IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 1, January 2026

DOI: 10.17148/IARJSET.2026.13173

Adaptive Dynamic Steganography Algorithm for Secure and Efficient Data Hiding

Shweta Sahu[1], Ms. Kusum Sharma[2]

Student, Computer Science & Engineering, RSR-Rungta College of Engineering and Technology, Bhilai, India[1]

Assistant Professor, Computer Science & Engineering, RSR-Rungta College of Engineering and Technology, Bhilai, India[2]

Abstract: The rapid growth of digital communication has increased the need for secure methods to protect sensitive information. Steganography conceals secret information within a seemingly normal cover medium, but conventional techniques often use fixed embedding strategies that may not suit different secret-data types and security requirements. This paper proposes an Adaptive Dynamic Steganography Algorithm that selects an appropriate data-hiding strategy according to secret-data characteristics, sensitivity, required security level, and cover-medium properties. The approach analyzes input conditions at runtime and selects suitable parameters to balance security, embedding capacity, imperceptibility, and computational efficiency. It aims to reduce unnecessary distortion for low-risk data while providing stronger protection for highly sensitive information. The framework can be evaluated using embedding capacity, imperceptibility, security, computational complexity, and resistance to steganalysis.

Keywords: Adaptive dynamic steganography, RASACA, machine learning, artificial intelligence, data hiding, information security

1. INTRODUCTION

With the increasing use of digital communication, protecting sensitive information from unauthorized access has become an important concern. Steganography is a security technique that conceals secret information within a cover medium such as an image, audio, video, or text, making the presence of the hidden information difficult to detect.
Conventional steganographic methods generally rely on fixed embedding techniques and parameters. However, different secret data may have different security requirements, and a single fixed strategy may not provide an optimal balance between security, capacity, and imperceptibility.

To address this limitation, this paper proposes an Adaptive Dynamic Steganography Algorithm that selects suitable embedding strategies and parameters according to the characteristics of the secret data, required security level, and cover medium. The proposed approach aims to provide a flexible data-hiding mechanism that dynamically adapts to different requirements while maintaining an appropriate balance between security, embedding capacity, imperceptibility, and computational efficiency.

2. LITERATURE REVIEW

Baluja (2017), in Hiding Images in Plain Sight: Deep Steganography, proposed a deep neural network-based encoder–decoder framework capable of hiding a full-size color image inside another image, demonstrating the potential of deep learning for high-capacity image steganography.

Hayes and Danezis (2017), in Generating Steganographic Images via Adversarial Training, introduced adversarial training for steganography, where neural networks representing the sender, receiver, and steganalyst were trained in an adversarial setting. Their work focused on improving security and resistance to detection.

Zhu et al. (2018) proposed HiDDeN, a deep encoder–decoder framework for hiding data in images. The study demonstrated recovery of hidden information after operations such as blurring, pixel dropout, cropping, and JPEG compression, highlighting the importance of robustness.

Zhang et al. (2018) investigated GAN-based invisible steganography and demonstrated the use of generative adversarial networks to improve the imperceptibility and security of hidden information.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 1, January 2026

DOI: 10.17148/IARJSET.2026.13173

Duan et al. (2019) proposed a reversible image steganography scheme based on a U-Net structure, addressing limitations such as low embedding capacity and focusing on reversible recovery.
Himthani et al. (2022) conducted a comparative assessment of deep-learning-based image steganography using U-Net, V-Net, and U-Net++ architectures. Their results showed differences in embedding capacity and reconstructed/stego-image quality.

Bui et al. (2023) proposed RoSteALS, which uses pretrained autoencoder latent spaces and a lightweight secret encoder, focusing on secret recovery, image quality, and robustness. Mou et al. (2023) proposed a large-capacity and flexible video steganography network based on an invertible neural network, enabling multiple secret videos and key-controlled recovery.

Shadmand et al. (2024) proposed StampOne, a GAN-based printer-proof steganography approach designed to remain robust against printing, scanning, JPEG compression, blur, brightness and contrast variations, and other distortions.
Overall, existing studies have improved steganography in terms of capacity, imperceptibility, robustness, reconstruction quality, and security. However, the reviewed work primarily focuses on particular architectures, media, or performance objectives. The proposed work instead focuses on dynamic selection of a steganographic strategy according to secret-data characteristics, required security level, and cover-medium properties.

3. METHODS AND MATERIALS

The proposed work introduces an Adaptive Dynamic Steganography Algorithm that selects the data-hiding strategy according to the requirements of the current hiding task. Unlike conventional approaches that use a fixed embedding technique, the proposed method dynamically analyzes the input before performing data embedding.

3.1 Input Collection
The system takes the cover medium, secret data, and user-defined security requirements as input.

3.2 Secret Data Analysis
The secret data is analyzed based on its characteristics, such as data type, size, and sensitivity. A security requirement is assigned according to the importance of the information.

3.3 Cover Medium Analysis
The selected cover medium is analyzed to determine its properties and suitability for data embedding.

3.4 Dynamic Strategy Selection
Based on the secret-data characteristics, security requirement, cover-medium properties, and available capacity, the algorithm dynamically selects an appropriate embedding strategy and its parameters.

3.5 Adaptive Data Embedding
The selected strategy is applied to embed the secret information into the cover medium while attempting to minimize perceptible distortion.

3.6 Stego-Medium Generation
After successful embedding, the system generates the stego medium, which can be transmitted or stored as an ordinary digital medium.

3.7 Extraction and Verification
At the receiver side, the corresponding parameters or key are used to extract the secret data. The recovered information is then verified to ensure correct extraction.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 1, January 2026

DOI: 10.17148/IARJSET.2026.13173

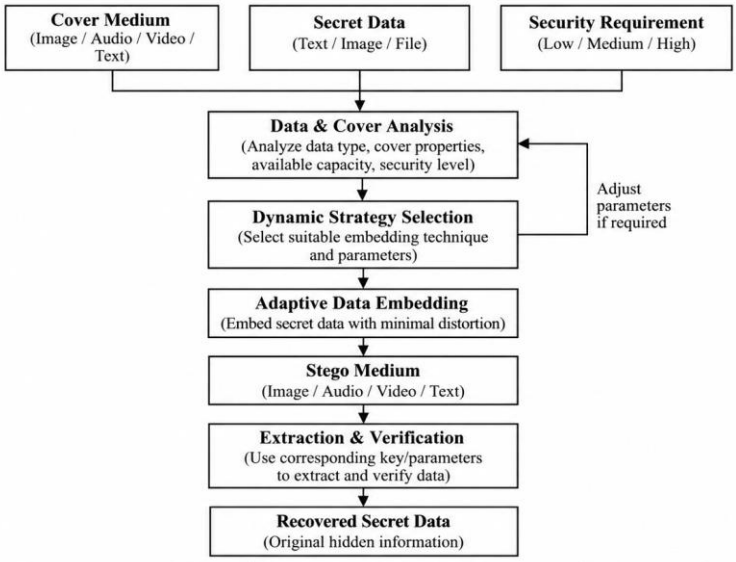

Fig. 1. Conceptual Flow of the Proposed Adaptive *Steganography* Framework

The overall objective of the proposed methodology is to dynamically balance security, embedding capacity, imperceptibility, and computational efficiency rather than optimizing only a single performance parameter.

4. RESULTS AND DISCUSSION

The supplied project material describes the proposed framework and identifies evaluation parameters including embedding capacity, imperceptibility, security, computational complexity, and resistance to steganalysis. It does not provide experimental datasets, numerical measurements, comparative tables, or completed test results. Therefore, no numerical performance claim is made here. The proposed framework can be evaluated by implementing the selected embedding strategies and comparing the resulting stego media using the identified metrics.

The evaluation should examine whether dynamic strategy selection can maintain an appropriate balance among security, embedding capacity, imperceptibility, and computational efficiency for different secret-data and cover-medium conditions.

5. CONCLUSION

This paper presents an Adaptive Dynamic Steganography Algorithm designed to select a suitable data-hiding strategy according to secret-data characteristics, security requirements, and cover-medium properties. The proposed framework replaces a single fixed embedding approach with runtime analysis and dynamic strategy selection. Its objective is to balance security, embedding capacity, imperceptibility, and computational efficiency. Future experimental evaluation should measure these factors and assess the framework against conventional fixed-parameter steganographic techniques.

REFERENCES

[1]. Baluja, S. (2017). Hiding Images in Plain Sight: Deep Steganography. NeurIPS.
[2]. Hayes, J., & Danezis, G. (2017). Generating Steganographic Images via Adversarial Training. arXiv.
[3]. Zhu, J., Kaplan, R., Johnson, J., & Fei-Fei, L. (2018). HiDDeN: Hiding Data with Deep Networks. ECCV.
[4]. Zhang, R., Dong, S., & Liu, J. (2018). Invisible Steganography via Generative Adversarial Networks. Springer.
[5]. Duan, X., et al. (2019). Reversible Image Steganography Scheme Based on a U-Net Structure. IEEE Access.
[6]. Himthani, V., et al. (2022). Comparative Performance Assessment of Deep Learning Based Image Steganography Techniques. Scientific Reports.
[7]. Bui, T., et al. (2023). RoSteALS: Robust Steganography Using Autoencoder Latent Space. CVPR Workshops.
[8]. Mou, C., et al. (2023). Large-Capacity and Flexible Video Steganography via Invertible Neural Network. CVPR.
[9]. Shadmand, F., et al. (2024). StampOne: Addressing Frequency Balance in Printer-proof Steganography. CVPR Workshops.