A Robust Audio Steganography Method Using Partial Knight Tour for Concealing Messages of Text and Image

Abdulmalek A. S. Alqobaty

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

Abstract:

The rapid growth in transfer of data over the Internet realized the need to secured data transmission. Moreover, there is a need to send message that contains a text and image. The steganography is the most promising technique for facilitating the secure communication without affecting the data quality. In this paper, we propose a robust audio steganography approach that hides secret messages of text and image in an audio WAV file using partial knight tour positions in 4×8 square blocks. The cover audio is divided into 4×8 (or 32) audio sample blocks. The secret data are converted to bits and selected 4×8 audio bytes then can hide ASCII codes of 4 characters. The hiding of secret data block is based on a random selected starting audio byte, and on a random selected tour of 32 predefined tours. The algorithm changes the least significant bit (LSB) of the audio bytes based, as mentioned, on randomly selected tours and randomly selected starting audio byte. The resulted stego file can be, then, transmitted over the communication channel such as Internet to the receiver side. After receiving, the extraction process is performed to extract the secret message. The proposed algorithm is implemented us[ing C# programming languages. The PSNR and MSE parameters are used to evaluate the efficiency of the proposed algorithm and they will be checked after implementation. The proposed technique provides a high quality of Peak Signal-to-Noise Ratio (PSNR) and Signal to Noise Ratio (SNR).

Keywords: Audio **s**teganography, LSB, Knight Tour, message hiding, image hiding, text and image hiding.

1- Introduction

With advent of the Internet, the rapid growth in transfer of data over the networks realized the need of secure data transfer. Usually, the secret messages need security measures to be transferred over insecure networks. Several techniques have been introduced to enable the security of data transmission. These techniques are based on the steganography [1] and cryptography [2] concepts. The Steganography is the art and science of hiding sensitive or secret data within a cover message so that no one apart from sender and intended recipient, suspects that a message is existed [3]. In steganography, the content of a cover message is modified with the secret message, and the result message is called stego-message. However, in cryptography, the data is encrypted to secure it from attackers, and then the encrypted data becomes meaningless until is reconstructed in its actual form.

The steganography is the most promising technique for facilitating the secure communication without affecting the data quality. The reason is that an attacker can identify the cryptographic data according to the deformed structure of data. The deformation of

data reveals that some sensitive information is being transmitted over the communication channel. However, in the steganography, the secret message can be embedded in a cover message data and be transmitted to the desired destination, and no one can suspect the existence of message. The steganography techniques use image, audio or video as a cover data for hiding the secret message, which commonly be in form of text. However, it can be image, audio or even video. The shortage of the LSB technique is the ease of extracting data. To overcome this shortage either secret-key or encryption techniques is used. The advantage of the secret-key over cryptographic is that it does not generate overhead. Many audio steganography techniques are proposed. Audio steganography, which hides secret messages in an audio signal [4], has a more potential to conceal data because audio files are often larger than the images, and by small change in the amplitude can store a huge amount of information.

In this work, we propose a robust audio steganography approach that hide text and image as secret message in an audio WAV file is proposed that uses partial knight tour positions in 4×8 square blocks. The cover audio is divided into 4×8 (or 32) audio sample blocks. The secret data are converted to bits and selected 4×8 audio bytes then can hide ASCII codes of 4 characters. The hiding process of secret data block into the audio sample block is performed depending on the positions of Knight in 4×8 chessboard starting from random audio sample positions and using a random selected tour. In other words, the hiding of secret data block is based on a random selected starting audio byte, and on a random selected tour of 32 predefined tours. The algorithm changes the least significant bit (LSB) of the audio bytes based, as mentioned, on randomly selected tours and randomly selected starting audio byte.

The rest of this paper is divided as follows. Section 2 describes the audio steganography model. It presents the applied model for the proposed algorithm. In section 3 we present the literature review is presented. We, then, describe the proposed algorithm in section 4. In section 5, we discuss the implementation and results of the proposed method. Finally, we provide the conclusion in section 6.

2- Audio Steganography Model

To secure a sensitive data, the steganography technique with either a strong stego-key or a cryptographic algorithm is required. The audio steganography techniques use the shortcoming of the Human Auditory System (HAS) to conceal data inside the sound data. To transfer the data securely over insecure channel such as Internet, we use a steganographic technique that applies a complicated stego-key depending on partial knight tour. Although the combination of steganography and cryptography techniques improve the security of sensitive information, it generates an extra data that affects the capacity of data hiding.

The other alternative is to use a strong secret-

key. Our basic model of audio steganography is shown in Figure 1. It consists of a cover file, a secret message, secret-key that is based on knight tour and steganographic algorithm. The cover file is an audio file hides the secret message [5]. The secret message is a data the sender wants to be confidential. Usually, message can be plain text, image, audio, video or any combination of them. The secret-key is used to ensure that only the recipient who knows the corresponding secret-key and algorithm will be able to extract the sent message from a stego-file.

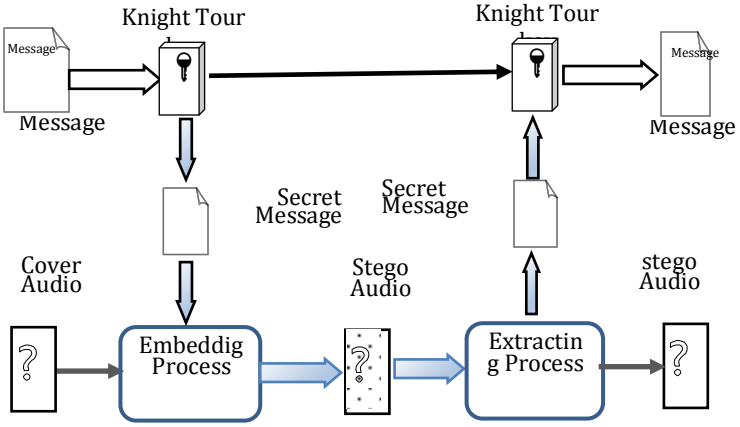


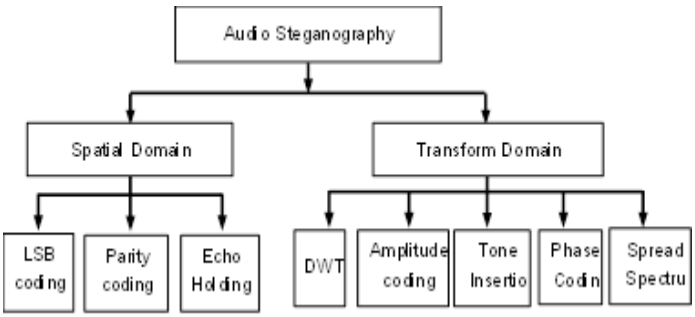
Figure 1: General audio steganography model

The algorithm consists of two process: the embedding process and extracting process. The embedding process consists also of two steps: identifying redundant bits that can be altered without destroying the integrity and exploiting the quality of the cover file. Then, embedding the secret data in the cover file, by replacing the redundant bits in the cover file with bits of the secret data. At the receiver side, the secret data extraction process consists, also, of two steps: first, identifying the secret data bits that was altered by the sender. Second, retrieving the secret message by extracting the bits of secret data embedded in the cover file.

3- Literature Review

Audio steganography, which hides secret messages in an audio cover message. Generally, audio steganography techniques are classified as spatial domain and transform domain [6]. This classification is shown in Figure 2. Mishra at el., however, presents more classes of audio steganographic techniques [7].

The spatial domain techniques include several techniques such as LSB, parity coding and Echo hiding. The LSB encoding technique is commonly used for audio steganography [8]. In LSB encoding, the least significant bits of the cover media are altered to include the secret message. In parity coding technique [9], individual samples are grouped and a parity bit of each group is calculated. Then, check the parity bit of a group of samples, if the parity bit and message bit does not match, then change the LSB's of any one of the individual samples in that group to make the parity bit equal to the message bit, otherwise do not make any changes. In echo hiding [10] method, the secret data is embedded in the echo part of the host audio signal.



In the transform domain, there are several techniques include the spread spectrum, phase coding, tone insertion techniques, DWT and amplitude coding. Cvejic at el. in [11] described audio steganography based on Discrete Wavelet Transform (DWT). Data is embedded in the LSBs of the wavelet coefficients. Therefore, a high capacity of 200 kbps in 44.1 kHz audio signal is achieved. However, to improve the imperceptibility of embedding data in the integer wavelet coefficients authors employed the hearing threshold, and avoided hiding data in silent parts of the audio signal. M. Fallahpour and D. Megias proposed the amplitude-coding method [12]. In this technique, the odd samples are used to generate the interpolated values of the even samples which are used for embedding the secret bits. The method has a capacity of 3 kbps and provides robustness against common audio signal processing. Nugrahaet et al. in [13], presented steganography technique for hiding the audio data using direct spread spectrum sequence mechanism. This model requires a secret-key to embed the data as data will be encoded as noisy signal which is modulated using the pseudo-noise. In the tone insertion method [14], the embedding of data into an audio signal is performed by inserting low power tones in the presence of a stronger tone. The Phase coding method [15] uses the fact that the phase components are not audible to human. In this method, the secret message bits is embedded as phase shift in the phase spectrum of the cover audio signal.

To insure security in audio steganography, the secret key and the combination of cryptography and steganography is presented in several researches. Das et al. in [16] presented audio- steganography model, in which the cover file was a form of audio and the secret message is a plain text. The DWT scheme is applied to generate the coefficients and encrypts these coefficients to generate the embedded audio file for secure transmission. Mohajon et al. in [17] developed improved approach for audio steganography using LSB method. In their work, authors combined security key and genetic algorithm (GA). The combination of cryptography and steganography is proposed in several works, for example, Gambhir et al. in [18] presented a new approach in which the RSA algorithm is applied to generate a cipher, which is processed through the LSB steganography scheme. While, at the receiver side, the same approach is implemented to recover the original data from ciphers and LSB extraction is applied to extract the complete data. Kanhe et al. in [19] introduced advance cryptography-based methods used an AES 128-bit encryption for encrypting the data and an LSB steganography for hiding the data in the cover file.

Recently, other techniques such as compression is used also with steganography in image and audio steganography. Osama F. el at., In [20], presented a comparison of two

different techniques, one used LSB with no encryption and no compression, while the other used a Discrete Cosine Transform (DCT) to transform the image into the frequency domain. Abdulrazzaq et al. in [21] presented a new secure steganography technique to hide images into audio files. The audio files are in the standard WAV format. This method involves compression–encryption of an image file by the GMPR technique and then hiding it into audio data by appropriate bit substitution. The encrypted image bits are hidden into multiple LSB layers.

4- The Proposed Algorithm

In this section, we discuss the proposed audio steganographic technique for securely hiding of secret message (text and/or image) in the Wav audio cover file. In this approach, the cover file is an audio Wav file, while the secret message can be either plain text and/or image data and the hiding method uses least significant bit (LSB) steganography methodology with a secret-key depends on partial knight tour concept. We use two channels to store data bits into the cover file one for text and the other for image.

In the proposed technique, we use the concept of the solution of the knight tour problem. The Knight tour is a continuous move of knight on a chessboard in such a way that it visits every square only once. If the knight moves end in the same square from which it started then is a closed tour otherwise it is open tour. The knight tour problem is the mathematical problem and first mathematician to solve this problem was Leonhard Euler. In 1823 H. C. von Warnsdorf. Schwenk described the method Warnsdorf's rule used to complete the Knight Tour. The number of all directed tours (open and closed) on an 8×8 board are $19,591,828,170,979,904$. [22]. The partial solution, in the proposed solution interests in 4×8 board. The partial tour numbers are totally 246. The number of geometrically distinct complete tours is 7772. This total was first given by Sainte-Marie (1877) [23].

In the proposed technique, the secret knight tour key (KTK) is selected randomly by first starting cell of 32 cells each cell can randomly uses one tour of 32 selected tours of 246 partial tours. Hence, the secret message is divided into multiple 32-bits $(4$-byte) blocks. The block of data is hidden into 32-bytes of the cover audio file based on starting cell and selected knight tour, which constitutes a random 32×32 numbers. In other words, the technique embeds and extracts the secret message into the blocks audio cover file in using randomly selected KTK.

Figure 3 provides an example of one knight tour starts from the first square using one tour of 32 steps. The figure shows that the second bit of data block is stored in the audio sample 18, and the bit 28 of data block is stored in audio sample 6.

1	*20*	*15*	*32*	*11*	*28*	*7*	*26*
14	*17*	*12*	*23*	*4*	*25*	*10*	*29*
21	*2*	*19*	*16*	*31*	*8*	*27*	*6*
18	*13*	*22*	*3*	*24*	*5*	*30*	*9*

Figure 3: Hiding sequence for 32 bits using partial knight tours

We use LSB steganography methodology, which is a simple, fast and popular, to embed information in a digital audio file. An example of embedding the secret message into LSBs is shown in the Figure 4. As shown in the figure, the cover file is organized into 8- bit columns. Also, the secret message is organized as 8-bit column matrex. The stego file is the results of replacing the last bits column of the bytes in the cover file by the message bits using the KTK. On the other hand, to extract the secret message from stego-file, just prepare the file as 8-bit columns. Next, extract the last column bits, then organize them as 8-bit column matrix. Finally, reorganize each 32 bits (4 rows) to get 4 bytes of the secret message using the same KTK that is used in hiding the original secret data.

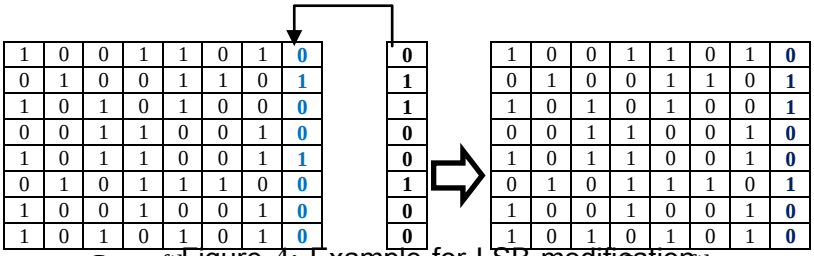


Figure 4: Example for LSB modification Technique for Audio Steganography

Figure 5 shows the flow chart of proposed algorithm. The model has two processes the first one is for hiding the secret message and the other is extracting process. In both processes, the LSB scheme is implemented to divide the secret message and cover file into blocks.

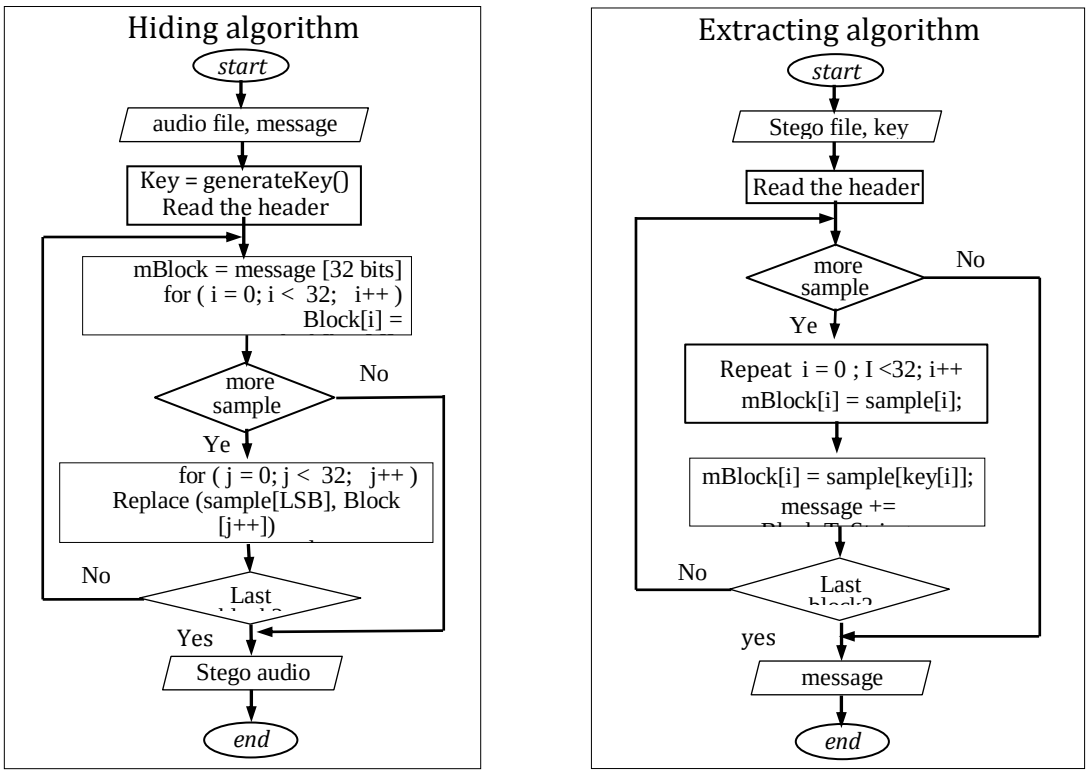


Figure 5: The LSB embedding and extracting protocols for audio steganography

To evaluate the proposed algorithm, we use the three most evaluation criteria for a good algorithm are Robustness, Imperceptibility and

Capacity [x]. Robustness: The strength of our proposed algorithm depends on the KTK which is represented as an array of 32 random integers in the set {0,1,...,31} to select the starting place of hiding data, which forms the first level of security. The hiding key is randomly constructed. Each element can be selected by 32 random knight tour, and hence the key space is $32^{32} \approx 1.5\times10^{48}$, which is a huge number of possible KTK. Moreover, the first position is random since it is computed using random values. Finally, each block of 32 bits (four bytes) of the message is hidden based on the corresponding knight tour, which adds a complexity to steganalysis process and form the third level of security. Therefore, we can say that, the proposed algorithm is robust enough. Imperceptibility: In the proposed technique only the LSN of a byte in cover file is altered, it is visually imperceptible by HAS. The mean square error (MSE) between the cover file and stego-file and peak signal to noise ratio (PSNR) are used for measuring the amount of imperceptibility. These parameters are shown in the results. Capacity: The embedding capacity is the maximum number of bits that can be embedded in a given cover file. The capacity of our proposed algorithm is one bit per byte, and hence the size the cover file controls the embedding capacity.

5- Implementation Results

Both embedding and extracting processes of the proposed algorithm are implemented and tested using C# programming language, as shown in Figures 6 and 7. We apply hiding the secret message with mixed of text and image in the LSB in the audio cover data file.

Figure 6: The embedding algorithm

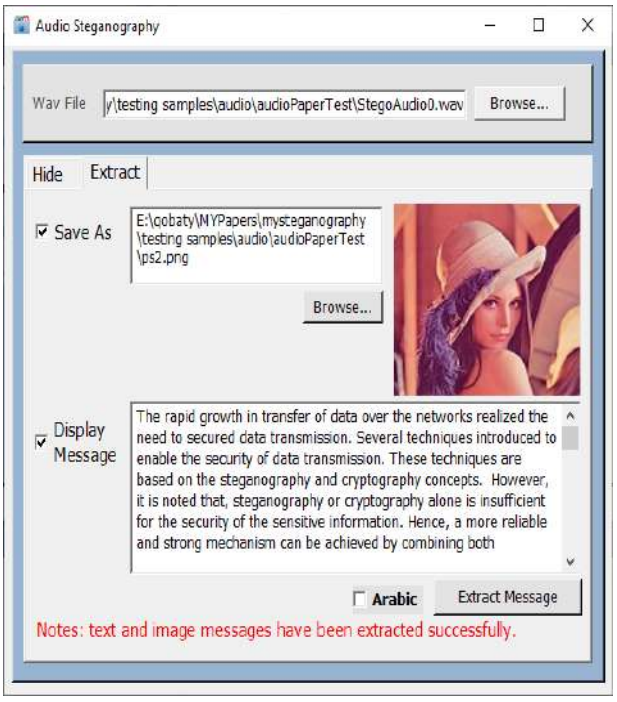


Figure 7: The extraction algorithm

To evaluate the performance of the proposed technique, Mean Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR) are used [y]. Mean Squared Error (MSE) is the average of the square of errors. It is the cumulative squared error between the stego and original cover file. MSE is performed to test if two sounds are similar. MSE calculations could be simply written according to the following equation:

$$M.S.E = \frac{1}{N}\sum_{n=1}^{N}(C_n - S_n)^2$$

Where S_n is the stego-audio signal and C_n is the cover-audio signal such as: $n = 1, \ldots N$.

$$MSE = \frac{1}{mn}\left(\sum_{i=1}^{m}\sum_{j=1}^{n}(C_{ij} - S_{ij})^2\right)$$

The PSNR ratio is used as a measure of quality between the cover file and a stego file; it is a measure of peak error. Higher the PSNR value better the quality of data hiding. The PSNR is a better test since it takes the error and signal strength into consideration. The following equation describes how the value of PSNR is obtained, in which MAX^2 is 256^2.

$$PSNR = 10 \log_{10}\left(MAX^2/_{MSE}\right)$$

Table 1 shows *PSNR* values for maximum allowed hiding rate in selected temporal. The PSNRs for original and stego images, in Table 1, were computed using MATLAB. The cover audio files are WAV CD-quality audio format sampled at 44.1KHz with 16 bits per sample. Hidden message in both text and image is encrypted before the embedding process. The files that is used for testing have been downloaded from the following site:

https://file-examples.com/ index.php/sample-audio-files/sample-wav-download/

Table 1: PSNR at a different message sizes

Secret Message			Total sixe	MSE	PSNR
type	Text	Image			
Size	530 B	1KB	1.5KB	0.0035	72.72
	1 KB	4 KB	5 KB	0.0238	64.40
	2 KB	11 KB	13 KB	0.0756	59.38
	7 KB	14 KB	21 KB	0.106	57.91

6. Conclusion

In many cases secret data may contain text and image. In this paper, we proposed a robust method for embedding a secret data of a plain text and/or image into an audio files using the LSB audio steganography. The proposed method has been, successfully, implemented and tested. For more security, the secret message is hidden using a 32×32 random numbers. Each column value of the 32 random number determines the first random bit position for hiding the block of data bits, and each row value of the second 32 random number determine the way used to hide the block of data bits. It, actually, select the using knight tour to hide the data bits. In the proposed technique, one LSBs has been changed in the cover audio bytes to produce the stego-file. The generated stego-file by the proposed method has high PSNR ratios, which indicate small noise distortions. Usually, the generated stego-audio file is almost identical to the cover audio file, and hence, the embedding is imperceptible.

References

[1] Jiang, N., Zhao, N., & Wang, L. (2016). "LSB based quantum image steganography algorithm", International Journal of Theoretical Physics, 55(1), 107-123.

[2] Abood, M. H. (2017). An efficient image cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms. 2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT). doi:10.1109/ntict.2017.7976154.

[3] R. Chandramouli and N. Memon, "Analysis of LSB based image steganography," IEEE ICIP, pp. 1022-1022, 2001.

[4] Shilpi Mishra, Virendra Kumar Yadav, Munesh Chandra Trivedi and Tarun Shrimal, " Audio Steganography Techniques: A Survey", Advances in Computer and Computational Sciences, Advances in Intelligent Systems and Computing 554, https://doi.org/10.1007/978-981-10-3773-3_56, Springer Nature Singapore Pte Ltd. 2018

[5] Nedeljko Cvej, "Algorithms for audio watermarking and steganography", Oulu 2004, ISBN: 9514273842

[6] Rejoy Chakraborty and Arpan Roy, "Audio Steganography- A Review", International Journal of Trend in Research and Development, Volume 6(3), ISSN: 2394-9333, May – June 2019, www.ijtrd.com

[7] Manisha Verma and Hardeep Singh Saini, Analysis of Various Techniques for Audio Steganography in Data Security, Available online at www.ijsrnsc.org IJSRNSC Volume 7(2), Apr 2019.

[8] M. Asad, J. Gilani, and A. Khalid, "An enhanced least significant bit modification technique for audio steganography", International Conference on Computer Networks and Information Technology (ICCNIT), IEEE, 2011.

[9] H. Kekre, A. Athawale, S. Rao, and U. Athawale, "Information hiding in audio signals", International Journal of Computer Applications, IJCA, vol. 7,no. 9, pp. 14-19, 2010.

[10] F. Djebbar, B. Ayad, H. Hassmam, and K. Abed-Meraim, "A view on latest audio steganography techniques", International Conference on Innovations in Information Technology (IIT), IEEE, 2011.

[11] N. Cvejic, T. Seppanen, "A wavelet domain LSB insertion algorithm for high capacity audio steganography", Proc. 10th IEEE Digital Signal Processing Workshop and 2nd Signal Processing Education Workshop, pp. 5355, 1316 October 2002.

[12] Mehdi Fallahpour and David Megias, "High capacity audio watermarking using FFT amplitude interpolation", IEICE Electron. Express, Vol. 6, No. 14, pp.1057-1063, 2009.

[13] Nugraha, R. M. (2011, July). "Implementation of direct sequence spread spectrum steganography on audio data". In Proceedings of the International Conference on Electrical Engineering and Informatics (pp. 1-6). IEEE, 2011.

[14] K. Gopalan and S. Wenndt, "Audio steganography for covert data transmission by imperceptible tone insertion", Proceedings of Communications Systems and Applications, IEEE, 2004.

[15] M. Nutzinger and J. Wurzer, "A novel phase coding technique for steganography in auditive media", 2011 Sixth International Conference on Availability, Reliability and Security (ARES), IEEE, 2011.

[16] Das, R., Mukherjee, D., Singh, R. S., Godara, S., & Kumar, S. (2017, August). DWTAS: A robust discrete wavelet transform

approach towards audio steganography. In 2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON) (pp. 198-204). IEEE.

[17] Mohajon, J., Ahammed, Z., &Talukder, K. H. (2018, December). An Improved Approach in Audio Steganography Using Genetic Algorithm with K-Bit Symmetric Security Key. In 2018 21st International Conference of Computer and Information Technology (ICCIT) (pp. 1-6). IEEE.

[18] Gambhir, A., &Khara, S. (2016, April). Integrating RSA cryptography & audio steganography. In 2016 International Conference on Computing, Communication and Automation (ICCCA) (pp. 481-484). IEEE.

[19] Kanhe, A., Aghila, G., Kiran, C. Y. S., Ramesh, C. H., Jadav, G., & Raj, M. G. (2015, August). Robust audio steganography based on advanced encryption standards in temporal domain. In 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 1449-1453). IEEE.

[20] Osama F. AbdelWahab, Aziza I. Hussein, Hesham F. A. Hamed, Hamdy M. Kelash, Ashraf A.M. Khalaf, and Hanafy M. Ali," Hiding data in images using steganography techniques with compression algorithms", TELKOMNIKA, Vol.17, No.3, June 2019, pp.1168~1175 ISSN: 1693-6930.

[21] Sazeen T. Abdulrazzaq, Mohammed M. Siddeq, and Marcos A. Rodrigues2, "A Novel Steganography Approach for Audio Files", SN Computer Science (2020) 1:97.

[22] Manjot kaur Bhatia, "Knight Tour for Image Steganography Technique", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-1, October 2019;

[23] Kevin McGown, Ananda Leininger, "Knight's , Oregon State University, MIT and Tour" Oregon State University, 15/8/2002.

[24] A. T. Al-Tamimi and A. Alqobaty, "Image Steganography Using Least Significant Bits (LSBs): A Novel Algorithm", International Journal of Computer Science & Information Security Vol. 13 No. 1, January 2015 , pp. 1-5.

[25] Ashwin P Patil, "AES Hybridization with DWT Audio Steganography", MSc Cyber Security, School of Computing National College of Ireland, 2019.