansion of information data steganography, and in some cases results in low quality sound. The MP3 file is compression file that means is not flexible as well as the size is less compared to other audio file types [12]. The Embedding secret message by using after compression methods is able to create audio corruption. Two methods after compression are used to embed secret message: embedding in header frames and embedding in audio data.

2.1 EMBEDDING IN HEADER FRAMES

Before describing methods using header frames to embed secret message, MP3 file structure is explained. MP3 file is divided into header frames and audio data frames. Techniques used for encoding MP3 files are: constant bit rate CBR, average bit rate ABR and variable bit rate VBR. These methods are expected to use padding bytes. Several methods have utilized unused bits in header frames and padding bytes before all frames and between frames, in order to replace bits from secret message. However, weaknesses of these methods include; limited capacity and

security. Using padding stuffing byte technique [13], the sender converts empty information in padding byte in the cover with secret message. However, the capacity of embedded secret message depends on the size of padding byte, which was added in the cover file using encoding methods: CBR, VBR and ABR. At the receiver side, information search within stego file is applied to find the location of padding byte in the cover and extract the secret message. Unused bits in header frames such as private bit, copyright bit, original bit, and emphasis bit can be used to embed secret message without affects the quality of sound [13]. This technique replaces bit from secret message with a bit in the header. However, using this technique it is easily to extract the secret message from the header and change it from attackers.

Using Before All Frames (BAF) technique [14], researchers develop new technique to embed hole secret message before the first frames in the header. The secret message with encrypted text is embedded in a cover file, will have a maximum size of 15 KB, however the size will reach 30 KB without using encryption. This technique is better capacity compared with padding and unused bit, but also is less security without using encryption method before embedding the secret message. In addition, Between Frames (BF) methods divide the secret message before embedding it into small size cover file [14]. This method depends on the size of secret message, and on the spaces between frames of the cover file. The maximum size of secret message can be embedded is not fixed, because it can expanded the size of the cover file. The advantages of BF technique are high capacity and imperceptibility, but the disadvantages are less security and robustness. It can be concluded that all methods of header frame are facing limited robustness against attackers [14].

2.2 EMBEDDING IN AUDIO DATA:

Several methods have addressed security problems in embedding the secret message in audio data using header frames. [14] presents a new method that embeds one, two, three or four bits from MP3 file by replacing one or two or three or four bits from the secret message, described in text format. The first byte from the cover file is selected randomly. Using this method, random position in the cover file is chosen to start embedding the secret message. This is sequentially repeated to embed the secret message in the cover file. The drawback for using this method is limited robustness as well as the random position it was used is not permanent with a fixed size.

3. PROPOSED ALGORITHM

To address limitations of embedding algorithms after compression, this work introduces a new technique in LSB. The algorithm is described as Advanced Least Significant Bit (ALSB) technique, which is developed to increase the security of secret message, and improves the method of embedding the secret message in the host file. The main problem in LSB is its weaknesses against intentional or unintentional attacks on the secret message. In ALSB, the sender side uses random position selection from initial 100 byte from the host file. Moreover, the value of LSB and MSB is used to select the bit location required to be embedded in the secret message. If LSB and MSB have the same value, ALSB uses 4 bits from the secret message in order to embed from location two to five of each byte. Otherwise, the technique uses just two bits from secret message to embed it in location two and three. This methodology has increased the security of LSB. The ALSB algorithm pseudo code is discussed below:

Algorithm: Advanced Least Significant Bit Algorithm

```
1:      // H is the host file and SM is the secret message and H,SM are the inputs.
2:      // H' is the host file (H+SM) and H' is output
3:      // beginning to read host file H from initial bit and save it in H'.
4:              start
5:      For i = 1 to Size of (H) do
6:              { H'i ← Hi
7:                  }
8:   // Create random position from earliest 100 byte in the host file by
        using random generation method Rp
9:      // H' is the input
10:     //  Rp  is the output
11:                     For i=1 to 100
12:     do
13: // choosing the random byte
14:     { Rp  =   position ( i )
15:                         }
16: // begin to create H' by using ALSB technique to insert message blocks MB
17:                     For i= Rp to size of (H')
18:               do
19:     { For j=1 to L (MB)
20:             do
21:     { Read the LSB and MSB value from the byte}
22:      if the LSB+MSB  = 00 or 11 then
23:     { embed MB from 2nd to 5th position }
24:                     else if LSB+MSB= 10 or 01 then
25:                     { embed MB from 3rd to 4th }
26:             Go to next byte
27:                     }
28:             }
```

After the sender side implements ALSB technique, the stego object is constructed. To evaluate stego object before send it via internet, the PSNR and BER methods are used to introduce the results of noise in stego object. At the receiver side, inverse method is applied to predict the secret message from the stego object. This prediction is based on the secret information received from safe channel.

4. MEASUREMENT AND EVALUATION

This section describes main measurement metrics used to evaluate the proposed NLSB in terms of reliability, imperceptibility and performance. These metrics include peak signal-to-noise ratio (PSNR), and Bit Error Rates (BER). PSNR is the statistical value (ratio) that compared a signal's maximum power with power of the signal's noise, it logarithmic scale and expressed in decibels (db) [15]. However, PSNR is the peak error measure. The PSNR is error metrics used for quality measurement. The PSNR value of the new algorithm is compared with PSNR of the SLSB algorithm. Low when PSNR value is high, this describes better quality [16]. The PSNR equation is shown below:

$$PSNR = 10 \log 10 \frac{(MAX(cov(i)))^2}{MSE} \quad (1)$$

Where MAX is the maximum differentiation of the inputs (host file sample) compared with stego object in order to validate if the stego object holds secret data or not.

The second metric used is Bit Error Rates (BER) which measures bit errors in a file, beside the summation number of bits required for the spread during a time period. The BER is the statistical measures in telecommunication transmission, the ratio result is percentage of a bit including errors comparing to entire bits. This measure is expressed as ten to a negative power. If the results is low data rate that means is very high in a transmission [15]. In addition, the BER is a measure of bit error probability. BER is considered more accurate while considering increased number of bit errors and long interval. BER is also used to measure the successful recovery of the hidden information. This will have its high effect in real communication channel where errors exists retrieving hidden information. BER is computed as described in the following equation:

$$BER = \frac{1}{Z(cov)} * \sum_{i=0}^{L(H)} (H(i) - H'(i)) \quad (2)$$

Where L is the length, H is host file and H' is stego object.

Table 1 describes audio generators used during the experiment and explains specifications of each audio file including duration in minutes and size in Mbps. These audio clips were used in the evaluation study to measure the effectiveness of the proposed ALSB technique comparing to Standard LSB (SLSB) and XLSB techniques.

Table 1. Audio file specifications

Name of Audio generator	Time (Minute)	Size under 320kbps (MB)
Pop	3:10	8.9
Rock	3:40	9.9
Blues	3:45	10.7
Hip-hop	4:30	12.4
Dance	5:30	14.2
Metal	7:00	14.8

As shown in table 2, proposed ALSB achieved high PSNR values comparing to SLSB [17] and eXtended LSB (XLSB) methods [18] for all audio files. XLSB was presented and evaluated in [18]. While performing a T-Test between PSNR values of ALSB and SLSB the result in (p=0.00088), which indicates a significant difference between these PSNR values with an advantage to ALSB. Moreover, the BER result confirmed that the proposed ALSB over performed SLSB and XLSB. ALSB algorithm achieved the lowest BER values comparing to other algorithms. T-test between BER values of ALSB and SLSB results in (p = 0.0000735103), which ensures a significant difference between BER values with an advantage to ALSB. Accordingly, the proposed ALSB achieved high performance and outperformed SLSB algorithms.

Table 2 PSNR and BER results

Name of Audio generator	XLSB PSNR	SLSB PSNR	ALSB PSNR	XLSB BER	SLSB BER	ALSB BER
Pop	67.0086	61.1675	69.0515	0.04	0.05	0.0025
Rock	66.758	61.9193	68.0656	0.038	0.041	0.0024
Blues	67.9554	62.4768	68.5194	0.037	0.04	0.0024
Hip-hop	58.8168	62.8794	59.9845	0.035	0.038	0.0022
Dance	65.2817	62.7883	66.4976	0.034	0.037	0.002
Metal	66.8681	62.9386	67.8172	0.031	0.034	0.0019

Figures 1 and 2 illustrate the PSNR and BER results for XLSB, SLSB and ALSB techniques.

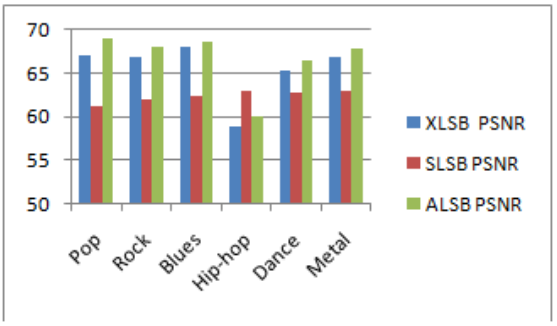

Figure1. PSNR Comparison Results

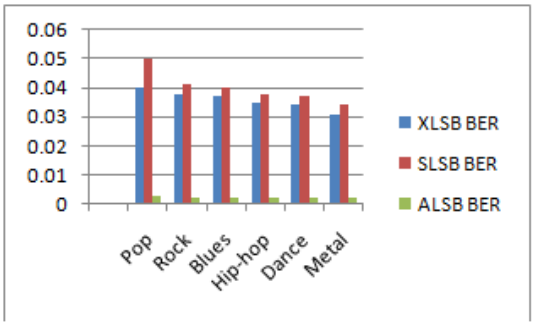

Figure2.BER Comparison Results

5. CONCLUSIONS

This paper has investigated audio steganography, particularly with respect to MP3 files after compression. In this concern, a new algorithm known as Advanced least significant bit algorithm (ALSB) was presented aiming to meet audio steganography requirements including; imperceptibility, capacity, and robustness. The proposed ALSB enhances steganography efficiency, by not embedding the message in every byte of audio file. Alternatively, the location of the first bit to be embedded is selected randomly and remaining bits are embedded considering odd and even byte values in the audio file.

ALSB algorithm is considered an extension of standard least significant bit (SLSB). SLSB holds sufficient information about cover format bits which are not manipulated. This increased errors or distortions. In this work, ALSB was implemented and evaluated with comparison to SLSB. Measurements and results indicated that in ALSB achieved improved capacity and increased PSNR values (as imperceptibility representative) comparing to other methods such as SLSB and XLSB. In addition, ALSB has shown an increased robustness against attacks by applying BER. Accordingly, experiments show that ALSB method achieves increased average of capacity, improved imperceptibility and advanced robustness.

REFERENCES

[1] Lentij J., "Steganographic Methods", Department Of Control Engineering And Information Technology, Budapest University. Periodica Poltechnica Ser. El. Eng. Vol.44, No. 3–4, P. 249–258 (2000), Url: Http://Www.Citesseer.Ist.Psu.Edu/514698.Html.

[2] Katzenbeisser S., Peticotas F., "Information Hiding Techniques For Steganography And Digital Watermarking", Artech House Inc.2000.

[3] Petitcolas F.A, Anderson R.J., Kuhn M.G., "Information Hiding – A Survey", Ieee, Special Issue On Protection Of Multimedia Content: 1062-1078, July, 1999.

[4] Cacciaguerra S., Ferretti S., "Data Hiding: Steganography And Copyright Marking", Department Of Computer Science, University Of Bologna, Italy, Url: Http://Www.Cs.Unibo.It/~Scacciag/Home-File/Teach/Datahiding.Pdf.

[5] Nedeljko C. (2004). Algorithms For Audio Watermarking And Steganography. Acta Universitatis Ouluensis. Series C., 2004..

[6] Andres G. (2002). Measuring And Evaluating Digital Watermarks In Audiofiles. Washington Dc. 2002.

[7] Andres G. (2002). Measuring and Evaluating Digital Watermarks in Audio Files. Washington DC. 2002.

[8] Nematollahi, Mohammad Ali, Chalee Vorakulpipat, and Hamurabi Gamboa Rosales. "Audio Watermarking." Digital Watermarking. Springer Singapore, 2017. 17-38…..

[9] Shrivastav, Vijay. "A study of different steganographic methods." Journal of Digital Integrated Circuits in Electrical Devices 2.1 (2017): 1-6.

[10] Arab, Farnaz, and Mazdak Zamani. "VW16E: A Robust Video Watermarking Technique Using Simulated Blocks." Multimedia Forensics and Security. Springer International Publishing, 2017. 193-221.

[11] Atoum, Mohammed Salem. "A Comparative Study of Combination with Different LSB Techniques in MP3 Steganography." Information Science and Applications. Springer Berlin Heidelberg, 2015. 551-560..

[12] Atoum, M. S., Suleiman, M., Rababaa, A., Ibrahim, S., & Ahmed, A. (2011). A Steganography Method Based on Hiding secrete data in MPEG / Audio Layer III. Journal of Computer Science, 11(5), 184-188 [12] Deng, K., Tian, Y., Yu, X., Niu, X., Yang, Y., & Technology, S. (2010). Steganalysis of the MP3 Steganographic Algorithm Based on Huffman Coding. Test, (1), 79-82

[13] L. Maciak And M. Ponniah And R. Sharma, "Mp3 Steganography", 2008.

[14] Atoum, Mohammed Salem, Subariah Ibrahimn, Ghazali Sulong, Akram Zeki, and Adamu Abubakar. "Exploring the challenges of MP3 Audio steganography." In Advanced Computer Science Applications and Technologies (ACSAT), 2013 International Conference on, pp. 156-161. IEEE, 2013. Bhattacharyya, S., Kundu, A., Chakraborty, K., & Sanyal, G. (2011). Audio Steganography Using Mod 4 Method. Computing, 3(8), 30-38.

[15] Bhattacharyya, S., Kundu, A., Chakraborty, K., & Sanyal, G. (2011). Audio Steganography Using Mod 4 Method. Computing, 3(8), 30-38.

[16] El-Bendary, Mohsen AM. "FEC merged with double security approach based on encrypted image steganography for different purpose in the presence of noise and different attacks." Multimedia Tools and Applications (2017): 1-39.

[17] AbedulsalamAlarood, Alaa, et al. "HIDING AMessage IN MP3 USING LSB WITH 1, 2, 3 AND 4 BITS." International Journal of Computer Networks & Communications (IJCNC) Vol.8, No.3, May 2016.

[18] Atoum, M.S, " MP3 audio steganography techniqu using extended least significant bit", Thesis (Ph.D (Sains Komputer)) - Universiti Teknologi Malaysia, 2014.