Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 5, pp. 1947–1956
DOI : 10.47974/JDMSC-2357

Enhancing image steganography through a novel multi-level chaotic encryption framework integrated with advanced deep neural networks

Munthir Bahir Tuieb *
Mohammed Hussein Ahmed †
Department of Computer Science
College of Education
Mustansiriyah University
Baghdad
Iraq

Ahmed Kareem Shibeeb §
Department of Computer Systems
Technical Institute of Suwaira
Middle Technical University
Baghdad
Iraq

Mohamed Abdulrahman Abdulhamed ‡
Department of Computer Science
College of Computer Science and Information Technology
University of Basrah
Basrah
Iraq

Abstract

Undetectable capabilities, capacity, and security are the biggest challenges facing information hiding in images. This paper presents methods to address these challenges. It utilizes an advanced deep learning architecture combined with a chaotic, multi-level encryption system. Lorenz and Rossler maps are used as chaotic methods to encrypt the message, which is then segmented to increase its resistance to chaotic analysis. High-level features are extracted using ResNet-50 CNNs, and the image is classified into four regions based on entropy. This results in an optimal payload distribution (16x16 to 2x2). The method

* *E-mail:* munthir_b_t87@uomustansiriyah.edu.iq (Corresponding Author)
† *E-mail:* mohammedalbawi@uomustansiriyah.edu.iq
§ *E-mail:* ahmed.kareem@mtu.edu.iq
‡ *E-mail:* mohammed@uobasrah.edu.iq

employs two techniques: Least Significant Bits Plus Plus (LSB++) for spatial modulation in textured regions and Discrete Cosine Transform (DCT) in smooth regions, which increases capacity and detectability. The results were obtained by evaluating two datasets, BOSSBase and COCO, with an average load of 4.2 bits per pixel, a signal-to-noise ratio (PSNR) higher than 54 dB, a structural similarity index (SSIM) higher than 0.97, and a modulation detection error rate of 89% using SRNet. The proposed method demonstrates significant improvements in modulation capacity and detection resistance compared to current methods.

Subject Classification: *94A60, 68P30.*

Keywords: *Steganography, Chaotic encryption, Advanced deep neural networks, Least significant bit plus-plus, Discrete cosine transform (DCT).*

1. Introduction

To ensure secure communication, steganography techniques are used to conceal data within digital images. Traditional methods, such as fixed-size, less important bit substitution in the spatial domain, suffer from limitations in image quality and data hiding capacity [1-2]. On the other hand, frequency-domain hiding techniques, such as DCT modulation, offer strong hiding capabilities but have lower hiding capacity and higher computational costs [3-4]. Chaotic systems, sensitive to their initial conditions and high entropy, have been combined with encryption methods to enhance security, but they rely on a single aspect and reduce complexity [3-5]. Convolutional neural networks (CNNs), as deep learning models, have been used for adaptive hiding. They are used to identify optimal regions, and previous studies have focused on relatively shallow architectures [2], [4], and [6]. This paper presents a comprehensive framework merging multilevel chaotic based coding, a ResNet as deep convolutional neural network, and a hybrid spatial/frequency hiding approach. Key contributions include:

- Data is segmented and encrypted using Lorenz and Rossler maps as a multi-level chaotic cipher to improve key space and reduce statistical predictive power.
- Data blocks are segmented using the pre-trained ResNet-50 technique to segment images into four entropy levels via Shannon entropy $H = -\sum pi \log2\ pi$, where pi denotes the probability distribution of pixel intensities in a 32×32 block. Thresholds $\theta1 = 4.2$, $\theta2 = 5.8$, $\theta3 = 7.0$ were empirically determined via grid search on BOSSBase.
- Dynamic Embedding Strategy, real-time selection between mid-band DCT modulation in low-entropy regions and high-entropy regions of LSB++.
- Comprehensive results, Indicating higher performance (4.2 bpp, PSNR > 54 dB, SSIM > 0.97, detection error > 89%) on BOSSBase and COCO datasets over state-of-the-art methods.

2. Related Work

Early methods using spatial hiding, such as LSB, proved to be simple and easily broken using statistical analysis [1], [7]. Therefore, a data hiding method emerged that relied on the variety of formats of the data carriers. These methods are suitable for different image formats or types, such as [2]. Data security and confidentiality were improved by using four layers, combining hiding and encryption, and applied to X-rays extracted from images of type [4]. One-dimensional chaotic encryption, such as the authors, has been used, achieving high key sensitivity, but its weakness lies in its predictability, especially when used alone [3-5], [8]. More advanced chaotic systems, such as Lorenz and the ultra-chaotic Rossler system, have been proposed, which enhance nonlinearity in subkey generation, thus increasing their strength and security [8-9]. A significant development in data hiding occurred with the advent of deep learning, where embedding or hiding was guided by the mapping features offered by convolutional networks. However, the superficial application of these networks diminishes their importance. While ResNet networks mitigate gradients and some vanish during hiding, and they also extract deeper features, they have not been sufficiently implemented for data hiding systems [2], [6]. Regarding data discovery or decryption, Cernet networks are used with results reaching up to 90%, leading to the discovery and implementation of more secure and robust methods [4], [10]. Improvements in error detection have emerged using competitive generative networks, but their drawbacks include increased computational and training complexity [11-12]. The method presented in [13] overcomes the problems found in Hoco and F5 by leveraging randomness in location and structure, similar to chaotic coding, and utilizing the capabilities of deep learning while reducing computational costs. The proposed system offers a method that overcomes the gaps identified in previous methods by using Recent Network Deep Learning as a deep learning approach combined with chaotic encryption and dynamically adaptive image content hiding.

3. Methodology

The proposed method involves integrating a chaotic system at multiple levels with deep learning techniques, ensuring improved security and steganography power, as follows:

3.1 *Multi-Level Chaotic Encryption*

The proposed method uses chaotic Rösler and Lorenz systems to encrypt the message, where their initial conditions are obtained from the keys entered by the user. SHA-256 is used to hash the key. What distinguishes this technique is its resistance to collisions and the collapse effect. This ensures that any change, however slight, to the key will produce completely different outputs.

Lorenz System Parameters:

$$\sigma = \mathrm{SHA}(\mathrm{key})_{1:8}, \tag{1}$$

$$\rho = \mathrm{SHA}(\mathrm{key})_{9:16}, \tag{2}$$

$$\beta = \mathrm{SHA}(\mathrm{key})_{17:24} \tag{3}$$

The Prantel number (σ) is defined by the first eight bits. The Rayleigh number (ρ) is represented by the next eight bits, and the geometric parameter (β) is the last eight bits. This method was used for partitioning to ensure that the parameters are diverse and also to guarantee their resistance to brute-force attacks, as demonstrated by the study by authors [2], who showed that effective keys can be extended to 264 case of derived SHA parameters.

A. Rössler System Parameters:

$$a = \mathrm{SHA}(\mathrm{key})_{25:32}, \tag{4}$$

$$b = \mathrm{SHA}(\mathrm{key})_{33:40}, \tag{5}$$

$$c = \mathrm{SHA}(\mathrm{key})_{41:4} \tag{6}$$

These parameters promote nonlinearity in addition to controlling the chaotic behavior of the proposed system, and for the purpose of future cryptographic expansions, the remaining hash bits are retained.

B. Chaotic Sequence Generation

For the purpose of generating pseudo-random sequences (CL and CR), Lorenz and Rösler techniques are frequently used, ensuring high entropy. Lorenz shown as:

$$x^{\cdot} = \sigma(y - x) \tag{7}$$

$$y^{\cdot} = x(\rho - z) - y \tag{8}$$

$$z^{\cdot} = xy - \beta z \tag{9}$$

The resulting chaotic trajectories are quantized into 8-bit values, ensuring compatibility with digital message segments. Similarly, Separate data are obtained from the Rösler outputs, which produce CR.

Encryption via XOR

The message to be hidden, M, is divided into two equal parts, designated M1 and M2, and encrypted using XOR with its corresponding chaotic sequence:

$$E1 = M1 \oplus CL \tag{10}$$

$$E2 = M2 \oplus CR \tag{11}$$

XOR operations are chosen for their reversibility and computational efficiency, while the unpredictability of the chaotic sequences ensures resistance to frequency analysis and known-plaintext attacks. As validated by the authors [5]. This approach achieves Shannon's definition of perfect secrecy when the chaotic sequence length matches the message length, and the key is non-repeating, as shown in Figure 1.

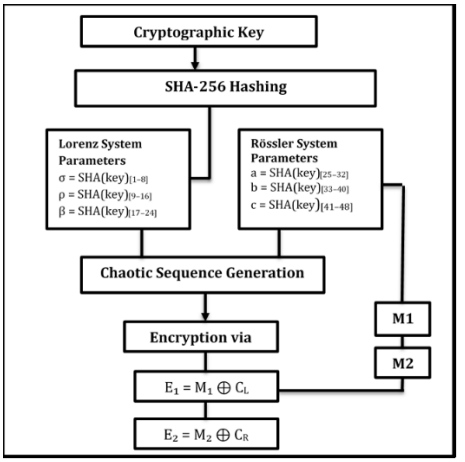

Figure 1
Workflow of Multi-Level Chaotic

3.2 *ResNet-Driven Adaptive Block Partitioning*

A pre-trained ResNet-50 model processes non-overlapping 32×32 patches of the cover image, outputting feature vectors used to compute local entropy H. Patches are classified into four entropy levels via thresholds θ1, θ2, θ3, dictating block sizes B ∈ {16,8,4,2} as listed in Algorithm 1.

Algorithm 1: Adaptive Block Sizing

1. Input:
- A single image patch.

2. Feature Extraction:
- Pass the patch through a pretrained ResNet-50 network to obtain a feature representation:
  features = ResNet50(patch)

3. Entropy Computation:
- Compute the Shannon entropy H of those features:
  H = ComputeEntropy(features)

4. Block-Size Decision:
- Compare the entropy H against three thresholds θ1 < θ2 < θ3:

1. If H < θ1, choose a 16×16 block.
2. Else if H < θ2, choose an 8×8 block.
3. Else if H < θ3, choose a 4×4 block.
4. Otherwise, choose a 2×2 block.

5. Output:
- Return the selected block size.

3.3 *Dynamic Embedding Strategy*

For each block, local entropy H determines the embedding domain, which is illustrated in Algorithm 2 as follows:

- If H > θ high: use spatial LSB++ embedding (up to 4 bits/pixel controlled by chaotic keys).
- Else: perform DCT on the block and modulate mid-frequency coefficients by ±1 according to encrypted bits.

Algorithm 2: Dynamic Embedding

1. Input:

• block (an image block)
• encrypted_bits (bitstream to embed) key (cryptographic key)

2. Entropy Measurement:

• Compute the entropy of the input block: H = ComputeEntropy(block)

3. Embedding Method Selection:

• If the block's entropy exceeds the high-entropy threshold θ_high:
◦ Call Embed_LSBPlus with (block, encrypted_bits, key). Return the result.
• Otherwise (low- to mid-entropy block):
◦ Call Embed_DCT with (block, encrypted_bits, key). Return the result.

4. Output:

• The function returns the stego-block produced by the selected embedding routine.

4. Experimental Setup

Experiments utilize the BOSSBase v1.01 (10,000 grayscale images) and a 5,000-image MS COCO subset (animal and vehicle categories), converted to grayscale to align with BOSSBase's format. Runtime Tests conducted on an NVIDIA RTX 3090 GPU. Average embedding times: Proposed: 23.1 sec/image Variable Block: 21.2 sec/image (+9.2% overhead).

Metrics include PSNR, SSIM, payload capacity (bpp), and steganalysis detection error rate measured with SRNet. The ResNet-50 is fine-tuned on a balanced set of cover and stego patches. Embedding payloads range from 0.2 bpp to 4.2 bpp.

5. Results and Discussion

Figure 2 shows a comparison of the resulting candidate image with the method presented in [2]:

Figure 2
Stego-Image Comparison (512×512)

This study benchmarks the proposed approach against Variable Block [14], Dynamic LSB, and the latest GAN-based JPEG steganography technique, JS-GAN, as in Table 1 and Table 2.

Table 1

Compares the proposed method against Variable Block, Dynamic LSB, and a recent GAN-based JPEG steganography (JS-GAN).

Method	Capacity (bpp)	PSNR (dB)	SSIM Detection Error	(%)
Variable Block	1.8	48.2	0.92	65
Dynamic LSB	2.5	50.1	0.94	72
JS-GAN	3.0	52.0	0.95	78
Proposed	**4.2**	**54.3**	0.97	**89**

Table 2

Presents detection error rates under varying payloads.

Payload (bpp)	**0.5**	**1.0**	**2.0**	**4.2**
Detection Err.	95%	92%	90%	89%

The Proposed Method shows the highest true-positive rates at given false-positive rates, indicating superior evasion performance as in Figure 3:

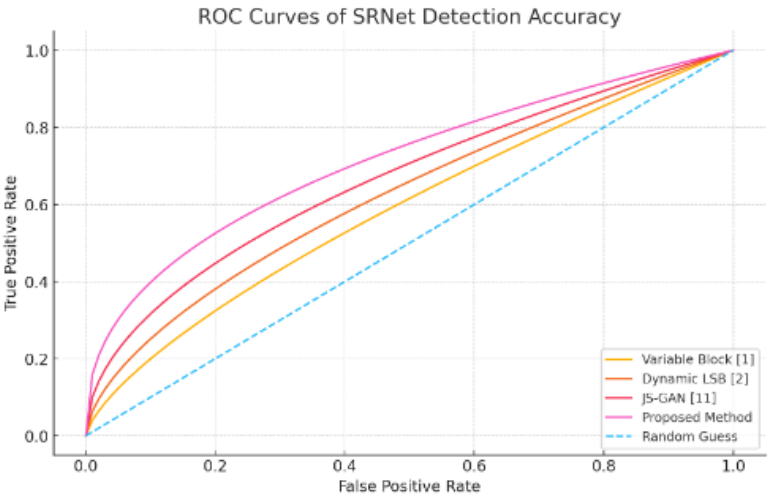

Figure 3

ROC curves comparing detection accuracy of SRNet on different methods

Figure 3 presents simulated ROC curves for SRNet steganalysis across four methods: Variable Block [14], Dynamic LSB, JS-GAN, and the Proposed Method.

The proposed method consistently outperforms prior techniques across all metrics, with minimal visual distortion (PSNR > 54 dB, SSIM > 0.97) and high security (detection error > 89%). In terms of computational load, it is minimal when using a dual-chaos scheme (Runtime increasing is less than 10%), and the ResNet achieves dynamic partitioning and hiding, resulting in increased capacity and robustness. When comparing the proposed method with the variable mass method [14], the correlation coefficient decreases with increasing entropy, indicating that the proposed method offers better security. As presented in Table 3.

Table 3

Security Analysis (Histogram Uniformity)

Method	Correlation Coefficient	Entropy
Variable Block	0.12	7.82
Proposed	**0.03**	**7.98**

Table 3 shows that lower CC indicates higher histogram uniformity; higher entropy signifies more randomness, strengthening security.

6. Conclusion and Future Work

A developed framework for image data hiding was implemented, employing multi-level chaotic encryption, a ResNet for adaptive block-segmenting network, dynamic hiding, and spatial/frequency attributes.

Measurements were performed on two datasets, BOSSBase and COCO, yielding results of high capacity (4.2 bits per pixel), undetectable performance (PSNR > 54 dB, SSIM > 0.97), and high security (detection error > 89%). Future integrated hiding based on generative adversarial networks (GANs) could lead to increased error detection rates. There is also interest in exploring chaotic maps resistant to quantum computing.

References

[1] A. M. Alhomoud, "Image steganography in spatial domain: Current status, techniques, and trends," *Intelligent Automation & Soft Computing,* vol. 27, no. 1 (2021).

[2] U. Pilania, M. Kumar, and V. Mittal, "Performance evaluation of LSB steganography based on multiple image formats," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 26, no. 7, pp. 1911–1924 (2023).

[3] S. Wang, C. Wang, and C. Xu, "An image encryption algorithm based on a hidden attractor chaos system and the Knuth–Durstenfeld algorithm," *Opt. Lasers Eng.,* vol. 128, p. 105995 (2020).

[4] D. Sharma, C. Prabha, A. Goyal, M. Malik, and R. Kumar, "Enhanced security of EMI using an edge-based steganography with four-layered cryptography," *J. Discrete Math. Sci. Cryptogr,* vol. 27, no. 2-B, pp. 775–784 (2024).

[5] X. Jin, X. Duan, H. Jin, and Y. Ma, "A Novel Hybrid Secure Image Encryption Based on the Shuffle Algorithm and the Hidden Attractor Chaos System," *Entropy,* vol. 22, no. 6, p. 640 (2020).

[6] P. Wu, Y. Yang, and X. Li, "Stegnet: Mega image steganography capacity with deep convolutional network," *Future Internet,* vol. 10, no. 6, p. 54 (2018).

[7] K. S. Kumar, K. B. Raja, and S. Pattnaik, "Hybrid domain in LSB steganography," *Int. J. Comput. Appl.,* vol. 19, no. 7, pp. 35–40 (2011).

[8] H. T. Elshoush, B. M. Al-Tayeb, and K. T. Obeid, "Enhanced Serpent algorithm using Lorenz 96 Chaos-based block key generation and parallel computing for RGB image encryption," *PeerJ Comput. Sci.,* vol. 7, p. 812 (2021).

[9] X. Wang and Y. Zhang, "An efficient method for the construction of block cipher with multi-chaotic systems," *Nonlinear Dyn.*, vol. 73, no. 1–2, pp. 53–61 (2013).

[10] M. Boroumand, M. Chen, and J. Fridrich, "Deep Residual Network for Steganalysis of Digital Images," *IEEE Transactions on Information Forensics and Security,* vol. 14, no. 5, pp. 1181–1193 (2018).

[11] L. Li, W. Zhang, C. Qin, K. Chen, W. Zhou, and N. Yu, "Adversarial batch image steganography against CNN-based pooled steganalysis," *Signal Processing,* vol. 181, p. 107920 (2021).

[12] D. Wang, G. Yang, J. Chen, and X. Ding, "GAN-based adaptive cost learning for enhanced image steganography security," *Expert Syst. Appl.,* vol. 249, p. 123471 (2024).

[13] S. M. Saber, M. B. Tuieb, K. K. Jabbar, M. H. Ahmed, and F. N. Abbas, "Utilizing variable hiding centers and dynamic block sizes to improve image steganography," *AIP Conf. Proc.,* vol. 3264, no. 1, p. 30020 (2025).

[14] A. K. Sahu, G. Swain, and E. S. Babu, "Digital image steganography using bit flipping," *Cybernetics and Information Technologies,* vol. 18, no. 1, pp. 69–80 (2018).

Received May, 2025