Journal of Information Security, 2015, 6, 161-165
Published Online July 2015 in SciRes. http://www.scirp.org/journal/jis
http://dx.doi.org/10.4236/jis.2015.63017

Scientific Research Publishing

Which Bit Is Better in Least Significant Bit?

Fatin E. M. Al-Obaidi, Ali Jassim Mohamed Ali

Department of Physics, College of Science, Al-Mustansiriyah University, Baghdad, Iraq
Email: fatinezzat@yahoo.com, sci.phy.fam@uomustansiriyah.edu.iq

Received 9 April 2015; accepted 11 May 2015; published 14 May 2015

Abstract

The weakness of Human Auditory System (HAS) led the audio steganography process to be used in hiding data in the digital sound. Audio steganography is implemented here by using Least Significant Bit (LSB) algorithm to hide message into multiple audio files. This is achieved by 1st, 2nd, 3rd, and 4th bits hiding ratios. In comparison to other used bits, hiding results show that the use of 1st bit in LSB method for embedding data is much better than those used bits as expected. In addition to that and according to the results, file's size affects strongly upon the effectiveness of the embedding process while hiding starting position doesn't affect upon the variation of the adopted statistical estimators regardless to which bit is used. Among the statistical estimators that have been adopted here, the Mean Absolute Error (MAE) seems to be the best one in testing hiding process.

Keywords

Audio Steganography, LSB Method, PSNR, MAE

1. Introduction

The process of embedding secret messages into digital sound is known as audio steganography [1]. The basic model of audio steganography consists of carrier (audio file) known as a cover-file, message and password (stego-key) as shown in **Figure 1**. The cover file conceals the secret information (data). Message is the embedded information that sender wants to be confidential. This message can be represented as an image, audio, plain text or any other file's type [2] [3]. A stego-key is a private key which is used to embed the message in the cover audio file and hence the stego-file is created once the message hidden successfully in the cover audio file [3]. The most popular file formats for sounds which have been used are the Windows Audio Visual (WAV) and the Audio Interchange File Format (AIFF) [4].

Embedding techniques are chosen according to requirement. Some of these are LSB coding, parity coding, spread spectrum phase coding and echo hiding [5].

How to cite this paper: Al-Obaidi, F.E.M. and Ali, A.J.M. (2015) Which Bit Is Better in Least Significant Bit? *Journal of Information Security*, **6**, 161-165. http://dx.doi.org/10.4236/jis.2015.63017

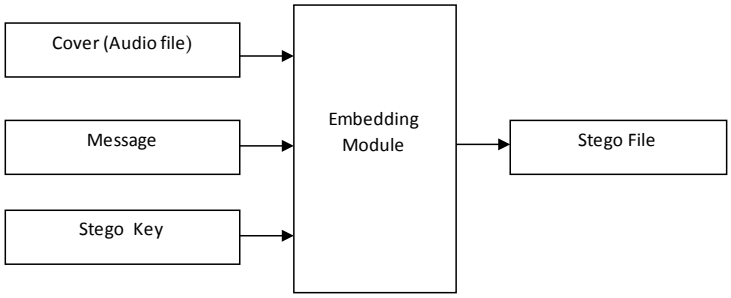

Figure 1. Basic audio steganographic model [2].

Because of its highest capacity for data and the easiest way to implement in comparing with the other techniques, Least Significant Bit (LSB) method has been adopted in this research.

2. Least Significant Bit

Least Significant Bit (LSB) technique is one of the simplest approach for secure data transfer. In this technique, LSB of binary sequences of each sample of digitized audio file is replaced with the binary equivalent of the secret message [4].

To hide the letter "D" as an example which has the ASCII code equal to 68 that is 01000100 inside eight bytes of a cover, the process of LSB can be shown as follow [6].

Original Audio Bytes		Text data to hide		Text data Embedded Audio Bytes
10010010		**0**		**1001001**0
01010011		**1**		**0101001**1
10011011		**0**		**1001101**0
11010011	⇒	**0**	⇒	**1101001**0
10001010		**0**		**1000101**0
00000010		**1**		**0000001**1
01110010		**0**		**0111001**0
00101011		**0**		**0010101**0

3. Proposed Work

Among different approaches to hide a secret message inside an audio file, LSB coding method is proposed. This can be achieved by replacing the first, second, third and fourth bit of the audio file (.WAV format) respectively with its equivalent bit in the binary message. This process begins from the starting hiding position which is only known by the encrypted and recipient persons. Hiding results have been examined through some statistical estimators [7]-[11].

I. Signal-to-Noise Ratio (SNR)

It is used as a measure of quality reconstruction of the audio file, given by

$$\text{Signal-to-noise rato expressed in dB} \equiv \text{SNR} = 10\frac{\log_{10}\left[\dfrac{\sum_{i=0}^{n-1}\left[r(i)\right]^2}{\sum_{i=0}^{n-1}\left[r(i)-t(i)\right]^2}\right]}{\log 10} \quad (1)$$

where $r(i)$, $t(i)$ are the values of the i^{th} samples in the original and stego audio file, respectively, n is the audio file's length.

II. Peak Signal-to-Noise Ratio (PSNR)

The PSNR is the ratio between maximum possible power and corrupting noise that affect the representation of the audio file. In this case, the signal is the original audio file and the noise is the produced error for the embedding process. The PSNR is given by;

$$\text{Peak signal-to-noise rato represented in dB as} \equiv \text{PSNR} = 10\frac{\log_{10}\left[\dfrac{\max\left(r(i)\right)^2}{\frac{1}{n}\sum_{i=0}^{n-1}\left[r(i)-t(i)\right]^2}\right]}{\log 10} \quad (2)$$

The high values of SNR and PSNR indicates the high security, because they indicate the minimum difference between the original and the stego values.

III. Root Mean Square Error (RMSE)

It is used to quantify the difference between values implied by the original and the stego files. The RMSE is defined as;

$$\text{Root mean square error} \equiv \text{RMSE} = \sqrt{\frac{1}{n}\sum_{i=0}^{n-1}\left[r(i)-t(i)\right]^2} \quad (3)$$

IV. Mean Absolute Error (MAE)

It is the difference between the original and stego values. So, no one can suspect the presence of any hidden information. The MAE is given by;

$$\text{Mean absolute error} \equiv \text{MAE} = \frac{1}{n}\sum_{i=0}^{n-1}\left[r(i)-t(i)\right] \quad (4)$$

The low values of RMSE and MAE indicate the high security, because they include the minimum difference between the original and new audio files.

4. Results and Discussions

The algorithm for LSB has been successfully tested through embedding a message into multiple wave audio files of various sizes which can be summarized in **Table 1**. According to HAS, no one can distinguishes the present of any difference between the cover (original) and the stego file.

Histograms for the audio wave file before and after coding are shown in **Figure 2(a)** and **Figure 2(b)**, **Figure 2(d)** and **Figure 2(e)** while the difference between them is represented in **Figure 2(c)** and **Figure 2(f)** for the case of 1st & 4th bits respectively.

The symmetric with periodic behaviors for the difference between the two histograms can be seen clearly for the case of using 1st bit, while it isn't the case for 4th bit in LSB. **Figure 3** illustrates the variation of the adopted statistical estimators with LSB bit's position. As expected and according to **Figure 3** and **Figure 4**, the use of 1st bit in LSB technique is better than other used bits. Regardless to which bit is used, embedding a secret message inside the largest file's size which have been examined here is better than with smallest one. This can be distinguished clearly through **Figure 4**.

For the first audio file, the process of hiding a secret message inside different positions of the audio wave file has been executed. Results show that starting hiding position doesn't affect upon the variation of the statistical estimators regardless to which bit is used. This can be seen clearly from **Figure 5**.

In all figures, a similar behavior with equally spaced curves can be seen obviously for all SNR and PSNR variations. On the other hand, an increasing gap has been noticed between MAE and RMSE variation curves. In addition to the previous notice and according to its lowest value, MAE seems to be the best statistical estimator in testing hiding process.

Table 1. Information of the adopted audio files.

File's size	Audio's file name
3338	Test1
44408	Test2
23992	Test3
21816	Test4

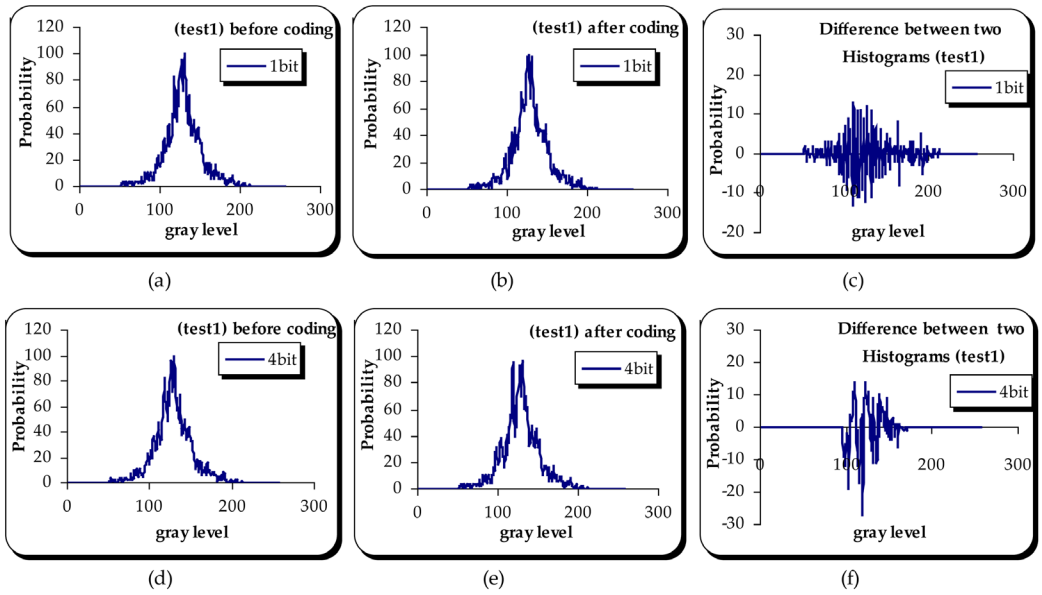

Figure 2. Results for LSB technique. (a), (b), (c) for the case of 1bit; (d), (e), (f) for the case of 4 bit.

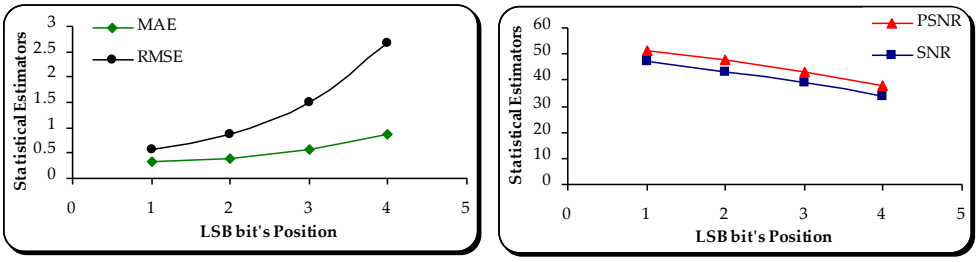

Figure 3. Variation of statistical estimators with LSB bit's position.

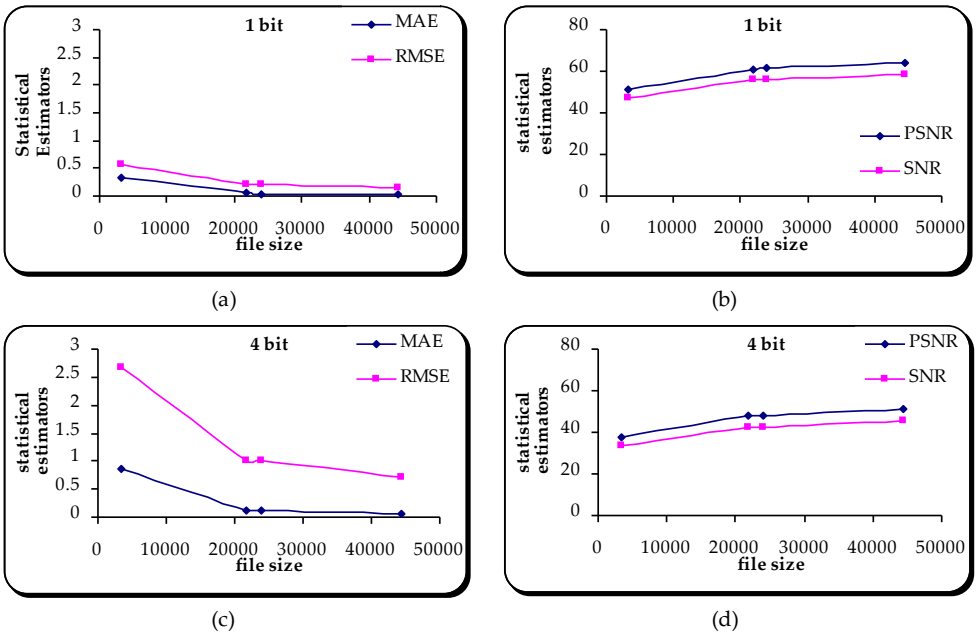

Figure 4. Variation of statistical estimators with file's size. (a), (b) for 1bit; (c), (d) for 4 bit.

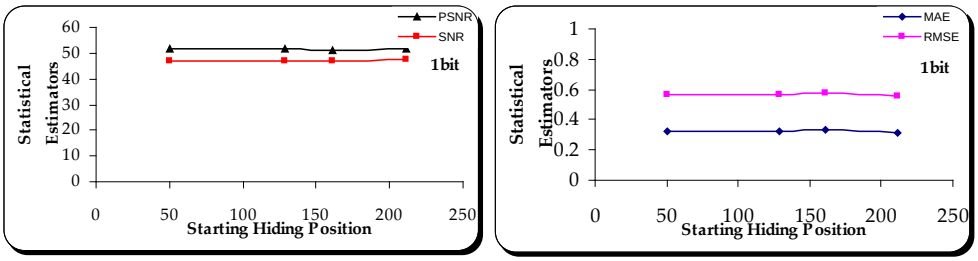

Figure 5. Variation of statistical estimators with starting hiding position.

5. Conclusion

Without any fear of eavesdropper, a new-audio file having a message hidden into it can be sent successfully by using different ways of LSB technique (*i.e.* 1st, 2nd, 3rd & 4th bit respectively). Regardless to which bit is used, starting hiding position doesn't affect upon the statistical estimators in their variation. Results show that MAE can be used as a best estimator in testing hiding process. After all one can ensure that 1st bit in LSB technique is better than other used bits in hiding process.

References

[1] Kumar, S., Barnali, B. and Banik, G. (2012) LSB Modification and Phase Encoding Technique of Audio Steganography Revisited. *International Journal of Advanced Research in Computer and Communication Engineering*, **1**, 1-4.

[2] Jayaram, P., Ranganatha, H.R. and Anupama, H.S. (2011) Information Hiding Using Audio Steganography—A Survey. *The International Journal of Multimedia & Its Applications* (*IJMA*), **3**, 86-96. http://dx.doi.org/10.5121/ijma.2011.3308

[3] Ali, A.J.M., Al-Zuky, A.A.D. and Ali, F.E.M. (2007) Text Hiding Technique in Digital Image. *Al-Mustansiriya Journal of Science*, **18**.

[4] Aigal, P. and Vasambekar, P. (2012) Hiding Data in Wave Files. *International Conference in Recent Trends in Information Technology and Computer Science*, *Proceedings Published in International Journal of Computer Applications*, 20-24.

[5] Chandrakar, P., Choudhary, M. and Badgaiyan, C. (2013) Enhancement in Security of LSB Based Audio Steganography Using Multiple Files. *International Journal of Computer Applications*, **73**, 21-24. http://dx.doi.org/10.5120/12754-9705

[6] Burate, D.J. and Dixit, M.R. (2013) Performance Improving LSB Audio Steganography Technique. *International Journal of Advance Research in Computer Science and Management Studies*, **1**, 67-75.

[7] Gadicha, A.B. (2011) Audio Wave Steganography. *International Journal of Soft Computing and Engineering* (*IJSCE*), **1**, 174-176.

[8] Chadha, A., Satam, N., Sood, R. and Bade, D. (2013) An Efficient Method for Image and Audio Steganography Using Least Significant Bit (LSB) Substitution. *International Journal of Computer Applications*, **77**, 37-45. http://dx.doi.org/10.5120/13547-1342

[9] Al-Obaidi, F.E.M. and Ali, A.J.M. (2013) A Comparison in Colored Text Enhancement. *International Journal of Scientific & Engineering Research*, **4**, 659-665.

[10] Kaushik, P. and Sharma, Y. (2012) Comparison of Different Image Enhancement Techniques Based Upon Psnr & Mse. *International Journal of Applied Engineering Research*, 7.

[11] Hemalatha, S., Acharya, D.U. and Renuka, A. and Kamath, P.R. (2013) A Secure and High Capacity Image Steganography Technique. *Signal & Image Processing*: *An International Journal* (*SIPIJ*), **4**.