A Novel Audio Steganographic Algorithm LSB based Subtraction Operation Used in Sattolo's and Crypto-algorithm

By

Name-Mohammad Fahim Muntasir

(213-44-233)

A thesis submitted in partial fulfillment of the requirement for the degree of Masters of Science in Software Engineering

Department of Software Engineering
DAFFODIL INTERNATIONAL UNIVERSITY

Fall – 2022

APPROVAL

This thesis titled on "A Novel Audio Steganographic Algorithm LSB based Subtraction Operation Used in Sattolo's and Crypto algorithm", submitted by Mohammad Fahim Muntasir, ID: 213-44-233 to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Masters of Science in Software Engineering and approval as to its style and contents.

BOARD OF EXAMINERS

Chairman

Dr. Imran Mahmud
Associate Professor and Head
Department of Software Engineering
Daffodil International University

Fazla Elahe 03.03.23

Internal Examiner 1

Dr. Md. Fazla Elahe
Assistant Professor and Associate Head
Department of Software Engineering
Daffodil International University

Internal Examiner 2

Afsana Begum
Assistant Professor
Department of Software Engineering
Daffodil International University

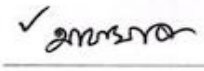
External Examiner

Dr. Md. Saiful Islam
Professor
The Institute of Information and Communication Technology (IICT)
Bangladesh University of Engineering and Technology (BUET)

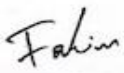
DECLARATION

This thesis was completed under the supervision of Nusrat Jahan, Associate Professor, Department of Software Engineering, Daffodil International University. It also states that neither this thesis nor any portion of it has been submitted for the granting of any degree anywhere.

Certified by:



Nusrat Jahan
Associate Professor
Department of Software Engineering
Faculty of Science & Information Technology
Daffodil International University



Mohammad Fahim Muntasir
Student ID: 213-44-233
Department of Software Engineering
Daffodil International University

ACKNOWLEDGEMENT

First and foremost, I am thankful to Almighty Allah for providing me with the chance to complete the last year. In the last one and half years of my academic life, I've learned about civility, ethics, and other topics. I am thankful to everyone. My instructors for making it possible for me to accomplish so I'd like to convey my deepest thanks to my supervisor, **Name: Nusrat Jahan**, Assistant Professor of the Software Engineering Department at Daffodil International University, for providing me with the chance and direction to accomplish my thesis on " A Novel Audio Steganographic Algorithm LSB based Subtraction Operation Used in Sattolo's and Crypto-algorithm." Under her mentorship, I was introduced to numerous new scientific methodologies and processes, for which I am forever thankful. In addition to my supervisor who has granted me permission to do my research and examination, as well as collaboration and assistance in carrying out the study.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

With the widespread use of digital communication operated by the need for ever-increasing interconnectedness and global events, the necessity for greater privacy and security during online information sharing is evident, as more enemies emerge to infringe on a fundamental human right. Cryptography and steganography have both failed to sufficiently safeguard data in transit. Audio steganography solutions have largely suffered from imperceptibility concerns, which manifest as glitches that may be heard, generating suspicion in the minds of those who are interested. This study proposes combining the two to produce a better solution that combines a unique Subtraction operation scheme with AES cryptography and LSB .wav audio steganography, which overcomes the flaws of the separate protocols and strengthens their merits. One such advantage of the suggested approach is its deep spatial analysis and high PSNR and MSE values. The finished product is capable of deception utilizing audio files, preserving secrets, and assuring private conversation.

Keywords: Subtraction, AES, Audio Steganography, Sattolo's, LSB

CHAPTER 1

INTRODUCTION

1.1 Background

In today's world, the internet's application is continuously expanding. Security on the internet and communication is one of the most essential subjects that people are interested in. Humans, being social creatures, interact with one another in all situations. Every person has their own communication style, and they sometimes want to discuss nonpublic information with the intended person [1]. But it couldn't constantly convey data or information to the specified individual while being safe and secure. As a consequence, in order to maintain genuine dialogue, data must be delivered covertly. As a consequence, data encryption is essential for two organizations to communicate safely. The most extensively used form of data encryption is cryptography. However, as we all know, depending only on encryption is risky since the presence of nonpublic information may be linked [2]. Steganography, on the other hand, uses a cover medium to hide the secret communication so that no one can see it. The fundamental benefit of Steganography rendering is that it hides the data behind a cover medium so that no one except the donor is aware of its presence. Furthermore, steganography is an important and influential approach for achieving high-level security, particularly through defeating encryption [3]. Steganography hides the fact of the message, so outsiders cannot assume communication is actually place. In this approach, data is delivered into an unanticipated channel carrying sensitive data [4].

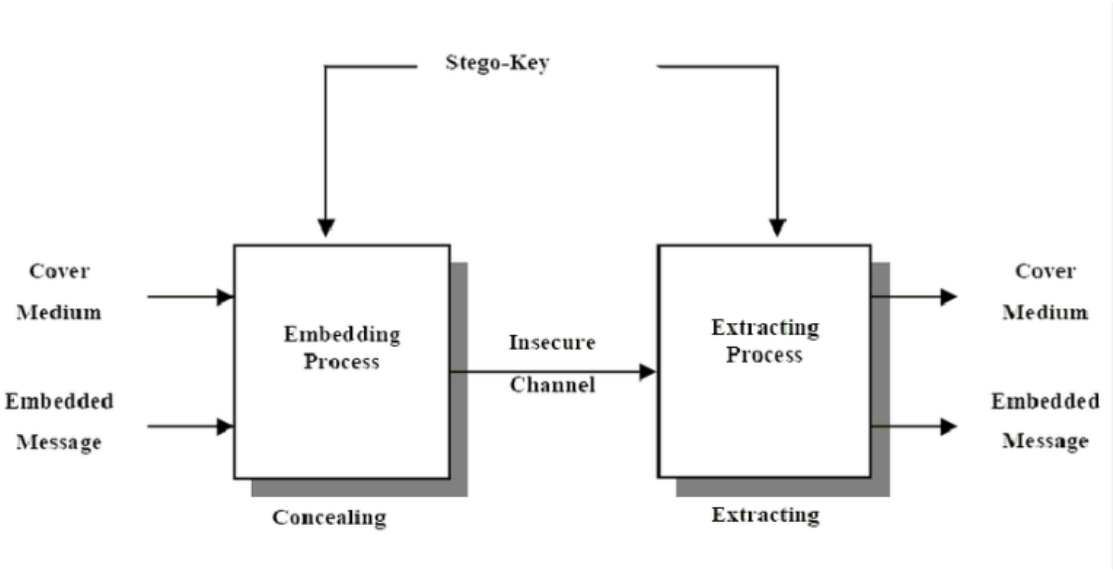


Figure 1: General Block Diagram of Steganography

Figure 1 depicts the outlines of the steganography method. Steganography can be used on a variety of different types of cover media. Steganography conceals sensitive information in carrier media such as images, sound, data, and film lines.

Figure 2: Types of Steganography

Figure 2 displays many conceivable cover mediums where steganography might be used successfully. However, the image is the widest and diversified medium for protecting educational materials. The human eye becomes more sensitive to brightness than chrominance as we age. Steganography exchanges data by taking use of the human eye's weakness in seeing image lines. Digital communication is at an all-time high, especially considering the last two years of global business and leisure operations volatility. Digital communication, particularly audio, has become the primary mode of communication in almost every aspect of life. A fundamental change can be observed as 9-to-5 jobs shift from the office to the home due to the reduction of manual jobs due to automation, and employers responding to labor market pressure to allow for work opportunities due to the increased work-life balance, time savings, and increased productivity enjoyed by many. The increased dependence on electronic communication has revealed security weaknesses and exploitative privacy practices of the common communication mediums in use [5-8]. This necessitates the development of covert secure communication that ensures user privacy and the security of their communications. Audio steganography offers itself as a viable alternative to conventional communication routes, capable of simultaneously improving consumer privacy and security by obfuscating the concealed message in the vast audio material that is now accessible and being created on a daily basis. Reinsel et. Al [9] Embedding messages in audio recordings keeps clandestine conversations hidden from prying eyes except for those with access to the material. The present corpus of audio steganography research has several design and technological faults, such as insufficient testing. [10-13] With a scarcity of condign algorithms capable of safely capitalizing on the early inflow of audio content to create a channel of communication free of backdoors and

vulnerabilities [14] is the deadline for establishing a secure channel for conducting secret transactions. A solution for audio steganography that ensures privacy and data secu rity is postulated, and it is supported by thorough quantitative and qualitative investigation demonstrating its imperceptibility during transit and increased steganographic susceptibility. The proposed technique encrypts audio conveying 16-bit Unicode Transformation Format (UTF-16) encoded messages utilizing AES-128 encryption and Subtraction based LSB steganography. Figure 3 depicts the fundamental basis of AES encryption.

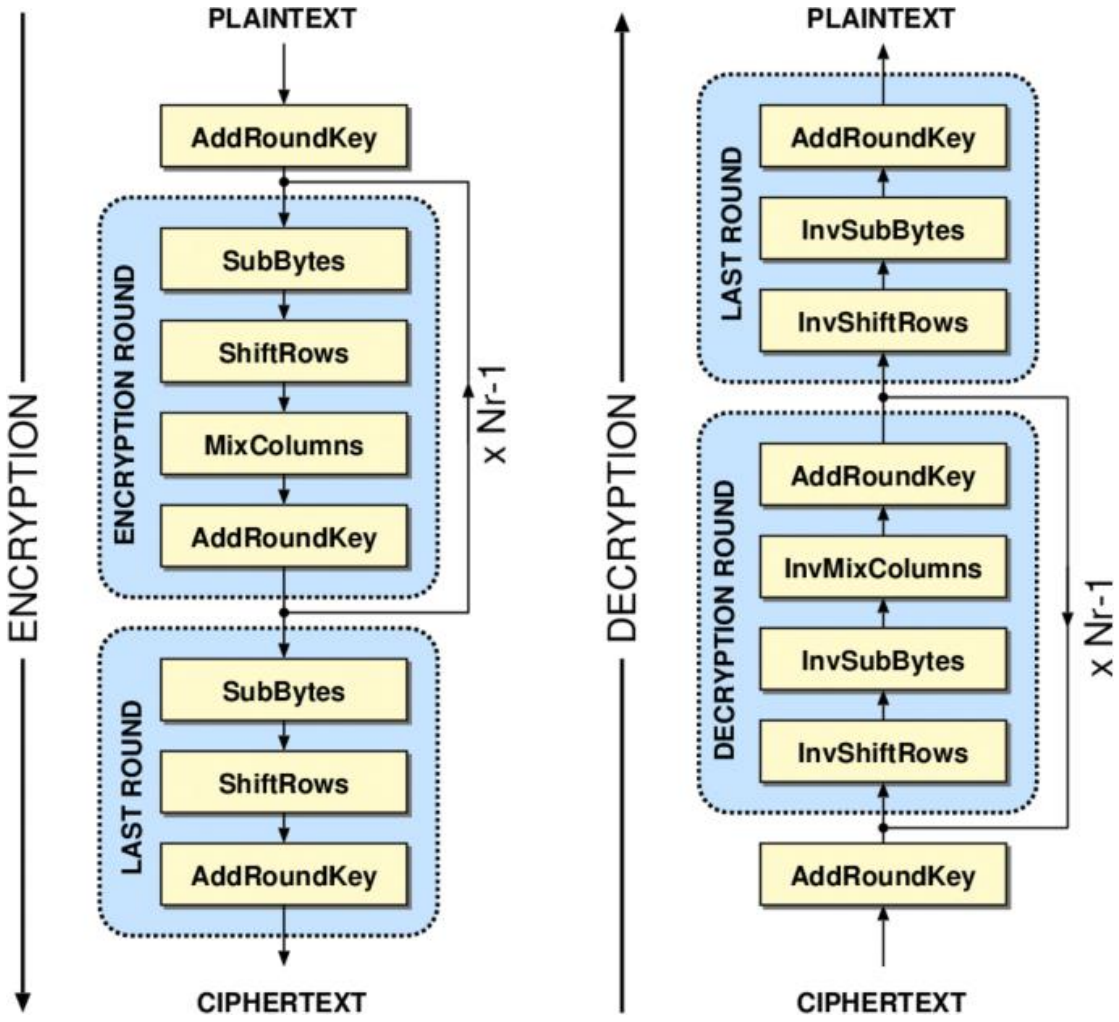


Figure 3: AES encryption

We utilize a user-defined term to qualify the typical LSB approach in this investigation. Rather than just modifying the LSB bit of an image pixel, we proposed a logical operation including a message bit and a word bit. To begin, we filter the whole image to choose the anticipated pixels for use with the steganography method. The following is the paper's main contribution.

(1) The system implements a revolutionary user-defined dynamic frame shuffle algorithm named as Sattolo's Shuffle Algorithm that varies from image to image. As a consequence, no one can know which pixels are being used to hide hidden messages.

(2) The proposed approach does not totally replace the LSB bits, but instead inserts the accompanying bit via the Subtraction operation.

(3) The system used AES cryptography before embedding the secret message in the image.

The rest of the paper is organized as follows. The second portion describes a recent steganography-related composition. The proposed algorithm is illustrated briefly in the next section. The flowchart and exemplification table are then used to show three distinct techniques for implementing the filtering, embedding, and rooting approaches. The fourth section of the report offers numerous experimental data and performance evaluation matrices used in the steganography approach. We also compared it to other methods. The article's conclusion is presented at the end.

1.2 Motivation of the Research

The internet has evolved in recent years into a vast technological framework for cutting-

edge industrial processes. Colorful organizations have lately moved away from organizing software and toward web hosting. They've supplied their services to internet visitors and druggies getting data via those web operations, and in order to identify the druggies of a certain association, they've used the word-based authentication approach, which is now handicapped. Interferers have devised a number of techniques for circumventing authentication systems, which may result in confidential data loss, abuse, or theft. The primary push for designing a security approach that would give a redundant sub caste in an authentication system is audio steganography, which is difficult to expose and may narrow the gap of frame selection.

1.3 Problem Statement

While going to review a being primary data was collected, it was noted that different investigators have offered steganography and cryptography together through validation, but in steganography, they've used quintessential frame feature selection algorithms that are easy to detect and particular behaviour may recognize the existence data using reliable findings, and in cryptography, they've used hash functions like MD5, SHA-0, BASE64, SHA-1 that have some weaknesses that can be broken by rainbow table attack.

1.4 Research Questions

1. Question 1: How does the planned enhanced data hiding model operative?
2. Question 2: How the applied authentication technique produce better results as compared to other authentication techniques?

1.5 Research Objectives

- To successfully propose an enhanced LSB audio steganography technique employing a dynamic frame filtering algorithm in a WAV audio file.
- To evaluate the effectiveness of the proposed methodology, the results were compared and analyzed with those of the existing model.

1.6 Research Scope

Authentication is a crucial component of security to prevent hacker breaches, especially in fields that offer online assistance to drug addicts. It is essential to keep enhancing protective measures in this area given the rise in assaults on authentication systems in recent years. Thus, it is essential to look into innovative approaches to improve authentication and stop unwanted access in order to protect user security and privacy. By doing this, we may effectively lower the possibility of security lapses and guard against the compromise of important data.

1.7 Thesis Organization

In this inquiry, the IEEE representation system is used. The article is broken down into five chapters, which are addressed more below.

Chapter 1 describes the exploration setting, provocation, problem statement, and objects.

Chapter 2 outlines affiliation work and calculating the exploration gap.

The exploration methodology and procedures described in Chapter 3 will be employed throughout the trip.

Chapter 4 compares experimental results to being techniques.

Chapter 5 discusses the research's exploratory extension and constraints, as well as the direction of the forthcoming exploration endeavor.

CHAPTER 2

LITERATURE REVIEW

While doing the investigation, there were figures of inquiry on audio steganography and cryptographic hash for authentication. The associated works are discussed further below.

Shanthakumari et al., 2021 [15] propose a modified LSBM bit extraction approach called Least Significant Bit Matching Revisited (LSBMR), which intercalates data into the audio by producing a portion of audio from the transporter media using phase-shifted discrete clips chosen pseudo randomly. The stego material cannot be recognized from the stego by aural methods; nonetheless, spectrograms of cover and stego audios are noticeably different, towards the point of being recognizable with the naked eye. The Pseudorandom Number Generator (PRNG) in use, as well as the statistical ramifications of directly embedding text into music, have not been examined. The disparity between unsecure PRNG and identifiable stego audio persists. Another research uses Taylor Series encryption to improve the security of conventional LSB steganography. Gençoglu, 2021 [16] uses a 64-bit key to encrypt plain text using a proprietary encryption algorithm based on the Taylor Series. Although the encoded audio is invisible to human hearing and resistance to different assaults has been theoretically argued for, the private encryption breaches Kerckhoffs' principles by creating security via secrecy de Kerckhoffs, 1883. The key space is 64 bits long, which

is often insufficient given the array of current machinery available for brute-forcing such passwords. Denning (2019) [17] The location and retrieval of the secondary key needed for data embedding have not been specified, which is a critical prerequisite for effective stego audio decryption. The little key space is a significant gap. In contrast to standard sequential data embedding procedures found during LSB, Aydn et al., 2020 [18] offer a color channel selection algorithm that intelligently emphasizes a certain channel in a bitmap picture for data concealing. The channels are chosen in such a way that the overall distortion of the cover picture is minimized, and the color channel is identified by a byte at the head utilized for information retrieval during the extraction phase. The majority of the published steganography protocols in the body of literature use LSB embedding methods with a 1:1 embedding ratio, which means that for every byte of secret, a byte of data is embedded into the cover. Enhanced Least Significant Bit (eLSB) tries to improve that by providing a more favorable ratio by necessitating the usage of fewer 1s and 0s in the data insertion process by searching a dictionary for regularly occurring bit spans. Jayapandiyan et al., 2020 [19] demonstrate the gains with the suggested approach; however, any robust compression technique will accomplish the same result and probably a more convincing results owing to being designed for high compression and the final solution being protean. Furthermore, compressed and encrypted data are unlikely to benefit from LSB since both, when effectively implemented and planned, are statistically random. Mukherjee et al., 2020 [20] invent an innovative LSB data embedding technique for audio steganography that attempts to denude the statistical fingerprint sown onto a cover by abandoning the trend of traditional bit flipping or matching LSB insertion practices in order to thwart steganalysis schemes, statistical or otherwise. The 50 Hz to 5000 Hz range is avoided

because the Human Auditory System (HAS) is most delicate to deformation in this range; despite this, the majority of vocal audio recordings tend to fall in this range, making clips predominantly composed of speech unsuitable for this application because the algorithm Švec and Granqvist, 2010. [21] While using four LSBs to store the indices of the Most Significant Bits (MSBs) that match the signal bit provides for a four-fold improvement in embedding capacity over a single LSB, it comes at the expense of visual quality. The difference between embedding capability and security remains unbridged. Straight LSB steganography of a secret often causes imbalances in the vessel material, which may lead to discovery, not to mention the capacity issue that all steganography systems have. Ali et al. (2018) [22] propose a model that incorporates fractal compression, LSB, and the logistic chaotic map to conceal hidden audio files under cover audio of the same bit length. The solution has been shown to be resilient in the face of statistical steganalysis; histogram discrepancies between the original and the message carrying medium are not equal, as are the fourth initial moments. The fractal encryption utilized is a lossy compression, which means that the message that goes in is fundamentally different from what comes out of the stego object, restricting the solution's routes to photos, audios, movies, and data of various kinds where data accuracy is not critical, such as sensitive papers, authentication tokens, and phrases. The compression method is famously computationally costly and has been virtually phased out of the industry. Mellin. 2021 [23] proposed a logistic map are not cryptographically safe and are vulnerable to considerable cryptanalysis. Couteau (2018) [24] There has been little mention of cutting-edge technology, and there is a significant research void. The usage of encryption for clandestine communication by these botnets across the internet for launching effective Distributed Denial of Service (DDOS) attacks

has not weathered this contemporary battery of protections. Divide-Embed-Combine Technique (DECM), a method based on LSB video steganography that leverages the Telegram app to subjugate hacked devices to execute the botnet master's bidding, is hailed as a solution by Kwak and Cho, 2021 [25]. Stegano divides a video into its components, then embeds harmful payloads within the video frames, which are then recombined into a video to be distributed through the Instant Message (IM) app. The payload is concealed in an unobtrusive movie to be processed later by the infected device, which avoids triggering any botnet detectors. A non-compressing Social Network Service (SNS) is required since messages delivered via irreversible compression to conserve space and bandwidth result in permanent loss of the payload, limiting the number of SNSes that may be utilized. There is currently a research gap on whether the process can be used to other protocols such as cloud file sharing and e-mail. Bazyar and Sudirman (2015) [10] attempt to improve the concealing capability of audio LSB steganography by changing additional bits, 7 to 4 LSBs of a cover sample depending on the first two MSB values. The audio encoder used has not been released, and it is unknown how this approach outperforms conventional LSB analogues, since flipping bits up to the 7th LSB would be damaging to the secrecy at bigger payload sizes. The experimental data is confined to audio recordings ranging in duration from 2 to 8 seconds, which is inadequate to determine if the procedure is practicable at longer lengths. Large recordings have not been tested, resulting in a research gap. Tayel et al. (2016) [26] offerd a hardware implementation of the 4-bit LSB audio steganography protocol utilizing two Arduino devices. Spectroscopy photos show significant differences between the cover and stego audio, with 4 bits of the available 8 bits modified, leading in 50% data loss of the reference audio. Future researchers can fill a

gap by reducing data loss. To provide invisibility, resilience, and capacity, a PRNG is utilized to encrypt the secret message before concealing it in the amplitude of WAVform (WAV) audio. To enable statistical steganalytical resistance, the sample zones are chosen at random. These accomplishments are offset by the hazy encryption technique and the corresponding random number generator. The embedding' durability has not been shown by bombarding the final output with distortion, compression, and noise assaults. Mingguang and Zhitang, 2014 [27] The scarcity of highly secure steganography solutions creates a gap that must be filled. To reconcile LSB approaches' inherent tendency to contribute to fragile data insertion persuasions, Gopalan and Fu (2015) [28] propose a flexible LSB approach that can be made more robust by trading payload capacity; information is obfuscated into higher MSBs to make the stego more robust against various types of attacks, and the higher cost of imperceptibility is offset by the aforementioned immolation. Along with sonographic comparisons, random data inserted into audio produces excellent results in Modified Bark Special Distortion (MBSD) and Perceptual Evaluation of Speech Quality (PESQ) tests. Practical protests against the assaults have yet to take place. Bhalde (2016) [29] develops an audio steganography approach that leverages Message Digest 5 (MD5) for data encryption before injecting the payload into the cover by inverting the audio sample's LSBs to match the message bit with the parity bit. The parity bit is subsequently read during the extraction procedure to reconstruct the secret. The erroneous choice of a one-way hash method for encryption, along with the faulty MD5, renders the proposal unfit for any serious security consideration. Few researchers [30-31, 48] describe a method that conceals sensitive data in the bits between the crests and troughs of a sound wave to safeguard sensitive data concealed in audio. An operation that reduces the cover LSB

for 0s and increases it for 1s, with the output being equal to the HAS. With that said, the password is encoded in the cover audio, implying that a determined attacker might decrypt the concealed message if they discovered it. The key exchange is accomplished by having the receiver send an audio recording that has been treated with "known transformations," which, when combined with the unmentioned password generator, does not inspire trust by breaching Kerckhoffs' desideratum de Kerckhoffs, 1883. The final output's resilience has been stated without any testing. Hashim et al. (2018) [32] propose a bit index volition table that deviates from the traditional steganography approach of LSB embedding. Data is contained in one of four LSBs dependent on the permutation of the first two MSBs, with Advanced Encryption Standard (AES)-256 encryption put on at the algorithm's inception for greater data security. Spectrogram pictures for the final three LSBs show no visual alterations; nevertheless, the secret key exchange procedure for symmetrical encryption is unknown, and the bit modification cut-off point of 4 of 8 bits might result in motley colored audio spectrograms. By switching audio channels mid-embedding, a concealing method hides Blowfish encrypted text data in a stereo recording using LSB, yielding information carrying stego with no tonal trace of manipulation. Hemeida et. al. 2019 [33] Because of the 64-bit block size, the encryption utilized is deemed antiquated and does not add much to the security of the proposed method. Few papers [34-36] use AES-128 encryption before embedding to implement the standard LSB approach for audio. For optimal payload capacity and performance, the 16-bit audio samples are linearly embedded. Audio differences between the cover and stego are nonexistent, however the same cannot be said for the audio plots, since fringes surrounding the peaks are discernible after embedding when contrasted for scrutiny. Ghosh et al., 2019 [37] employ a PRNG for a

placement selection procedure that pseudo randomly diffuses the message into the resting medium to alleviate the usual limitations associated with stego protocols that adopt a linear approach to embedding into the cover materials. The PRNG Linear Feedback Shift Register (LFSR) is used to highlight the pixels in the grayscale picture for LSB to occur. The approach uses padding to transform the collection of pixels to a square matrix that maintains the image's aspect ratio. LFSRs alone are not regarded cryptographically safe, and the byzantine implementation details required for correct operation severely limit access to the solution. Few researchers [38-40] hide data using Rivest-Shamir-Adleman (RSA) encryption and basic LSB steganography. There are no visible differences between the cover and stego spectrograms, and the only apparent difference is the use of RSA encryption. Al-Juaid and Gutub, 2019 [41] use 1–3 bit LSB steganography with RSA for 16-bit security. As the cover material, wav audio is utilized. The gap is that the procedure cannot be utilized with faster symmetric cryptosystems and does not allow Arabic letters since ASCII characters are used. Rajput et al., 2017 [42] develop an effective LSB-based technique for concealing text in audio. The text is encrypted using a shared key shared by the sender and recipient. The gap is that nothing new has been offered, and the random embedding renders this and IO-bound, resulting in appalling performance.

We adopted the 1-Bit Least Significant Bit (LSB) strategy, which is a spatial domain way to embed secret data, to work out the foregoing shortcomings and flaws. Before encoding it into cover dispatch, we employed Advanced Encryption Standard (AES) data encryption with a 128-bit secret key (randomly produced by automated using c# language) to save time. As a result, a dynamic frame selection approach is used with LSB during embedding, resulting in increased performance in arbitrary permutations.

As a consequence, we selected WAV with a trendy perceptibility quality as the cover audio. Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), and Root Mean Square Error (RMSE) were also used as quality dimension criteria (RMSE).

CHAPTER 3

RESEARCH METHODOLOGY

To show the proposed paradigm, an experimental design approach was applied. In this approach, the experimental terrain has been divided into two parts: the proposed steganography model and the perpetration of the whole proposed model for the testing of its effectiveness. This study demonstrated an automated two-layered safe data concealing strategy for signal steganography using 1-bit LSB and a user-selected dynamic frame selection approach, with the encryption system and steganography perpetration detailed in detail in the following subsections.

3.1 Encrypting the Secret Message

The client simply input the secret data using our recommended tool, that quickly decodes it once entered. It is translated using AES, a widely known and secure symmetric key encryption algorithm [43] that may produce data blocks with symmetric keys of 128, 192, or 256 bits and uses the same encryption key for cracking and decrypting secret data. Nonetheless, in this investigation, a 128-bit crucial length was used to encrypt all secret information, which delivers better results quicker and uses less RAM [44]. Although a crucial length of 128 bits is unbreakable, [45] which is immediately passed from the computerizing procedure. As a result, 128-bit AES was designed to provide data privacy for everyone, regardless as to whether material was retrieved from video frames or not. The reproduction phase frequency is 10 rounds for

crucial lengths of 128 bits. SubBytes, ShiftRows, MixColumns, and AddRoundKey are the four steps of each round [46]. SubBytes is a byte negotiation mechanism that processes each byte separately before returning a new value. The S-box table and its hexadecimal logic are also used to patch the byte into another value. Each row of AES's 128-bit internal state is moved during the ShiftRows step. The MixColumns approach is necessary as long as rotation provides prolixity for the AES. The branch number ensures that any AES constant four rounds have at least 25 active S-Boxes, safeguarding the AES against difference and direct cryptanalysis. The colored rounds use a separate 128-bit round key that is calculated from the core AES key. The whole AES approach is performed using a function written in the C Sharp programming language. The cipher text is ready to be incorporated into the cover carrier once it has been encrypted in C Sharp and converted to WAV formatted audio.

3.2 Frame Filtering Algorithm

The Sattolo gyration is a system for arbitrarily rearranging an array similar that each element ends up in a different position. It makes in- place changes to the input array. However, you may change the algorithm to return the scuffled rudiments as a new array, if it isn't possible in your computer language. However, the algorithm may be changed to reiterate from left to right, If it's more accessible. As long as there are at least two factors, this assures that every element ends up in a brand-new place. Induction may be used to demonstrate that Sattolo's system always yields a cycle of length. Assume by induction that the remaining duplications of the circle permute the first n- 1 particulars according to a cycle of length n- 1 (those remaining duplications are just Sattolo's system applied to those first n- 1 rudiments). This indicates that after following the original element towards its new position p, the element originally at position p to its

new part, and so on, one can only return to the morning position after visiting all other positions. Assume the first replication shifted the final element with the bone at(non-final) position k, and the following permutation of the first n- 1 element moved it to position l; we compare the permutation of all n rudiments with the remaining permutation of the first n- 1 element. When tracing successive places, there's no difference between and until you reach position k. The element originally in position k is also moved to position l rather than region k, while the element originally in position l is moved to position l. The series of places for also follows the race for, and all positions are visited before returning to the morning position, as necessary. Concerning the invariant chances of commodity like the permutations, it's sufficient to note that the modified algorithm involves (n- 1)! distinct possible sequences of arbitrary figures produced, each of which easily produces a different permutation and each of which occurs with equal probability (assuming the arbitrary number source is unprejudiced). The (n- 1)! distinct permutations exactly exhaust the set of cycles of length n each similar cycle has a unique cycle memorandum with the value n in the last place, allowing for (n- 1)! permutations of the other values to fill the remaining positions of the cycle title.

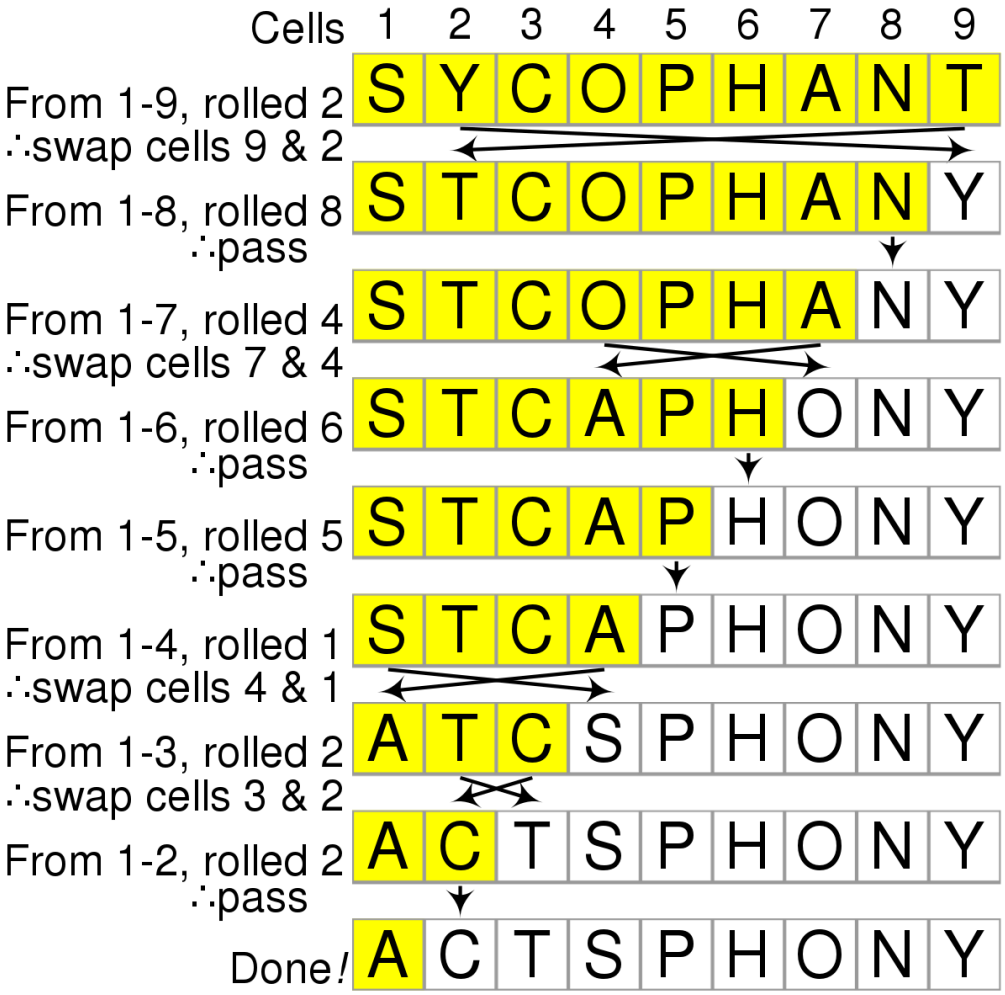


Figure 4: Sattolo Shuffle

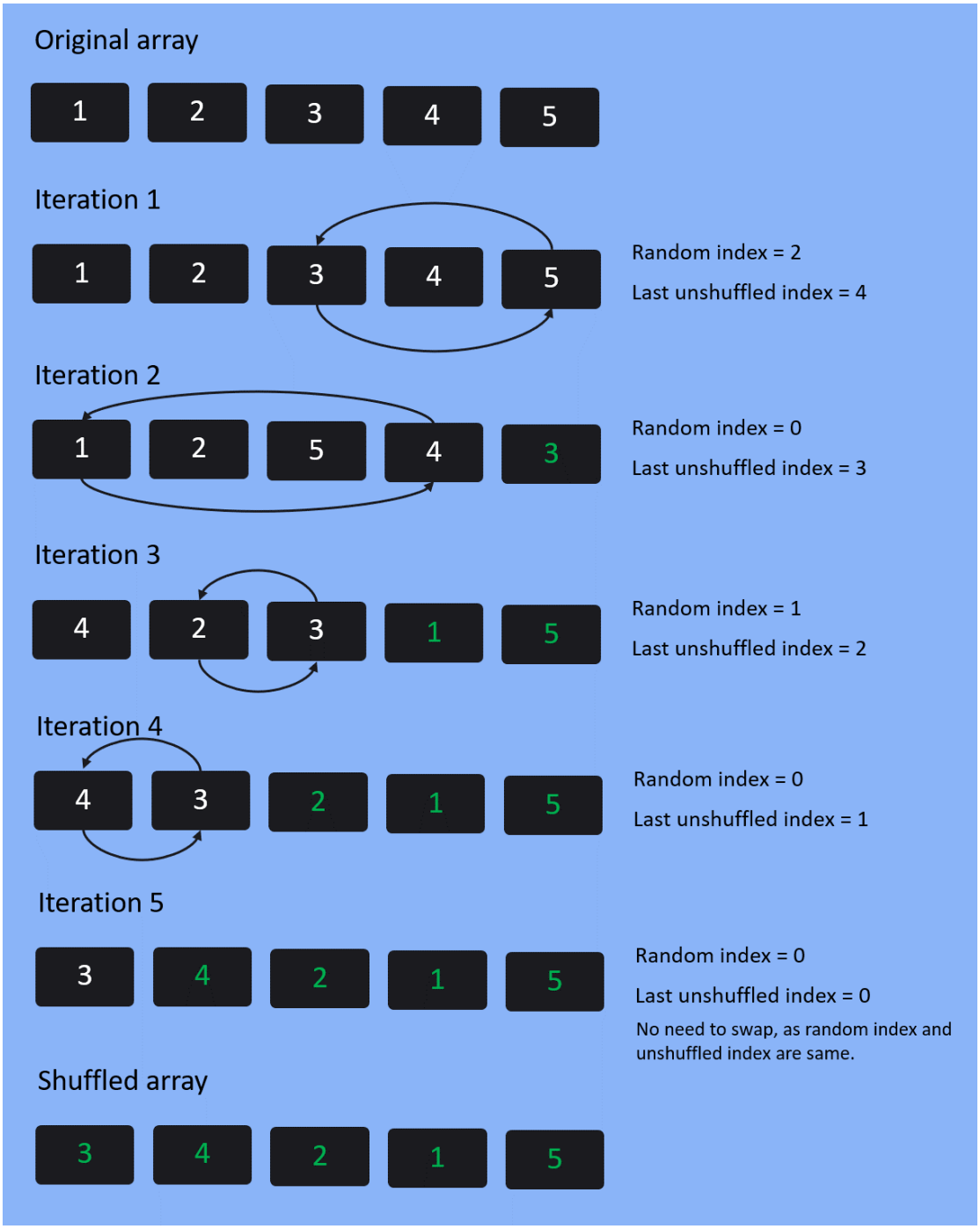


Figure 5: Frame Shuffling.

3.3 Steganographic Process

The steganographic process is divided into two corridors: The Embedding approach and another called the Retrieve approach. Figure 6 depicts the proposed system's embedding process, which takes secret plain text from the stoner and encrypts the communication with a 128-bit AES algorithm. The images are uprooted from the cover carrier in the second phase, and the pixel selection system then interacts with the aforementioned systems. The encoded secret message will be converted into 8-bit binary data and embedded with 1 bit LSB position of filtered pixels via subtraction operation in the third phase. In this case, subtraction will be used with the secret message bit and the sixth indexed bit, and the last indexed to RGB blocks will be replaced. Figure 7 depicts the retrieval procedure. To retrieve secret data, you must first understand the metadata, which includes the secret message embedding key, message size, and pixel filtering algorithm, which will store the fixed four pixels using Equation.

$$\text{1st-frame position (X1, Y1)} = (W - W, 1) \tag{1}$$

$$\text{2nd- frame position (X2, Y2)} = (W - W, 2) \tag{2}$$

$$\text{3rd- frame position (X3, Y3)} = (W - W + 1, 1) \tag{3}$$

$$\text{4th- frame position (X4, Y4)} = (W - W + 1, 2) \tag{4}$$

Those frames are used to record information that is utilized to extract the AES key and message size, as well as the filtering frames method. Knowing the filtering method will allow our system to get filtering frames where the secret message bit is stored in the embedding approach. Then, to get the secret message bit, we will do a subtraction operation with the 6th and 7th indexed bit for frame blocks. After obtaining the bits

depending on message size, we may decode the secret message using the AES key and get the required plain text that was hidden.

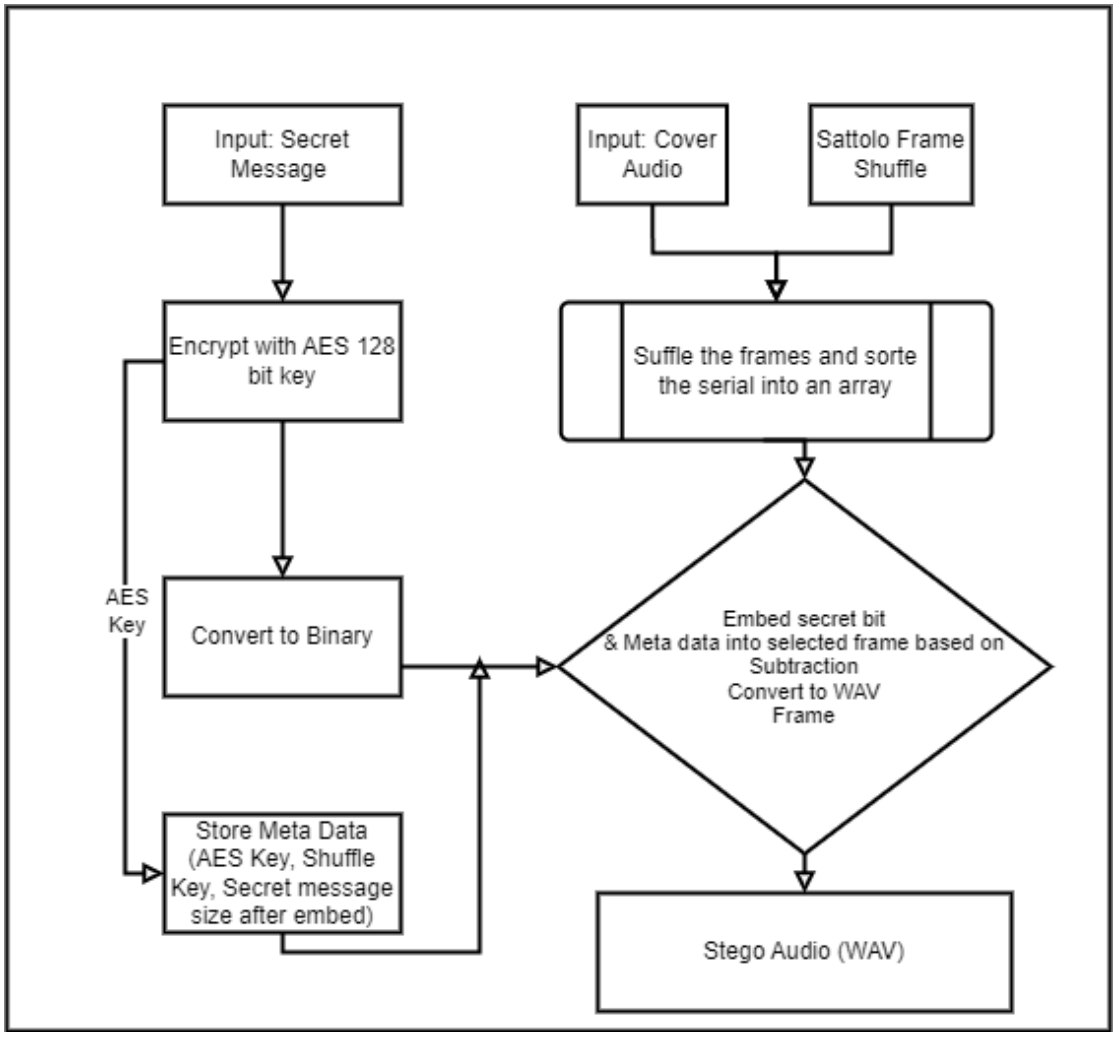


Figure 6: Embedding Process

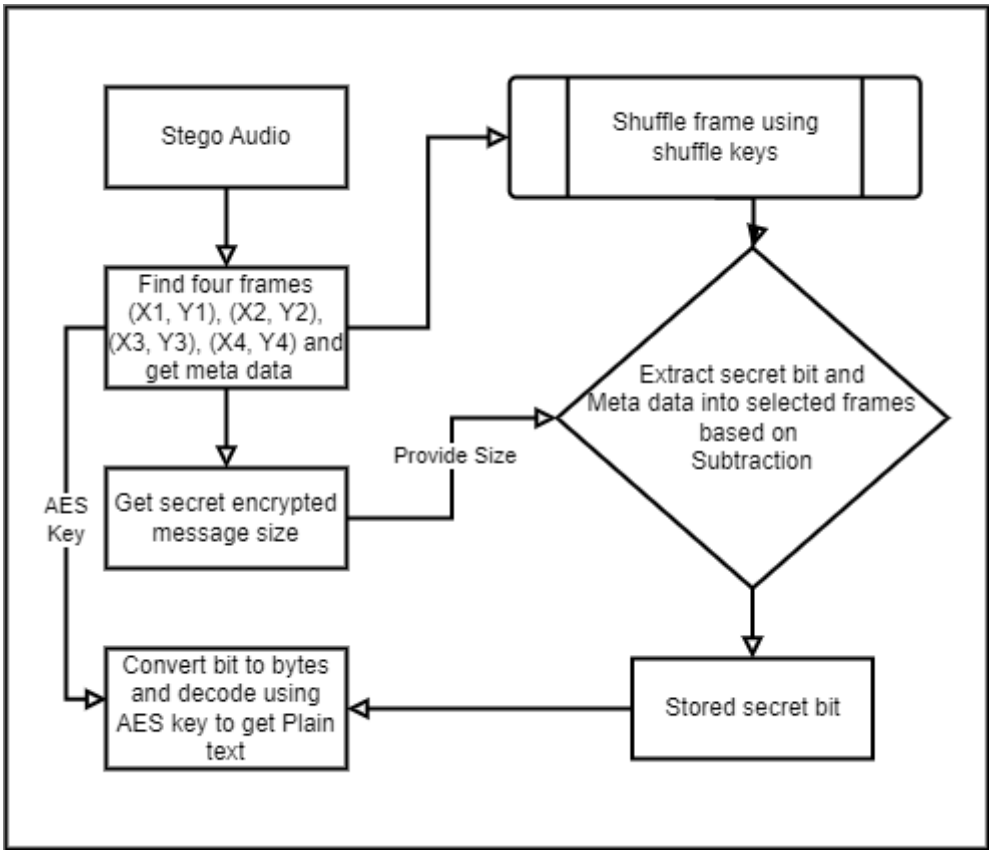


Figure 7: Retrieving Process

3.4 Algorithm for embedding and retrieving

The user must submit a secret message, cover picture, and frames filtering method throughout the embedding procedure. The machine will then initially load the specified information into memory. Second, the AES key is produced at random using 128 bits. The system, on the other hand, will begin filtering frames based on the frames filtering algorithm and saving them in a frames list for use in the embedding process. These frames are used to hide secret bits from the encoded message that was transformed by the AES key. The retrieving procedure, on the other hand, is the inverse of the embedding process.

Embedding Algorithm:

Result: Stego Audio

$S_m \leftarrow$ input

$C_I \leftarrow$ input

$F_A \leftarrow$ input

E_K = AESKey();

ES_m = AESEncryption(S_m, E_K);

Filteredframes[] = F_{XB}(Fxr(X, Y))[0][1](C_I);

M_D = F_{XB}(E_K+F_A+Size(ES_m));

(x1, y1), (x2, y2), (x3, y3), (x4, y4) $\leftarrow M_D$

S_{MB} = F_{XB}(ES_m);

For a ≤ Filteredframes[]

FV = Read(FilteredFrames[n]);

embedLSBSubtraction(FrameValue, S_{MB})

UpdatedFrameValue();

End For

Retrieving Algorithm

Result: Secret Message

$S_I \leftarrow$ input

$M_D \leftarrow$ (x1, y1), (x2, y2), (x3, y3), (x4, y4)

Filteredframes[] = Fx(M_D,S_I);

M_S = M_D[Size(ES_m)]

For a ≤ Filteredframes[]

SecretBit[] = retrieveLSBSubtraction(FrameValue, S_{MB})

if(SecretBit[] >= M_S)

Break;

End For

encryptedMessage = BitToBytes(SecretBit[])

Plaintext = Decode(encryptedMessage, Key)

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Result Discussion

The effects are demonstrated in this part by visual explanation and assessment of the cover and stego picture. In addition, the proposed system's findings are linked to other well-known steganographic systems to demonstrate its efficacy. The statistical disquisition of the research is well-appointed with six quality dimension criteria such as Peak Signal-to-Noise Ratio (PSNR), Root Mean Square Error (RMSE), and Mean-Square Error (MSE).

Figure 8 shows three photographs chosen for the experimental test (Audio 1, Audio 2, and Audio 3). The three audios are in WAV format and have various length. The suggested approach is implemented using the.NET Framework version 4.8, which is a C Sharp language framework.

		
Audio 1	Audio 2	Audio 3

Figure 8: Cover Audios

The scientific illustrations for the stated three quality measure matrices (i.e., PSNR, RMSE, and MSE) are shown in Eqs. 7 to 9, which are often used envoys to quantify the efficacy and safety of the steganographic activity.

The Mathematical illustration for PSNR is [38]

$$PSNR = 10\log_{10}\frac{255^2}{MSE}\text{dB} \tag{7}$$

Formerly the unit of PSNR is dB which depends on MSE. Several types of exploration prove that if the value of PSNR between cover and stego frame comes to more than 40 dB also it's considered respectable.

The Mathematical definition for MSE and RMSE [39, 40]

To find the MSE, take the observed value, abate the prognosticated value, and forecourt that difference. Reprise that for all compliances. Also, sum all of those squared values and peak by the number of compliances.

$$\text{MSE} = \frac{1}{n}\sum_{i=1}^{n}(y_i - \tilde{y}_i)^2 \tag{8}$$

$$RMSE = \sqrt{\sum_{i=1}^{n}\frac{(\hat{y}_i - y_i)^2}{n}} \tag{9}$$

The suggested system's output is limited to a 15 Kilobyte payload on the specified four videotape frames. The findings of PSNR commitment to improving matrix for specified frames are shown in Table I. Then, for Audio 1, Audio 2, and Audio 3, same length (33Sec) frames were used with a payload of 15 Kilobytes or 15000 bytes, and also to bed all secret data, the current proposal was capable of hiding 66997 bytes for different audio gradationally, but it was observed that the frames of Audio 3 achieved slightly higher PSNR values than other named images.

TABLE I. Quality measurement metrics of the projected method

Audio	Length	Sample Rate(Hz)	Dimension (Frame in Each Ch.)	Payload	PSNR	MSE	RMSE
Audio 1	33 Sec	8000	268237 X 2	512 Bytes	120.566416696623	0.00381192751186451	0.0617408091286833
	33 Sec	8000	268237 X 2	256 Bytes	123.989483893395	0.00200009692920813	0.0447224432383577
	33 Sec	8000	268237 X 2	128 Bytes	126.750629826533	0.00092828357012 6418	0.0304677463906738
Audio 2	33 Sec	16000	536474 X 2	512 Bytes	124.521939333959	0.00185936317510261	0.0431203336617728
	33 Sec	16000	536474 X 2	256 Bytes	127.338054573517	0.00091803144234 3897	0.0302990336866359
	33 Sec	16000	536474 X 2	128 Bytes	130.07253976272	0.00048464604062825	0.0220146778452071
Audio 3	29 Sec	44100	1306624 X 2	512 Bytes	127.461180769622	0.00077336708953 7618	0.0278094784118224
	29 Sec	44100	1306624 X 2	256 Bytes	131.157827099102	0.00038802287421 6301	0.0196982962262298
	29 Sec	44100	1306624 X 2	128 Bytes	134.086063253186	0.00019401143710815	0.0139287988393885

In this table, various sized and various dimensioned audio are tested.

TABLE 2 The comparison of three steganographic algorithms This section deals with the comparison of the proposed algorithm with the existing methods [32, 48, 41, 33]. Model 1 represents [32], Model 2 denotes [48], Model 3 represents [41], and model 4 denotes [33]. The competing solutions have been implemented in C and tested with various lengths of audio. PSNR and MSE has been use to quantify the results.

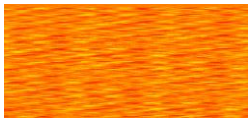
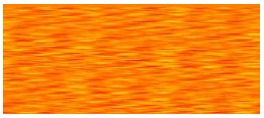
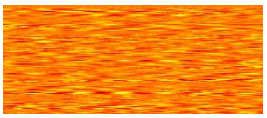
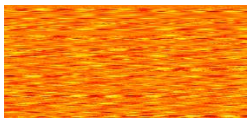
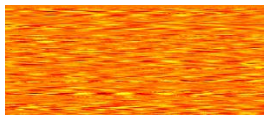
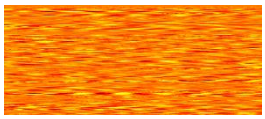
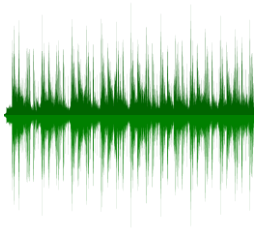
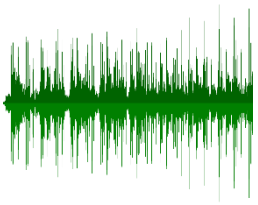
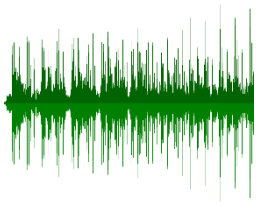
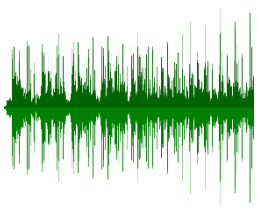
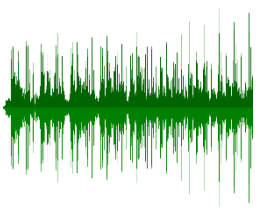
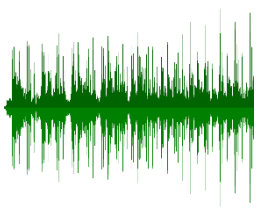
TABLE II. Comparison among recent steganographic techniques

Audio	Model	Sample Rate(Hz)	Dimension(Frame in each cha.)	Payload	PSNR
Audio 1	Model 1	8000	268237 X 2	512 Bytes	120.49049916006
	Model 2	8000	268237 X 2	512 Bytes	106.293381613029
	Model 3	8000	268237 X 2	512 Bytes	119.749292347042
	Model 4	8000	268237 X 2	512 Bytes	119.813203627201
	P-Model	8000	268237 X 2	512 Bytes	120.566416696623
Audio 2	Model 1	16000	536474 X 2	512 Bytes	123.547475084316
	Model 2	16000	536474 X 2	512 Bytes	109.399218601368
	Model 3	16000	536474 X 2	512 Bytes	122.753544228367
	Model 4	16000	536474 X 2	512 Bytes	122.822514325162
	P-Model	16000	536474 X 2	512 Bytes	124.521939333959
	Model 1	44100	1306624 X 2	512 Bytes	127.404970667935

Audio 3	Model 2	44100	1306624 X 2	512 Bytes	113.09330 4672459
	Model 3	44100	1306624 X 2	512 Bytes	126.97725 4144327
	Model 4	44100	1306624 X 2	512 Bytes	126.54062 0529766
	P-Model	44100	1306624 X 2	512 Bytes	127.46118 0769622

We can see that the performance of our proposed model is better than existing model. The Table 3. shows the pixel image for both cover and stego images for the above three images.

TABLE III. Pixel Image among recent steganographic techniques

Frames Type	Audio 1	Audio 2	Audio 3
Cover			
Stego			
Cover			
Stego			

Consistent with a result of the pixel based image, the difference between two frames is inconsequential, i.e.- these alterations cannot be predicted with bare eyes.

4.2 Implementation on Desktop App

We have implemented using c-sharp language

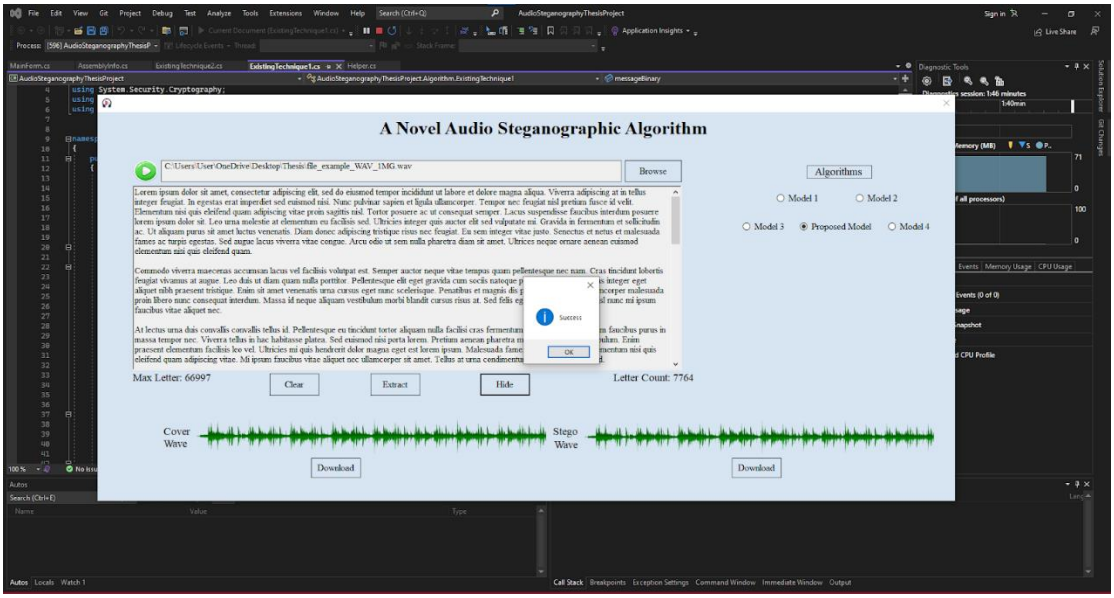


Figure 9: Desktop Application

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

This paper describes an automated this double secure data concealing approach for audio steganography that combines LSB and Subtraction with a user-selected dynamic frame selection strategy to hide the secret data in the cover audio with 128-bit AES encryption. In compared to current data concealing techniques, the overhead explanation and proper result analysis show that the proposed steganography data concealing approach provides redundant security and lowered imperceptibility.

REFERENCES

[1] Delenda, S., & Noui, L. (2018, May 4). A new steganography algorithm using polar decomposition. Information Security Journal: A Global Perspective, 27(3), 133–144.

[2] Shehzad, D., & Dag, T. (4–5 August. 2017). A novel image steganography technique based on the similarity of bits pairs. 2017 IEEE 8th Control and System Graduate Research Colloquium (ICSGRC), Shah Alam, Malaysia

[3] Tiwari, R. K., & Sahoo, G. (2011, February 11). A novel methodology for data hiding in PDF files. Information Security Journal: A Global Perspective, 20(1), 45–57.

[4] Shirafkan, M. H., Akhtarkavan, E., & Vahidi, J. (5–6 November. 2015). An image steganography scheme based on discrete wavelet transforms using lattice vector quantization and reed-Solomon encoding. 2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI), Tehran, Iran

[5] John, A. S. (2020). It's not just zoom. google meet, microsoft teams, and webex have privacy issues, too. https://www.hawaii.edu/its/wp - content/uploads/sites/2/2020/05/Google -Meet -Microsoft - Teams -Webex - Privacy - Issues -Consumer -Reports.pdf (cit. on p. 2)

[6] Khan, N. A., Brohi, S. N., & Zaman, N. (2020). Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. https://doi.org/10/gmndgs (cit. on p. 2)

[7] Wagenseil, P. (2021, August). Zoom security issues: Everything that's gone wrong (sofar). Retrieved August 30, 2021, from https://supremeacademics.com/samples/ Information%20Security%20(1).pdf. (Cit. on p. 2)

[8] Herzberg, A., Leibowitz, H., Seamons, K., Vaziripour, E., Wu, J., & Zappala, D. (2021). Secure Messaging Authentication Ceremonies Are Broken. IEEE Security Privacy, 19(2), 29–37. https://doi.org/10/gmndgr (cit. on p. 2)

[9] Reinsel, D., Gantz, J., & Rydning, J. (2017). Data age 2025: The evolution of data to lifecritical don't focus on big data; focus on the data that's big. IDC.

https://www.import.io/wp - content/ uploads/ 2017/ 04/Seagate -WP - DataAge2025 - March -2017.pdf (cit. on p. 2)

[10] Bazyar, M., & Sudirman, R. (2015). A New Method to Increase the Capacity of AudioSteganography Based on the LSB Algorithm. Jurnal Teknologi, 74(6). https://doi.org/10/gmc75v (cit. on pp. 2, 7, 17)

[11] Ing, X., Huang, W., Zhang, M., & Zhao, I. (2016). A topography structure used in audio steganography. 2016 IEEE International Conference on Acoustics, Speech and SignalProcessing (ICASSP), 2134–2138. https://doi.org/10/gmfjcb (cit. on pp. 2, 13, 17)

[12] Tayel, M., Gamal, A., & Shawky, H. (2016). A proposed implementation method of an audio steganography technique. 2016 18th International Conference on Advanced Communication Technology (ICACT), 180–184. https://doi.org/10/gmfg4s (cit. on pp. 2, 7, 17)

[13] Johri, P., Kumar, A., & Mishra, A. (2015). Review paper on text and audio steganographyusing GA. International Conference on Computing, Communication & Automation, 190–192. https://doi.org/10/gmgbxc (cit. on pp. 2, 17)

[14] Buchanan, P. B. (2019, May). A Major Backdoor in WhatsApp! Retrieved September 2,2021, from https://medium.com/asecuritysite - when- bob-met-alice/a-majorbackdoor-in-whatsapp-e15a48530f87. (Cit. on p. 2)

[15] Shanthakumari, R., Devi, E. M. R., Rajadevi, R., & Bharaneeshwar, B. (2021). Information Hiding in Audio Steganography using LSB Matching Revisited. Journal ofPhysics: Conference Series, 1911(1), 012027. https://doi.org/10/gmb8jv (cit. on pp. 4,17)

[16] Gençoglu, M. T. (2021). Enhancing The Data Security by using Audio Steganographywith Taylor Series Cryptosystem. Turkish Journal of Science and

Technology, 16(1),47–64. Retrieved July 17, 2021, from https://dergipark.org.tr/en/pub/tjst/839014(cit. on pp. 4, 17)

[17] Denning, D. E. (2019). Is Quantum Computing a Cybersecurity Threat? Although quantum computers currently don't have enough processing power to break encryption keys, future versions might. American Scientist, 107(2), 83+. Retrieved July17, 2021, from https : / / link . gale . com / apps / doc / A580224313 / AONE ? sid =googleScholar&xid=14d9f06a (cit. on p. 4)

[18] Aydın, Ö., Mesut, A. Ş., & Öztürk, E. (2020). Finding the Optimal Color Channel forInformation Hiding in LSB Insertion Method. Journal "Fundamental Sciences andApplications", 26(1), 1–5. https://journals.tplovdiv.bg/index.php/journal/article/view/175 (cit. on pp. 5, 17)

[19] Jayapandiyan, J. R., Kavitha, C., & Sakthivel, K. (2020). Enhanced Least Significant BitReplacement Algorithm in Spatial Domain of Steganography Using Character Sequence Optimization. IEEE Access, 8, 136537–136545. https://doi.org/10/gmb8js(cit. on pp. 5, 17)

[20] Mukherjee, N., Paul, G., & Saha, S. K. (2020, August). A Novel Position ConcealmentAudio Steganography in Insensible Frequency. In H. S. Behera, J. Nayak, B. Naik & D. Pelusi (Eds.), Computational Intelligence in Data Mining (pp. 383–392). Springer.https://doi.org/10/gmbv7f. (Cit. on pp. 5, 17)

[21] Švec, J. G., & Granqvist, S. (2010). Guidelines for Selecting Microphones for HumanVoice Production Research. American Journal of Speech-Language Pathology, 19(4),356–368. https://doi.org/10/d54gbw (cit. on p. 6)

[22] Ali, A. H., George, L. E., Zaidan, A. A., & Mokhtar, M. R. (2018). High capacity, transparent and secure audio steganography model based on fractal coding and chaoticmap in temporal domain. Multimedia Tools and Applications, 77(23), 31487–31516.https://doi.org/10/gfm7hc (cit. on pp. 6, 17)

[23] Mellin, F. (2021). Introduction to Fractal Image Compression. https://www.diva-portal.org/smash/get/diva2:1561273/FULLTEXT01.pdf. (Cit. on p. 6)

[24] Couteau, G. (2018). Encryption - Explaining Chaotic Cryptography. Retrieved July 28,2021, from https : / / crypto . stackexchange . com / questions / 64723 / explaining -chaotic-cryptography. (Cit. on p. 6)

[25] Kwak, M., & Cho, Y. (2021). A Novel Video Steganography-Based Botnet Communication Model in Telegram SNS Messenger. Symmetry, 13(1), 84. https://doi.org/10/gmctjx (cit. on pp. 7, 17)

[26] Tayel, M., Gamal, A., & Shawky, H. (2016). A proposed implementation method of anaudio steganography technique. 2016 18th International Conference on Advanced Communication Technology (ICACT), 180–184. https://doi.org/10/gmfg4s (cit. on pp. 2,7, 17)

[27] Mingguang, Z., & Zhitang, L. (2014). A Wav-Audio Steganography Algorithm Basedon Amplitude Modifying. 2014 Tenth International Conference on Computational Intelligence and Security, 489–493. https://doi.org/10/gmfqd6(cit. on pp. 8, 17)

[28] Gopalan, K., & Fu, J. (2015). An imperceptible and robust audio steganography employing bit modification. 2015 IEEE International Conference on Industrial Technology (ICIT),1635–1638. https://doi.org/10/gmfvqj (cit. on pp. 8, 17)

[29] Bhalde, P. (2016). Performance Improvement: Audio Steganography Technique Parity BitCombined With Cryptography. Proceedings of the Second International Conference onInformation and Communication Technology for Competitive Strategies - ICTCS ’16. https://doi.org/10/gmhd5q (cit. on pp. 8, 17)

[30] Mendel, F., Rechberger, C., & Schläffer, M. (2009). MD5 Is Weaker Than Weak: Attacks on Concatenated Combiners. In M. Matsui (Ed.), Advances in cryptology –ASIACRYPT 2009 (pp. 144–161). Springer Berlin Heidelberg. https://doi.org/10/d6sq5t. (Cit. on p. 9)

[31] Kumar, R., Punetha, M., Bhattacharya, M., & Jain, N. (2014). Safe Transmission of TextFiles through a New Audio Steganography Technique. 2014 2nd International Symposium on Computational and Business Intelligence, 58–62. https://doi.org/10/gmghwj(cit. on pp. 9, 17)

[32] Hashim, J., Hameed, A., Abbas, M. J., Awais, M., Qazi, H. A., & Abbas, S. (2018). LSBModification based Audio Steganography using Advanced Encryption Standard (AES-256) Technique. 2018 12th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), 1–6. https://doi.org/10/gjsnkg (cit. onpp. 9, 17, 21, 23)

[33] Hemeida, F., Alexan, W., & Mamdouh, S. (2019). Blowfish–Secured Audio Steganography. 2019 Novel Intelligent and Leading Emerging Sciences Conference (NILES), 1, 17–20.https://doi.org/10/gjsnkj (cit. on pp. 10, 17, 21, 23)

[34] Leadbeater, D. (2014, October 1). Vim blowfish encryption... or why you shouldn't roll your owncrypto (D. Leadbeater, Ed.). Retrieved August 16, 2021, from https://dgl.cx/2014/10/vim-blowfish. (Cit. on p. 10)

[35] Red Hat, I. (2017, January 31). Cve-2016-6329 (NIST, Ed.). NIST. Retrieved August 15,2021, from https://nvd.nist.gov/vuln/detail/CVE-2016-6329#VulnChangeHistorySection.(Cit. on p. 10)

[36] Vaudenay, S. (1996). On the weak keys of blowfish. In D. Gollmann (Ed.), Fast softwareencryption (pp. 27–32). Springer. https://doi.org/10/cwhkhz. (Cit. on p. 10)

[37] Ghosh, D., Chattopadhyay, A. K., Chanda, K., & Nag, A. (2019, July). A secure steganography scheme using LFSR. In J. K. Mandal & D. Bhattacharya (Eds.), Emergingtechnology in modelling and graphics (pp. 713–720). Springer Singapore. https://doi.org/10/gmg9b8. (Cit. on pp. 10, 17)

[38] fgrieu. (2014, January 7). Random number generator - can a LFSR be cryptographically secure?(fgrieu, Ed.). Retrieved August 15, 2021, from https://crypto.stackexchange.com/questions/12754/can-a-lfsr-be-cryptographically-secure. (Cit. on p. 10)

[39] Atti, N. B., Diaz–Toca, G. M., & Lombardi, H. (2006). The berlekamp-massey algorithmrevisited. Applicable Algebra in Engineering, Communication and Computing, 17(1), 75–82. https://doi.org/10/b6bj3d (cit. on p. 10)

[40] Gambhir, A., & Khara, S. (2016). Integrating RSA cryptography & audio steganography. 2016 International Conference on Computing, Communication and Automation (ICCCA), 481–484. https://doi.org/10/gmhd3c (cit. on pp. 10, 17)

[41] Al-Juaid, N., & Gutub, A. (2019). Combining RSA and audio steganography on personalcomputers for enhancing security. SN Applied Sciences, 1(8), 830. https://doi.org/10/gmr5p9 (cit. on pp. 10, 17, 21, 23)

[42] Rajput, S. P., Adhiya, K. P., & Patnaik, G. K. (2017). An Efficient Audio Steganography Technique to Hide Text in Audio. 2017 International Conference on Computing,Communication, Control and Automation (ICCUBEA), 1–6. https://doi.org/10/gmr5rw(cit. on pp. 11, 17)

[43] K. Patel, "Performance analysis of aes, des and blowfish cryptographic algorithms on small and large data files," International Journal of Information Technology 11(4), 813–819 (2019).

[44] E. S. I. Harba, "Secure data encryption through a combination of aes, rsa and hmac," Engineering, Technology Applied Science Research 7, 1781–1785 (Aug 2017)

[45] S. E. W. Ria Andriani and F. W. Wibowo, "Comparision of aes 128, 192 and 256 bit algorithm for encryption and description file," 2018 3rd International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE) , 120–124 (Nov 2018).

[46]. H. K. Hoomod and A. M. Radi, "New secure e-mail system based on bio-chaos key generation and modified aes algorithm," Journal of Physics: Conference Series 1003, 012025 (May 2018)

[47] Hazra, Tapan Kumar, et al. "File encryption using fisher-yates shuffle." 2015 International Conference and Workshop on Computing and Communication (IEMCON). IEEE, 2015.

[48] Rakshit, P., Ganguly, S., Pal, S., & Le, D.-N. (2021). Securing technique using patternbased LSB audio steganography and intensity-based visual cryptography. Computers, Materials & Continua, 67(1), 1207–1224. https://doi.org/10/gmgcg2 (cit. on pp. 17, 21, 23)