Chaos-Based Audio Steganography and Cryptography Using LSB Method and One-Time Pad

Samah M.H. Alwahbani(✉) and Huwaida T.I. Elshoush

Faculty of Mathematical Sciences, University of Khartoum, Khartoum, Sudan
samahmahdi22@gmail.com, htelshoush@uofk.edu

Abstract. This paper presents a chaos-based audio steganography and cryptography method that is based on Least Significant Bit (LSB) and one-time pad, respectively. In the proposed scheme, two chaotic maps were used, Piecewise Linear Chaotic Map (PWLCM) and logistic map for encryption and steganography, respectively. For encryption, a quantized generated chaotic sequence of PWLCM is used as key for one-time pad algorithm. For message hiding, a chaotic sequence is generated by the logistic map and ordered ascendingly or descendingly. Then, the encrypted data are embedded based on the indices for the ordered sequence of the host audio LSB's samples. An analysis is discussed for the proposed scheme. It overcomes the drawbacks of key generation and distribution for one-time pad by using the chaotic maps. The proposed method satisfies the main requirements of steganography, perceptual transparency, capacity of hidden data and robustness. Experimental results were made, waveform analysis and signal-to-noise ratio, which indicated that the stego audio has high quality. The analysis demonstrates the efficiency of the proposed method, and so it can be applied to secure communications.

Keywords: Steganography · Least Significant Bit (LSB) · One-time pad · Chaotic maps

1 Introduction

Recently, with the rapid development of digital communications and networking technologies, large amount of data have been distributed, shared, and transmitted over open networks. So, securing these data has become a critical issue. Cryptography and steganography are two security solutions that provide data confidentiality [1]. Cryptography scrambles the secret message so that it cannot be read by eavesdroppers while, steganography conceals the secret message into a file so that it cannot be seen by eavesdroppers.

In steganography, different types of data can be hidden within a cover file. The resulted file contains the hidden information called stego file. It is virtually identical to the cover file [3].

Y. Bi et al. (eds.), *Proceedings of SAI Intelligent Systems Conference (IntelliSys) 2016*,
Lecture Notes in Networks and Systems 16, DOI 10.1007/978-3-319-56991-8_54

The basic requirements of steganographic scheme are as follow [3,16]:

- **Secrecy:** It should not be able to extract the secret message from the stego file without knowing the secret key of the extraction algorithm.
- **Imperceptibility:** It should not be able to distinguish the cover file after being embedded with the secret data from the original one.
- **High capacity:** The size of secret data that a steganography scheme can successfully embedded in the cover file without introducing perceptual distortion should be as large as possible.

There are numerous steganography techniques that have been proposed to hide messages inside images, audio and video files due to the high redundancy of the multimedia objects. One of the widely used multimedia objects that has been used for steganography is an audio.

Audio steganography is the art and science of hiding digital data into audio files such as WAV and MP3 files. In audio stenography, the perceptual properties of the Human Auditory System (HAS) is used to hide information in the audio, because the human ear cannot discriminate the slight differences between the original version of a file and the altered one.

The developed techniques for audio steganography include Least Significant Bit, Parity Coding, Echo Hiding, Phase Coding, Silence Interval and Spread Spectrum [26]. Among these techniques, LSB coding is the simplest method. The LSB of binary representation of each sample of digitized audio file is replaced with a bit of the binary representation of the secret message [2,4].

The main advantage of the LSB coding method is the high embedding capacity; if only one LSB of the host audio sample is used with sampling rate 16,000 HZ, it gives a capacity of 16 kbps if all samples are used. In addition, the LSB method has a very small computational complexity compared with other steganography methods such as phase coding and echo hiding methods. However, the secret message can be easily destroyed by simple random changes of the LSBs [6]. Furthermore, the secret data is concealed in a very predictable way, making them easy to be recovered by attackers [1].

The rest of the paper is organized as follows, the next section discuses some related work. Then, Sect. 3 describes the chaotic maps, while the one-time pad is explained in Sect. 4. Section 5 presents the proposed method, and Sect. 6 shows the experimental results for it. Finally, Sect. 7 presents the conclusion.

2 Related Work

This research considers the LSB coding techniques for audio steganography due to the advantages of simplicity and high capacity. There are several researches that were proposed for audio steganography based on LSB coding, this section introduces some of them.

In 2004, Cvejic and Seppanen [6] proposed a method that had high bit rate of LSB. The proposed method consisted of two steps. First, a secret message bit was embedded into the i^{th} LSB layer of the host audio. Then, a bits adjustment algorithm was applied to minimize the distortion of the host audio after secret message is embedded.

In 2009, Zamani et al. [7] developed a genetic based LSB steganography method. The authors presented two solutions to LSB problems which are attacks that try to discover the hidden message and distortions with high average power. For the first problem, the proposed method modified the other bits than LSBs in samples which increased the difficulty of discovering which bits were embedded, also it selected a group of the samples and not all of them. To decrease the distortion, the secret message bits were embedded in deeper layers with adjustment to decrease the error rate.

In the same year of Zamani et al. [7] publication, Parthasarathy and Srivatsa [8] proposed a method that shift the limit for transparent data hiding from the 4^{th} LSB layer to the 6^{th} LSB layer, using a two-step approach like Cvejic and Seppanen approach.

After two years from the work of Parthasarathy and Srivatsa [8], Gadicha [9] presented a method similar to Cvejic and Seppanen [6] approach that shift the secret message to the fourth LSB layer.

Although the proposed methods of [8,9] use secret key to select the group of samples in the host audio, they did not increase the LSB robustness significantly.

Bandyopadhyay and Banik [10] in 2011 proposed a method that is named as multi-level steganography. It consists of two algorithms, LSB and parity coding at layer 1 and layer 2, respectively. First, the cover file was embedded with the first secret message. Then, in the next level the secret message was embedded. At last, The resulted stego file held the both secret messages. Multi-Level steganography has the advantages of difficult decoding, and sending two secret messages in a single cover file.

A year later in 2012, Hmood et al. [11] hid images in the audio based on two LSB insertion method of the low part of the audio file. The secret image was converted from color image to gray image, encrypted and finally it was converted into binary representation. The cover audio was broken up into two parts, low frequency and high frequency by using Wavelet Transform. Then, the high frequency part was used to embed the encoded image. Signal to noise ratio was calculated to test the system performance.

In the same year of Hmood et al. publication [11], Deepak et al. [12] proposed LSB audio steganography method that increased the robustness. They encoded the secret message in a WAV file which consisted of number of channels. A pattern was used to embed the bits in the LSB, instead of embedding bit of the message only in the consecutive bytes of WAV file as in the standard algorithm. The secret message was encoded using the pattern in the different channels of the WAV file. The same pattern was used to decode the cover file to recover the hidden message. This scheme is simple, and it increased the robustness of the conventional LSB algorithm. However, the pattern should be random and large enough to consider this proposed scheme secure.

To enhance the security of LSB algorithms, many researchers proposed hybrid methods that combine the cryptography and steganography. Priyanka et al. [14]

in 2012, encrypted the secret message using RSA algorithm, and then the encrypted message bits are embedded at random higher LSB layer position of the host audio. Another method that uses RSA was proposed by Padmashree and Venugopala in the same year [15]. First, the secret message is encrypted by the RSA, and then it was embedded in the 4^{th} and 5^{th} LSB bits. Peak Signal to Noise Ratio (PSNR) of both original cover audio file and the stego file are tested to demonstrate that there was a little noise intrusion even after embedding the 4^{th} and 5^{th} LSB bit of the original audio.

After one year, Patil et al. [5] also introduced a hybrid system of audio steganography and cryptography based on asymmetric encryption. First, the message is encrypted by public key encryption algorithm. Then for data hiding, the ciphertext is hidden in cover audio WAV file in random manner.

For symmetric encryption, in 2011 Zameer et al. [19] proposed LSB audio steganography method in which the data is encrypted by AES algorithm. The scheme uses 16 sub keys generated from a modified random key to encrypt the data. Also, to increase the amount of data hiding, the data are compressed before the embedding.

Dengre [20] in 2013, introduced LSB based audio steganography for AVI videos that encrypt the secret message using a group of symmetric algorithms include DES, Rijndael, RC2 and Triple DES algorithm. Then, it concealed the encrypted data into LSB bit position of selected samples. The authors used different sizes for videos, and different layers of LSB.

Also in 2013, Olanrewaju and Abdul Rahman [13] proposed LSB algorithm that encodes two binary data into the LSB part of the audio WAV file. The proposed method was introduced for any file type format. However, this method was basically based on the standard LSB algorithm, and it did not increase the robustness of the LSB algorithm.

In addition, Sinha et al. [27] presented a combination method of cryptography and steganography in 2015. The secret message was encrypted using modified Vigenre cipher, which is classical Vigenre cipher followed by double columnar transposition. Then, the encrypted data was concealed in the cover audio LSB's. At last, Blum Blum Shub pseudo random number generator was used to reorder the audio frames.

Another hybrid audio steganography and cryptography method was proposed by Krishnan and Abdullah in 2016 [28]. This paper aimed to improve the robustness by embedding the secret message in higher layers LSB. Before embedding, the secret message was encrypted by AES encryption algorithm. Several experimental results for method robustness against audio compression, noise addition and imperceptibility and stego audio quality were presented.

Most of the discussed methods aimed to increase the robustness of LSB coding by embedding the data in higher LSB layers or by encrypting the data before hiding. In the first technique, hiding the data in higher LSB layer will increase the robustness but the choices of hiding in the high layers are not large enough. Using the encryption converts a message into unintelligible form. But, most of the proposed methods use the standard LSB coding method which embeds the data bits in LSB starting from the beginning of the host audio and proceeds the embedding process sequentially until the end of the secret data. However, the standard method makes the message easy to be recovered by attackers. So, the steganography process will not be efficient. Such solution for this problem is the embedding in random positions in the host audio. However, no algorithm uses random numbers to embed the secret data in random positions to increase the robustness. Furthermore, the used encryption algorithms were complex algorithms and they have many computations which degrade the performance.

To enhance the robustness of LSB audio steganography method, the indices of audio samples LSB's should be selected randomly. The random numbers should pass the randomness tests. Also, the secret data should be encrypted first using an efficient algorithm to enhance the system, and the steganography system should satisfy the main requirements of a good system.

This study searches for an efficient random numbers generator that produces pseudo random numbers with good randomness properties. Also, this generator should have many requirements such as non-periodicity to guarantee that it does not generate the same values again and unpredictability to make the prediction of next random number in a sequence difficult even if the previous values are known. Furthermore, it should be simple for generation, distribution and storing. All these properties and more are satisfied by using a chaotic map, the following section introduces it in some details.

3 Chaotic Maps

Generally, chaos is an unpredictable, non-periodic, pseudo-random and long-term evolution that results from deterministic nonlinear systems that exhibits sensitive dependence on initial conditions [21,22].

Definition: Nonlinear and chaotic one-dimensional maps are the simplest class of chaotic dynamic systems which is of the form:

$$f : S \rightarrow S \qquad S \subset R \tag{1}$$

In most cases, S = [0, 1] or S = $[-1, 1]$. The one-dimensional map can also be written as the following:

$$x_{n+1} = f(x_n) \qquad n = 0, 1, 2, ... \qquad x_0 \,\epsilon\, S \tag{2}$$

Starting from an initial value x_0 ϵ S, by iterating the map the following chaotic sequence is generated:

$$x_0, x_1, x_2, ... \tag{3}$$

The following subsections introduce Logistic map and Piecewise Linear Chaotic Map briefly, which are used for the proposed method.

3.1 Logistic Map

Among one-dimensional chaotic maps, Logistic map is one of the simplest and well studied chaotic map. It is defined by the following equation:

$$x_{n+1} = \mu\, x_n(1 - x_n) \tag{4}$$

Where μ is a system parameter, $0 < \mu \leq 4$ and x_n is a real number in the interval *(0, 1)* and n = *0, 1, ...*, in case of $\mu >$ *3.569945672*, this system becomes chaotic [24].

3.2 Piecewise Linear Chaotic Map

A Piecewise Linear Chaotic Map (PWLCM) is an one-dimensional chaotic map that is defined by the following equation:

$$y_n = F(y_{n-1}) = \begin{cases} y_{n-1} \times \frac{1}{p} & \text{if } 0 \leq y_{n-1} < \text{p} \\ (y_{n-1} - p) \times \frac{1}{0.5-p} & \text{if } p \leq y_{n-1} < 0.5 \\ F(1 - y_{n-1}) & \text{if } 0.5 \leq y_{n-1} < 1 \end{cases} \tag{5}$$

Where $p\,\epsilon\,(0, 0.5]$ is the system parameter and $y_0\epsilon$ *[0, 1]* is the initial condition [25].

Compared to the Logistic map, PWLCM has a larger range of system parameter space than the Logistic map. Also, the PWLCM has a better balance property and uniform invariant density function [25].

4 One-Time Pad

One-time pad [17] is a symmetric unbreakable cipher that uses a random key to encrypt one message and then it discarded. This key is in the same length of the plaintext. The one-time pad algorithm produces random ciphertext that bears no statistical relationship to the plaintext.

By using the one-time, there is no way to break the ciphertext because it does not contain any information about the plaintext. In addition, for any plaintext of equal length to the ciphertext, there is a key that produces that plaintext. Therefore, if an exhaustive search is done for all possible keys, there are many legible plaintexts with no way of knowing which one is the intended plaintext.

The security of the algorithm is entirely depends on the key randomness. If it is truly random, then the ciphertext will be truly random. Therefore, there are no patterns or regularities to be used by cryptanalyst to attack the ciphertext.

The one-time pad offers complete security but, in practice, it has two fundamental difficulties [23]:

- It is impractical to generate large quantities of random keys. Generating large volumes of truly random keys is very difficult.

- The key distribution and protection. For every message to be sent, a key of equal length is needed for both sender and receiver. So, the key distribution is a significant problem.

In the proposed scheme, the chaotic maps are used for the key generation. They produce chaotic sequences with good randomness properties. Also, they have large key space to generate many random sequences. For the key distribution problem, the sender and receiver only exchange the initial conditions and system parameters for the chaotic map, and so there is no need to exchange the entire chaotic sequences which are very large. So, the chaotic maps solve the two problems for the one-time pad, if a chaotic map with good randomness properties is used.

5 The Proposed Method

This paper presents a method for audio steganography where the secret data is encrypted first using the one-time pad algorithm, then it is embedded into the host audio signal using LSB algorithm. This scheme depends on chaotic maps for the two processes, encryption and steganography. This section describes the two processes, encryption and steganography.

5.1 Message Encryption

The secret message is encrypted using the one-time pad algorithm, before embedding it in the host audio. The chaotic maps are used to generate a sequence of pseudo random numbers which is used as the key for the one-time pad. The PWLCM is chosen, due to its good chaotic properties and randomness behavior. For the encryption, the sender and receiver must have obtained copies of the initial value and system parameter for PWLCM to generate the key for the one-time pad. The encryption algorithm is described as follow:

Algorithm 1. The Encryption Algorithm

(1) *Consider the plain message M of length L as input.*

(2) *Generate a sequence of PWLCM y_n as long as the message M, using the initial condition y_0 and system parameter p.*

(3) *Convert the chaotic sequence y_n to integer numbers as follow:*

$$z_i = (round\,(y_i \times 10^{15}))\, mod\, 2^8 i = 1,2, \ldots, L \tag{6}$$

(4) *Apply the one-time pad using the sequence zn as key algorithm as follow:*

$$C_i = (m_i + z_i)\, mod\, 2^8 i = 1,2, \ldots, L \tag{7}$$

Where C_i is the cipher text, m_i is the secret message, z_i is the quantized chaotic sequence and L is the message length.

5.2 Message Hiding

After encrypting the message, it is embedded in the host digital audio using LSB method. The embedding method substitutes the least significant bit of each sampling point with a bit of the encrypted message. To increase the robustness of the LSB method, the samples indices, which will be used for the embedding process, are specified randomly by the following approach:

Algorithm 2. The Hiding Algorithm

(1) Generate a sequence x_n, $n = 0, 1, \ldots L$ of a logistic map using x_0 and μ as initial condition and system parameter, respectively
(2) Sort the generated sequence x_n ascendingly or descendingly, then put the corresponding indices of the unsorted sequence in vector called permutation vector P
(3) Use the permutation vector P to embed the secret encrypted message C by mapping each bit of the message to the LSB of the corresponding value of P.

Now, the secret message is hidden encrypted in the LSB of the host audio at random positions of the audio samples.

At the receiver, the message is extracted and then it is decrypted using the one-time pad. For message extraction, the receiver uses the same initial condition and system parameter to generate the same sequence of logistic map, and does the same steps to extract the encrypted message.

The decryption process is similar to the encryption with some variations. All the steps are the same, but the one-time pad is applied as follow:

$$m_i = (C_i - z_i)\, mod\, 2^8 \qquad i = 1, 2, 3, \ldots, L \tag{8}$$

Where m_i is the secret message, C_i is the cipher text, z_i is the quantized PWLCM sequence and L is the message length.

The proposed algorithm has two layers, encryption and hiding, which make the attacking for the message hard. The attacker must have the key for the two processes, encryption and steganography. The key is x_0, μ, y_0 and p. The proposed algorithm has large key space which will be discussed in the following section. Also, the presented method uses simple operations for encryption, addition and module functions, which are simple to implement for hardware and software.

To verify that the requirements of steganography algorithms are met:

- **Perceptual transparency:** The secret message is hidden using LSB algorithm. Thus, the audio samples are changed by 1 or they might not be changed (if the embedded bit is identical to the LSB sample bit). So, there are small differences between the cover audio and the stego one
- **Capacity of hidden data:** The proposed audio steganography based on standard LSB method uses all the LSB of the audio samples for hiding. For example, if the cover audio has duration of 10 seconds with sampling rate 8 KHZ, it can hide 80,000 bits. So, the algorithm has large capacity for hiding

- **Robustness:** The secret message is encrypted by the one-time pad which is a perfect cipher. Also, the encrypted data are hidden in random positions of the cover audio with a very large set permutation which is factorial L ($L!$). It is a very huge value. To extract the secret message correctly, the chaotic sequences should be known, and the encryption-steganography algorithms have a large key space as will be discussed in the next section.

6 Experimental Results

This section discuss several experimental results to demonstrate the efficiency of the proposed design.

The proposed method is implemented using MATLAB software. All the experimental results were conducted using some WAV sound files were taken from the web page http://www.1speechsoft.com/voices.html. These files are spoken English sentence: *"This is an example of the AT&T natural voice speech engine; it is the most human sounding text to speech engine in the world"*.

6.1 Wave Form Analysis

To analyze the proposed method, a waveform of the cover audio and stego audio are visualized and compared. Figure 2 shows an example to embed a message: 100 bytes in a cover file "julia8" which is one of the tested file, with sampling rate 8000 HZ, 8 bits for each sample, 65644 samples and 8.2055 s duration.

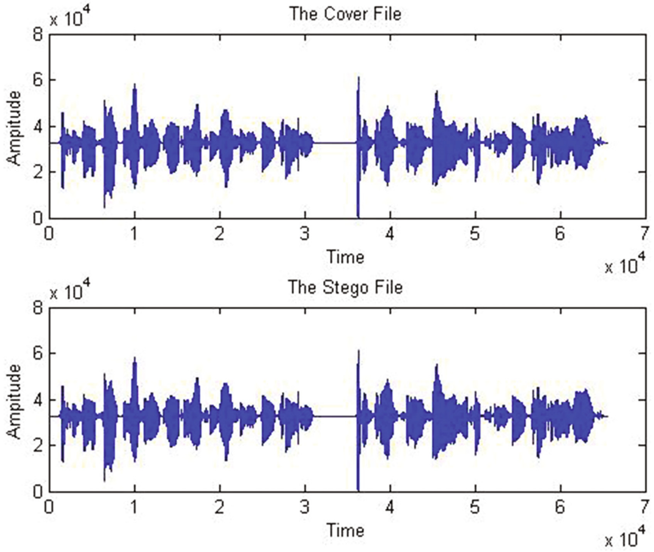

Fig. 1. Waveform of cover and stego audio for message of 10 bytes.

From Figs. 1, 2 and 3, it is clear that there are no clear differences between the cover audio and the corresponding stego. The difference percentage between them in Fig. 1 is 0.033514%, in Fig. 2 is 0.51% and 7.62% in Fig. 3, which are all very small.

Table 1 presents the percentage differences between the cover audio and the stego audio when messages with different sizes are embedded in the host audio.

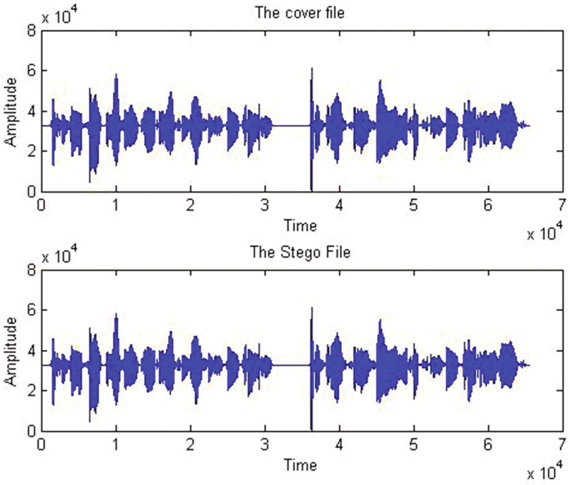

Fig. 2. Waveform of cover and stego audio for message of 100 bytes.

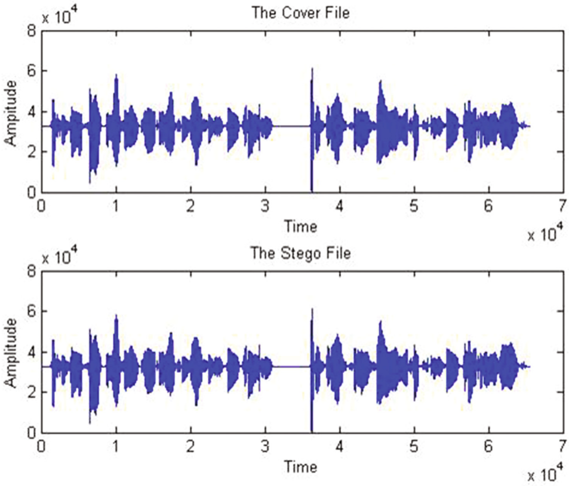

Fig. 3. Waveform of cover and stego audio for message of 1000 bytes.

Table 1. Percentage differences in the cover with different message sizes

Message size (in bytes)	Difference in %
1	0.0015234
10	0.033514
100	0.51
1000	7.62

6.2 Signal to Noise Ratio

Signal-to-noise ratio (SNR) is a common measurement for the audio signal quality, that is measure the noise in the signal. It is given by the following equation [18]:

$$SNR(s(i), sn(i)) = 10 \times \log_{10} \frac{\sum_{i=1}^{i=N} s(i)^2}{\sum_{i=1}^{i=N} (s(i) - sn(i))^2} \tag{9}$$

Where N is the total number of samples, *s(i)* is the amplitude of the original (cover) signal and *sn(i)* is the amplitude of the reconstructed signal. A high values of SNR means high precision of data, while a low values indicates of large a mount of noise.

In this research, SNR is used to measure the differences between the original audio (cover) and the stego audio. Table 2 presents the SNR values for the speech file when different message sizes are embedded.

From the Table 2, it is clear that the SNR values are very large even large messages are embedded, which indicate high precision and quality of the stego file. Also, there is no significant degradation of the audio file quality when the message size is increased.

Table 2. SNR values for different message sizes.

Message size (in bytes)	SNR
1	138.5404
10	125.1162
100	113.3290
1000	101.5498
10000	89.2206

6.3 Key Space

For the encryption algorithm, the key space is the total number of different keys that can be used for the algorithm. It should be large enough to resist against the exhaustive attack. For the proposed method, the secret key for the encryption is

y_0 and p. All key parameters are used with a precision of 10^{-14}. Therefore, the key space is $(10^{14})^2 = 10^{28}$.

For the steganography algorithm, the key is μ and x_0 for logistic map. Using precision of 10^{-14}, the key space is $(10^{14})^2 = 10^{28}$. So, to extract the secret message and decrypt it correctly, the key space is $(10^{14})^4 = 10^{56}$, which is large enough to resist the brute force attack.

7 Conclusion

This study designs and implements a hybrid chaos-based audio steganography cryptography algorithm. It is based on LSB method and one-time pad. Among all audio steganography methods, LSB method offers high embedding rate and high simplicity, but it has low robustness which is solved in the proposed method using chaotic maps. The chaotic maps are studied to choose maps with good randomness properties and non-periodicity. This study uses two chaotic maps, Piecewise Linear Chaotic Map (PWLCM) for encryption and logistic map for steganography. For message encryption, the PWLCM sequence is generated and processed to be used as a key for the one-time pad. For message hiding, the logistic map is used to generate a random sequence. Then, indices of ordered generated sequence are used to hide the encrypted data in random positions of the host audio samples. The one-time pad is used for encryption, which is unbreakable and perfect cipher if a random key is used. However, it has two fundamental drawbacks; it is impractical to generate large numbers of random keys and the other problem is the key distribution.

This research overcomes these problems by using chaotic maps. Chaotic maps produce random sequences with large key space which they are processed to be used as keys for the one-time pad. For the key distribution problem, the sender and receiver only exchange the initial conditions and system parameters for the chaotic maps, and so there is no need to exchange the whole large keys.

The experimental results demonstrate the efficiency of the proposed hybrid method. For encryption, the key space of one-time pad algorithm is analyzed. The signal-to-noise ratio is tested which indicated that the stego audio has high quality. The tests are applied for different audio file, speech and music. Therefore, the proposed method can be successfully applied to secure audio communications.

Acknowledgment. This research was supported by the University of Khartoum and the Nile Center for Technology Research.

References

1. Bassil, Y.: A two intermediates audio steganography technique. J. Emerg. Trends Comput. Inf. Sci. (CIS) **3**(11) (2012)
2. Divya, S., Reddy, M.R.: Hiding text in audio using multiple LSB steganography and provide security using cryptography. Int. J. Sci. Technol. Res. **1**(6), 68–70 (2012)

3. Jayaram, P., Ranganatha, H., Anupama, H.: Information hiding using audio steganography - a survey. Int. J. Multimedia Appl. (IJMA) **3**(3) (2011)
4. Nehru, G., Dhar, P.: A detailed look of audio steganography techniques using LSB and genetic algorithm approach. IJCSI Int. J. Comput. Sci. Issues **9**(2), 402–406 (2012)
5. Adhiya, K.P., Patil, S.A.: Hiding text in audio using LSB based steganography. Inf. Knowl. Manag. IISTE **2**(3), 8–14 (2012)
6. Cvejic, N., Seppanen, T.: Increasing robustness of LSB audio steganography using a novel embedding method. In: Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC04). IEEE (2004)
7. Zamani, M., Manaf, A.A., Ahmad, R.B., Zeki, A.M., Abdullah, S.: A genetic-algorithm-based approach for audio steganography. World Acad. Sci. Eng. Technol. **30**, 355–358 (2009)
8. Parthasarathy, C., Srivatsa, S.K.: Increased robustness of LSB audio steganography by reduced distortion LSB coding. J. Theoret. Appl. Inf. Technol. **7**(1), 80–86 (2009)
9. Gadicha, A.B.: Audio wave steganography. Int. J. Soft Comput. Eng. (IJSCE) **1**(5), 174–176 (2011)
10. Bandyopadhyay, S., Datta, B.: Higher LSB layer based audio steganography technique. Int. J. Electron. Commun. Technol. **2**(4) (2011)
11. Hmood, D.N., Khudhiar, K.A., Altaei, M.S.: A new steganographic method for embedded image in audio file. Int. J. Comput. Sci. Secur. (IJCSS) **6**(2), 135–141 (2012)
12. Deepak, D., Karthik, M.L., Manjunath, A.E.: Efficient method to increase robustness in audio steganography. Int. J. Adv. Res. Electr. Electron. Instrum. Eng. **1**(6), 531–536 (2012)
13. Olanrewaju, R.F., Khalifa, O., Abdul Rahman, H.: Increasing the hiding capacity of low-bit encoding audio steganography using a novel embedding technique. World Appl. Sci. J. (Math. Appl. Eng.) **21**, 79–83 (2013)
14. Priyanka, R.B., Vrushabh, R.K., Komal, K.P., Pingle, S.M., Sanghavi Mahesh, R.: Audio steganography using LSB. In: 1st International Conference on Recent Trends in Engineering and Technology, Special Issue of International Journal of electronics, Communication and Soft Computing Science and Engineering, pp. 90–92, March 2012
15. Padmashree, G., Venugopala, P.S.: Audio stegnography and cryptography: using LSB algorithm at 4th and 5th LSB layers. Int. J. Eng. Innov. Technol. (IJEIT) **2**(4), 177–181 (2012)
16. Patil, B.A., Chakkarwar, V.A.: Review of an improved audio steganographic technique over LSB through random based approach. IOSR J. Comput. Eng. (IOSR-JCE) **9**(1), 30–34 (2013)
17. Sheikhan, M., Asadollahi, K., Shahnazi, R.: Improvement of embedding capacity and quality of DWT-based audio steganography systems. World Appl. Sci. J. **13**(3), 507–516 (2011)
18. Prabu, A.V., Srinivasarao, S., Apparao, T., Rao, M.J., Rao, K.B.: Audio encryption in handsets. Int. J. Comput. Appl. **40**(6), 40–45 (2012)
19. Zameer, F., Tarun, K.: Audio steganography using DES algorithm. In: Proceedings of the 5th National Conference, New Delhi, India (2011)
20. Dengre, A.R., Gawande, A.D., Deshmukh, A.B.: Effect of audio steganography based on LSB insertion with image watermarking using AVI video. Int. J. Appl. Innov. Eng. Manag. (IJAIEM) **2**(6), 363–370 (2013)

21. Sathishkumar, G., Bhoopathy, K., Sriraam, N.: Image encryption based on diffusion and multiple chaotic maps. Int. J. Netw. Secur. Appl. (IJNSA) **3**(2) (2011)
22. Hung, K.: A study on efficient chaotic image encryption schemes, Department of Electronic Engineering, City University of Hong Kong, Master thesis (2007)
23. Stallings, W.: Cryptography and Network Security Principles and Practice, 5th edn. Prentice Hall, Boca Raton (2011)
24. Andrade, J., Campos, M., Apolinario, J.: Speech privacy for modern mobile communication systems. In: Proceedings of IEEE Conference on Acoustics, Speech, and Signal Processing, pp. 1777–1780. IEEE Press, Nevada (2008)
25. Awad, A., Saadane, A.: New chaotic permutation methods for image encryption. IAENG Int. J. Comput. Sci. **37**(4), 14–21 (2010)
26. Zielinska, E., Mazurczyk, W., Szczypiorski, K.: Trends in steganography. Commun. ACM **57**(3), 86–95 (2014)
27. Sinha, N., Bhowmick, A., Kishore, B.: Encrypted information hiding using audio steganography and audio cryptography. Int. J. Comput. Appl. **112**(5) (2015)
28. Krishnan, S., Abdullah, M.S.: Enhanced security audio steganography by using higher least significant bit. J. Adv. Res. Comput. Appl. **2**(1), 39–54 (2016)