Journal of Engineering and Technology for Industrial Applications

ITEGAM-JETIA

Manaus, v.11 n.52, p. 136-147. March./April., 2025.
DOI: https://doi.org/10.5935/jetia. v11i52.1235

ISSN ONLINE: 2447-0228

RESEARCH ARTICLE OPEN ACCESS

A NOVEL HYBRID STEGANOGRAPHY APPROACH FOR SECURING TEXT, IMAGES, AND AUDIO WITH ROBUST ENCRYPTION IN AUDIO STEGANOGRAPHY

T Srinivasa Padmaja[1] and Shaik Mahaboob Basha [2]

[1] Dept of E.C.E, Research Scholar, Jawaharlal Nehru Technological, Anantapur, India.
[2] Dept of E.C.E Professor, N.B.K.R. Institute of Science &Technology, Vidyanagar, India.

[1]http://orcid.org/0000-0001-6218-910x, [2]http://orcid.org/0000-0002-5843-4472

Email: padmajats@gmail.com, mohisin7@yahoo.co.in

ARTICLE INFO

Article History
Received: August 11, 2024
Revised: October 20, 2025
Accepted: March 15, 2025
Published: April 30, 2025

Keywords:
Hybrid Steganography,
Audio Steganography,
Data Encryption,
Secure Communication,
Data Security.

ABSTRACT

This research proposes an imaginative hybrid steganography technique meant to strengthen the protection of text, pictures, and audio in response to the critical problem of information security. The incorporation of strong encryption in audio steganography adds to the innovation. In response to rising dangers in digital communication, the study investigates the vulnerabilities of text, picture, and audio mediums. The inquiry looks into White Space and Least Significant Bit (LSB) approaches for text steganography, while Quantization Index Modulation (QIM) is combined with LSB for image steganography. A revolutionary hybrid solution for audio steganography develops, combining Adaptive QIM and LSB. Python implementations are provided to demonstrate the use and effectiveness of these strategies in maintaining data integrity and secrecy. The study broadens its reach by presenting a novel data security paradigm in audio files that combines AES encryption, Rubik's Cube-like scrambling, and adaptive steganography. The method begins with strong AES encryption, which is then followed by a clever scrambling algorithm inspired by the Rubik's Cube. The distinguishing characteristic is seen in the last stage, when adaptive QIM embeds scrambled data into audio files, thereby disguising encrypted material. This innovative solution not only strengthens data security through the complexities of AES and Rubik's Cube-like scrambling, but it also provides a full framework for safe data transfer, exemplifying the synergy of classical encryption and current steganography techniques. The results reveal a considerable improvement in information security across various digital forms, indicating a big step forward in reinforcing sensitive data transfer.

I. INTRODUCTION

The current explosion in web technology has resulted in increasing social networking and online media sharing. Images, music, and video are exchanged in massive amounts via the internet. Obviously, data and privacy must be protected. To overcome this barrier, employ chaotic systems for picture encryption to improve security in the field of Steganography [1]. Steganography and steganalysis are key tools for information concealing and extraction. Steganography is concerned with strategies for concealing information, whereas steganalysis finds the concealed information with little or no knowledge of the steganography algorithm or its parameters [2]. The fast evolution of digital communication technology has ushered in an era where information security and privacy are of the utmost significance. This research study digs into the intricate world of steganography, a critical component of current cybersecurity, and investigates novel strategies for hiding

information inside various digital mediums [3]. The study presents and investigates cutting-edge techniques such as whitespace manipulation, Quantization Index Modulation (QIM), and Least Significant Bit (LSB) embedding, with a focus on text, image, and audio steganography [4].

Text Steganography is at the forefront of this investigation, demonstrating how messages may be surreptitiously buried within the whitespace of text documents using the intricacy of binary encoding to preserve stealth. Image Steganography expertly complements this, using QIM and LSB methods to encode binary messages into an image's pixel structure, quietly modifying its composition without detectable alterations [5]. The research then delves into Audio Steganography, which involves embedding messages in audio recordings using a combination of LSB and Adaptive QIM. This technology assures that the encoded data is imperceptible to the human ear, demonstrating the intricacy of modern steganographic technologies [6].

Furthermore, the study integrates Advanced Encryption Standard (AES) encryption with Rubik's Cube-like scrambling as well as audio steganography, a ground-breaking method in digital security [7]. This approach not only encrypts but also obfuscates data, making pattern detection in encrypted data much more difficult. The integration of these sophisticated approaches, each with its own set of obstacles and weaknesses, is systematically examined to get a thorough grasp of their potential and limits [8]. Aside from technical research, the paper examines the ethical and legal issues that emerge with the deployment of such advanced data protection mechanisms, notably in the areas of privacy and digital rights. Looking ahead, the possible influence of upcoming technologies such as quantum computing and artificial intelligence on the fields of cryptography and steganography is also examined [9]. The research study intends to make a substantial contribution to the field of secure digital communication byusingamultidimensionalapproach.Itemphasizestherisingrelevanceandpromiseof steganography in information security, emphasizing its important role in an increasingly linked digital world [10].

II. THEORETICAL REFERENCE

The literature research included here analyses important advancements in steganography techniques over a wide range of domains, including text, image, audio, and video. Notable contributions include the use of bit cycling to increase the security of encrypted text, the use of LSB methods in audio steganography for enhanced concealment, and the invention of unique picture and video steganography algorithms. Maintaining data integrity, optimizing embedding procedures for real-time applications, and resolving the trade-off between data capacity and security are among the challenges mentioned. Future research directions include improving algorithms, improving encryption meth- ods, and doing comprehensive testing to increase the overall efficacy, security, and practicality of steganographic system sinsecure data transfer and concealment.

The unique use of bit cycling in the area of secure communication is highlighted by the work of [11] who use this approach to improve the security of en- crypted text through the refining of the Least Significant Bit (LSB) method. This is an important contribution to audio steganography methods, presenting a unique method- ology that has shown excellent results in improving the concealment of encrypted data within audio recordings. The protocol's effectiveness is based on its ability to improve security and effectively avoid discovery. Nonetheless, issues such as sensitivity to sophisticated steganalysis methods, probable loss of audio quality while embedding, and embedding capacity constraints have emerged. Addressing these issues in future re- search will need a concentrated effort to preserve audio quality, investigate complex algorithms to improve detection resistance, and increase embedding capacity while keeping a high degree of confidentiality. In the context of India, [12] created a technique for hiding sensitive information in text, image, video, and audio files by applying the Least Significant

Bit (LSB) algorithm (MH). Their study showed that secret data could be successfully concealed; however, issues persisted with the LSB algorithm's ability to embed bigger data volumes without appreciably degrading the quality of the host media and the method's resilience against sophisticated detection techniques. By strengthening the algorithm's resistance to steganalysis techniques and investigating cutting-edge data embedding techniques to reduce quality loss in host media, these challenges may be overcome and the steganographic approach's overall efficacy increased. In order to improve data hiding capabilities and fortify security, [13] introduced an audio steganography technique.

The developed technique demonstrated improved security measures and a greater ability to conceal information in audio files, which led to encouraging findings from the study. The authors did, however, face some challenges, including the need to maintain audio quality when embedding data and potential issues with the method's computational complexity, which could have an impact on real-time applications. Subsequent studies could tackle these problems by optimizing the algorithm's performance to reduce computational over- head and simplifying the embedding process to reduce the loss of audio quality.

This would make the suggested audio steganography method more beneficial and effective. A novel text steganography method was introduced by [14] in their study. Although the uniqueness of their research held promise, more research is necessary to address issues like the method's security and resilience to steganalysis techniques. Future research should concentrate on conducting thorough security evaluations and strengthening the method's resistance to detection techniques in order to overcome these obstacles and ultimately improve the efficacy and dependability of this cutting-edge text steganography technique. Arabic letters' diacritical marks and picture layers were used by [15] in their study to present a dynamic multi-layer steganography technique.

The study demonstrated the method's efficacy in hiding data in images, but issues like possible deterioration of image quality and security risks related to detection techniques must be resolved. In order to address these issues and improve the practicality and dependability of this novel steganography method, further research can concentrate on optimizing the embedding procedure to reduce the impact on image quality, investigating sophisticated encryption and authentication methods for increased security, and carrying out extensive testing to guarantee resilience against steganalysis techniques.

In the investigation conducted by [16] looked into audio steganography. The specific methods the authors used were not made explicit, even though their study illuminated the field. Yet, the study most likely yielded conclusions regarding audio

steganography, its applications, or upcoming advancements in the industry. Common issues in audio steganography include data hiding while maintaining audio quality, security and resilience against detection, and optimizing the embedding process for real-time applications.

To address these challenges, further research may involve refining embedding algorithms, employing advanced encryption techniques, and conducting extensive testing to enhance the security and viability of audio steganography approaches. For [14] did not specifically develop their own methods; instead, they performed a thorough review of the methods that are currently in use in audio steganography as part of their survey. The survey probably provided a summary of different approaches and findings in the field, illuminating the development and variety of audio steganography techniques.

The survey may have covered challenges pertaining to data capacity, imperceptibility, and resilience to steganalysis. Future research may focus on creating sophisticated audio steganography methods that balance high data hiding capacity, low perceptual distortion, and resistance to contemporary detection techniques in order to overcome these difficulties. Furthermore, the security of audio steganography may be further improved by adding encryption and authentication methods, guaranteeing its efficacy in safe data transmission and storage. According to [17] assessed audio steganography as an image file embedding technique in his study, using Snappy compression and encryption. It's possible that the study included results about how well this method works to safely hide picture data inside audio files.

Typical problems with audio steganography include embedded capacity constraints, possible loss of audio quality, and robustness against detection. Future studies may look into ways to reduce quality loss in the compression and encryption processes, maximize embedding capacity, and strengthen the method's resilience against contemporary steganalysis techniques in order to address these issues. By doing this, audio steganography for image file embedding can become more viable and reliable, increasing its usefulness for safe data transfer and storage. In order to assess the advantages and disadvantages of different audio steganography techniques, [18] carried out a comparative analysis of these methods in their study.

Most likely, the study offered a thorough analysis of the various audio steganography techniques currently in use and how well they work in comparison. Creating uniform evaluation criteria and figuring out the best methods for various application scenarios are two common problems in these kinds of comparative research. Future work may focus on improving evaluation metrics, creating uniform benchmarks, and offering guidance for choosing the best audio steganography technique based on particular use cases in order to address these issues and help make well-informed decisions regarding secure data protection and communication.

Created an image steganography technique using a Matlab-implemented graphical user interface (GUI). It's possible that their research involved developing an easy-to-use tool for embedding and extracting hidden data from image files. While specific outcomes and difficulties were not covered in detail in the reference, maintaining a balance between security and usability as well as maximizing the steganographic method's robustness are frequent problems in image steganography with GUI implementations. The practicality and dependability of this image steganography tool in secure data communication and concealment may be advanced by further research focusing on improving the GUI design for a better user experience, implementing robust encryption and authentication mechanisms to increase security, and conducting extensive testing to evaluate the method's performance and resilience against steganalysis.

A novel coverless audio steganography technique based on Generative Adversarial Networks (GANs) was presented by [19] in their research. Although the reference did not include all of their findings, it is likely that this method showed improvements in safe data embedding in audio files. A common challenge in coverless audio steganography is maintaining data integrity and resilience to detection methods. Future research may focus on developing more sophisticated steganalysis-resistant mechanisms, optimizing the steganographic process for better data integrity, and further refining GAN-based techniques in order to address these issues.

Through these efforts, coverless audio steganography for safe data transmission and protection would become more reliable and practical. A hybrid encryption algorithm and the Least Significant Bit (LSB) technique were combined to create an image steganography method by [20]. Although the reference did not provide specific findings and challenges, their approach probably involved data concealment within images, integrating LSB for data embedding, and using hybrid encryption algorithms to increase security.

The trade-off between data capacity and security, as well as the requirement to guarantee robustness against detection, are common challenges in image steganography. Future research may focus on improving the hybrid encryption algorithms, enhancing data embedding for increased security and data integrity, and creating defences against sophisticated steganalysis techniques in order to address these issues.

These initiatives would help to improve the usefulness and dependability of this image steganography technique for safe data transmission and archiving. To hide images within audio data, [21] set out to develop a deep steganography technique. Although the source did not specify the precise outcomes and difficulties they faced, their work probably contributed to the development of image-in-audio steganography. Optimizing the embedding process for data capacity and minimizing perceptual distortions while maintaining robustness against steganalysis techniques are common challenges in deep steganography.

Future research may concentrate on improving deep steganography algorithms, investigating cutting-edge neural network architectures, and carrying out extensive testing to evaluate the efficacy and security of the technique in order to address these issues. This would make image-in-audio deep steganography more useful and dependable, increasing its efficacy for secure data transmission and concealment. A coverless video steganography method based on the combination of audio and frame features was created in [22].

This approach probably involved innovations in secure data embedding within video files through the fusion of audio and frame characteristics, though specific results and challenges were not specified in the reference. Problems with data capacity, preserving video quality, and guaranteeing robustness against steganalysis are frequently linked to coverless video steganography. Future research may focus on improving the steganographic procedure to strike a balance between data capacity and video quality, streamlining the integration of frame and audio features, and putting in place sophisticated steganalysis-resistant techniques in order to overcome these

difficulties. These initiatives would help to improve coverless video steganography's usefulness and dependability for secure data communication and protection. An innovative JPEG steganography technique with high capacity and robustness was created via adversarial training in the study done by [23].

This technique probably represented advancements in safely embedding data within JPEG images, with an emphasis on data capacity and resilience against detection, even though specific results and challenges were not mentioned in the reference. Keeping data capacity and image quality in check while also addressing flaws in current steganalysis methods are common problems in JPEG steganography.

Future work may focus on improving adversarial training strategies, streamlining the embedding procedure to minimize visual distortion and increase data capacity, and creating defences against sophisticated detection techniques in order to address these issues. These initiatives would help to improve the usefulness and dependability of robust and high-capacity JPEG steganography for safe data transfer and security.

Previous steganography research encountered issues such as steganalysis sensitivity, probable audio quality loss, limited embedding capacity, and detection method flaws. Future research will try to tackle these challenges by optimizing algorithms for audio quality preservation, boosting resistance to steganalysis, investigating advanced data embedding methods, and increasing confidentiality capacity.

GAN-based algorithms improve coverless audio steganography, hybrid encryption improves picture steganography, and deep steganography is optimized for image-in-audio applications. Coverless video steganography is enhanced by improved frame-audio integration and steganalysis-resistant methods. Improved adversarial training and reduced embedding techniques in JPEG steganography provide increased capacity and robustness. By addressing these issues, steganographic systems for secure data transport and protection become more reliable.

III. METHODOLOGY

III.1 TEXT STEGANOGRAPHY(STEGOTEXT)

The message is translated to binary form and then carefully inserted among the whites- pace of the original text. Each character of the binary message corresponds to the least important bits of the characters in the text; this strategy depends on changing inconsequential components of the carrier (text) to hide the message without visible changes to the human eye [24].

The key approach used includes manipulating whitespace characters; the script finds existing whitespace in the text and adds extra spaces that encode the binary message. The whitespace works as a carrier for the concealed information, successfully disguising it within the seemingly benign spaces between words and lines. This delimiter helps the extraction procedure by specifying when the encoded binary message ends, assuring correct and ambiguous recovery [25].

III.2 IMAGE STEGANOGRAPHY(PIXEL QUANTA)

Our proposed work demonstrates a technique called Quantization Index Modulation (QIM) combined with the Least Significant Bit (LSB) method for steganography, embedding secret messages into images and extracting them without perceptible visual changes [26].

The suggested work represents transforming a text message to binary and hiding it in a picture using LSB substitution in the least significant bits of the RGB channels. Retrieves the concealed binary message from the stego picture by analyzing the LSBs of the RGB channels, and finds any pixel-wise discrepancies between the original and stego images to ensure the steganographic process's integrity [27].

Finally, compare the original and stego photos to visually analyze any variations between the two photographs. The QIM method provides detection resistance, but the LSB method allows for minimum visual distortion, making it suited for hidden communication.

III.3 AUDIO STEGANOGRAPHY (QUANTUMAUDio)

The amalgamation of Adaptive Quantization Index Modulation (QIM) and Least Significant Bit (LSB) methods forms the foundation for our proposed work, enabling the concealment of both audio and textual information within audio files.

The technique includes calculating frame energies to allow adaptive embedding inside the audio stream, guaranteeing an optimum concealment strategy. The Adaptive QIM embedding technology smoothly embeds pieces of information by modifying audio samples based on a predetermined delta value. In addition, the Least Significant Bit (LSB) approach conceals textual information within audio samples, resulting in a hybrid model for strong and thorough data concealment [28].

III.4 ADAPTIVE QUANTIZATION INDEX MODULATION (QIM)

Adaptive QIM Embedding: This technique modifies audio samples by embedding information in their quantized representations based on a predefined delta value, using a QIM scheme.

The Adaptive QIM technique is a sophisticated approach geared towards embedding an audio message into a host audio file. This method hinges on the principle of selectively modifying certain parts of the audio based on their energy levels – a strategy that brings adaptiveness into play. Audio steganography system marries the robustness and perceptual transparency of Adaptive QIM with the simplicity and subtlety of LSB. Adaptive QIM is adept at embedding messages in parts of the audio that are less likely to reveal alterations, while LSB offers a straightforward way of hiding text messages with negligible impact on the audio quality.

Adaptive QIM Extraction: It reverses the embedding process to extract the hidden information from the modified samples [29].

Steganography Embedding (QIM)

Given:
Audio frame F.
Binary bit to embed b.Delta value Δ.

The embedding function for QIM can be defined as:

$$\begin{cases} \left\lfloor \frac{F}{\Delta} \right\rfloor . \Delta + \frac{\Delta}{4}, \text{if } b = 1 \\ \left\lfloor \frac{F}{\Delta} \right\rfloor . \Delta - \frac{\Delta}{4}, \text{if } b = 0 \end{cases} \quad (1)$$

Steganography Extraction (QIM)

Given:

$$\begin{cases} 1, & \text{if} F > [\frac{F}{\Delta}] . \Delta \\ 0, & \text{otherwise} \end{cases} \quad (2)$$

Modified audio frame F ‘.
Delta value Δ.

III.5 LEAST SIGNIFICANT BIT (LSB) EMBEDDING

This method embeds text information by manipulating the least significant bits of the audio samples. The proposed steganographic model combines QIM and LSB approaches, proving its effectiveness through actual application. The encoded information is unnoticeable to aural examination, and the original audio quality is effectively preserved. The QIM-based embedding's adaptive nature, directed by energy thresholds, enables optimal concealing capacity without compromising audio fidelity [30].

Finally, the presented research adds a unique way to audio steganography by combining QIM and LSB approaches. The hybrid architecture proposed provides a stable and extensible framework for hidden data transfer within audio recordings. The imperceptibility of embedded information, together with message extraction efficacy, highlights the potential for real-world applications needing secure and covert communication routes.

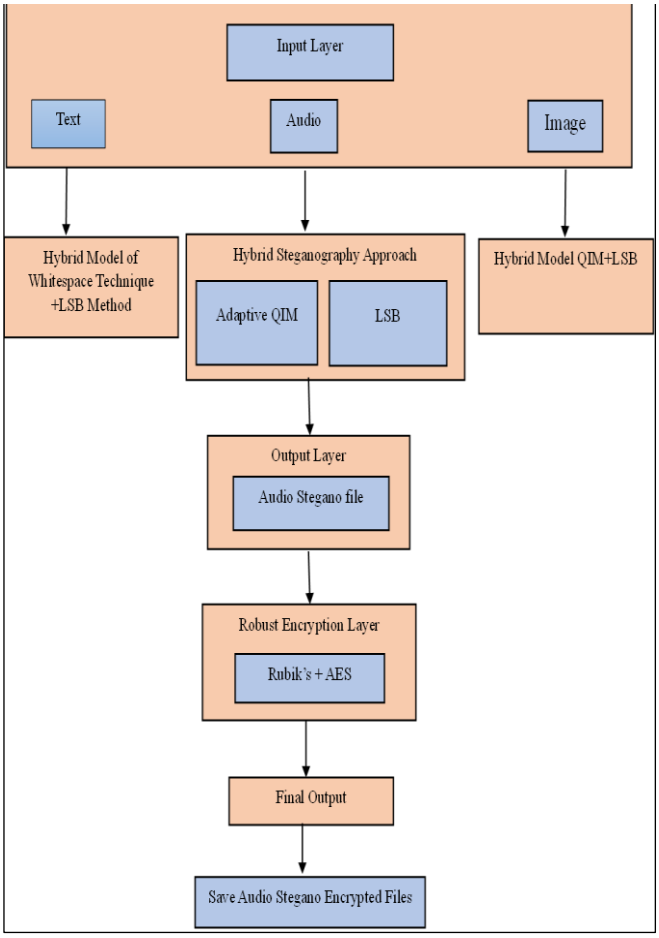

Figure 1: Hybrid Audio Security Process Flow Diagram.
Source: Authors, (2025).

The diagram shows how to safeguard audio recordings using a multi-layered security approach that combines encryption and steganography. At first, the Input Layer supports a number of media formats, such as text, audio, and photos. The data is then processed using a Hybrid Steganography Approach, which hides the data from view by embedding it into an audio file using methods like LSB and Adaptive QIM [6]. At the Output Layer, the resultant file is called an Audio Stegano file, signifying that the data has been hidden inside the audio. This steganographically enhanced file is then subjected to an additional layer of security called a Robust Encryption Layer, which uses a combination of the Advanced Encryption Standard (AES) and Rubik’s Cube algorithmic strategies in addition to Quantum Key Encryption, which proposes the use of quantum-resistant encryption techniques. At the Final

Output, the proce- dure is complete. The Audio Stegano files are now encrypted, offering a high degree of confidentiality and privacy, and are prepared for safe transmission or storage.

III.6 RUBIK CIPHER AUDIO

Embedding data within an audio file using atechnique called Quantization Index Modulation (QIM), allowing to modify audio samples to encode hidden information our proposed work implements Advanced Encryption Standard

(AES) encryption, a symmetric key algorithm renowned for its security and efficiency in data encryption [31]. Our proposed work implements Advanced Encryption Standard (AES) encryption, a symmetric key algorithm renowned for its security and efficiency in data encryption.

AES operates in Cipher Block Chaining (CBC) mode, providing confidentiality through block-level encryption. After that we initializes the AES cipher in CBC mode with a specific key finally, we perform encryption and decryption using AES with padding to ensure the input data is of the correct block size.

AES Encryption:
Given:

Plaintext P.
Key K.
Initial Vector IV generated randomly.

The AES encryption process can be represented as:

$$C = AES_{K,IV}(P) \quad (3)$$

Where C is the cyphertext $AES_{K,IV}(P)$is the AES encryption of plaintext P using key K

And initial vector IV .

AES Decryption:

Given:

Ciphertext C.
Key K.
Initial Vector IV.

The AES decryption process is represented as:

$$P = AES^{-1}_{K,IV}(C) \quad (4)$$

Where P is the decrypted plaintext, and $AES^{-1}_{K,IV}(C)$ is the AES decryption of ciphertext C

Using key K and initial vector IV.

Steganography conceals information within other data (here, an audio file) without arousing suspicion. Our proposed work uses Quantization Index Modulation (QIM) for embedding bits into audio samples [32]. It embeds a binary message into an audio file by slightly modifying audio samples based on a delta value, extracts the hidden binary message from the modified audio file using the same delta value employs custom algorithms for data manipulation, including reversible scrambling inspired by the

Rubik's Cube and binary representation conversion, scrambles and unscrambles data using a key, implementing a custom reversible algorithm inspired by the Rubik's Cube, and applying text messages into binary representations for embedding within the audio file and reverses the process for message extraction [33].

III.6.1 RUBIK'S CUBE-LIKE SCRAMBLING:

Given:
Scrambled data D.
Key K represented as a sequence of integers K = [k_1, k_2, …, k_n].

The unscrambling process for each byte Di in D can be described as:

$$D_i = \text{Unscramble}(D_{i,}K) \quad (5)$$

where D_i is the unscrambled byte. The unscrambling process involves reversing the scrambling steps applied previously.

The struct module facilitates the conversion between Python values and binary data, Audio frames are manipulated at the sample level to embed and extract hidden bits, ensuring minimal perceptual impact [34].

3.6.2 Mean Squared Error (MSE):

The difference in squares between the original and stego audio signals' equivalent values is measured by the Mean Squared Error.

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(x_i - y_i)^2 \quad (6)$$

Where N is the number of samples and x_i and y_i are the corresponding sample the original and stego.

3.6.3 Peak Signal-to-Noise Ratio (PSNR):

PSNR is a measure of the quality of the stego audio signal compare to the original audio signal. Its express in decibels(dB).

$$PSNR = 10.\log_{10}\left(\frac{MAX^2}{MSE}\right) \quad (7)$$

Where MAX is the maximum possible pixel value (usually 1 for normalized audio) and MSE is the Mean Squared Error.

3.6.4 Signal-to-Noise Ratio (SNR):

SNR is measure of the quality of the stego audio compared to the original audio signal. It is also expressed in decibels (dB).

$$SNR = 10\,.\log_{10}\left(\frac{signalpower}{Noisepower}\right) \quad (8)$$

When it comes to audio processing, the signal power (signal power) can be thought of as the original. The energy difference between the original and stego signals is known as the noise power, and it is represented by the audio signal.

IV. RESULTS AND DISCUSSIONS

The steganography techniques demonstrated in the text, picture, and audio domains are successful in concealing information. Binary messages are discretely encoded in text whitespace, and picture pixels are subtly altered by Quantization Index Modulation (QIM). The audio steganography uses adaptive QIM embedding, and a strong encryption method assures safe connection. Evaluation measures like as MSE, PSNR, and SNR indicate the success of these technologies, which provide a complete and secure way of covert communication across several media.

IV.1. TEXT.

Figure 2 shows contain some original message which we are going to use to apply steganography techniques. The message is converted into binary form and then strategically embedded within the whitespace of the original text. Each character of the binary message corresponds to the least significant bits of the characters in the text, this technique relies on altering insignificant components of the carrier (text) to hide the message without perceptible changes to the naked eye.

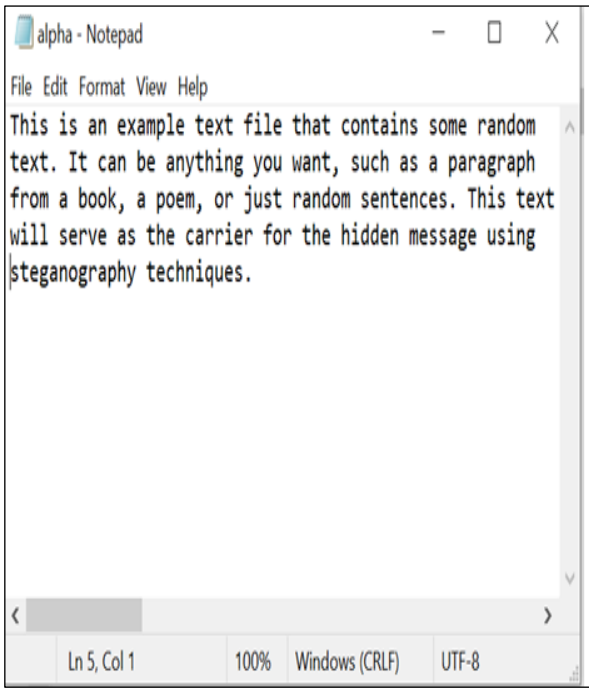

Figure 2: Original Text.
Source: Authors, (2025).

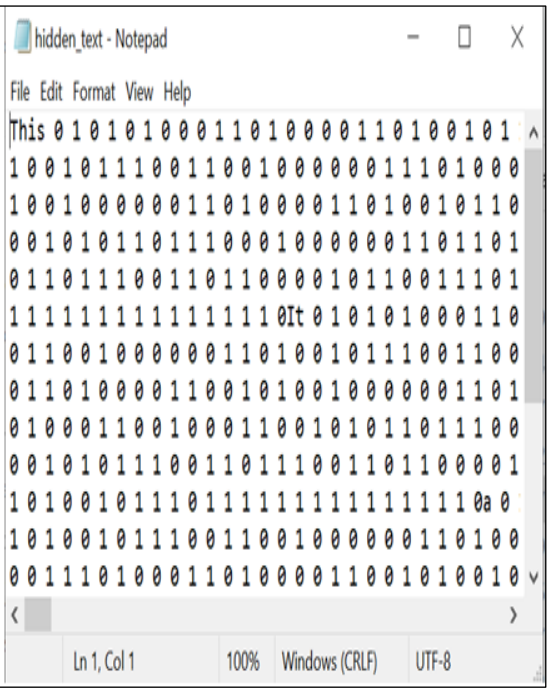

Figure 3: Hidden text.
Source; Authors, (2025).

This is an example text file that contains some random text. It can be anything you want, such as a paragraph from a book, a poem, or just random sentences. This text will serve as the carrier for the hidden message using steganography techniques.

Figure 4: Screenshot of Output text.
Source: Authors, (2025).

Figure 3 shows the primary technique employed in this code involves manipulating whitespace characters, the script identifies existing whitespace in the text and inserts additional spaces that encode the binary message.

The whitespace acts as a carrier for the hidden message, effectively concealing it within the seemingly innocuous gaps between words and lines. This delimiter helps the extraction process by indicating where the embedded binary message concludes, ensuring accurate retrieval without ambiguity.

Figure 4 shows Our final step is performed to showcase the final appearance of the text after the steganography process, emphasizing the effectiveness of concealing information within seemingly innocuous text through subtle whitespace alterations.

IV.2. IMAGE

Figure 4: Original Image.
Source; Authors, (2025).

Figure 5: Steganographic image.
Source; Authors, (2025).

Figure 4 shows the original image (lena_std.tif) most likely represents the well-known "Lena" image, a typical test image often used in image processing. Figure 5 shows the `embed_message` function takes an image and a textual message as inputs. Initially, it converts the message into a binary representation and appends a delimiter to mark the end of the message. Subsequently, the function traverses each pixel of the input image. During this iteration, it embeds the binary message into the least significant bits (LSBs) of the red, green, and blue channels of each pixel. The process involves bitwise operations to modify the LSBs while preserving the overall

color information. This embedding ensures that the alterations are subtle and often imperceptible to the human eye. Finally, the function saves the modified image, known as the stego image, preserving the original appearance but concealing the binary message within its pixel values. This steganographic technique, Quantization Index Modulation (QIM), enables hidden communication within the visual content of the image, providing a means of covert information transfer.

IV.3 AUDIO

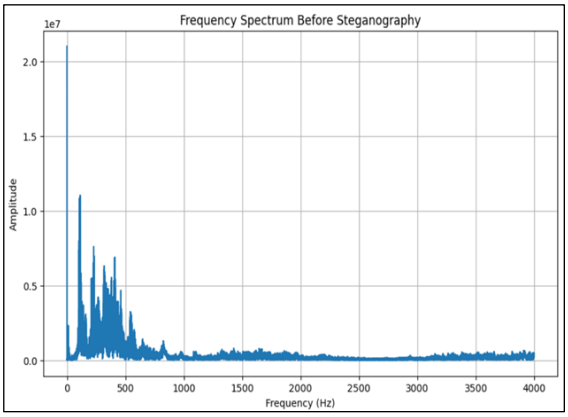

Figure 6: Frequency Spectrum Before Steganography.
Source; Authors, (2025).

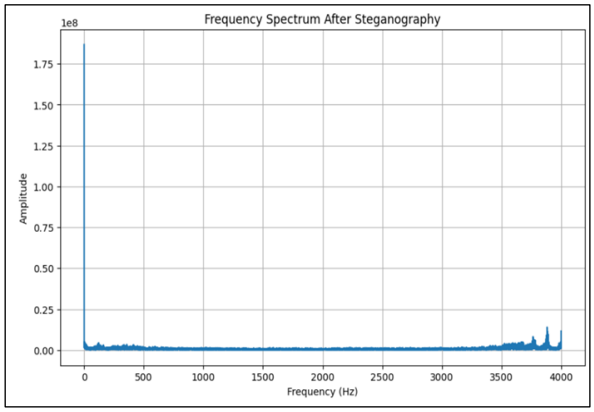

Figure 7: Frequency Spectrum After Steganography.
Source; Authors, (2025).

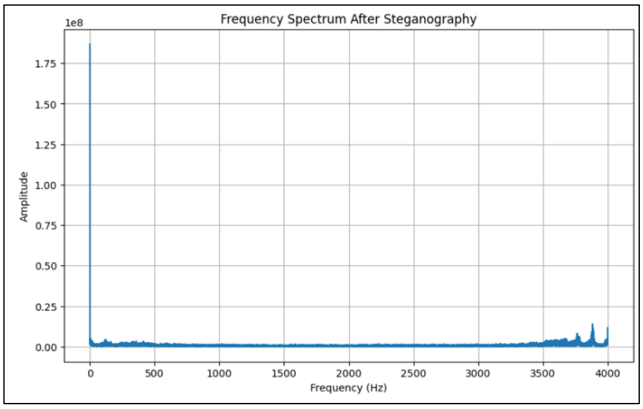

Figure 7: Frequency Spectrum After Steganography.
Source; Authors, (2025).

The provided parameters detail the components and settings for an audio steganography process. The "Input audio file" serves as the original audio source for message embedding, and the "Output audio file" designates where the steganographic audio will be saved. Users have the option to embed either a "Secret audio message" or a "Text message" within the input audio file.

The "Delta" value is specified for the Adaptive QIM embedding technique, influencing the degree of message concealment. Additionally, an "Energy threshold" is established for adaptive steganography, determining the level of energy required for effective concealment. These parameters collectively define the configuration and goals of the audio steganography operation, allowing for customization based on the user's preferences and requirements.

The resulting visualizations depict the amplitude distribution across frequencies, allowing for a comparative analysis of the spectral characteristics before and after the steganographic process. These plots serve as valuable insights into the alterations introduced by the steganography method, aiding in the assessment of its impact on the audio signal. By comparing the plots before and after steganography, one can observe any changes introduced during the embedding process, aiding in the assessment of how steganography affects the frequency characteristics of the audio signal in Figure 6 and 7.

IV.3.1 Steganography Audio Encryption.

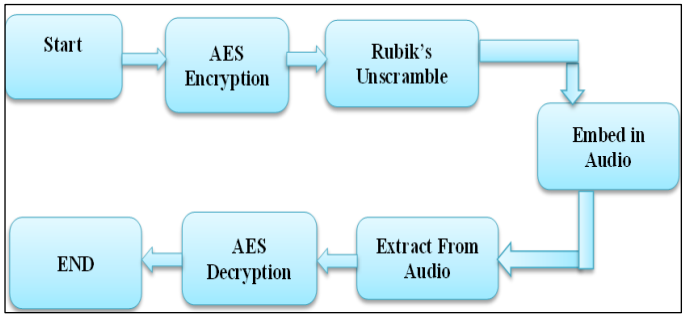

Figure 8: Robust Encryption Approach.
Source: Authors, (2025).

Figure 8 illustrates the study begins with AES encryption in CBC mode, a commonly used approach for assuring plaintext security by mixing a random initialization vector (IV) with a predetermined key. The succeeding Rubik's Unscramble method takes a novel approach to reversing data scrambling by rearranging pieces depending on byte values

inside a certain key, with the goal of restoring data to its pre-scrambling condition. Quantization Index Modulation (QIM) is an audio embedding technique that surreptitiously encodes binary signals into audio files, gently modifying audio samples that are unnoticeable to the human ear. This entails translating a textual message to binary for embedding and recovering embedded binary messages via audio extraction. Furthermore, the explanation of AES decryption emphasizes the significance of safe key generation, as demonstrated by the development of a random 16-byte AES key. Finally, the research shows generic data encryption and decryption using AES-CBC mode, emphasizing the symmetric aspect of AES by utilizing the same key for both encryption and decryption. These strategies, when combined, demonstrate the flexibility of cryptographic methods in safeguarding information and enabling clandestine communication.

Table 1**:** Audio Files with after Steganography Analysis of MSE, PSNR and SNR.

Audio Name	Stego Name	Audio Size	Stego Size	MSE	PSNR	SNR
Audio1.wav	stego_audio1.wav	1.51 mb	1.50 mb	0.09282929450273514	10.323149501470688 dB	-2.794678807258606 dB
Audio2.wav	stego_audio2.wav	3.33 mb	3.29 mb	0.07753556221723557	11.104990596574197 dB	-2.8700366616249084 dB
Audio3.wav	stego_audio3.wav	3.36 mb	3.27 mb	0.030982017517089844	15.088903048463372 dB	-12.872124910354614 dB

Source: Authors, (2025).

The table presents information on original audio files and their stego versions, including file names, sizes, and quality metrics. The "MSE" (Mean Squared Error) indicates the difference between original and stego signals, with lower values indicating better quality. "PSNR" (Peak Signal-to-Noise Ratio) measures stego audio quality, higher values suggesting better fidelity. "SNR" (Signal-to-Noise Ratio) reflects the overall quality of stego audio. The table provides a concise assessment of steganography effectiveness for each audio pair.

IV.4 COMPARATIVE ANALYSIS.

Table 2: Comparison Analysis (A), (B), (C) with the Existing System for our Proposed System.

A. Comparative Analysis for Proposed System with Existing System (Text)		
Aspects	Stegotext Steganography	Traditional Text Steganography
Security and Detectability	High security owing to obscurity; modifications are less detected.	Lower security; modifications may be more obvious and detected.
Resistance to Automated Detection	Less likely to be detected by automated tools due to subtle changes.	More likely to be detected by tools designed to analyze text patterns.
Adaptability to Text Formats and Inspection Resistance	Adaptable to a broad range of text types and difficult to recognize through casual inspection.	May be confined to certain formats or need specific text circumstances. Possibility of discovery by close reading or text analysis.
Integrity of Original Text	Maintains the original content and structure of the text.	May require altering the actual text content or structure.
Ease of Implementation	Relatively simple to implement using standard text editing tools.	Might require more complex manipulations or specific software.
Capacity for Hidden Information	Limited capacity due to dependency on whitespace and LSB only.	It may have greater capacity since it can employ more text features for hiding.
B. Comparative Analysis for Proposed System with Existing System (Image)		
Aspects	PixelQuanta	Traditional Image Steganography
Robustness Against Compression	Higher robustness against lossy compression like JPEG.	Lower robustness; often susceptible to quality loss during compression.
Capacity for Hidden Information	The combination of QIM and LSB methods results in a high capacity.	Variable, but often lower when compared to QIM + LSB.
Image Quality Preservation	Preserves image quality better making changes less detectable.	Image quality may degrade, making steganography more detectable.
Security and Detectability	Enhanced security due to less detectability of hidden data.	Less secure, as alteration can be more evident.
Resistance to Image Manipulation	More resistance to picture alteration such as cropping and scaling.	Less resistant; tampering has the potential to erase the secret data.
Complexity and Computational Load	Higher complexity and computational requirements.	Simpler and less computationally intensive.
Flexibility and Adaptability	Highly flexible and adaptable to various image formats and condition.	May have limitation in adaptability to different image types.
C. Comparative Analysis for Proposed System with Existing System (Audio)		
Aspects	Quantum audio	Traditional Audio Steganography
Robustness Against Compression	Offers robust resistance to lossy audio compression due to the resilience of Adaptive QIM; LSB also contributes but is less robust.	Typically, more susceptible to degradation from compression.
Capacity for Hidden Information	High capacity achieved through the efficient use of Adaptive QIM for audio messages and LSB for text, utilizing different aspects of the audio.	Lower capacity; limitations based on the audio format and method used.
Audio Quality Preservation	Superior preservation of audio quality; adaptive nature of QIM ensures less perceptible alterations, complemented by the subtlety of LSB.	This might result in obvious quality decrease or artefacts.

Security and Detectability	Enhanced security with challenging detectability due to the adaptive embedding of QIM and the subtleness of LSB alterations.	Less secure, as modifications can be more evident or predictable.
Resistance to Audio Manipulation	Higher resistance to audio processing like filtering and equalization, particularly due to Adaptive QIM's selective embedding.	Decrease resistance; processing has the ability to disrupt or erase concealed information.
Complexity and Computational Load	Higher, reflecting the sophisticated nature of Adaptive QIM combined with LSB, requiring more computational resources.	Generally simpler and less computationally demanding.
Flexibility and Adaptability	Highly adaptable to varying audio contents and conditions, benefiting from the selective embedding of Adaptive QIM and the universality of LSB.	May have limited adaptability depending on the technique used.
Suitability for High-Security Needs	More suitable for high-security applications due to enhanced stealth and difficulty in detecting embedded messages.	Due to increased detectability, it is less suitable for high-security applications.

Source: Authors, (2025).

Table 2 shows the comparative analysis demonstrates that when compared to the suggested systems, typical steganographic approaches, whether in the context of text, picture, or audio, frequently have major shortcomings. One significant disadvantage is their lack of security and detectability. Traditional text steganography makes modifications more visible and identifiable, making it less appropriate for high-security applications. Similarly, traditional picture steganography techniques are frequently subject to quality loss during compression, making them less resilient, while traditional audio steganography may result in apparent quality deterioration or artefacts, reducing their capacity to successfully conceal secret information.

The flexibility and resilience to manipulation of classic steganography technologies is another major drawback. Traditional text and picture steganography may be confined to certain forms or need specific circumstances, making them less adaptable and practical for a wide range of applications. In contrast, the suggested systems in each domain provide improved flexibility, compression resistance, and manipulation resistance. These benefits make them more suitable for high-security applications and scenarios requiring the preservation of original content quality.

Table 3: Comparison of Traditional and Hybrid Audio Steganography with Robust Encryption.

Aspects	Rubik Cipher Audio	Traditional Encryption Methods
Encryption Strength	Extremely high due to AES's strong encryption algorithm combined with additional scrambling.	Varies, but often lower, especially in older or simpler algorithms.
Computational Complexity	Higher, due to the two-step process involving both AES encryption and Rubik's Cube-like Scrambling.	Generally lower, involving straightforward encryption processes.
Resistance to Cryptanalysis	Enhanced resistance; the scrambling adds an extra layer of complexity for attackers.	Depends on the algorithm; some older methods are more vulnerable.
Data Pattern Obfuscation	Superior, as the Rubik's Cube-like method disrupts data patterns, making analysis more difficult.	Less effective, especially if the encryption doesn't include additional obfuscation techniques.
Key Management Complexity	Increased complexity due to the need for managing both AES and scrambling keys.	Simpler, usually involving a single key or key pair.
Decryption Process	Requires precise reverse steps, adding to the complexity and time for decryption.	Typically, straightforward and faster.
Suitability for Sensitive Data	Highly suitable for highly sensitive data due to the robustness of the combined methods.	Suitability varies; some methods may not be recommended for highly sensitive data.
Implementation Difficulty	More challenging due to the integration of two distinct methods.	Generally easier to implement with standard libraries and tools.
Flexibility and Adaptability	Highly adaptable to different types of data and security requirements.	Varies; some methods are less adaptable to new or varied requirements.

Source: Authors, (2025).

Table 3 shows the comparison of Rubik Cipher Audio and traditional encryption methods for audio steganography reveals that the Rubik Cypher Audio method combines AES encryption with Rubik's Cube-like scrambling to achieve exceptionally high encryption strength and enhanced resistance to cryptanalysis, making it highly suitable for safeguarding highly sensitive data. It does, however, come with increasing computational complexity and implementation difficulties. Traditional encryption methods, on the other hand, while typically simpler to apply, vary in encryption strength and may provide less protection, with limited flexibility to diverse data types and security needs. As a result, the decision between both ways is determined by the application's individual security requirements and complexity, with the Rubik Cypher Audio method providing a strong solution for maximal data protection.

V. CONCLUSIONS

This study presents a ground-breaking hybrid steganography technique that combines strong encryption methods like the Advanced Encryption Standard (AES) and Rubik's Cube-like scrambling with advanced steganographic techniques like White Space, Least Significant Bit (LSB), Quantization Index Modulation (QIM), and Adaptive Modulation. The study demonstrates the feasibility and efficacy of these strategies in real-world circumstances, emphasizing their potential to improve data integrity and

confidentiality across text, picture, and audio data in digital communication.

In comparison to previous systems, this hybrid method provides improved security, increased resistance to detection, and better flexibility to multiple formats, placing it as a flexible option for secure digital communication. The study not only represents a huge advancement in information security, but it also sets the path for future research, notably in the fields of quantum computing and artificial intelligence, to further develop these strategies and solve increasing cybersecurity concerns.

VI. AUTHOR'S CONTRIBUTION

Conceptualization: T.Srinivasa Padmaja, Shaik Mohammod Basha.
Methodology: T.Srinivasa Padmaja, Shaik Mohammod Basha.
Investigation: T.Srinivasa Padmaja, Shaik Mohammod Basha.
Discussion of results: T.Srinivasa Padmaja. Shaik Mohammod Basha.
Writing – Original Draft: T Srinivasa Padmaja.
Writing – Review and Editing: T.Srinivasa Padmaja. Shaik Mohammod Basha.
Resources: T.Srinivasa Padmaja, Shaik Mohammod Basha.
Supervision: Shaik Mohammod Basha.
Approval of the final text: T.Srinivasa Padmaja. Shaik Mohammod Basha.

VII. REFERENCES

[1] Aruna, Ms& Nandika, L & Sneha, C & Xavier, imothy& George, Treesa. (2023). Text, Image and Audio Steganography. International Journal for Research in Applied Science and Engineering Technology. 11. 4435-4439. 10.22214/ijraset.2023.51091.

[2] Kumar, A.V. & G., Rahul &Musirin, I. & Irawati, Indrarini& Amine, Abdelmalek & Bri, Seddik. (2023). A Study of Steganography Approach for Securing Data in a Confidential Communication Using Encryption. 10.4018/978-1-6684-6581-3.ch005.

[3] Nasr, Marwa & El-Shafai, Walid & El-Rabaie, El-Sayed & El-Fishawy, Adel & Dessouky, M.I. & Abdelsalam, Naiman & Abd El-Samie, Fathi. (2023). A Robust Technique for Steganography of Enhanced Audio Signals. 1-6. 10.1109/ICEEM58740.2023.10319573.

[4] Monika, A. & Rajagopal, Eswari & Singh, Swastik. (2023). Detection of Location of Audio-Stegware in LSB Audio Steganography. 10.1007/978-981-99-0609-3_31.

[5] Adhanadi, Fikri &Novamizanti, Ledya & Budiman, Gelar. (2020). DWT-SMM-based audio steganography with RSA encryption and compressive sampling. TELKOMNIKA (Telecommunication Computing Electronics and Control). 18. 1095. 10.12928/telkomnika.v18i2.14833.

[6] Subhi, Nooruldeen& Salih Mahdi, Mohammed. (2023). Using Special Letters And Diacritics In Steganography In Holy Quran. Iraqi Journal for Computers and Informatics. 49.

[7] Sultani, Zainab &Dhannoon, Ban. (2021). Image and audio steganography based on indirect LSB. Kuwait Journal of Science. 48. 10.48129/kjs.v48i4.8992.

[8] Zhuo, Peiwen & Yan, Diqun& Ying, Kaiyu & Wang, Rangding& Dong, Li. (2023). Audio steganography cover enhancement via reinforcement learning. Signal, Image and Video Processing. 10.1007/s11760-023-02819-1.

[9] Joshi, Ranjana & Trivedi, (Dr.) Munesh & Goyal, Vishal & Bhati, Deepshikha. (2022). Recent Trends for Practicing Steganography Using Audio as Carrier: A Study. 10.1007/978-981-19-5292-0_52.

[10] Abikoye, Oluwakemi &Ogundokun, Roseline & Misra, Sanjay & Agrawal, Akasht. (2022). Analytical Study on LSB-Based Image Steganography Approach. 10.1007/978-981-16-8484-5_43.

[11] W.Abood, Enas& Abdullah, Abdulhussein & Al Sibahee, Mustafa & Abduljabbar, Zaid & Nyangaresi, Vincent & Ahmad, Saad &Kalafy, Ali & Jalil, Mudhafar&Ghrabta, Jassim & Wahab, Enas. (2022). Audio steganography with enhanced LSB method for securing encrypted text with bit cycling. Bulletin of Electrical Engineering and Informatics. 11. 185-194. 10.11591/eei.v11i1.3279.

[12] Kumar, Madhurendra& Kumari, Muskan & Patil, Tushar & Pradhan, Rahul & Giri, Manish. (2023). Hiding secret data in audio,video,image,text steganography using least significant bit algorithm(MH)India. 9. 874-877.

[13] Tasnim, Orora& Hossain, Md & Rahman, Mahfujur. (2023). Audio Steganography with Intensified Security and Hiding Capacity. European Chemical Bulletin. 12. 162-173. 10.48047/ecb/2023.12.10.013.

[14] Singh, Mr& Diwakar, Anirudra & Upadhyaya, Ms. (2023). A Novel Approach to Text Steganography. 10.7763/IPCSIT.2014.V59.2.

[15] Alqahtany, Saad &Alkhodre, Ahmad & Al Abdulwahid, Abdulwahid &Alohaly, Manar. (2023). A Dynamic Multi-Layer Steganography Approach Based on Arabic Letters' Diacritics and Image Layers. Applied Sciences. 13. 7294. 10.3390/app13127294.

[16] Naik, Vaibhavi & Fernandes, Dr. (2022). Audio Steganography. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 196-201. 10.32628/CSEIT5228368.

[17] Firman Ashari, Ilham. (2022). The Evaluation of Audio Steganography to Embed Image Files Using Encryption and Snappy Compression. Indonesian Journal of Computer Science. 11. 318-336. 10.33022/ijcs.v11i2.3050.

[18] ASLANTAŞ, Funda & HANİLÇİ, Cemal. (2022). Comparative Analysis Of Audio Steganography Methods. Journal of Innovative Science and Engineering (JISE). 6. 10.38088/jise.932549.

[19] Li, Jing & Wang, Kaixi& Jia, Xiaozhu. (2023). A Coverless Audio Steganography Based on Generative Adversarial Networks. Electronics. 12. 1253. 10.3390/electronics12051253.

[20] Alanzy, May &Alomrani, Razan & Alqarni, Bashayer& Almutairi, Saad. (2023). Image Steganography Using LSB and Hybrid Encryption Algorithms. Applied Sciences. 13. 11771. 10.3390/app132111771.

[21]Ros, Jaume & Geleta, Margarita & Pons, Jordi &Giró-i-Nieto, Xavier. (2023). Towards Robust Image-in-Audio Deep Steganography. 10.48550/arXiv.2303.05007.

[22] Zhang, Chunhu (2022). Coverless Video Steganography Based on Audio and Frame Features. Security and Communication Networks 10.1155/2022/1154098.

[23] Shang, Fei (2023). Toward High Capacity and Robust JPEG Steganography Based on Adversarial Training. Security and Communication Networks.10.1155/2023/3813977.

[24] Rashmi, S.. (2023). Implementation of Image Steganography and Combination of Cryptography and Steganography. 10.4018/978-1-6684-9317-5.ch014.

[25] Rani, Rajneesh & Singh, Samayveer. (2022). A survey of recent advances in image steganography. Security and Privacy. 6. 10.1002/spy2.281.

[26] Khodher, Maisa'A& Khairi, Teaba. (2020). Review: A comparison Steganography Between Texts and Images. Journal of Physics: Conference Series. 1591. 012024. 10.1088/1742-6596/1591/1/012024.

[27] Ramadoss, Janarthanan (2022). A Three-Dimensional Autonomous System with a Parabolic Equilibrium: Dynamical Analysis, Adaptive Synchronization via Relay Coupling, and Applications to Steganography and Chaos Encryption. Complexity 10.1155/2022/8362836.

[28] Jain, Jaishree (2022). Securing E-Healthcare Images Using an Efficient Image Encryption Model. Scientific Programming 10.1155/2022/6438331.

[29] Hao, Chaolong& Yang, Xukui& Ma, Quangong& Qu, Dan & Wang, Ran & Zhang, Tao. (2023). Quantum Audio LSB Steganography with Entanglement-assisted Modulation. 10.21203/rs.3.rs-3366077/v1.

[30] Guan, Bo (2022). A Novel Coverless Text Steganographic Algorithm Based on Polynomial Encryption. Security and Communication Networks 10.1155/2022/1153704.

[31] Thabit, R.; Udzir, N.I.; Yasin, S.M.; Asmawi, A.; Roslan, N.A.; Din, R. A Comparative Analysis of Arabic Text Steganography. Appl. Sci. 2021, 11, 6851. https://doi.org/10.3390/app11156851

[32] J. Sharafi, Y. Khedmati, M.M. Shabani, Image steganography based on a new hybrid chaos map and discrete transforms, Optik, Volume 226, Part 2, 2021, 165492, ISSN 0030-4026, https://doi.org/10.1016/j.ijleo.2020.165492.

[33] K. Manjunath, G.N. Kodanda Ramaiah, M.N. GiriPrasad,Backward movement oriented shark smell optimization-based audio steganography using encryption and compression strategies, Digital Signal Processing, Volume 122, 2022, 103335, ISSN 1051-2004, https://doi.org/10.1016/j.dsp.2021.103335.

[34] Rui Wu, Suo Gao, Xingyuan Wang, Songbo Liu, Qi Li, Uğur Erkan, Xianglong Tang, AEA-NCS: An audio encryption algorithm based on a nested chaotic system, Chaos, Solitons & Fractals, Volume 165, Part 1, 2022, 112770, ISSN 0960-0779, https://doi.org/10.1016/j.chaos.2022.112770.[1].