IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, October 2026
Impact Factor: 8.2

Steganography Information Sharing via Sound & Image for Secure Data Transmission

Prof. Khamkar P. J.[1], Vhankade Netra Balu[2], Bhopate Snehal Ananda[3], Auti Sakshi Thakaram[4], Jadhav Sakshi Dilip[5]
Guide, Department of Computer Engineering[1]
Students, Department of Computer Engineering[2-5]
HSBPVT'S GOI Faculty of Engineering, Kashti, India

Abstract: *Secure information exchange is an important requirement in digital communication. Conventional encryption transforms readable information into an encoded form, while steganography aims to conceal the existence of the information by embedding it within an ordinary-looking carrier such as an image or an audio signal. This paper presents a project design for information sharing through image and sound steganography. The proposed system allows a sender to select a secret text message or file, choose an image or audio carrier, embed the secret data, and transmit the resulting media to a receiver. The receiver uses the appropriate extraction procedure and, where enabled, a shared password or key to recover the hidden information. For image steganography, a least-significant-bit (LSB) approach may be used to modify selected pixel values with minimal visible change. For audio steganography, selected sample bits can carry message bits while attempting to preserve perceptual sound quality. The design considers capacity, imperceptibility, extraction accuracy, processing time, and robustness as evaluation criteria. It also recognizes that simple LSB methods can be vulnerable to compression, resizing, filtering, or other transformations; therefore, steganography should be combined with encryption when confidentiality is required. This document is a research-paper draft and project proposal. Performance values and experimental conclusions must be added only after implementing and testing the system on a defined dataset*

Keywords: Steganography, Image Steganography, Audio Steganography, Least Significant Bit (LSB), Secure

I. INTRODUCTION

The growth of online communication has increased the need to exchange information privately and reliably. Messages, documents, and other digital files are commonly shared through networks, but visible transmission of sensitive information can attract unwanted attention. Cryptography protects the content by converting plaintext into ciphertext; however, the presence of an encrypted message may still be noticeable. Steganography addresses a different problem by concealing a message inside an ordinary digital object, called a cover medium.

Digital images and audio files are widely available and can serve as cover media. In image steganography, secret bits may be placed in selected pixel values. In audio steganography, message bits may be embedded in digital audio samples. If the embedding is designed carefully, the resulting stego-image or stego-audio should remain perceptually similar to the original carrier.

The proposed project, "Steganography: Information Sharing via Sound and Image for Secure Data Transmission," combines image- and audio-based information hiding in a single workflow. The sender can choose the carrier type, embed a message, and share the generated media. The receiver selects the corresponding extraction option and retrieves the message. A password-based step and optional encryption can be included to add a separate layer of protection

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, October 2026
Impact Factor: 8.2

A. Problem Statement

A secure communication method is required that hides the presence of a message during ordinary media sharing and enables an intended receiver to extract it. The system should support both image and audio carriers, preserve acceptable media quality, and provide a clear sender–receiver workflow.

B. Objectives

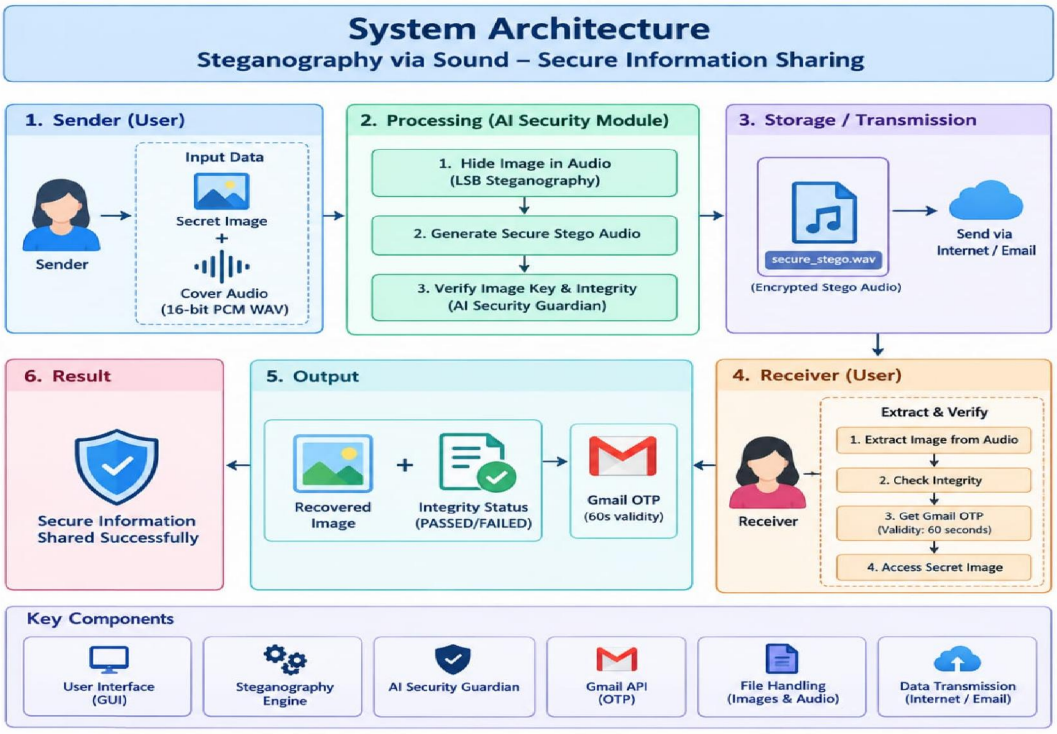
- To design a unified application for hiding and retrieving secret information using images and audio files.
- To implement an image-based embedding and extraction method, such as least-significant-bit substitution.
- To implement an audio-based embedding and extraction method suitable for digital audio samples.
- To evaluate media quality, message recovery accuracy, embedding capacity, and processing time.
- To support password-based access and recommend encryption of the secret payload before embedding.

II. LITERATURE REVIEW

Research on information hiding includes methods that conceal data in images, audio signals, video, and other digital media. Least-significant-bit substitution is a simple spatial-domain technique: selected low-order bits of image pixels or audio samples are modified to represent secret bits. It is comparatively easy to implement and can provide good perceptual quality when the payload is small, but it is not inherently robust against media transformations.

More advanced approaches use transform domains, adaptive embedding, or signal features to balance payload capacity, perceptual quality, and robustness. Cryptography and steganography can also be combined: encryption protects the payload contents, while steganography conceals the payload's presence. The best method depends on the application requirements and the expected processing of the carrier media.

III. PROPOSED ARCHITECTURE



Copyright to IJARSCT
www.ijarsct.co.in
DOI: 10.48175/IJARSCT-40368

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, October 2026
Impact Factor: 8.2

The system is organized into sender and receiver modules. The sender selects a secret message or file, optionally encrypts it, chooses an image or audio carrier, and embeds the payload. The generated stego-media is then transmitted using a normal file-sharing channel. At the receiver side, the matching extraction module reads the embedded data and restores the original payload. If encryption is enabled, the receiver decrypts it with the agreed key.

System Modules:

- Input module: accepts a text message or supported file and validates the input.
- Carrier selection: accepts a supported image or audio file.
- Payload preparation: encodes the message and may encrypt it before embedding.
- Embedding engine: inserts payload bits into the selected carrier using the chosen algorithm.
- Transmission/storage: saves or shares the generated stego-media.
- Extraction engine: retrieves payload bits using the corresponding method and validates the payload length or marker.
- Output module: reconstructs the message or file and, if applicable, decrypts it.

IV. METHODOLOGY

A. Image Steganography

In a basic LSB implementation, the binary representation of a secret message is embedded into the least significant bits of selected pixel colour channels. A length header or delimiter can identify the payload boundary. The receiver reads the same positions and reconstructs the message. A practical implementation should validate the image format, message size, and available embedding capacity before writing data.

For an RGB image, a simple capacity estimate is approximately the number of eligible colour-channel samples divided by eight bytes per character only when one bit is used per channel sample and the payload is represented as eight-bit bytes. Actual capacity is lower when headers, keys, error correction, or restrictions on eligible pixels are included.

B. Audio Steganography

For uncompressed digital audio, a basic LSB method can store message bits in the least significant bits of selected audio samples. The implementation should retain the sample rate, channel count, and sample format, and should avoid unsupported lossy formats during the embedding stage. The receiver reads the designated sample positions and reconstructs the payload. Changes must be evaluated to ensure that they do not introduce unacceptable audible distortion.

A basic sample-LSB method may fail after lossy compression, resampling, filtering, or format conversion. If the application must withstand these operations, a more robust audio-domain or transform-domain method should be considered and tested.

C. Payload Protection and Validation

Steganography alone does not guarantee confidentiality. The recommended design encrypts the secret payload with a well-established authenticated encryption method before embedding it. The system should not invent its own cryptographic algorithm. It should also validate file types and sizes, handle incorrect passwords safely, and avoid exposing the secret message in logs or error messages.

D. Evaluation Metrics

- Embedding capacity: maximum payload size that can be hidden in a carrier.
- Peak Signal-to-Noise Ratio (PSNR): image-quality comparison between cover and stego-image.
- Mean Squared Error (MSE): average squared difference between corresponding image samples.
- Signal-to-Noise Ratio (SNR) or an appropriate audio quality measure: comparison of cover and stego-audio.
- Extraction accuracy: proportion of payload bits or bytes recovered correctly.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, October 2026
Impact Factor: 8.2

• Execution time: time required for embedding and extraction.
• Robustness: successful recovery after specified transformations, if robustness is a project requirement.

V. SYSTEM REQUIREMENTS

The system requirements for the proposed project, "Steganography: Information Sharing via Sound & Image for Secure Data Transmission," are given in the following tables.

TABLE I: HARDWARE REQUIREMENTS

Sr. No.	Hardware Component	Minimum Requirements
1	Processor	Intel Core i3 or equivalent
2	RAM	4 GB
3	Hard Disk	10 GB free space
4	System Type	64-bit computer system
5	Input Devices	Keyboard and Mouse
6	Output Devices	Monitor
7	Audio Device	Microphone and Speaker (optional)
8	Network	Internet or LAN connection for file transmission

TABLE II: SOFTWARE REQUIREMENTS

Sr. No.	Software Component	Requirements
1	Operating System	Windows 10/11 or Linux
2	Programming Language	Python
3	IDE	Visual Studio Code or PyCharm
4	Image Processing Library	OpenCV, Pillow
5	Audio Processing Library	Sound File, Librosa or PyDub
6	Numerical Processing	NumPy
7	Cryptography Library	Python Cryptography package
8	File Formats	PNG, BMP, WAV, TXT
9	Testing Tool	Python interpreter and test files
10	Network/Transfer Tool	Web browser or local file transfer mechanism, as required

VI. EXPECTED RESULTS AND DISCUSSION

The expected outcome is a working prototype that supports both image and audio carriers and provides a sender–receiver process for hiding and retrieving a message. With a small payload and an appropriate carrier, basic LSB embedding may produce changes that are difficult to notice under ordinary viewing or listening conditions. However, the actual quality, capacity, accuracy, and processing time depend on the implementation and test data.

No numerical results are claimed in this draft because no implementation results or experimental dataset were provided. The final paper should report measured values in tables, describe the hardware/software environment, identify the test files and payload sizes, and compare the original and stego media. It should also test failure cases such as oversized payloads, unsupported formats, corrupted media, and incorrect keys.

VII. APPLICATIONS

• Private exchange of short messages through ordinary image or audio files.
• Educational demonstrations of information hiding and digital media processing.
• Confidential document transfer when combined with appropriate encryption and access control.

Copyright to IJARSCT
www.ijarsct.co.in
DOI: 10.48175/IJARSCT-40368

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, October 2026
Impact Factor: 8.2

• Controlled watermarking or ownership-verification experiments, if the embedding method is designed for that purpose.

VIII. LIMITATIONS AND SECURITY CONSIDERATIONS

The existence of hidden data may be detected through statistical steganalysis, particularly when simple embedding patterns are used. Basic LSB methods may be damaged by image resizing, recompression, audio transcoding, filtering, or sample-rate conversion. Capacity is limited by carrier size and acceptable distortion. Sharing the password through the same channel as the stego-media can weaken protection. For these reasons, the system should use a vetted encryption library, protect keys separately, validate all inputs, and describe its security claims conservatively.

IX. CONCLUSION

This paper proposes a unified steganography system for secure information sharing through image and sound carriers. The design includes payload preparation, optional encryption, media-specific embedding, transmission, extraction, and validation. Image and audio LSB techniques provide accessible starting points for a student prototype, while their limitations make evaluation essential. Future work can investigate adaptive or transform-domain methods, error correction, key-based embedding positions, and systematic robustness testing. The final assessment should be based on measured results rather than assumed performance.

X. ACKNOWLEDGMENT

We would like to express our sincere gratitude to our internal guide, Prof Khamkar P.J., for providing invaluable technical direction and support. We also extend our thanks to Dr. Sayyad J. I., Head of the Computer Engineering Department and Dr. Dhagate M. D., Principal of HSBPVT'S GOI Faculty of Engineering, Kashti, for providing the necessary laboratory infrastructure and continuous encouragement to pursue this research

REFERENCES

[1]. Johnson, N. F., and Jajodia, S. (1998). "Exploring Steganography: Seeing the Unseen." Computer, 31(2), 26–34. URL: https://doi.org/10.1109/MC.1998.4655281

[2]. Petitcolas, F. A. P., Anderson, R. J., and Kuhn, M. G. (1999). "Information Hiding—A Survey." Proceedings of the IEEE, 87(7), 1062–1078. URL: https://doi.org/10.1109/5.771065

[3]. Katzenbeisser, S., and Petitcolas, F. A. P. (2000). "Information Hiding Techniques for Steganography and Digital Watermarking." Artech House.

[4]. Cachin, C. (2004). "An Information-Theoretic Model for Steganography." Information and Computation, 192(1), 41–56. URL: https://doi.org/10.1016/j.ic.2004.02.003

[5]. Fridrich, J. (2009). "Steganography in Digital Media: Principles, Algorithms, and Applications." Cambridge University Press. URL: https://doi.org/10.1017/CBO9781139192903

[6]. Abdulrazzaq, S. T., Siddeq, M. M., and Rodrigues, M. A. (2020). "A Novel Steganography Approach for Audio Files." SN Computer Science, 1, Article 97. URL: https://doi.org/10.1007/s42979-020-0080-2

[7]. Nasr, M. A., El-Shafai, W., El-Rabaie, E. S. M., et al. (2024). "A Robust Audio Steganography Technique Based on Image Encryption Using Different Chaotic Maps." Scientific Reports, 14, Article 22054. URL: https://doi.org/10.1038/s41598-024-70940-3

[8]. Kombrink, M. H., Geradts, Z. J. M. H., and Worring, M. (2025). "Image Steganography Approaches and Their Detection Strategies: A Survey." ACM Computing Surveys, 57(2), Article 33. URL: https://doi.org/10.1145/3694965

[9]. Krishnan, A. A., Ramesh, Y., Urs, U., and Arakeri, M. (2025). "Audio-in-Image Steganography Using Analysis and Resynthesis Sound Spectrograph." IEEE Access, 13, 75180–75189. URL: https://doi.org/10.1109/ACCESS.2025.3563781

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, October 2026
Impact Factor: 8.2

[10]. Abd, A. S., Al-Thahab, O. Q. J., and Hamad, A. A. (2025). "New Approach in Steganography Algorithm by Using Audio and Image as Secure Information Based on Chaotic Method." International Journal of Safety and Security Engineering, 15(2), 349–358. URL: https://doi.org/10.18280/ijsse.150216