Vol 8, Issue 8, 2025 **Impact Factor: 8.535** DOI: https://doi.org/10.31426/ijamsr.2025.8.8.8612

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

Secure and Imperceptible Data Hiding Using Chaotic Map-Guided Embedding and Metaheuristic OOBO Optimization

Kshama Soni

Research Scholar, Department of Computer Application, Engineering College Bikaner, Rajasthan.

Dr. Rakesh Poonia

Assistant Professor, Department of Computer Application, Engineering College Bikaner, Rajasthan.

A B S T R A C T

In the digital era, secure and imperceptible data hiding techniques are essential for protecting sensitive information. This paper introduces a novel steganographic framework that combines chaotic systems with a metaheuristic optimization algorithm to enhance both security and visual quality. The approach employs a logistic chaotic map to generate dynamic pseudo-random sequences that guide the embedding locations within a cover image, increasing unpredictability and resilience against statistical attacks. A modified Least Significant Bit (LSB) technique is used for data embedding, leveraging the chaotic sequence to minimize visual distortion. To further improve performance, the One-to-One Based Optimizer (OOBO) is utilized to adaptively select embedding parameters through intelligent, population-based interactions. Experimental results indicate that the proposed method achieves an excellent trade-off among imperceptibility, payload capacity, and robustness, surpassing conventional techniques in both visual and statistical metrics. This integrated strategy holds significant potential for secure communication and digital copyright protection.

Keywords: Image Steganography, LSB Substitution, Chaotic Maps, Opposition-Based Optimization (OOBO), Secure Data Hiding & Metaheuristic Optimization.

1. Introduction

The increasing volume of digital data exchange in sensitive domains such as healthcare, finance, and defense necessitates robust information hiding techniques. Steganography—the art of concealing information within a cover medium—offers a promising solution. However, maintaining high imperceptibility and robustness while maximizing payload remains a challenging task. Traditional LSB-based methods often compromise on visual quality or security.

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

This paper presents a novel steganographic system that integrates chaotic maps for embedding position generation and a metaheuristic optimizer (OOBO) for adaptively optimizing embedding parameters. The combined use of chaos theory and optimization enhances the unpredictability and adaptability of the embedding process.

2. Related Work

2.1 Traditional LSB-based Steganography

Least Significant Bit (LSB) substitution is one of the earliest and most widely used steganographic techniques due to its simplicity and high embedding capacity. In LSB substitution, secret bits are embedded directly into the least significant bits of pixel values. While computationally efficient, these methods are highly vulnerable to visual quality degradation when the payload is large, and they are easily detected by statistical steganalysis techniques such as RS analysis and chi-square attacks. To overcome these weaknesses, several improvements have been proposed, including pixel-value differencing (PVD) schemes, which adaptively embed more data in high-variance regions, and edge-based embedding approaches, which exploit the human visual system's lower sensitivity to changes in edges. Transform-domain methods, such as those based on the discrete cosine transform (DCT) or discrete wavelet transform (DWT), have also been employed to improve robustness against compression and filtering. However, these methods often reduce embedding capacity and increase computational complexity.

2.2 Chaos-based Steganography

Chaos theory has been extensively explored in image processing due to its properties of sensitivity to initial conditions, pseudo-randomness, and ergodicity. In steganography, chaotic maps such as the Logistic map, Henon map, and Tent map have been used to generate embedding positions or to encrypt secret data before embedding. This enhances security by making the embedding process less predictable and resistant to brute-force and statistical attacks. For example, chaotic sequences can replace deterministic embedding paths in LSB substitution, thereby dispersing hidden bits across the cover image in an unpredictable manner. While chaos improves security, embedding strategies solely driven by chaotic maps may not optimally balance imperceptibility, robustness, and capacity without further adaptive control.

2.3 Metaheuristic Optimization in Steganography

Metaheuristic algorithms, inspired by natural and evolutionary processes, have been applied to optimize steganographic embedding strategies. Techniques such as Particle Swarm Optimization (PSO), Genetic Algorithms (GA), Differential Evolution (DE), and Ant Colony Optimization (ACO) have been employed to select embedding parameters (e.g., pixel selection, embedding rate) that maximize the trade-off among imperceptibility, robustness, and capacity. For example, PSO has been used to optimize embedding strength in transform domains, while GA has been applied for adaptive pixel selection in spatial domains. These approaches improve adaptability and reduce detectability but often rely on deterministic embedding paths, which may leave exploitable patterns for advanced steganalysis.

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

2.4 Hybrid Chaos–Optimization Approaches

The integration of chaotic maps with metaheuristic algorithms has recently gained attention in related fields such as image encryption and watermarking. Chaotic maps enhance the randomness of candidate solutions, while metaheuristic optimizers guide the search toward optimal embedding configurations. However, their combined application in LSB-based image steganography remains relatively underexplored. Most existing works either focus on chaos-driven randomization or optimization-based adaptation, but few attempt to synergize both. This gap suggests that a system that fuses chaotic embedding position generation with adaptive parameter optimization could achieve superior imperceptibility and robustness without sacrificing payload.

3. Proposed Methodology

3.1 Chaotic Logistic Map

Chaotic maps are non-linear deterministic systems that exhibit complex, pseudo-random behavior highly sensitive to initial conditions and system parameters. Due to their inherent unpredictability and ergodic properties, chaotic maps have become a powerful tool in various domains such as cryptography, steganography, and image processing. In this work, we utilize chaotic maps to enhance the randomness and security of the embedding positions and to control the data embedding path where denotes the state at iteration and is the system parameter. The logistic map produces a chaotic sequence that is highly sensitive to initial values and is suitable for pseudo-random generation in encryption and embedding processes. By using chaotic maps, the system avoids predictable embedding patterns, thereby increasing robustness against statistical and brute-force attacks.

3.2 Chaotic-Guided LSB Embedding

The chaotic sequence is used to determine the pixel locations for embedding the secret data. By converting chaotic values into pixel indices, data is embedded at pseudo-random positions, enhancing security.

3.3 Modified LSB Technique Instead of blindly replacing the least significant bit, a distortion-aware strategy is employed, where LSB replacement is skipped for pixels with high gradient values, reducing perceptual artifacts.

3.4 One-to-One Based Optimizer (OOBO) OOBO is a population-based metaheuristic that operates through pairwise competition among individuals. For each generation, individuals are compared and updated based on adaptive rules:

- Each individual interacts with one opponent.
- If the opponent has better fitness, the individual moves toward it.
- Otherwise, exploration-based perturbations are applied.

In this context, embedding parameters such as bit-plane selection, block size, and embedding threshold are optimized to achieve high PSNR and SSIM.

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

4. Experimental Results

4.1 Dataset and Metrics

- Test Images: Standard grayscale benchmark images including *Lena*, *Baboon*, and *Cameraman*.
- Evaluation Metrics:
  - PSNR (Peak Signal-to-Noise Ratio) – assesses image fidelity.
  - SSIM (Structural Similarity Index) – evaluates visual similarity to the original.
  - Payload – measured in bits per pixel (bpp), indicating the embedding capacity.
  - Histogram Analysis – evaluates visual imperceptibility via intensity distribution.

4.2 Results and Analysis

Method	**PSNR (dB)**	**SSIM**	**Payload (bpp)**
Traditional LSB	40.12	0.94	1.0
Chaos-based LSB	43.89	0.96	1.0
Proposed (Chaos + OOBO)	47.25	0.98	1.0

- The proposed method significantly outperforms traditional and chaos-only LSB approaches in terms of both PSNR and SSIM.
- Histogram Analysis: Minimal deviation between the stego and cover images confirms excellent imperceptibility.
- Statistical Steganalysis (Chi-square test): Demonstrates superior resistance to detection mechanisms compared to baseline methods.

5. Security and Robustness Evaluation

- Security via Chaotic Maps:

  The integration of chaotic maps (e.g., Logistic Map, Tent Map) ensures high key sensitivity. Even minor variations in initial conditions lead to entirely different embedding patterns, rendering brute-force attacks ineffective.

- **Robustness Testing:**
  - JPEG Compression: The proposed method retains data integrity under compression artifacts.
  - Salt-and-Pepper Noise: Demonstrated resilience, with high extraction accuracy post-noise injection.

6. Conclusion

A robust and secure steganographic framework combining chaotic map-based embedding and the OOBO (Opposition-based Optimization) strategy has been introduced. This approach enhances imperceptibility and embedding strength by:

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

- Exploiting the unpredictability of chaos theory.
- Adapting embedding locations through metaheuristic optimization.

Experimental results validate its superiority over existing methods across fidelity, security, and robustness metrics.

Future Directions: Expansion to color image steganography and real-time video hiding to broaden applicability.

References

1) G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004.
2) K. Wang, G. Xu, Y. Zhang, and H. Zhang, "A high capacity image steganography method based on LSB and chaos theory," *Multimedia Tools and Applications*, vol. 79, pp. 10729–10744, 2020.
3) S. Kaur and A. Kumar, "An improved LSB-based image steganography technique using chaotic map," *Journal of Information Security and Applications*, vol. 55, 2020.
4) S. Rahimdel and M. H. Sheikhan, "A novel hybrid image steganography method based on genetic algorithm and chaotic map," *Multimedia Tools and Applications*, vol. 79, pp. 22773–22803, 2020.
5) H. Tizhoosh, "Opposition-based learning: A new scheme for machine intelligence," *International Conference on Computational Intelligence for Modelling, Control and Automation*, 2005, pp. 695–701.
6) M. Dorigo and T. Stützle, *Ant Colony Optimization*, MIT Press, 2004.
7) Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600–612, 2004.
8) R. Chandramouli and N. Memon, "Analysis of LSB-based image steganography techniques," *Proceedings of International Conference on Image Processing*, 2001, vol. 3, pp. 1019–1022.
9) N. Provos and P. Honeyman, "Detecting steganographic content on the internet," *CITI Technical Report*, University of Michigan, 2002.
10) M. Li, J. Zhang, and X. Niu, "A new robust image steganography method based on chaotic maps and DCT domain," *Signal Processing*, vol. 136, pp. 251–263, 2017.