Wasit Journal for Pure Science

Journal Homepage: https://wjps.uowasit.edu.iq/index.php/wjps/index
e-ISSN: 2790-5241 p-ISSN: 2790-5233

A survey on Rijndael based LSB Audio Steganography techniques

Sajaa G. Mohammed[1]*, Nuhad Salim Al-Mothafar[2]

[1] Department of Mathematics,
College of Science, University of Baghdad, Baghdad, Iraq

[2] Department of Mathematics,
College of Science, University of Baghdad, Baghdad, Iraq

Corresponding Author* Sajaa G. Mohammed:

DOI: https://doi.org/10.31185/wjps.245
Received 01September 2023; Accepted 22 October 2023; Available online 30 December 2023

ABSTRACT: The need to protect multimedia data security including audio, video, and text and the data it contains has persisted, whether in physical or digital form. This is due to the fact that the fabrication and fake of Multimedia data is widespread throughout the world, causing serious costs to people, societies, and the industrial sectors in addition to compromising national security. People are therefore concerned about safeguarding their employment and avoiding these illegal behaviors. To safeguard sensitive data, a variety of strategies including steganography, cryptography, and coding have been used. Steganography is a suitable technique that allows the user to hide a message inside of another message (cover media). The majority of steganography research makes use of cover material, like videos, images, and sounds. Notably, because to the challenges involved in locating embedded bits in an audio recording, audio steganography is typically not prioritized. By altering the least significant bits (LSBs) of audio samples, a technique known as audio steganography (LSB) can be used to conceal information in an audio stream. The least significant bits (LSBs) in a number's binary representation are the least weighted bits and are typically undetectable to the human ear. The audio signal can have a hidden message inserted in it without significantly affecting its perceptual quality by changing or manipulating the LSBs of the audio samples. To incorporate information into an audio, however, because to the slight audio difference, an assailant or other outsider might be able to hear this. To solve this problem, it is important to alter the audio in a way that it cannot be heard by the human ear but may still be understood by other means. This paper is a summary of the available research in the field. We start by outlining the fundamentals of audio steganography and how it works. Then, three categories of audio steganography statistical and random generation; and linguistics are described. Each class's tactics are examined, with a focus on how a special method is offered for concealing sensitive information. In addition, we survey the existing works in the advancement of strategies and algorithms relevant to audio steganography; our survey, which covers work published from 2016 to 2023, is not exhaustive. This study gathers the present approaches, difficulties, and future directions in this topic with the goal of assisting other researchers. In addition; we survey the existing works in the advancement of strategies and algorithms relevant to audio steganography.

Keywords: Steganography, Rijndael Algorithm, Audio Steganography, LSB Method, LSB technique in steganography, LSB (Least Significant Bit), LSB substitution.

1. INTRODUCTION

Cryptography is technique for ensuring communication confidentiality. To maintain the message's confidentiality, a variety of encoding and decoding techniques as well as methods for applying encryption, decryption, and hiding information have been used. The Advanced Encryption Standard (AES), which is a commonly used block encryption algorithm, is built on the Rijndael algorithm. Due to the fact that it uses symmetric keys, the same key is utilized for both encryption and decryption. Rijndael supports a variety of block sizes and key lengths and operates on fixed-size data

blocks. By altering the least significant bits of audio samples, the technique known as audio steganography (LSB, or Less Significant Bit), can be used to conceal information within audio recordings. [1][2], the sound is In Windows operating systems, digital audio data is frequently saved in WAVE format files. It was first used for photos and videos in 1991 as a component of the Resource Interchange File Format (RIFF). The descriptor chunk, the format chunk, and the data chunk are the three different sorts of chunks that make up the standard audio data format WAVE. The format chunk contains significant characteristics like sample rate, byte rate, and bits per sample, whereas the descriptor chunk is the WAVE header. The data chunk includes raw data and specifies the size of the sound data. It is generally advised to skip unfamiliar chunks because new kinds of chunks could be added in the future. [3][4]. Keeping the existence of the communication a secret might also be crucial. Steganography is a technique for hiding the existence of the message.[5],[6],[7] The words steganos (which means cover or protection) and graphy (which means to write) are combined to form the term steganography. Steganography is therefore defined as protected writing in its literal sense. It is a technique for concealing any kind of data or information (text, picture, audio, and video) in any kind of media or cover (image, audio, and video) in a way that only the sender and recipient are aware it is there.[8],[9][10] Steganography is the art and science of undetectable message transmission. Steganography is mostly used today on computers, with computers acting as the carriers of the information and systems as the quick delivery channels. Steganography and cryptography are commonly compared since both protect data from unauthorized third parties [11], [12],[13]. However, the two approaches operate very differently. The experiment's findings demonstrated that, in compares on to applying each technique separately, a combination of techniques maintains stego and expands the extent of secret data. The security and capacity issue might be resolved in part thanks to this study. [14], [15][16] ,[17], We've seen that error-correcting codes and steganographic methods have a close relationship. He introduced a new steganography that combines LSB and a new error-correcting code with Rijndael phonetic steganography. Different performance measures were used to evaluate the suggested technology, and the findings revealed that it offers greater embedding capacity and superior security to existing methods. It can be difficult to balance how much information can be concealed in an audio file with the need to remain unaware of the modification when utilizing LSB audio steganography. [18],[19],[20] Steganography's main objective is to securely transmit secret data in an entirely ambiguous manner while avoiding any possibility of introducing any doubt. While it's not to prevent them from learning the secret information, it is to prevent them from acknowledging that it even exists.[21],[22],[23][24], Only the sender and the recipient are aware of the presence of the message in steganography, but with cryptography, everyone is aware of the message's existence. In contrast to Steganography, which encrypts or modifies the message using a key so that only the recipient can decode it, Steganography allows the message to be protected to remain in its original form.[25][26],[27],[28], The research on Rijndael-based LSB Audio Steganography approaches that was published from 2016 to 2023 is surveyed in this study. The later portions also demonstrate the current research directions in the area. The following is a summary of this paper's contributions: gives a brief summary of the Rijndael-based LSB Audio Steganography approaches currently in use; reviews linguistics, LSB methodology, and audio steganography, while identifying their methodologies from 2016 to 2023; The rest of this essay is structured as follows: Section 2 Problem Statement. Section 3 Computational Complexity. Section 4 Computational Complexity Reducing., followed by the Procedure Steps for Audio Steganography based Rijndael Algorithm in Section 5. Then, Section 6 Literature Review, Section 7 Maximum Payload Capacity for Audio Steganography, and finally, Section 8 concludes this paper.

2. PROBLEM STATEMENT

The main problems could be summarized in the next few points:

- Attacks are likely against these methods. While LSB technique methods and Rijndael cipher are generally considered secure, there may be security holes in specific implementations or in the overall design of these technologies that attackers can exploit.
- There may be challenges in ensuring the robustness and reliability of Rijndael-based LSB Steganography technologies, particularly when dealing with different types of audio signals or when large amounts of data are involved.
- Is the potential for a conflict between security and usability? While Rijndael-based LSB Audio Steganography technologies may provide high levels of security, they can also be complex and difficult to use, especially for inexperienced users. This may lead to problems in adopting and implementing these technologies in real-world applications.

3. COMPUTATIONAL COMPLEXITY

Certainly! Computing complexity: This relates to how long embedding and extraction operations should take to process. This is especially true for restricted devices, which can perform exceptionally well in terms of embedding capacity and computing complexity. Due to the lost bandwidth storage and squandered computing complexity, this is not a satisfactory option. The computational complexity of this is very expensive. Accordingly, we concentrate primarily on boosting the security parameter. Combining a crypto system with data concealing can boost security, but it involves

complicated calculation. We create an LSB-based audio data hiding technique under this scenario, taking into account the payload, quality, secrecy, and computational complexity factors.. In the worst-case scenario, We utilize 10 audio *.wav files for the audio cover, each with its own duration and size, all sampled in 16 bit depth this strategy takes about 30.20 seconds to complete, whereas cryptographic schemes can waste a lot of computing complexity and storage [29][30]**.**

When used with Genetic algorithm –GA-, LSB may support a number of file types, including.aiff,.wav, and.Au. This technique extends message length up to 1000 characters. Although this method has a significant computational complexity. With a high channel bit rate, LSB has a low computational complexity, but it is less reliable when the data rate is low. There are a number LSB method variants available to address these issues.[31],[32]. Based on the quantity of fundamental operations needed to carry out the algorithm, a block cipher's computational complexity and energy consumption performance are assessed. A set of logical operations, including byte wise-AND, byte wise-OR, and shifts of bytes, can be used to represent all of the relevant algorithmic transformations. It is regarded as the sum of two bitwise-ANDs and one bitwise-OR for a straightforward bitwise-XOR. Similar to this, a byte wise-OR and 8 shifts are used to represent a circular shift (rotate) operation of an 8-bit word by n places. examines the Rijndael-AES computational load and energy consumption characteristics. For the various AES stages, straightforward computation complexity models are created in order to design and assess energy-efficient cryptographic techniques. The findings of energy consumption simulations support the relationship between computational models of encryption methods and several factors, including key size, block size, and number of rounds. The simulation findings quantify the AES-Rijndael's energy consumption and computational complexity overhead when different operating parameters are used. It is possible to reduce the number of computational clock cycles by using code optimization techniques for crucial encryption phases.[33] Rijndael-based audio LSB methods' computational complexity relies on a number of variables, notably the high sample capacity of audio.[34],[35] Using Rijndael-based LSB Steganography techniques, it is possible to encrypt and hide sensitive information in audio samples. This requires a number of intricate processes, including bitwise operations, byte substitution, permutation, and key expansion. These processes need a lot of computational resources, including memory and CPU cycles. [36] Furthermore, the amount of security and durability required raises the computational complexity of Rijndael-based LSB masking solutions. For instance, methods that embed private information into audio samples by means of key-dependent mapping functions or adaptive thresholds demand more processing power to develop the mapping functions or thresholds. substantial, and is dependent on a number of variables, including the duration of the audio samples, the size of the encryption block and key, and the needed level of security and robustness. [34] Consequently, it is essential to carefully assess these technologies' computing needs in real-world applications. [36] Cipher keys are used for encrypting small blocks, but their computational cost is crucial for one-way functions or hash functions. The key schedule execution is essential for each encryption, as consumes

$$\boldsymbol{nb(r+1)} \quad \ldots\ldots\ldots \quad (\mathbf{1})$$

For example, Rijndael requires 176 bytes of key storage for 128 bits and 480 bytes for 256 bits. Resource-limited platforms may have insufficient storage for expanded keys [37**].**

4. COMPUTATIONAL COMPLEXITY REDUCING

The computational complexity of Rijndael-based LSB audio steganography algorithms can be decreased in a number of ways. Here are a few potential strategies:

- Use lower block sizes: The Rijndael cipher algorithm's computational complexity depends on the block size chosen for encryption.
- Use smaller key sizes: The Rijndael cipher algorithm's computational complexity is also influenced by the size of the encryption key.
- Employ basic embedding methods: Some Rijndael-based LSB audio steganography methods make use of sophisticated modulation strategies, like adaptive thresholds or key-dependent mapping functions. By utilizing straightforward embedding methods
- Use parallel processing: To simplify calculation, the Rijndael encryption technique can be parallelized.
- Use compression: Prior to embedding the secret data in the audio samples, the secret data can be compressed to further minimize the computational complexity.

[38], [39], [40].

It is important to keep in mind that lowering the computational complexity of Rijndael-based LSB audio steganography methods might result in decreased security, resilience, or capacity. Therefore, when developing and putting these strategies into practice, it is crucial to properly balance these aspects. [40]

.

5. PROCEDURE STEPS for AUDIO STEGANOGRAPHY based RIJNDEL ALGORITHM

The new approach uses a modified LSB method with random distribution to exchange bits around a key point, which is subsequently concealed inside a cover sound file.

Algorithm (1):- The proposed algorithm steps for audio steganography using Rijndael algorithm

Process: Begin

Step 1: Read sound file as the cover media to hide the secret message.

Step 2: Convert the secret message into binary data.

Step 3: Generate a random key of required length (128-bit, 192-bit or 256-bit) encryption key.

Step 4: Use the Rijndael algorithm (AES) to encrypt.

Step 5: Select the LSB (Least Significant Bit) of the cover audio file.

Step 6: Substitute the LSB of the audio samples with the bits of the encrypted message.

Step 7: To extract the message, the receiver needs the audio file .

Step 8: Perform checks to ensure proper message hiding and extraction.

Step 9: Return (S). End. [41],[42],[43]

6. LITERATURE REVIEW

In 2016, Chaos-based Audio Steganography and Cryptography have been introduced by Huwaida S.M.H. and et al [44]. This method was based on LSB Method and One-Time Pad. It was applied For the purpose of secure audio communications, two chaos maps—the Piecewise Linear Chaotic Map (PWLCM) and the cryptographic and steganographic logistic map, respectively—are combined into one audio file..

In 2018, Cryptography and Audio Video Steganography have been introduced by Yadav M. and et al [45]. This method was based on Improved Security of data. In order to secure the secret data, we employed LSB (Least Significant Bit) replacement technology to hide an encrypted secret image behind the audio signals of the audio and video file and the encryption key behind the video frame.

In 2020, Steganography have been introduced by Bansal K. and et. ‹al [46]. This method was based on Least Significant bit (LSB) Embedding Approach. It was employed by LSB to provide a method of verifying data from an unreliable client and to improve communication using cutting-edge audio in order to increase the security of our data.

In 2022, Audio steganography have been introduced by Abdulkadhim H.A. and et al [47]. This method was based on least significant bits algorithm with 4D grid multi-wing hyper-chaotic system, For a higher level of security and power, a video file was encrypted using the Least Significant Bits (LSB) algorithm method and a four-dimensional highly chaotic multi-wing (GMWH) system.

In 2022, Audio steganography have been introduced by Abood E. W. and et al [41]. This method was based on bit cycling and an enhanced LSB method. For the purpose of securing data, steganography and encryption were combined to create a potent hybrid security system into an audio file in the wav format.

In 2022, Hiding secret data have been introduced by Kumar M. and et al [48]. This approach was derived from the LSB algorithm. It was used to the LSB algorithm, which replaces the least significant part of each pixel or sample in digital media with a bit of confidential data, thereby embedding confidential data within the media for the purpose of a high level of concealment ability and robustness while maintaining a low probability of detection.

In 2023, A Modified Enhanced Method of Audio – Video Steganography have been introduced by PL N. and et. ‹al [49]. This approach was based on the LSB algorithm's modified pixel value differencing. For the purpose of secure data transmission, it was used to incorporate encoded audio data into a video file.

.

7. MAXIMUM PAYLOAD CAPACITY for AUDIO STEGANOGRAPHY

The following variables affect the maximum payload capacity for audio steganography using the Rijndel algorithm:

- The longer the cover voice coil, the more payload it can support.
- Audio sampling frequency: When the sampling frequency is higher, there are more samples available for processing, which results in a higher overhead.
- LSB usage: Increasing the LSB count.
- Compression algorithm: Formats with less compression, like WAV, offer greater redundancy and a larger payload capacity than formats with high compression, like MP3.
- Tolerance for errors: More LSBs can be updated, increasing capacity, if minor faults in the extracted message are tolerated.

It is only possible to estimate an audio file's true capacity empirically by attempting to hide messages that grow progressively larger and assessing the level of tolerable distortion. The degree of message concealment while keeping acceptable sound quality determines the capacity. Sound caliber. [50]

Where M takes the highest value of the x samples while MSE represents the mean square error between x,y and it is computed by:

$$\mathrm{MSE} = \frac{\sum_{i=1}^{m} \|x(i) - y(j)\|^2}{M} \quad \ldots\ldots\ldots\ldots \quad (2)$$

Where x is the original wav file before hiding while y is after hiding

Peak signal to noise ratio (PSNR) metric calculates the ratio of the noise between the same signal before and after making changes on it to expose any distortion after change. It is computed with the formula: A higher PSNR suggests greater sound quality and less distortion, whereas a lower PSNR indicates worse quality and more distortion. Conventional:

$$\mathrm{PSNR}(x, y)\ 10\log 10\left(\frac{M^2}{\mathrm{MSE}}\right) \quad \ldots\ldots\ldots\ldots (3)$$

- More than 30 dB = High Quality
- 20 to 30 dB equals Fair Quality

Less than 20 dB indicates low quality.

So, using the estimated PSNR value, you may assess the sound quality after masking your message. [41]

8. CONCLUSION

In order to examine performance and security concerns, this study introduces the art of steganography in LSB technologies' schemes. Numerous researchers have made contributions to this topic, and some of them are present here to illustrate Rijndael's algorithm. Although these technologies have been researched in a variety of modern application situations, the Steganography community is still searching for design schemes that are more reliable and secure. You'll probably emphasize how crucial it is to use these technologies properly and cautiously in order to provide safe and reliable data anonymization in audio signals. LSB Audio Steganography systems based on Rijndael, in summary, offer a high level of security for concealing hidden messages within an audio file. Nevertheless, each type of algorithm has its own advantages and disadvantages, therefore selecting the best algorithm depend on the requirements of the application.

CONFLICTS OF INTEREST

The author declares no conflict of interest.

REFERENCES

[1] Stallings.W. , "Cryptography and Network Security" Principles and Practice (7th ed.). Pearson Education. 2017

[2] Abdul-Jabbar S.S., Abed A.E., Mohammed S.G., Mohammed F.G.," Fast 128-bit Multi-Pass Stream Ciphering Method," Iraqi Journal of Science, 64 (5) , pp. 2589-2600.2023.

[3] Ali N.H.M., Rahma A.M.S ,"An Improved AES Encryption of Audio Wave Files", THESIS P.H.D, University of Technology, Department of Computer Science, 2015,https://www.researchgate.net/publication/312277403,

[4] Mohammed F.G., Athab S.D., Mohammed S.G.," Disc damage likelihood scale recognition for Glaucoma detection," Journal of Physics: Conference Series, 2114 (1) , art. no. 012005.2021

[5] Khodher M.A.A., AlabaichiA., AltameemiA.A. ," Steganography Encryption Secret Message in Video Raster Using DNA and Chaotic Map ," Iraqi Journal of Science, 2022, Vol. 63, No. 12, pp: 5534-5548,2022 DOI: 10.24996/ijs.2022.63.12.38

[6] Mohammed S.G., Abdul-Jabbar S.S., Mohammed F.G.," Art Image Compression Based on Lossless LZW Hashing Ciphering Algorithm," Journal of Physics: Conference Series, 2114 (1) , art. no. 012080.2021

[7] Harba I.S.E. , "Advanced Password Authentication Protection by Hybrid Cryptography & Audio Steganography," Iraqi Journal of Science, vol. 59, no. 1C, pp. 600-606, 2018.

[8] M. M. Hoobi, S. S. Sulaiman, I. A. AbdulMunem, "Enhanced Multistage RSA Encryption Model," 2nd International Scientific Conference of Al-Ayen University (ISCAU), IOP Conf. Series: Materials Science and Engineering, p. 455, 2020.

[9] Simanjuntak H.L., Pramudyo A.S.,Fahrizal R.,"Similarity Analysis of Audio Steganography Combined With Rijndael Cryptography Algorithm", The 4th ICIBA 2015, International Conference on Information Technology and Engineering Application Palembang-Indonesia, 20-21, 2015, DOI:10.13140/RG.2.1.3867.7600.

[10] Maarez HG, Jaber HS, Shareef MA. Utilization of Geographic Information System for hydrological analyses: A case study of Karbala province, Iraq. Iraqi Journal of Science. 4118-30.2022

[11] A. H. M., Mohammed G. S., "Efficient Plain Password Cryptanalysis Techniques," Iraqi Journal of Science, vol. 58, no. A4, pp. 1946-1954, 2021

[12] Faisel G. Mohammed , Hind M. Al-Dabbas, "Application of WDR Technique with different Wavelet Codecs for Image Compression", Journal Iraqi journal of science,2128-2134,2018

[13] N. Gupta and N. Sharma, "Dwt and Lsb based Audio Steganography," 2014 International Conference on Reliability Optimization and Information Technology (ICROIT), Faridabad, India, 2014, pp. 428-431, doi: 10.1109/ICROIT.2014.6798368.

[14] Nur A, Yuana H, Febrinita F. Aplikasi Kompresi Citra dengan Menggunakan Algoritma Lempel Ziv Welch (LZW). JATI (Jurnal Mahasiswa Teknik Informatika). 6(2):684-95.2022

[15] Hussein A. M. , Al-Momen S. " Linear Feedback Shift Registers-Based Randomization for Image Steganography", Iraqi Journal of Science, Vol. 64, No. 8, pp: 5031-5046,2023 DOI: 10.24996/ijs.2023.64.8.34

[16] Hussein NH, Ali MA. Medical Image Compression and Encryption Using Adaptive Arithmetic Coding, Quantization Technique and RSA in DWT Domain. Iraqi Journal of Science.2279-96.2022

[17] Awadh W.A. ,Alasady A.S. , Hamoud A.K.., "Hybrid information security system via combination of compression, cryptography, and image steganography". International Journal of Electrical and Computer Engineering (IJECE) ,Vol. 12, No. 6, pp. 6574~6584,2022ISSN: 2088-8708, DOI: 10.11591/ijece.v12i6.pp6574-6584

[18] Makhdoom I, Abolhasan M, Lipman J. A comprehensive survey of covert communication techniques, limitations and future challenges. Computers & Security.120:102784.,2022

[19] Thamir, N.N. And Mohammed, F.G., "Early Esophageal Cancer detection using Deep learning Techniques. (Review Article)", Journal of Physics: Conference Series, 1963(1), 012066,2021

[20] George LE, Hassan EK, Mohammed SG and Mohammed FG, " Selective image encryption based on DCT, hybrid shift coding and randomly generated secret key". Iraqi J Sci 61(4):920–935.2020

[21] Hasan A. Kazum , Faisel G. Mohammed, "White blood cell recognition via geometric features and naïve bays classifier", International Journal of Engineering & Technology, 7 (4) (2018) 3642-3646

[22] Munuera C. ,"Steganography and error-correcting codes", (Signal Processing 87 (2007) 1528–1533 ,2007, doi:10.1016/j.sigpro.2006.12.008

[23] Ali, A.H., George, L.E., Zaidan, A.A. and Mokhtar, M.R., 2018. High capacity, transparent and secure audio steganography model based on fractal coding and chaotic map in temporal domain. *Multimedia Tools and Applications*, *77*, pp.31487-31516.

[24] Makhdoom I, Abolhasan M, Lipman J. A comprehensive survey of covert communication techniques, limitations and future challenges. Computers & Security. 2022 Sep 1;120:102784.

[25] A. Kanhe, G. Aghila, C. Y. S. Kiran, C. H. Ramesh, G. Jadav and M. G. Raj, "Robust Audio steganography based on Advanced Encryption standards in temporal domain," 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Kochi, India, 2015, pp. 1449-1453, doi: 10.1109/ICACCI.2015.7275816.

[26] Ogundokun RO, Awotunde JB, Adeniyi EA, Ayo FE. Crypto-Stegno based model for securing medical information on IOMT platform. Multimedia tools and applications.80:31705-27,2021

[27] Dutta H, Das RK, Nandi S, Prasanna SM. An overview of digital audio steganography. IETE Technical Review. 37(6):632-50.,2020

[28] Joshi, Amit M., et al. "Combined DWT–DCT-based video watermarking algorithm using Arnold transform technique." Proceedings of the International Conference on Data Engineering and Communication Technology: ICDECT 2016, Volume 1. Springer Singapore, 2017.

[29] Al-Hooti M.H. , Ahmad T. , Djanali S. , "Developing audio data hiding scheme using random sample bits with logical operators", Indonesian Journal of Electrical Engineering and Computer Science Vol. 13, No. 1, pp. 147~154 ISSN: 2502-4752,2019, DOI: 10.11591/ijeecs.v13.i1.pp147-154

[30] Mahmoud MM, Elshoush HT. Enhancing LSB using binary message size encoding for high capacity, transparent and secure audio steganography–An innovative approach. IEEE Access.,10:29954-71.,2022

[31] Bah J. , Ramakishore R. ,"LSB Technique And Its Variations Used In Audio Steganography: A Survey", International Journal of Engineering Research & Technology (IJERT),Vol. 2 Issue 4, April – 2013, ISSN: 2278-0181

[32] Manjunath K, Ramaiah GK, GiriPrasad MN. Backward movement oriented shark smell optimization-based audio steganography using encryption and compression strategies. Digital Signal Processing. ,122:103335.,2022

[33] M. Razvi Doomun, K. M. Sunjiv Soyjaudah and D. Bundhoo, "Energy consumption and computational analysis of rijndael-AES," 2007 3rd IEEE/IFIP International Conference in Central Asia on Internet, Tashkent, Uzbekistan, 2007, pp. 1-6, doi: 10.1109/CANET.2007.4401683.

[34] Alwahbani S.M.H. , Elshoush H.T.I.,"Hybrid Audio Steganography and Cryptography Method Based on High Least Significant Bit (LSB) Layers and One-Time Pad—A Novel Approach ", Springer International Publishing AG 2018 Y. Bi et al. (eds.), Intelligent Systems and Applications, Studies in Computational Intelligence 751,2018, https://doi.org/10.1007/978-3-319-69266-1_21

[35] Abdulkadhim HA, Shehab JN. Audio steganography based on least significant bits algorithm with 4D grid multi-wing hyper-chaotic system. International Journal of Electrical and Computer Engineering. ,12(1):320-30.2022

[36] F. Granelli, G. Boato, "A novel methodology for analysis of the computational complexity of block ciphers: Rijndael, Camellia and Shacal-2 compared", In Third Conference on Security and Network Architectures (SAR'04), June 2004.

[37] Daemen, J.; Rijmen, V.. In The Design of Rijndael: The Advanced Encryption Standard (AES);, Eds.; Information Security and Cryptography; Springer: Berlin/Heidelberg, Germany, 2001;. ISBN 978-3-662-60769-5.

[38] Biham, Eli, and Nathan Keller. "Cryptanalysis of reduced variants of Rijndael." 3rd AES Conference. Vol. 230. 2000.

[39] Granelli F. Boato G., "A novel methodology for analysis of the computational complexity of block ciphers: Rijndael,Camellia and Shacal-2 compared," in Proceedings of 3rd Conference one Security and Network Architectures (SAR '04), LaLonde, France, June 2004.

[40] Rudra, A., Dubey, P.K., Jutla, C.S., Kumar, V., Rao, J.R., Rohatgi, P. (2001). Efficient Rijndael Encryption Implementation with Composite Field Arithmetic. In: Koç, Ç.K., Naccache, D., Paar, C. (eds) Cryptographic Hardware and Embedded Systems — CHES 2001. CHES 2001. Lecture Notes in Computer Science, vol 2162. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-44709-1_16

[41] Abood E. W. , Abdullah A. M. ," Audio steganography with enhanced LSB method for securing encrypted text with bit cycling ", Bulletin of Electrical Engineering and Informatics Vol. 11, No. 1, February 2022, pp. 185~194 , DOI: 10.11591/eei.v11i1.3279.

[42] Kadhem M.S.,"Text Steganography Method Based On Modified Run Length Encoding", Iraqi Journal of Science, Vol. 57, No.3C, pp:2338-2347,2016

[43] Abdulrazzaq S. T. , Siddeq M.M. , Rodrigues M.A. ,"A Novel Steganography Approach for Audio Files", SN Computer Science (2020) 1:97 https://doi.org/10.1007/s42979-020-0080-2

[44] Huwaida S.M.H. , Elshoush T.I. "Chaos-based Audio Steganography and Cryptography Using LSB Method and One-Time Pad', SAI Intelligent Systems Conference 2016 September 21-22, London, UK,2016.

[45] Yadav M., Yadav S. ," Improved Security of data using Cryptography and Audio-Video Steganography ", IJRECE VOL. 6 ISS. 2 APR.-JUNE 2018 .

[46] Bansal K., Agrawal, A., Bansal, N." A Survey on Steganography using Least Significant bit (LSB) Embedding Approach", IEEE, 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184), pp. 64-69. 2020, doi:10.1109/ICOEI48184.2020.9142896

[47] Abdulkadhim H.A., Shehab J.N.," Audio steganography based on least significant bits algorithm with 4D grid multi-wing hyper-chaotic system ", International Journal of Electrical and Computer Engineering (IJECE) Vol. 12, No. 1, pp. 320~330 , 2022, DOI: 10.11591/ijece.v12i1.

[48] kumar M., patil T., Kumari M., Raj A., Pradhan R., Giri M.,"Hiding secret data in a au dio,video,image,text steganography using least significant bit algorithm', GIS SCIENCE JOUR, VOL 9, ISS 12, 2022.

[49] PL N., V R. , A I., K S. ,"A Modified Enhanced Method of Audio – Video Steganography for High Security Data Transmission". E3S Web of Conferences 399, 01003 (2023) , ICONNECT-2023, https://doi.org/10.1051/e3sconf/202339901003

[50] Hameed A.S.,"High Capacity Audio Steganography Based on Contourlet Transform", Tikrit Journal of Engineering Sciences 25 (1) 2018 (1-7), : http://dx.doi.org/10.25130/tjes.25.1.01