Acknowledgments

All the praise to the Almighty Creator, whose blessing helped us to successfully complete this thesis work. We show significant and indescribable gratefulness to our honorable supervisor Prottoy Saha, Assistant Professor, Department of Computer Science and Engineering, Khulna University of Engineering & Technology for his outstanding helpful contribution in giving support, suggestion and encouragement. We acknowledge his constant co-operation and proper guidance throughout the development process. He has been a great source of effective and feasible ideas, profound knowledge and all time feedback for us.

Abstract

Transferring multimedia files like audio is a common problem with information security. Therefore, good encryption technologies are needed to protect these contents. This thesis proposes a new asymmetric encryption scheme based on DNA encoding for both text and audio data. The novelty of this scheme is the use of information vector generation in a new way. This method consists of random sequence mixing motivated from farming crops that ensures the diffusion and confusion property of Shannon characteristics. Comparison experiments using audio sample show that the algorithm works well and is secure enough to withstand many common attacks and can be recommended for audio encryption.

Contents

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

Introduction

1.1 Background

The rapidly evolving nature of multimedia and mobile technologies has raised the bar for security technology. In daily life, audio, video, and image are essential. Multimedia data, in particular audio data, is crucial [1]. If it is not properly encrypted, the user's privacy will be compromised, which will cause a significant effect. As a consequence, research on audio encryption algorithms has become vital.

Information security [2]–confidentiality, integrity, and availability (the CIA triad) of information, plays a significant role in today's society. Complex and sophisticated encryption systems [3] depending on hard computational problems have been developed for secure communication in order to fulfill these requirements [4]–[6].

The enormous and ongoing progress of electronic computers [7] will soon enable it to break currently used cryptography protocols within a reasonable amount of time by brute-force attacks [8], while the rise of novel quantum computers [9] will make it possible to break keys based on prime factorization through the use of Shor's algorithm [10]. Therefore, next-generation encryption that overcomes these concerns has generated a significant amount of attention. Particularly, quantum encryption techniques that take advantage of the quantum mechanical uncertainty principle have enormous potential for ensuring communication confidentiality [11]. It is unknown, however, whether quantum communication would facilitate complete CIA of information.

As an alternative to computational encryption systems, biomolecular cryptography has been proposed, which makes use of highly precise, thermodynamically regulated biomolecular interactions [12]–[14].

DNA(Deoxyribonucleic Acid) is a long, double-stranded molecule that contains the genetic information for all living organisms. It is composed of nucleotides, which are the building blocks of DNA and are made up of a sugar molecule, a phosphate group, and a nitrogenous base. The nitrogenous bases in DNA include adenine (A), cytosine (C), guanine (G), and thymine (T), and the sequence of these bases determines the genetic code and the instructions for the development and functioning of living organisms [15].

DNA encryption refers to a method of encoding data into DNA molecules for secure storage and retrieval. The idea of using DNA for data storage [16] was first proposed in the 1990s and has since been developed into a practical technology. DNA provides a dense and durable storage medium, with the potential to store large amounts of data for hundreds or even thousands of years. Encryption is used to protect this stored data from unauthorized access, as DNA samples can be easily obtained and sequenced [17]. To encrypt data into DNA, the binary code of the data is first converted into a sequence of the four DNA bases (A, C, G, and T). This sequence is then synthesized into DNA strands and stored [18]. To retrieve the encrypted data, the DNA strands are sequenced and the original binary code is reconstructed using the same encoding method. DNA encryption is an emerging field with promising applications in data security, privacy, and long-term data preservation.

Audio encryption refers to the process of converting an audio signal into a form that can only be accessed or played back by authorized individuals or systems. The goal of audio encryption is to protect the confidentiality and integrity of the audio data and to prevent unauthorized access or modification [19]. There are various methods for audio encryption, including symmetric key algorithms, such as Advanced Encryption Standard (AES), and asymmetric key algorithms, such as the RSA algorithm [19]. The choice of encryption method depends on factors such as the desired level of security, computational requirements, and the intended use of the encrypted audio. In general, audio encryption is used in applications where sensitive or confidential information is being transmitted or stored in an audio format, such as secure voice communication systems, protected digital audio files, and encrypted voice memos.

DNA encryption on text data involves encoding text data as sequences of DNA nucleotides and using DNA-based algorithms and protocols to encrypt and decrypt the data. The basic idea is to map each letter of the text to a specific nucleotide and then concatenate the nucleotides to form a DNA sequence [20].

DNA encryption of audio is a novel and innovative approach to audio cryptography that involves encoding audio signals as sequences of DNA nucleotides and using DNA-based algorithms and protocols to encrypt and decrypt the audio data [21].

In theory, DNA encryption of audio offers several advantages over traditional audio encryption methods, including its ability to store large amounts of data in a compact form and its ability to perform parallel and highly scalable computations. Additionally, DNA is a robust and durable material that can withstand harsh environmental conditions, which makes it an attractive option for secure storage and transmission of audio data. [21]

DNA encryption of audio is a promising area of research with the potential to offer new solutions for secure audio communication. However, more research and development are needed to realize its full potential.

1.2 Motivation

The requirement for safe and long-term storage of substantial volumes of data serves as a major driving force behind the use of DNA encryption. Because DNA is very resistant to deterioration and data loss and can retain information for hundreds or thousands of years, it is a desirable alternative. Additionally, DNA encryption offers a very high level of security because it is difficult to decipher the encryption and access the stored data due to the complexity and unpredictability of DNA sequences.

The main motivations for using DNA encryption are [22]–[25]:

Long-term storage: DNA has the potential to store large amounts of information for hundreds or thousands of years, making it an attractive option for preserving data over long periods of time.

High security: DNA encryption provides a high level of security due to the complexity and randomness of DNA sequences, making it difficult for unauthorized individuals to access the stored information.

Increased data density: DNA has a high data density compared to other storage media, which allows for a large amount of data to be stored in a small amount of physical space.

Resistance to degradation: DNA is highly resistant to degradation and data loss, making it a stable and reliable option for storing data.

Non-volatility: Unlike other storage media, DNA does not require power to maintain its stored information, making it an ideal option for long-term storage and archiving.

Implementing DNA encryption of audio is a complex and challenging task that requires the development of new DNA-based algorithms and protocols, as well as the optimization of DNA sequencing and storage methods. At present, this is an active area of research, and there is limited published work on the topic.

1.3 Problem Statement

Audio encryption provides a way to secure and protect audio signals from unauthorized access, modification, or disclosure, ensuring the privacy and security of sensitive information [26].

Audio encryption is needed for several reasons, including:

Data Security: Audio signals often contain sensitive information, and encryption helps to protect this information from unauthorized access.

Intellectual property protection: Audio signals can be valuable intellectual property, and encryption helps to prevent unauthorized distribution and piracy.

Privacy: Audio signals can contain private or personal information, and encryption helps to protect this information from being intercepted or disclosed.

Compliance: Certain regulations, such as HIPAA [27] in the healthcare industry, require the secure storage and transmission of sensitive audio information.

Data integrity: Encryption can help to prevent unauthorized modification of audio signals during storage or transmission, ensuring the integrity of the information.

Theoretically, DNA encryption of audio offers several benefits compared to traditional audio encryption methods. One of these benefits is its ability to store a large amount of data in a compact format. DNA has a high data density, which allows for a lot of information to be stored in a small space. This makes DNA encryption ideal for audio data, as it allows for large audio files to be stored in a secure, compact form. Another advantage of DNA encryption is that it can perform complex computations in a parallel and highly scalable manner. The parallel processing capabilities of DNA can be utilized to perform calculations at a large scale, making it well-suited for audio encryption applications that require scalability.

While the potential benefits of DNA encryption for audio are significant, the technology is still in its early stages of development [21]. Therefore, we took different approach to a novel DNA-based encryption methods for audio data as well as text data.

1.4 Scopes and Objectives

The scope of this thesis on DNA encryption for audio signals will be to conduct a comprehensive study of the current state-of-the-art in this field and to make contributions to the field by addressing some of the current challenges. The thesis will cover the following aspects:

Overview of DNA encryption: This section will provide an introduction to DNA encryption, its benefits, and its suitability for audio signals.

Overview of audio signals: This section will provide a detailed overview of audio signals, their characteristics, and the challenges of storing and transmitting audio signals.

DNA encryption methods for audio signals: This section will provide an in-depth analysis of the existing DNA encryption methods for audio signals, including their strengths, weaknesses, and limitations.

Implementation and evaluation of a DNA encryption system for audio signals: This section will describe the implementation of a DNA encryption system for audio signals, including the design and development of a proof-of-concept system. The system will be evaluated in terms of its performance, security, and reliability.

Challenges and future directions: This section will discuss the challenges faced in the implementation of DNA encryption for audio signals and suggest areas for future research.

The aim of this thesis is to provide a comprehensive study of DNA encryption for audio signals and to make contributions to the field by addressing some of the current challenges.

Objectives of this thesis are:

i. To ensure more security over traditional cryptosystems.

ii. To build a novel DNA-based encryption and decryption technique.

iii. To apply the technique on both text and audio data.

iv. To compare the method with existing methods and algorithms.

1.5 Layout of the Thesis

This thesis is organized as follows.

Chapter I briefly explains the introduction of the thesis and motivation of works. Problem statement and objectives of this thesis are also discussed elaborately here.

Chapter II represents the existing works in the related field and focuses on the advantages and drawbacks of existing works.

Chapter III discusses the proposed methodology of the thesis.

Chapter IV explains the experimental and security analysis. This chapter also explains the experimental setup and the analyzing results and performance that compares with existing techniques.

Chapter V summarizes all findings and applications with concluding remarks and provides some recommendations on future research directions.

CHAPTER II

Literature Review

2.1 Introduction

A literature review of the article on DNA encryption for audio signals can provide a comprehensive understanding of the state-of-the-art in this field. DNA encryption has emerged as a promising solution for secure storage and communication of digital audio signals due to its large storage capacity, error correction capabilities, and high level of security. The use of DNA as a data storage medium has been widely studied in recent years, but its application to audio signals has only recently been explored. In this literature review, we will explore the recent advancements in DNA encryption for audio signals and the challenges that still need to be addressed. We will also discuss the existing methods for DNA encryption and their suitability for audio signals. The aim of this literature review is to provide a comprehensive overview of the current state of the art in DNA encryption for audio signals and to identify areas for future research.

2.2 Audio Encryption

There are several existing methods for audio encryption:

Symmetric encryption: This method uses a single key to encrypt and decrypt audio data. Examples of symmetric encryption algorithms used for audio encryption include Advanced Encryption Standard (AES) [28] and Twofish [29].

Asymmetric encryption: This method uses a pair of keys, a public key for encryption and a private key for decryption. Examples of asymmetric encryption algorithms used for audio encryption include RSA [4] and Elliptic Curve Cryptography (ECC) [30].

End-to-end encryption: This method encrypts audio data at the source (e.g. microphone) and decrypts it at the destination (e.g. speaker). This ensures that audio data is protected while in transit, even if it passes through untrusted networks [31]–[34].

Format-preserving encryption: This method encrypts audio data in a way that preserves the original format of the audio, making it possible to encrypt and decrypt audio data without changing its format [35]–[38].

Encrypted audio streaming: This method encrypts audio data in real-time as it is being streamed from a source to a destination [39]. This is particularly useful for VoIP and other real-time audio communication applications.

Steganography: This method involves hiding audio data within another media file, such as an image or video file, to conceal its presence [40].

Digital Rights Management (DRM): This method [41] uses encryption to control the access and distribution of digital media, including audio. DRM systems often use a combination of encryption and digital signatures to enforce copyright and usage restrictions on audio data.

These are some of the existing methods for audio encryption. The choice of a particular method depends on the specific requirements and constraints of the audio encryption system.

2.3 DNA Encryption

DNA encryption is a novel approach to secure storage and communication of digital data, where data is encrypted and stored in the form of DNA sequences. The use of DNA as a data storage medium has been widely studied in recent years, but its application to encryption is still in its early stages. In this literature review, we will explore the recent advancements in DNA encryption and the challenges that still need to be addressed.

One of the key benefits of DNA encryption is its large storage capacity. DNA has a storage density that is orders of magnitude greater than conventional storage media, such as hard drives or solid-state drives. This makes DNA encryption an attractive solution for storing large amounts of data, especially for long-term archival purposes. In addition, DNA has error correction capabilities that can help to ensure the reliability of stored data over long periods of time.

Several methods for DNA encryption have been proposed in recent years. One of the most popular methods is the use of DNA code words, where each symbol in the encrypted data is represented by a specific DNA sequence (Kim et al., 2017) [42]. Another method is the use of DNA code conversion, where the encrypted data is represented by a sequence of nucleotides that is different from the original DNA sequence (Kang et al., 2016) [43]. A third method is the use of DNA cryptography, which involves the use of cryptographic algorithms to encrypt data before it is stored in DNA (Rani, 2018) [44].

Biswas et al. [45] proposed a technique for DNA cryptography based on dynamic mechanisms i.e. 'dynamic sequence table' and 'dynamic DNA encoding'. Here, the way of encryption is: to transform the plaintext into DNA bases, to assign them w.r.t. ASCII characters using dynamic sequence table, to divide these data into a finite number of chunks, to encrypt them using an asymmetric cryptosystem, and lastly to merge the ciphertext of chunks through dynamic DNA encoding.

Biswas et al. [46] proposed a new DNA cryptographic technique based on dynamic DNA encoding and asymmetric cryptosystem to increase the level of secrecy of data. The key idea is: to split the plaintext into fixed sized chunks, to encrypt each chunk using asymmetric cryptosystem and finally to merge the ciphertext of each chunk using dynamic DNA encoding.

Despite the many benefits of DNA encryption, there are still several challenges that need to be addressed. One of the major challenges is the cost of DNA synthesis and sequencing, which is still much higher than the cost of conventional storage media. Another challenge is the speed of DNA sequencing, which is still much slower than the speed of conventional storage and retrieval operations. Finally, there is a need for standardized protocols and data formats for DNA encryption, to ensure interoperability between different systems.

These proposed methods and techniques are not applied on audio signal. Therefore, the effect and application on audio data of above works are still unknown and left as future works.

2.4 DNA Encryption on Audio

There have been several studies that have explored the feasibility and performance of DNA encryption for audio data. For example, Zhang et al. [47] proposed a DNA encryption algorithm for audio signals, which uses a combination of chaotic systems and DNA encoding to securely encrypt audio data. The algorithm was evaluated using a set of test audio signals, and the results showed that the encrypted audio data was highly secure and resistant to attacks.

Another study by Wang et al. [48] investigated the use of DNA encryption for audio watermarking, which is a technique for embedding a digital watermark into an audio signal for the purpose of copyright protection. The authors proposed a DNA-based audio watermarking scheme, which was able to effectively embed a watermark into an audio signal while maintaining the original quality of the audio.

X. Wang et al. [21] proposed the use of chaotic systems and DNA coding to confuse and diffuse audio data. The initial value of the chaotic system is controlled by the hash value of the audio, making the chaotic trajectory unpredictable.

2.5 Conclusion

In conclusion, the literature review on DNA encryption of audio data highlights the potential of DNA encryption as a new and promising approach for securing audio data. However, it also identifies several challenges and limitations that need to be addressed in order to fully realize the potential of this technology. Considering these, we have proposed a novel DNA-based encryption and decryption (cryptosystem) on text and audio data.

CHAPTER III

Proposed Methodology

3.1 Introduction

This thesis proposed a novel technique to encrypt and decrypt text and audio data based on DNA encoding. The proposed methodology has 3 major steps:

1. Key generation
2. Encryption
3. Decryption

They are described below.

3.2 Key Generation

A key of DNA sequence is randomly generated. This key is needed to be known by both sender and receiver.

Suppose, the randomly generated key is *AATC*.

3.3 Encryption

Encryption is executed in 6 steps:

1. Binary conversion
2. DNA sequence conversion
3. Index search
4. Random sequence generation
5. Information vector generation
6. Data encryption

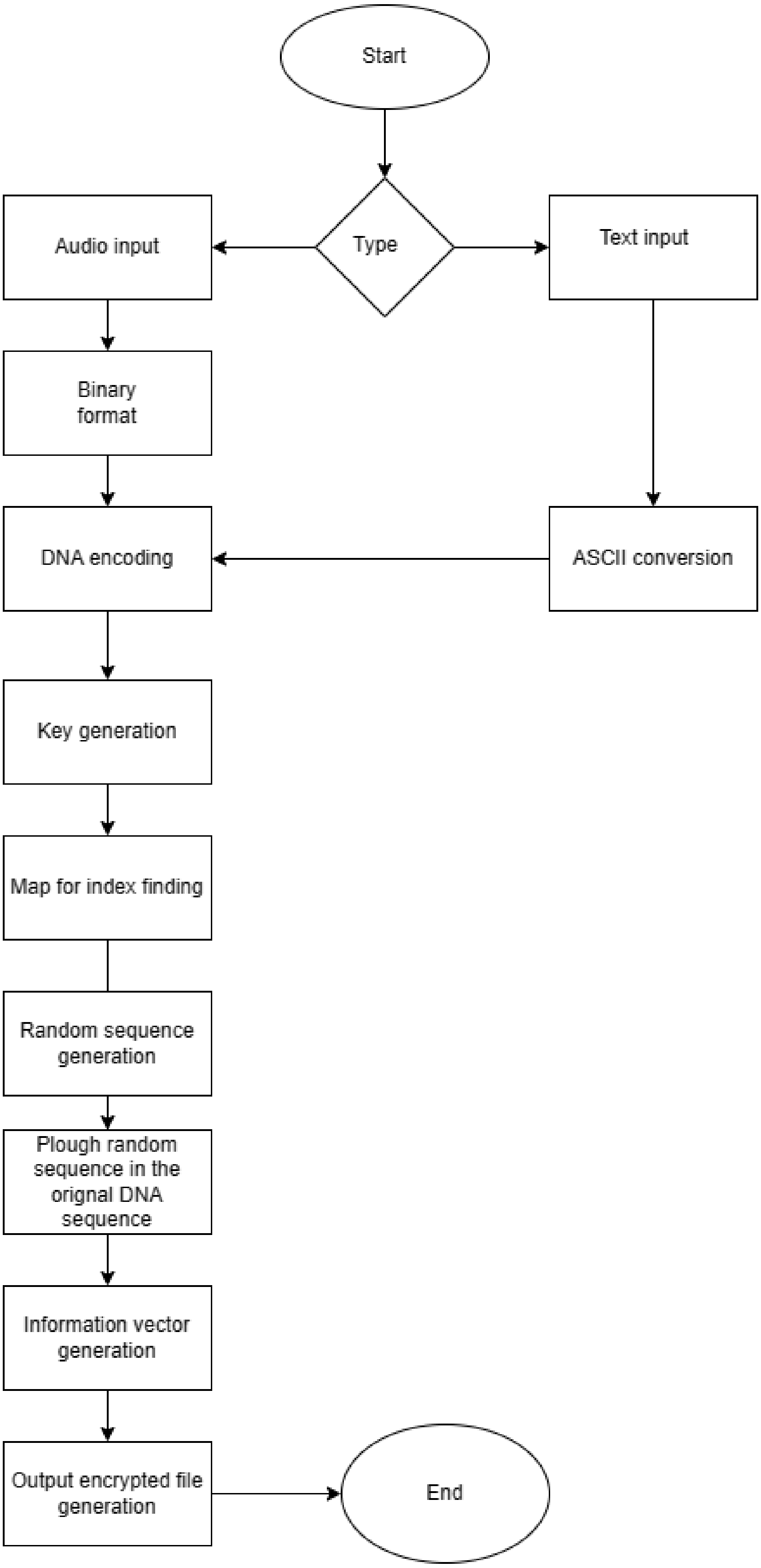
Start
Type
Audio input
Text input
Binary format
ASCII conversion
DNA encoding
Key generation
Map for index finding
Random sequence generation
Plough random sequence in the orignal DNA sequence
Information vector generation
Output encrypted file generation
End

Figure 3.1: Flowchart of encryption process

3.3.1 Binary Conversion

Firstly, the data is converted into binary format. Text data is converted into ASCII code and the audio signal is converted into digital signal. This signal is in binary format.
Suppose, an audio signal is converted into a binary data
0011001110110110011100100111001001110010011100100100101010

3.3.2 DNA sequence conversion

The digital signal is converted into DNA encoding. This conversion follows the table below:

Binary	**DNA code**
00	A
01	G
10	C
11	T

Table 3.1: Binary to DNA Encoding

The binary data converted into a DNA sequence *ATATCTGCGTACGTACGTACGTACGACCC*

3.3.3 Index searching

Index from the converted DNA sequence are chosen where the sequence from key are matched. The matching follows the pattern- *A* matches with *T* and *C* matches with *G* and vice versa. As an example, from above data, the key matches with the indexes [1, 2, 5, 9, 10, 13, 14, 17, 18, 21, 22]

3.3.4 Information vector generation

A matrix M is generated based on the position and length of random values. The first column is the position of matched indexes, after which random values are put. And the second column is the length of random values corresponding to the position of each member of column. A row from the multiplication of the matrix M and M^T is selected for using as an information vector.

$$M = \begin{bmatrix} 1 & 3 \\ 2 & 3 \\ 5 & 4 \\ 9 & 5 \\ 10 & 2 \\ 13 & 3 \\ 14 & 4 \\ 17 & 1 \\ 18 & 1 \\ 21 & 4 \\ 22 & 1 \end{bmatrix}$$

For the above example, the information vector will be

$$\begin{bmatrix} 10 & 11 & 17 & 24 & 16 & 22 & 26 & 20 & 21 & 33 & 25 \end{bmatrix}$$

3.3.5 Data encryption

Random sequences of random lengths are pushed into the DNA sequences and an encrypted sequence is generated.

Here, the encrypted sequence is-

$AT\underline{GTG}A\underline{AGA}TCT\underline{TTGT}GCGT\underline{TGAGC}A\underline{TA}CGT\underline{TGC}A\underline{GAAC}CGT\underline{C}A\underline{A}CGT\underline{TGAA}A\underline{C}CGACCC$

The underlined portions are the randomly added DNA sequences.

3.4 Decryption

For decrypting the encrypted data, it is necessary to know the key and information vector. Decryption process of encrypted data is executed in 4 steps:

1. Index matching
2. Random sequence length generation
3. Repeat step 1
4. Data decryption

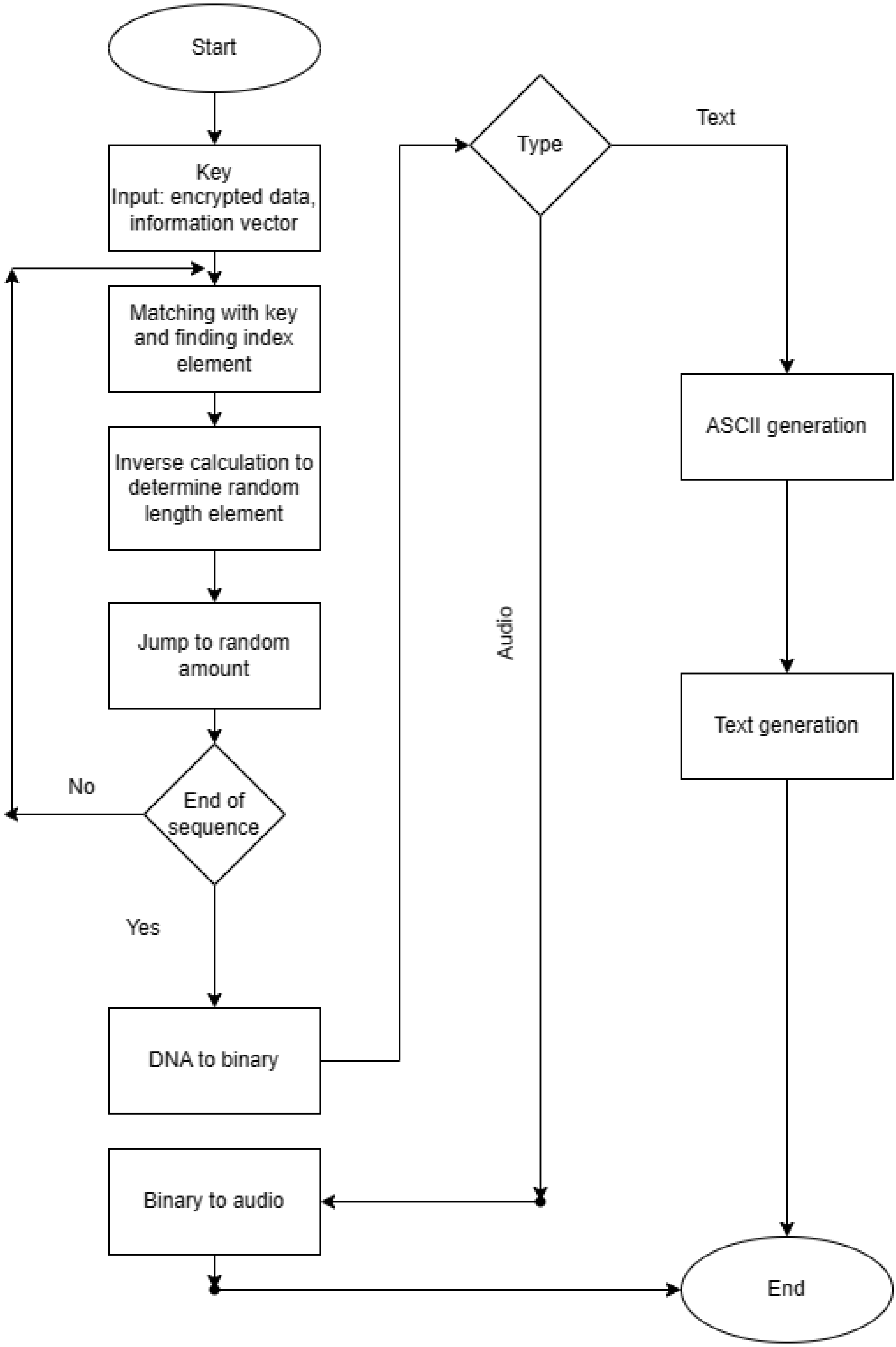

Figure 3.2: Flowchart of decryption process

3.4.1 Index matching

Let, M = $\begin{bmatrix} i_1 & i_2 & i_3 & \dots & i_n \\ r_1 & r_2 & r_3 & \dots & r_n \end{bmatrix}$, where i is the matched index and r is the length of the randomly added sequence.

From the encrypted DNA sequence, the first matched bit with key is taken.

We know,

$$M^T M[1,1] = i_1^2 + r_1^2 \tag{3.1}$$

Using this, the first value of randomly added DNA sequence's length is achieved.

3.4.2 Random sequence length calculation

$$M^T M[1,2] = i_1 * i_2 + r_1 * r_2$$

$$M^T M[1,3] = i_1 * i_3 + r_1 * r_3$$

$$\dots$$

$$M^T M[1,n] = i_1 * i_n + r_1 * r_n \tag{3.2}$$

Using this, the length of extra-added random sequence length can be calculated.

3.4.3 Repeat step 1

Step 1 is repeated to get the next matched index(i).

3.4.4 Data decryption

After getting all the i and r, we can extract the original DNA sequence removing the randomly added portion of r length in ith index of the sequence.

CHAPTER IV

Experimental Analysis

4.1 Introduction

The proposed technique was implemented practically and applied on sample data in order to measure the performance and to find the drawbacks. Different types of comparisons were done to understand its strength and drawbacks.

4.2 Experimental Setup

To evaluate the performance of the proposed technique, a prototype has been developed and analyzed in a personal computer.

Configuration of the environment: Intel(R) CoreTM i5-8265U 1.60 GHz CPU with 8 GB RAM.

Operating System: 64-bit Windows 10

Programming Language: Python

IDE: Jupyter Notebook

Frameworks: NumPy, Matplotlib, Sounddevice, PyCryptodome, ASH-crypto

Tools: Git

4.3 Result Analysis

An audio sample was used to measure the performance of this proposed thesis. The encrypted sample was unable to read. Then the decrypted file was similar to the original format.

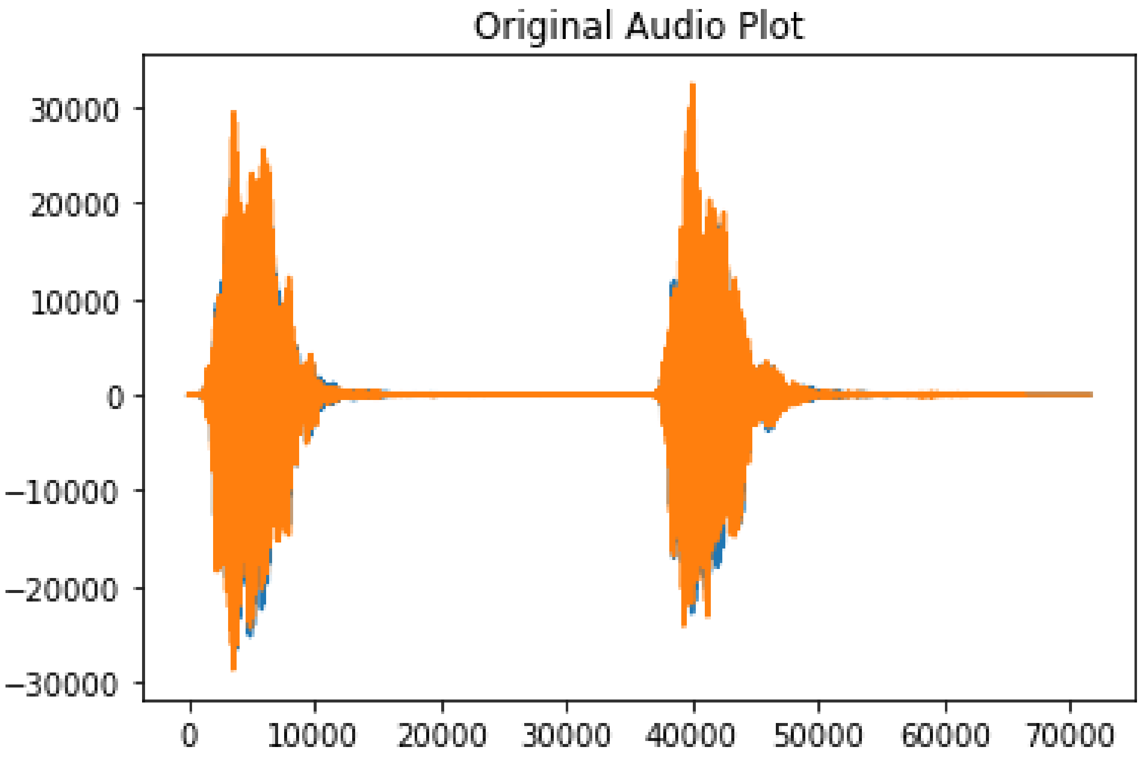

Figure 4.1: Original audio signal

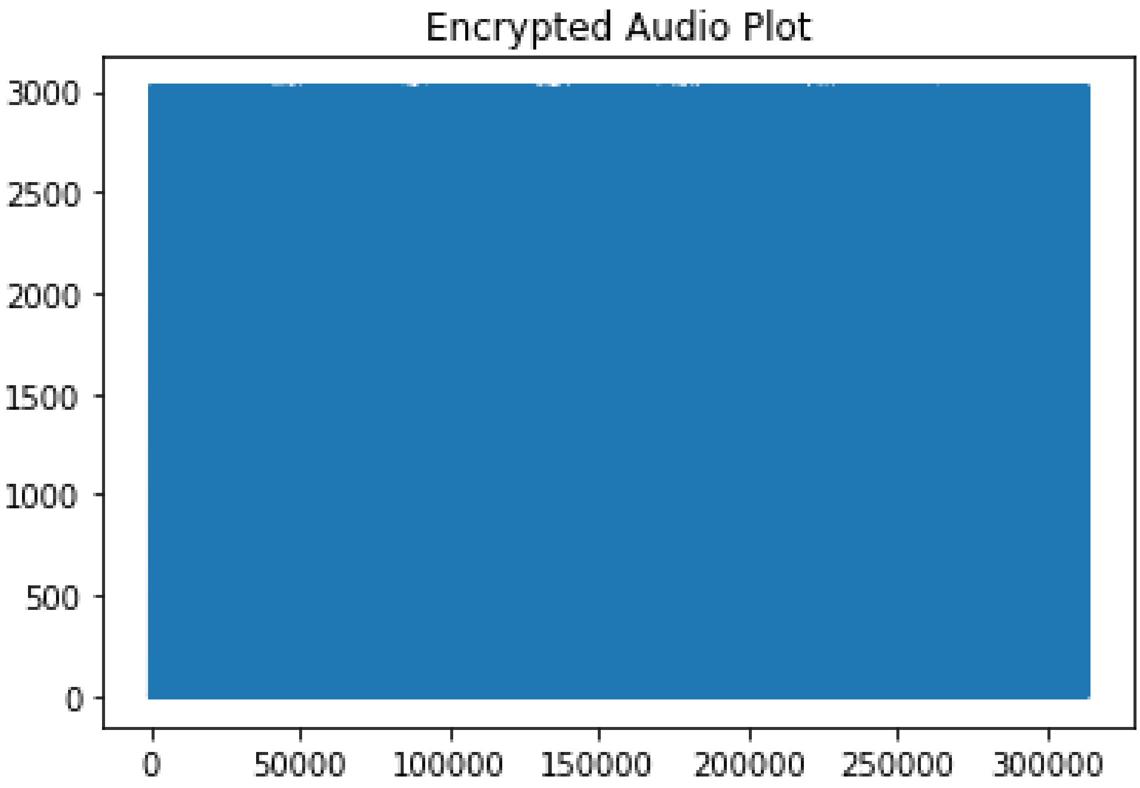

Figure 4.2: Encrypted file

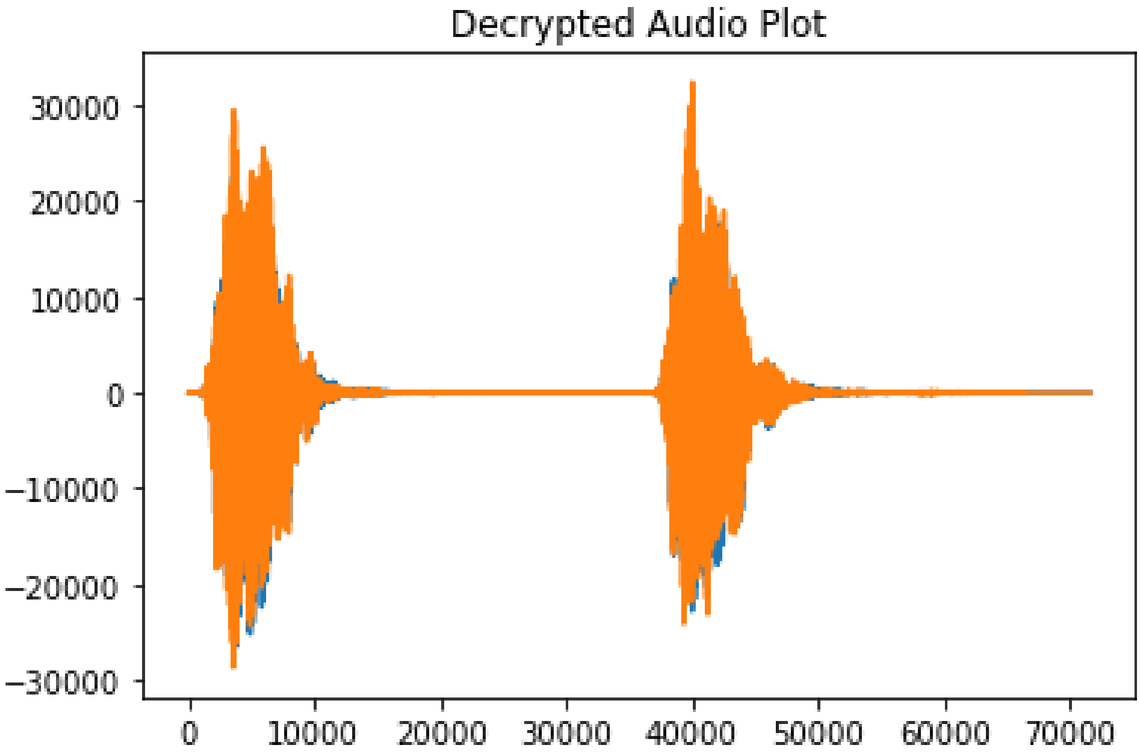

Figure 4.3: Decrypted file

For different lengths of key, it does not give drastic change in time. Time increases with key length but the difference is inconspicuous. The following table shows the time for different key lengths.

Key length	**Key**	**Time(seconds)**
10	GACCATAGGT	9.4
10	TGTACTGTTC	12
10	GCACGECAAC	8.31
15	GCAAGGGCCATCTTG	9.17
15	ACCGTCATCCAGGTA	9
15	TIGGGCCETTATTGC	9.37
20	AAGTGGCAGTTGGGACTGCG	7.92
20	CGRCGTARACTTTAACATGA	10.2
20	AATTCAATCAGAGTTGGACA	10
25	CAGACGTATACGACTACGCTATATC	8.84
25	AGTGAAGTGCGGGGAAGCCGATCTT	9
25	ATGATATGAGACAGGCGTCCGTGAG	9.9
30	CTATCGGGCTATGGATTCCAACACACCTCC	8.32
30	ACGCAGAGGTTTTCTCCGACTGGTAGAAAT	10.25
30	TACTAGGTCTGTTTGCACTCGGAGGTAAGA	9.76

Table 4.1: Time for different keylengths

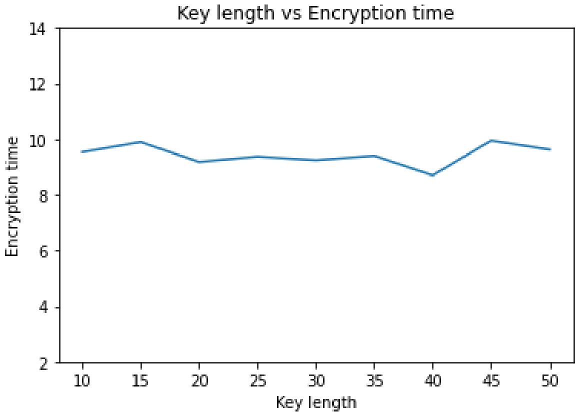

Figure 4.4: Comparison of encryption time w.r.t. keylength

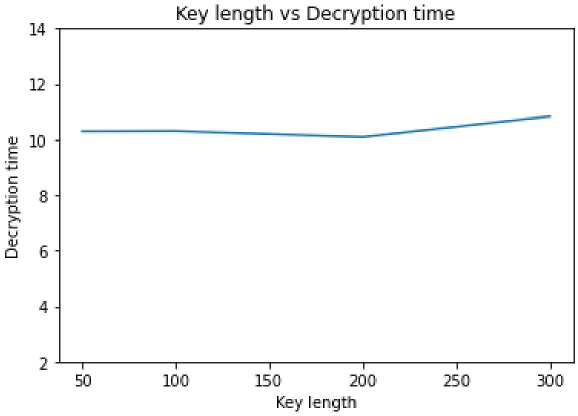

Figure 4.5: Comparison of encryption time w.r.t. keylength

The Peak Signal-to-Noise Ratio (PSNR) is a commonly used metric to evaluate the quality of audio compression or transmission, or image and video compression. The PSNR value is expressed in decibels (dB).

There is no standard PSNR value that applies to all cases. The PSNR value depends on the specific audio, image, or video signals being processed and the compression or transmission methods used. In general, a higher PSNR value indicates better quality and a lower PSNR value indicates lower quality.

A PSNR value of about 30 dB is often considered the minimum acceptable quality for audio signals, while a PSNR value of about 40 dB is considered acceptable for image and video signals. However, these values may vary depending on the specific application and the human perception of quality.

It's important to note that PSNR is not always a perfect indicator of the perceived quality of an audio, image, or video signal. There are other metrics, such as Structural Similarity (SSIM), Mean Opinion Score (MOS), and Bit-rate, that can provide a more comprehensive evaluation of the quality.

$$Mean\ Squared\ Error(MSE) = (Original - Decrypted)^2/length\ of\ original\ data \tag{4.1}$$

$$PSNR = 10log(\frac{max(original)^2}{MSE}) \tag{4.2}$$

By add-N smoothing,

$$PSNR = 10log(\frac{max(original)^2 + length\ of\ original\ data}{MSE + length\ of\ original\ data}) \tag{4.3}$$

Using these, the data of proposed methodology are:
MSE: 286284.0
PSNR: 54.57570405193728 dB
which are comparatively satisfied.

4.4 Comparison

Comparing with traditional algorithms like RSA(Asymmetric encryption) and AES (Symmetric encryption), it is shown that this proposed methodology is slower than AES but comparatively faster than RSA.

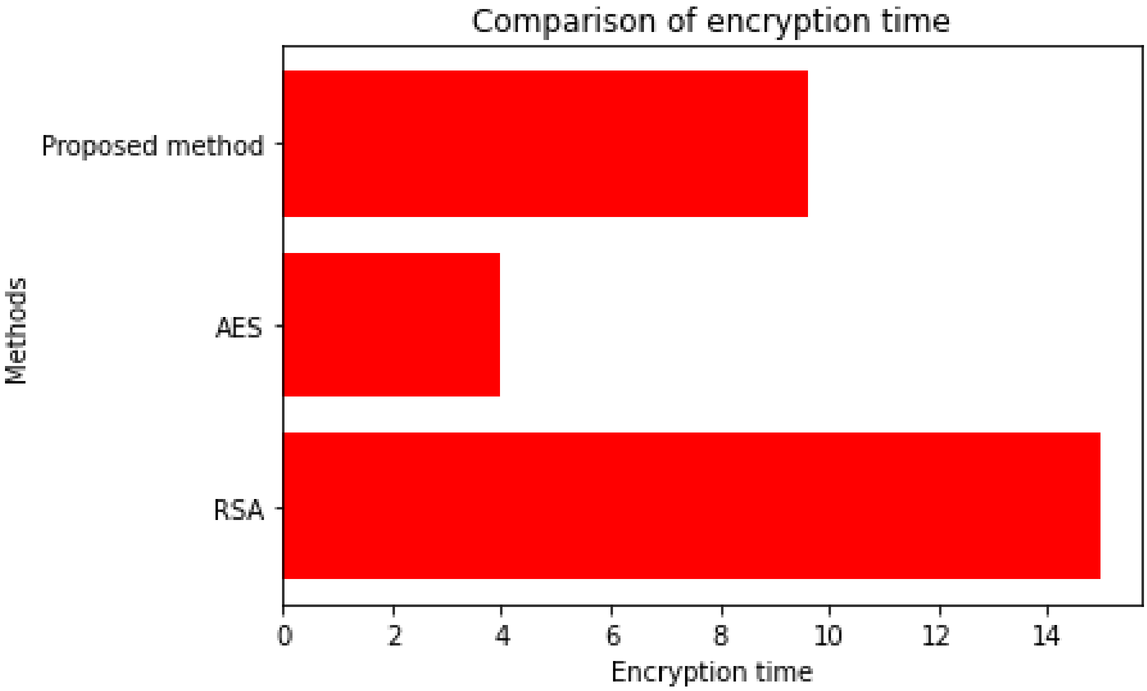

Figure 4.6: Comparison of encryption time with AES and RSA

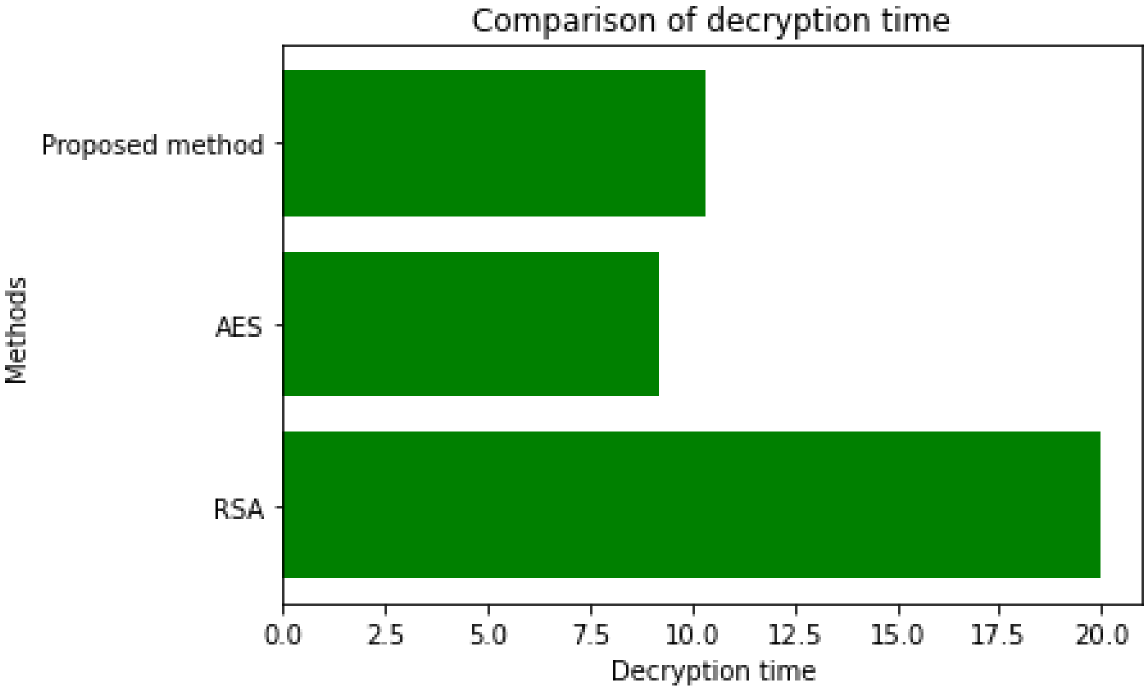

Figure 4.7: Comparison of decryption time with AES and RSA

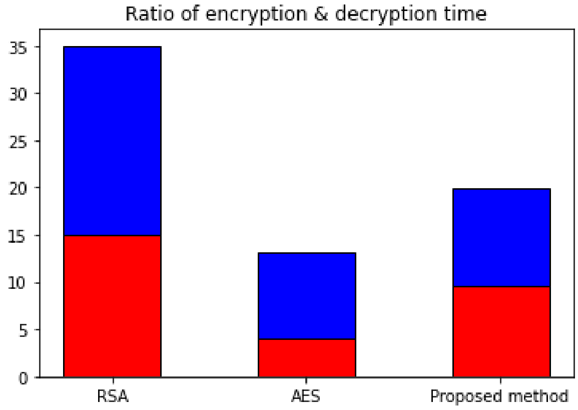

Figure 4.8: Ratio comparison of encryption and decryption time with AES and RSA

But comparing the size of the cipher file after encryption, the proposed methodology has the least size among RSA and AES.

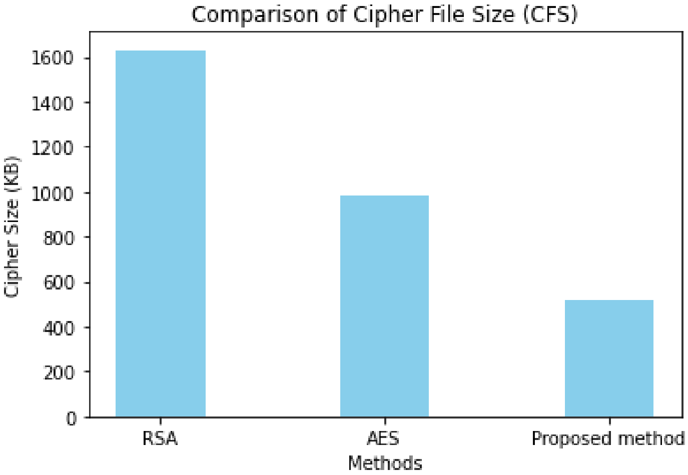

Figure 4.9: Cipher file size comparison with AES and RSA

4.5 Conclusion

The proposed methodology has worked on both text and audio data as expected. The experimental analysis is shown for mainly audio data. Proposed technique is comparatively faster and more optimized than many of the conventional algorithms in various perspectives. Though more security analysis must be executed on the proposed technique to ensure the security demands and CIA triads.

CHAPTER V

Conclusions and Future Works

5.1 Conclusion

In conclusion, the study of audio DNA encryption has provided valuable insights into the potential of using DNA as a secure storage medium for digital information. The results of this thesis show that audio data can be successfully encrypted and stored within the structure of synthetic DNA, and that the encoded information can be retrieved with high accuracy with the proposed technique.

This research demonstrates the viability of DNA as a secure storage medium, and highlights the importance of developing robust encryption algorithms for this new technology. The successful implementation of audio DNA encryption has far-reaching implications for the preservation of digital information, and could have a significant impact on the future of data storage and retrieval.

Furthermore, the results of this study have important implications for the fields of cryptography, biology, and computer science. The integration of these disciplines will be critical for the continued development of DNA-based data storage, and for ensuring its security and reliability.

In summary, the research on audio DNA encryption has shown the potential for this technology to revolutionize the way we store and preserve digital information. It is an exciting area of study that has the potential to shape the future of data storage and retrieval, and has many applications in a variety of fields.

5.2 Future work

Future work in the field of audio DNA encryption should focus on several key areas:

Algorithm optimization: Further optimization of the encryption algorithm used in this study could lead to even greater levels of security and accuracy in the encoding and decoding of audio data.

Large-scale implementation: While this study demonstrated the feasibility of audio DNA encryption on a small scale, further research is needed to demonstrate its scalability for large-scale data storage applications.

Error correction: Currently, the accuracy of the encoded audio data is subject to errors introduced during the encoding and decoding processes. Research is needed to develop error correction algorithms that can reduce or eliminate these errors.

Alternative DNA storage media: The use of synthetic DNA as a storage medium is currently limited by its cost and the need for specialized laboratory equipment. Research is needed to develop alternative DNA-based storage media that are more accessible and cost-effective.

Integration with existing storage technologies: Further work is needed to explore the integration of DNA-based storage with existing storage technologies, such as cloud storage and data centers. This will be critical for the widespread adoption of DNA-based storage and its integration into existing systems.

Security analysis: As DNA-based storage becomes more widely adopted, it will become increasingly important to analyze its security and to develop methods for protecting against potential attacks.

In conclusion, the field of audio DNA encryption has the potential to revolutionize the way we store and preserve digital information. Further research in this area will be critical for ensuring the continued development and widespread adoption of this technology.

References

[1] A. Kaur and A. Kaur, “An optimized high payload audio watermarking algorithm based on lu-factorization,” *Multimedia Systems*, vol. 24, pp. 341–353, 2018. DOI: 10.1007/s00530-017-0545-x.

[2] R. Anderson and T. Moore, “The economics of information security,” *Science*, vol. 314, pp. 610–613, 2006. DOI: 10.1126/science.1130992.

[3] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*. CRC, Boca Raton: Chapman & Hall, 2008.

[4] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the ACM*, vol. 21, pp. 120–126, 1978. DOI: 10.1145/359340.359342.

[5] M. Smid and D. Branstad, “Data encryption standard: Past and future,” *Proceedings of the IEEE*, vol. 76, no. 5, pp. 550–559, 1988. DOI: 10.1109/5.4441.

[6] W. Stallings, “The advanced encryption standard,” *Cryptologia*, vol. 26, no. 3, pp. 165–188, Jul. 2002, ISSN: 0161-1194. DOI: 10.1080/0161-110291890876. [Online]. Available: https://doi.org/10.1080/0161-110291890876.

[7] S. Mittal and J. S. Vetter, “A survey of methods for analyzing and improving gpu energy efficiency,” *ACM Comput. Surv.*, vol. 47, no. 2, Aug. 2014, ISSN: 0360-0300. DOI: 10.1145/2636342. [Online]. Available: https://doi.org/10.1145/2636342.

[8] W. Diffie and M. Hellman, “Special feature exhaustive cryptanalysis of the nbs data encryption standard,” *Computer*, vol. 10, no. 6, pp. 74–84, 1977. DOI: 10.1109/C-M.1977.217750.

[9] B. E. Kane, “A silicon-based nuclear spin quantum computer,” *Nature*, vol. 393, pp. 133–137, 1998. DOI: 10.1038/30156.

[10] E. Lucero, R. Barends, Y. Chen, *et al.*, "Computing prime factors with a josephson phase qubit quantum processor," *Nature Physics*, vol. 8, no. 10, pp. 719–723, Oct. 2012, ISSN: 1745-2481. DOI: `10.1038/nphys2385`.

[11] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, 6 Aug. 1991. DOI: `10.1103/PhysRevLett.67.661`. [Online]. Available: `https://link.aps.org/doi/10.1103/PhysRevLett.67.661`.

[12] Z. Jin and et al., "Metallized DNA nanolithography for encoding and transferring spatial information for graphene patterning," *Nature Communications*, vol. 4, p. 1663, 2013. DOI: `10.1038/ncomms2663`.

[13] K. W. Kim, V. Bocharova, J. Halamek, M. K. Oh, and E. Katz, "Steganography and encrypting based on immunochemical systems," *Biotechnology and Bioengineering*, vol. 108, pp. 1100–1107, 2011. DOI: `10.1002/bit.23038`.

[14] D. Margulies, C. E. Felder, G. Melman, and A. Shanzer, "A molecular keypad lock: a photochemical device capable of authorizing password entries," *Journal of the American Chemical Society*, vol. 129, pp. 347–354, 2007. DOI: `10.1021/ja068230r`.

[15] J. D. Watson and F. H. Crick, "Molecular structure of nucleic acids: A structure for deoxyribose nucleic acid," *Nature*, vol. 171, pp. 737–738, 1953.

[16] E. Birney and N. Goldman, "DNA storage of digital information," *Nature*, vol. 494, pp. 236–240, 2013. DOI: `10.1038/nature11875`.

[17] M. A. DePristo, E. Banks, R. Poplin, *et al.*, "Next-generation dna sequencing," *Nature Reviews Genetics*, vol. 12, no. 6, pp. 329–340, 2011.

[18] J. C. Venter, M. D. Adams, E. W. Myers, *et al.*, "Synthetic biology: A definition," *Nature Reviews Genetics*, vol. 5, no. 1, pp. 27–31, 2004.

[19] R. Kankar and D. Dhole, "A study of audio encryption techniques for secure communication," *Journal of Computer Science*, vol. 7, pp. 765–772, 2011.

[20] L. Yang and Y. Guan, "Dna cryptography: A review," *Frontiers in genetics*, vol. 8, p. 312, 2017.

[21] X. Wang and Y. Su, “An audio encryption algorithm based on dna coding and chaotic system,” *IEEE Access*, vol. 8, pp. 9260–9270, 2020. DOI: 10.1109/ACCESS.2019.2963329.

[22] Z. Al-shaer and N. Al-haj, “Dna-based data storage systems: Promises, challenges and perspectives,” *Frontiers in Bioengineering and Biotechnology*, vol. 8, p. 593, 2020.

[23] D. Alrefaei and A. Khaliq, “Securing data with dna encryption,” *International Journal of Computer Applications*, vol. 2, no. 8, pp. 35–39, 2010.

[24] F. Ullah and S. Asad, “A new encryption technique using dna sequence,” *Journal of Applied Sciences Research*, vol. 8, no. 7, pp. 3234–3240, 2012.

[25] S. H. Raza, W. Wang, and H. Wang, “Data hiding in dna: A review,” *International Journal of Computer Science and Information Security*, vol. 11, no. 2, pp. 126–133, 2013.

[26] J. Zhang and Y. Li, “A secure audio encryption scheme using chaos and singular value decomposition,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, no. 3, pp. 491–499, 2018.

[27] D. of Health and H. Services. “The health insurance portability and accountability act (hipaa).” (1996), [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-administrative-simplification-regulations/index.html.

[28] N. I. of Standards and T. (NIST), *Fips 197: Advanced encryption standard (aes)*, 2001. [Online]. Available: https://csrc.nist.gov/publications/detail/fips/197/final.

[29] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, “Twofish: A 128-bit block cipher,” in *Fast Software Encryption, 6th International Workshop*, Springer, 1999, pp. 171–182.

[30] C. Research, *Standards for Efficient Cryptography (SEC 1): Recommended Elliptic Curve Domain Parameters*. Certicom Standards for Efficient Cryptography, 2010. [Online]. Available: https://www.secg.org/sec1-v2.pdf.

[31] X. Wang, W. Zhao, and J. Wang, “A secure end-to-end audio conferencing system based on aes algorithm,” *International Journal of Computer Science and Network Security*, 2009.

[32] Y.-j. Lee and I.-h. Kim, “A study on the security of end-to-end audio streaming services,” *International Journal of Security and Its Applications*, 2011.

[33] W. Wang, X. Ma, and W. Wang, “End-to-end encryption for real-time voice communication systems,” *Journal of Network and Computer Applications*, 2012.

[34] X. Li and X. Ding, “End-to-end encryption for voice over ip communication,” *Journal of Computer Science and Technology*, 2013.

[35] P. Rogaway and M. Bellare, “Format-preserving encryption,” *Journal of Cryptology*, 2011.

[36] A. Bogdanov, D. Catalano, and G. Avoine, “Format-preserving encryption: An overview of the state-of-the-art,” *IEEE Journal of Selected Topics in Signal Processing*, 2015.

[37] D. Catalano and G. Avoine, “The security of format-preserving encryption schemes,” *IEEE Transactions on Information Forensics and Security*, 2013.

[38] T. Hamamura and T. Tsukamoto, “Format-preserving encryption for ipv6 addresses,” *IEICE Transactions on Communications*, 2015.

[39] Y.-j. Lee and I.-h. Kim, “A study on the security of end-to-end audio streaming services,” *International Journal of Security and Its Applications*, 2011.

[40] J. Wu, Y. Chen, and K. J. R. Liu, “Steganography in digital media: Concepts, attacks, and challenges,” *IEEE Transactions on Information Forensics and Security*, 2011.

[41] R. T. Chakraborty and A. Mukherjee, “Digital rights management: An overview,” *International Journal of Computer Science and Security*, 2010.

[42] J. Kim, J. Lee, D. Kim, and D. Lee, “Dna cryptography based on dna code words,” *Biosensors and Bioelectronics*, vol. 92, pp. 189–195, 2017.

[43] C. Kang, D. Kim, and D. Lee, “Dna code conversion for secure dna data storage,” *Scientific Reports*, vol. 6, p. 18 673, 2016.

[44] A. Rani, “A review on dna cryptography: A biometric approach to information security,” *International Journal of Computer Science and Mobile Computing*, vol. 7, no. 1, pp. 8–14, 2018.

[45] M. R. Biswas, K. M. R. Alam, S. Tamura, and Y. Morimoto, “A technique for dna cryptography based on dynamic mechanisms,” *Journal of Information Security and Applications*, vol. 48, p. 102 363, 2019, ISSN: 2214-2126. DOI: `https://doi.org/10.1016/j.jisa.2019.102363`. [Online]. Available: `https://www.sciencedirect.com/science/article/pii/S221421261930095X`.

[46] M. R. Biswas, K. M. R. Alam, A. Akber, and Y. Morimoto, “A dna cryptographic technique based on dynamic dna encoding and asymmetric cryptosystem,” in *2017 4th International Conference on Networking, Systems and Security (NSysS)*, 2017, pp. 1–8. DOI: `10.1109/NSYSS2.2017.8267782`.

[47] X. Zhang, Y. Wang, and J. Liu, “Dna encryption for audio signals,” in *Proceedings of the International Conference on Signal Processing*, 2009, pp. 1–4.

[48] L. Wang, X. Chen, and J. Xu, “Dna-based audio watermarking scheme,” in *Proceedings of the International Conference on Digital Signal Processing*, 2012, pp. 452–456.