Jurnal Teknologi

Full paper

A New Method to Increase the Capacity of Audio Steganography Based on the LSB Algorithm

Mohsen Bazyar, Rubita Sudirman*

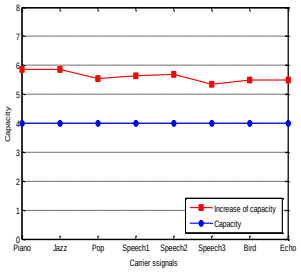
Faculty of Electrical Engineering, University Teknologi Malaysia, 81310 UTM Johor Bahru, Malaysia

*Corresponding author: rubita@fke.utm.my

Article history

Received : 25 March 2015
Received in revised form :
11 April 2015
Accepted : 13 April 2015

Graphical abstract



Abstract

Audio techniques have been developed for audio streaming on the internet. Using the TCP/IP protocol, audio file can be uploaded, downloaded, and transmitted through the internet. This benefit of transmission makes the interest in using audio as cover object in steganography become much stronger. Capacity which is one of the most important properties of audio steganographic methods, evaluates the amount of possible embedding data within the audio file. A new embedding technique of audio steganography is proposed to increase the carrier medium capacity for substitution additional hidden message. With respect to the performed tests, the algorithm succeeds to increase the depth of embedding layer, without having effects on the signal transparency. The maximum number of bits without significant effect on host audio signal for LSB audio steganography is 4 LSBs. The secret message bits are hidden into variable and multiple LSBs layer in this method. Experimental results show that the use of this new technique which apply 7 LSBs for data embedding in comparison the LSB standard algorithm with 4 LSBs improve data hiding capacity of carrier audio by 35% to 55%. It can be observed from listening tests that there is no significant difference between the stego audio acquired from the novel technique and the main signal.

Keywords: Audio steganography; most significant bit (MSB); embedding data; least significant bit (LSB)

Abstrak

Teknik audio yang telah dibangunkan untuk streaming audio di internet. Menggunakan protokol TCP/IP, fail audio boleh dimuat naik, turun, dan dihantar melalui internet. Manfaat penghantaran ini menjadikan kepentingan dalam menggunakan audio sebagai objek perlindungan di steganografi menjadi lebih kuat. Kapasiti yang merupakan salah satu sifat yang paling penting dalam kaedah steganografi audio, menilai jumlah data yang boleh dibenamkan dalam fail audio. Satu teknik baru pembenaman steganografi audio adalah dicadangkan untuk meningkatkan kapasiti pengangkut sederhana untuk penggantian mesej tersembunyi tambahan. Berkenaan dengan ujian yang dijalankan, algoritma berjaya untuk meningkatkan kedalaman menerapkan lapisan, tanpa mempunyai kesan ke atas ketelusan isyarat. Bilangan maksimum bit tanpa kesan yang ketara kepada hos isyarat audio untuk LSB steganografi audio adalah 4 LSBs. Bit mesej rahsia tersembunyi ke dalam LSBs berubah-ubah dan pelbagai lapisan dalam kaedah ini. Hasil uji kaji menunjukkan bahawa penggunaan teknik baru ini yang terpakai 7 LSBs untuk membenamkan data dalam perbandingan algoritma LSB standard dengan 4 LSBs memperbaiki data bersembunyi kapasiti pengangkut audio sebanyak 35% kepada 55%. Ia dapat dilihat dari mendengar ujian yang tidak terdapat perbezaan yang signifikan di antara audio stego yang diperoleh daripada teknik novel dan isyarat utama.

Kata kunci: steganografi Audio; bit yang paling penting (MSB); membenamkan data; bit paling kurang penting (LSB)

1.0 INTRODUCTION

The act of being able to hide imperceptible information within digital media has become an area of increasing interest in the computing world. Data hiding techniques have many potential purposes such as watermarking, covert communication, hiding executable data and digital rights management (DRM). The method used to conceal data for all of the above situations is called steganography [1]. Steganography, which literally means "concealed writing", is a method of covert communication that has existed for thousands of years. Today steganography has been adapted to the digital era and can be implemented in pictures, audio, text and even other forms of digital multimedia as well. In addition, digital steganography has two rudimentary requirements that must be fulfilled. The first requirement is that the stego object is virtually imperceptible to any third-parties who may obtain the file or files; whereas the second requirement is that there must be a reasonably high bandwidth for the stego-data.

Steganography, as art of hiding information, has been known for over 2500 years. Back then steganography was mainly used for diplomatic, military and a very few people used it for personal purposes along with cryptography. Steganography as well as cryptography has a goal to secure transmitted information between the sender and the recipient, but both systems are used in a different way [2-3]. Cryptography is aimed on transformation of input data into unreadable output. The level of information security depends on the quality of cryptographic algorithm and correct cipher key selection. Steganography has a different approach, stegomessages also referred as steganograms are made in such a way that they do not attract attention to themselves [4].

Cryptography and steganography are normally related with each other. Cryptography is effective in the utilization of the secret message and the key is a kind of coded. If it is sent insecurely, an attacker will detect it immediately and will attempt to decode it. However, a steganographic system is available that helps to improve the secure transfer of encoded information [5]. These systems code a secret message within a picture or other multimedia file. If you see a steganographic picture, you will not recognize the secret message inside of the picture. And this is the point. Attackers will go through and will not pay attention to the message. Digital steganography involves the use of two entities that make up the transfer file. The first entity is the cover object, which is the overt data being sent, and the second entity is the stego object, which is the secret or covert message embedded in the cover object [6].

In this internet era, digital media are commonly transferred over the internet both through individual file transfer and streaming of raw data. Given these new developments there has been an increasing focus on embedding hidden information into audio. There are several classic ways that are used to hide information in audio. Least Significant bit (LSB) encoding, echo hiding, phase coding, and spread spectrum coding are among the most common techniques used [7-8]. Embedding hidden data in audio signal is a more complicated process than embedding data in other media like images or video. Furthermore, since the audio sequences have one dimension less than 2-dimensional video or image files, the data capacity, which could be concealed inside an audio signal is considerably lower than the amount of information which could be concealed within video or image files. This article proposes a new method that considerably increases the capacity of carrier audio in comparison with the LSB standard algorithm without any remarkable effect on transparency of encoded audio signal [9].

Remaining of this paper is organized as follows. In the next section we described the standard LSB method. Then, we explained our proposed method, followed by discussing the experimental results.

■2.0 AUDIO STEGANOGRAPHY METHODS

2.1 Echo Hiding

This method adds an echo to the main audio signal to embedding information within an audio file. Three echo parameters that are important to embedding data: decay rate, offset and initial amplitude. Just one bit of information can be encoded, If only one echo is created from the original signal. It becomes more difficult for the human ear to separate among the two signals as the delay decrease between the echo and the original audio. Furthermore, offset to show the binary message is varied. A binary one shows by the first offset, and binary zero shows by a second offset value. Just one information bit can be encoded, if just one echo from the original signal is created. Thus, before starting the encoding process the original signal is broken into the blocks. The blocks are combined together when the encoding process is finished to produce the last signal [10].

2.2 Phase Coding

Depends on the fact that the phase components of sound unlike the noise are not comprensible to the human auditory system and it addresses the disadvantages of the noise based approaches of audio Steganography. Phase coding works by replacing a reference phase which shows the information with the initial audio phase segment, example is shown in Figure 1. To keep the relative phase among the segments the phase of other segments is adjusted [11]. Overall, this technique substitutes a reference phase that represents the hidden data with the phase of an initial audio segment. This can be consider as an encryption which is nothing more than a transformation algorithm for the audio signal by using Discrete Fourier Transform (DFT). Having low data transmission rate and complexity are disadvantages of this method.

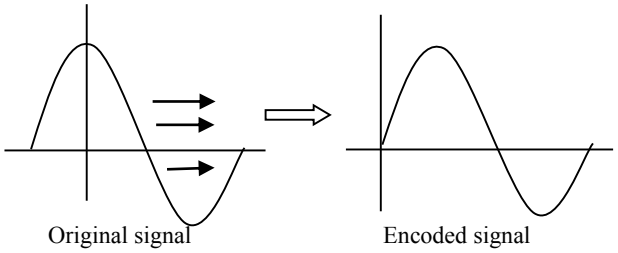


Figure 1 Phase coding

2.3 Spread Spectrum

Frequency-hopping schemes and the direct-sequence are two versions of Spread spectrum which can be used in audio Steganography. It tries to spread out the encoded information throughout the existing frequencies as far as it possible. It is like a system that uses the LSB coding implementation which spreads the bits of the message over the audio file randomly. On the other hand, the SS technique, unlike the LSB method, spreads out the hidden message throughout the frequency spectrum of audio file utilizing a code which is independent on actual signal and plays an important role in military, secure communications and commercial [12].

■3.0 STANDARD LSB ALGORITHM

In the scope of steganography, LSB algorithm is one of the best methods to analyze information hiding. In this method least significant of binary sequences of each digitized audio sample is replaced with the secret message binary equivalent LSB coding permits to a large amount of information to be encoded by replacing a binary message with the least significant bit of each sampling point [13-14]. For instance, for embedding the sample value of '1000001' which is equivalent to letting 'A' into an audio signal that each sample are introduced with 16 bits, after that, least significant bit of 7 sequential samples are substituted with each bit of the binary equivalent of the letter 'A'. 1 kbps per 1 kHz is the

ideal data transmission rate in LSB coding. Therefore, before choosing the LSB we must consider the used signal content. For instance, an audio file would mask low-bit encoding noise when it was recorded in a busy subway station [15]. However, the same noise would be heard in an audio file including a piano. The recipient requires access to the sample indices sequence to extract hidden information inside an LSB encoded audio file which utilize in the embedding step. One must determine then on how to select the subset of samples that will consist of hidden information and connect that decision to the receiver [16]. A simple method is to begin at the start of the audio signal and carry out LSB technique until the secret message has been totally concealed and leave the remaining samples without any change. It generates a security problem; anyway, statistical feature of the second component of the audio file which was not modified is different Compared with the first component of the audio file.

It is clear that the human auditory system (HAS) is very sensitive to additive white Gaussian noise (AWGN) and the random choose of the samples applied for hiding introduces low power AWGN. This fact limits the number of LSBs which can be imperceptibly modified during embedding. Use of only one LSB of the host audio sample gives capacity of 44.1 kbps [17]. This is the main advantage of the LSB coding method and a low computational complexity. According to this fact that simple random changes of the LSBs destroy the coded, the clear disadvantage is low robustness. Probability of making the hidden secret message statistically increases as the depth of the modified LSB layer becomes larger or the number of used LSBs during LSB encoding increases. Perceptual transparency of stego audio is decreased by increase the depth of LSB layers. Thus, there is a limit for the depth of the used LSB layer in each sample of host audio that can be applied for information embedding. Hence, robustness improvement of steganography obtained by the depth increment of the used LSB layer is limited by perceptual transparency that is the 4th LSB layer for the standard LSB algorithm [18].

■4.0 PROPOSED LSB ALGORITHM

A new method is proposed in this study, which is able to shift the limit from the fourth LSB layer to the seventh LSB layer for transparent data hiding in the audio file.

4.1 Data Embedding

At the data embedding process, a data hidden bit is embedded into the ith LSB layer of the host audio using a new LSB coding method. This algorithm chooses the LSBs number of data embedding based on the values of MSBs of corresponding samples after checking the MSBs of the carrier audio samples. Variable and multiple LSBs are utilized for embedding the secret message in this approach.

The algorithm succeeds to increase the depth of embedding layer which is assumed to be 4 LSBs for LSB standard, without having effects on the signal transparency. Capacity of data embedding is remarkably increased in the case of the new method compared to the standard LSB algorithm.

The first two Most Significant Bits (MSBs) values of the carrier audio samples are checked for information hiding by this technique [19]. Embedding process based on the MSB is shown in Table 1. The first step of the process is to read the carrier audio. Then, convert the audio signal into a sequence of binary bits after reading it in second step.

Table 1 Embedding process using 2 MSBs

Most significant bit		Number of LSBs
1	2	
0	0	4
0	1	5
1	0	6
1	1	7

Then in third step, every data bit obtained from step 2 is hidden into the multiple and variable LSBs of the digitized carrier audio samples. First 2 MSBs of the samples of the carrier audio are checked for embedding purpose as follow:

- 4 LSBs are used for embedding if 2 MSBs are '00'.
- 5 LSBs are used for embedding if 2 MSBs are '01'.
- 6 LSBs are used for embedding if 2 MSBs are '10'.
- 7 LSBs are used for embedding if 2 MSBs are '11'.

At the end, the modified samples of carrier audio signal are written to the stego audio signal forming.

Table 2 Samples distribution of proposed algorithm

Carrier audio	Samples with first two MSBs (%)			
	00	01	10	11
Piano	0.35	37.34	26.45	0.26
jazz	0.09	29.98	54.78	0.07
Pop	0.21	72.39	23.13	0.08
Speech1	8.75	51.22	89.11	11.98
Speech2	11.43	46.80	55.43	13.70
Speech3	12.22	48.65	55.76	9.87
Bird	0	33.98	30.06	0
Echo	0	67.87	30.13	0
Average	4.1312	48.5248	45.6062	4.495

Table 3 Proposed technique results

Carrier audio	SNR	PSNR	MSE	Increase of capacity	Increase of capacity (%)
Piano	54.32	154.76	5.66×10^{-7}	5.87	144.34
Jazz	51.09	150.02	6.03×10^{-7}	5.85	145.65
Pop	50.69	151.15	8.34×10^{-7}	5.54	144.01
Speech1	71.03	160.16	2.45×10^{-6}	5.65	142.16
Speech2	70.66	160.65	2.76×10^{-6}	5.68	142.46
Speech3	70.08	161.02	2.12×10^{-6}	5.34	141.33
Bird	62.12	158.16	1.89×10^{-7}	5.5	144.45
Echo	67.44	158.98	4.92×10^{-7}	5.5	146.67
Average	62.18	156.86	4.27×10^{-7}	5.62	144.26

4.2 Data Extraction

After data embedding process, data extraction steps will be explained in this section: the first 2 MSBs of the carrier audio samples are checked for data bits extraction after reading the stego audio file.

- 4 LSBs are extracted if 2 MSBs are '00'.
- 5 LSBs are extracted if 2 MSBs are '01'.
- 6 LSBs are extracted if 2 MSBs are '10'.
- 7 LSBs are extracted if 2 MSBs are '11'.

Finally the hidden audio message is reconstructed after each 16 data bits are extracted and converted to decimal equivalents. Equation (1) estimates the proposed method capacity.

$$CA = F4*4 + F3*5 + F2*6 + F1*7 \quad (1)$$

where CA is capacity increment; and the samples probabilities with the first two MSBs as '00', first two MSBs as '01', first two MSBs as '10' and first two MSBs as '11'are shown by *F4, F3, F*2 and *F1* respectively.

Equation (2) shows the percentage capacity increment:

$$CAP = (CA / B)*100 \quad (2)$$

Here, B = 4 bits/sample

Estimate of capacity increment, which is shown with *CAE* and given by Equation (3), calculate when all the 4 probabilities are equi-probable, that is *F1*, *F2*, *F3* and *F4* are 0.25:

$$CAE = 0.25*4 + 0.25*5 + 0.25*6 + 0.25*7 = 5.4 \quad (3)$$

The above equation shows the estimate of capacity increment of carrier audio signal using the proposed algorithm. The percentage of samples distribution of carrier audio files used for proposed approach is given in Table 2.

Referring to Table 2, the most number of the samples have values of '10' and '01' at the first 2 MSBs. Based on the last row in Tabl2 2, which shows the percentage of average values of the samples, 48.52 and 45.61 are the average percentage of samples with the first 2 MSBs as '01' and '10' respectively. Both of them consist of about 95% of the samples, it means the other combinations of MSBs ('11' and '00') can be ignored because they have included a very low percentage of samples. Therefore, only the MSB of the samples can be considered. Combination of '11' and '10' is based on considering only MSB which is 1. Combination of '00' and '01' is based on considering only MSB which is 0. This obviously shows that only by considering the Most Significant Bit (MSB) of the carrier samples would be enough to extend the proposed algorithm.

5.0 EXPERIMENTAL RESULTS

Different types of audio files are used in this study to evaluate the effectiveness of the proposed algorithm. These files are included the sounds of music, speech, and animals which are tested on ten audio signal sequences. Duration of each audio segment by 16 bits per sample is changed from 2 to 8 seconds with different sampling frequencies (44100 Hz, 22050 Hz and 110025 Hz). Signal-to-Noise Ratio (SNR), Mean Squared Error (MSE), Peak Signal-to- Noise Ratio (PSNR) Are three parameters to analyze the proposed method's performance. Increase of carrier audio capacity in terms of bits per sample. The evaluation of proposed algorithm quality has been done by listening tests including eight persons. It can be observed from listening tests that there is no significant difference between the stego audio acquired from the novel technique and the main signal.

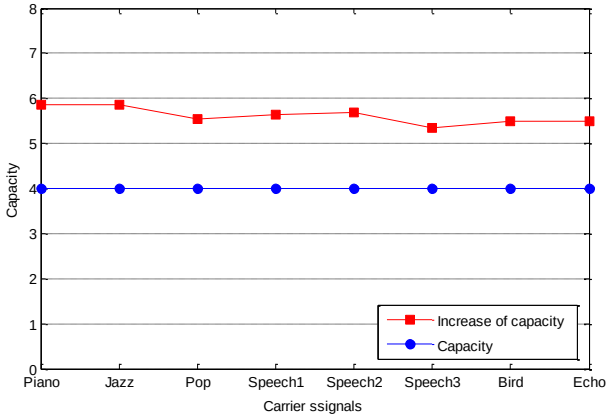


Figure 2 Evaluation of capacity in proposed LSB algorithm and LSB standard

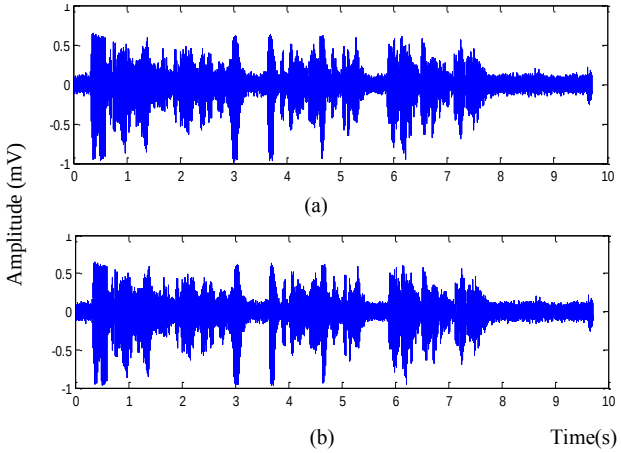


Figure 3 Carrier audio and stego audio signal using proposed method; (a) before, (b) after LSB algorithm

According to Table 3 that showed the proposed algorithm results, 146.6% is the highest increase the percentage of capacity which used two MSBs for capacity increment of the carrier audio file. The estimated capacity increment for proposed algorithm was computed to be 5.5 using Equation (3). It is clear from Table 3 that for all carrier audio signals, the capacity increment is near or more than this estimated value. The average value of capacity increment is 5.62.

The evaluation of capacity increment for both LSB standard algorithms which used 4 LSBS for embedding and proposed algorithm using 2 MSBs is shown in Figure 2. Figure 3 indicates the plotting of the carrier audio signal stego signal obtained after

using the proposed algorithm. There is not any difference observed in the stego audio acquired from the proposed methods in comparison to the carrier audio signal. This indicates that the embedding process is successful.

6.0 CONCLUSION

A new method has been proposed in this article to increase the capacity of data embedding of carrier audio. This method hides information in variable and multiple LSBs based on the MSBs of the samples of the carrier audio in comparison with the standard LSB technique. 2 MSBs of the samples of carrier audio file are checked in this study. Experimental results show a significant increase in carrier audio capacity for embedding additional information without having effects on the signal transparency of the host audio. As compared to the capacity of the original signal (4 bits per sample), the average increase in carrier audio capacity is by 5.61 (bits per sample) Using the proposed method based on 2 MSBs. It has been seen from listening tests that there is no remarkable difference between cover and stego audio file in the perceptual quality. Hidden data recovery without any error and no complicated calculations are the main advantages of the proposed algorithm.

Acknowledgement

The authors would like to thank Universiti Teknologi Malysia for funding the research under vot 05H37. We also would like to thank our research group in supporting and giving positive comment to improve our paper.

References

[1] P. Jayaram, H. R. Ranganatha, and H. S. Anupama. 2011. Information Hiding using Audio Steganography–A Survey. *International Journal of Multimedia & Its Applications (IJMA)*. 3: 89–96.

[2] M. M. Amin, M. Salleh, S. Ibrahim, M. R. Katmin and M. Z. I. Shamsuddin. 2003. Information Hiding using Steganography. 4th National Conference on Telecommunication Technology. 21–25.

[3] M. Bazyar and R. Sudirman. 2014. A Recent Review of MP3 Based Steganography Methods. *International Journal of Security and Its Applications*. 8(6): 405–414.

[4] S. Narayana and G. Prasad. 2010. Two New Approaches for secured image Steganography using cryptographic Techniques and Type Conversions. *International Journal of Signal & Image Processing*. 1: 60–73.

[5] M. S. Atoum, M .S. Al Rababaa, D. S. Ibrahim and O. A. Ahmed. 2011. A Steganography Method Based on Hiding Secrete Data in MPEG/Audio Layer III. *Journal of Computer Science*. 11(5): 184–188.

[6] A. Delforouzi and M. Pooyan. 2008. Adaptive Digital Audio Steganography Based on Integer Wavelet Transform. *Circuits, Systems & Signal Processing*. 27(2): 247–259.

[7] F. Djebbar, B. Ayad, H. Hamam and K. Abed-Meraim. 2011. A View on Latest Audio Steganography Techniques. International Conference on Innovations in Information Technology (IIT). 409–414.

[8] H. B. Kekre, A. Athawale, S. Rao, and U. Athawale. 2010. Information Hiding in Audio Signals. *International Journal of Computer Applications*. 7(9): 14–19.

[9] B. A. Patil and V. A. Chakkarwar. 2013. Review of an Improved Audio Steganographic Technique over LSB through Random Based Approach. *Consumer Electronics, IOSR Journal of Computer Engineering (IOSR-JCE)*. 7(9): 30–34.

[10] H. Matsuoka, 2006. Spread Spectrum Audio Steganography using Sub-Band Phase Shifting. International Conference on Intelligent Information Hiding and Multimedia Signal Processing. 3–6.

[11] W. H. Zeng and H. Ruimin Hu, 2007. A Novel Steganalysis Algorithm of Phase Coding in Audio Signal. Sixth IEEE International Conference on Advanced Language Processing and Web Information Technology. 261–264.

[12] S. Shlien. 1994. Guide to MPEG-1 Audio Standard. *IEEE Transactions on Broadcasting*. 40(4): 206–218.

[13] S. Dumitrescu, X. Wu and Z. Wang. 2003. Detection of LSB Steganography Via Sample Pair Analysis. *IEEE Transactions on Signal Processing*. 51(7): 1995–2007.

[14] P. K. Singh and R. K. Aggrawal. 2010. Enhancement of LSB Based Steganography for Hiding Image in Audio. *International Journal on Computer Science and Engineering*. 2(5): 1652–1658.

[15] M. A. Ahmed, M. L. M. Kiah, B. B. Zaidan and A. A. Zaidan. 2010. 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 Science*. 10(7): 59–64.

[16] C. Parthasarathy and D. S. Srivatsa. 2005. Increased Robustness of LSB Audio Steganography by Reduced Distortion LSB Coding. *Journal of Theoretical and Applied Information Technology*. 7(1): 80–86.

[17] N. Cvejic and T. Seppanen. 2002. Increasing the Capacity of LSB-Based Audio Steganography. IEEE Workshop on Multimedia Signal Processing. 336–338.

[18] M. Asad, J. Gilani and A. Khalid. 2011. An Enhanced Least Significant Bit Modification Technique for Audio Steganography. International Conference on Computer Networks and Information Technology (ICCNIT). 143–147.

[19] K. Gopalan, 2003. Audio Steganography using Bit Modification. Proceedings of International Conference on Multimedia and Expo. 1: 629–632.