International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(19s) 2026 pp. 203-212
https://doi.org/10.70917/ijcisim-2026-5014
Article

AN ADAPTIVE CROSS-MEDIA STEGANOGRAPHY FRAMEWORK FOR INTELLIGENT HIDING MEDIUM SELECTION

S. Julia Little Sha[1], Dr. M. Ramesh Kumar[2]

[1] Research Scholar, PG and Research Department of Computer Science, Government Arts College (Autonomous), Nandanam, Chennai – 600035, Tamil Nadu, India. Email: julialittlesha@gmail.com ORCID: 0009-0001-3687-5533
[2] Associate Professor & Head, PG and Research Department of Computer Science, Government Arts College (Autonomous), Nandanam, Chennai – 600035, Tamil Nadu, India. Email: proframeshkumar@gmail.com

Abstract: Most of the steganography techniques now in use, use single carrier media and fixed embedding techniques, which impairs performance under different payload sizes and channel circumstances. This study suggests a dynamic cross-media steganography framework based on payload and channel analysis to get around these restrictions. In order to choose the best hiding medium and embedding technique, the suggested system intelligently evaluates payload size and channel conditions. When compared to traditional steganography techniques, experimental results demonstrate enhanced imperceptibility, embedding capacity, and robustness. This offers a single steganography system that can handle various payload sizes without the need for human interaction.
Keywords: Steganography, Cross-Media, Data Hiding, LSB, MSE, PSNR

1. INTRODUCTION

Fixed embedding techniques are the primary method used by conventional steganography systems, which do not take payload size and transmission conditions into account. These static methods frequently fall short of striking the right balance between robustness, imperceptibility, and embedding capacity. While unreliable communication links can harm the hidden information during transmission, large payload embedding may cause considerable distortion.

However, most existing approaches are designed for a single carrier medium and rely on predefined embedding parameters. In practical communication environments, payload size and channel conditions vary dynamically, making fixed embedding mechanisms inefficient for secure multimedia communication.

This research suggests a dynamic cross-media steganography architecture based on payload and channel analysis to overcome these drawbacks. Prior to choosing a suitable hiding medium and embedding technique, the suggested system intelligently evaluates payload size and channel conditions. The framework seeks to enhance embedding capacity, imperceptibility, and robustness by modifying the embedding process based on communication requirements.

Current steganography techniques usually work on a single carrier medium, therefore depending on the payload features, users must manually choose an image, audio, or video. When communication needs change, this kind of manual selection restricts scalability and adaptability. The suggested architecture overcomes this restriction by introducing an adaptive decision engine that chooses the best carrier medium by automatically analyzing payload size and channel conditions.

2. EXISTING CHALLENGES

The efficacy of current data hiding techniques is still constrained by a number of issues, despite notable developments in steganography. The majority of traditional methods use fixed embedding techniques without taking communication environments' dynamic nature into account. Because of this, these technologies' performance differs greatly depending on the payload and transmission conditions.

The payload-size dependency is one of the main issues. Significant distortion may happen when a lot of hidden data is embedded in a carrier medium, making the stego media less imperceptible. On the other hand, employing cautious embedding techniques for small payloads could result in an ineffective use of the embedding capacity.

The fluctuating channel conditions present another significant obstacle. Stego media may experience data loss, interference, noise, or compression during transmission. Reduced resilience and unsuccessful recovery of the hidden information are the results of conventional steganography algorithms' frequent inability to adjust to these shifting settings.

Furthermore, the majority of current systems are made for a single carrier medium, such audio, video, or picture. These methods are not adaptable enough to deal with a variety of communication situations. Their overall performance and flexibility are further restricted by the lack of an intelligent system for choosing a suitable hiding medium.

These difficulties emphasize the necessity for an adaptive steganography framework that can dynamically choose appropriate embedding techniques and analyze communication requirements. Resolving these issues can greatly increase communication reliability, robustness, and embedding efficiency.

3. ADAPTIVE CROSS-MEDIA STEGANOGRAPHY FRAMEWORK

An adaptive steganography system that can dynamically choose a suitable hiding medium based on payload size and channel conditions is introduced by the suggested framework. The suggested framework examines communication requirements prior to carrying out the embedding process, in contrast to traditional steganography techniques that use predefined embedding algorithms.

Payload Characterization, Channel Condition Estimation, Adaptive Medium Decision Process, and Dynamic Embedding Mechanism are the four main parts of the framework. To determine the embedding requirement, the secret message's payload size is first examined. Concurrently, the communication channel is assessed to determine the necessary robustness and transmission reliability.

The Adaptive Medium Decision Process chooses the best carrier medium between image, audio, and video based on the factors that were examined. Due to their great imperceptibility, image-based embedding is typically used for smaller payloads with steady transmission circumstances. To increase embedding capacity and robustness, audio or video media may be targeted by larger payloads or unstable channel circumstances.

The Dynamic Embedding Mechanism uses a suitable embedding technique to carry out the data hiding operation after the medium has been chosen. The framework may balance embedding capacity, imperceptibility, and robustness in accordance with communication requirements thanks to its adaptive decision-making capabilities. The overall workflow of the proposed framework is illustrated in Figure 1.

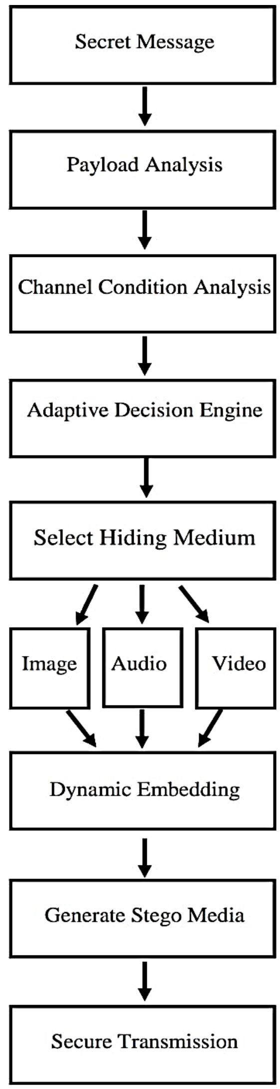


Figure 1: CMS Framework

4. MATHEMATICAL MODELING AND OPTIMIZATION

The suggested CMS architecture makes use of mathematical models based on payload properties and channel conditions to enable intelligent medium selection. These models let the Adaptive Decision Engine choose the best hiding medium by quantifying communication requirements.

A. Payload Model

The amount of confidential data to be encoded in a carrier media is represented by the payload size. It is stated as:

$$P=|M|$$

where:

- P = Payload size
- M = Secret message

To normalize the embedding requirement, the payload ratio is calculated as:

$$\rho = \frac{P}{Cmax}$$

where:

- ρ = Payload ratio
- $Cmax$= Maximum embedding capacity

Increased embedding demand is indicated by a higher payload ratio, which also affects medium choice.

B. Channel Quality Model

The channel condition is represented through a Channel Quality Index (CQI).

$$CQI = \frac{1}{N + Cp + L + I}$$

where:

- N = Noise level
- Cp = Compression probability
- L = Packet loss rate
- I = Interference level

Higher CQI values indicate better transmission conditions, while lower values represent unstable communication environments.

C. Medium Selection Score

The suitability of each medium is determined using a decision score:

$$Sm = \alpha Cm + \beta Rm + \gamma Dm$$

where:

- Sm= Selection score
- Cm = Embedding capacity
- Rm = Robustness
- Dm = Distortion
- α, β, γ= Weight factors

The medium with the highest score is selected:

$$m* = \arg\max(Sm)$$

where:

$$m \in \{Image, Audio, Video\}$$

D. Optimization Objective

The objective of the proposed framework is:

$$\max(\text{Capacity} + \text{Robustness} - \text{Distortion})$$

This improvement maintains transmission reliability and media quality while enabling effective embedding.

5. EXPERIMENTAL SETUP AND PERFORMANCE METRICS

Under various payload sizes and channel conditions, the effectiveness of the suggested Adaptive Cross-Media Steganography (CMS) framework was assessed. The purpose of the tests was to evaluate the adaptive medium selection mechanism's performance in terms of robustness, capacity, and embedding quality.

A. Experimental Environment

Python was used to implement the suggested framework on a computer running Windows, an Intel Core i5 processor, and 8 GB of RAM. The adaptive medium selection procedure was assessed using image, audio, and video files as carrier media.

B. Test Parameters

The experiments were conducted using varying payload sizes categorized as:

- Small Payload: 1–10 KB
- Medium Payload: 10–50 KB
- Large Payload: Above 50 KB

Similarly, channel conditions were classified as:

- Stable Channel
- Moderate Channel
- Noisy Channel

The performance of the proposed framework was evaluated using the following metrics:

- Mean Squared Error (MSE): Lower values indicate less distortion between the cover and stego media (Ideal: Closer to 0).
- Peak Signal-to-Noise Ratio (PSNR): Higher values indicate better stego media quality (PSNR > 40 dB indicates good quality, while PSNR > 50 dB indicates excellent quality).

These parameters were utilized to evaluate the adaptability of the proposed framework under different communication scenarios.

C. Performance Metrics

The effectiveness of the proposed CMS framework was measured using the following performance metrics.

Peak Signal-to-Noise Ratio (PSNR)

PSNR evaluates the visual quality of the stego media after embedding.

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

where:

- MAX = Maximum pixel value
- MSE = Mean Square Error

Higher PSNR values indicate better imperceptibility.

Mean Square Error (MSE)

MSE measures the difference between the cover media and stego media.

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(X_{ij} - Y_{ij})^2$$

where:

- X = Original media
- Y = Stego media

Lower MSE values indicate lower distortion.

Embedding Capacity

Embedding capacity represents the amount of secret information successfully hidden within the carrier medium.

$$\text{Capacity} = \frac{Embedded\ Data}{Carrier\ Size}$$

Higher embedding capacity indicates efficient utilization of the carrier medium.

Robustness

Robustness measures the ability of the hidden information to survive transmission disturbances such as noise and compression.

$$\text{Robustness} = \frac{Recovered\ Data}{Embedded\ Data} \times 100$$

Higher robustness values indicate better resistance against transmission effects.

The performance of the suggested adaptive framework under various payload and channel conditions was compared using the aforementioned metrics. The next section presents and analyzes the results that were collected.

6. RESULTS AND PERFORMANCE ANALYSIS

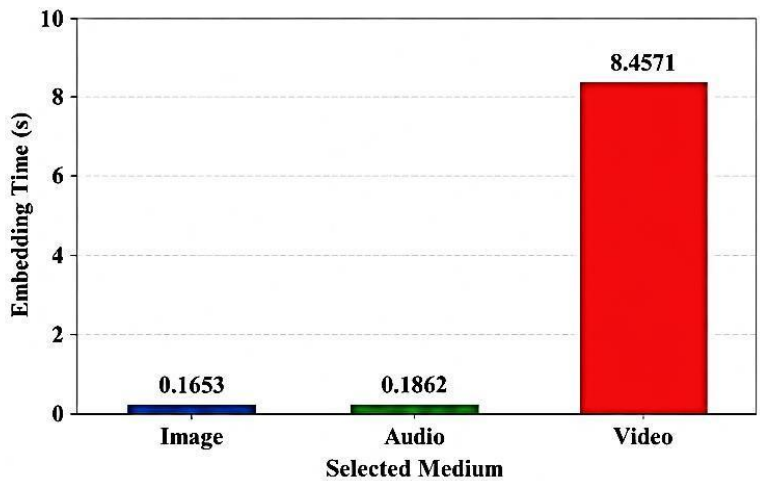
Under moderate channel conditions, the suggested Adaptive Cross-Media Steganography (CMS) framework was assessed using various payload sizes. The framework chose the best carrier medium for embedding after automatically analyzing the payload size. Embedding time, MSE, PSNR, and embedding capacity were used to assess the performance. To confirm the efficacy of the adaptive medium selection process, several validation experiments were carried out.

A. Experimental Results:

Before choosing the carrier media, the suggested framework first examines the payload size and channel condition. The secret message is automatically categorized into Small, Medium, or Large groups based on the payload size, and the transmission environment is assessed by evaluating the channel condition. The channel condition in the experimental setup was determined to be moderate. The Adaptive Decision Engine automatically chose the best carrier medium for secure data embedding based on these inputs.

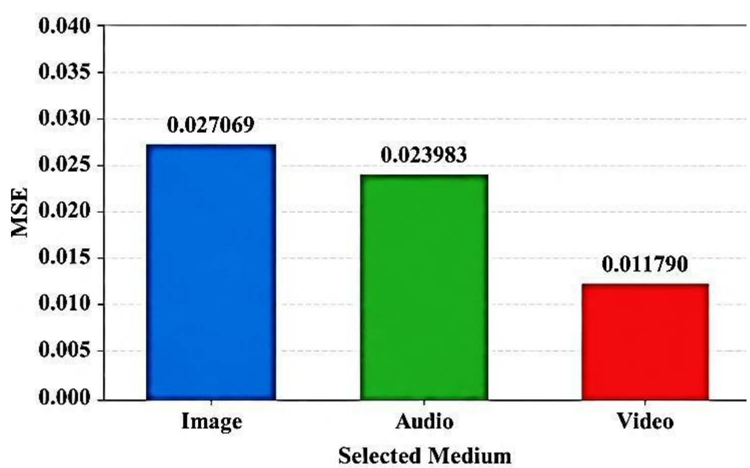
Experiment	Payload Size (Bytes)	Payload Category	Channel Condition	Selected Medium	Embedding Time (s)	MSE	PSNR (dB)	Status
1	4,985	Small	Moderate	Image	0.1653	0.027069	63.81	Success
2	19,983	Medium	Moderate	Audio	0.1862	0.023983	64.33	Success
3	349241	Large	Moderate	Video	8.457091	0.01179	67.42	Success

Table 1. Experimental Result



6.1 Figure 2: Embedding Time Comparison

The embedding times of the three embedding media are contrasted in Figure 2. Due to frame-by-frame processing, video embedding took significantly longer to execute than image and audio embedding.



6.2 Figure 3: MSE Comparison

The MSE values obtained upon embedding are shown in Figure 3. Low MSE values were attained by all three media, suggesting that only slight changes were made to the cover media throughout the embedding procedure.

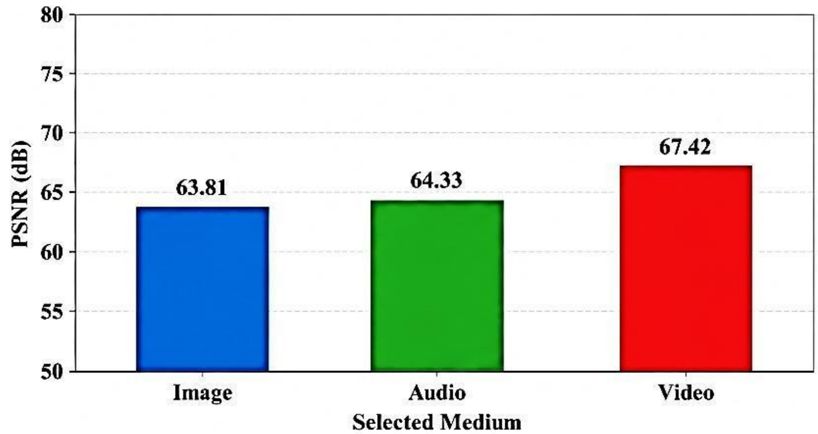


Figure 4:PSNR Comparison

The PSNR values for the chosen media are shown in Figure 4. Better media quality upon embedding is indicated by higher PSNR values. The experimental findings verify that the suggested framework safely embeds the hidden message while maintaining the carrier media's quality.

B. Validation of Adaptive Medium Selection

Further tests were carried out to see whether the chosen embedding media was appropriate for various payload categories in order to confirm the efficacy of the suggested Adaptive Cross-Media Steganography Framework. Verifying that the adaptive decision engine chooses the best carrier media based on payload size while preserving embedding quality and reducing distortion was the goal.

Validation Scenario	**Status**	**Embedding Time (s)**	**MSE**	**PSNR (dB)**	**Observation**
Medium Payload → Image	Success	**0.2265**	**0.133788**	**56.87**	Medium payload was successfully embedded into the image with acceptable quality.
Large Payload → Image	Failed	—	—	—	Embedding failed due to insufficient image embedding capacity.
Large Payload → Audio	Success	**1.2019**	**0.312593**	**53.18**	Large payload was successfully embedded into the audio medium.

Table 2. Validation of Adaptive Medium Selection

The suggested Adaptive Medium Selection strategy's validation results are shown in Table 2. With respectable embedding quality, the medium payload was successfully incorporated into the picture. However, because the needed embedding capacity was greater than the available picture capacity, the huge payload could not be integrated into the image, leading to embedding failure. With acceptable MSE and PSNR values, the same sizable payload was successfully incorporated into the audio medium. These validation findings show that choosing the embedding medium based on payload size enhances embedding capability and confirms the efficacy of the suggested adaptive framework.

C. Discussion

The experimental findings show that the suggested adaptive framework was successful in choosing the right embedding medium according to payload size. Low distortion and high media quality are shown by the obtained MSE and PSNR values. Adaptive medium selection enhances embedding capability, especially for big payloads, as the validation studies further shown.

7. CONCLUSION

An Adaptive Cross-Media Steganography Framework for intelligent medium selection based on payload size was presented in this paper. The successful embedding with minimal distortion and adequate media quality was proven by the experimental results. The validation findings also showed that, particularly for big payloads, adaptive medium selection offers superior embedding capacity compared to a fixed-medium strategy.

REFERENCES

1. M. H. Kombrink, Z. J. M. H. Geradts and M. Worring, "Image Steganography Approaches and Their Detection Strategies: A Survey," ACM Computing Surveys, vol. 57, no. 2, pp. 1–40, 2024.
2. B. A. Dharani, B. Yashaswini, G. R. Shyashyankha Reddy and S. M. Rajagopal, "Multimodal Steganography: A Comparative Analysis of LSB and DCT Methods for Image and Audio Data Concealment," 2024 IEEE 9th International Conference for Convergence in Technology (I2CT), 2024.
3. L. Zhao, H. Li, X. Ning and X. Jiang, "THInImg: Cross-Modal Steganography for Presenting Talking Heads in Images," Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision (WACV), pp. 5553–5562, 2024.
4. H. Elshoush and M. Mahmoud, "Ameliorating LSB Using Piecewise Linear Chaotic Map and One-Time Pad for Superlative Capacity, Imperceptibility and Secure Audio Steganography," IEEE Access, vol. 11, pp. 33354–33380, 2023.
5. Y. Wang, "Hiding Data within Thumbnail Videos: An Adaptive Downsampling-Resilient Video Steganography Method," IEEE Access, 2024.
6. Y. Zhao, Y. Liu, H. Zhao and Y. Wang, "A Video Security Verification Method Based on Blockchain," 2023 IEEE International Conference on Blockchain, 2024.
7. "Adaptive Reversible Image-Data Hiding Algorithm Based on Blockchain and Zero Watermarking," Optics & Laser Technology, vol. 179, 2024.
8. "A Novel Encrypted Data Hiding and Image Encryption for Authentication Based Communication Framework," 2024 IEEE International Conference on Smart Electronics and Secure Systems (ICSESS), 2024.
9. "Enhancing Audio Steganography: Advancing Audio Steganography with Cryptographic Hashing," 2024 IEEE International Conference on Advanced Computing, Communication and Networks, 2024.
10. I. M. A., M. B. Muazu, A. E. Adedokun and B. O. Sadiq, "An Extensive Survey of Digital Image Steganography: State of the Art," arXiv, 2024.
11. R. F. Bunyamin, A. W. C. D'Layla, N. J. De La Croix, and T. Ahmad, "Adaptive Steganography Approach in RGB Images Based on Color Channels to Enhance Stego Image Quality," Proc. 2024 IEEE 16th Int. Conf. on Communication Systems and Network Technologies (CICN), pp. 542–546, 2024.
12. L. Zhang, Y. Lu, T. Li, and G. Lu, "Joint Adaptive Robust Steganography Network," IEEE Transactions on Industrial Informatics, vol. 20, no. 8, pp. 10156–10166, 2024.
13. Y. Wang, "Hiding Data Within Thumbnail Videos: An Adaptive Downsampling-Resilient Video Steganography Method," IEEE Access, vol. 12, 2024.
14. L. Zhao, H. Li, X. Ning, and X. Jiang, "THInImg: Cross-Modal Steganography for Presenting Talking Heads in Images," Proc. IEEE/CVF Winter Conference on Applications of Computer Vision (WACV), pp. 5553–5562, 2024.
15. A. A. M. Fadhl, H. O. M. Shareif, M. A. E. Ali, and A. M. A. Elmangoush, "Adaptive Image Steganography: A Review and Research Directions," Proc. 2024 IEEE 7th Int. Conf. on Advanced Technologies, Signal and Image Processing (ATSIP), 2024.
16. S. M. Jati, N. J. De La Croix, and T. Ahmad, "Enhanced Secret Data Hiding in Audio Samples via Bit Distribution and Segmentation," Proc. IEEE, 2024.

17. L. A. Sandhu, E. Shahzad, F. Yaqoob, S. A. Butt, W. Khan, and I. M. Qureshi, "A New Paradigm for Improved Image Steganography by Using Adaptive Number of Dominant Discrete Cosine Transform Coefficients," 2023.
18. S. Song, S. Yang, C. D. Yoo, and J. Kim, "Implicit Steganography Beyond the Constraints of Modality," 2023.
19. H. Kheddar, M. Hemis, Y. Himeur, D. Megías, and A. Amira, "Deep Learning for Steganalysis of Diverse Data Types: A Review of Methods, Taxonomy, Challenges and Future Directions," 2023.
20. I. M. A., M. B. Muazu, A. E. Adedokun, and B. O. Sadiq, "An Extensive Survey of Digital Image Steganography: State of the Art," 2024.