International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 10, No.1 (Apr-2021)

http://dx.doi.org/10.12785/ijcds/100153

# A Comparative Study of Audio Steganography Schemes

**Farah Hemeida[1], Wassim Alexan[1] and Salma Mamdouh[1]**

[1] *Faculty of Information Engineering and Technology, The German University in Cairo, Cairo, Egypt*

*Received 5 Jul. 2020, Revised 31 Aug. 2020, Accepted 30 Nov. 2020, Published 21 Apr. 2021*

**Abstract:** Steganography conceals the existence of secret information, while cryptography hides the meaning of the confidential information. Therefore, combining these two can provide a secure communication between a sender and a receiver. This article proposes a double–layer message security scheme where cryptography is the first layer and steganography is the second layer. AES–256, Blowfish, or a Logistic map is used in the cryptography layer. The LSB substitution technique is used for the steganography layer to embed a secret message inside cover audio. The LSB substitution technique is applied by alternating between the left and the right channels, respectively. Performance of the proposed schemes is evaluated in terms of a hearing test, running time, embedding capacity, waveform plots, as well as a large number of statistical, time–domain, and frequency–domain metrics. Furthermore, a comparison between the proposed scheme using AES–256 and its counterparts from the literature is also provided. The numerical results show that the proposed schemes exhibit very good performance.

**Keywords:** Audio steganography, AES–256, Blowfish , Logistic map, LSB.

## 1. INTRODUCTION

Steganography is the science of hiding the existence of information, so that it cannot be detected. The aim of steganography is to avoid drawing suspicion to the transmission of the concealed data and to secure communication in a completely undetectable manner [1]. In a steganographic scenario, the secret information is hidden in another object called the cover object to form the stego object, which can be saved and transmitted [2]. There are many types of steganography where different cover objects can be used including text [3], audio [4, 5, 6, 7], video [8, 9], 2D images [10, 11], 3D images [12, 13, 14, 15], as well as information matrices [16]. In audio steganography, the secret information is hidden in digital audio signals which results in a slight change in the cover audio, however this change is unrecognizable since audio steganography makes use of the psycho–acoustical masking phenomenon of the human auditory system (HAS) [17]. Audio steganography is more challenging to perform since the human auditory system (HAS) is more sensitive than the human visual system (HVS) [18]. While there may be a large number of methods to hide secret information in audio signals, the most common ones utilize the least significant bit (LSB) algorithm. Such algorithms basically alter the LSBs of the cover audio file with the secret message bits. The LSB is the rightmost bit of a binary integer [7]. Fig. 1 illustrates this process.

On the other hand, cryptography scrambles the structure of a message to make the message meaningless, unless a decryption key is available. Therefore, cryptography enables the transmission of secret information between the sender and the receiver without enabling a third party to read the secret information [7]. The plaintext, which is the secret message, is encrypted by the sender using the key and then the ciphertext is sent to the receiver. The encrypted message is decrypted by the receiver to retrieve the secret message by using the key [19]. There are two types of cryptography; symmetric key cryptography and asymmetric key cryptography. Symmetric key cryptography also known as secret key cryptography uses the same key for both encryption and decryption. The key is only shared among the sender and the receiver and kept secret from any third party. Asymmetric key cryptography, also known as public key cryptography, uses two different keys; one for encryption and the other for decryption. The key used for encryption is public and the key used for decryption is secret or private [20]. The advanced encryption standard (AES) is an example of a symmetric key algorithm that encrypts and decrypts secret data in blocks of 128 bits. It supports key lengths of 128, 192 and 256 bits. The size of the

*E-mail: farah.hemeida@gmail.com, wassim.alexan@ieee.org, salmasadek1597@gmail.com*


Figure 1. LSB substitution.

ciphertext produced from AES is the same as that of the plaintext. AES is based on a design principle known as the substitution permutation network [19]. Blowfish is another example of a symmetric key algorithm that encrypts and decrypts secret data in blocks of 64 bits. The key used in Blowfish can have a length that ranges from 32 to 448 bits. The Blowfish algorithm is based on a Feistel network, iterating a simple encryption function 16 times [21]. On the other hand, Chaos theory provides non–deterministic systems that are based on randomness and non–linearities [22]. Cryptographic systems based on chaotic systems can be constructed and used as symmetric cryptography techniques due to the sensitivity of a chaotic system to the initial value or seed used [23, 24]. A Logistic map is one such example, such that it is used to generate random numbers which are then converted to a binary stream and employed as an encryption key.

The combined use of cryptography and steganography techniques offers a plethora of very secured message transmission systems. The literature is in fact rich with examples that carry out both techniques before transmitting a message over unsecured channels such as the internet [3, 4, 6, 7, 10, 25, 26].

Therefore, cryptography can protect the secret message, but not hide its existence. However, steganography focuses on the degree of invisibility of the secret message. The purpose of steganography is partly defeated once the existence of the secret data is revealed or even suspected. Combining cryptography with steganography tremendously increases the strength of steganography, allowing for more secured communication [25, 26].

As a matter of fact, there are many applications for steganography and cryptography in different fields. Steganography can be used to hide plans for a new invention or to hide a secret chemical formula in the business world. Moreover, it can be used for corporate espionage or by terrorists to coordinate attacks and to keep their communications secret. There are many peaceful applications as well. These include map making and adding fictional names to mailing lists as a check against unauthorized resellers. Furthermore, steganography can be used in watermarking to protect a copyright on information. In addition, photo collections on CDs and DVDs have hidden messages which are used to detect unauthorized use [27].

In this article, the authors extend their work previously published as a conference paper in [28] where Blowfish encryption was carried out and followed by LSB embedding in audio files. While in [28] only the Blowfish algorithm was employed for the encryption part, in this article a comparative study is carried out among the following encryption algorithms: Blowfish, AES and a Logistic map. Furthermore, the performance evaluation has been significantly increased, carrying out an extensive evaluation in terms of multiple new metrics, as well as a comparison with another counterpart scheme from the literature [4]. More specifically, in this article, a double–layer message security scheme is proposed. The first layer is the cryptography layer where encryption takes place at the sender side and decryption takes place at the receiver side, implementing either AES–256, Blowfish, or a Logistic map. The second layer is the steganography layer which implements the LSB substitution technique which is carried out by alternating between the left and right channels of a cover audio file. The rest of the article is organized as follows. Section 2 carries out a state–of–the–art review. Section 3 discusses the proposed scheme. Section 4 presents the numerical results and finally Section 5 draws the conclusions. An appendix is provided at the end, with links to the cover and stego audio files.

## 2. LITERATURE REVIEW

Steganography and cryptography have been gaining a lot of attention by researchers in different fields in the last few years. In [4], the secret message is encrypted using AES–128. Next, the encrypted message is LSB embedded inside cover audio using a tan Logistic map generated sequence. The MSE, PSNR, a hearing test and waveform plots are used to evaluate the performance of the proposed scheme. In [7], the authors carry out bit permutation of their message before the steganography step. Furthermore, they carry out a validation step, in terms of a checksum, at the receiver side to make sure that the secret message has not been intercepted by a third party or tampered with. The employed performance evaluation metrics utilized in [7] were the MSE, PSNR and a $\chi^2$ calculation for the probability of message interception. In [29], the authors proposed a technique utilizing the RSA algorithm and LSB audio steganography. Only waveform plots were employed for performance evaluation purposes. Moreover, the authors of [30] proposed two methods to hide secret information in cover audio using the LSB coding technique along with encryption. The first technique utilizes the parity of the digital samples of the cover audio and the other utilizes the XOR operation. In addition, the authors of [6] proposed two different double–layer message security schemes where the first layer is a cryptography layer, which applies AES–128, and the second layer is the steganography layer, which

applies the LSB substitution technique. The authors of this article carried out similar performance evaluations as those of [4], for their proposed technique which implemented AES alongside LSB embedding in an audio file. Furthermore, the authors of [31] proposed a new way for hiding data using a mixture of text encryption, audio steganography and audio encryption. First, a modified Vigenère cipher algorithm is used to encrypt the original text message. Then, the cipher text is LSB embedded inside cover audio. Finally, transposition using the Blum Blum Shub pseudo random number generator is performed on the stego audio. This encrypted stego audio is transmitted to the receiver and the proposed scheme is evaluated by providing the waveforms of the original audio file, the stego audio file containing the encrypted text, and the encrypted stego audio file after transposition. The authors of [32] proposed a multilayer security technique by combining RSA cryptography and dual audio steganography for a higher level of security. Moreover, the authors of [33] proposed an audio steganography scheme where the data hiding points are selected randomly such that they change with every new embedding process. Therefore, the embedding process randomly varies from 1 LSB to 7 LSB. In addition, the authors of [34] proposed an audio steganography technique based on a random approach and uses the PKE algorithm to provide security. The paper combines steganography with cryptography as well. The authors of [35] proposed a three–level security technique where the first level uses a DNA based playfair encryption. The second level hides the encrypted secret file in a randomly generated DNA sequence. The embedded DNA is hidden in an audio file in the third level.

However, in this article, a comparative study is carried out, implementing and comparing the use of AES, Blowfish as well as a Logistic map. Then, LSB substitution is carried out inside a number of audio files. This article mainly extends the work [28], and compares between the different proposed schemes. Furthermore, this article carries out a deep examination of the morphological changes that affect the audio file upon carrying out the LSB substitution. Those include a security analysis and a performance evaluation.

## 3. PROPOSED SCHEME

Fig. 2 shows the block diagram of the proposed message security scheme at the sender side which is the left half and at the receiver side which is the right half.

### A. Sender Side

First, the samples of the cover audio are represented by signed 16–bit integers ranging from $-2^{15}$ until $2^{15}-1$. Therefore, in order to represent the sample values in binary, they have to be positive. That is why $2^{15}$ is added to the sample values to be able to convert them into binary where each sample value is represented by 16 bits.

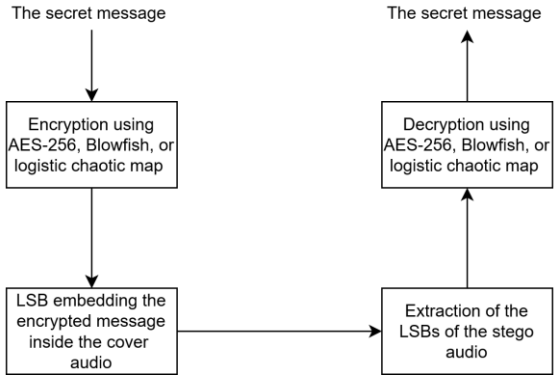



Figure 2. Block diagram illustrating the proposed message security scheme.

Then, the secret message is encrypted using either AES–256, Blowfish, or a Logistic map. The length of the key used for AES–256 and Blowfish is 256 bits. The Logistic map used has a non–linear iterative equation defined as

$$x_{k+1} = \mu\, x_k(1 - x_k), \quad (1)$$

where $x_k \in ]0,1[$ and the parameter $\mu \in ]3,4]$ to generate a random sequence of real numbers. A threshold $\gamma_{th}$ is then chosen and the generated real numbers $x_{k+1}$ are compared to it as follows, generating the secret key bits

$$b_i = \begin{cases} 0 & x_{k+1} < \gamma_{th,} \\ 1 & x_{k+1} > \gamma_{th.} \end{cases} \quad (2)$$

This process continues until a key having the same length as that of the secret message binary stream is generated. Next, the key is XORed with the secret message binary stream, producing the ciphertext. The characteristics of the generated key from the Logistic map is very similar to that of white noise. For the proposed scheme utilizing the Logistic map, an initial seed is chosen to have a value of $x_0 = 0.5$, a control parameter of $\mu = 3.6$ and threshold of $\gamma_{th} = 0.6$ is employed. Next, the ciphertext is LSB embedded in the samples of the cover audio by alternating between the left and the right channels of the cover audio file, respectively. Lastly, $2^{15}$ is subtracted from the sample values after converting them back to decimal values to be able to form the stego audio file.

### B. Receiver Side

$2^{15}$ is added to the stego audio samples received to be able to convert them back to a binary stream. Next, the LSBs are extracted by alternating between the left channel and the right channel, respectively, forming the encrypted message which is then decrypted, utilizing either AES–256, Blowfish, or the Logistic map. The key

for decryption is the same as that for encryption since both AES–256 and Blowfish are symmetric key algorithms. Moreover, the Logistic map used for generating the decryption key is the same as that used for generating the encryption key with the same parameters ($x_0$, $\mu$ and $\gamma_{th}$). Thus, the encryption and decryption keys are identical and easily generated by the Logistic map at both of the sender and receiver sides. Finally, the decryption key is XORed with the encrypted message, resulting in the plaintext of the secret message.

## 4. NUMERICAL RESULTS

The proposed security scheme is implemented using Wolfram Mathematica® 11.3 on a machine with an operating system of Microsoft Windows® 10 and a processor of Intel® Core™ i7–5500U CPU @ 2.4 GHz with 16 GB of RAM. The first 600,000 characters of the novel Pride and Prejudice are used as the secret message to be encrypted and embedded inside the cover audio. Different music genres are used as the cover audio. Those include classic, country, pop, rock and slow. The cover audio is a .wav file with a sampling rate of 44.1 kHz. The duration of the cover audio is 1 minute. The proposed scheme is evaluated for each cryptographic algorithm used in terms of performance and security, as showcased in the next subsections. Furthermore, a comparison is carried out between the performance of the proposed scheme using AES–256 with its counterparts from the literature.

### *A. Performance Evaluation*

The simplest test to gauge the performance of the employed steganography technique is a hearing test. A hearing test is performed to detect any differences between the cover audio and the stego audio by attentively listening to both of them. The links of the cover audio and the stego audio using each cryptographic algorithm are provided in Appendix A. No audible difference can be detected between the cover audio and the stego audio using each cryptographic algorithm. This proves the effectiveness of the proposed scheme.

Fig. 3 shows a comparison between the waveform plot of the classic cover audio and the waveform plots of the stego classic audio using AES–256, Blowfish and the Logistic map that were obtained from the proposed scheme. For each scheme, there exist 2 waveform plots, one for each audio channel (since the used audio files are stereo, with a left channel and a right channel). It is clear that there is no observable difference between the waveform plots that the human eye can detect, therefore the superiority of steganographic ability of the proposed scheme is showcased.

Tables I, II and III show the performance of the proposed scheme using AES–256, Blowfish and the Logistic map respectively for the five music genres. It can be seen that the performance using the three

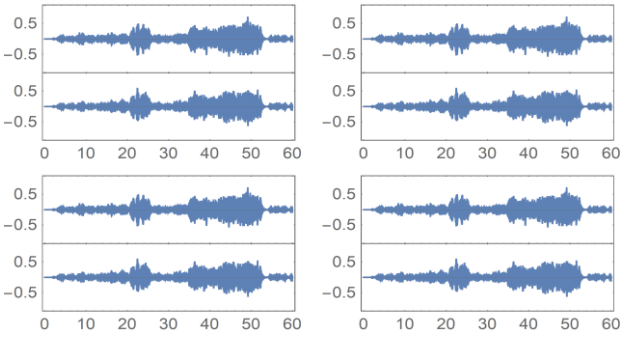



Figure 3. Waveform plot of the cover classic audio (top left) followed by waveform plots of the stego classic audio using AES, Blowfish and the Logistic map respectively in a clockwise direction.

cryptographic algorithms is very similar, there are only slight differences in the values of the mean squared error (MSE) and peak signal–to–noise ratio (PSNR). The pop music genre always exhibits the highest PSNR value. It can also be observed that the time used for encryption and embedding ($t_E$) is relatively higher than the time used for extraction and decryption ($t_D$) for all music genres using AES–256, Blowfish and the Logistic map. The country music genre has the lowest total running time ($t_T$) using AES–256, Blowfish and the Logistic map. On the other hand, the rock music genre has the highest $t_T$ using AES–256 and the slow music genre has the highest $t_T$ using Blowfish. In addition, the classic music genre has the highest $t_T$ using the Logistic map. The overall performance of the proposed scheme is very good with high values for the PSNR and low values for the MSE using AES–256, Blowfish and the Logistic map.

Table IV compares 3 intensity properties of the cover and the stego audio files. Those include power, given in terms of the mean of the squared values; the root mean square (RMS) of the values; and finally the loudness, computed with Stevens' power law ($power^{0.67}$). Across all 3 metrics, the obtained values are near–identical.

Table V compares 4 time–domain properties of the cover and the stego audio files. Those include the crest factor (CF), computed as the maximum divided by the RMS; the peak–to–average power ratio (PAPR), computed as the maximum power divided by the average power; the temporal centroid (TC) values; and finally, the number of zero crossings (ZC). Across all 4 metrics, the obtained values are near–identical.

Table VI compares 7 frequency–domain properties of the cover and the stego audio files. Those include the centroid of the power spectrum; the spectral crest, computed as the maximum divided by the mean of the power spectrum; the spectral flatness, computed as the geometric mean divided by the mean of the power

spectrum; the spectral kurtosis, computed as the kurtosis of the magnitude spectrum [36]; the spectral roll off, computed as the frequency below which most of the energy is concentrated; the skewness and the estimated slope of the magnitude spectrum; and finally, the spectral spread which is a measure of the bandwidth of the power spectrum. Across all 7 metrics, the obtained values are near–identical.

### B. *Security Analysis*

Statistical tests are performed in order to make sure that the security system is robust against attacks [37].

Table VII compares the basic histogram properties of the cover and the stego audio files. Those include the maximum and minimum values, as well as statistical measures, including the mean, median and standard deviation of the values. Except for the median, all other metrics are near–identical.

Table VIII shows a comparison between the information entropy of the cover and the stego audio files. Information entropy is a measure of the amount of information in a file. Thus, while all 4 values are near–identical, it is only natural for the cover audio file to exhibit a slightly lower entropy value in comparison with any of the stego audio files.

Table IX shows the statistical analysis for the stego audio files. Those include the correlation, R measurement, normalized cross correlation (NCC) and audio fidelity. All of the values are exactly equal to 1 which indicate that the stego audio files are exactly the same as the cover audio file without observing any difference due to embedding.

### C. *Comparisons with the Literature*

Finally, Table X shows a comparison between the proposed scheme using AES–256 and other proposed schemes from the literature in terms of the PSNR. The scheme proposed in [4] theoretically offers a better performance. But this is the case because it utilizes less capacity with a secret message length of only 30,000 characters, while the proposed scheme allows a capacity of double that size (600,000 characters). Moreover, the proposed scheme has a better performance than the scheme proposed in [5].

TABLE I. PERFORMANCE EVALUATION USING AES–256.

| Music Genre | Performance evaluation metrics | | | | |
|---|---|---|---|---|---|
| | ***MSE*** | ***PSNR*** | $t_E$ | $t_D$ | $t_T$ |
| Classic | 0.453775 | 91.0097 | 49.4647297 | 49.2809709 | 98.7457006 |
| Country | 0.453333 | 91.0078 | 54.2392871 | 36.1283536 | 90.3676407 |
| Pop | 0.453803 | 93.7401 | 52.5489674 | 48.1214963 | 100.6704637 |
| Rock | 0.453573 | 90.6892 | 66.6119466 | 53.2056099 | 119.8175565 |
| Slow | 0.453492 | 90.6466 | 58.7000650 | 33.8096768 | 92.5097418 |

TABLE II. PERFORMANCE EVALUATION USING BLOWFISH.

| Music Genre | Performance evaluation metrics | | | | |
|---|---|---|---|---|---|
| | ***MSE*** | ***PSNR*** | $t_E$ | $t_D$ | $t_T$ |
| Classic | 0.453479 | 91.0126 | 50.5976085 | 49.1573488 | 99.7549573 |
| Country | 0.453146 | 91.0096 | 54.6617297 | 33.7926881 | 88.4544178 |
| Pop | 0.453474 | 93.7432 | 52.0072593 | 55.8056268 | 107.8128861 |
| Rock | 0.453011 | 90.6946 | 60.7292736 | 52.2931510 | 113.0224246 |
| Slow | 0.453375 | 90.6477 | 71.2578557 | 58.9732941 | 130.2311498 |

TABLE III. PERFORMANCE EVALUATION USING THE LOGISTIC MAP.

| Music Genre | Performance evaluation metrics | | | | |
|---|---|---|---|---|---|
| | ***MSE*** | ***PSNR*** | $t_E$ | $t_D$ | $t_T$ |
| Classic | 0.45462 | 91.0016 | 80.6529035 | 74.4944390 | 155.1473425 |
| Country | 0.453422 | 91.0069 | 69.6062351 | 48.2883989 | 117.894634 |
| Pop | 0.453806 | 93.74 | 66.1871743 | 62.0765213 | 128.2636956 |
| Rock | 0.457118 | 90.6554 | 72.3486332 | 67.2795474 | 139.6281806 |
| Slow | 0.453199 | 90.6494 | 78.1523112 | 62.8629575 | 141.0152687 |

TABLE IV. INTENSITY PROPERTIES.

| Property | Audio file | | | |
|---|---|---|---|---|
| | ***Cover*** | ***Stego AES*** | ***Stego Blowfish*** | ***Stego Chaotic*** |
| Power | 0.00379443 | 0.00379443 | 0.00379443 | 0.00379443 |
| RMS Amplitude | 0.061599 | 0.0615989 | 0.061599 | 0.0615989 |
| Loudness | 0.0238797 | 0.0238797 | 0.0238797 | 0.0238797 |

TABLE V. TIME–DOMAIN PROPERTIES

| Property | Audio file | | | |
|---|---|---|---|---|
| | *Cover* | *Stego AES* | *Stego Blowfish* | *Stego Chaotic* |
| CF | 9.2813 | 9.28155 | 9.28105 | 9.2813 |
| PAPR | 86.1426 | 86.1472 | 86.1379 | 86.1426 |
| TC | 0.635738 | 0.635738 | 0.635737 | 0.635738 |
| ZC Rate | 1652.87 | 1654.07 | 1654 | 1653.9 |

TABLE IX. STATISTICAL ANALYSIS.

| Statistical property | Audio file | | |
|---|---|---|---|
| | *Stego AES* | *Stego Blowfish* | *Stego Chaotic* |
| Correlation | 1 | 1 | 1 |
| R measurement | 1 | 1 | 1 |
| NCC | 1 | 1 | 1 |
| Audio fidelity | 1 | 1 | 1 |

TABLE VI. FREQUENCY–DOMAIN PROPERTIES.

| Property | Audio file | | | |
|---|---|---|---|---|
| | *Cover* | *Stego AES* | *Stego Blowfish* | *Stego Chaotic* |
| Centroid | 648.908 | 648.909 | 648.908 | 648.909 |
| Crest | 2832.85 | 2832.86 | 2832.89 | 2832.85 |
| Flatness | 0.000127782 | 0.000133166 | 0.000103892 | 0.000131275 |
| Kurtosis | 226.415 | 226.419 | 226.411 | 226.417 |
| Roll off | 1124.92 | 1124.92 | 1124.92 | 1124.92 |
| Skewness | 11.0809 | 11.0809 | 11.0807 | 11.0809 |
| Spread | 628.521 | 628.528 | 628.515 | 628.527 |

TABLE VII. HISTOGRAM PROPERTIES.

| Property | Audio file | | | |
|---|---|---|---|---|
| | *Cover* | *Stego AES* | *Stego Blowfish* | *Stego Chaotic* |
| Max | 0.571719 | 0.571734 | 0.571703 | 0.571719 |
| Min | −0.529785 | −0.529755 | −0.52977 | −0.529755 |
| Mean | −0.0000301518 | −0.0000297358 | −0.000029733 | −0.000028574 |
| Median | 0 | 0.0000152593 | 0.0000152593 | 0.0000152593 |
| SD | 0.061599 | 0.0615989 | 0.061599 | 0.061599 |

TABLE VIII. INFORMATION ENTROPY VALUES.

| Audio file | | | |
|---|---|---|---|
| *Cover* | *Stego AES* | *Stego Blowfish* | *Stego Chaotic* |
| 14.3687 | 14.4068 | 14.4066 | 14.4014 |

TABLE X. A COMPARISON BETWEEN THE PSNR VALUE OBTAINED FROM THE PROPOSED SCHEME USING AES–256 WITH THE PSNR VALUES OBTAINED FROM OTHER PROPOSED SCHEMES IN THE LITERATURE.

| Music Genre | Schemes | | | |
|---|---|---|---|---|
| | *Scheme proposed in [4]* | *Scheme proposed in [5]* | *Scheme proposed in [6]* | *Proposed scheme* |
| Classic | 101.971 | 75.8143 | 74.179 | 91.0097 |
| Country | 101.861 | NA | 74.1758 | 91.0078 |
| Pop | 97.7964 | 73.4542 | 74.1801 | 93.7401 |
| Rock | 98.5415 | NA | 74.225 | 90.6892 |
| Slow | NA | NA | 74.2525 | 90.6466 |

## 5. CONCLUSION

This paper proposed a double–layer message security scheme, where the first layer is the cryptography layer, while the second layer is the steganography layer. The proposed scheme utilizes AES–256, Blowfish, or a Logistic map for the cryptography layer. The steganography layer utilizes the LSB substitution technique to hide the encrypted message inside cover audio by alternating between the left and the right channels of the cover audio respectively. The performance of the proposed scheme was evaluated and a security analysis was performed. Furthermore, the performance of the proposed scheme using AES–256 was compared with its counterparts from the literature and was shown to exhibit superior performance in terms of PSNR.

## ACKNOWLEDGMENT

A preliminary version [28] of this work has been published in NILES 2019.

## APPENDIX A. LINKS FOR COVER AND STEGO AUDIO FILES

Cover audio:
https://drive.google.com/open?id=1tIYeLbb33UhTwkh7CY7lv1asCKihPYwV
Stego audio:
https://drive.google.com/open?id=18pXi6MUJbEVVuAX13y6o_IolS3mmxlOy

## REFERENCES

[1] M. M. Amin, M. Salleh, S. Ibrahim, M. R. Katmin and M. Z. I. Shamsuddin, "Information hiding using steganography," in *4th National Conference of Telecommunication Technology, 2003. NCTT 2003 Proceedings.*, 2003.

[2] A. Mane, G. Galshetwar and A. Jeyakumar, "Data hiding technique: Audio steganographyusing lsb technique," *International Journal of Engineering Research and Applications (IJERA)*, vol. 2, p. 1123–1125, 2012.

[3] Z.-L. Yang, X.-Q. Guo, Z.-M. Chen, Y.-F. Huang and Y.-J. Zhang, "RNN-stega: Linguistic steganography based on recurrent neural networks," *IEEE Transactions on Information Forensics and Security*, vol. 14, p. 1280–1295, 2018.

[4] M. T. Elkandoz and W. Alexan, "Logistic Tan Map Based Audio Steganography," in *2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*, 2019.

[5] M. M. Salih and M. Al-Jarrah, "Secret Message Integrity of Audio Steganography Using Bi-LSB Embedding," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 15, p. 20, 2015.

[6] R. Hussein and W. Alexan, "Secure message embedding in audio," in *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, 2019.

[7] P. Jayaram, H. R. Ranganatha and H. S. Anupama, "Information hiding using audio steganography–a survey," *The International Journal of Multimedia & Its Applications (IJMA) Vol*, vol. 3, p. 86–96, 2011.

[8] K. J. Velmurugan and S. Hemavathi, "Video Steganography by Neural Networks Using Hash Function," in *2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)*, 2019.

[9] J. Wang, X. Jia, X. Kang and Y.-Q. Shi, "A cover selection HEVC video steganography based on intra prediction mode," *IEEE Access*, vol. 7, p. 119393–119402, 2019.

[10] W. Alexan, H. Medhat, A. Hamza and H. Hussein, "Sequence-based bit-cycling in double layer message security," in *2018 Advances in Wireless and Optical Communications (RTUWO)*, 2018.

[11] M. Mardanpour and M. A. Z. Chahooki, "Robust transparent image watermarking with Shearlet transform and bidiagonal singular value decomposition," *AEU-International Journal of Electronics and Communications*, vol. 70, p. 790–798, 2016.

[12] S. Farrag and W. Alexan, "A high capacity geometrical domain based 3d image steganography scheme," in *2019 International Conference on Advanced Communication Technologies and Networking (CommNet)*, 2019.

[13] M. T. Elkandoz, W. Alexan and H. H. Hussein, "3D Image Steganography Using Sine Logistic Map and 2D Hyperchaotic Map," in *2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*, 2019.

[14] W. Alexan, M. El Beheiry and O. Gamal–Eldin, "A comparative study among different mathematical sequences in 3d image steganography," *International Journal of Computing and Digital Systems*, vol. 9, p. 545–552, 2020.

[15] S. Farrag and W. Alexan, "Secure 3D data hiding technique based on a mesh traversal algorithm," *Multimedia Tools and Applications*, p. 1–15, 2020.

[16] M. Mashaly, A. El Saied, W. Alexan and A. S. Khalifa, "A Multiple Layer Security Scheme Utilizing Information Matrices," in *2019 Signal Processing: Algorithms, Architectures, Arrangements, and Applications (SPA)*, 2019.

[17] H. A. Prajapati and D. N. G. Chitaliya, "Secured and robust dual image steganography: A survey," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 3, p. 534–542, 2015.

[18] M. Asad, J. Gilani and A. Khalid, "Three layered model for audio steganography," in *2012 International Conference on Emerging*

*Technologies*, 2012.

[19] D. R. Sridevi, P. Vijaya and K. S. Rao, "Image steganography combined with cryptography," *Council for Innovative Research Peer Review Research Publishing System Journal: IJCT*, vol. 9, 2013.

[20] P. Kumar and V. K. Sharma, "Information security based on steganography & cryptography techniques: A review," *International Journal*, vol. 4, p. 246–250, 2014.

[21] S. Manku and K. Vasanth, "Blowfish encryption algorithm for information security," *ARPN journal of engineering and applied sciences*, vol. 10, p. 4717–4719, 2015.

[22] M. Khan and F. Masood, "A novel chaotic image encryption technique based on multiple discrete dynamical maps," *Multimedia Tools and Applications*, vol. 78, p. 26203–26222, 2019.

[23] H. Pan, Y. Lei and C. Jian, "Research on digital image encryption algorithm based on double logistic chaotic map," *EURASIP Journal on Image and Video Processing*, vol. 2018, p. 142, 2018.

[24] F. Masood, J. Ahmad, S. A. Shah, S. S. Jamal and I. Hussain, "A Novel Hybrid Secure Image Encryption Based on Julia Set of Fractals and 3D Lorenz Chaotic Map," *Entropy*, vol. 22, p. 274, 2020.

[25] S. A. Laskar and K. Hemachandran, "High Capacity data hiding using LSB Steganography and Encryption," *International Journal of Database Management Systems*, vol. 4, p. 57, 2012.

[26] V. Sharma and others, "Two new approaches for image steganography using cryptography," in *2015 Third International Conference on Image Information Processing (ICIIP)*, 2015.

[27] R. Doshi, P. Jain and L. Gupta, "Steganography and its Applications in Security," *International Journal of Modern Engineering Research (IJMER)*, vol. 2, p. 4634–4638, 2012.

[28] F. Hemeida, W. Alexan and S. Mamdouh, "Blowfish–Secured Audio Steganography," in *2019 Novel Intelligent and Leading Emerging Sciences Conference (NILES)*, 2019.

[29] A. Gambhir and S. Khara, "Integrating RSA cryptography & audio steganography," in *2016 International Conference on Computing, Communication and Automation (ICCCA)*, 2016.

[30] H. B. Kekre, A. Athawale, S. Rao and U. Athawale, "Information hiding in audio signals," *International Journal of Computer Applications*, vol. 7, p. 14–19, 2010.

[31] N. Sinha, A. Bhowmick and B. Kishore, "Encrypted information hiding using audio steganography and audio cryptography," *International Journal of Computer Applications*, vol. 112, 2015.

[32] K. N. Bangera, N. S. Reddy, Y. Paddambail and G. Shivaprasad, "Multilayer security using RSA cryptography and dual audio steganography," in *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, 2017.

[33] L. Rana and S. Banerjee, "Dual layer randomization in audio steganography using random byte position encoding," *International Journal of Engineering and Innovative Technology*, vol. 2, 2013.

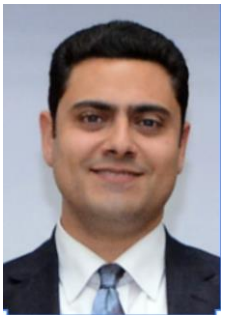
[34] B. A. Patil and V. A. Chakkarwar, "Review of an improved audio steganographic technique over LSB through random based approach," *IOSR J Comput Eng*, vol. 9, p. 30–34, 2013.

[35] C. M. Shyamasree and S. Anees, "Highly secure DNA-based audio steganography," in *2013 International Conference on Recent Trends in Information Technology (ICRTIT)*, 2013.

[36] G. M. Nita, "Spectral Kurtosis statistics of transient signals," *Monthly Notices of the Royal Astronomical Society*, vol. 458, p. 2530–2540, 2016.

[37] M. Mostaghim and R. Boostani, "CVC: Chaotic visual cryptography to enhance steganography," in *2014 11th International ISC Conference on Information Security and Cryptology*, 2014.

**Farah Hemeida** was born in Cairo, Egypt, in 1997. She received the BSc in Communications Engineering from the German University in Cairo in 2020. Her research interests lie in the fields of mobile communications, signal processing, machine learning and security.



**Wassim Alexan** was born in Alexandria, Egypt, in 1987. He received the BSc, MSc and PhD in Communications Engineering and an MBA from the German University in Cairo (GUC), respectively in 2010, 2012, 2017 and 2019. From 2010 till 2017 he was with the Mathematics department and is now an assistant professor at the faculty of Information Engineering and Technology at the GUC. His research interests lie in the fields of wireless communications, security, image and signal processing.

**Salma Mamdouh** was born in Cairo, Egypt, in 1997. She received the BSc in Networks Engineering from the German University in Cairo in 2020. Her research interests lie in the fields of cloud computing, cryptography and steganography.