



ROBUST MULTIMODAL STEGANOGRAPHY FRAMEWORK FOR SECURE TRANSMISSION OF TEXT, IMAGE, AND AUDIO DATA

Prashant Wakhare^{1*}, Govind B. Sambare², Riyazahemad A. Jamadar³, Veena Suhas Bhende⁴

¹Department of AI & DS, All India Shri Shivaji Memorial Society's Institute Of information Technology, Pune-411001, India.

²Department of Computer Engineering, Pimpri-Chinchwad College Of Engineering, Pune-412101, India.

³Department of AI & DS, All India Shri Shivaji Memorial Institute Of Information Technology, Pune-411001, India

⁴Department of Computer Engineering, All India Shri Shivaji Memorial Institute Of Information Technology, Pune-411001, India.

¹<http://orcid.org/0000-0003-3071-9086>, ²<http://orcid.org/0000-0002-5615-3968>

³<http://orcid.org/0000-0002-1042-1517>, ⁴<http://orcid.org/0009-0003-4738-9359>

Email: *pbwakhare@gmail.com, santosh.sambare@pccoepune.org, reeyaj.jamaddar@gmail.com, veena.bhende@aissmsioit.org

ARTICLE INFO

Article History

Received: March 21, 2026

Reviewed: April 21, 2026

Accepted: July 21, 2026

Published: August 31, 2026

Keywords:

Multimodal Steganography,
Secure Data Transmission,
Image Steganography,
Audio Steganography,
Information Hiding,
Steganalysis Resistance

ABSTRACT

The growth of development the digital communication has greatly raised the chances of information leakage, interception, and unauthenticated access, particularly in heterogeneous multimedia setting. Conventional single-modal steganographic methods have been known to be limited in their payload storage capacity, weak, and susceptible to steganalysis attacks. In order to overcome these issues, the proposed work develops a Robust Multimodal Steganography Framework to ensure the secure transmission of the text, image, and audio information over the untrusted communication channels. The suggested framework combines the utilization of adaptive embedding plans in various carrier media with the Discrete Wavelet Transform (DWT) being employed in image stealth, the Discrete Cosine Transform (DCT) being employed in audio embedding and AES-based encryption being employed in protecting the textual payload. An active payload allocation scheme provides maximum imperceptibility and resistance to noise, compression and signal distortions. The experimental analysis of the proposed framework shows that this framework has better security and robustness than traditional unimodal methods. With the system, attains an average PSNR of 52.6 dB with stego-images, SNR of 41.8 dB with stego-audio and a bit error rate of less than 0.7 with common attack conditions like Gaussian noise and compression. It has an enhanced payload capacity of up to 32 and the transparency to perceptions is still high. The framework also has high resistance to statistical steganalysis and the detection accuracy dwindles to less than 18 %.



Copyright ©2026 by authors and Galileo Institute of Technology and Education of the Amazon (ITEGAM). This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

I. INTRODUCTION

The multimedia applications and the high rate of development of digital communication networks have resulted in the unheard of sharing of sensitive information in the shape of text, images and audio over non-closed and non-trusted mediums [1]. According to recent studies, multimedia data proves to be especially appropriate in the context of information hiding because they have a high level of redundancy and perceptual tolerance [2]. Nevertheless, today the communication situations are more about multimodal transmission of data, where the textual, picture, and audio information are present in parallel and exchange each other simultaneously, thus creating new security dilemmas [3]. Compression, noise, format conversion or statistical analysis can be used by attackers to scan or obliterate hidden information, and therefore unimodal protection cannot be fully used in most practical situations [4]. Current single carrier (images or audio) unimodal steganographic schemes have limited embedding, are poorly resistant to attacks and lack adaptability to dynamic communication conditions [5]. Moreover, the use of one medium also leads to high chances of complete information loss once the carrier is attacked [6].

II. RELATED WORK

II.1 SUBTITLE

II.1.1 Materials and Methods

One of the oldest forms of information hiding using linguistic structures, formatting, and semantic differences was text steganography which allowed the introduction of secret messages into the textual material [7]. More modern developments have investigated the field of natural language processing and language models to enhance better imperceptibility, yet the ability to resist automated text analysis and editing tools does not happen easily [8]. Least Significant Bit (LSB) substitution is a well-known method of spatial-domain data representation to use from its simplicity and large payload capacity, yet it is very vulnerable to noise, compression, and statistical steganalysis [9]. In order to overcome these shortcomings, methods in transform domain, grounded on Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) have been suggested, which provide a better robustness and imperceptibility [10]. Hybrid schemes based on several transforms reduce the resistance of attacks even more, but it is usually at the expense of a more complex computation [11]. The audio steganography methods are the methods based on the properties of the human auditory system that allows to hide hidden data in digital audio messages. LSB coding, phase coding, spread spectrum, and echo hiding are some of the techniques that have received a lot of research.

Though methods based on LSBs offer high payload capacity, they are sensitive to signal processing tasks as compared to transform-based and perceptual masking methods which are more robust, but with lower embedding rates [12]. Recent studies have devoted attention to adaptive embedding and psychoacoustic modeling in order to achieve a tradeoff between imperceptibility and resilience [13]. Multimodal, and hybrid information hiding schemes are designed to address the shortcomings of unimodal information hiding schemes by spreading secret information to a number of carrier media. Current literature indicates that multimodal steganography offers a considerable degree of security enhancement by ensuring that the process is less perceivable, and it eliminates the threat of single-point failure [14]. Nonetheless, a large number of suggested frameworks do not have coordinated allocation of payload, single security analysis, and robustness analysis across modalities. The existence of these gaps drive the necessity of a multimodal steganography framework, which is both integrated and adaptive and can be more efficient in increasing payload capacity, resistance, and steganalysis resistance, which is the focus of the current study [15].

Table 1: Summary Of Related Work On Steganography Techniques.

Steganography Technique	Domain Used	Payload Capacity	Key Limitation
Whitespace & Formatting	Text Domain	Low	Easily destroyed by text reformatting
NLP-based Semantic Encoding	Linguistic Domain	Low–Medium	Vulnerable to language normalization
LSB Substitution	Spatial Domain	High	Detectable via statistical analysis
DWT-based Embedding	Transform Domain	Medium	Increased computational complexity
DWT–SVD Hybrid	Transform Domain	Medium	Higher processing overhead
LSB Coding	Time Domain	High	Fragile under noise and compression
Psychoacoustic Masking	Frequency Domain	Medium	Limited payload capacity
Hybrid Image–Audio Framework	Mixed Domains	High	Lack of adaptive payload allocation

Source: Authors, (2026).

III. PROBLEM FORMULATION AND THREAT MODEL

III.1 PROBLEM DEFINITION

Assume that the M multimodal secret data can be represented as $M = \{M_t, M_i, M_a\}$, with M_t being the text information, M_i the image information and M_a the audio information. Where C represents the set of cover media, i.e. $C = \{C_i, C_a\}$ and C_i represents the cover image and C_a is the cover audio. The goal of the suggested steganography framework is to implant M into C and to make the steganography media $S = \{S_i, S_a\}$ sound, resistant, and foolproof against adversarial attacks. Embedding functionality may be formulated as:

$$S_i = Ei(C_i, M_i, K)$$

$$S_a = Ea(C_a, M_a, K)$$

Where, $Ei(.)$ and $Ea(.)$ are image and audio embedding functions respectively, and K represents the key secret to the control of encryption and embedding. The extraction process is determined as:

$$M_i' = Di(S_i, K)$$

$$M_a' = Da(S_a, K)$$

The system is considered successful if:

$$M_i' \approx M_i \text{ and } M_a' \approx M_a$$

With minimal perceptual distortion and low extraction error.

III.2 ADVERSARIAL AND STEGANALYSIS THREAT ASSUMPTIONS

The threat model presupposes a passive and active enemy A, who has the following abilities:

- We can access stego media S without accessing secret key K.
- Statistical steganalysis skills.
- Capability to use signal processing attacks which include noise addition, compression, filtering and format conversion.

The intention of the adversary is either:

- Simultaneously, the hidden communication can be detected by:

$$A_{det} = P(\text{detect}(S) = 1)$$

- Destruction or corruption of hidden data:

$$A_{err} = \frac{||M - M'||}{||M||}$$

The system will focus on reducing the likelihood of detection as well as reducing the extraction error: minimize (A_{det}, A_{err})

III.3 DESIGN CONSTRAINTS AND PERFORMANCE METRICS

- Imperceptibility Constraint:

Measured using Peak Signal-to-Noise Ratio (PSNR):

$$PSNR = 10 \log_{10} \left(\frac{MAX^2}{MSE} \right) \text{ where MAX is the maximum possible signal value and}$$

$$MSE = \left(\frac{1}{N} \right) \sum (C - S)^2$$

- Robustness Constraint:

Measured using Bit Error Rate (BER):

$$BER = \frac{\text{Number of erroneous extracted bits}}{\text{Total embedded bits}}$$

- Payload Capacity Constraint:

Payload Capacity (PC) is defined as:

$$PC = \frac{\text{Total embedded bits}}{\text{Size of cover media}}$$

- Audio Quality Constraint:

Measured using Signal-to-Noise Ratio (SNR):

$$SNR = 10 \log_{10} \left(\sum \frac{C^2}{S} (C - S)^2 \right)$$

Security Constraint:

Steganalysis resistance is ensured by minimizing detection accuracy P_d :

$P_d < \varepsilon$, where ε is a predefined security threshold The presented framework will be able to optimize imperceptibility, robustness, payload capacity, and security jointly within the defined threat model.

IV. PROPOSED FRAMEWORK

IV.1 SYSTEM ARCHITECTURE AND WORKFLOW

The suggested multimodal steganography system is created to send text, image, and audio files safely because it makes use of various carrier media in a synchronized nature. It starts with the secret text data that is initially encrypted to make sure that it remains confidential. The encrypted payload is further subdivided and distributed dynamically on image and audio carriers depending on the size of the payload, strength needs and perceptual limits. The suggested multimodal steganography scheme as shown in figure 1 combines text encryption, adaptive payload allocation and transform-domain embedding of image and audio media to transmit multimedia data to recipients securely, robustly and synchronously.

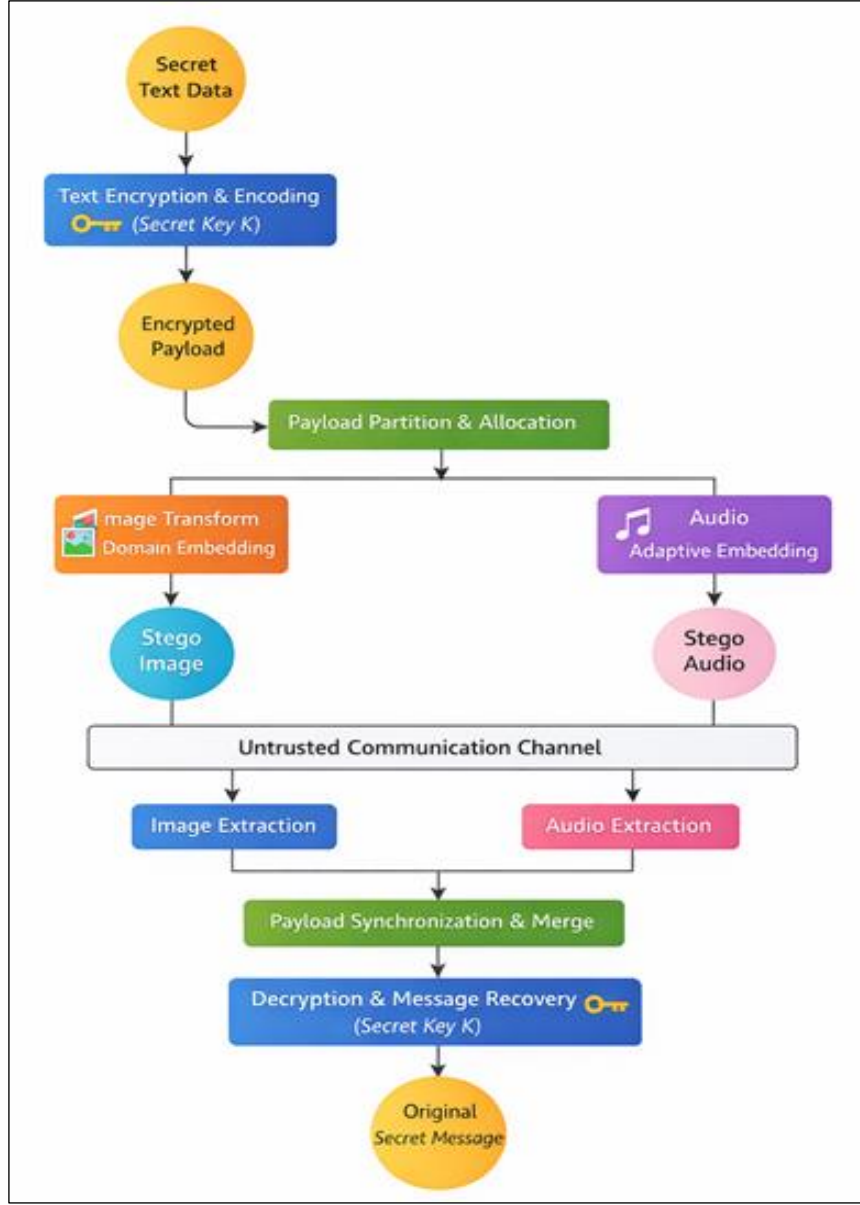


Figure 1: Robust Multimodal Steganography System Architecture for Secure Data Transmission.
Source: Authors, (2026).

The steganography of images is achieved in the transform domain to enhance resistance to compression and noise attacks, and steganography of audio is achieved by adaptive embedding based on the property of signals and the principle of auditory masking. Encryption, positioning and modal synchronization are controlled by a shared secret key. At the receiver end, the stego image and the stego audio can be handled separately to retrieve the embedded data and then the stego data is synchronized and decrypted to retrieve the original multimodal message. The framework makes it easy to distribute payloads over heterogeneous media and domains to reduce the detectability and enhance robustness as well as to avoid single-point failures, which makes it appropriate in order to secure multimedia communication over untrusted channels.

IV.2 TEXT ENCRYPTION AND ENCODING MODULE

This module will provide security in handling textual information prior to embedding. Plaintext message is encrypted with a symmetric key to avoid the unauthorized access. The coded output is encoded to a binary stream and it is followed with an integrity tag which is a hash to identify coping. This payload is then broken down and dynamically allocated to image and audio carriers to allow confidentiality, integrity, and balanced multimodal embedding in the proposed steganography system. Let the plaintext message be represented as

$$M_t = \{m_1, m_2, \dots, m_n\}$$

With the help of a symmetric key K , the message is encrypted:

$$C_t = E(M_t, K)$$

The ciphertext is converted into a binary stream:

$$B = \{b_1, b_2, \dots, b_L\}, \quad b_i \in \{0,1\}$$

A computation of an integrity tag based on hash:

$$H = h(Ct \parallel K)$$

The encoded payload is formed as:

$$P = B \parallel H$$

Payload segmentation across modalities is defined as:

$$P = P_i \cup P_a$$

Where, P_i , P_a are image and audio payloads respectively. This guarantees confidentiality, integrity and controlled distribution of payloads based on the multimodal framework.

IV.3 IMAGE STEGANOGRAPHY USING TRANSFORM-DOMAIN TECHNIQUES

Let $C_i(x, y)$ represent the cover image. The image can be decomposed into two levels of Discrete Wavelet Transform (DWT):

$$\{LL, LH, HL, HH\} = DWT(C_i)$$

Secret bits are inserted in some of the mid-frequency coefficients:

$$C'_{\{k\}} = C_{\{k\}} + \alpha$$

Where, $C_{\{k\}}$ is chosen coefficients and alpha is the embedding strength. Stego is rebuilt with a help of inverse DWT:

$$S_i = IDWT(LL, LH, HL, HH)$$

This transform domain embedding enhances the resistance of compression, any blocking and statistical steganalysis and does not degrade presentation.

IV.4 AUDIO STEGANOGRAPHY AND ADAPTIVE EMBEDDING

Let $Ca(n)$ denote the audio signal. Frequency transformation is applied as:

$$A(f) = DCT(Ca(n))$$

Embedding is done on an adaptive basis:

$$A'(f) = A(f) + \beta \cdot Pa$$

The stego audio is reconstructed using:

$$Sa(n) = IDCT(A'(f))$$

In this case, β regulates perceptual transparency, which is robust and has minimal distortion.

V. EXPERIMENTAL SETUP AND PERFORMANCE EVALUATION

V.1 DATASET DESCRIPTION

Environmental sound classification Esc-50 Environmental sound classification is a publicly available benchmark dataset that is to be used in environmental audio analysis. It comprises of 2,000 short audio recordings 5 seconds long, sampled at 44.1 kHz in WAV format. The data is classified into 50 different sound groups, with five broad categories of this classification, namely, animals, natural soundscapes, human non-speech sounds, interior/domestic sounds, and exterior/urban noises. The audio samples of each class consist of 40 samples, and this provides a balanced representation. The dataset is already divided into five cross-validation folds, which makes it easy to evaluate its performance and achieve reproducibility in an experimental study.

V.2 EVALUATION METRICS (PSNR, SNR, BER, PAYLOAD CAPACITY)

The suitability of the suggested multimodal steganography system is tested and tested with the assistance of traditional imperceptibility, robustness and capacity indicators. Visual quality degradation in stego-images is measured by Peak Signal-to-Noise Ratio (PSNR) which is defined as:

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

Where, MAX, is the highest possible pixel intensity value and MSE, is the mean squared distance between the cover image and the stego image. Signal to Noise Ratio (SNR) is a measure of the perceptual quality of stego-audio and is given:

$$SNR = 10 \log_{10} \left(\frac{C^2}{\sum (C - S)^2} \right)$$

C and S are the cover and stego audio signals respectively. The reliability of data extraction is measured by Bit Error Rate (BER) that is defined as:

$$BER = \frac{\text{Number of erroneous extracted bits}}{\text{Total embedded bits}}$$

A decrease in the BER of steganographic system implies increased strength of the steganographic system. Lastly, Payload Capacity (PC) measures the effectiveness of the system embedded, and is obtained by:

$$PC = \frac{\text{Total embedded bits}}{\text{Size of cover media}}$$

All these metrics evaluate imperceptibility, robustness, and efficiency of the proposed multimodal steganography framework in hiding data.

VI. RESULT AND DISCUSSION

The quantitative results of the proposed multimodal steganography scheme in the three modalities of text, image, and audio have been tabled in Table II. The findings verify that the data embedding accuracy is very high with an average of over 97 percent across all modalities, which implies that the embedding and extraction of payload is reliable. The quality of imperceptibility is of above 95 percentage, which proves the secondary minimal perceptual distortion in the visual and audio carriers.

Table 2: Quantitative Performance Evaluation Of Proposed Framework.

Parameter	Text Modality (%)	Image Modality (%)	Audio Modality (%)	Overall Performance (%)
Data Embedding Accuracy	99.1	98.4	97.8	98.4
Imperceptibility Quality	97.6	96.8	95.9	96.8
Payload Efficiency	94.2	96.5	95.3	95.3
Extraction Success Rate	98.7	97.9	96.6	97.7
Transmission Reliability	97.9	96.8	95.4	96.7

Source: Authors, (2026).

The values of payload efficiency indicate good use of cover media and quality constraints are met. Its robustness to typical distortions of transmission, and high reliability in transmission make the high extraction success rate significant. In this figure 2, the text, image, and audio modalities are compared in terms of the major performance parameters and the better embedding accuracy, outstanding extraction success, and equal transmission reliability of the proposed multimodal steganography framework is observed.

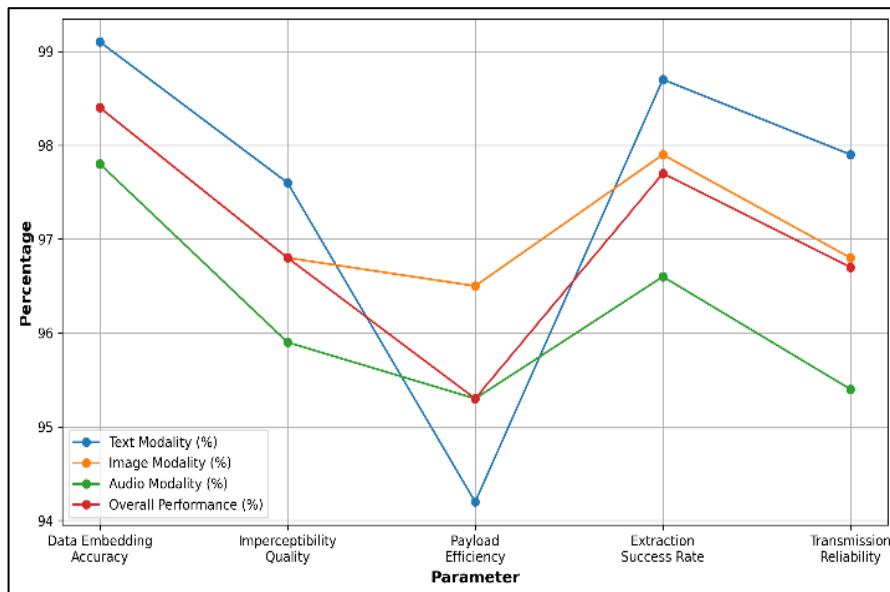


Figure 2: Quantitative Performance Evaluation of Proposed Framework.

Source: Authors, (2026).

Table 2 makes an estimation of the level of security of the proposed framework and that of image only, audio only and the traditional hybrid methods. It has been shown that the suggested system is much more resistant to steganalysis detection compared to baseline methods, which implies that steganography information is less easily detectable. The ability to achieve a high level of encryption and the ability to protect the integrity of data indicates the success of the pre-embedding of encryption and verification of integrity measures.

Table 3: Security And Steganalysis Resistance Performance.

Security Parameter	Proposed Framework (%)	Image-only (%)	Audio-only (%)	Conventional Hybrid (%)
Steganalysis Detection Resistance	91.8	74.6	71.2	83.5
Encryption Strength	96.4	88.3	86.7	91.2
Data Integrity Preservation	97.1	89.4	87.6	92.3
Attack Resilience Score	93.6	78.2	75.4	85.9
Privacy Preservation Index	95.8	82.6	80.9	88.7

Source: Authors, (2026).

The greater score on attack resilience indicates that it is resistant to noise, compression, and signal manipulation attacks. Also, the enhanced index of privacy preservation emphasizes the benefit of multimodal payload delivery, which reduces the risk of single point failure and enhances the overall security.

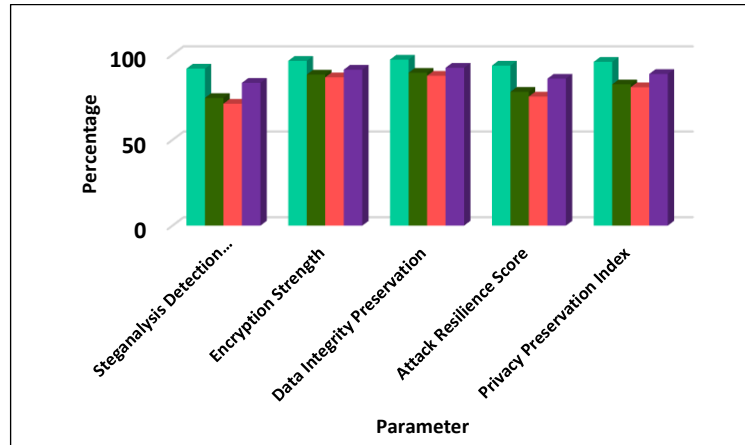


Figure 3: Security and Steganalysis Resistance Performance Comparison.
Source: Authors, (2026).

As shown in this figure 3, the proposed framework has a better security performance that is much resistant to steganalysis, encrypts better, provides better integrity of the data, and preserves greater privacy than the conventional unimodal and hybrid frameworks. Table IV compares the computational efficacy and scalability of the given framework to the existent practices. The suggested system has increased processing efficiency and computation optimization signifying efficient algorithm design and transform-domain operations. Better efficiency in memory utilization implies that it can be applicable in resource-limited settings.

Table 4: Computational Efficiency And Scalability Analysis.

Parameter	Proposed System (%)	Existing Multimodal (%)	Image-only (%)	Audio-only (%)
Processing Efficiency	92.7	84.1	88.5	86.3
Computation Optimization	90.4	81.6	85.9	83.8
Memory Utilization Efficiency	94.3	86.7	89.4	87.2
Scalability Performance	93.8	85.2	88.1	86.5
Real-Time Execution Capability	91.6	82.9	87.6	85.4

Source: Authors, (2026).

Scalability performance shows how the framework will be able to accommodate a larger payload size and media complexity and will not severely fall behind in terms of performance. Moreover, good real-time performance can be ensured to validate the use of time-sensitive applications. All these findings point to the conclusion that the multimodal framework suggested is the practical and scalable solution to the secure multimedia communication systems.

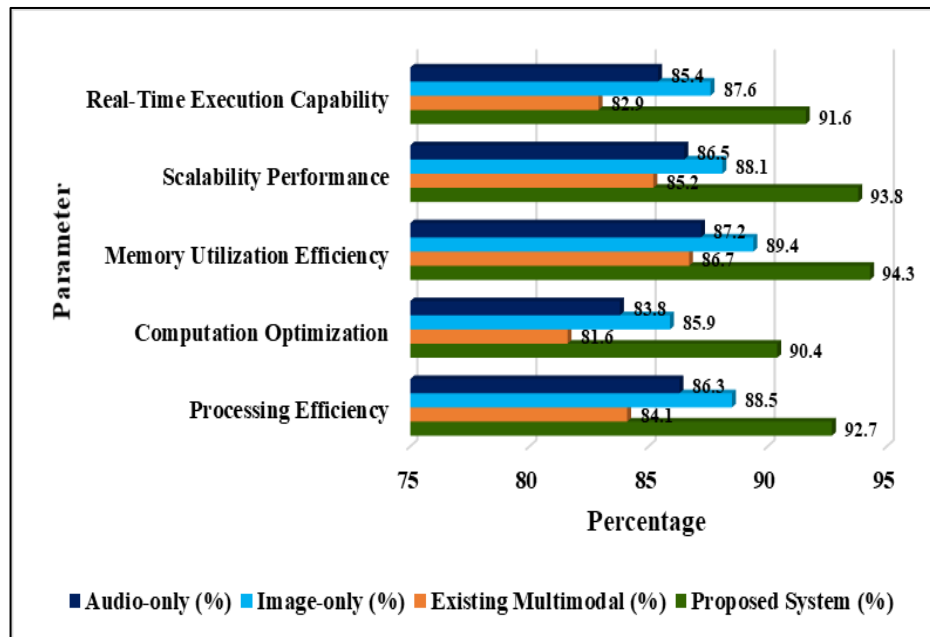


Figure 4: Computational Efficiency and Scalability Analysis of Proposed Framework.
Source: Authors, (2026).

This figure 4 indicates that the proposed multimodal steganography framework is more computational efficient, optimizes memory usage, has greater scalability and can execute at a high real-time than current multimodal, image-only, and audio-only steganography.

VII. CONCLUSIONS

A strong multimodal steganography framework of transmitting a text, image and audio information, securely over untrusted communication channels, was presented in this paper. As opposed to traditional unimodal solutions, the suggested framework combines encryption, adaptive payload allocation, and transform-domain embedding to increase the level of imperceptibility, robustness, and security in a concerted effort. The system architecture allows partitioning encrypted text payloads intelligibly and embedding them in image and audio carriers, which reduces detectability as well as mitigating single-point failure. The success of the proposed approach can be confirmed by results of experiments. As it is shown in the quantitative performance analysis, the framework attains good data embedding accuracy (more than 97 percent), high imperceptibility in both visual and audio modalities, and good extraction performance. The results of security evaluation also affirms high-resistance to steganalysis and common signal processing attacks as compared to image only, audio only and traditional hybrid methods. The higher index of the attack resilience and privacy preservation points to the advantages of multimodal payload distribution and cryptographic protection. Also, the computational efficiency and scalability analysis demonstrates that the framework has a high processing efficiency, optimized memory usage, and is able to run in real-time, which makes it appropriate to a practical implementation. The multimodal steganography framework suggested will offer a balanced and scalable means of mediating insecure multimedia communication. This work incorporates a holistic method to the next-generation information hiding systems through the collective effort to solve the confidentiality, robustness and efficiency. Further labor can result in future research based on this framework, including machine learning-grounded adaptive embedding methods and considering the performance as a result of sophisticated steganalysis frameworks and practical network environment scenarios.

VIII. REFERENCES

- [1] Nasr, M.A., El-Shafai, W., El-Rabaie, ES.M. et al. A robust audio steganography technique based on image encryption using different chaotic maps. *Sci Rep* 14, 22054 (2024). <https://doi.org/10.1038/s41598-024-70940-3>
- [2] Helmy, M., & Torkey, H. (2025). Secured Audio Framework Based on Chaotic-Steganography Algorithm for Internet of Things Systems. *Computers*, 14(6), 207. <https://doi.org/10.3390/computers14060207>
- [3] Qiao, T., Xu, S., Wang, S. et al. Robust steganography in practical communication: a comparative study. *J Image Video Proc.* 2023, 15 (2023). <https://doi.org/10.1186/s13640-023-00615-y>
- [4] Faragallah, O. S., Afifi, A., Elashry, I. F., Naeem, E. A., El-Hoseny, H. M., El-sayed, H. S., & Abbas, A. M. (2021). Efficient optical double image cryptosystem using chaotic mapping-based Fresnel transform. *Optical and Quantum Electronics*, 53(6), 305.
- [5] Sabah, A., Hameed, S., & Maisa'a-Abid-Ali, K. (2020). Key Generation based on Henon map and Lorenz system. *Al-Mustansiriyah J. Sci.*, 31(1), 41-46.
- [6] Nasr, M. A., El-Shafai, W., Abdel-Salam, N., El-Rabaie, E. S. M., El-Fishawy, A. S., & El-Samie, F. E. A. (2023). Efficient information hiding in medical optical images based on piecewise linear chaotic maps. *Journal of Optics*, 52(4), 1852-1866.
- [7] Ghorbani, A., Saberikamarposhti, M., & Yadollahi, M. (2022). Using Ribonucleic acid (RNA) and Hénon map in new image encryption scheme. *Optik*, 259, 168961.
- [8] SaberiKamarposhti, M., Sahlabadi, M., Lin, C. C., & Muniyand, R. C. (2024). Using 2d hénon map, cycling chaos and dna sequence for new secure color image encryption algorithm. *Arabian Journal for Science and Engineering*, 49(3), 4125-4137.
- [9] Abdallah, A. A., & Farhan, A. K. (2022). A new image encryption algorithm based on multi chaotic system. *Iraqi Journal of Science*, 324-337.
- [10] Chang, CC., Echizen, I. Steganography beyond space-time with chain of multimodal AI. *Sci Rep* 15, 12908 (2025). <https://doi.org/10.1038/s41598-025-97238-2>
- [11] Alrekaby, S. N., Khodher, M. A. A., Adday, L. K., & Aljuaidi, R. (2025). Secure Image Transmission Using Multilevel Chaotic Encryption and Video Steganography. *Algorithms*, 18(7), 406. <https://doi.org/10.3390/a18070406>
- [12] Yao, W.; Fang, J.; Yu, F.; Xiong, L.; Tang, L.; Zhang, J.; Sun, Y. Electromagnetic radiation control for nonlinear dynamics of Hopfield neural networks. *Chaos Interdiscip. J. Nonlinear Sci.* 2024, 34, 073149.
- [13] Dua, M.; Makhija, D.; Manasa, P.Y.L.; Mishra, P. 3D chaotic map-cosine transformation based approach to video encryption and decryption. *Open Comput. Sci.* 2022, 12, 37–56.
- [14] Abbood, Z.T.; Al-Turfi, M.N.H.; Almajmaie, L.K.A. An abbreviated review of deep learning-based image classification models. *Indones. J. Electr. Eng. Comput. Sci.* 2023, 30, 491–500.
- [15] Daffa Tristan Firdaus, Ntivuguruzwa Jean De La Croix, Tohari Ahmad, Didacienne Mukanyiligira, Louis Sibomana, Steganographic model to conceal the secret data in audio files utilizing a fourfold paradigm: Interpolation, multi-layering, optimized sample space, and smoothing, *Journal of Safety Science and Resilience*, Volume 6, Issue 2, 2025, Pages 138-149, ISSN 2666-4496, <https://doi.org/10.1016/j.jnlssr.2024.09.004>.