J Inf Process Syst, Vol.12, No.3, pp.525~537, September 2016
http://dx.doi.org/10.3745/JIPS.03.0054

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Audio Data Hiding Based on Sample Value Modification Using Modulus Function

Mohammed Hatem Ali Al-Hooti*,**, Supeno Djanali**, and Tohari Ahmad**

Abstract

Data hiding is a wide field that is helpful to secure network communications. It is common that many data hiding researchers consider improving and increasing many aspects such as capacity, stego file quality, or robustness. In this paper, we use an audio file as a cover and propose a reversible steganographic method that is modifying the sample values using modulus function in order to make the reminder of that particular value to be same as the secret bit that is needed to be embedded. In addition, we use a location map that locates these modified sample values. This is because in reversible data hiding it needs to exactly recover both the secret message and the original audio file from that stego file. The experimental results show that, this method (measured by correlation algorithm) is able to retrieve exactly the same secret message and audio file. Moreover, it has made a significant improvement in terms of the following: the capacity since each sample value is carrying a secret bit. The quality measured by peak signal-to-noise ratio (PSNR), signal-to-noise ratio (SNR), Pearson correlation coefficient (PCC), and Similarity Index Modulation (SIM). All of them have proven that the quality of the stego audio is relatively high.

Keywords

Audio, Data Hiding, Modulus Function, Information Security, Network Security

1. Introduction

The transmission of information via public networks has become an essential need for decades. This transmitted information itself might be either useful and significant or non-useful and non-significant. Furthermore, there is highly secured information such as bank accounts, passwords and so on, which is in need to be fully protected and not to be seen by other parties. It is well-known that there are many algorithms that are used to secure the information such as encryption [1,2], data hiding (steganography) [3]. This last method has been growing fast since, in some cases, it is more useful and reasonable than other security methods. It has two types: digital watermarking and steganography which can be used and applied in many fields such as military, banking, police, and even health.

Steganography is a Greek word which means hidden writing. In different words, steganography means concealing secret data inside another media [4,5]. The secret message or the cover media can be text, image, audio, or video [4,6]. In case the resulted embedded data is obtained by third parties, they may only be able to find carrier media without knowing the existence of the secret information.

※ This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.org/licenses/by-nc/3.0/) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
Manuscript received February 15, 2016; accepted June 17, 2016.
Corresponding Author: Mohammed Hatem Ali Al-Hooti (moh_hat84@yahoo.com)
* Dept. of Computer Science, Sana'a University, San'a, Yemen (moh_hat84@yahoo.com)
**Dept. of Informatics, Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia (supeno@its.ac.id, tohari@if.its.ac.id)

Copyright© 2016 KIPS

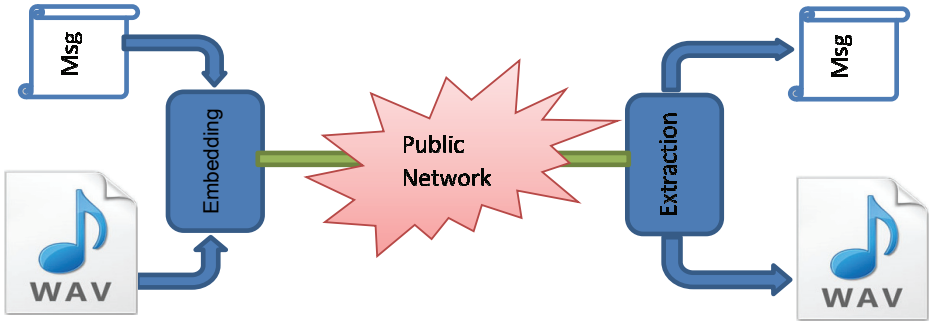

Fig. 1. Reversible data hiding algorithm.

Steganography is one of the most important aspects in information and communication security [7]. There are two main types of data hiding methods: reversible and non-reversible. While the former considers on recovering both the embedded secret message and the original cover media as shown in Fig. 1; the latter only focuses on the secret message and pays less attention on the recovery of the original cover media [8]. In general, data hiding system consists of the following items [9]:

Cover file: it is a file which is used for hiding the secret message. The cover also means that the file still not yet filled with data.

Secret message (payload): it is the data that are intended to be concealed.

Stego file: it is a file which is already carrying the secret data. In different words, it is called stego because it is processed by the embedding operation to combine both the cover media and the secret message.

The most popular type of the audio file formats is WAV which is easy to be converted into samples, and MP3 which needs to be preprocessed until we are able to obtain the sample values [10]. Furthermore, WAV type is more guaranteed for obtaining the secret message. Therefore, many authors prefer to use the WAV type. Additionally, there are two kinds of data hiding schemes which use an audio file as a cover in the embedding process: temporal and transform domains. The former directly uses and handles the value of the audio samples and directly embed the data such as LSB methods and difference expansion; while the latter, which is called frequency domain, converts the audio into another domain and then embeds the secret bits within that particular domain such as discrete wavelet transform (DWT). In [10,11], The obtained values from this DWT are used to hide the secret binary bits.

In data hiding research, there are many features that we need to consider such as: the robustness, which refers to the ability of the stego file to stand against the attacks and any other noise; the security, which means the difficulty when someone has the will to illegally obtain the secret message; the capacity, which refers to the amount of the secret bit which can be embedded within the carrier media; the quality, which means the amount of the distortion that occurs on the stego file after being embedded with the secret data. Some evaluation can be done to measure those values. This includes peak signal-to-noise ratio (PSNR) that the more its value the better the quality, and vice versa; the computational complexity that focuses on constructing the method which is used for the embedding and extraction process; and the tamper resistance that can be measured by the hard possibility for faking the secret

message after being embedded [12,13].

In this paper, the cover is an audio (WAV) file, and the secret information could be audio or text converted into binary. Since we are looking for misleading other irrelevant people not to realize the distortion that occurs on the cover file and it is common that, the image distortion can be noticed more than the one which might occurs on an audio file. This is because we are dealing with sound levels, it is difficult for the human being auditory to specify the sound whether it is high or low. In addition, based on the idea of the previous work [14] we propose a method that is called Sample Value Modification (SVM). It modifies the sample values using modulus function in order to make the reminder of that particular value to be same as the secret bit that is in need to be hidden. Furthermore, we use a location map that locates these modified sample values. This is because in reversible data hiding, it is needed to recover exactly the same both the secret message and the original audio file, as it is described above. Additionally, this research focuses on enhancing four stenographic characteristics namely: (i) the capacity (payload) which proves that the amount of the secret binary bits are equals to the amount of the sample values that are available within the cover audio file; (ii) the quality that verifies the difficulty of public about the notice of the hidden data, measured by SNR, PSNR; (iii) the robustness that evaluates the strength of the method to defend against illegal retrieval or modification launched by attackers such as audio conversion from WAV to MP3; (iv) the security (which is normally based on the quality of the stego file, that means, the better the quality, the higher the security, and vice versa).

This paper is organized as follows: Section 1 provides the introduction. Section 2, explains the literature review and related works. In Section 3, the proposed method is presented with its two embedding and extraction operations; while the experimental results are presented in Section 4. Finally, the conclusion and some future research directions are drawn in Section 5.

2. Related Works

Data hiding has become a very well-known and significant research. It is highly recommended to consider some of these previous works that have relation to our current research. Many data hiding methods based modulus function are focusing only on using an image as a cover file such as follows.

In [15], Wang et al. focus on producing a scheme that uses pixel-value differencing (PVD) and a modulus function. Here, the difference value of two neighboring pixels is taken. If this difference is low, then it will be ignored. Otherwise, it will be used for carrying the secret data. However, if the difference value is not same as the secret data, then the reminder of those two pixel values will be adjusted in order to make it suitable for carrying the secret data. However; this method does not perform well in terms of quality.

In order to increase the performance, Maleki et al. [16] present adaptive and non-adaptive schemes for grayscale images based on modulus functions. The average difference value of the neighboring quad pixels via a threshold secret key, is used in the adaptive method. The pixels which are located on the edge are embedded more than the ones in the smooth areas. In the non-adaptive scheme, an error reduction procedure is applied for achieving a better performance. This has made a good improvement in the capacity, quality and security.

Jung and Yoo [17] has proposed an improved method of exploiting modification direction (EMD) that is using each pixel of the image individually to hide data, and it has made a good quality. In further

research, Shen and Huang [18] propose a method that explores the difference of pixel values, which is able to improve the directions of exploiting modification. This work converts the image into 1D array of pixels by employing the Hilbert space-filling curve. Additionally, this work has considered embedding more data within bigger difference of pixel pairs. They also have used optimization to solve the overflow problem.

Zhao et al. [19] has proposed a simple algorithm that employs PVD and modulus function (MF) proposed by the study of Wang et al. [15]. They improved this method by building a new equation that developed both the visual quality of the stego image and the secret message capacity. Next, Choi et al. [20] have presented an application of a generalized difference expansion-based reversible audio data hiding algorithm by using the intelligent partitioning algorithm. This method has exploited the schemes which are used to handle an 8 bit 2D image as the cover. It is applied on a 16 bit waveform sample audio file. As the result, a reasonable capacity and quality can be achieved.

Finally Nagaraj et al. [14] provide a data hiding method based on pixel value modification (PVM) by using modulus function, which works on color images. This research is able to embed a secret bit within each individual pixel in each RGB channels. Moreover, this method modifies only the pixels which their reminders differ from the secret bits. This has made both the capacity and the quality excellent. However, they have paid less attention on retrieving the exact original cover file after the extraction process. Overall, they modify the value of the pixels either by decreasing or increasing it by one in order to make similarities between the reminders and the secret bits. Its disadvantage is that this method ignored using the pixels values which are in the range (0 and 255) and are not in the the interval [0,250], for their reason which indicated these ignored values might cause an overflow or underflow problem.

3. The Proposed Method

Based on the idea of [14] and [5], we propose a data hiding method by using an audio file as a cover. This scheme concerns to successfully develop a reversible audio data hiding application, which has the capability for retrieving the exact secret data and the exact cover audio file. This method modifies the sample to make their reminder values similar to the secret message. This modification differs from the previous work since this method pays attention to the overflow and underflow problems. For example, we can avoid the overflow problem by always decreasing the sample values by one which we need to modify, except that with zero value; thereby, we increase it by one in order to avoid the underflow problem. In addition, the location map [5] is essentially used for locating the modified samples so that, these modified values can be retrieved easily in the extraction process. Moreover, this method mainly focuses not only on enhancing and increasing the secret message capacity and the stego audio quality, but also pays attention on the robustness and the security. On the extraction process, we treat each sample value by using a modulus function so that, the reminder value of that particular sample will be exactly the secret binary bit. As in other data hiding methods, this scheme has two processes as follows.

3.1 The Embedding Process

The process usually happens at the sender node. This overall embedding process can be depicted in Fig. 2 where S is a sample value, S' is the respective stego sample value, and LM is the location map

which locates the modified values. For example, suppose the sample value is S=240, the reminder $SR=mod(240/2)=0$, and the secret bit b=1. The sample value is decreased by one in order to make the reminder same as the secret message S'=240–1=239. Similar to [14], there are some steps to do in order to smoothly process the embedding operation as the following:

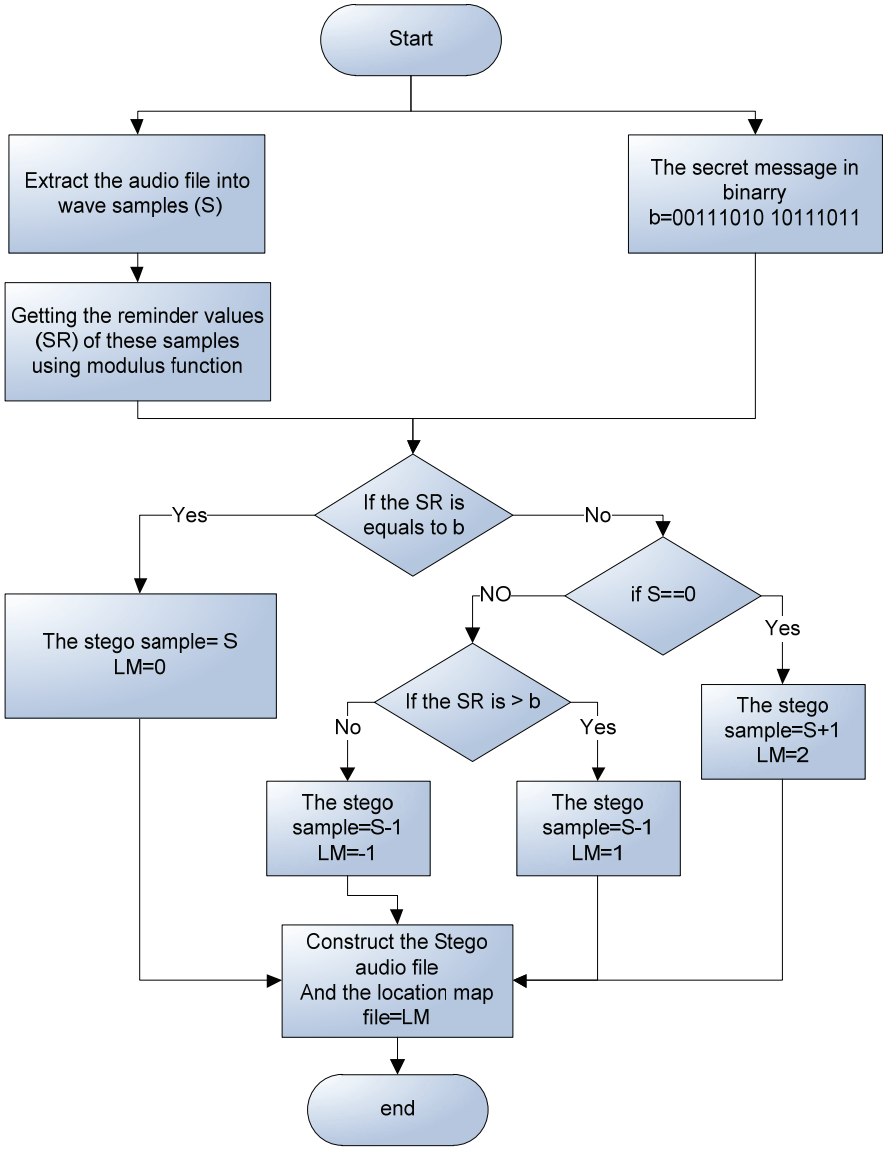

Fig. 2. The embedding process.

- Step 1: extract the audio file into wave sample values (S) which are in the interval [0, 65536] since we are dealing with a 16 bit depth audio file.
- Step 2: convert the secret data (b) which is to be embedded, in binary (0, 1).
- Step 3: different from the previous method, modulus function based 2 is used to obtain the reminder (SR) of each sample by using Eq. (1).

$$SR = mod(S/2) \tag{1}$$

- Step 4: compare the reminder values SR with the binary values of the secret message as presented in Eq. (2). This is because if the reminder of the original sample value is not equal to the secret binary bit, then different from the previous works, the sample value is decreased by one in order to make its reminder SR as similar as the secret binary bit b. Except if the sample value equals to zero, and its reminder doesn't match with secret bit. In this case, it is increased by one instead of decreased in order to avoid the underflow problem. Additionally, the location map is included to help fully 100% recovering the original audio file. This is because by locating these modified samples, we are able to obtain exactly the same original audio file without a need for the cover file in the destination part.

$$\begin{gathered} S' = S \; and \; LM = 0, if \; SR = b \\ S' = S + 1 \; and \; LM = 2, if \; SR <> b \; and \; S == 0 \\ S' = S - 1 \; and \; LM = 1, if \; SR > b \; and \; S <> 0 \\ S' = S - 1 \; and \; LM = -1, if \; SR < b \; and \; S <> 0 \end{gathered} \tag{2}$$

  where S is sample value, S' is the stego sample value, and LM means the location map which locates the modified values. For example, suppose the sample value is S=240, the reminder SR=mod(240/2)=0, and the secret bit b=1. Therefore, the sample value has to be decreased by one in order to make the reminder value same as the secret message S'=240–1=239 so, the reminder value will be equals to the secret binary bit SR=mod(239/2)=1. In this case, we can say that the location map LM is –1. This because before the modification, the reminder value SR was lesser than the secret binary bit b, and the sample value S=240 is not zero.
- Step 5: construct the stego audio file that is carrying the secret data. Using the modulus function you can easily obtain the secret data from this stego audio file.

These above steps help processing the audio file during the embedding process. Up to this point, we have got the stego audio file and the location map that is saved in an excel file and it will be sent separated.

3.2 The Extraction Process

This operation is always the opposite operation of the embedding process, and it is carried out at the receiver nodes. In order to successfully extract the data, the receiver must have two files: the stego audio and the location map files. The extraction process as shown in Fig. 3 can be performed as the following steps.

- Step 1: extract the stego audio file into samples S', and read the location map from the file.
- Step 2: obtain the secret binary bit b' using modulus function as presented in Eq. (3).

$$b' = mod(S'/2) \tag{3}$$

- Step 3: to obtain the exact original audio file, it is necessary to check the location map as in Eq. (4). So, the recovered sample S is equals to the stego sample S' if the location map, LM is 0. Moreover, the recovered sample S is equals to the stego sample S' minus one, if the

location map LM is 2 and the stego sample is 0; otherwise the recovered sample is equals to stego sample S' plus one. For instance, we consider stego sample values in the previous embedding stage example, that is the stego sample S'=239 and the location map is –1. We can obtain the secret bit by $b'=mod(239/2)=1$. Then the recovered sample S=239+1=240 which is exactly the same as the original sample before the embedding.

$$\begin{aligned} S=S', if\ LM==0 \\ S=S'-1, if\ LM==2 \\ S=S'+1, if\ otherwise \end{aligned} \tag{4}$$

- Step 4: create the recovered audio file and save the secret message.

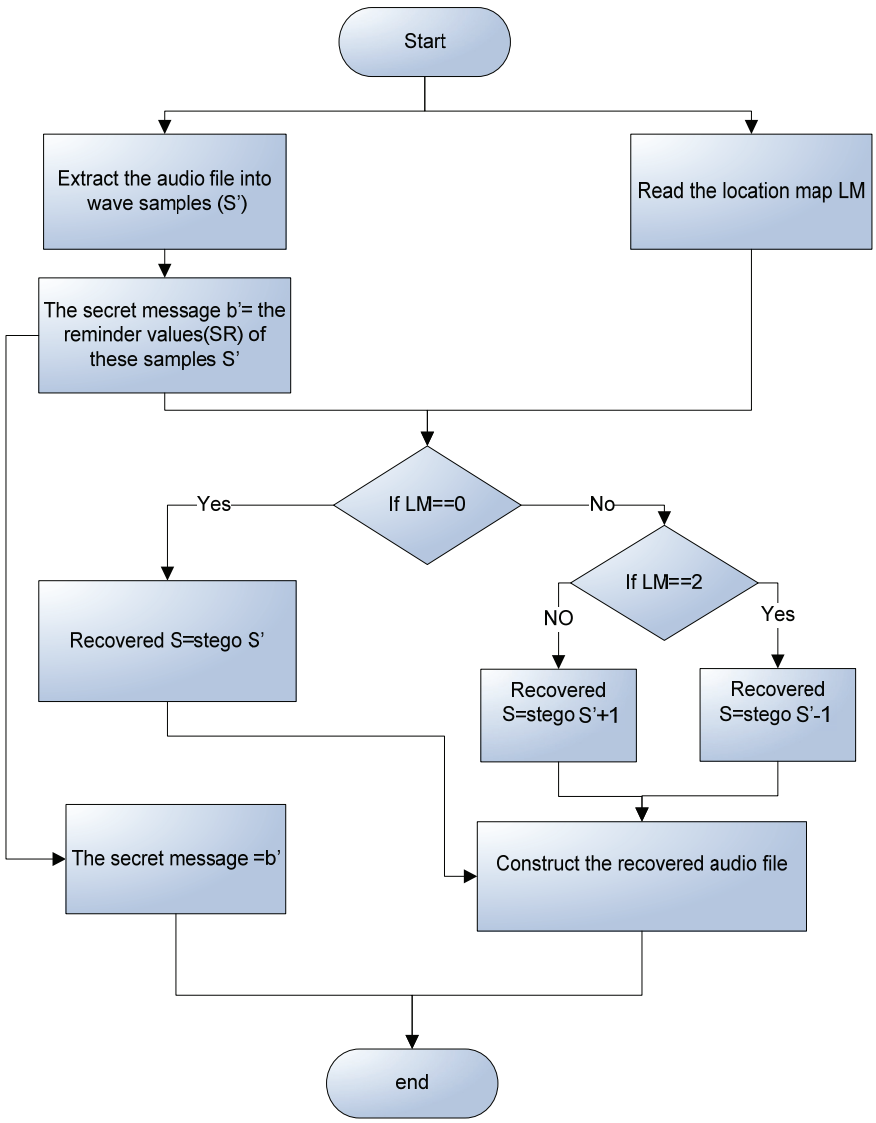

Fig. 3. The extraction process.

4. The Experimental Results

This proposed method is evaluated in MATLAB 2013a with Intel Core 2 Duo CPU at 2.00 GHz, 3 GB RAM. The secret message is randomly generated in binary bits using "Randi" function in MATLAB. The audio file that is considered as a cover is bird.wav [21]. The first 40 samples are not used in this experiment because usually these samples cause a complete distortion for the audio file. Therefore, the samples which are used in this cover file are 157176. We have tried the embedding process ten times, each of which with different secret messages each acts as certain percentage from the number of the audio file samples. The bit depth and the respective number of samples are depicted in Table 1. As described previously, this proposed method is evaluated in terms of some factors as follows.

The capacity: This feature is measured by the amount of the secret message binary bits which can be embedded within each audio file. This method uses each sample to carry a secret bit. As shown in Table 2, this method is able to embed 1 bit per sample.

Table 1. The maximum value of wave audio samples based on the bit depth

Bit depth	Value of the sample
8	255
16	65,336
24	16,777,216

Table 2. The amount of the embedded secret binary bits

Embedding percentage (%)	Number of the audio samples	Amount of secret bits	Modified samples	Unmodified samples	Balance of the unused samples
10	157176	15717	7842	7875	141459
20	157176	31435	15709	15726	125741
30	157176	47200	23708	23492	109976
40	157176	62870	31421	31449	94306
50	157176	78588	39246	39342	78588
60	157176	94117	47101	47016	63059
70	157176	109913	54813	55100	47263
80	157176	125740	62775	62965	31436
90	157176	141600	71220	70380	15576
100	157176	157176	78661	78515	0

The quality: In order to measure the quality, we perform an evaluation from some points of view. First, subjectively if we take a look at Fig. 4 (which shows the original audio file signal) and Fig. 5 (that demonstrates the stego audio file signal), we can notify that there is no clear difference between both of them. This is because the distortion that is done on the stego file is not that much since not all the samples are modified. Second, we objectively measure the stage quality by comparing it with the original file by using the following measurement methods:

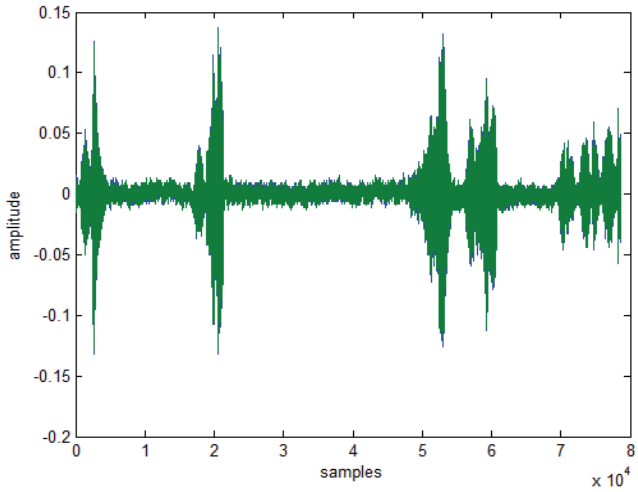

Fig. 4. The original audio file signal.

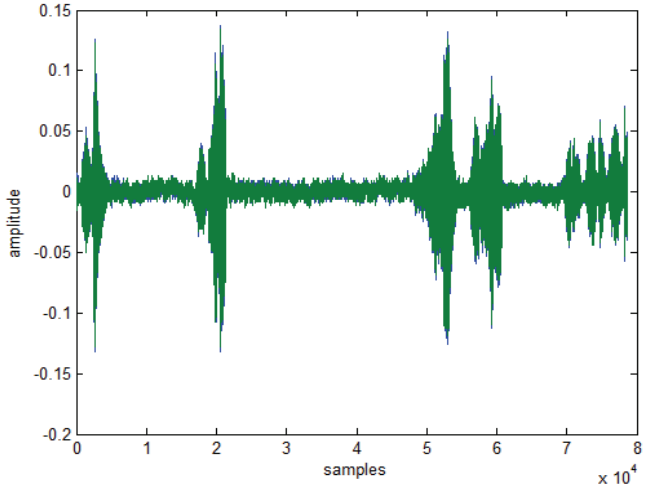

Fig. 5. The stego audio file signal.

(i) SNR [11] that uses the square value of each sample S_i^2 to demonstrate the difference between the original audio signal and the stego audio signal as presented in Eq. (5), where N is the number of the samples, S_i is the original cover audio samples, and S_i' is the stego audio samples. The more the value of the SNR the better the quality of the stego audio file, and vice versa. The SNR results are shown in Table 3 which proves that the stego file has a good quality since its value is still high 95.3868 dB while it is fully embedded 1 bpp.

$$SNR = 10 * log_{10}\left(\frac{\frac{1}{N}\sum_{i=1}^{N} S_i^2}{MSE}\right) \tag{5}$$

(ii) PSNR [22] as depicted in Eq. (6) which is almost same as SNR, however; this method uses the maximum value of the sample. It is known that, this max value can be determined based on the audio file bit depth as shown in Table 1. This is because Max value=2^b. Its results are also

shown in Table 3 which demonstrates that the stego file has a good quality since its value is 99.3557 dB while it is completely embedded 1 bpp. Both SNR and PSNR applies MSE as presented in Eq. (7) where b is the bit depth whose value is equals to 16. This mean that the amount of distortion that occurs on the stego audio file. The more the value of the MSE the more the distortion that happens on that particular file, and vice versa.

$$PSNR = 10 * log_{10} \frac{(2^b-1)^2}{MSE} \tag{6}$$

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(S_i - S_i')^2 \tag{7}$$

(iii) Similarity Index Modulation (SIM) [22]: as specified in Eq. (8), it is used for measuring the correlation between two files. These files might be images, audios, or even text files. In this case we use it to measure the correspondence between the original audio file and the stego audio file. Its value is in between 0 and 1. The closer the value to 1 the better the quality of the stego file. The measurement results which are shown in Table 3 validate that the similarity between the cover and the stego audio files is almost the same since the SIM and correlation values are 1.000.

Table 3. The quality of the stego audio file

Amount of the embedded secret data (%)	Quality of the stego audio file				
	Correlation	SIM	MSE	PSNR	SNR
10	1.000	1.000	0.0499	109.3491	105.3802
20	1.000	1.000	0.0999	106.3318	102.3629
30	1.000	1.000	0.1508	104.5444	100.5755
40	1.000	1.000	0.1999	103.3211	99.3522
50	1.000	1.000	0.2497	102.3554	98.3865
60	1.000	1.000	0.2997	101.5630	97.5941
70	1.000	1.000	0.3487	100.9045	96.9356
80	1.000	1.000	0.3994	100.3155	96.3466
90	1.000	1.000	0.4531	99.7673	95.7984
100	1.000	1.000	0.4982	99.3557	95.3868

(iv) The Pearson correlation coefficient (PCC) [23]: it is shown in Eq. (9), that this method can also be used to evaluate the similarity between the stego and the cover audio files. Its value is in the interval [0, 1]. Same as SIM, the more the value the better the quality of the stego file.

$$SIM = \frac{\sum_{i=1}^{N} S_i * S_i'}{\sum_{i=1}^{N}(S_i)^2} \tag{8}$$

$$PCC = \frac{\sum_{i=1}^{N}(X_i-\bar{X})*(Y_i-\bar{Y})}{\sqrt{\sum_{i=1}^{N}(X_i-\bar{X})^2}\sqrt{\sum_{i=1}^{N}(Y_i-\bar{Y})^2}} \tag{9}$$

The robustness: Based on the Eqs. (8) and (9), it can be inferred that this method can generate high quality stego data, but it has no strength to stand against attacks which may happen to the stego file, such as compression or conversion. This is because this method is not able to retrieve the secret message after the stego file is being attacked. However, this also could be a positive side since it guarantees the originality of the stego file. The secret message similarity is measured by using correlation [22] as presented in Eq. (10) that compares the original secret message and the extracted secret message. Where X_i the original is secret message in bits and Y_i is the extracted secret message in bits $\bar{X}$ and $\bar{Y}$ are the mean values of the original and the extracted secret messages, respectively.

$$Correlation = \frac{\sum_{i=1}^{N}(X_i-\bar{X})*(Y_i-\bar{Y})}{\sqrt{\sum_{i=1}^{N}(X_i-\bar{X})^2*(Y_i-\bar{Y})^2}} \tag{10}$$

The security: This feature mainly can be measured based on the quality of the stego file. Therefore, if the quality is high, then the security is also high, and vice versa.

5. Conclusions

This paper has presented a reversible data hiding method based on the audio file. This SVM method considers embedding a secret bit within each individual sample. The experimental results show that the amount of the secret bits is same as that of the sample values that are available within the cover audio file. Moreover, in terms of the quality this method has made a successful stego quality measured by SNR, PSNR values. The quality of the stego audio is almost same as the quality of the original cover image. This is because we only modify the samples whose their modulus reminder is not same as the secret binary bit. Furthermore, by using the location map this method is able to retrieve exactly the same original audio file as well as the secret message.

This method successfully achieves three characteristics: capacity, quality, and security. Therefore, we recommend paying more attention on the other features such as robustness to make this method able to stand for the conversion attacks, and so on.

Acknowledgement

We would like to give our warmest thanks to both of the governments of Indonesia and Yemen for their kind support. We would also like to show our gratitude to the Department of Informatics, Institut Teknologi Sepuluh Nopember (ITS), for sharing their pearls of wisdom with us during the course of this research.

References

[1] Y. Feng, J. Li, F. Han, and T. Ahmad, "A novel image encryption method based on invertible 3D maps and its security analysis," in *Proceedings of 37th Annual Conference on IEEE Industrial Electronics Society (IECON)*, Melbourne, Australia, 2011, pp. 2186-2191.

[2] T. Ahmad, J. Hu, and S. Han, "An efficient mobile voting system security scheme based on elliptic curve cryptography," in *Proceedings of 3rd International Conference on Network and System Security (NSS)*, Gold Coast, Australia, 2009, pp. 474-479.

[3] M. Holil and T. Ahmad, "Secret data hiding by optimizing general smoothness difference expansion-based method," *Journal of Theoretical and Applied Information Technology*, vol. 72, no. 2, pp. 155-163, 2015.

[4] W. C. Kuo, C. C. Wang, and Y. C. Huang, "Binary power data hiding scheme," *AEU-International Journal of Electronics and Communications*, vol. 69, no. 11, pp. 1574-1581, 2015.

[5] M. H. A. Al-Huti, T. Ahmad, and S. Djanali, "Increasing the capacity of the secret data using DE pixels blocks and adjusted RDE-based on grayscale images," in *Proceedings of 2015 International Conference on Information & Communication Technology and System (ICTS)*, Surabaya, Indonesia, 2015, pp. 225-230.

[6] T. S. Nguyen and C. C. Chang, "A reversible data hiding scheme based on the Sudoku technique," *Displays*, vol. 39, pp. 109-116, 2015.

[7] A. M. Bagade and S. N. Talbar, "A high quality steganographic method using morphing," *Journal of Information Processing Systems*, vol. 10, no. 2, pp. 256-270, 2014.

[8] R. M. Rad, K. Wong, and J. M. Guo, "A unified data embedding and scrambling method," *IEEE Transactions on Image Processing*, vol. 23, no. 4, pp. 1463-1475, 2014.

[9] V. K. Yadav and S. Batham, "A novel approach of bulk data hiding using text steganography," *Procedia Computer Science*, vol. 57, pp. 1401-1410, 2015.

[10] D. Yan, R. Wang, X. Yu, and J. Zhu, "Steganography for MP3 audio by exploiting the rule of window switching," *Computers & Security*, vol. 31, no. 5, pp. 704-716, 2012.

[11] S. Hemalatha, U. D. Acharya, and A. Renuka, "Wavelet transform based steganography technique to hide audio signals in image," *Procedia Computer Science*, vol. 47, pp. 272-281, 2015.

[12] B. Saha and S. Sharma, "Steganographic techniques of data hiding using digital images," *Defence Science Journal*, vol. 62, no. 1, pp. 11-18, 2012.

[13] F. Djebbar, B. Ayad, K. A. Meraim, and H. Hamam, "Comparative study of digital audio steganography techniques," *EURASIP Journal on Audio, Speech, and Music Processing*, vol. 2012, pp. 1-16, 2012.

[14] V. Nagaraj, V. Vijayalakshmi, and G. Zayaraz, "Color image steganography based on pixel value modification method using modulus Function," *IERI Procedia*, vol. 4, pp. 17-24, 2013.

[15] C. M. Wang, N. I. Wu, C. S. Tsai, and M. S. Hwang, "A high quality steganographic method with pixel-value differencing and modulus function," *Journal of Systems and Software*, vol. 81, no. 1, pp. 150-158, 2008.

[16] N. Maleki, M. Jalali, and M. V. Jahan, "Adaptive and non-adaptive data hiding methods for grayscale images based on modulus function," *Egyptian Informatics Journal*, vol. 15, no. 2, pp. 115-127, 2014.

[17] K. H. Jung and K. Y. Yoo, "Improved exploiting modification direction method by modulus operation," *International Journal of Signal Processing, Image Processing and Pattern*, vol. 2, no. 1, pp. 79-87, 2009.

[18] S. Y. Shen and L. H. Huang, "A data hiding scheme using pixel value differencing and improving exploiting modification directions," *Computers & Security*, vol. 48, pp. 131-141, 2015.

[19] W. Zhao, Z. Jie, L. Xin, and W. Qiaoyan, "Data embedding based on pixel value differencing and modulus function using indeterminate equation," *Journal of China Universities of Posts and Telecommunications*, vol. 22, no. 1, pp. 95-100, 2015.

[20] K. C. Choi, C. M. Pun, and C. P. Chen, "Application of a generalized difference expansion based reversible audio data hiding algorithm," *Multimedia Tools and Applications*, vol. 74, no. 6, pp. 1961-1982, 2015.

[21] Animal.wav files [Online]. Available: http://www.externalharddrive.com/waves/animal/index.html.

[22] G. Kasana, K. Singh, and S. S. Bhatia, "Data hiding algorithm for images using discrete wavelet transform and Arnold transform," *Journal of Information Processing Systems*, 2015. http://dx.doi.org/10.3745/JIPS.03.0042.

[23] L. Sheugh and S. H. Alizadeh, "A note on pearson correlation coefficient as a metric of similarity in recommender system," in *Proceedings of 5th Conference on Artificial Intelligence and Robotics (AI & Robotics)*, Qazvin, Iran, 2015, pp. 1-6.

Mohammed Hatem Ali Al-Hooti

He has got a Bachelor degree in information system from Al-Yemenia University, Sana'a, Yemen. His master in informatics is received from Institut Teknologi Sepuluh Nopember (ITS), Surabaya, Indonesia. In this current time, he is still doing his PhD program at ITS as well. His interest is in net centric computing, data hiding, systems and database development and administration (oracle), Java programming, and information security.

Supeno Djanali

He is a Professor of Network Architecture and Design in Department of Informatics, Institut Teknologi Sepuluh Nopember, Indonesia. He graduated at the University of Wisconsin-Madison, USA, for both his Master and Ph.D. degrees. His research areas are primarily network security and mobile computing.

Tohari Ahmad

He has obtained his Bachelor, Master and Ph.D. degree from ITS, Monash University and RMIT University, respectively. All are in computer science and information technology. His research interest is in data hiding, biometric security and information security.