ISSN: 0067-2904

An Efficient Methodology for Encrypting Audio Data by Combining Rijndael and Steganography Algorithms

Sajaa G. Mohammed, Nuhad Salim Al-Mothafar*
Department of Mathematics, College of Science, University of Baghdad, Baghdad, Iraq

Received: 31/12/2023 Accepted: 6/3/2024 Published: 30/3/2025

Abstract

Data security and its characteristics are considered one of the most important requirements of the modern era, as this generation is in rapid digital development. Therefore, it needs an effective methodology for a strong and effective encryption algorithm, by incorporating the standard encryption algorithm known as Rijndael. And steganography. The goal of this study is to transfer and store audio data with complete confidentiality and security. This study converts audio data into a 256 bit audio sample that we use for the purpose of encryption using the Rijndael algorithm, as this algorithm is known for its strength and for winning many awards. The principle of this algorithm's work is to create multiple blocks of different block sizes and keys. We create keys for the purpose of encryption, and they are integrated into audio files using the developed data steganography technique. Saving the data is done using an image with the bmp extension. After that, we expose these images to compression to know and evaluate whether the steganography is successful. After that, we return it, remove the compression, and decrypt it. We note the return of the original text. The goal of this proposed methodology is to protect audio data from attacking persons and reduce the chances of revealing this data. This methodology is used for the purpose of transferring, storing, and safely preserving secret audio files with a security aspect. This research has one of its most important features in that it combines the strength of encryption, which is represented by the Rigndael algorithm, and the strength of data hiding technology, which resulted in the time of breaking the code and returning it in a record time of up to 99.9%. It also gives a developed and innovative methodology, for securing, transferring, storing and protecting audio data in all modern digital fields.

Keyword: algorithm Rijndael. Steganography, data audio, Lsb, cover ,stego, image.

منهجية فعالة لتشفير البيانات الصوتية من خلال الجمع بين ريجنديل وخوارزميات إخفاء المعلومات

سجا غازي محمد , نهاد سالم المظفر

الرياضيات , كلية العلوم , جامعة بغداد, بغداد, العراق

الخلاصه

يعتبر أمن البيانات وخصائصها من أهم متطلبات العصر الحديث، حيث أن هذا الجيل في تطور رقمي سريع وبالتالي يحتاج إلى منهجيه فعاله لخوارزمية تشفير قوية وفعالة، عن طريق دمج وهي خوارزمية التشفير القياسية المعروفة باسم Rijndeal. واخفاء البيانات الهدف من هذه الدراسة هو نقل وتخزين البيانات الصوتيه بكل سرية وامان , تقوم هذه الدراسه بتحويل البيانات الصوتيه الى عينه صوتيه 256 ساميل نستخدمها لغرض

*Email: sajaa.mohammed@sc.uobaghdad.edu.iq

التشفير بواسطه خوارزميه ريجندل حيث عرفت هذه الخوارزميه بقوتها وفوزها بجوائز عديدة, مبدء عمل هذه الخوارزميه هي تكوين كتل متعددة من احجام ومفاتيح مختلفة تقوم بتكوين مقاتيح لغرض التشفير ويتم دمجها في الملفات الصوتية بااستخدام تقنيه اخفاء البيانات المطورة حفظ البانات يكون بواسطة صورة ذات امتداد bmp وبعد ذلك نقوم بتعريض هذه الصور لضغط لغرض معرفة وتقييم الاخفاء هل و ناجح ام لاء وبعد ذلك نقوم باارجعها وازالة الضغط وفك اتشفير نلاحظ عودة النص الاصلي , الهدف من هذه المنهجيه المقترحه هي حماية البيانات الصوتيه من الاشخاص المهاجمين وتقليل فرص الكشف عن هذه البيانات، تسخدم هذه المنهجيه لغرض النقل والتخزين والحفظ الامان للملفات الصوتيه السريه ذات الجانب الامني هذا البحث من اهم مميزاته انه يجمع بين قوة التشفير والتي تتمثل بخوارزمية الريجندل وقوة تقنيه اخفاء البيانات التي انتجت وقت كسر للشفرة واعادتها بوقت قياسي يصل الى 99.9 % ويعطي كذلك منهجيه مطورة ومبتكرة لغرض تامين ونقل وتخزين وحماية البيانات الصوتية في كافه المجالات الرقميه المتعددة الحديثه

1. Introduction

These days, audio data security plays a major role in the IT business and expands quickly.[1],[2],[3] Encrypting audio data prevents illegal access and manipulation while guaranteeing its integrity and confidentiality.[4],[5] Technology preservation of audio files from hackers and eavesdroppers became crucial for the Technology professional. Thus, the necessity for swifter and more secure audio file encryption algorithms remains continual. Encrypting audio using cryptography involves simultaneously adding noise, or the key, to a plain text file. Decryption is using the same key to reveal the original plain text. Speech is an attractive hands-free human-computer interface broker that only requires basic hardware to purchase high-quality microphones and comes at a very low bit rate. Human speech is essentially recognized as continuous, connected speech without tedious practice (free speaker) since a vocabulary with the appropriate complexity (100,000 words) is incredibly difficult [6], [7],[8]. Nonetheless, algorithms, procedures, and techniques make it simple to process voice signals and recognize text spoken by a speaker. This study proposes a new algorithm that uses Rijndael algorithm keys generated from speech audio files (WAV) to conduct encryption on audio files. The suggested algorithm was put to the test and used. [9],[10],[11], The Rijndael method serves as the foundation for the Advanced Encryption Standard (AES), and a popular block encryption algorithm. The same key is used for both encryption and decryption since it employs symmetric keys. Rijndael runs on fixed-size data blocks and supports a range of block sizes and key lengths. The Rijndael algorithm is a symmetric block cypher with lengths of 128, 192, and 256 bits that can handle data blocks of 128 bits. Under the restrictions that the input and output sequences have the same length, the Rijndael encryption key, the input, and the output are all bit sequences of 128, 192, or 256 bits apiece. [12],[13],[14]. Advanced encryption standard-based stenographic algorithm (AES). AES is used to encrypt the sound after it has first been transformed into a picture. Security assessments and simulations show how well the suggested algorithm performs. [15],[16], The sound is Digital audio data is often preserved in WAVE format files on Windows operating systems. In 1991, it made its debut as a part of the resource interchange file format (RIFF) for images and movies. The three distinct types of chunks that comprise the standard audio data format are the descriptor chunk, the format chunk, and the data portion Wave. While the WAVE header is the descriptor portion, the format chunk provides important attributes like sample rate, byte rate, and bits per sample. The data chunk indicates the size of the sound data and contains raw data. Generally speaking, it is the best to avoid unfamiliar pieces as new ones that might be added in the future.[6], [17],[18] Steganography is a method of concealing the existence of a message, combining the terms steganos (cover) and graphy (writing). It involves hiding information under various covers, allowing only the sender and recipient to know. Currently, most steganography applications are computer-based. Although often compared, a combination of steganography and cryptography can preserve stego and increase hidden data,

potentially addressing capacity and security concerns. [19],[20], The present research proposes an efficient methodology for encrypting audio data by combining Rijndael and steganography algorithms approaches that were published from 2016 to 2023 that are 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 summary of the Investigating Rijndael-Based Algorithms for Audio Ciphering. The rest of this essay is structured as follows: Section 2 presents the Problem Statement. Section 3 shows some related Work. Section 4. is devoted to Encryption Methodology, followed by the Procedure Steps for Audio Ciphering based Rijndael Algorithm and steganography in section 5. Then, in section 6,7, we present the obtained results and discussion, and finally, in section 8, we give the conclusion and future work of this paper.

2. PROBLEM STATEMENT

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

- Attacks on voice data and privacy can occur in today's digital age. There is an Increased need to exchange voice data over the network, although Rijndael voice encryption is generally considered safe, because this algorithm is considered one of the advanced algorithms in data encryption, and hidden encryption leads to its concealment. Data in digital media increases security in communications and complicates detection.
- There may be challenges in ensuring the robustness, reliability and analysis of Rijndael-based voice coding technology, especially when dealing with different types of audio signals or when large amounts of data are involved.
- Is there a potential conflict between security and ease of use? Developing an Efficient Rijndael-Based Voice Encryption System and increasing its Robustness Using Backdoor Cryptography While Rijndael-based voice encryption technology may provide high levels of security, it 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. RELATED WORK

In 2016, Chaos-based Audio Steganography and Cryptography were introduced by Huwaida S.M.H.. and et al [21]. This approach was derived from the One-Time Pad and LSB Method. It was accustomed to being used. For the purpose of secure audio communications, two chaos maps are combined into an audio file: the Piecewise Linear Chaotic Map (PWLCM) and the Cryptographic and Steganography Logistic Map, respectively.

In 2018, Cryptography and Audio Video Steganography were introduced by Yadav M. and et al [22]. This approach was predicated on enhanced data security. Using LSB (Least Significant Bit) replacement technique, we were able to secure the secret data by concealing an encrypted secret image behind the audio signals of the audio and video file and the encryption key behind the video frame.

In 2021, Information Hiding in Audio Steganography was introduced by Shanthakumari R. and et al [23]. The foundation of this approach was LSB Matching Revisited. Secure communication and data security are crucial, so it was utilized to the idea of a -LSB Matching Revisited -LSBMR algorithm to create chosen samples as an input unit to conceal ambiguous signals into audio samples.

In 2021, Audio Steganography Schemes were introduced by Hemeida F. and et al [24]. This approach was derived via a comparative analysis. It was utilized to as audio sample for

the purpose of Schemes indicating greater performance utilizing AES-256 when compared with its equivalents. The dual-layer message security system comprises encryption as the first layer and anonymity as the second.

In 2022, Hiding secret data was introduced by Kumar M. and et al [25]. This method was based on the LSB algorithm, which works by replacing the least significant part of each pixel or sample in digital media with a bit of confidential data, thus embedding confidential data within the media to achieve a high level of concealment and robustness while maintaining a low probability of detection.

In 2022, Audio steganography was introduced by Wahhab. A.E.L. and et al [26]. This technique was built upon bit cycling and the improved LSB approach. In order to create a strong hybrid security system into a video file in the wav format for secure data, steganography and encryption were combined.

In 2022, Audio steganography was introduced by Abdulkadhim H.A. and et al [27]. In order to increase security and strength, this method combined the Least Significant Bits (LSB) algorithm method with a four-dimensional highly chaotic multi-wing (GMWH) system into a video file. It was based on the Least Significant Bits algorithm with 4D grid multi-wing hyper-chaotic system.

In 2023, A Modified Enhanced Method of Audio – Video Steganography was introduced by PL N. and et. ‹al[28]. This technique was built around the LSB algorithm's modified pixel value differencing. For the aim of safe data transfer, encoded audio data was embedded into a video file.

In 2023, Audio Steganography was introduced by Nisha O.T. and et al [29]. Genetic algorithms formed the basis of this technique. In order to provide reliable and confidential communication that is secure, high-capacity data Stegano technology was included in audio signals.

4. METHODOLOGY

Three areas of work focus are identified in this system design: the encryption and decryption process, Steganography, the key generation method and block size. [30] An information cypher conceals information by employing redundant cover data, including documents, audio files, movies, and photos. Recently, this method has grown in significance in many application fields. For instance, digital video, audio, and audio steganography involve using the human hearing system's limited capacity to conceal information in the audio data's least significant bit (LSB).[31]

The algorithm was designed to disguise all data entered within audio to protect data privacy. As a result, the system was created using a brand-new Rijndael algorithm. This suggested system gives the
user two options for encrypting and decrypting data. Encryption involves hiding secret information with an audio file, while decoding involves retrieving the hidden information.

1. Present a method for using encryption

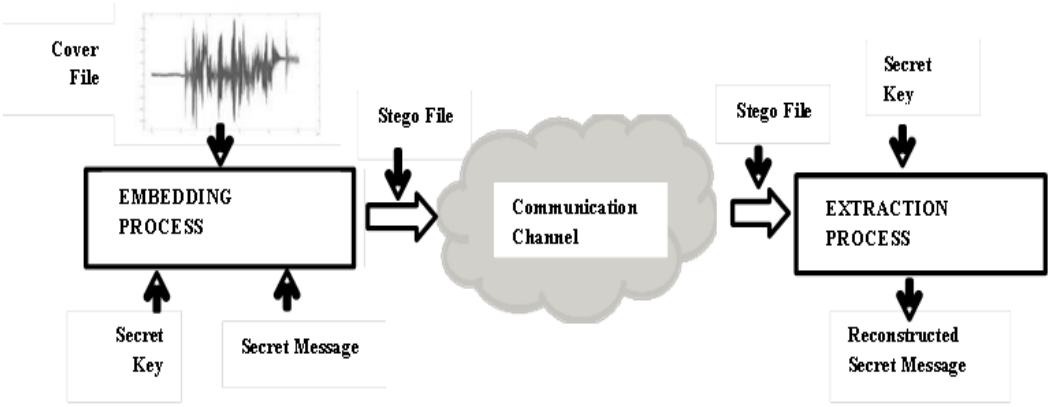

Figure 1: Terminology in general steganography [32]

2. The algorithm that provides better accuracy and quality of encryption V.B.studio is used in information concealment, the Rijandnel algorithm is used. and use Steganography They are encoded and put into an audio file, which is transferred along with text and other file formats to the destination, as one can see in the Figure 1.

4.1 Audio Ciphering

One technique to protect data in a sound file against invasive attacks is using audio encryption. We utilize the precise algorithm and the (noise) key on the source text. Our primary focus is on encryption Techniques for handling audio data. Analysing and comparing fundamental encryption standards has shown that ways of encryption can be used to encode audio. Like AES, DES and Triple DES (3-Data Encryption Standard). [33],[34],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 Resource Interchange File Format (RIFF) component. The three distinct types of chunks that comprise the standard audio data format WAVE are the descriptor chunk, the format chunk, and the da ta chunk. 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 chunks could be added in the future. [6],[17] ,This reach focuses on the aspects Previous chaotic audio algorithms did not consider its advantages and disadvantages. Analog and digital signal processing are important foundations for encryption. The requirements for these algorithms as well as the security and statistical tests for evaluating such algorithms have been shown.[35]

4.2 Rijndael Algorithm

NIST published an excellent 116-page report summarizing all contributions and justifying the decision on October 2, 2000, when it officially announced that unaltered Rijndael would become the AES. NIST uses the following lines in at the conclusion of this report, a decision has been made regarding the Rijndael. It appears that the Rijndael has always performed very well in both hardware and software across a wide range of computing data, regardless of its use in comments or not giving feedback. The key setting time ways are very excellent and the key agility is good.[36] Daemen and V. created the Rijndael algorithm, and renamed the AES. The steps involved in AES Encoding and decoding are depicted in Fig. 2. These actions, which include Sub Bytes, Shift Rows, Mix Columns, Add Round Key, Inv Shift Rows, Inv Sub Bytes, and Inv Mix Columns, are described in the Federal Information Processing Standard, or FIPS, 197. The final round differs slightly and does not include the Mix Columns action during encoding. The AES algorithm implements key extending routine to create a key

schedule. Given an employee provides the key of 16, 24, or 32 bytes, it returns what is known as an Expanded Key of 16 × 11, 16 × 13, and 16 × 15 bytes, respectively [37], [38].

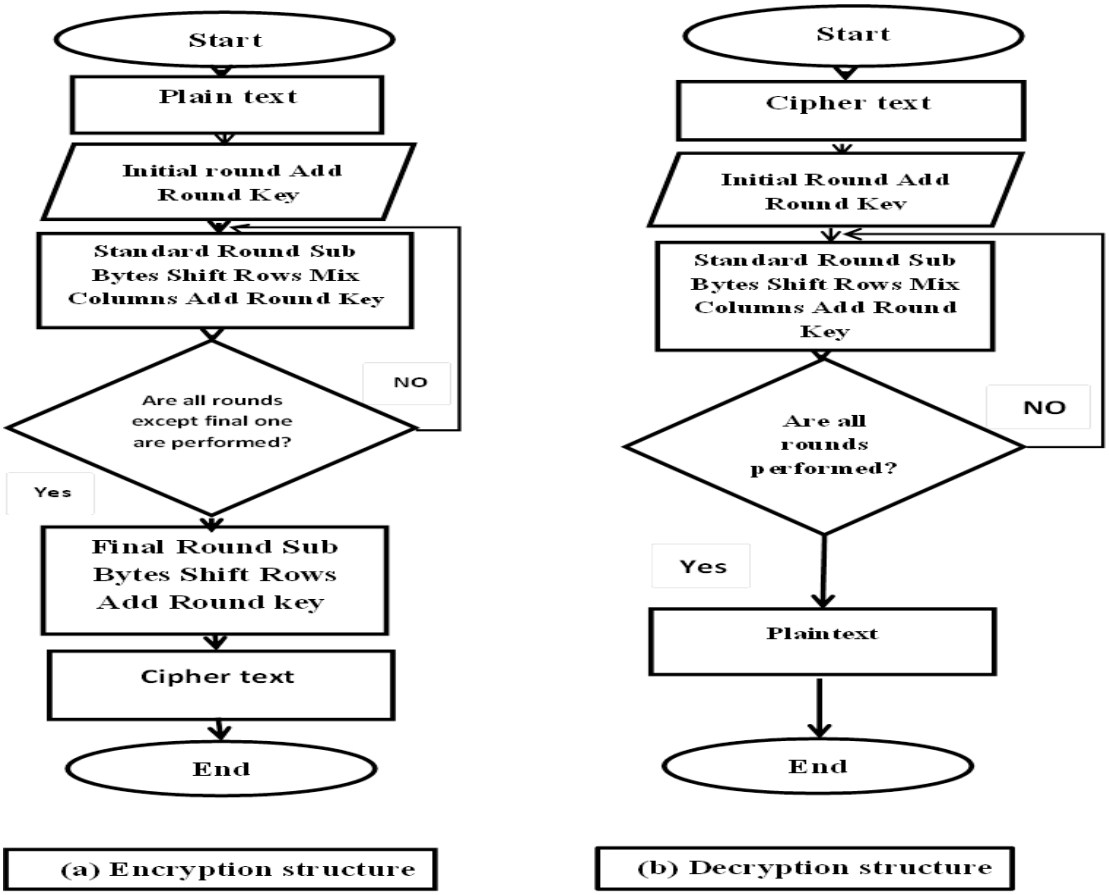

Figure 2: Rijndael algorithm (a) Encryption structure; (b) Decryption structure [37]

Lastly, Rijndael's internal round structure appears to have good potential to benefit from instruction-level parallelism. Security was the most important category, here now the most complex evaluation can show only a small number of some explanatory laws, The majority of them fall into the category that does not show any weakness, Rijndael operations are among the easiest operations to defend against hackers and timing attacks. In addition to this, it provides some definitions against such attacks without affecting performance in a very significant way. [39]

4.3 Block Cipher Rijndael Algorithm

AES has three possible key standards: 128 bits, 192 bits, or 256 bits. The terms AES 128, AES 192, and AES 256 refer to the three distinct AES implementations. However, 128 bits is always the block size. The original Rijndael cipher supported block and key sizes that could be changed in increments of 32 bits (Daemen and Rijmen 1998). The Rijndael algorithm, it should be emphasized, enables different key and block sizes. Block and key sizes of 128, 160, 192, 224, and 256 bits are supported by Rijndael. Nevertheless, the AES standard states the block standard of 128 bits and the key standard of 128, 192, and 256 bits. Two cryptographers from Belgium named Daemen and Rijmen created this algorithm. Belgian cryptographer Daeman has devoted much of his career to the cryptanalysis of hash functions, stream ciphers, and block ciphers. Rijmen is another Belgian cryptographer who worked on ciphers like KHAZAD, Square, and SHARK and contributed to creating the WHIRLPOOL cryptographic hash. Rijndael uses a replacement permutation matrix rather than a Feistel network. The 128-

bit plain text block needs to be first arranged into a 4-byte by 4-byte matrix in order for the Rijndael cipher to work (Daemen and Rijmen 1998). The state of this matrix will change as the algorithm goes through its series of stages. As a result, the plain text block must first be converted to binary before being placed into a matrix, as illustrated in Fig. 3 [40].

11011001	01110010	10110000	11101010
01011111	00011001	11011001	10011001
10011001	11011101	00011001	11111101
11011001	10001001	11011001	10001001

Figure 3: convert the plain text block into binary

Rijndael is an iterated block cypher with a variable block length and variable key length. It is possible to independently set the block and key lengths to 128, 192, or 256 bits. Similar to Square and BKSQ, the wide trail technique was used in the design of Rijndael. This design technique offers protection from both differential and linear cryptanalysis. The round transformation is broken down into various components in the approach, each with a distinct function. [40],[41].

4.4 METHOD : COMBINING RIJNDAEL CRYPTOGRAPHIC STEGANOGRAPHY ALGORITHMS

The Advanced Encryption Standard (AES), also known as Rijndael, is the encryption specification used for electronic data developed by the National Institute of Standards and Technology (NIST) in the United States. Its foundation is the substitution arrangement network plan principle. Its key standard can be 128, 192, or 256 bits, while its block size is set at 128 bits. Each phase of a round in the decryption algorithm is the inverse of its corresponding stage in the encryption algorithm. These four basic processes apply to both encryption and decryption. The following are the four phases:

- Sub Bytes Transformation: Each byte is substituted with a different one in this non-linear substitution step based on the entries in a lookup table called an S-box. A one-to-one mapping of all byte values from 0 to 255. Where r'(α,β) is the new value ,and r(α,β) is the original value.

$$r'^{(\alpha,\beta)} = r\big(r(\alpha,\beta)\big) \quad (1)$$

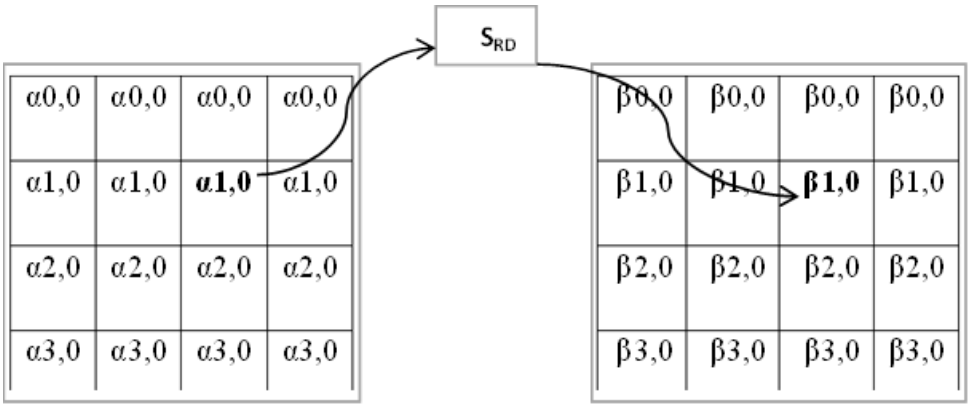

Figure 4: Sub Bytes Operates on individual bytes of state.

- Shift Rows: This transposition phase involves cyclically shifting each state row a predetermined number of steps. Where b is the row number, the rows are moved left by a certain number of bytes. where r'(α,β) is the new value , and r(α,β) is the original value.

$$r'^{(\alpha,\beta)} = r(\alpha, (\alpha + \beta) mod\ 4) \quad (2)$$

Initial state

1α	1β	1γ	1δ
2α	2β	2γ	2δ
3α	3β	3γ	3δ
4α	4β	4γ	4δ

after shifted rows

1α	1β	1γ	1δ
2β	2γ	2α	2α
3γ	3δ	3α	3β
4δ	4α	4β	4γ

Figure 5: Shift Rows

● Mix Columns: The operation of a Mix Column is utilized following the application of the S-box and shift rows operation to the state. In this stage, the four bytes in each of the state's columns are combined by a mixing operation. A fixed polynomial, μ, is multiplied by the outcome.

$$(x) = 3x^2 + x^2 + x + 2\ modulo\ x^4 + 1 \quad (3)$$

$$\begin{pmatrix} \beta0 \\ \beta1 \\ \beta2 \\ \beta3 \end{pmatrix} = \begin{pmatrix} 02\ 03\ 01\ 01 \\ 01\ 02\ 03\ 01 \\ 01\ 01\ 02\ 03 \\ 03\ 01\ 01\ 02 \end{pmatrix} \otimes \begin{pmatrix} \alpha0 \\ \alpha1 \\ \alpha2 \\ \alpha3 \end{pmatrix}$$

Figure 6: Shows the effect of the column mix step on the state

● Add Round Key: A 4-word round key is provided for the first Add Round Key stage and each of the cypher's ten rounds using the RIJNDAEL key expansion algorithm, which accepts a 4-word (16-byte) key as input. The first step is to copy the key into a group of four words. Next, four groups are created based on the values of the preceding four words. At last, the encryption text is obtained. Where r'$(\alpha, \beta)$is the new value to added key , r(α,β) is the original value. $k(i,j)$Value of key.

$$r'(i,j) = r(\alpha,\beta) XOR\ k(i,j) \quad (4)$$

α0,0	α0,0	α0,0	α0,0
α1,0	α1,0	α1,0	α1,0
α2,0	α2,0	α2,0	α2,0
α3,0	α3,0	α3,0	α3,0

=

k0,0	k0,0	k0,0	k0,0
k1,0	k1,0	k1,0	k1,0
k2,0	k2,0	k2,0	k2,0
k3,0	k3,0	k3,0	k3,0

+

β0,0	β0,0	β0,0	β0,0
β1,0	β1,0	β1,0	β1,0
β2,0	β2,0	β2,0	β2,0
β3,0	β3,0	β3,0	β3,0

Figure 7: In Add Round Key, the round key is added to the state with a bitwise XOR

All of the layers must be inverted in order to decode; that is, the Mix Column layer must become the Inv Mix Column layer, the Byte Substitution layer must become the Inv Byte Substitution layer, and the Shift Rows layer must become the Inv Shift Rows layer. On the other hand, there are certain similarities between the inverse layer operations and the encryption layer processes. [31],[39],[42].

4.5 Steganography

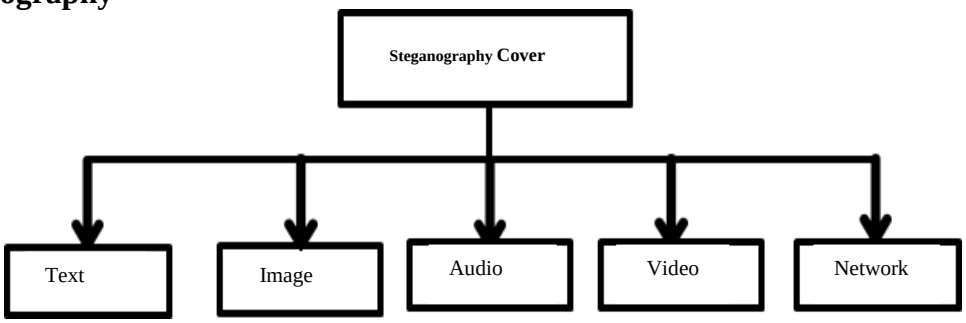

Figure 8: Steganography Cover

Utilizing a file as a container or cover, also known as a cover file, Sensitive information can be securely transferred and received to the designated destination by using steganography to hide it over unsecure networks. These days, a variety of digital file formats are utilized to hide sensitive information. Nevertheless, not all file formats may be used as cover files for steganography since each cover file needs to have enough redundant space for the hidden message to be placed in. [43], Due to their widespread usage on the Internet and the thousands of times they are exchanged among users every day, multimedia files are often used.[32] , Additionally, network protocols can be used to embed or conceal data. The sizes of the cover files, which serve as the concealed data's cover, are often dictated by the amount of the secret data that is intended to be embedded. Thus, the core elements of stenographic systems are cover files. This section reviews and generally classifies the covers used as cover files to encode hidden data in various steganography techniques into four categories (text, image, audio, video, and network), as seen in Figure 8.[44][45],[46].

Audio steganography, sometimes called Less Significant Bit (LSB) is a technique that can be used to hide information from audio recordings by changing the least significant bits of audio samples [47],[48],[49]. As we've seen, stenographic techniques and error-correcting codes are closely related. He unveiled a brand-new steganography that blends Rijndael phonetic steganography with LSB and a fresh error-correcting code. The proposed technique was assessed using several performance metrics, and the results showed that it provides better security and more embedding capacity than the current approaches. When using LSB audio steganography, it can be challenging to strike a compromise between the amount of information that can be hidden in an audio recording and the requirement that the user be ignorant of the modification.[7]

4.6 Image Encryption

Information security is one of the biggest obstacles to sharing private information over the internet. The proliferation of technology has made it necessary to develop more effective techniques for guaranteeing the integrity of data while it is being transmitted. Security algorithms can be broadly classified into two groups. The first category includes encryption algorithms, which modify data appropriately (encryption) so that it is not understandable to a potential interceptor. However, the sender and recipient can still share the data by encrypting and decrypting messages using a pair of public-private keys (asymmetric encryption) or a common key (symmetric encryption). For more information on the fundamentals of cryptography techniques, especially image encryption, in theory, the communication is secure if the right cryptosystem is used. However, in reality, no encryption technique is impenetrably secure against successful attacks. [50] The technique of utilizing a secret key to conceal photographs from unwanted access is known as image encryption. The arrangement of digital visual data is done using rectangular array frames. Pixels are the units used to represent members of an array; a pixel is a numerical value. As information technology (IT) has advanced, so too have digital images a type of information that includes binary, colour,

grayscale, and medical images, among others., have been used, saved, and communicated more and more. Thus, safeguarding this kind of data presents a significant challenge. Many existing image encryption algorithms, such as SCAN, circular random grids, elliptic curve El Gamal, gray code, wave transmission, vector quantization, fractional wavelet transform, p-Fibonacci transform, and chaos, have been proposed based on various technologies while taking into account the characteristics of the image data. [51]

5. PROCEDURE STEPS for AUDIO CIPHER-based RIJNDEL and STEGANOGRAPHY ALGORITHS

The new approach uses an audio cipher-based Rijndael and steganography algorithms

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

Process: Begin

Step 1: Read the sound file (WAV).

Step 2: Convert the sound file into hex data.

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

Step 4: Use the Rijndel algorithm (AES) of the required length

(128-bit, 192-bit or 256- bit) block cipher to encrypt WAV file.

Step 5: stego the audio file in cover by the image

Step 6 : compression the image and convert it to the bmp extraction

Step 7: To extract the decrypted file (WAV) data, the receiver

needs the new audio file(WAV) with a different key and block cipher .

Step 9: Return (S). End.

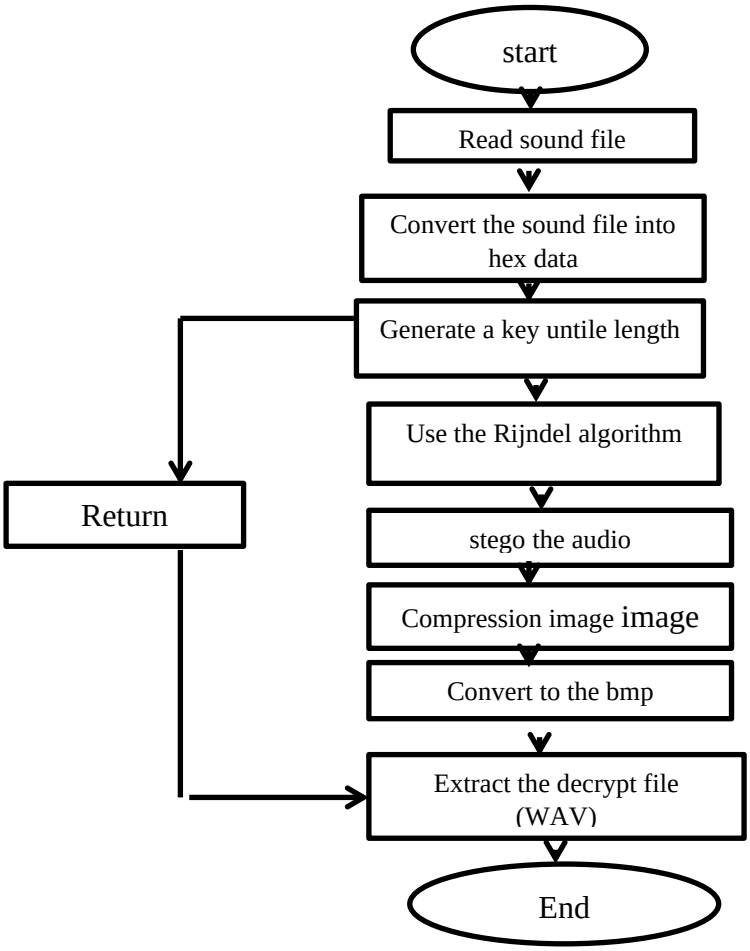

Figure 9: Audio Encryption System

6. Results and Discussion

A computer equipped with a 1 TB hard disk drive, 8 GB RAM, and an Intel Core i5 processor running Visual Basic was used to implement the proposed method, which is a combination of data encryption and hiding. First, regular audio files (with different sizes, keys, and samples) are converted into encoded audio files of an audio clip with a sample of 256. The outcomes of encrypting and decrypting data with steganography and Rijndal algorithms are displayed in Table 1. In the first scenario, we successfully encrypt the audio while restoring the original data in plaintext using a key size of 128 and a block size of 128 Next, different encryption keys and block sizes are used in each situation to complete Decryption process. The block and key size are limited to 256 up to this point. Secondly, hiding the data. After preparing the audio files encoded using the Rijndal algorithm, this data is now hidden inside an image with the bmp extension. We carry out the process of hiding the data in it and note the encryption time used (with different sizes, keys and samples) and we perform a compression process on it. We notice the weight reduction of the image and then we decompress it. By converting the bmp format from to Png and returning it to the bmp format, we also decrypt it and note that the time used for decryption is longer when using 256 (with different sizes, keys and samples), and the time is less for 128. The ultimate goal of the study and the criteria by which encryption and data hiding algorithms are evaluated, which is a complex method in terms of effectiveness and performance, are the foundations on which we base our analysis of these results. According to Rijndael. This is the 256th time that the block size and key is reached. Regarding encryption, decryption, data steganography and plaintext return, the success of the decryption process and recovery of the original data can be considered as very positive points. By comparing the key and block sizes used and their effect on sound quality, encoding strength and restoration of the original audio, performance and efficiency can also be examined. Two images were used, as shown in the figure, Table No. 1 continues to Image No. 1 and Table No. 2 continues to Image No. 2

Imag-1-

Imag-2-

Table 1: for image 1

Block Size	Key size	Plain Text	Encrypt	Encrypt time	Decrypt	Decrypt time
128	128	00010203040506070809 0A0B0C0D0E0F	5352E43763EEC1A8502433D6D520B1F0	0.020375	00010203040506070809 0A0B0C0D0E0F	0.00000000
128	192	5352E43763EEC1A8502433D6D520B1F0	6A6BC554EEDC117D00727EB7647E4993	0.003813	5352E43763EEC1A8502433D6D520B1F0	0.00000000
128	256	6A6BC554EEDC117D00727EB7647E4993	6220515108AAEC7BCA7DF06F7E629687	0.008000	6A6BC554EEDC117D00727EB7647E4993	0.05468750
192	128	6220515108AAEC7BCA7DF06F7E6296871011121314151617	BE8E606C012042FDB13991849C3FAC824637B597D90BA1F5	0.003125	6220515108AAEC7BCA7DF06F7E6296871011121314151617	0.00000000
192	192	BE8E606C012042FDB13991849C3FAC824637B597D90BA1F5	C28772D7B45F9156E80672A7AE0F020C56911484BF68BF69	0.002625	BE8E606C012042FDB13991849C3FAC824637B597D90BA1F5	0.00000000
192	256	C28772D7B45F9156E80672A7AE0F020C56911484BF68BF69	9C9BCEE110FB19DE2AEA7F2CD4361FED82B8C3D926B6EFC8	0.012063	C28772D7B45F9156E80672A7AE0F020C56911484BF68BF69	0.09375000
256	128	9C9BCEE110FB19DE2AEA7F2CD4361FED82B8C3D926B6EFC818191A1B1C1D1E1F	B0CB4FC1CCEEDF769D8458980E2A226762D58D697CBB2FAB6C4320A5644F7190	0.023875	9C9BCEE110FB19DE2AEA7F2CD4361FED82B8C3D926B6EFC818191A1B1C1D1E1F	0.00000000
256	192	B0CB4FC1CCEEDF769D8458980E2A2267 62D58D697CBB2FAB6C4320A5644F7190	80E78DF65415A59D0A404EB8AABB4E9B0BCB7F8322311B3E808ACAF440FAE887	0.019813	B0CB4FC1CCEEDF769D8458980E2A226762D58D697CBB2FAB6C4320A5644F7190	0.00781250
256	256	80E78DF65415A59D0A404EB8AABB4E9B0BCB7F8322311B3E808ACAF440FAE887	9F7A23FBA038CDCC88054D86BC571A3AD09385ACD7FE332DF647F63C7AEB8A93	0.036875	80E78DF65415A59D0A404EB8AABB4E9B0BCB7F8322311B3E808ACAF440FAE887	0.00078125 0

Table 2: for image 2

Block Size	Key size	Plain Text	Encrypt	Encrypt time	Decrypt	Decrypt time
128	128	000102030405060708090A0B0C0D0E0F	5352E43763EEC1A8502433D6D520B1F0	0.021000	000102030405060708090A0B0C0D0E0F	0.00000000
128	192	5352E43763EEC1A8502433D6D520B1F0	6A6BC554EEDC117D00727EB7647E4993	0.010875	5352E43763EEC1A8502433D6D520B1F0	0.00781250
128	256	6A6BC554EEDC117D00727EB7647E4993	6220515108AAEC7BCA7DF06F7E629687	0.007500	6A6BC554EEDC117D00727EB7647E4993	0.00000000
192	128	6220515108AAEC7BCA7DF06F7E6296871011121314151617	BE8E606C012042FDB13991849C3FAC824637B597D90BA1F5	0.002063	6220515108AAEC7BCA7DF06F7E62968710111213141516 17	0.00000000
192	192	BE8E606C012042FDB13991849C3FAC824637B597D90BA1F5	C28772D7B45F9156E80672A7AE0F020C56911484BF68BF69	0.000688	BE8E606C012042FDB13991849C3FAC824637B597D90BA1F5	0.00000000
192	256	C28772D7B45F9156E80672A7AE0F020C56911484BF68BF69	9C9BCEE110FB19DE2AEA7F2CD4361FED82B8C3D926B6EFC8	0.007375	C28772D7B45F9156E80672A7AE0F020C56911484BF68BF69	0.01562 50
256	128	9C9BCEE110FB19DE2AEA7F2CD4361FED82B8C3D926B6EFC818191A1B1C1D1E1F	B0CB4FC1CCEEDF769D8458980E2A226762D58D697CBB2FAB6C4320A5644F7190	0.007000	9C9BCEE110FB19DE2AEA7F2CD4361FED82B8C3D926B6EFC818191A1B1C1D1E1F	0.00000000
256	192	B0CB4FC1CCEEDF769D8458980E2A226762D58D697CBB2FAB6C4320A5644F7190	80E78DF65415A59D0A404EB8AABB4E9B0BCB7F8322311B3E808ACAF440FAE887	0.01875	B0CB4FC1CCEEDF769D8458980E2A226762D58D697CBB2FAB6C4320A5644F7190	0.00000010
256	256	80E78DF65415A59D0A404EB8AABB4E9B0BCB7F8322311B3E808ACAF440FAE887	9F7A23FBA038CDCC88054D86BC571A3AD09385ACD7FE332DF647F63C7AEB8A93	0.003563	80E78DF65415A59D0A404EB8AABB4E9B0BCB7F8322311B3E808ACAF440FAE887	0.00000050

7. Discussion and Future Work

The results were wonderful and distinctive, especially considering that most of the encryption using the Rijndahl algorithm only works with text, as well as Steganography. Now we were able to work and combine the two methods together. However, we tried the audio and were able to encrypt and hide the key and block size to 256, which makes it more difficult to hack. This provides a guide to improving the security and effectiveness of audio data encryption and Steganography methods. We are keen to experiment with different algorithms and methodologies using different types of images.

8. Conclusion

An ancient field, cryptography has evolved into a critical field of study for the security of communications, confidential transmission and storage. We can prevent our information from being compromised by using steganography and encryption for secure communication. As a result, encryption algorithms based on the Rijndael series of algorithms increase the security of an effective audio encryption method. After encryption, we hid the data in the images. We exposed the images to compression and then retrieved the audio data as it is in this work. We have successfully established a reliable and effective use of Rijndael-based combined Steganography to secure the transmission or storage of audio data by carefully evaluating all performance and security considerations. The results of this methodology have helped develop voice encryption methods in various industries and have contributed to voice security.

References

[1] Kakde Y., Gonnade P., Dahiwale P. ,"Audio Video Steganography for Authentication and Data Security", *Journal of Emerging Technologies and Innovative Research (JETIR)*, vol. 2, no. 6, pp.1763-1769, 2015.

[2] Khodher M.A.A., Alabaichi A.W., Altameemi A. A. ," Steganography Encryption Secret Message in Video Raster Using DNA and Chaotic Map ," *Iraqi Journal of Science*, vol. 63, no. 12, pp. 5534-5548, 2022 DOI: 10.24996/ijs.2022.63.12.38

[3] Faisel G. Mohammed , Hind M. Al-Dabbas, "Application of WDR Technique with different Wavelet Codecs for Image Compression", *Journal Iraqi journal of science*, vol. 59, no.4B, pp. 2128-2134 , 2018

[4] El Hanouti I., El Fadili H., "Security analysis of an audio data encryption scheme based on key chaining and DNA encoding". *Multimedia Tools and Applications, Springer Science and Business Media LLC*, vol. 80, no. 8, pp. 12077–12099, 2021. doi.org/10.1007/s11042-020-10153-8

[5] 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*, vol. 64 , no. 5 , pp. 2589-2600, 2023.

[6] Hassan N.A., Al-Mukhtar F.S. ,Ali E.H.," Encrypt Audio File using Speech Audio File As a key", in 2nd International Scientific Conference of Al-Ayen University (ISCAU-2020), IOP Conf. Series: Materials Science and Engineering 928, 2020 , doi:10.1088/1757-899X/928/3/032066

[7] Maarez H.G., Jaber H.S., Shareef M.A. ,"Utilization of Geographic Information System for hydrological analyses: A case study of Karbala province", *Iraqi Journal of Science*. , vol. 63, no. 9, pp. 4118-4130,2022

[8] Sethia P. , Kapoorb V. ,"A Proposed Novel Architecture for Information Hiding in Image Steganography by using Genetic Algorithm and Cryptography," in 2016 International Conference on Computational Science , Procedia Computer Science vol. 87, pp. 61 – 66, 2016, doi: 10.1016/j.procs.2016.05.127

[9] 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..

[10] Kazum H.A. , Mohammed F.G., "White blood cell recognition via geometric features and naïve bays classifier", *International Journal of Engineering & Technology*, vol. 7, no. 4 ,pp. 3642-3646, 2018.

[11] 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

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

[13] Aslam M., Alkhaldi A.H. ,"A Novel Method of Audio Steganography using Advanced Encryption Standard", *Nonlinear Engineering* ,vol. 4, no. 3, pp. 155–159,2015, doi: 10.1515/nleng-2015-0018

[14] 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

[15] 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

[16] Cheroiu, D.-G., Raducanu, M., Nitu, C.M.,"Fast Image Encryption Algorithm Based on Multiple Chaotic Maps", 202214th International Conference on Communications, COMM 2022 - Proceedings , DOI: 10.1109/COMM54429.2022.9817317

[17] Masure L., Strullu R. ,"Side-channel analysis against ANSSI's protected AES implementation on ARM: end-to-end attacks with multi-task learning", J Cryptogr Eng 13,129–147(2023). https://doi.org/10.1007/s13389-023-00311-7

[18] Hussein N.H, Ali M.A. ,"Medical Image Compression and Encryption Using Adaptive Arithmetic Coding, Quantization Technique and RSA in DWT Domain", *Iraqi Journal of Science*,2279-96,2022

[19] Shukla S.S. , Jaiswal V. , Gupta S. , Singh A.,"Steganography Technique of Sending Random Passwords on Receiver's Mobile", *IOSR Journal of Computer Engineering (IOSR-JCE)* e-ISSN: 2278-0661, ISSN: 2278-8727,vol.15, Iss. 3 ,2013, pp. 17-25 ,www.iosrjournals.org

[20] Fateh M. , Rezvani M. , Irani Y.,"A New Method of Coding for Steganography Based on LSB Matching Revisited", *Hindawi ,Security and Communication Networks*, 2021, 6610678, pag15 ,https://doi.org/10.1155/2021/6610678

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

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

[23] Shanthakumari R. , Devi EM.R.. , Rajadevi R., Bharaneeshwar B.," Information Hiding in Audio Steganography using LSB Matching Revisited", *IOP Publishing, Journal of Physics: Conference Series ICITSD* , 2021 1911 012027 ,2021, doi:10.1088/1742-6596/1911/1/012027

[24] Hemeida1 F., Alexan1 W., Mamdouh1 S. ," A Comparative Study of Audio Steganography Schemes", *International Journal of Computing and Digital Systems, Int. J. Com. Dig. Sys*. vol. 10, no.1,pp.556-562 ,2021, http://dx.doi.org/10.12785/ijcds/100153

[25] 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.

[26] 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, pp. 185~194,2022, DOI: 10.11591/eei.v11i1.3279.

[27] 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.

[28] 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

[29] Nisha O.T. Hossain M.S., Rahman M.,''Audio Steganography with Intensified Security and Hiding Capacity", *European Chemical Bulletin* , vol. 12, no. 10, pp. 162-173,2023 ,DOI: 10.48047/ecb/2023.12.10.013

[30] Macovei C., Răducanu M., Cheroiu, D.-G. ,"Fast speech encryption algorithm based on Arnold 3D chaotic system," *Proceedings of SPIE - The International Society for Optical Engineering*, 12493, art. no. 124932E,2023, DOI: 10.1117/12.2643008

[31] Shakya S. , Lamichhane S., "Secured Crypto Stegano Data Hiding Using Least

Significant Bit Substitution and Encryption''. *Journal of Advanced College of Engineering and Management*, 2, 105-112.,2016,

[32] Abdulla A.A. ,"Exploiting Similarities Between Secret and Cover Images for Improved Embedding Efficiency and Security in Digital Steganography ", thesis Submitted to the School of Science in the University of Buckingham,2015

[33] Albahrani1 E.A. , AlsheklyT.K. , Lafta S.H.,"A Review on Audio Encryption Algorithms Using Chaos Maps-Based Techniques ," *Journal of Cyber Security and Mobility*, vol. 11, no. 1, pp. 53–82, 2021, doi: 10.13052/jcsm2245-1439.1113

[34] 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,

[35] Mritha R., Isa N.A.M., R P., "An in video steganography." *Procedia Computer Science*, 171: 1147-1156. 2020

[36] Daemen, J.; Rijmen, V.. In The Design of Rijndael: The Advanced Encryption Standard (AES);, Eds.; Information Security and Cryptography; Springer: Berlin/Heidelberg, Germany, 2020;. ISBN 978-3-662-60769-5.

[37] Li, K., Li, H. & Mund, G. A reconfigurable and compact subpipelined architecture for AES encryption and decryption''. *EURASIP J. Adv. Signal Process*., 2023, 5 2023,https://doi.org/10.1186/s13634-022-00963-3

[38] Rathod C., Gonsai A. ," Performance Analysis of AES, Blowfish and Rijndael: Cryptographic Algorithms for Audio", In: Rathore, V.S., Dey, N., Piuri, V., Babo, R., Polkowski, Z., Tavares, J.M.R.S. (eds) Rising Threats in Expert Applications and Solutions. Advances in Intelligent Systems and Computing, vol 1187. Springer, Singapore. 2021, https://doi.org/10.1007/978-981-15-6014-9_24

[39] Easttom W. ,"Modern Cryptography: Applied Mathematics for Encryption and Information Security", ISBN: 978-3-030-63114-7 ,2021, DOI:10.1007/978-3-030-63115-4

[40] Daemen, J., & Rijmen, V.," The block cipher Rijndael", In International Conference on Smart Card Research and Advanced Applications (pp. 277–284). Springer, Berlin, Heidelberg,1998

[41] Raducanu M., Cheroiu D. G., Nitu C.M. ,"A Novel Comparison between Different Composite Chaotic Maps Applied on Sound Encryption", *46th International Conference on Telecommunications and Signal Processing, TSP*, pp. 225-229,,2023 DOI: 10.1109/TSP59544.2023.10197783

[42] Cheroiu D.G., Raducanu M., Nitu C.M. ,"Fast Image Encryption Algorithm Based on Multiple Chaotic Maps", *Proceedings 14th International Conference on Communications, COMM* , 2022 , DOI: 10.1109/COMM54429.2022.9817317

[43] R G. , KLAIB M.F. D.J. , SAMANTA , KHANM. Z.,"Social Media and Steganography: Use, Risks and Current Status", *IEEE Access* ,vol. 9 no.9, pp.153656-153665, 2021, DOI 10.1109/ACCESS.2021.3125128, IEEE Access

[44] Hamza Ali H. R. , Kadim J. M. ,"Text-based Steganography using Huffman Compression and AES Encryption Algorithm ", *Iraqi Journal of Science*, vol. 62, no. 11, pp. 4110-4120,2021, DOI: 10.24996/ijs.2021.62.11.31

[45] Simanjuntak H. L., Anggoro Suryo Pramudyo A. S., Rian Fahriza F.,"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,

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

[47] Liu D., Caceres M., Robichaux T.,Forte D.V., Seagren E.S., Ganger D. L. , Smith B.,"Next Generation SSH2 Implementation Securing Data in Motion,CH3 ,An Introduction To Cryptography", Syngress,2009,pp. 41-64,ISBN 9781597492836, https://doi.org/10.1016/B978-1-59749-283-6.00003-9.

[48] Mahmoud M., Elshoush H.T.I. ,"A Novel Enhanced LSB Algorithm for High Secure Audio Steganography", *Conference: 2018 10th Computer Science and Electronic Engineering (CEEC)*, 2018, DOI: 10.1109/CEEC.2018.8674230.

[49] George L.E., Hassan E.K., Mohammed S.G. , Mohammed F.G., " Selective image encryption based on DCT, hybrid shift coding and randomly generated secret key". *Iraqi J Sci*, 61(4):920–935.2020

[50] Darani A. Y., Yengejeh Y.K., Navarro G., Pakmanesh H., Sharafi J.,"Optimal location using genetic algorithms for chaotic image steganography technique based on discrete frame let transform'', *Digital Signal Processing*, 144,104228,ISSN 1051-2004, 2024,https://doi.org/10.1016/j.dsp.2023.104228.

[51] Ghadirli H.M., Nodehi A., Enayatifar R., "An overview of encryption algorithms in colour images", *Signal Processing*, vol. 164, pp. 163-185, ISSN 0165-1684,2019, https://doi.org/10.1016/j.sigpro.2019.06.010.