VLSI IMPLEMENTATION OF SPEECHSTEGANOGRAPHY WITH ADVANCEDWAVELET TRANSFORMS

Dohan Goud.CH[1],Durga Prasad.G [2],Mani Ratnam.P[3],Venkanna.M [4]
[1,2,3] UG Scholar, Dept.of ECE, St. Martin's Engineering College, Secunderabad, Telangana, India-500100
[4]Associate Professor, Dept.of ECE, St. Martin's Engineering College, Secunderabad, Telangana, India-500100
dohangoud123@gmail.com

Abstract:

The integration of speech steganography with advanced wavelet transforms presents a promising avenue for secure communication in an increasingly digital world. Current statistics indicate that the global speech recognition market is expected to reach $26.79 billion by 2025, highlighting the growing reliance on voice-based technologies. Despite these advancements, existing frequency-based approaches, such as Fast Fourier Transform (FFT), face significant challenges, including susceptibility to noise and inefficiencies in handling time-frequency localization, which hinder their effectiveness in speech steganography applications.In this work, we propose a novel VLSI implementation utilizing Discrete Wavelet Transform (DWT) in conjunction with a Ripple Carry Adder (RCA) and an array multiplier to enhance the robustness and efficiency of speech steganography systems. DWT offers superior time-frequency localization capabilities, allowing for more precise embedding of secret information within speech signals without compromising audio quality. The integration of RCA and array multipliers enables efficient data processing and extraction, leading to enhanced performance in steganographic applications. This innovative approach not only improves the concealment of information within speech but also provides a framework for efficient data processing, addressing the limitations of traditional FFT-based methods.

1. INTRODUCTION

Speech steganography hides message data within cover speech without degrading its quality. Audio steganography modifies an audio signal to transmit hidden information undetectably. The original and stego messages retain similar characteristics, making detection difficult. Embedding secret messages in digital sound is complex, with various techniques developed for secure transmission. Unlike images, audio steganography leverages human auditory system (HAS) features such as a wide hearing range. Unlike cryptography, which encrypts messages, steganography conceals their existence by embedding them in a medium, ensuring secrecy from intruders while maintaining the original message's integrity.

Steganography, cryptography, and obfuscation are three related terms; they all refer to practices that make data more difficult to understand. However, these words are not interchangeable subtle, yet crucial distinctions exist between them.

Cryptography attempts to encode a message, making it difficult or impossible for anyone except the intended recipient to message and its encrypted version.

Steganography attempts to hide a message within another object. Not only does steganography seek to make this information harder to understand, but it also seeks to Obfuscation is any technique that prevents third parties from understanding a message. For example, a program's source code was obfuscated by removing the whitespace, making the message difficult for humans to read.

2. LITERATURE SURVEY

The Abood et al. [1] developed a compressive sensing-based system that efficiently compresses and encrypts audio signals. The method segments audio signals into matrices, multiplying them with a Gaussian-generated sensing matrix. Reconstruction is achieved via the Moore-Penrose pseudo-inverse. Their system reduced audio size by 28% while maintaining high fidelity, achieving a correlation of 0.98-0.99. Performance metrics such as MSE, PSNR, and SSIM indicated minimal distortion. Additionally, the encryption process ensured data security, addressing prior challenges in balancing compression and security. The results suggest this approach significantly improves storage efficiency and secure transmission of sensitive audio data.

Mawla et al. [2] proposed a cryptographic approach leveraging biological data, using protein bases to generate encryption keys twice the length of the plaintext. Data was encrypted via arithmetic operations and logic gates, ensuring high randomness. The encrypted data was then hidden within protein chains, distributing fragments in a non-detectable manner. This method enhanced security by making statistical analysis ineffective for detecting hidden data. By combining cryptography and steganography in a novel biological framework, the study introduced a robust means of protecting sensitive information from unauthorized access in an evolving cybersecurity landscape.

Mohammad Gauhar et al. [3] explored reversible image steganography, embedding secret data into image pixels while ensuring lossless recovery of the original image. Their research focused on optimizing Peak Signal-to-Noise Ratio (PSNR) and embedding capacity, comparing various reversible image steganography techniques. They analyzed methods that balanced compression, encryption, quality, and robustness, ensuring high imperceptibility and minimal computational complexity. Their study concluded that improved steganographic techniques enhance security while maintaining image quality, making them suitable for secure communications and data hiding applications.

Roselinkiruba et al. [4] introduced a video steganography method utilizing edge-based moving object detection, compression, and encryption. Their approach applied rank approximation and prediction error for frame compression, followed by encryption using threshold and pixel value differencing (PVD). Moving objects underwent pixel shuffling, while non-moving areas used circular shift encryption. Data hiding leveraged weight-based interpolation, distributing hidden information across RGB channels. Experimental results demonstrated improved compression, object identification, and security, with high PSNR and robustness against RS and PVD histogram attacks. Their technique significantly outperformed existing video steganography approaches in imperceptibility and embedding efficiency.

Christy Atika et al. [5] examined the effectiveness of Fibonacci sequences in cryptographic steganography. Their study compared encrypted images using Fibonacci-generated keys with those encrypted traditionally. The Fibonacci sequence enhanced randomness in key generation, improving security. Performance was evaluated using metrics like PSNR, UACI, and NPCR. The highest PSNR was observed in a 512x512 grayscale image, while UACI and NPCR exceeded 49% and 99%, respectively. Their findings confirmed that Fibonacci-based encryption improved data security without significantly degrading image quality, offering a novel approach to securing sensitive data in digital communications.

Zolfaghari et al. [6] explored the dual role of neural networks in cryptanalysis, depicting them as both attackers and defenders in cybersecurity. Neural networks were used to break encryption algorithms and to strengthen cryptographic security. Their study highlighted a lack of comprehensive research on how AI interacts with cryptosystems, addressing gaps by analyzing adversarial and cooperative roles. Their findings emphasized the growing need to integrate machine learning in cryptographic applications, balancing its potential to enhance security while mitigating risks posed by AI-driven attacks.

Xue et al. [7] addressed domain mismatch issues in linguistic steganalysis by proposing a cross-domain adaptation framework. Their novel approach introduced a steganographic domain distance metric (SDDM) to quantify distribution discrepancies in training and testing data. Additionally, an adaptive weight selection network improved model robustness against diverse linguistic steganography methods. Experiments demonstrated state-of-the-art detection performance in cross-domain scenarios, highlighting the method's effectiveness in identifying hidden information within text-based steganography, even when datasets differed in distribution.

Noorallahzadeh et al. [8] focused on reversible logic synthesis in quantum computing, emphasizing parity-preserving reversible circuits for fault detection. Their study introduced six optimized parity-preserving blocks, synthesized using multiple-control Toffoli (MCT) gates and later optimized using elementary quantum gates. The proposed full-adder and multipliers exhibited lower quantum cost compared to existing designs. Their approach improved fault tolerance and efficiency, contributing to the advancement of quantum circuit design for future computing applications.

Roselinkiruba et al. [9] proposed a data hiding method in wireless networks using moving object detection and feature extraction. Their technique encrypted hidden data using a binary tree structure (BTS), ensuring secure transmission. The approach improved embedding capacity, PSNR, and security analysis, outperforming conventional data hiding techniques. Their method provided an enhanced balance between imperceptibility and robustness, making it suitable for secure communications in modern wireless environments.

Hazzazi et al. [10] introduced a Turbo Code-based encryption algorithm for secure communications in high-risk environments. Their approach utilized a secret key-controlled puncturing process within Turbo encoding, enhancing data protection. Key generation relied on pre-existing data, eliminating the need for secure key exchanges. Encryption was further reinforced using recurrence relations and LU decomposition. The proposed method demonstrated superior security and error correction capabilities compared to traditional cryptographic techniques.

Al Hadad et al. [11] explored digital image steganography, emphasizing its importance in modern security systems. Their study reviewed methods balancing quality and capacity in steganographic techniques, highlighting its role in secure communication. They discussed the increasing demand for robust steganographic methods as data security concerns grow.

Gutub et al. [12] addressed audio watermarking challenges by proposing a counting-based secret sharing strategy. Their method ensured ownership authentication even when audio files underwent slight modifications. Their experiments analyzed hiding capacity and PSNR security, showing promising results in watermark robustness and copyright protection.

Evsutin et al. [13] classified speech steganography methods for cyber-physical systems, identifying four primary data embedding approaches. Their study emphasized the need for secure communication in these systems, differentiating cyber-physical steganography from traditional digital steganography and watermarking.

Semenov et al. [14] developed a stegano-graphic encryption model for UAV communication, focusing on ADS-B data security. Their approach incorporated the Chinese Remainder Theorem and Finite Integra Ring Theorem, enhancing data protection in unmanned aerial vehicle operations.

Hosny et al. [15] reviewed multimedia encryption techniques, evaluating cryptographic schemes for securing digital images, videos, and audio. Their survey analyzed existing encryption methods, contributing to the development of more effective and secure multimedia protection strategies.

Alwen et al. [16] introduced an image encryption technique combining the Rabbit Algorithm with Aizawa's chaotic attractor. Their method enhanced security by leveraging the unpredictability of chaotic maps, improving encryption performance based on PSNR, entropy, and correlation coefficient analysis.

Kolivand et al. [17] provided a comprehensive review of image encryption, focusing on chaos-based techniques. They explored full and selective encryption methods, emphasizing their applications in securing images transmitted over the internet.

.3. PROPOSED METHODOLOGY

Speech steganography is an interesting field that merges the realms of information security and audio processing. At its core, it involves hiding sensitive information within audio signals to ensure covert communication. Unlike traditional encryption methods, which focus on encoding data to prevent unauthorized access, speech steganography delves into the realm of hiding information in plain auditory sight. This concealed technique poses unique challenges and opportunities, pushing the boundaries of covert communication in an increasingly interconnected world.

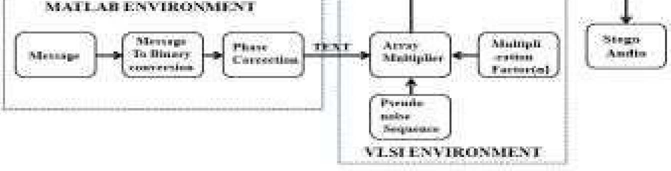


Figure 1: Proposed System

STEP-1: In the proposed stego system, the initial step involves the examination of the audio signal, particularly analyzing its properties to ensure accurate processing. Let us consider the audio signal and read the audio signal. STEP-2: The discrete wavelet transform (DWT) is applied to the input audio signal, facilitating the generation of the Low-Low (LL) Band. The LL Band is planned, as it eliminates the interference from high-frequency components present in other bands such as HH, HL, and LH. By separating the LL Band, which closely approximates the input data, the system ensures a robust foundation for embedding the user-defined message. And generate the Low-Low (LL) Band Contains the low-frequency components of the signal.Avoid remaining bands like HH, HL, LH Bands because these bands consist high frequency components.STEP-3: Consider the user-defined input message, such as the friendly greeting "Hi" or "Hello," the system smoothly moves to the next stage of operation. Once the LL Band is extracted from the audio signal, the system exactly integrates the provided message, regardless of its length or complexity. This adaptability ensures that whether the user chooses for a short greeting or a more elaborate phrase, such as "Electronics and communication engineering" the system can readily accommodate it, adjusting its mechanisms accordingly.The approach lies in its flexibility, which not only improves the user experience but also include the system's adaptability in meeting diverse communication needs. By smoothly handling messages of varying lengths and complexities, the system demonstrates its capacity to provide a wide range of user preferences and requirements.Whether it's a brief exchange or a more detailed conversation, the system stands ready to encode the message within the LL band with accuracy and efficiency, by embedding the message within the LL Band.The system employs a reliable method of steganography smoothly combine the user's communication into the structure of the audio signal while maintaining its integrity, the system's reliability and effectiveness in covert communication. As such, users can rest certain messages are transmitted securely. The system not only facilitates covert communication but also encourage trust and confidence in its capabilities.STEP-4: In data communication, ASCII (American Standard Code for Information Interchange) is a widely used character encoding standard that represents text in computers and other devices. ASCII uses a 7-bit binary code to represent each character, allowing for a total of 128 different characters including letters, numbers, punctuation marks, and control characters. However, with the initiation of extended ASCII, which uses 8 bits, an additional 128 characters was represented, allowing for a wider range of symbols and characters to be encoded. When transmitting data, especially over digital communication channels, it is often necessary to convert textual information into binary form.

This conversion involves representing each character in the message as a series of 0s and 1s according to its ASCII code. For instance, the ASCII code for the letter 'A' is 65, which in binary are 01000001. Similarly, each character in the message is converted into its corresponding binary representation, resulting in a stream of digital data that was easily transmitted and understood by digital systems.By converting text into binary, digital data is generated as output, which was efficiently transmitted and processed by computers and digital devices. This binary representation of data ensures reliable communication and facilitates the exchange of information between different systems, regardless of the specific hardware or software being used.Moreover, ASCII's simplicity and universality make it a fundamental aspect of modern computing and data communication, serving as a standard encoding scheme for textual information across various platforms and applications.

STEP-5: In the event of phase mismatches occurring during data transmission, it becomes necessary to implement corrective measures to ensure the integrity of the communication. One such method involves the utilization of a phase constant represented by the imaginary unit 'j'. When a phase difference is detected, the digital signal undergoes multiplication by this phase constant 'j' to address the mismatch. This corrective action serves to adjust the phase of the transmitted data, mitigating any possible distortions or errors that occur due to phase misalignment.By incorporating the phase constant 'j' into the transmission process, the system effectively compensates for phase discrepancies, thereby enhancing the reliability and accuracy of data exchange. The multiplication operation with 'j' enables precise adjustment of the phase, ensuring that the transmitted signal aligns correctly with the intended phase reference.This corrective mechanism is particularly critical in applications where precise phase synchronization is top, such as in telecommunications, digital signal processing, and wireless communication systems. Implementing multiplication with the phase constant 'j' in response to phase mismatches enables smooth data transmission and reception, even in the presence of phase distortions or variations. This adaptive approach to phase correction enhances the robustness and flexibility of digital communication systems, enabling them to maintain optimal performance under varying conditions. By effectively compensating for phase misalignments, the system ensures that transmitted data remains coherent and accurate, so facilitating efficient and dependable communication across diverse environments and scenarios.STEP-6: To convert step-2 and step-5 into digital text data files, you first segment each step's content into its respective file. In Step-2, the focus is on applying the discrete wavelet transform (DWT) to an audio signal, generating the Low pass Low (LL) Band, which is chosen to eliminate interference from high-frequency components in other bandslike HH, HL, and LH.STEP-7: Converting these steps into digital text files involves maintaining their content exact in separate files, Step-2.txt and Step-5.txt, for easy access and reference in digital format. And also read the text data files.

STEP-8: After reading the text data files, the next step involves performing multiplication between the output obtained from step-5, the pseudo-random sequence, and a multiplication factor denoted as "α." This process aims to apply a specific mathematical operation to combine the information extracted from step-5 with the pseudo-random sequence, scaled by the multiplication factor α.By executing this multiplication operation, the resulting data set will incorporate the characteristics of both the step-5 output and the pseudo-random sequence, adjusted by the determined factor α. It increment the no. of bits and the steganography process is completely depends upon the multiplication factor STEP-9: Performing addition between the output of the Discrete Wavelet Transform (DWT) and the output of a multiplier involves combining the results obtained from these two processes to generate a combined dataset. The DWT output typically represents the transformed signal containing information about different frequency components or features, while the multiplier output represents the result of a specific multiplication operation, which involve scaling or adjusting the original data. This addition operation allows for the integration of diverse processing stages or techniques enable the creation of more complicated and modified solutions in various fields such as signal processing, image processing, and data analysis.STEP-10: After all these create output text files.STEP-11: The process of converting text files into stego audio involves several steps. Initially, the content of the text files is extracted and prepared for encoding. This embedding process involve modifying certain properties of the audio signal, such as amplitude or frequency, to contain the hidden information. Once the text data is successfully encoded into the audio waveform, a stego audio file is generated as the output.

Applications:

- **Secure Military & Intelligence Communication**: Enables covert transmission of sensitive information through audio signals, ensuring secure military and intelligence communications without detection.
- **Confidential Corporate Communication;** Protects confidential business data by embedding secret messages within speech signals, preventing unauthorized access or industrial espionage.
- **Medical Data Embedding in Telemedicine;** Facilitates secure storage and transmission of sensitive

patient records, biometric data, or medical reports within audio communications in telemedicine applications.

- **Anti-Piracy & Digital Watermarking;** Embeds hidden security information in audio files to prevent unauthorized reproduction, ensuring copyright protection for digital media and intellectual property.
- **Forensic & Law Enforcement Applications;** Assists in forensic investigations by embedding crucial evidence in covert audio messages, allowing secure communication between law enforcement agencies.

4. EXPERIMENTAL ANALYSIS

Fig. 2 depicts the original data results obtained from the proposed system. This graph serves as a baseline, illustrating the quality of the data before any embedding or extraction processes take place.

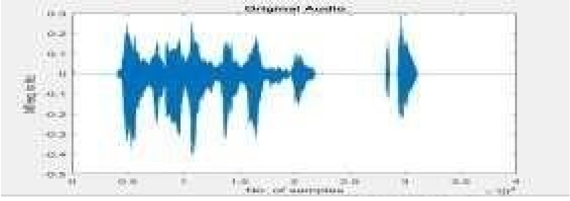


Figure 2: Original Data Results

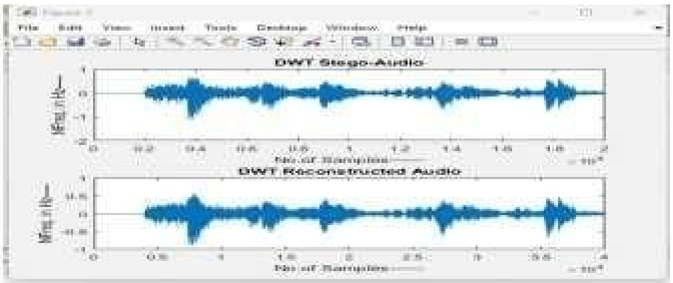
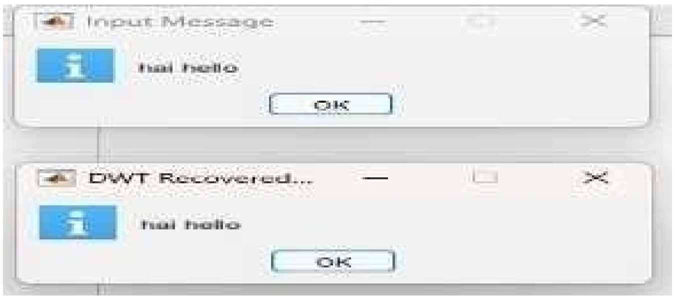


Figure 3: Extracted Data Results



Input Message

hai hello

OK

DWT Recovered...

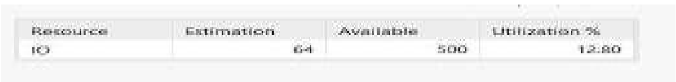
hai hello

OK

Figure 4: Proposed System Results Comparison

VLSI RESULTS:

Figure 5: Simulation Results

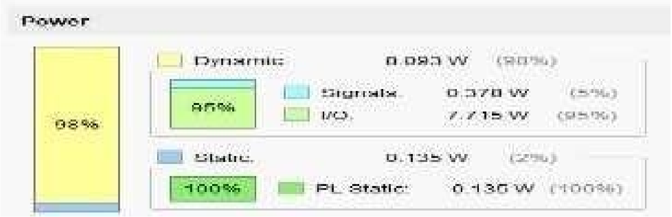


Resource	Estimation	Available	Utilization %
IO	64	500	12.80

Figure 6: Area Results

Figure 3 showcases the extracted data results from the proposed system, emphasizing the accuracy of the data extraction process. The graph aims to demonstrate that the proposed system performs more effectively in recovering the original data from the stego audio, potentially addressing the issues observed in the existing system.

Figure 4 provides a comprehensive comparison of the results between the existing system and the proposed system. This visual representation aims to highlight the improvements achieved byte proposed system in terms of data embedding, extraction, and overall system performance, emphasizing the potential advancements in steganographic techniques using the FFT method. Figure 5 , the VLSI results are presented, starting with Figure 7.6, which depicts the simulation outcomes. This figure provides a visual representation of the performance of the VLSI system, capturing various aspects such as area, power, and delay.



Power

98%

Dynamic: 0.093 W (98%)

85%

Signals: 0.378 W (5%)

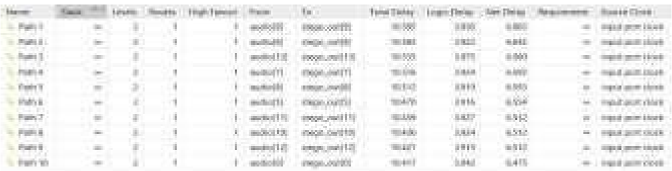
I/O: 7.715 W (95%)

Static: 0.135 W (2%)

100%

PL Static: 0.135 W (100%)

Figure 7: Power Results



Name	Slack	Levels	Routes	High Fanout	From	To	Total Delay	Logic Delay	Net Delay	Requirement	Source Clock
Path 1	∞	2	1	1	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	∞	input port clock
Path 2	∞	2	1	1	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	∞	input port clock
Path 3	∞	2	1	1	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	∞	input port clock
Path 4	∞	2	1	1	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	∞	input port clock
Path 5	∞	2	1	1	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	∞	input port clock
Path 6	∞	2	1	1	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	∞	input port clock
Path 7	∞	2	1	1	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	∞	input port clock
Path 8	∞	2	1	1	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	∞	input port clock
Path 9	∞	2	1	1	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	∞	input port clock
Path 10	∞	2	1	1	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	∞	input port clock

Figure 8: Delay Results

Metric	Existing	Proposed
Mean square error	334.9221	1.1022
Signal-to-Noise Ratio	0.0002	21.1468
Total Harmonic Distortion	21.2641	0.0335
Correlation Coefficient	0.0026	0.0873

Table 1: Audio Processing Metrics Comparison

Metric	Existing	Proposed
IO	85	64
Total Power	100	98
Delay	20.97	10.595
Signal power	8.95	0.378
Dynamic power	5.34	0.135
PL Static power	8.85	0.135

Table 2: VLSI Metrics Comparison

Figure 6 provides precise information regarding the area results, offering valuable insights into the spatial demands of the VLSI implementation. Figure 7 , the focus is on power outcomes, offering a visual print of crucial metrics about power usage in the VLSI system.

Figure 8 displays delay results such as total delay, logic delay, and net delay values, as reported by the software.

Table 1 provides a comparison of audio processing metrics between the existing and proposed systems. The mean square error (MSE) is significantly reduced in the proposed system, indicating improved accuracy in reproducing the audio signal. Table 2 presents a comparative analysis of VLSI metrics between the existing and proposed systems. In terms of input/output (IO), the proposed system shows a reduction from 85 to 64, indicating potential efficiency gains.

5. CONCLUSION

The Speech steganography is a powerful tool for secret communication, authorizing the hiding of secret messages within speech signals. One common technique involves using the (FFT) to manipulate the frequency domain of speech signals, allowing for the embedding of messages by adjusting the magnitudes of frequency components in each frame. However, FFT-based methods have limitations, such as sensitivity to alterations in the time domain and vulnerability to compression, which can affect speech quality and security. Despite these challenges, FFT-based speech steganography remains a valuable method for hiding information within speech signals.The proposed stego system introduces a new approach using the discrete wavelet transform (DWT) to generate the Low-Low (LL) Band, which eliminates high-frequency interference and provides a robust foundation for embedding messages of varying lengths and complexities. This system Expresses adaptability and flexibility in covert communication, accepting user-defined messages while ensuring the integrity of the audio signal. By combining information security and audio processing, speech steganography offers a unique method for secure communication that hides information in basic audio sight, presenting both challenges and opportunities for further development. Speech steganography differs from encryption by concealing data within audio signals however; this approach requires careful manipulation of audio signal properties to ensure that embedded messages remain undetectable to human listeners. Advances in signal processing and machine learning have enhanced the efficiency and security of speech steganography, but concerns about mishandling and detection efforts continue.

REFERENCES

[1] Abood, Enas Wahab, Zaid Alaa Hussien, Haifaa Assy Kawi, Zaid Ameen Abduljabbar, Vincent Omollo Nyangaresi, Junchao Ma, Mustafa A. Al Sibahee, Ali Kalafy, and Saad Ahmad. "Provably secure and efficient audio compression based on compressive sensing." International Journal of Electrical & Computer Engineering (2088-8708) 13, no. 1 (2023).

[2] Mawla, Noura A., and Hussein K. Khafaji. "“Three Layered Model for Audio Steganography." Computers 12, no. 8 (2023).

[3] Nayab, Mohammad Gauhar, Aditya Pratap Singh, Ritik Sharma, and Gaurav Raj. "Reversible Image Steganography to Achieve Effective PSNR." In International Conference on Information Technology, pp. 145-156. Singapore: Springer Nature Singapore, 2023.

[4] Roselinkiruba, R., T. Sree Sharmila, and JK Josephine Julina. "An efficient Moving object, Encryption, Compression and Interpolation technique for video steganography." Multimedia Tools and Applications (2024).

[5] Sari, Christy Atika, Muhammad Hafizh Dzaki, Eko Hari Rachmawanto, Rabea Raad Ali, and Mohamed Doheir. "High PSNR Using Fibonacci Sequences in Classical Cryptography and Steganography Using LSB." International Journal of Intelligent Engineering & Systems 16, no. 4 (2023).

[6] Zolfaghari, Behrouz, Hamid Nemati, Naoto Yanai, and Khodakhast Bibak. "The Dichotomy of Crypto and NN: War and Peace." An audio steganography by a low-bit coding method with wave files, pp. 15-39. Cham: Springer Nature Switzerland, 2023.

[7] Xue, Yiming, Jiaxuan Wu, Ronghua Ji, Ping Zhong, Juan Wen, and Wanli Peng. "Adaptive domain-invariant feature extraction for cross-domain linguistic steganalysis." “Audio Steganography using LSB” (2023).

[8] Noorallahzadeh, Mojtaba, Mohammad Mosleh, and Kamalika Datta. "“Data Hiding Technique: Audio Steganography using LSB Technique." Frontiers of Computer Science 18, no. 6 (2024): 186908.

[9] Roselinkiruba, R., and G. Bhuvaneshwari. "Feature extraction-based pixel segmentation techniques data hiding and data encryption." Multimedia Tools and Applications (2023): 1-18.

[10] Hazzazi, Mohammad Mazyad, Raja Rao Budaraju, Zaid Bassfar, Ashwag Albakri, and Sanjay Mishra. "A Finite State Machine-Based Improved Cryptographic Technique." Mathematics 11, no. 10 (2023): 2225.

[11] Al Hadad, Zeina, and Ibtisam Hassoun Ali. "Survey in Image and Audio Steganography by using the Deep Learning Methods." Journal of Kufa for Mathematics and Computer 10, no. 2 (2023): 132-139.

[12] Gutub, Adnan. "Regulating watermarking semi-authentication of multimedia audio via counting-based secret sharing." Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi 28, no. 2 (2022): 324-332.

[13] Evsutin, Oleg, Anna Melman, and Ahmed A. Abd El-Latif. "Overview of information hiding algorithms for ensuring security in IoT based cyber-physical systems." Security and Privacy Preserving for IoT and 5G Networks: Techniques, Challenges, and New Directions (2022): 81-115.

[14] Semenov, Serhii, Minjian Zhang, O. O. Mozhaiev, N. H. Kuchuk, S. A. Tiulieniev, Yu V. Hnusov, M. O. Mozhaiev, V. M. Strukov, Yu M. Onyshchenko, and H. A. Kuchuk. "Construction of a model of steganographic embedding of the UAV identifier into ADS-B data." (2023).

[15] Hosny, Khalid M., Mohamed A. Zaki, Nabil A. Lashin, Mostafa M. Fouda, and Hanaa M. Hamza. "Multimedia Security Using Encryption: A Survey." IEEE Access (2023).

[16] Alwan, Mohammed Gheni, Ekhlas Falih Naser, and Enas Tariq Khudair. "A Hybrid Algorithms Based on the Aizawa Attractor and Rabbit-Lightweight Cipher for Image Encryption." Iraqi Journal of Science (2023): 6534-6547.

[17] Kolivand, Hoshang, Sabah Fadhel Hamood, Shiva Asadianfam, and Mohd Shafry Rahim. "Image encryption techniques: A comprehensive review." Multimedia Tools and Applications (2024): 1-36.

[18] Abdirahman, Abdullahi Ahmed, Abdirahman Osman Hashi, Ubaid Mohamed Dahir, Mohamed Abdirahman Elmi, and Octavio Ernest Romo Rodriguez. "Concealed Data Exchange via Temperature Manipulation in FPGA Systems." International Journal of Electrical and Electronics Engineering 10, no. 8 (2023): 127-136.