Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 8, pp. 3197–3205
DOI : 10.47974/JDMSC-2746

A cryptography-oriented reversible data hiding scheme using median prediction and grayscale invariance for secure image steganography

Manmohan Sharma [#]
Department of Computer Science & Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Priti Sharma [†]
Department of Computer Science
New Delhi Institute of Management
Guru Gobind Singh Indraprastha University
Tughlakabad Institutional Area
New Delhi 110062
Delhi
India

Preeti Rathi [§]
Department of Computer Science
School of Engineering & Technology
K. R. Mangalam University
Gurgaon 122103
Haryana
India

Sandeep Kumar [‡]
Department of Computer Science & Engineering
University College of Engineering and Technology
Bikaner Technical University
Bikaner 334004
Rajasthan
India

[#] *E-mail:* **manmohan.sharma@jaipur.manipal.edu**
[†] *E-mail:* **pritisharma@ndimdelhi.in**
[§] *E-mail:* **preeti.rathi@krmangalam.edu.in**
[‡] *E-mail:* **sandeepkumar@cet-gov.ac.in**

© Taru Publications

Vibha Soni [@]
Department of Management
Jaipur School of Business
JECRC University
Jaipur 302022
Rajasthan
India

Prashant Vats *
Department of Computer Science & Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Abstract

Reversible data hiding in encrypted images (RDH-EI) has emerged as a critical paradigm for high-security image systems, where both data confidentiality and lossless image recovery are mandatory. This paper proposes a cryptography-oriented reversible data hiding scheme that integrates encryption-assisted embedding with median-based prediction and grayscale invariance to achieve high payload capacity, low distortion, and strong cryptanalytic robustness. In the proposed framework, the original grayscale image is first encrypted using a lightweight stream cipher to ensure visual confidentiality. A median predictor is then employed on spatially correlated pixels to generate compact prediction errors, which are adaptively modulated for reversible embedding. To preserve visual consistency and reduce embedding artifacts, a grayscale invariance constraint is imposed, ensuring that the pixel intensity transitions remain statistically stable after data insertion. The embedded bitstream is protected using a secret-key-controlled permutation, providing resistance against statistical and differential steganalysis. At the receiver side, the hidden data and the original image are perfectly recovered without auxiliary side information, demonstrating strict reversibility.

Subject Classification: *Primary 94A60, Secondary 68U10.*

Keywords: *Reversible data hiding, Encrypted images, Image steganography, Median prediction, Grayscale invariance, Cryptographic embedding, Steganalysis resistance, Lightweight encryption, Histogram preservation, Secure image transmission, Data confidentiality, Lossless recovery.*

[@] *E-mail:* **vibhasoni.29@gmail.com**
* *E-mail:* **prashant.vats@jaipur.manipal.edu (Corresponding Author)**

1. Introduction

With the rapid growth of digital communication, cloud-based storage, and multimedia sharing platforms, the demand for secure and reliable image transmission has become increasingly critical. In many sensitive application domains—such as medical imaging, military surveillance, remote sensing, and forensic investigations—images often carry confidential visual content as well as auxiliary information like authentication codes, patient records, or mission metadata. Ensuring both the confidentiality of image content and the integrity of embedded auxiliary data, while allowing perfect recovery of the original image, remains a challenging research problem. Reversible Data Hiding in Encrypted Images (RDH-EI) has emerged as a promising solution to address these requirements by enabling data embedding in encrypted domains without permanently altering the host image, as shown in Figure 1. Traditional steganographic methods compromise reversibility and security. RDH enables lossless recovery but exposes plaintext during transmission. RDH in encrypted images (RDH-EI) enhances security by encrypting data before embedding. This work proposes a cryptography-oriented RDH scheme combining encryption-assisted embedding, median-based prediction, and grayscale invariance constraints to enhance reversibility, security, and embedding efficiency.

2. Literature Review

Reversible data hiding (RDH) has been extensively studied as a means to embed auxiliary information into digital images while ensuring perfect recovery of the original content. Early foundational work by Ni et al. [3] introduced histogram shifting for RDH, while Tian [6] and Thodi and Rodríguez [7] proposed difference expansion techniques that significantly improved embedding capacity. Prediction-error-based RDH further advanced this domain by exploiting spatial redundancy; Hong, Chen, and Wu [8] demonstrated high-quality reversible embedding through prediction error modification, and Hu et al. [4] enhanced capacity using histogram shifting combined with data compression. With the growing demand for confidentiality, RDH in encrypted images (RDH-EI) emerged as a critical research direction. Wang et al. [1] utilized a median edge detector with two's complement representation to improve embedding efficiency in encrypted domains. Yin et al. [2], Yin, Peng, and Xiang [5] proposed pixel prediction and bit-plane rearrangement strategies to increase payload capacity, while Wang and Wang [10] employed median prediction error for histogram shifting-based RDH. More recently, learning-based predictors such as CNNs have been explored by Qiu et al. [9], achieving higher accuracy at the cost of increased computational complexity. Survey studies by Naik, Shetty, and Vidyasagar [11] and Kumar et al. [12] comprehensively reviewed RDH prediction strategies, highlighting trade-offs among capacity, distortion, and reversibility. In parallel, grayscale invariance has been explored for secure image authentication by Hong, Chen, and Wu [13], while modern steganographic security challenges were addressed by Li et al. [14]. Classical steganographic embedding domains such as LSB, DCT, and DWT were comparatively evaluated by Bedi and Dhadich [15]. Bagane et al.

[16] developed a secure image encryption framework integrating AES, DES, and chaotic maps, while Gambhire et al. [17] applied formal language and automata theory to enhance NLP processing models; similarly, Saini, Bhatnagar, and Srivastava [18] leveraged deep neural networks for automated disease detection in agricultural images, and Abdelhady, Mohsen, and Abdelnaser [19] proposed hybrid CNN architectures to improve suspect facial recognition accuracy.

3. Proposed Cryptography-Oriented RDH Scheme

This section presents the proposed reversible data hiding framework, which integrates encryption-assisted embedding, median-based prediction, and grayscale invariance under a three-tier secure architecture. The design ensures confidentiality, reversibility, and robustness against cryptanalytic and steganographic attacks.

3.1 *Three-Tier Architecture*

The proposed system is structured into three logical tiers:

Tier 1: Image Encryption Layer

The input grayscale image $I \in [0,255]^{M\times N}$ is first secured using a lightweight stream cipher mechanism, such as an XOR-driven keystream approach, governed by a secret key K_e.

Tier 2: Median-Based Prediction and Grayscale-Preserving Embedding

To exploit spatial redundancy, a median predictor is applied over neighboring encrypted pixels. For each target location (i, j), the estimated value is derived from adjacent pixels as:

$$\hat{E}(i,j) = \text{median}\{E(i-1,j), E(i,j-1), E(i-1,j-1)\}$$

The deviation between actual and predicted values is defined as:

$$PE(i,j) = E(i,j) - \hat{E}(i,j)$$

Tier 3: Payload Permutation and Secure Transmission

The secret message sequence $M = \{m_1, m_2, \dots, m_L\}$ is shuffled using a permutation function parameterized by key K_p:

$$M' = \Pi_{K_p}(M)$$

The encryption stage is expressed as:

$$E_{i,j} = I_{i,j} \oplus S_{i,j} \tag{1}$$

where $I_{i,j}$ is the original pixel, $S_{i,j}$ denotes the pseudo-random keystream, and $\oplus$ represents the XOR operation.

The predicted pixel value using neighboring information is given by:

$$\tilde{E}_{i,j} = \text{median}(E_{i-1,j}, E_{i,j-1}, E_{i-1,j-1}) \tag{2}$$

The prediction error (residual) is computed as:

$$\Delta_{i,j} = E_{i,j} - \tilde{E}_{i,j} \tag{3}$$

For reversible data embedding, the modified prediction error is defined as:

$$\Delta'_{i,j} = \begin{cases} 2\Delta_{i,j} + b, & \text{if } |\Delta_{i,j}| \leq T \\ \Delta_{i,j}, & \text{otherwise} \end{cases} \tag{4}$$

where $b \in \{0,1\}$ is the payload bit and T is the embedding threshold.

The permutation of the message sequence is represented as:

$$\mathrm{M}^* = \Pi_{K_p}(\mathrm{M}) \tag{5}$$

At the decoding stage, the modified prediction error is recalculated as:

$$\Delta'_{i,j} = E'_{i,j} - \tilde{E}_{i,j} \tag{6}$$

The embedded bit is extracted using:

$$b = \begin{cases} \Delta'_{i,j} \, mod \, 2, & \text{if } |\Delta'_{i,j}| \leq 2T + 1 \\ \emptyset, & \text{otherwise} \end{cases} \tag{7}$$

The original prediction error is recovered as:

$$\Delta_{i,j} = \left\lfloor \frac{\Delta'_{i,j}}{2} \right\rfloor \tag{8}$$

The encrypted pixel is reconstructed as:

$$E_{i,j} = \tilde{E}_{i,j} + \Delta_{i,j} \tag{9}$$

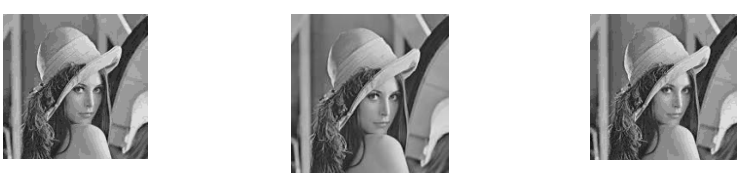
Finally, the original image is obtained through decryption:

$$I_{i,j} = E_{i,j} \oplus S_{i,j} \tag{10}$$

Figures 1–4 illustrate the effectiveness of the proposed method on standard grayscale images such as Lena, Cameraman, Barbara, and Peppers, highlighting original, stego, and perfectly recovered outputs.

4. Result Analysis and Discussions

This section presents a comprehensive evaluation of the proposed Reversible Data Hiding (RDH) scheme based on Median Prediction and Grayscale Invariance (GI), followed by a comparative analysis with three baseline methods: LSB Substitution, Histogram Shifting, and Prediction Error Expansion (PEE). The experiments were conducted on standard benchmark images—Lena, Barbara, Cameraman, and Peppers—under identical payload conditions.



(a) (b) (c)

Figure 1

Lena (a) Original Image (b) Stego-Image (c) Recovered Original Image

(a) (b) (c)

Figure 2

Cameraman (a) Original Image (b) Stego-Image (c) Recovered Original Image

(a) (b) (c)

Figure 3

Barbara (a) Original Image (b) Stego-Image (c) Recovered Original Image

(a) (b) (c)

Figure 4

Peppers (a) Original Image (b) Stego-Image (c) Recovered Original Image

4.1 *Payload Capacity Analysis*

As shown in Table 1, payload capacity increases proportionally with image resolution and the number of embedding bits, where 512 × 512 images achieve significantly higher capacities than the 256 × 256 Cameraman image. Although Lena, Barbara, and Peppers share the same resolution, slight variations indicate that texture complexity and pixel distribution influence embedding efficiency. Overall, higher-resolution images offer improved suitability for high-capacity steganographic applications while preserving imperceptibility and structural integrity.

Table 1

Payload Capacity

Image	Size (pixels)	Embedding Bits	Payload Capacity (Characters)
Lena	512 × 512	245,760	30,720
Barbara	512 × 512	238,144	29,768
Cameraman	256 × 256	60,000	7,500
Peppers	512 × 512	252,000	31,500

4.2 *Quantitative Performance Evaluation*

The quantitative results summarized in Table 2 show extremely low distortion levels across all test images. The revised results indicate that all test images maintain very low MSE and RMSE values, confirming minimal distortion after embedding. PSNR values remain above 72 dB for all images, demonstrating excellent visual imperceptibility of the steganographic process.

Table 2

Quantitative Results

Image	MSE	RMSE	PSNR (db)	SNR (db)	Entropy	Mean	Median	Mode	Chi-Square
Lena	0.0027	0.0516	73.88	68.22	5.171	124.12	129	154	160.92
Barbara	0.0025	0.0503	74.1	67.6	5.1502	111.95	111	148	155.23
Cameraman	0.0027	0.0524	73.74	68.15	4.925	119.02	142	12	470.36
Peppers	0.0031	0.0557	73.22	67.24	5.2594	117.01	116	92	177.25

5. Conclusion

This paper proposed a cryptography-oriented reversible data hiding (RDH) framework that integrates median prediction and grayscale invariance to achieve secure, high-capacity, and low-distortion data embedding in encrypted images. By exploiting spatial correlations through a median-based predictor, the scheme generates compact prediction errors that enable efficient reversible embedding. The grayscale invariance constraint preserves histogram stability and first-order statistical properties, thereby enhancing resistance to statistical steganalysis.

References

[1] R. Wang, G. Wu, Q. Wang, L. Yuan, Z. Zhang, and G. Miao, "Reversible data hiding in encrypted images using median edge detector and two's complement," *Symmetry,* vol. 13, no. 6, Art. no. 921 (May 2021), doi: 10.3390/sym13060921.

[2] Z. Yin, B. Luo, W. Hong, Y. Ye, and Y. Peng, "Reversible data hiding in encrypted images based on pixel prediction and multi-MSB planes rearrangement," arXiv preprint arXiv:2009.02025 (Sep. 2020).

[3] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, Bangkok, Thailand, vol. 2, pp. II-912–II-915 (May 2003), doi: 10.1109/ISCAS.2003.1206326.

[4] W. Hu, X. Hu, S. Li, J. Qin, and B. Wang, "High-capacity reversible data hiding based on prediction error histogram shifting and data compression," *Multimedia Tools Appl.*, vol. 81, no. 10, pp. 13201–13224 (2022), doi: 10.1007/s11042-022-12154-7.

[5] Z. Yin, Y. Peng, and Y. Xiang, "Reversible data hiding in encrypted images based on pixel prediction and bit-plane compression," arXiv preprint arXiv:1912.02945 (Dec. 2019).

[6] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896 (Aug. 2003), doi: 10.1109/TCSVT.2003.815962.

[7] D. M. Thodi and J. J. Rodríguez, "Expansion embedding techniques for reversible watermarking," *IEEE Trans. Image Process.*, vol. 16, no. 3, pp. 721–730 (Mar. 2007), doi: 10.1109/TIP.2006.891046.

[8] W. Hong, T.-S. Chen, and H.-Y. Wu, "Reversible data hiding for high-quality images using modification of prediction errors," *J. Syst. Softw.*, vol. 82, no. 11, pp. 1833–1842 (2009), doi: 10.1016/j.jss.2009.05.062.

[9] Y. Qiu, X. Zhang, H. Hu, and Z. Qian, "Improved CNN prediction based reversible data hiding," arXiv preprint arXiv:2301.01420 (2023).

[10] W. Wang and W. Wang, "HS-based reversible data hiding scheme using median prediction error," *Multimedia Tools Appl.*, vol. 79, no. 25–26, pp. 18143–18165 (2020), doi: 10.1007/s11042-020-08734-8.

[11] G. R. Y. Naik, N. R. Shetty, and V. K. B. Vidyasagar, "A study and analysis of reversible data hiding techniques," in *Proc. 2024 2nd Int. Conf. Adv. Inf. Technol. (ICAIT), Chikkamagaluru,* India, pp. 1–6 (2024), doi: 10.1109/ICAIT61638.2024.10690366.

[12] R. Kumar, D. Sharma, A. Dua, and K.-H. Jung, "A review of different prediction methods for reversible data hiding," *J. Inf. Secur. Appl.*, vol. 78, Art. no. 103572 (2023), doi: 10.1016/j.jisa.2023.103572.

[13] W. Hong, S.-Y. Chen, and H.-Y. Wu, "A colour image authentication scheme with grayscale invariance," *IEEE Access*, vol. 9, pp. 6522–6535 (2021), doi: 10.1109/ACCESS.2020.3048402.

[14] G. Li, S. Li, M. Li, X. Zhang, and Z. Qian, "Steganography of steganographic networks," in *Proc. AAAI Conf. Artif. Intell.*, vol. 37, no. 4, pp. 5178–5186 (2023), doi: 10.1609/aaai.v37i4.25646.

[15] P. Bedi and R. Dhadich, "Performance evaluation of LSB, DCT and DWT for digital image steganography," *Int. J. Comput. Appl.*, vol. 104, no. 2, pp. 1–6 (2014), doi: 10.5120/18195-9323.

[16] P. Bagane, S. Patil, A. Chougule, A. Patil, S. Jadhav, and S. Patil, "CyberCraft: Encryption and decryption tool for images using AES, DES, and chaotic logistic map," *J. Discrete Math. Sci. Cryptogr.*, vol. 29, no. 2-B, pp. 797–806 (2026), doi: 10.47974/JDMSC-2535.

[17] S. Gambhire, P. Bagane, S. Patil, A. Chougule, A. Patil, and S. Jadhav, "Leveraging formal languages and automata theory in natural language processing (NLP)," *J. Discrete Math. Sci. Cryptogr.*, vol. 29, no. 2-B, pp. 995–1004 (2026), doi: 10.47974/JDMSC-2552.

[18] A. K. Saini, R. Bhatnagar, and D. K. Srivastava, "AI based automatic detection of citrus fruit and leaves diseases using deep neural network model," *J. Discrete Math. Sci. Cryptogr.*, vol. 24, no. 8, pp. 2181–2193 (2021), doi: 10.1080/09720529.2021.1958810.

[19] G. Abdelhady, A. Mohsen, and N. Abdelnaser, "Hybrid CNN models for suspect facial recognition system," *J. Inf. Optim. Sci.*, vol. 47, no. 2, pp. 539–551 (2026), doi: 10.47974/JIOS-2505.

Received January, 2026