INTERNATIONAL JOURNAL OF RESEARCH AND SCIENTIFIC INNOVATION (IJRSI)
ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

Audio Steganography Using LSB

Bhagyalakshmi V [1]; Bhagyashree Parashuram Rajput [2]; Keerthana K M [3]; Madhushree B S [4]; Priya HU [5]

[1]Assistant Professor, Department of Electronics and Communication Engineering, Maharaja Institute of Technology Thandavapura, Nanjangud, Mysore, Karnataka, India

[2,3,4,5] Students Department of Electronics and Communication Engineering, Maharaja Institute of Technology Thandavapura, Nanjangud, Mysore, Karnataka, India

DOI: https://doi.org/10.51244/IJRSI.2026.1307000421

Received: 06 August 2026; Accepted: 11 August 2026; Published: 22 August 2026

ABSTRACT

Steganography enables the concealment of confidential information within a digital medium such that the presence of the hidden data is not easily detected. Audio files, especially WAV formats, provide suitable redundancy for embedding, making them ideal carriers for covert communication. This work presents a secure audio steganography system that combines an enhanced Least Significant Bit (LSB) scheme with AES–RSA hybrid encryption to improve confidentiality and resilience. The system encrypts the secret message using AES, secures the AES key with RSA, and then embeds the encrypted bits into the LSBs of audio samples without creating noticeable distortion. The proposed method ensures strong security, practical usability, and highly accurate message extraction.

Keywords: Audio Steganography, LSB Encoding, WAV Files, AES-RSA Hybrid Encryption, Data Hiding, Secure Communication, Python Tkinter GUI.

INTRODUCTION

Despite the availability of cryptographic techniques, secure communication continues to face challenges because encryption alone cannot hide the presence of the message. An intercepted encrypted file can still raise suspicion. Steganography reduces this risk by embedding data within an audio file in a way that is imperceptible to listeners. However, traditional LSB techniques often suffer from low robustness and are sensitive to audio compression and noise. In addition, methods that modify audio samples directly may compromise fidelity if not implemented carefully. To address these limitations, this project aims to design a system that embeds encrypted information inside audio with minimal distortion while ensuring that only authorized users can retrieve the original message. This need for improved security and imperceptibility—highlighted in earlier work on LSB capacity improvement [1] and the reliability challenges discussed in LSB-based hiding methods [3]—motivated the development of this enhanced system.

METHODOLOGY

The methodology of this work is built around a structured pipeline consisting of message preparation, encryption, LSB embedding, transmission, extraction, and decryption. The process begins with converting the user's message into its binary form. To secure the data before hiding it inside the audio, AES encryption is used because of its high speed and strong symmetric-key protection. However, since sharing AES keys securely is crucial, RSA encryption is implemented to safeguard the AES key. This hybrid encryption strategy is inspired by earlier research that emphasized the importance of cryptographic integration with LSB steganography to strengthen security [2].

After encryption, the audio samples of the chosen WAV file are analyzed, and their least significant bits are modified to embed the encrypted data. Instead of directly replacing each LSB with corresponding data bits, the system employs a controlled LSB adjustment technique that compares message bits with sample-specific values, ensuring that modifications remain as natural as possible. This idea was partly motivated by prior studies that explored ways to preserve audio quality while still performing bit-level embedding [4] on compressed text embedding and [6] on efficient substitution strategies.

During data extraction, the process is reversed. The LSBs are retrieved, reassembled into the bitstream, and decrypted first using RSA to recover the AES key and then using AES to obtain the original message. This approach ensures reliable restoration of the message and minimizes the chance of data corruption, aligning with earlier work that highlighted the importance of secure retrieval and robustness in audio steganography systems [5].

Block Diagram

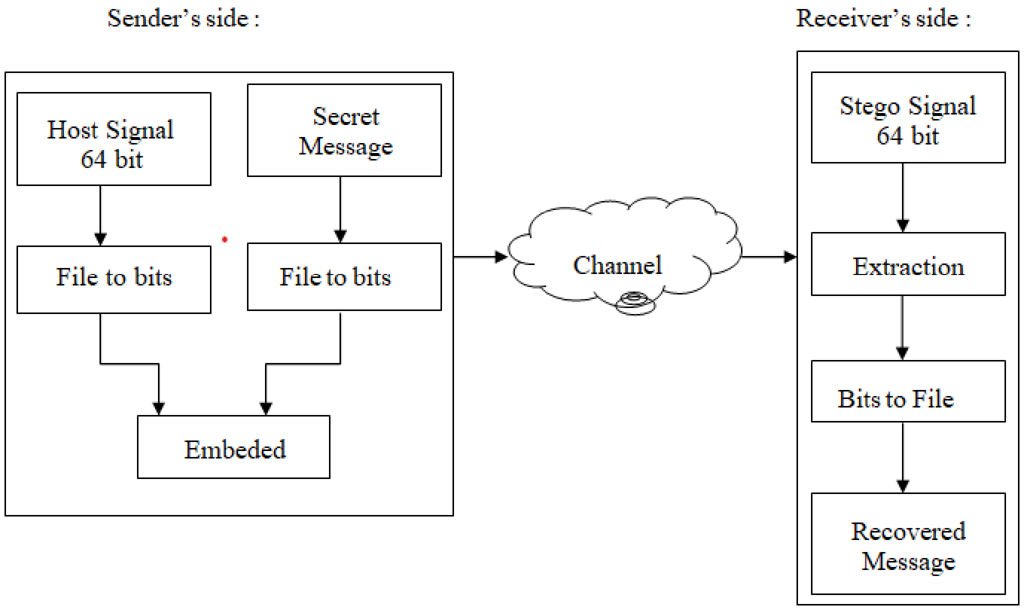

Fig 3.1 : Block Diagram Audio Steganography Using LSB

The block diagram illustrates the flow of the embedding and extraction mechanisms. In the embedding stage, the input message is transformed into binary form, encrypted using the AES–RSA hybrid model, and inserted into the LSBs of the audio samples to produce a stego audio file. The fundamental principle of this stage is derived from the classical LSB replacement approach described in previous research [7], where data bits are written into the least significant positions of WAV samples. However, while earlier works sometimes rely on direct bit replacement, this system adapts the embedding in a controlled way to preserve the waveform's natural characteristics.

The extraction phase begins by scanning the stego audio to retrieve the embedded LSB bits. These bits are combined to reconstruct the encrypted message and then decrypted to restore the original text. Though several studies have proposed more complex embedding schemes involving randomness [8] or transform-domain methods such as DWT-based embedding [9], this project intentionally focuses on simplicity and practicality.

The goal was to create a system that balances usability with high security rather than maximizing robustness against all forms of audio manipulation. Thus, the block diagram represents a streamlined yet secure approach to audio steganography that builds on the strengths of earlier LSB-based systems while avoiding unnecessary implementation complexity.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

IMPLEMENTATION AND SIMULATION

The implementation of this project centers on building a secure audio steganography system in Python, paired with an intuitive Tkinter interface that manages user registration and login. To ensure account security, user passwords are stored as SHA-256 hashes, and each registered user is automatically assigned an RSA key pair to facilitate secure encryption and decryption during communication.

A hybrid cryptographic model forms the backbone of the system. The secret message is encrypted using AES for fast and reliable data protection, while the AES key itself is secured through RSA to guarantee safe key exchange. After encryption, the message is embedded into a WAV audio file using the Least Significant Bit (LSB) technique, which allows data to be hidden without noticeably altering the audio quality. During the extraction process, the embedded bits are read back from the stego file, decrypted using the recovered keys, and converted into the original readable message.

The system relies on several Python libraries—such as rsa, hashlib, numpy, and soundfile—to implement cryptographic operations, hashing, bit-level processing, and audio manipulation. Together, these modules create an efficient and secure framework that can be applied to confidential communication and basic digital watermarking scenarios.

When compared with existing work, this implementation differs in its design priorities. The method in [10] focuses on improving LSB performance by adapting embedding behavior to characteristics of both the carrier signal and the message. In contrast, the present system places greater emphasis on security through layered AES–RSA encryption. Similarly, while the approach in [11] aims to increase embedding capacity and strengthen resistance to attacks, this project prioritizes cryptographic protection before performing any LSB substitution. Additionally, although [12] provides an efficient mechanism for concealing text within audio, the system presented here extends beyond simple embedding by incorporating user authentication and secure key management to enhance overall protection.

The operational workflow is organized into two primary phases. In the embedding phase, the encrypted message is inserted into the LSBs of the audio samples to generate the stego audio file. In the extraction phase, the hidden bits are retrieved, decrypted, and reconstructed to recover the original message. Through this combination of cryptography and steganography, the system delivers secure hidden communication while maintaining the perceptual quality of the audio signal.

RESULT AND ANALYSIS

The proposed system effectively hides secret data inside WAV audio using LSB embedding combined with AES and RSA encryption. Because only the least significant bits are modified, the audio quality remains unchanged, and the hidden message is accurately recovered during extraction.

Compared with earlier methods, the approach in [13] reduces distortion through a pyramid-based structure but lacks encryption. Similarly, [14] improves audio fidelity without providing strong protection for the hidden data. The indirect LSB method in [15] achieves good imperceptibility but still does not secure the embedded information cryptographically.

By integrating AES encryption and RSA-based key exchange with LSB embedding, the system developed in this study ensures that the hidden data is both difficult to detect and protected from unauthorized access. Overall, it provides a secure and efficient solution for covert communication, with future improvements aimed at increasing capacity and robustness.

The fig.5.1 This figure shows a Python Tkinter-based graphical user interface for a login and registration system displayed beside the corresponding source code.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

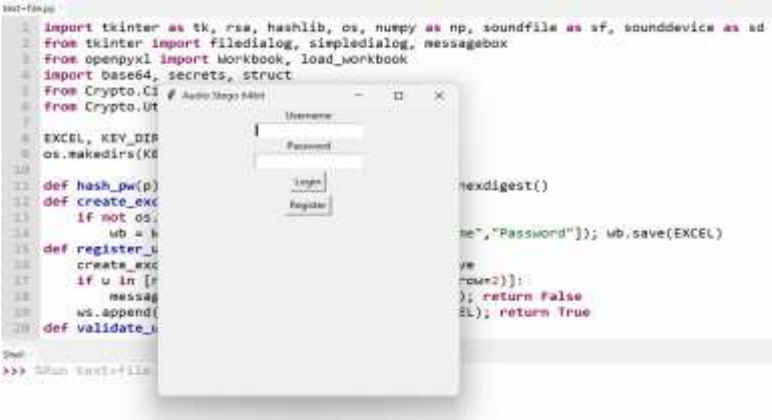

Fig.5.1 : Tkinter Login and Registration Interface

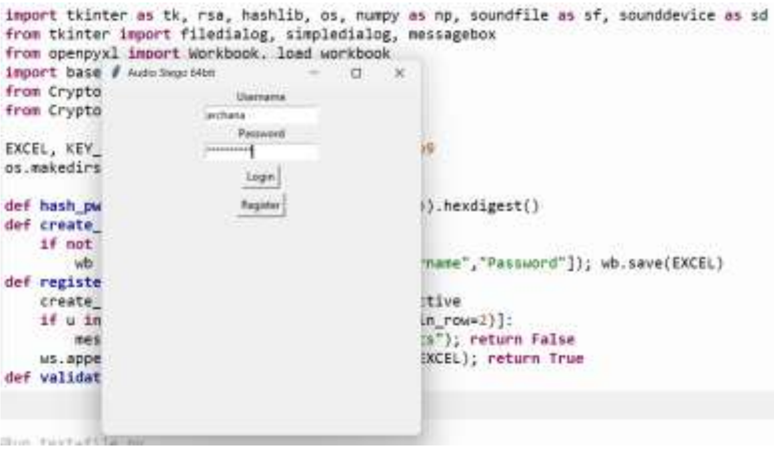

Fig.5.2 : GUI of the Audio Steganography Application with Login/Registration Interface

The fig.5.3 represents sender selecting original WAV file for encrypting the message.

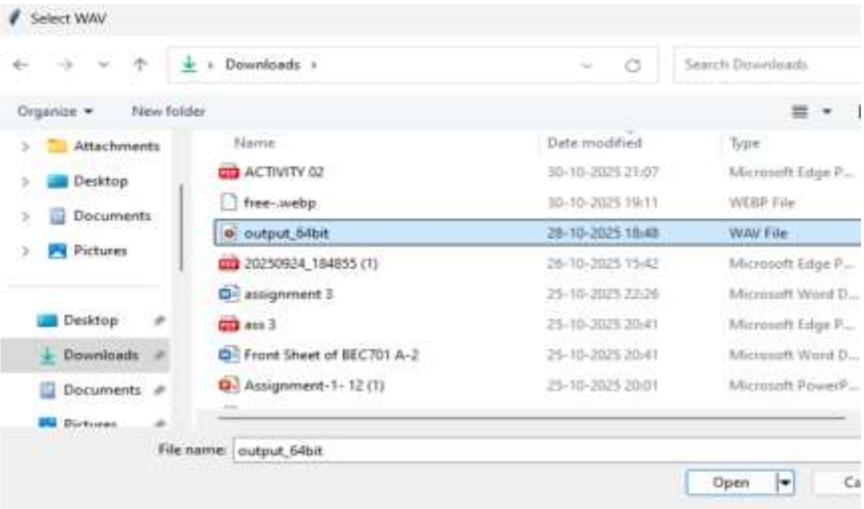

Fig.5.3 : Selection of original WAV file

The fig 5.4 shows the file Buttons for Encode, Decode, Play, and Logout are shown for user operations. A popup dialog is visible prompting the user to enter the secret text to embed into the audio file.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

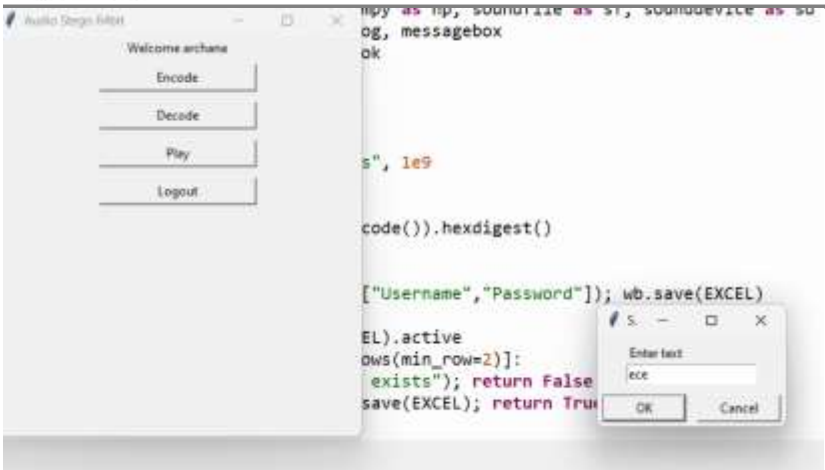

Fig.5.4:Audio Stego Application Interface Showing Encoding Options and Text Input Dialog

The fig.5.5 The figure shows a file dialog window where the user selects the receiver's public key fil(receiver_public.pem) for use in the encryption or secure communication process.

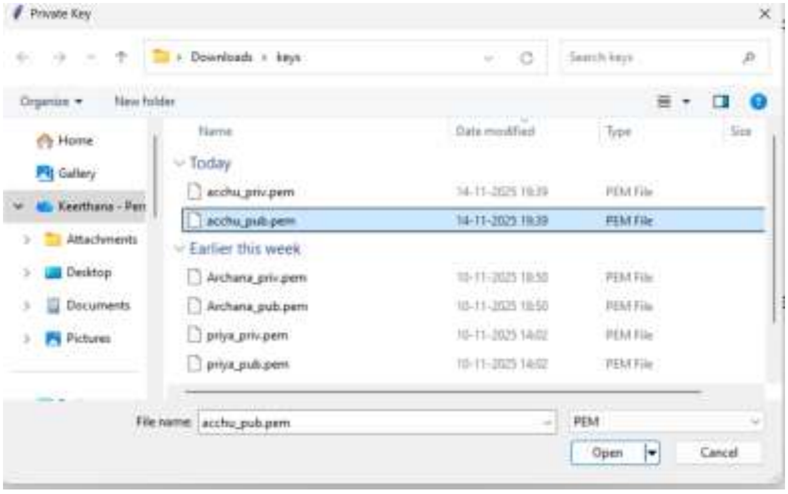

Fig.5.5: Selection of Receiver's Public Key File

The fig.5.6 A dialog box prompting the user to select a stego WAV file (e.g., "stego out") for processing or extraction in the audio steganography system.

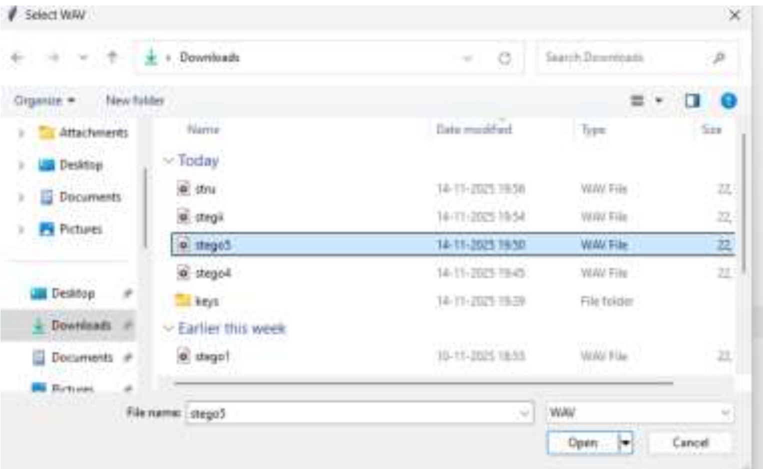

Fig.5.6 : File Selection Window for Private Key

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

The fig.5.7 shows a dialog where the user is selecting a private key file for use in a cryptographic process.

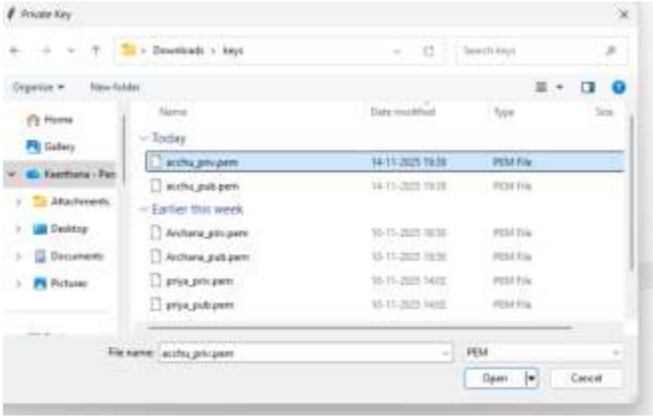

Fig.5.7 : File Selection Window for Private Key

The fig.5.8 Options for Encode, Decode, Play, and Logout are presented to the user. A popup dialog allows the user to choose whether to embed plain text or a file into the audio.

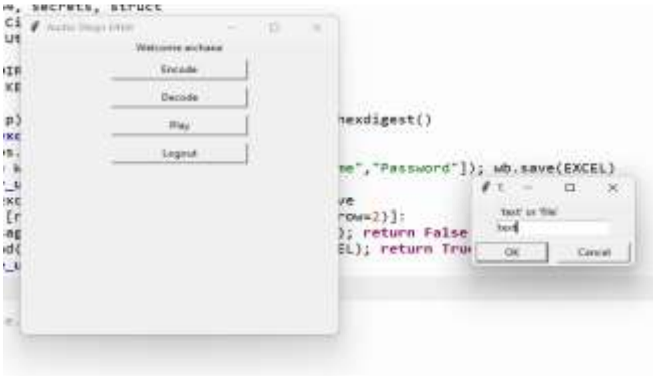

Fig.5.8 : Audio Stego Application with Encode/Decode Menu and Text/File Input Prompt

The fig.5.9 A popup window labeled “Decoded” displays the extracted hidden message from the audio file.

Fig.5.9: Decoded Message Display in the Audio Steganography Application

CONCLUSION, CHALLENGES AND FUTURE ENHANCEMENTS

Conclusion

This project successfully implements a secure audio steganography system that combines LSB embedding with AES–RSA hybrid encryption. The method preserves audio quality, enables accurate message recovery, and ensures that only authorized users can access the hidden data. The user-friendly GUI further enhances the practicality of the system for secure communication.

Challenges

- Limited payload capacity depending on audio size and format
- Maintaining audio quality while embedding data
- Vulnerability of LSB to compression, noise, and format changes
- Secure handling of RSA keys
- Designing a smooth and efficient GUI workflow

Future Enhancements

- Implement error correction codes to improve robustness against noise and compression.
- Support more audio formats and compressed audio files (e.g., MP3) with robust steganography techniques.
- Increase payload capacity by combining multiple audio channels or advanced embedding methods.
- Add multi-factor authentication or biometric integration for stronger user security.
- Integrate real-time audio steganography and streaming support.
- Develop a more intuitive GUI with drag-and-drop features and batch processing capabilities.

REFERENCES

1. Audio Steganography Using LSB Encoding Technique with Increased Capacity and Bit Error Rate Optimization
2. Sajaa G. Mohammed and Nuhad Salim Al-Mothafar, “A survey on Rijndael based LSB Audio Steganography techniques,” Wasit Journal for Pure Sciences, vol. 2, no. 4, pp. 80–87, Dec. 2023.
3. Anu Binny and Maddulety Koilakuntla, “Hiding Secret Information Using LSB Based Audio Steganography,” in 2014 International Conference on Soft Computing & Machine Intelligence (ISCMI), 2014
4. LSB Based Audio Steganography Based on text compression .M.BarithaBeguma ,Y.Venkataramanib
5. Increaing Robustness Of LSB Audio Steganography Using A Novel Embedding MetodN. CvejicMediaTeam Oulu Group, Information Processing Laboratory, University of Oulu, FinlandT.SeppanenMediaTeam Oulu Group, Information Processing Laboratory, University of Oulu, Finland
6. An Efficient Method For Image And Audio Steganography Using Least Significant Bit (LSB) SubstitutionAnkit Chadha, Neha Satam
7. Modified LSB On Audio Steganography Using WAV Format Rini Indrayani Faculty Of Computer Science Universitas AMIKOM Yogyakarta Yogyakarta, Indonesia
8. Audio Steganography Using Dual Randomness LSB Method.Jithu Vimal PG Scholar, Dept.of Electronics and Communication Engineering Mar Baselios College of Engg& Technology Trivandrum, India jithulmc@gmail.com Ann Mary Alex Assistant Professor, Dept. of Electronics and Communication Engineering Mar Baselios College of Engg& Technology
9. Dwt And LSB Based Audio SteganographyNehagupta Department Of Computer Engineering, The Technological Institute Of Textile & Sciences, Bhiwani Haryana, India.

Gupta.Neha.221@Gmail.Com Ms. Nidhi Sharma Assistant Professor In Department Of Computer Engineering The Technological Institute Of Textile & Sciences, Bhiwani Haryana, India Nidhisharmal725@Gmail.Com

10. Enhancement of LSB Audio Steganography Based on Carrier and Message Characteristics Hussein A. Nassrullah, Wameedh N. Flayyih, Mohammed A. Nasrullah Department of Computer Engineering University of Baghdad Baghdad.
11. Enhanced LSB Technique For Audio Steganography Harish Kumarl , Anuradha2 1. Associate Professor(CSE), Krishna Engineering College, Ghaziabad .E-Mail - Harishtaluja@Gmail.Com 2. Lecturer, MIET, Meerut, E-Mail- Anutaluja@Gmail
12. An Efficient Audio Steganography Technique To Hide Text In Audio Shital P. Rajput Dept. Of Computer Engineering SSBT's COET Jalgaon, Maharashtra, India Shital_Pr27@Rediffmail.Com Krishnakant P. Adhiya Dept. Of Computer Engineering SSBT's COET Jalgaon, Maharashtra, India Kpadhiya@Yahoo.Com Girish K. Patnaik Dept. Of Computer Engineering SSBT's COET Jalgaon, Maharashtra, India Girishpat2001@Yahoo.Com
13. Audio Steganography: LSB Technique Using A Pyramid Structure And Range Of Bytes Satish Bhalshankar1 , Avinash K. Gulve2
14. A Proposed Implementation Method of an Audio Steganography Technique Mazhar Tayel, Ahmed Gamal, Hamed Shawky.
15. Image and audio steganography based on indirect LSBZainab N. Sultani , Ban N. DhannoonDept. Computer Science, College of Science, Al-Nahrain University, Baghdad,Iraq Corresponding author zna@sc.nahrainuniv.edu.iqs
16. LSB and Encryption Techniques: A Review. International Journal of Computer Applications, 149(4), 30-34.
17. Audio Steganography using LSB Priyanka, Bankar R; Vrushabh, Katariya R; Komal, Patil K; Pingle, Shashikant M; Mahesh, Sanghavi R
18. Hiding Secret Information Using LSB Based Audio Steganography Anu Binny Dr. K. N Modi University, Newai, India Maddulety Koilakuntla
19. Steganography In Images Using LSB Technique Arun Kumar Singh Department Of Electronics And Communication Engineering Amity University Gurgaon, HR, India Juhi Singh Department Of Computer Science Engineering Amity University Gurgaon, HR, India Dr. Harsh Vikram Singh Department Of Electronics And Communication Engineering KNIT Sultanpur UP, India
20. Enhancing LSB Using Binary Message Size Encodingfor High Capacity, Transparent And Secure Audiosteganography An Innovative Approach Mahmoud M. Mahmoud And Huwaida T. Elshoush Department Of Computer Science
21. A View On LSB Based Audio Steganography
22. Ratul Chowdhury 1 , Debnath Bhattacharyya 2 , Samir Kumar Bandyopadhyay3 And Tai-Hoon Kim4 1Department Of Information Technology, Institute Of Engineering And Management, Kolkata
23. LSB Based audio steganography method based on lifting wavelet transform. Mohammad Pooyan Department Of Electrical & Computer Engineering, Shahed University, Iran Ahmad Delforouzi Department Of Electrical & Computer Engineering, Shahed University, Iran
24. Securing Technique Using Pattern-Based LSB Audio Steganography and Intensity-Based Visual Cryptography.Pranati Rakshit1 , Sreeparna Ganguly1 , Souvik Pal2 , Ayman A. Aly3 and Dac-Nhuong Le4.
25. Katzenbeisser, S., & Petitcolas, F.A.P. (2000). Information Hiding Techniques for Steganography and Digital Watermarking. Artech House. Kaur, G., & Singh, M. (2016).
26. A Detailed Look Of Audio Steganography Techniques Using LSB And Genetic Algorithm Approach Nehru , Gunjan ; Dhar Puja

INTERNATIONAL JOURNAL OF RESEARCH AND SCIENTIFIC INNOVATION (IJRSI)
ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

AUTHORS PROFILE

Bhagyalakshmi V, Holds an M.Tech degree in Industrial Electronics from VTU Belagum and is currently pursuing a Ph.D. at VTU Belagum. Completed PG Diploma In Child and School Conseling.Working as an Assistant Professor with 14 years of teaching experience in the field of engineering education.

Academic interests include Electronic Circuits, and advanced research in engineering technologies, with a strong commitment to teaching, research, and student mentoring.

Bhagyashree Parashuram Rajput an undergraduate student pursuing Electronics and Communication Engineering with a strong interest in systems to solve real-world problems. Technical interests include Embedded Systems, Internet of Things (IoT), Artificial Intelligence and Machine Learning, VLSI, and Automation. Has hands-on experience with Python, C programming, MATLAB, Arduino, and CAD tools, along with strong problem-solving, teamwork, and communication skills.

She has earned professional certifications in VLSI, Python Fundamentals, Artificial Intelligence & Machine Learning, and Arduino, reflecting commitment to continuous learning and technical skills.

Keerthana K M ,Electronics and Communication Engineering Student with expertise in embedded systems, VLSI, communication networks, and signal processing. Skilled in C, Python, and MATLAB programming, with experience in circuit design and microcontroller-based projects.

Strong understanding of communication systems, digital signal processing, and VLSI design.. Familiar with tools like Simulink, LabVIEW, Cadence software. Strong problem-solving skills, with a keen eye for detail. Team player with excellent communication skills. Seeking an opportunity to leverage my ECE skills and learn from industry experts, contributing to innovative projects and growing as a professional

Madhushree B S Electronics and Communication Engineering student with a strong foundation in embedded systems and digital design. Demonstrated competence in 8051 microcontroller programming and Verilog hardware description language for modeling basic digital systems.

Proficient with embedded development and simulation tools including Keil v4/5, Arduino IDE and MATLAB. Skilled in C for hardware-oriented applications; possesses working knowledge of Python for auxiliary analysis. Experienced in Windows operating systems and MS Office for technical documentation. A self-motivated, detail-oriented researcher aiming to apply core ECE skills in a professional engineering and research environment.

Priya H U is an undergraduate student pursuing a Bachelor of Engineering in Electronics and Communication Engineering at Maharaja Institute of Technology, Thandavapura, Mysuru, India. She is passionate about applying electronics and intelligent systems to solve real-world problems .Her technical interests include Embedded Systems, Internet of Things (IoT), Artificial Intelligence & Machine Learning, VLSI, and Automation. She has successfully completed projects such as a Audio steganography using LSB. She possesses hands-on experience with Python, C programming, MATLAB, Arduino, and CAD tools, along with strong problem-solving and teamwork skills. She has also completed professional certifications in VLSI, Python Fundamentals, AI & ML, and Arduino, reflecting her commitment to continuous learning and technical growth .She aspires to build a career in the field of Electronics and Intelligent Systems, contributing to innovative, reliable, and technology-driven solutions.