DOI: 10.24996/ijs.2024.66.2.14

ISSN: 0067-2904

Investigating Rijndael-Based Algorithms for Audio Ciphering

Sajaa G. Mohammed, Nuhad Salim Al-Mothafar*

Department of Mathematics, College of Science, University of Baghdad, Baghdad, Iraq

Received: 29/10/2023 Accepted: 17/2/2024 Published: xx

Abstract

Voice encryption is crucial to protecting data during transmission and storage due to the widespread problem of document fabrication and forgery. Various methods have been used to protect important data, including encryption. Voice data encryption is a way to encrypt important messages within transmissions. Therefore, it needs a strong and efficient encryption algorithm, using the standard encryption algorithm known as Rijndeal. This method is reliable, secure and efficient, because the Rijndael algorithm is characterized by its key lengths and blocks of different sizes. The Rijndael algorithm is a method of decrypting audio files, making it a powerful tool for protecting sensitive information. This paper presents a method for encoding WAV audio files using the Rijndael algorithm that is compatible with many audio formats. This study converts audio data into a 256-bit audio sample that has been used to encode using the Rijndael algorithm, as this algorithm is known for its robustness and has won many awards. The working principle of this algorithm is to create multiple blocks with different sizes and keys (128 bits, 192 bits or 256 bits). The algorithm creates keys for the purpose of encryption, and they are combined into the audio files using the Rijndael algorithm and decrypted that has been noted as the return of the original text. The goal of this proposed methodology is to protect audio data from attacking people and reduce the chances of this data being disclosed. This methodology is used for the purpose of transferring, storing and keeping confidential audio files securely with security aspects. One of the most important features of this research is the strength of the encryption, which is represented by the Rigndael algorithm, which led to the file being broken and restored at a record rate of up to 100%. It also provides a cutting-edge and innovative methodology. For the purpose of securing, transmitting, storing and protecting audio data in all modern digital fields.

Keywords: : Rijndael, Advanced Encryption Standard, Audio encryption, Audio ciphering, Block cipher Rijndael

دراسة الخوارزميات المبنية على ريجنديل للتشفير الصوتي

سجا غازي محمد , نهاد سالم المظفر

قسم الرياضيات , كلية العلوم , جامعة بغداد, بغداد, العراق

الخلاصة

يعد التشفير الصوتي أمرًا بالغ الأهمية لحماية البيانات أثناء النقل والتخزين نظرًا لانتشار مشكلة تلفيق المستندات وتزويرها. تم استخدام أساليب مختلفة لحماية البيانات المهمة، بما في ذلك التشفير. يعد تشفير البيانات الصوتية وسيلة لتشفير الرسائل المهمة ضمن عمليات الإرسال. ولذلك فهو يحتاج إلى خوارزمية تشفير قوية وفعالة، وذلك

باستخدام خوارزمية التشفير القياسية المعروفة باسم Rijndeal هذه الطريقة موثوقة وآمنة وفعالة، لأن خوارزمية Rijndael تتميز بأطوال مفاتيحها وكتلها ذات أحجام مختلفة. تعد خوارزمية Rijndael طريقة لفك تشفير الملفات الصوتية، مما يجعلها أداة قوية لحماية المعلومات الحساسة. يقدم هذا البحث طريقة لترميز الملفات الصوتية WAV باستخدام خوارزمية Rijndael المتوافقة مع العديد من صيغ الصوت. تقوم هذه الدراسة بتحويل البيانات الصوتية إلى عينة صوتية بحجم 256 بت نستخدمها للتشفير باستخدام خوارزمية Rijndael، حيث أن هذه الخوارزمية معروفة بقوتها وقد حازت على العديد من الجوائز. مبدأ عمل هذه الخوارزمية هو إنشاء كتل متعددة بأحجام ومفاتيح مختلفة ذات (128 بت، 192 بت أو 256 بت)، تقوم الخوارزمية بإنشاء مفاتيح لغرض التشفير، ويتم دمجها في الملفات الصوتية باستخدام خوارزمية Rijndael وفك تشفيرها. ونلاحظ عودة النص الأصلي. الهدف من هذه المنهجية المقترحة هو حماية البيانات الصوتية من مهاجمة الأشخاص وتقليل فرص الكشف عن هذه البيانات. يتم استخدام هذه المنهجية لغرض نقل وتخزين والحفاظ على الملفات الصوتية السرية بشكل آمن مع الجانب الأمني. ومن أهم مميزات هذا البحث هي قوة التشفير والتي تتمثل بخوارزميةRigndael والتي أدت إلى كسر الملف وإعادته بمعدل قياسي يصل إلى 100%. كما أنه يوفر منهجية متطورة ومبتكرة. لغرض تأمين ونقل وتخزين وحماية البيانات الصوتية في كافة المجالات الرقمية الحديثة.

1. Introduction

These days, audio data security plays a major role in the IT business and is expanding quickly.[1,2] Encrypting audio data prevents illegal access and manipulation while guaranteeing its integrity and confidentiality.[3,4] Technology preservation of audio files from hackers and eavesdroppers became crucial for the tech 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 [5, 6]. Nonetheless, algorithms, procedures, and techniques make it simple to process voice signals and recognize text spoken by a speaker. This an 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. [7],[8] the Rijndael algorithm is a symmetric block cypher with lengths of 128, 192, and 256 bits that can handle data blocks of 128 bits. Of the restriction 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. [9,10] 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. [11,12] The research on Investigating Rijndael-based algorithms for Audio Ciphering approaches that were published from 2015 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: In this article, we give a summary of the investigating Rijndael-Based Algorithms for Audio Ciphering. The rest of this work is structured as follows: Section 2 is devoted to Problem Statement. Section 3 is related to the work review. In Section 4, we present Encryption Methodology, followed by the Procedure Steps for Audio Ciphering based Rijndael Algorithm in Section 5. Then, in Section 6,7, we present the mresults and discussion, and finally, Section 8 is devoted to discussion and Future works, concludes this paper.

2. PROBLEM STATEMENT

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

- We have increased complexity by using multiple block sizes and different key sizes (128-bit, 192-bit, or 256-bit).
- Although Rijndael voice encryption is generally considered secure, increasing the length to 256 bits meant that attackers could not exploit it.
- Complexity and difficulty are used to increase security, especially for inexperienced users.

3. RELATED WORK REVIEW

In 2015, Audio Steganography was introduced by Simanjuntak H. L. et al. [13]. This method was Combined with the Rijndael Cryptography Algorithm. The Rijndael algorithm in cryptography and the Least Significant Bit (LSB) in steganography were combined into an audio file for a strong security system.

In 2018, Audio Steganography was introduced by Mahmoud M. and et al. [14]. This method was the Enhanced LSB Algorithm for High Secure. To ensure audio transmission was secure, an audio file was first encrypted using the Huffman method, then concealed using the AES technique, and then revealed using the cutting-edge LSB-Block algorithm.

In 2019, the Audio Encryption Algorithm was introduced by Kordov K. [15]. This method was Permutation-Substitution Architecture. It used a pseudo-random number generator composed of a chaotic circle map and modified rotation equations into an audio form for necessary Cryptographic security for audio file encryption.

In 2020, Wang X introduced Audio Encryption Algorithm et al. [16]. This method was DNA coding and a chaotic system. It employed chaotic systems and DNA coding to confuse and disperse audio data into an audio file for high security.

In 2020, Encrypt Audio File was introduced by Hassan N.A. et al. [5]. This method uses Speech Audio File As a key. It stores a two-secret key by converting a voice audio file to text. This text generates a seed with two keys using a hash function. Then, it encrypts the original audio file using the Rijndael algorithm into text form for strong audio transmission security.

In 2022, the audio Encryption Algorithm was introduced by Dai W.and et al. [17]. his method was the Chen Memristor Chaotic System. First, the signal was compressed and denoised using the Fast Walsh–Hadamar Transform (FWHT), which has superior energy compression properties to the Fast Fourier Transform (FFT) and the Discrete Cosine Transform (DCT). This was done to obtain higher security by encoding the audio file.

In 2023, Audio Signal Encryption was introduced by Abdallah H.A. et al. [18]. his approach was taken. In the first technique, random numbers are projected onto the audio signals' DWT coefficients. The third approach, which operates in three stages—fusion, substitution, and chaotic permutations improves security by using multiple layers of processing for encryption. The second approach uses salting methods. To stop unapproved outsiders from listening to audio that has been encrypted.

4. ENCRYPTION METHODOLOGY

Three areas of work focus are identified in this system design: the encryption and decryption process, the key generation method and block size. [19] 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).[20]

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- Rijdnal algorithm. This suggested system gives the users two options for encrypting and decrypting data. Encryption hidden information.

1. Presenting a method for using encryption
2. Algorithm that provides better accuracy and quality of encryption V.B.studio is used by of In information concealment, the Rijandnel algorithm is used. They are encoded and put into an audio file, which is transferred along with text and other file formats to the destination.

4.1Audio Ciphering

Audio encryption is a way to immune data in a sound file from intrusive attacks that have been applied the (noise) key and the exact algorithm to the original text. Our primary focus is on encryption Techniques for handling audio data. Analyzing and comparing fundamental encryption standards that has shown that ways of encryption can be used to encode audio.. like AES, DES and Triple DES (3-Data Encryption Standard). [21,22],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 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 chunks could be added in the future. [5,23]

This reach focuses on the aspects of previous chaotic audio algorithms did not consider its advantages and disadvantages. Analogy 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 [24]

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 at the conclusion of this report, a decision has been made regarding the Reijndael. 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.[25] Daemen and V. created the Rijndael algorithm, renamed the AES.The steps involved in AES Encoding and decoding are depicted in Figure 1. These action, 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 a key extending routine to create a key schedule. Given an employee provide 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 [26, 27]. Lastly, Rijndael's internal round structure appears to have good potential to benefit from instruction-level parallelism. Security is 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, Reijndeal operations are among the easiest operations to defend against hacker and timing attacks. In addition to this, it provides some defines against such attacks without affecting performance in a very significant way. Reijndeal encryption, designed to withstand brute force attacks, employs a strong key, proper encryption algorithm, secure hardware, and software to prevent side-channel attacks and thwart cryptanalysis attempts [25], [28]

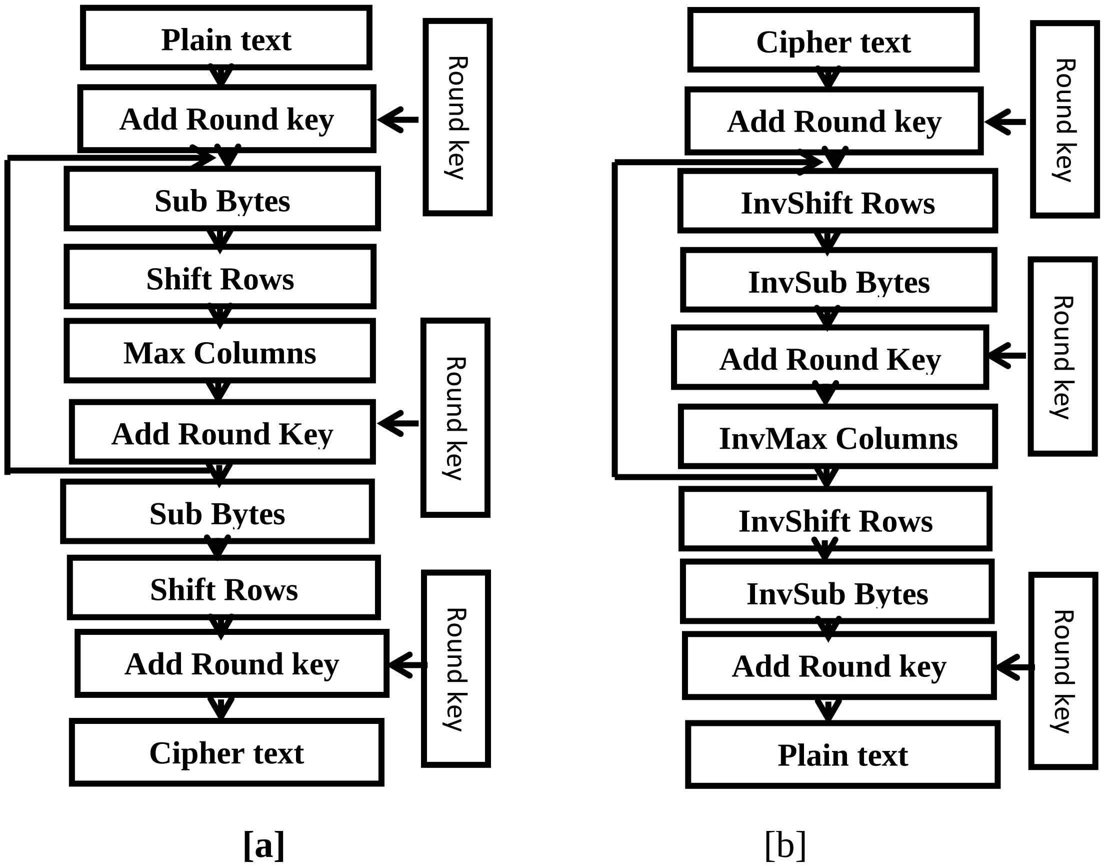


Figure 1: Rijndel algorithm (a) Encryption structure; (b) Decryption structure [26].

4.3 Block cipher Rijndael Algorithm

The AES has three key standards: 128 bits, 192 bits, or 256 bits. The Rijndael cipher, created by Belgian cryptographers Daemen and Rijmen, supports different block and key sizes, including 128, 160, 192, 224, and 256 bits. However, the AES standard states the block standard of 128 bits and the key standard of 128, 192, and 256 bits. The Rijndael algorithm uses a substitution permutation matrix instead of a Feistel network. To function, the 128-bit plain text block must be placed into a 4-byte by 4-byte matrix, which will change as the algorithm runs through its sequence of phases. This matrix, known as the state, must be converted to binary before being placed into a matrix. The Rijndael cipher is a significant advancement in the field of ciphers, allowing for more flexible and secure encryption methods, as illustrated in Figure 2 [29]

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

Figure 2: convert the plain text block into binary

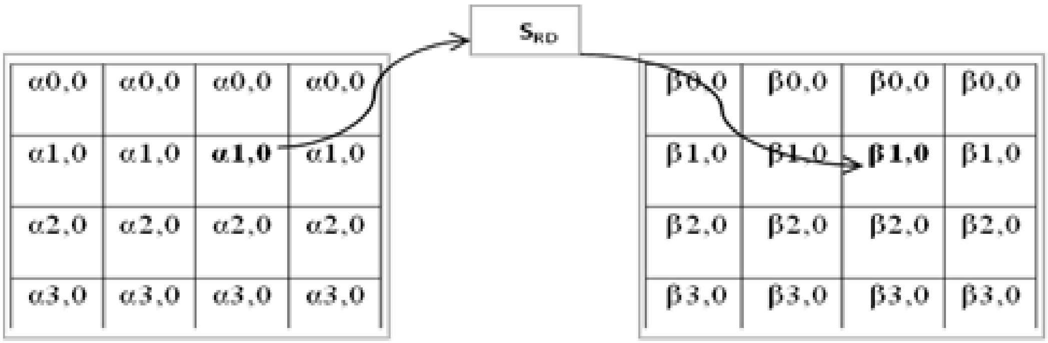
Rijndael is an iterated block cypher with a variable block length and variable key length. It is possible to independently set the block and key lengths to 128, 192, or 256 bits. Similar to Square and BKSQ, the wide trail technique was used in the design of Rijndael. This design technique offers protection from both differential and linear cryptanalysis. The round transformation is broken down into various components in the approach, each with a distinct function. [30, 29]

4.4 METHOD: RIJNDAEL CRYPTOGRAPHIC ALGORITHM

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)new value , r(α,β) Original value.

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



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

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 3: 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)new value , r(α,β) Original value.

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

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 4: 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.

$$(x) = 3x^2 + x^2 + x + 2 \text{ modulo } x^4 + 1 \tag{3}$$

$$\begin{pmatrix} \beta 0 \\ \beta 1 \\ \beta 2 \\ \beta 3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \otimes \begin{pmatrix} \alpha 0 \\ \alpha 1 \\ \alpha 2 \\ \alpha 3 \end{pmatrix}$$

Figure 5: 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'(α, β)new value to an added key , r(α,β) Original value. $k(i, j)$Value of the key.

$$r'(i, j) = r(\alpha, \beta) \text{XOR } k(i, j) \tag{4}$$

$$\begin{array}{|c|c|c|c|} \hline \alpha 0,0 & \alpha 0,0 & \alpha 0,0 & \alpha 0,0 \\ \hline \alpha 1,0 & \alpha 1,0 & \alpha 1,0 & \alpha 1,0 \\ \hline \alpha 2,0 & \alpha 2,0 & \alpha 2,0 & \alpha 2,0 \\ \hline \alpha 3,0 & \alpha 3,0 & \alpha 3,0 & \alpha 3,0 \\ \hline \end{array} = \begin{array}{|c|c|c|c|} \hline k0,0 & k0,0 & k0,0 & k0,0 \\ \hline k1,0 & k1,0 & k1,0 & k1,0 \\ \hline k2,0 & k2,0 & k2,0 & k2,0 \\ \hline k3,0 & k3,0 & k3,0 & k3,0 \\ \hline \end{array} + \begin{array}{|c|c|c|c|} \hline \beta 0,0 & \beta 0,0 & \beta 0,0 & \beta 0,0 \\ \hline \beta 1,0 & \beta 1,0 & \beta 1,0 & \beta 1,0 \\ \hline \beta 2,0 & \beta 2,0 & \beta 2,0 & \beta 2,0 \\ \hline \beta 3,0 & \beta 3,0 & \beta 3,0 & \beta 3,0 \\ \hline \end{array}$$

Figure 6: 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. [20, 28–31]

5. PROCEDURE STEPS for AUDIO CIPHER-based RIJNDEL ALGORITHM

The prove procedure for an audio cipher-based Rijndel algorithm

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 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.

Step 5: To extract the decrypted file (WAV) data, the receiver needs the new audio file(WAV) with a different key and block cipher .

Step 6: Return (S). End.

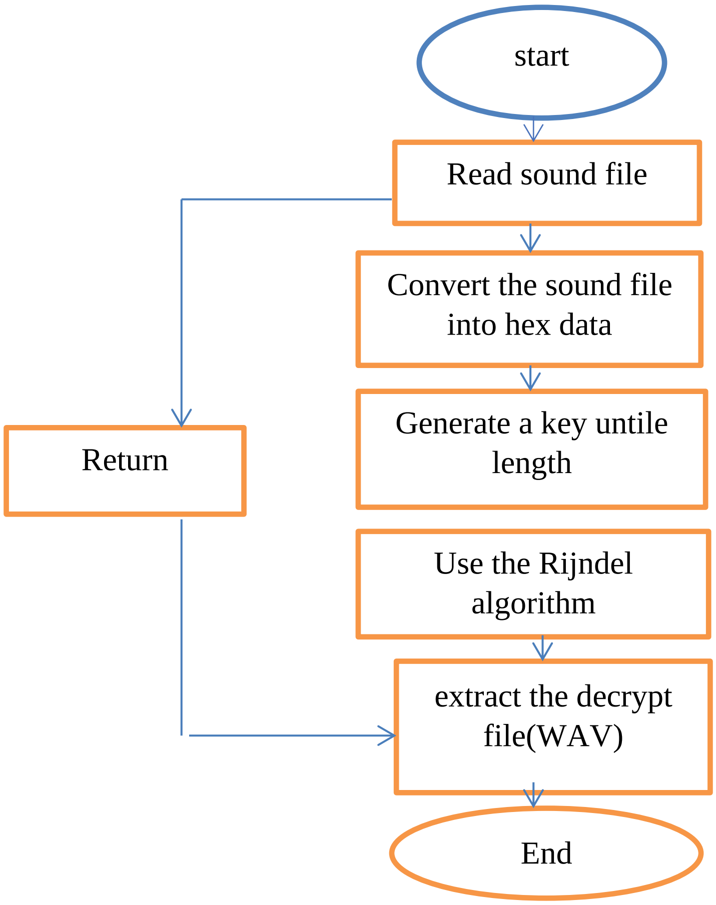

start
Read sound file
Convert the sound file into hex data
Generate a key untile length
Use the Rijndel algorithm
extract the decrypt file(WAV)
Return
End

Figure 7: audio encryption system

6. Results and Discussion

The work was implemented through a Visual Basic 6 operating program to implement the proposed algorithm. Regular audio files with multiple block sizes and different key sizes (128-bit, 192-bit, or 256-bit) are converted into encrypted audio files. The results of the encryption and decryption processes using Rijndal algorithms are shown in Table 1. In the first scenario, we successfully encrypted the audio while recovering the original data in plain text using a key size of 128 and a block size of 128. Next, we used a key size of 192 and a block size of 192 to arrive at a key size of 256. 256 and block size 256 Different encryption keys and block sizes are used in each situation to complete the decryption process. The size of the block and key is limited to 256, so at this point, when the length increases, it will be difficult to break. The ultimate goal of the study and the criteria by which cryptographic algorithms are evaluated for effectiveness and performance are the foundations on which we base our analysis of these results. According to Rijndael, This is due to the increased length of 256 bits at which the block and key size are reached. We previously knew that increasing the length would affect the non-decryption. Regarding encryption, decryption, and return of the plaintext, the success of the decryption process and recovery of the original data can be considered 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.

Table 1: Results of the encryption and decryption

Block Size	Key size	Plain	Encrypt	Decrypt
128	128	000102030405060708090A0B0C0D0E0F	E43763EEC1A8502433D6D520B1F0525	000102030405060708090A0B0C0D0E0F

128	192	000102030405060708090A0B0C0D0E0F	8046725C5FE415DC926CB08F54B1681A	000102030405060708090A0B0C0D0E0F
128	256	000102030405060708090A0B0C0D0E0F	000102030405060708090A0B0C0D0E0F	000102030405060708090A0B0C0D0E0F
192	128	000102030405060708090A0B0C0D0E0F1011121314151617	9F6DCA7965C74923C77A4A0A32FB43994C2E1B5BA0FB8035	000102030405060708090A0B0C0D0E0F1011121314151617
192	192	000102030405060708090A0B0C0D0E0F1011121314151617	1B83638F6919CA2C5D8B4999D13793E19180DAFDBDCA7372	000102030405060708090A0B0C0D0E0F1011121314151617
192	256	000102030405060708090A0B0C0D0E0F1011121314151617	88C27972B10BCCA2B4312B05CA87A541DBD6034A3AC070EC	000102030405060708090A0B0C0D0E0F1011121314151617
256	128	000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F	4D82D84A04FAA83D78D666369A8FC1FD611859EE3A7FF6C3B0D5C8D15E5737F5	000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
256	192	000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F	EA79CCB5328288A7A3B24E537CC77E34A6AB17F0012C2CC04F303900BFC195EE	000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
256	256	000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F	DC6214B7820FC68E844B42025A33C020CA578F2B73C80A48B220E6C0EE76EBBB	000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F

7. Discussion and Future Work

The results were impressive, especially considering that most cryptography using the Rijndahl algorithm only works with text. However, we tried to experiment with the sound and we were able to encrypt multiple blocks with different sizes and keys (128-bit, 192-bit or 256-bit), especially at 256 blocks and keys, which makes it more difficult to hack. This provides a guide to improving the security and effectiveness of audio encryption methods. We are keen to experiment with different algorithms and methodologies in all areas of audio.

8. Conclusion

From an antiquated discipline, cryptography has developed into a crucial study area for communication security. We can guard against having our information compromised by employing steganography and encryption for secure communication. As a result, encryption algorithms based on the Rijndael encryption algorithm series serve to increase the security of the efficient audio encryption method. An examination of the use of Rijndael-based algorithms for phonetic encryption was provided in this work. We have successfully created a reliable and efficient usage of the Rijndael-based method to secure the transmission or storage of voice data by carefully weighing all performance and security considerations. The outcomes of these investigations aided in developing speech encryption methods across various industries and 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] 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

[4] 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.

[5] 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

[6] 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

[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] 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

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

[10] 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

[11] 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

[12] 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

[13] 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,

[14] 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.

[15] Kordov k. ,"A Novel Audio Encryption Algorithm with Permutation-Substitution Architecture ", *Electronics*, vol. 8, no. 5 ,pp. 530 ,2019, doi:10.3390/electronics8050530

[16] Wang X, Su Y ," An audio encryption algorithm based on DNA coding and chaotic system". IEEE Access 8:9260–9270. https://doi.org/10.1109/ACCESS.2019.2963329.2020

[17] Dai W., Xu X., Song X. , Li G., "Audio Encryption Algorithm Based on Chen Memristor Chaotic System", *Symmetry*, vol. 14, no. 1, pp.17,2022, https://doi.org/10.3390/sym1401001

[18] Abdallah H.A. , Meshoul S.,"A Multi-layered Audio Signal Encryption Approach for Secure" *Electronics*, vol. 12, no. 1, pp.2 ,2023, https://doi.org/10.3390/electronics12010002,

[19] 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

[20] 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, pp. 105-112.,2016,

[21] 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

[22] 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,

[23] 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

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

[25] 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.

[26] 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

[27] 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

[28] 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

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

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

[31] 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