Al - Saeed University Journal of Applied Sciences
journal@alsaeeduni.edu.ye
Vol (8), No (1), Aug., 2025
ISSN: 2616 - 6305 (Print) ISSN: 2790-7554 (Online)

Encrypted Text Steganography in Audio Files Using ECC, LSB and Chaotic Maps

Abdullah Jaafar
Department of Computer Science
Faculty of Computers and Information Technology
Turba Branch, University of Taiz, Taiz, Yemen
dr.abdullahjaafar@yahoo.com

Mayadah Abdullwale
Department of Computer Science
Faculty of Applied Sciences
University of Taiz, Taiz, Yemen
Almthhgy2020@gmail.com

Ahmed Abdulqader Mohammed
Department of Computer Science
Faculty of Computers and Information Technology
Turba Branch, University of Taiz, Taiz, Yemen
ahmed772338911@gmail.com

Received: 3/7/2025 **Accepted: 2/8/2025**

Journal Website: **https://journal.alsaeeduni.edu.ye**

إخفاء النصوص المشفرة في ملفات الصوت باستخدام ECC وLSB والخرائط الفوضوية

الباحث/ عبدالله جعفر
قسم علوم حاسوب، كلية الحاسبات وتقنية المعلومات
جامعة تعز فرع التربة، اليمن

الباحثة/ مياده عبدالولي
قسم علوم حاسوب، كلية العلوم التطبيقية
جامعة تعز ، اليمن

الباحث/ احمد عبدالقادر
قسم علوم حاسوب، كلية الحاسبات وتقنية المعلومات
جامعة تعز فرع التربة، اليمن

الملخص

يضمن التخفي نقلًا آمنًا للبيانات من خلال إخفاء المعلومات الحساسة داخل ملفات ناقلة غير ضارة، مثل الصوت، لتجنب الكشف. تقترح هذه الورقة إطارًا متينًا للتخفي يجمع بين تشفير المنحنى الإهليلجي (ECC) للتشفير مع التخفي الصوتي القائم على أقل بت أهمية (LSB)، مع تعزيزه بخرائط فوضوية لتحسين الأمان وعدم القدرة على التنبؤ. تبدأ المنهجية بتشفير البيانات السرية باستخدام ECC، مستفيدةً من أمانها العالي بأحجام مفاتيح صغيرة، ثم تُدمج النص المشفر في ملفات صوتية عبر استبدال ديناميكي لأقل بت أهمية، مسترشدةً بتسلسلات فوضوية لتوزيع مواقع البتات عشوائيًا. تُظهر التقييمات التجريبية فعالية هذا النظام في الحفاظ على دقة الصوت (يتم تقييمه عبر مقاييس PSNR وSNR) مع ضمان قدرة تضمين عالية ومتانة ضد تحليل التخفي. يؤكد تحليل الأمان على قدرته على مواجهة هجمات القوة الغاشمة والانتروبيا بفضل الحماية ثنائية الطبقات التي توفرها تقنية ECC والتوزيع العشوائي الفوضوي. تقدم هذه الدراسة نهجاً مبتكراً يتناول بشكل شامل المتطلبات الأساسية لتقنية التخفي، وهي عدم الإدراك، وسعة التضمين، ومقاومة الكشف، مما يوفر إطاراً موثوقاً به لنقل البيانات السرية في التطبيقات الحساسة أمنياً.

الكلمات المفتاحية: إخفاء المعلومات الصوتية، LSB، تشفير المنحنى الإهليلجي (ECC)، الخرائط الفوضوية، تشفير البيانات، إخفاء المعلومات.

Encrypted Text Steganography in Audio Files Using ECC, LSB and Chaotic Maps

Abdullah Jaafar
Department of Computer Science
Faculty of Computers and Information Technology
Turba Branch, University of Taiz, Yemen

Mayadah Abdullwale
Department of Computer Science
Faculty of Applied Sciences
University of Taiz, Taiz, Yemen

Ahmed Abdulqader Mohammed
Department of Computer Science
Faculty of Computers and Information Tecnology
Turba Branch, University of Taiz, Yemen

Abstract

Steganography ensures secure data transmission by concealing sensitive information within innocuous carrier files, such as audio, to evade detection. This paper proposes a robust steganographic framework that combines Elliptic Curve Cryptography (ECC) for encryption with Least Significant Bit (LSB)-based audio steganography, enhanced by chaotic maps to improve security and unpredictability. The methodology first encrypts the secret data using ECC, leveraging its high security with compact key sizes, and then embeds the ciphertext into audio files via dynamic LSB substitution, guided by chaotic sequences to randomize bit positions. Experimental evaluations demonstrate the scheme's effectiveness in maintaining audio fidelity (assessed via PSNR and SNR metrics) while ensuring high embedding capacity and robustness against steganalysis. Security analysis confirms resilience to brute-force and entropy-based attacks due to the dual-layer protection of ECC and chaotic randomization. This study presents an innovative approach that comprehensively addresses the core steganographic requirements of imperceptibility, embedding capacity, and resistance to detection, thus providing a reliable framework for clandestine data transmission in security sensitive applications.

Keywords: Audio steganography, LSB, Elliptic Curve Cryptography (ECC), Chaotic maps, Data encryption, Information hiding.

Introduction

In the current era characterized by advances in information technology, protecting confidential data and ensuring secure methods for storing and transmitting data has gained great importance. Steganography techniques have emerged as effective strategies for hiding sensitive information within multimedia formats such as images and audio. Among these methods, audio steganography using Least Significant Bit (LSB) stands out as a widely adopted method, allowing secret data to be embedded within an audio file with minimal impact on audio quality [1]. The chaotic maps generate unexpected patterns that complicate the discovery and extraction of hidden information without the appropriate key [2]. In addition, Elliptic Curve Cryptography (ECC) used to encrypt the secret text before hiding it, thus providing an additional layer of security. ECC is known for its ability to provide a high level of security with relatively short key lengths, making it particularly suitable for applications that require high efficiency and strong security [3].

The researchers propose a hybrid approach of cryptography and steganography to achieve a higher level of security when both technologies are used together. In [4], the proposal conducted a comparative study of previous research between cryptography and steganography, where they concluded that the authors cannot guarantee that steganography can be used as an alternative to cryptography because each aspect has its own characteristics; cryptography refers to the process of secret writing by encrypting and decrypting secret messages, while steganography refers to the methods of concealing a secret message in a cover letter in such a way that its entire existence is hidden. Using only one of these techniques will make the system vulnerable to third parties. Therefore, the combination of information hiding and encryption gives more security and strength.

In [5] Abood et al., the authors proposed, as a first stage, to encode the text based on substitution by cutting the first half of the ASCII code and then adding it to the end. Keys are also encrypted and exchanged using an elliptic curve. They are also used as a second stage in the process of hiding the information of the encrypted message in a random and unspecified way. Although their method has a low computational cost, it works on WAV audio only, and is evaluated with PSNR, MSE, and SSIM only.

In [1] Jayapandiyan et al., they proposed a modified eLSB embedding technique to hide a text message in an image file, where the secret message is encrypted into two stages. In the first stage, metadata is created and header information is included in the first few bytes of the cover image. In the second stage, the secret message is stored after processing it by segmenting the repeated words in the cover image in an improved way. While it gives a smaller volume of secret data in the cover file, it requires more complex calculations.

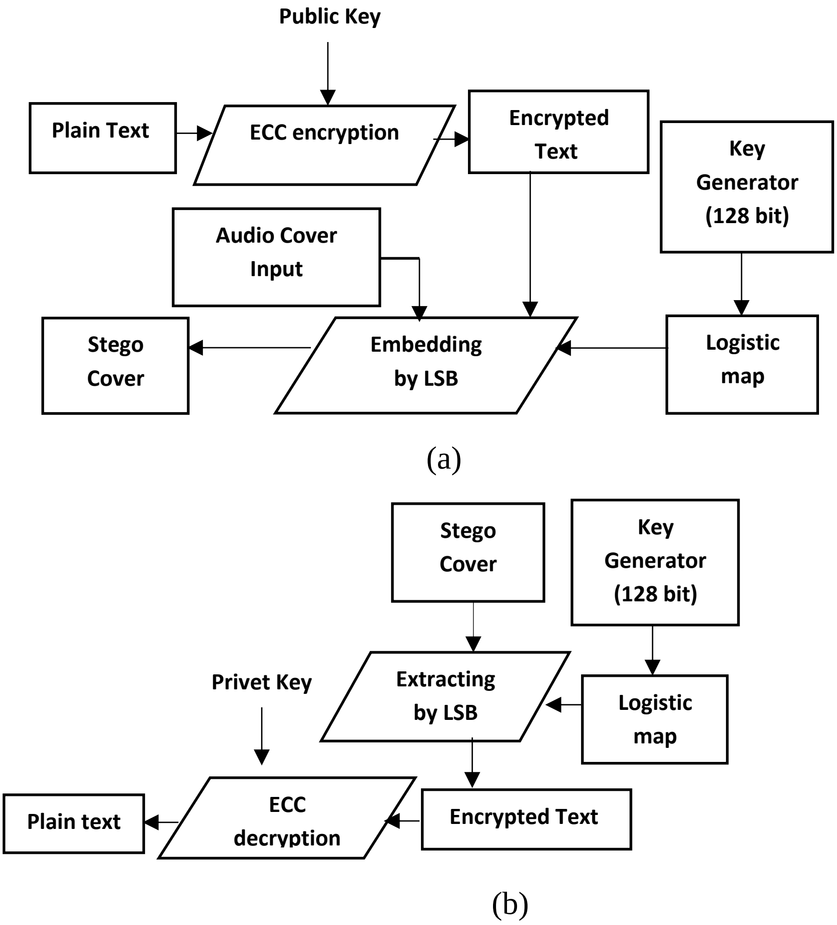
In [6] Manjunath et al., they proposed unexpected steganography chaotic maps, taking them to encrypt the secret message after compressing it using a modified Huffman cipher. The 2D logistic map was improved along with optimized sample selection through Shark Small Optimization (SSO) called Backward Movement Oriented SSO (BM-SSO).

In [7 - 10] are just a few examples of improvements made to LSB audio steganography. These improvements to traditional LSB are undoubtedly more secure as they are more resistant to steganalysis attacks and many have resulted in improved invisibility. Moreover, subjective imperceptibility testing shows that the maximum depth that gives imperceptible distortion is the fourth layer LSB in the case of 16 bits per sample audio sequence [11].

The Proposed Scheme

This section explains the proposed method, which involves encryption and concealment using ECC and LSB. It also shows how to generate random numbers using the logistic map that occurs during the embedding process. Next, the process of extracting and decrypting the information will be explained.

Figure 1 shows the block diagram of the proposed encrypted text steganography scheme, where (a) shows the encrypting and embedding process, (b) shows the extracting and decrypting process.



(a)

(b)

Fig.1 The block diagram of the proposed scheme: (a) the encrypting and embedding process, (b) the extracting and decrypting process

The ECC algorithm is applied to improve the imperviousness of the secret message in the proposed method. If the message is discovered to be hidden in an audio file, it will be necessary to identify its encryption and decryption method. Also in Algorithm 1, to increase the efficiency of the proposed method, a chaotic key generation method is added and used in conjunction with the LSB method.

The key is converted from binary value to decimal value as shown in the following equation (Eq 1):

$$K_{doc} = \sum_{i=1}^{n} k_n(i)\ 2^{-i} \qquad (1)$$

where Kn(i) is bit i in the sequence Kn.

Algorithm 1: Generate the chaotic key used in Embedding Algorithm

```
input: x0 the initial values, and n number of single in Audio cover file
output: key stream
begin
j = 1
x = x0(j)
$\mu$ = 3.99
for I = 1 to n do
    x = $\mu \times x \times (1 - x)$                /* Logistic map */
    $K(i)$ = x
    If (i mod 512 = 0) then
        x0(j) = x
        j = (j mod 16)+1
        x = x0(j)
    end if
end for
[~, $key\_index$] = $sort$(K)
return $key\_index$
end
```

In Algorithm 2, a 128-bit sequence is selected as the key, signals are read from the audio cover file, and the number of individual signals as well as the length of the text data file are determined. In addition to converting the data into bits, the data is then read from a secret file, the byte is converted into 8 bits, and the embedding process is carried out according to some mathematical operations from the logistic map. Then, the data is extracted and the hidden data is decrypted using Algorithm 3.

Algorithm 2: The Embedding Algorithm

Input: The message to be hidden, the cover Audio, and the stego-key.

Output: Stego Audio.

```
Begin
Select a sequence of 128 bits as the key.
Read signals from the audio cover file.
n = number of single in Audio cover file;
Msg = EllipticCurveEncrypion (Msg) // Encrypting Msg using Elliptic Curve
m = length of secret data file;
k = logistic_map(key , n);
A = convert_to_32bits(m)
L = Bit per sample                    // 8 bit or 16 bit
b = $2^L - 2$;
For I = 1 to 32 do
    signal(k(i)) = ((signal(k(i)) and b) or A[i])
end For;
i = 33;
while not end of secret data file and i<=n do
    Read byte(BS) from the secret data file
    A = convert_byte_to_8bits(BS)
    for j = 1 to 8 do
        signal(k(i)) = ((signal(k(i)) and b) or A[j])
        i = i+1;
        if i > n then
            No more sub- single for embedding data;
            Exit the application;
        end if;
    end for;
end While;
end
```

Algorithm 3: The Extracting Algorithm

Input: The stego Audio, the stego-key.

Output: The secret message.

```
begin
Select a sequence of 128 bits as the key.
Read signals from the stego audio file.
n= number of single in Audio cover file;
k = logistic_map(key , n);
m=0;
for i = 1 to 32 do
    A = signal(k(i)) mod 2
    $m = m+A*2^{32-i}$
end for;
i = 33;
while I <= m do
    C = 0;
    for j = 0 to 7 do
        A = signal(k(i)) mod 2
        $C = C+ A*2^{7-j}$
        i = i+1;
        if i > n then
            Exit the application;
        end if;
    end for;
    N = C
    Write the byte(N) into the new secret data file
end While;
Msg = EllipticCurveDecrypion (Msg) // Decrypting Msg using Elliptic Curve
End
```

A set of experiments was conducted using six different audio files and different message sizes. Figure (2) shows the original audio and the stego audio and that the original audio does not differ to some extent from the stego audio.

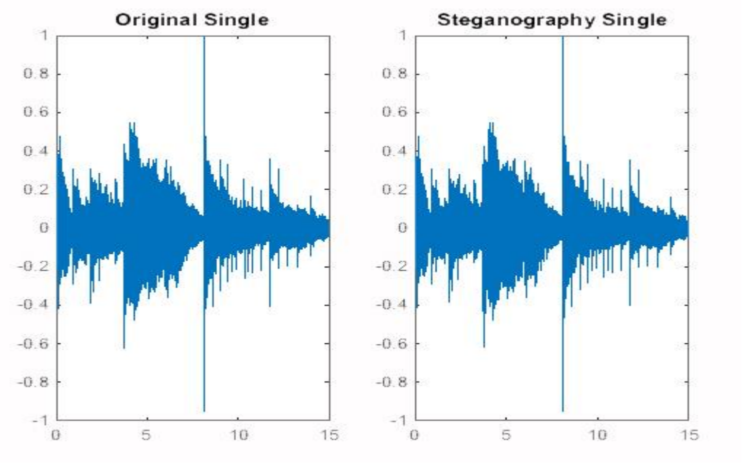


Fig.2 Original and stego audio signals

Results and Discussion

This section discusses the experimental implementation of the proposed scheme. Experiments were conducted using MATLAB R2014b, on a laptop running Windows 7, a 2.5 GHz Core i5 processor, and 4 GB of RAM. Uncompressed audio envelope files from the GTZAN dataset. Furthermore, this scheme can be effectively applied to multiple multimedia file formats, such as MIDI for digital music data, and MP3 for audio compression.

Histogram Analysis

The histogram of the original audio and stego audio indicates the pixel density in the audio frame represented by the histogram. In the original audio frame, to obtain good hiding of the text to be hidden, the pixels should be approximately uniform. Figure 3 shows the histogram representation of the original audio before and after embedding a secret message size of 100KB using five different audio files. This definitely confirms that the proposed method is resistant to various attacks.

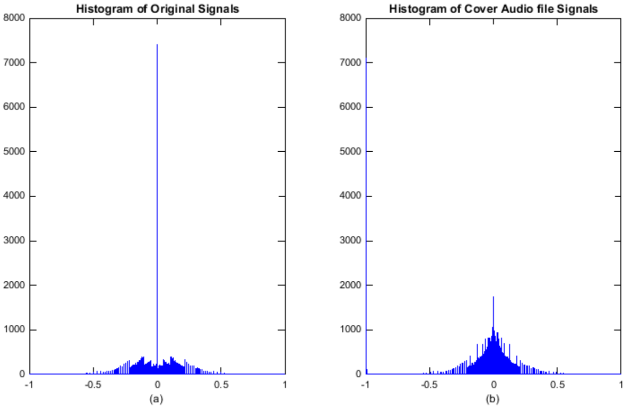


Fig.3 Histogram: (a) original audio signals, (b) cover audio signals

Security Analysis

In this section, we will analyze the strength of the proposed algorithm, as the evaluation process in good information-hiding techniques requires three well-known criteria: robustness, imperceptibility, and capacity.

Robustness:

The strength of the proposed algorithm depends on the masking key that can be used for a long time, and the length of this key is 128 bits. Thus, the key space is the total number of trial keys that can be used for decryption. It contains 2128 groups (1038*3.40), which is practically a huge space. An attacker cannot comprehensively search this number of keys in full and in a short time.

Imperceptibility:

The imperceptibility is the accuracy between the original audio envelope and Stego's audio. To evaluate the accuracy and quality between the original audio envelope and the stego audio, the most common and widely used metrics are PSNR and MSE. PSNR is a model for evaluating the efficiency of the original audio and the stego audio and how similar they are. In contrast, MSE is the statistical difference in pixel values between the original audio and the stego audio. Therefore, the best stego audio can be found when the MSE value is close to zero, the better the quality of information hiding. It is measured in decibels (dB). Moreover, PSNR is inversely proportional to MSE, so the higher the PSNR value, the better the hiding and the less distortion.

MSE is defined as follows [2]:

$$\mathrm{MSE} = \frac{1}{N} \sum_{i=1}^{N} (x1_i - x2_i)^2 \qquad (2)$$

where $x1_i$ and $x2_i$ are the i^{th} samples of the original and stego signals, and N is the number of signal samples.

The PSNR is defined as follows [2]:

$$\mathrm{PSNR} = 10 \log_{10} \frac{(2^n - 1)^2}{\mathrm{MSE}} \qquad (3)$$

where n is the maximum number of bits used to represent each signal sample.

Table 1 presents the MSE and PSNR values for various sizes of the secret message, all indicating a high level of imperceptibility.

Capacity:

SNR is a measure of capacity between original audio and stego audio of the SNR should be more than 20 db. The higher the SNR value, the more indistinguishable the sound from the audio file, which is defined in the equation [2]:

$$\mathrm{SNR} = 10 \log_{10} \frac{\sum_{i=1}^{N} (x1_i)^2}{\sum_{i=1}^{N} (x1_i - x2_i)^2} \qquad (4)$$

where x1i and x2i are the ith samples of the original and stego signals.

In Table 1, our proposed method succeeded in achieving a signal-to-noise ratio (SNR) of 99.99 dB for the Chimes sound.

Table 1.

The PSNR, MSE, SNR values of the proposed steganography system for different audio samples

Audio Sample	Message size (KB)	PSNR	MSE	SNR
music	**1.44**	**73.3483**	**0.003009**	**67.3974**
	36.56	**59.3052**	**0.0763**	**53.3543**
male	**1.44**	**56.4947**	**0.14575**	**50.7053**
female	**1.44**	**54.0611**	**0.25525**	**49.2345**
Guitar tune	**1.44**	**68.6653**	**0.008842**	**62.7192**
	36.56	**54.6174**	**0.2246**	**48.6713**
handle	**1.44**	**69.4268**	**0.00742**	**63.6148**
	36.56	**55.3921**	**0.1879**	**49.5801**
chimes	**1.44**	**54.7643**	**0.0002**	**99.9999**
	36.56	**57.77**	**0.0001**	**0.0845**

Comparison with Related Schemes

In this subsection, according to the ITU standards PESQ, PEAQ, and perceptibility (specifically SNR, MSE, and PSNR), we make a comparison between our scheme and other related schemes as mentioned in Tables 2, 3, 4 respectively. Comparisons have been made with the following schemes [2, 5, 7, 13, 14, 15, 16] according to their published results. It was found that the SNR value of our scheme is 99.99, and thus the signal-to-noise ratio is considered to be somewhat negligible, and it cannot detect the presence of hidden data. Also, the MSE is fairly close to zero, and the closer it is to zero, the lower the average error.

Table 2.
The SNR values for the related schemes

Method	SNR
Ahmed A Alsabhany, Farida Ridzuan, et al [12]	**60.16**
Huwaida T Elshoush and Mahmoud M Mahmoud. [2]	**90.6455**
K Manjunath, GN Kodanda Ramaiah,et al [13]	**25.767**
K Manjunath, GN Kodanda Ramaiah, et al [14]	**29.202**
Enas Wahab Abood, Abdulhssein M Abdullah, et al [5]	**60.6343**
Our scheme	**99.99**

Table 3.
The MSE values for the related schemes

Method	MSE
K Manjunath, GN Kodanda Ramaiah,et al [13]	**0.47686**
K Manjunath, GN Kodanda Ramaiah, et al [14]	**0.16641**
Mahmoud M Mahmoud and Huwaida T Elshoush [7]	**0.279**
Our scheme	**0.0001**

Table 4.
The PSNR values for the related schemes

Method	PSNR
Shirole Rashmi PrakashRao and K Jyothi. [15]	**40.514125**
Hussein Abdulameer Abdulkadhim, et al [16]	**42.2367**
Enas Wahab Abood, Abdulhssein M Abdullah, et al [5]	**60.6332**
Our scheme	**73.3483**

Conclusion:

In this paper, we propose a model for steganography and cryptography. The cryptography process uses Elliptic Curve Cryptography (ECC) after selecting the appropriate curve and its parameters. This encrypted data is then hidden into an audio file using the least significant bit (LSB) method. To enhance security, a chaotic map is used to generate random locations within the audio signal of the ciphertext data. Experimental results show that the proposed system achieves high efficiency in hiding and retrieving data while maintaining audio quality. In addition, it provides a strong level of security against hacking attempts.

References:

[1] J. R. Jayapandiyan, C. Kavitha and K. Sakthivel, "Enhanced Least Significant Bit Replacement Algorithm in Spatial Domain of Steganography Using Character Sequence Optimization," IEEE Access, pp. 136537-136545, 2020.

[2] H. T. ELSHOUSH and M. M. MAHMOUD, "Ameliorating LSB Using Piecewise Linear Chaotic Map and One-Time Pad for Superlative Capacity, Imperceptibility and Secure Audio Steganography," IEEE Access, pp. 33354 - 33380, 6 April 2023.

[3] Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh,” Implementation of Text Encryption using Elliptic Curve Cryptography”, IEEE Access, pp. 73 – 82, 2015.

[4] M. S. Taha, Mohd Shafry Mohd Rahim, Sameer abdulsattar lafta, Mohammed Mahdi Hashim and Hassanain Mahdi Alzuabidi, "Combination of Steganography and Cryptography: A short Survey," International Conference on Sustainable Engineering Techniques (ICSET), 2019.

[5] E. W. Abood, A. M. Abdullah, M. A. A. Sibahe, Z. A. Abduljabbar, V. O. Nyangaresi, S. A. A. Kalafy and M. J. J. Ghrabta, "Audio steganography with enhanced LSB method for securing encrypted text with bit cycling," Bull. Electr. Eng. Informat., p. 185–194, Feb. 2022.

[6] K. Manjunath, G. N. K. Ramaiah and M. N. G. Prasad, "Backward movement oriented shark smell optimization-based audio steganography using encryption and compression strategies," Digit. Signal Process., p. 1–13, Jan. 2022.

[7] M. M. Mahmoud and H. T. Elshoush, "Enhancing LSB using binary message size encoding for high capacity, transparent and secure audio steganography—An innovative approach," IEEE Access, p. 29954–29971, 2022

[8] M. Junaid and K. Farhan, "Enhanced audio LSB steganography for secure communication," Int. J. Adv. Comput. Sci. Appl, p. 340–347, 2016.

[9] G. M. Kamau, ‘‘An enhanced least significant bit steganographic method for information hiding,’’ M.S. thesis, Softw. Eng., Jomo Kenyatta Univ. Agricult. Technol., Juja, Kenya, 2013.

[10] P. G. P. Jaya, B. Hidayat and F. Y. Suratman, "Enhanced LSB steganography with people detection as stego key generator," in Proc. Int. Conf. Signals Syst., p. 99–104, May 2017.

[11] S. M. Alwahbani and H. T. Elshoush, "Hybrid audio steganography and cryptography method based on high least significant bit (LSB) layers and one-time pad—A novel approach.," in Intelligent Systems and Applications (Studies in Computational Intelligence). Cham, Switzerland: Springer, p. 431–453, Jan 2018.

[12] A. A. Alsabhany, F. Ridzuan and A. H. Azni, "The Progressive Multilevel Embedding Method for Audio Steganography," Journal of Physics: Conference Series, May 2020.

[13] K. Manjunath ،G. N. K. Ramaiah M. N. G. Prasad ،"An efficient audio steganography technique using hybridization of compression and cryptography algorithm "،J. Adv. Res. Dyn. Control Syst ،.p. 132–147 1 ،Oct 2020.

[14] K. Manjunath ،G. N. K. Ramaiah M. N. G. Prasad،"Backward movement oriented shark smell optimization-based audio steganography using encryption and compression strategies," Digit. Signal Process., p. 1–13, Jan. 2022.

[15] S. R. PrakashRao and K. Jyothi, "A novel audio steganography technique integrated with a symmetric cryptography: A protection mechanism for secure data outsourcing," Int. J. Comput. Sci. Eng., p. 530, 2021.

[16] H. A. Abdulkadhim and J. N. Shehab, "Audio steganography based on least significant bits algorithm with 4D grid multi-wing hyper-chaotic system," International Journal of Electrical and Computer Engineering (IJECE), pp. 320-330, 1 February 2022.

[17] D. R. I. M. Setiadi, S. Rustad, P. N. Andono and G. F. Shidik, "Digital image steganography survey and investigation (goal, assessment, method, development, and dataset)," Signal Process Elsevier, May 2023.

[18] R. Chakraborty and A. Roy, "Audio steganography—A review," Int.J. Trend Res. Develop., p. 144–149, Jul. 2019.

[19] M. Mustafa, M. Mahmoud, H. Tagelsir and I. Elshoush, "A novel enhanced LSB algorithm for high secure audio steganography," in Proc. 10th Comput. Sci. Electron. Eng. (CEEC), p. 1–6, Sep. 2018.

[20] M. H. N. Azam, F. Ridzuan, M. N. S. M. Sayuti and A. A. Alsabhany, "Balancing the trade-off between capacity and imperceptibility for least significant bit audio steganography method: A new parameter," in Proc. IEEE Conf. Appl., Inf. Netw. Secur. (AINS), p. 48–53, Nov. 2019.

[21] A. A. Alsabhany, F. Ridzuan and A. H. Azni, "The adaptive multilevel phase coding method in audio steganography," IEEE Access, p. 129291–129306, 2019.

[22] J. Kour and D. Verma, "Steganography techniques—A review paper," Int. J. Emerg. Res. Manage. Technol., p. 132–135, May 2014.

[23] A. H. Ali, L. E. George, A. A. Zaidan and M. R. Mokhtar, "High capacity, transparent and secure audio steganography model based on fractal coding and chaotic map in temporal domain," Multimedia Tools Appl., p. 31487–31516, Jun. 2018.

[24] Lindawati and R. Siburian, "Steganography Implementation on Android Smartphone Using the LSB (Least Significant Bit) to MP3 and WAV Audio," IEEE, pp. 170 - 174, 27 - 28 July 2017.