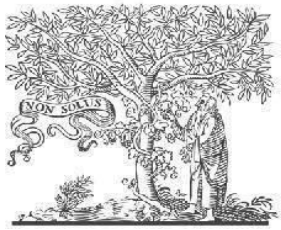
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT



ELSEVIER SSRN

IJIEMR Transactions, online available on 31th Jan 2021. Link

https://ijiemr.org/downloads.php?vol=Volume-10&issue= Issue01

DOI:10.48047/IJIEMR/V10/ ISSUE01/72

Title: " DESIGN AND VLSI IMPLEMENTATION OF ENHANCED SPEECH STEGANOGRAPHY BASED ON ADVANCED WAVELET TRANSFORM"

Volume 10, ISSUE 01, Pages: 366- 374

Paper Authors
Durgaprasad Anagandula, Kurva Chaithanya, Senthil Kumar Murugesan

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper as Per UGC Guidelines We Are Providing A ElectronicBar code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

DESIGN AND VLSI IMPLEMENTATION OF ENHANCED SPEECH STEGANOGRAPHY BASED ON ADVANCED WAVELET TRANSFORM

Durgaprasad Anagandula, Kurva Chaithanya, Senthil Kumar Murugesan

Department of Electronics and Communication Engineering, Sree Dattha Group of Institutions, Sheriguda, Hyderabad, Telangana.

ABSTRACT

The incorporation of sophisticated wavelet transforms into speech steganography systems has emerged as a potentially fruitful avenue in the field of secure communication systems. The protection of personal information in telecommunication networks, the secure transmission of sensitive information in military communications, and the secret exchange of data in corporate contexts are all examples of the importance of data communications security. On the other hand, the system that is now in place makes use of traditional methods of speech steganography, which need the utilization of fundamental encryption strategies and straightforward embedding algorithms. However, despite their functionality, these systems are not robust and do not adequately disguise secret data within speech signals. As a result, they are susceptible to detection and interception without adequate protection. For this reason, the method that has been presented makes use of sophisticated wavelet transformations in order to improve the safety and effectiveness of voice steganography. The system is able to achieve greater embedding capacity while maintaining perceptual transparency because it makes use of the capabilities of wavelets to perform analysis at several resolutions. In addition, the utilization of dynamic embedding methods that are founded on wavelet coefficients guarantees adaptability to a wide range of signal characteristics, hence boosting resistance against attacks and interference from noise. As a result of the VLSI implementation of this system, which maximizes resource consumption and computational efficiency, it is suited for use in real-time applications inside communication systems.

Keywords: Speech steganography, Wavelet transforms, secure communication systems, Robustness, VLSI implementation, Real-time applications

1. Introduction

Speech steganography is a process of hiding the message data into a cover speech without degrading the quality of cover speech. Audio Steganography is a technique used to transmit hidden information by modifying an audio signal in an undetectable manner It is the science of hiding some secret text or audio information in a host message. The host message before steganography and stego message after steganography have the same characteristics. Embedding secret messages in digital sound is a more difficult process. Varieties of techniques for embedding information in digital audio have been established. Audio steganography is an approach of hiding information within an audio signal. As data is embedded in the signal, it gets changed. This modification should be creating interchangeable to the human ear. Image can also be taken as a medium, but audio steganography is more impressive because of the features of Human Auditory System (HAS) like large power, powerful range of hearing and high range of audible frequency. Cryptography includes the encryption of message. It creates no attempt to conceal the encrypted message. In steganography, the original message is not

changed but the very continuation is secret from the intruder by embedding the message in the selected medium.

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 decrypt it. The encoding and decoding process is accomplished using cryptographic keys that translate back and forth between the true 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 conceal that a message is being sent in the first place. Obfuscation is any technique that prevents third parties from understanding a message. For example, a program's source code may be obfuscated by removing the whitespace, making the message difficult for humans to read.

In the Domain of VLSI implementation for speech steganography, a comprehensive literature survey is indispensable to navigate the complicated landscape of existing research and innovations. Speech steganography, the art of concealing secret information within speech signals, has garnered increasing attention owing to its potential applications in secure communication and data transmission. The literature survey serves as a foundational exploration, delving into the excess of studies that have paved the way for advancements in this specialized field. Additionally, it examines recent breakthrough in hardware implementation, cracking light on advancements in the design and optimization of VLSI circuits for efficient and secure speech steganography applications. Through this literature survey, a comprehensive understanding of the evolving landscape emerges, providing a valuable foundation for researchers and engineers in their pursuit of cutting-edge developments in VLSI-based speech steganography

2. Literature Survey

Abood, et.al [1] designed the advancement of systems with the capacity to compress audio signals and simultaneously secure was a highly attractive research subject. This was because of the need to enhance storage usage and speed up the transmission of data, as well as securing the transmission of sensitive signals over limited and insecure communication channels. Mawla, et.al [2] suggested that the increase in cyber-attacks, hacking, and data theft, maintaining data security and confidentiality became of paramount importance. They highlighted several techniques used in cryptography and steganography to ensure the safety of information transferred between two parties without interference from an unauthorized third party. Mohammad Gauhar, et.al [3] implemented the Image Steganography is one of the most well-known methods where top-secret data is embedded into the pixels of an image by altering some of its pixel values. Reversible Image Steganography is used extensively due to its property of reconstructing the original cover image without any loss. Roselinkiruba, et.al [4] developed the Video steganography approach and has been widely used to preserve secret information while transmitting through the internet. This approach has become attractive among many researchers due to its feature high Embedding Capacity (EC).

Christy Atika, et.al [5] proposed the exchange of confidential information should be done in a secure environment. Therefore, security is needed if the exchange of information is carried out using Internet media. Zolfaghari, et.al [6] proposed that Neural Networks (NNs) play dual roles in cryptanalysis, acting as potential adversaries in attacks against encryption algorithms and encrypted data, creating a metaphorical "war" scenario. Xue, et.al [7] designed the Existing linguistic steganalysis methods required the training and testing datasets to be independent and identically distributed (i.i.d). However, in real-world scenarios, various types of text and steganography algorithms were employed to generate stegano graphic text, making it challenging to fulfill the requirement of independent and identical distribution between training and test datasets known as the domain mismatch problem, significantly diminished the detection performance. Noorallahzadeh, et.al [8] implemented the recent demonstration of quantum computers, interest in the field of reversible logic synthesis and optimization took a different turn. As every quantum operation is inherently reversible, there was immense motivation for exploring reversible circuit design and optimization. Roselinkiruba, et.al [9] Developed Data hiding, along with security, played a vital role in wireless networks. In recent years, techniques such as object detection, Feature Extraction (FE), and correlation-based methods were developed to predict suitable pixels for embedding.

Hazzazi, et.al [10] suggested the advent of several new means of communication, safeguarding the confidentiality of messages became more crucial. Financial institutions, virtual currencies, and government organizations were all examples of high-risk contexts where information exchanges needed particular care. Al Hadad, et.al [11] proposed the system Steganography was the practice of secretly encoding information into another medium (called a cover media) such that its existence could not be identified. Steganography was the method that was utilized to successfully do this task. Gutub, Adnan, et.al [12] designed the process of embedding specific data to prove ownership copyright authentication was needed whenever media files were used without proper permission being granted for authentication accuracy. Evsutin, et.al [13] suggested the speech steganography in Cyber-physical systems was one of the key technological trends in the modern world. However, its use was associated with the need to counter a variety of cyber threats. Semenov, et.al [14] implemented Secure data exchange in unmanned aerial vehicle management systems was an important aspect to prevent unauthorized access and ensure the security of aircraft. Hosny, et.al [15] developed, ensuring data confidentiality, authentication, integrity, and non-repudiation was crucial. Multimedia encryption-based security techniques became increasingly important as they allowed for the secure sharing of multimedia content on digital platforms. This survey aimed to review the state of secure and privacy-preserving encryption schemes applicable to digital multimedia, such as digital images, digital video, and digital audio.

3. Proposed Methodology

Figure 1 shows the proposed DWT based speech steganography. The detailed operation illustrated as follows

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, 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.

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, uses 8 bits, an additional 128 characters can be 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.

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 may occur due to phase misalignment.

STEP-6: To convert step-2 and step-5 into digital text data files, you would 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, is chosen to eliminate interference from high-frequency components in other bands like HH, HL, and LH.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

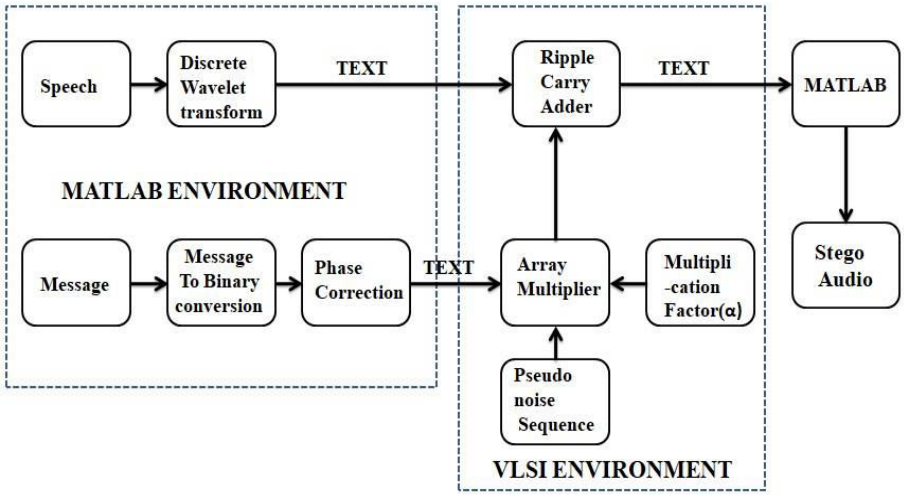


Figure 1: Proposed DWT based Speech Steganography.

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 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 increments the number of bits, and the steganography process is completely depending upon the multiplication factor

STEP-9: Performing addition between the output of the 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, may 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 may 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.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

4. Results and Discussion

Figure 2 shows the simulation results of the proposed speech steganography method, likely indicating its effectiveness in hiding information within speech signals. Figure 3 presents the area outcome of the proposed speech steganography method, possibly indicating the hardware resources required for its implementation. Figure 4 provides the power result of the proposed speech steganography method, showing the power consumption associated with the implementation. Figure 5 displays the delay outcome of the proposed speech steganography method, indicating any delays incurred during the processing.

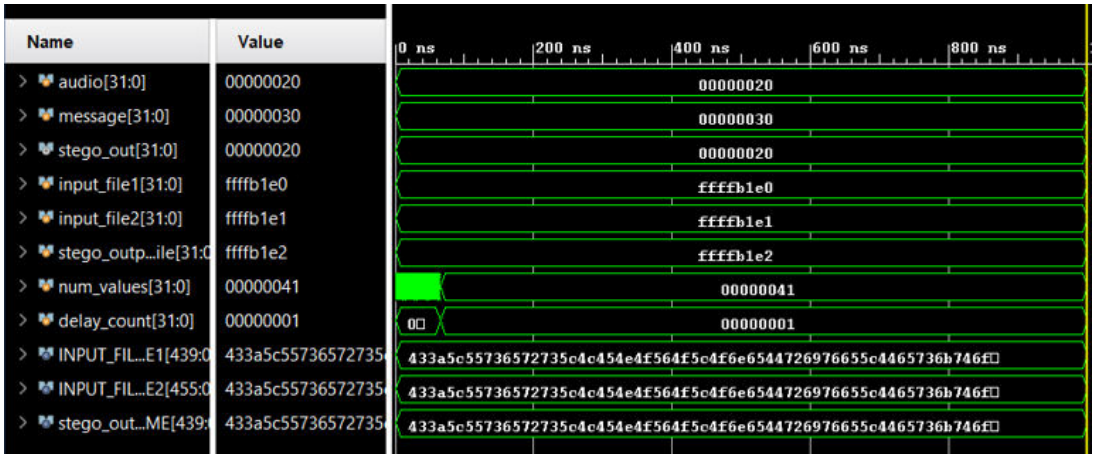


Figure 2: Proposed Simulation Result.

Resource	Estimation	Available	Utilization %
IO	64	500	12.80

Figure 3: Proposed Area Outcome.

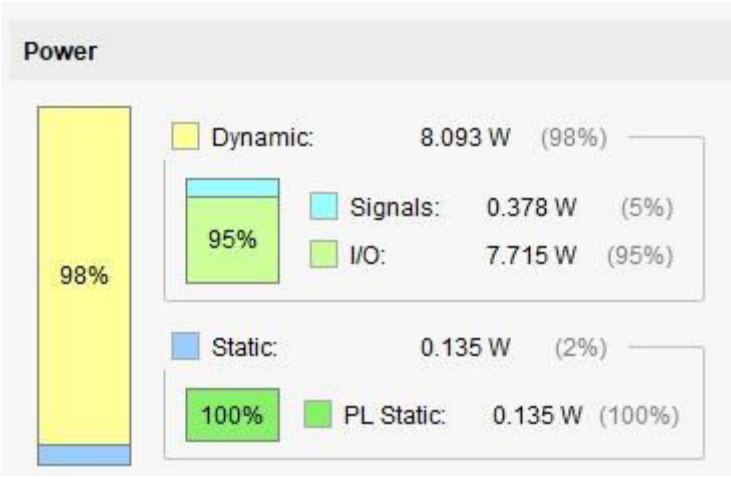


Figure 4: Proposed Power Result.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Name	Slack ^1	Levels	Routes	High Fanout	From	To	Total Delay	Logic Delay	Net Delay	Requirement	Source Clock
Path 1	∞	2	1	1	audio[9]	stego_out[9]	10.595	3.930	6.665	∞	input port clock
Path 2	∞	2	1	1	audio[6]	stego_out[6]	10.565	3.922	6.642	∞	input port clock
Path 3	∞	2	1	1	audio[13]	stego_out[13]	10.535	3.975	6.560	∞	input port clock
Path 4	∞	2	1	1	audio[7]	stego_out[7]	10.516	3.924	6.593	∞	input port clock
Path 5	∞	2	1	1	audio[8]	stego_out[8]	10.512	3.919	6.593	∞	input port clock
Path 6	∞	2	1	1	audio[5]	stego_out[5]	10.470	3.916	6.554	∞	input port clock
Path 7	∞	2	1	1	audio[11]	stego_out[11]	10.439	3.927	6.512	∞	input port clock
Path 8	∞	2	1	1	audio[10]	stego_out[10]	10.436	3.924	6.512	∞	input port clock
Path 9	∞	2	1	1	audio[12]	stego_out[12]	10.427	3.915	6.512	∞	input port clock
Path 10	∞	2	1	1	audio[0]	stego_out[0]	10.417	3.942	6.475	∞	input port clock

Figure 5: Proposed delay outcome.

Table 1 compares the performance of the existing and proposed speech steganography methods based on audio processing metrics such as mean square error, signal-to-noise ratio, total harmonic distortion, and correlation coefficient. The comparison suggests improvements in these metrics for the proposed method compared to the existing one, indicating better fidelity and effectiveness in hiding information in speech signals. Table 2 compares the VLSI metrics of the existing and proposed speech steganography methods, including IO (Input/Output) count, total power consumption, delay, signal power, dynamic power, and PL static power. The comparison suggests potential improvements in resource utilization, power efficiency, and delay characteristics for the proposed method compared to the existing one.

Table 1. Audio Processing Metrics Comparison of Existing and Proposed Speech Steganography Methods.

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 2.VLSI Metrics Comparison of Existing and Proposed Speech Steganography Methods.

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

5. Conclusion

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 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).