

# Adaptive Dynamic Steganography Algorithm for Secure and Efficient Data Hiding Using RACESA

Shweta Sahu<sup>1</sup>, Kusum Sharma<sup>2</sup>

Student, Computer Science and Engineering, RSR Rungta College of Engineering and Technology, Bhilai,

Chhattisgarh, India<sup>1</sup>

Assistant Professor, Computer Science and Engineering, RSR Rungta College of Engineering and Technology, Bhilai,

Chhattisgarh, India<sup>2</sup>

**Abstract:** Steganography provides a means of concealing secret information within a cover medium while maintaining its perceptual quality and security. However, the use of a fixed embedding technique may not provide an appropriate balance between security, capacity, distortion, and computational requirements for different data-hiding scenarios. This paper proposes RACESA (Runtime-Adaptive Cover and Embedding Strategy Algorithm), a framework that dynamically selects a suitable cover medium, existing embedding strategy, and embedding parameters according to runtime requirements. The proposed approach considers secret-data characteristics, security requirements, payload capacity, allowable distortion, execution time, and memory limitations. Candidate configurations are filtered and evaluated using a multi-criteria selection mechanism, followed by embedding and constraint verification. If the selected configuration fails to satisfy the specified requirements, an alternative feasible configuration is considered. The proposed framework provides a flexible decision-making mechanism for adapting existing steganographic techniques to different application requirements.

**Keywords:** Steganography, Adaptive Steganography, Dynamic Data Hiding, Cover Selection, Embedding Strategy, Secure Data Hiding, RACESA.

## 1. INTRODUCTION

The increasing exchange of digital information has created a need for secure methods of data protection. Steganography addresses this need by concealing secret information within a digital cover so that the presence of the hidden data is difficult to detect. The effectiveness of a steganographic system depends on factors such as security, embedding capacity, distortion, and computational cost.

Conventional methods generally use a predefined embedding technique, which may not perform equally well for different secret data and application requirements. Adaptive approaches improve this process by considering the characteristics of the cover or secret data during embedding. However, selecting an appropriate cover, embedding strategy, and parameter configuration simultaneously remains a challenging decision.

To address this issue, this paper proposes RACESA (Runtime-Adaptive Cover and Embedding Strategy Algorithm). The proposed framework evaluates the secret-data characteristics, security requirements, available covers, capacity, distortion tolerance, execution time, and memory constraints to select a suitable existing embedding strategy at runtime. The objective is to provide a flexible decision-making mechanism that can adapt the steganographic configuration to different data-hiding requirements.

## 2. LITERATURE REVIEW

Liao, Qin, and Ding (2017), in “Data Embedding in Digital Images Using Critical Functions,” investigated uniform and adaptive embedding frameworks. Their adaptive approach considers image contents and pixel correlations while determining embedding behavior. The study demonstrated that adapting the embedding process to image characteristics can improve visual quality and statistical undetectability.

Baluja (2017) proposed “Hiding Images in Plain Sight: Deep Steganography,” where neural networks were trained to hide a full-size color image inside another image of the same size. Instead of conventional LSB-based embedding, the

secret representation was compressed and distributed throughout the available cover information. This work established an important direction for high-capacity learned steganography.

Hayes and Danezis (2017) introduced “Generating Steganographic Images via Adversarial Training.” Their framework used an adversarial training process involving an encoder, decoder, and steganalyzer to learn embedding behavior while reducing detectability. The study demonstrated the potential of learning-based methods for jointly considering message recovery and resistance to steganalysis.

Zhang, Dong, and Liu (2018) proposed “Invisible Steganography via Generative Adversarial Networks.” Their ISGAN architecture concealed a grayscale secret image within a color cover image and used adversarial learning to improve security and visual similarity. The approach considered capacity, invisibility, and security within a learned embedding framework.

Wang, Tang, and Wang (2020) proposed “High-Capacity Adaptive Steganography Based on LSB and Hamming Code.” The method combined LSB replacement with Hamming coding and assigned more payload to edge regions because these regions can tolerate greater modification. Performance was evaluated using payload capacity, MSE, PSNR, and histogram analysis.

Shyla, Shiva Kumar, and Das (2021) investigated genetic-algorithm-based cover selection and embedding. Their approach used characteristics of candidate cover images to select a suitable carrier before embedding. The study demonstrates the relevance of automated cover selection in improving steganographic performance.

Alobaidi and Mikhael (2023) proposed “An Adaptive Steganography Insertion Technique Based on Wavelet Transform.” Their method used a two-dimensional discrete Haar filter and DWT to select coefficients for embedding. The work demonstrates how transform-domain characteristics can be used to adapt embedding locations according to cover properties.

Li, Guo, and Qin (2023) proposed “Diversified Cover Selection for Image Steganography.” Their method extracts steganalytic features from candidate images and uses a classifier to estimate their suitability for carrying secret information. The main objective is to select covers that provide improved resistance to steganalysis.

Wu, Hu, and Liu (2024) proposed “Security-Oriented Steganographic Payload Allocation for Multi-Remote Sensing Images.” Their method combines cover selection with adaptive payload allocation. A pretrained steganalysis model is used to assess cover security, while payloads are allocated according to the security and capacity of individual covers. The study is particularly relevant to RACESA because it connects cover selection, security, and payload allocation.

Kumar et al. (2024) proposed “Efficient Three Layer Secured Adaptive Video Steganography Method Using Chaotic Dynamic Systems.” Their adaptive control mechanism allows partial or full use of video-frame capacity, while a chaotic system provides multiple security layers. The reported payload range is 0.56–2.25 bpp, with PSNR values of 50.25–62.05 dB.

Wang et al. (2024) introduced “GAN-Based Adaptive Cost Learning for Enhanced Image Steganography Security.” Their work focuses on learning improved embedding-cost maps using a GAN-based architecture. The primary objective is to improve security by obtaining more suitable modification probabilities and reducing embedding distortion.

Chahine and Kim (2024) proposed “Neural Cover Selection for Image Steganography.” Instead of relying entirely on exhaustive searching based on perceptual or complexity measures, their approach searches the latent space of pretrained generative models to obtain suitable cover images. The study demonstrates the increasing importance of automated cover selection.

More recently, Azam et al. (2025) presented a systematic review of cover-selection methods for steganography. Their review examined 34 methods and analyzed cover types, search mechanisms, selection attributes, and evaluation metrics. The review indicates that cover selection has become an important independent research direction, while computational time and complexity remain less consistently reported across existing studies.

Recent 2025 studies have continued to explore adaptive embedding, including methods based on attention maps, transform-domain embedding, and adaptive privacy protection. These approaches further demonstrate the importance of adapting embedding behavior to image characteristics and application requirements.

**Research Gap**

The reviewed studies show that adaptive embedding, cover selection, payload optimization, security enhancement, and distortion reduction have each been investigated extensively. However, these capabilities are generally implemented within a particular medium or a particular embedding technique. The selection of a complete embedding configuration based simultaneously on secret-data characteristics, security, capacity, distortion, execution time, memory, available cover media, and existing embedding strategies remains comparatively less explored. Therefore, RACESA introduces a runtime decision layer that integrates these factors to select a suitable cover–strategy–parameter configuration.

**3. METHODS AND MATERIALS**

The proposed Runtime-Adaptive Cover and Embedding Strategy Algorithm (RACESA) dynamically selects a suitable steganographic configuration according to the characteristics of the secret data and the requirements of the embedding task. Unlike a fixed embedding approach, RACESA considers security, payload capacity, allowable distortion, available cover media, execution time, and memory limitations before selecting an appropriate configuration.

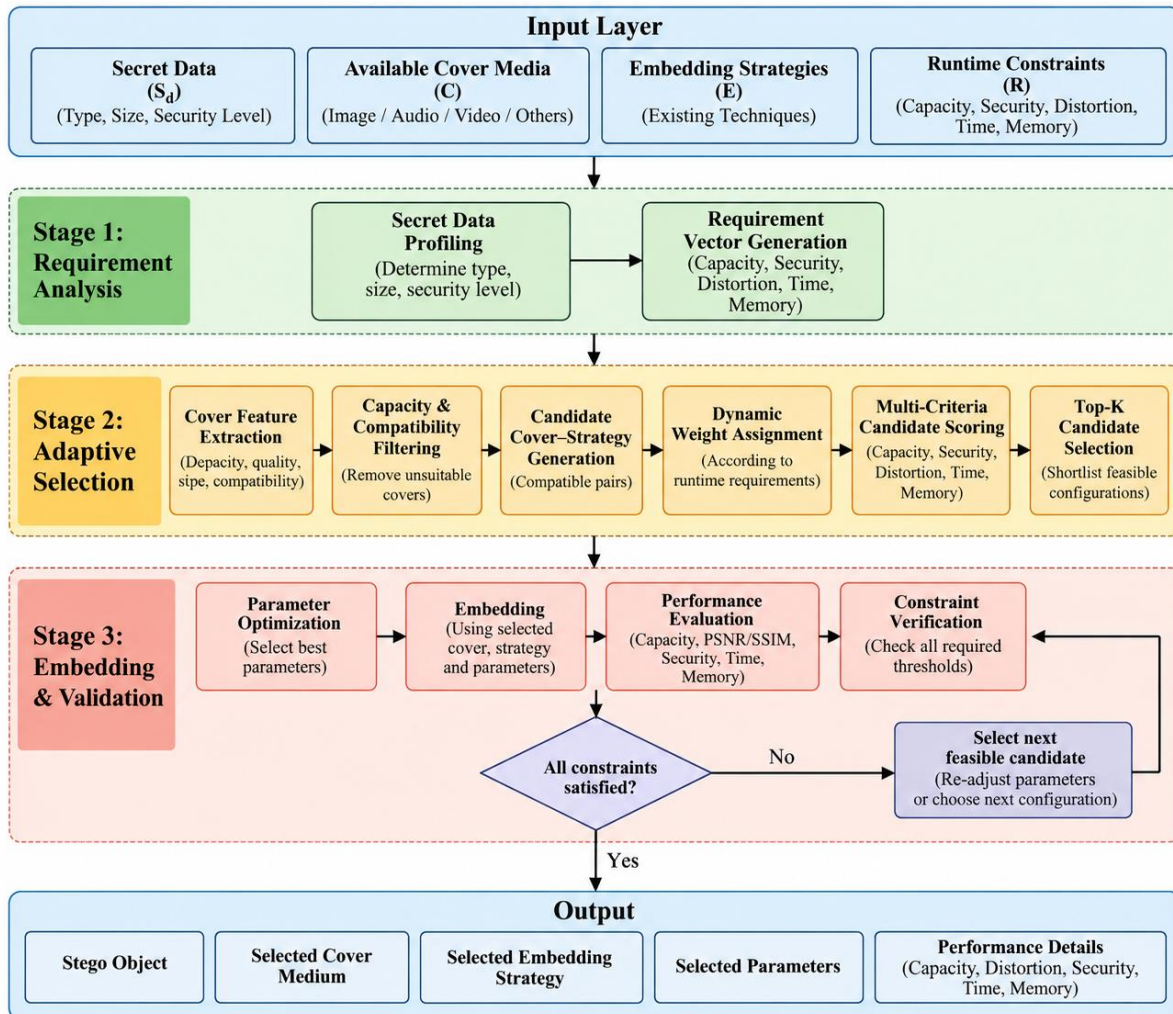
**3.1 Overall RACESA Procedure**

1. Secret Data Analysis: The secret data are analyzed according to their type, size, and required security level.
  2. Requirement Profiling: A requirement profile is generated based on capacity, security, distortion tolerance, execution time, and memory constraints.
  3. Cover Analysis and Filtering: Available cover media are examined for capacity, compatibility, and relevant characteristics. Covers that fail the basic requirements are eliminated.
  4. Candidate Generation: Compatible cover–embedding-strategy combinations are generated using established embedding techniques.
  5. Adaptive Selection: Dynamic weights are assigned according to the current requirements, and candidate configurations are evaluated using a multi-criteria scoring mechanism.
  6. Parameter Selection and Embedding: Suitable parameters are selected for the shortlisted configuration, followed by the embedding process.
  7. Performance Evaluation: The generated stego object is evaluated in terms of capacity, security, distortion/quality, execution time, and memory consumption.
  8. Constraint Verification: The obtained results are compared with the predefined requirements. If the selected configuration does not satisfy the mandatory constraints, an alternative feasible configuration is evaluated.
- The process continues until a satisfactory configuration is obtained or no feasible candidate remains. The output consists of the stego object and the selected cover, embedding strategy, and associated parameters.

**3.2 RACESA Framework**

The overall operation of RACESA is illustrated in Figure 1. The framework consists of three major stages: Requirement Analysis, Adaptive Selection, and Embedding & Validation. These stages enable the system to dynamically determine an appropriate configuration according to the requirements of the current data-hiding task.

## RACESA FRAMEWORK



**Figure 1. Proposed RACESA framework for runtime-adaptive selection of cover medium, embedding strategy, and embedding parameters.**

## 4. RESULTS AND DISCUSSION

The proposed RACESA framework is expected to provide adaptive selection of a suitable cover and embedding strategy according to the specified requirements. Since the framework considers multiple parameters simultaneously, its expected performance is evaluated in terms of capacity, imperceptibility, security, execution time, and memory consumption. Table 1 presents illustrative performance ranges for commonly considered embedding methods and the adaptive behavior targeted by RACESA.

Table 1. Predicted Performance Comparison

| Method | Capacity    | PSNR (dB) | SSIM      | Security Level | Time (s)              | Memory (MB)           |
|--------|-------------|-----------|-----------|----------------|-----------------------|-----------------------|
| LSB    | High        | 45–52     | 0.95–0.98 | Medium         | 0.10–0.30             | 40–60                 |
| PVD    | Medium–High | 48–55     | 0.96–0.99 | Medium–High    | 0.20–0.50             | 50–70                 |
| DCT    | Medium      | 50–58     | 0.97–0.99 | High           | 0.30–0.70             | 60–80                 |
| DWT    | Medium      | 52–60     | 0.97–0.99 | High           | 0.40–0.90             | 70–100                |
| RACESA | Adaptive    | ≥50       | ≥0.97     | Adaptive       | Requirement-dependent | Requirement-dependent |

The table demonstrates the principal idea behind RACESA: the selected technique is not fixed. When the security, capacity, distortion, or computational requirements change, the framework can select another feasible configuration.

## 5. CONCLUSION

This paper proposed RACESA (Runtime-Adaptive Cover and Embedding Strategy Algorithm) for dynamic selection of a suitable steganographic configuration. The framework considers secret-data characteristics, security, capacity, distortion, execution time, and memory requirements before selecting an appropriate cover, embedding strategy, and parameters. By evaluating and validating candidate configurations at runtime, RACESA provides a flexible decision-making layer over existing steganographic techniques. Future work will focus on implementation and experimental validation across different cover media and embedding strategies.

## REFERENCES

- [1]. S. Baluja, "Hiding Images in Plain Sight: Deep Steganography," *Advances in Neural Information Processing Systems (NeurIPS)*, vol. 30, 2017.
- [2]. J. Hayes and G. Danezis, "Generating Steganographic Images via Adversarial Training," *Advances in Neural Information Processing Systems (NeurIPS)*, vol. 30, pp. 1954–1963, 2017.
- [3]. X. Liao, Z. Qin, and L. Ding, "Data Embedding in Digital Images Using Critical Functions," *Signal Processing: Image Communication*, vol. 58, pp. 146–156, 2017. DOI: 10.1016/j.image.2017.07.006.
- [4]. R. Zhang, S. Dong, and J. Liu, "Invisible Steganography via Generative Adversarial Networks," 2018.
- [5]. Y. Wang, M. Tang, and Z. Wang, "High-Capacity Adaptive Steganography Based on LSB and Hamming Code," *Optik*, vol. 213, 164685, 2020. DOI: 10.1016/j.ijleo.2020.164685.
- [6]. T. Alobaidi and W. Mikhael, "An Adaptive Steganography Insertion Technique Based on Wavelet Transform," *Journal of Engineering and Applied Science*, vol. 70, article 144, 2023. DOI: 10.1186/s44147-023-00300-x.
- [7]. X. Li, D. Guo, and C. Qin, "Diversified Cover Selection for Image Steganography," *Symmetry*, vol. 15, no. 11, 2024, 2023. DOI: 10.3390/sym15112024.
- [8]. T. Wu, X. Hu, and C. Liu, "Security-Oriented Steganographic Payload Allocation for Multi-Remote Sensing Images," *Scientific Reports*, vol. 14, 4826, 2024. DOI: 10.1038/s41598-024-55474-y.
- [9]. D. Kumar, V. K. Sudha, N. Manikandan, and K. Ramaswamy, "Efficient Three Layer Secured Adaptive Video Steganography Method Using Chaotic Dynamic Systems," *Scientific Reports*, vol. 14, 18301, 2024. DOI: 10.1038/s41598-024-67074-x.
- [10]. D. Wang, G. Yang, J. Chen, and X. Ding, "GAN-Based Adaptive Cost Learning for Enhanced Image Steganography Security," *Expert Systems with Applications*, vol. 249, 123471, 2024. DOI: 10.1016/j.eswa.2024.123471.
- [11]. K. Chahine and H. Kim, "Neural Cover Selection for Image Steganography," 2024.
- [12]. M. H. Noor Azam, F. Ridzuan, M. N. S. M. Sayuti, A. H. Azni, N. H. Zakaria, and V. Potdar, "A Systematic Review on Cover Selection Methods for Steganography: Trend Analysis, Novel Classification and Analysis of the Elements," *Computer Science Review*, vol. 56, 100726, 2025. DOI: 10.1016/j.cosrev.2025.100726.