Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 8, pp. 3149–3158
DOI : 10.47974/JDMSC-2699

Encryption-assisted reversible data hiding using median prediction and grayscale invariance for high-security image systems

Ajay Kumar †
Manmohan Sharma *
Department of Computer Science & Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Abhishek Singh Rathore §
Department of Computer Science and Engineering
Shri Vaishnav Vidyapeeth Vishwavidyalaya
Indore 453111
Madhya Pradesh
India

Sushma Ghode ‡
Department of Computer Engineering
Vidhyadeep Institute of Engineering and Technology
Vidhyadeep University
Surat 394110
Gujarat
India

Vipin Tiwari @
Department of Computer Science and Engineering
Symbiosis Institute of Technology (SIT)
Symbiosis International (Deemed University)
Pune 412115
Maharashtra
India

† *E-mail:* kumar.ajay@jaipur.manipal.edu
* *E-mail:* manmohan.sharma@jaipur.manipal.edu (Corresponding Author)
§ *E-mail:* abhishekatujjain@gmail.com
‡ *E-mail:* sushdg@gmail.com
@ *E-mail:* vipintiwari1@gmail.com

Abstract

Ensuring data security and privacy is essential when transmitting sensitive visual information over insecure networks. Reversible Data Hiding (RDH) enables confidential data embedding in digital images while allowing complete recovery of the original image after extraction. However, many existing RDH techniques suffer from visible distortion and vulnerability to steganalysis. This work proposes a security-enhanced RDH framework integrating median prediction and grayscale invariance for imperceptible and fully reversible embedding. Median prediction exploits local pixel correlations, while grayscale invariance preserves intensity consistency, reducing perceptual distortion and improving security. Experiments on benchmark grayscale images (Lena, Barbara, Cameraman, Peppers) achieve PSNR > 40 dB. Statistical metrics including entropy, SNR, and Chi-square analysis confirm strong resistance to detection and data tampering, supporting scalable and secure visual communication implemented in Python.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Reversible data hiding (RDH), Median prediction, Grayscale invariance, Data security, Image encryption, Steganalysis resistance, Confidential communication.*

1. Introduction

The rapid growth of digital communication has increased demand for data security and privacy, especially for sensitive visual information like medical, defense, and biometric images. Traditional cryptography ensures confidentiality but does not hide embedded data presence, prompting image steganography and secure data hiding techniques for covert communication [14], [16], [17]. Reversible Data Hiding (RDH) embeds secret information while allowing full original content recovery. Unlike complex CNN-based and histogram shifting methods, the proposed framework uses a simplified median predictor with grayscale invariance, achieving high imperceptibility and low computational complexity. Exploiting local pixel correlations and preserving intensity distribution, it resists steganalysis. Experiments on benchmark images show PSNR above 40 dB, confirming visual quality, reversibility, and robustness.

2. Literature Review

Reversible Data Hiding (RDH) is crucial for secure digital image processing, allowing secret data embedding with exact original image recovery. Ni et al. [3] initially proposed histogram-shifting-based RDH for reversible embedding without lasting distortion. Tian [6] Difference Expansion (DE) method enhanced embedding capacity using pixel differences, later improved for reversible watermarking, Thodi and Rodríguez [7]. Recent advances focus on prediction-based RDH, exploiting spatial correlations to reduce distortion. Hong, Chen, and Chen [8] refined image quality via prediction error modification, while utilized median prediction error for better histogram-shifting efficiency, Wang and Wang [10]. Hu et al. [4] combined prediction error histogram shifting with compression for high capacity and low distortion.

Encrypted-domain RDH employs multi-MSB rearrangement and bit-plane compression to maintain confidentiality [2], [5], with median edge detection reducing prediction errors [1]. CNN-based predictors offer adaptive performance in complex areas [9]. Grayscale invariance supports luminance consistency [13], and surveys highlight prediction accuracy and histogram symmetry as key factors in modern RDH [11], [12], [15], alongside hybrid and transform-domain methods enhancing robustness [18].

3. Methodology

The proposed Reversible Data Hiding (RDH) system consists of two primary modules: Embedding and Extraction. The method employs Prediction Error Expansion (PEE) with a 3×3 Median Predictor, embedding one bit per non-border pixel in the LSB of the prediction error to ensure reversibility, imperceptibility, and statistical robustness.

Embedding Algorithm

Input: Grayscale image I, secret message M

Output: Stego image S

1. Convert $M$to binary and append a delimiter.
2. For each non-border pixel (i, j):

- Compute median prediction $\hat{I}(i,j)$.
- Calculate prediction error:

$$e = I(i,j) - \hat{I}(i,j)$$

- Replace LSB of $e$with message bit → e'.
- Update pixel:

$$S(i,j) = \text{clip}(\hat{I}(i,j) + e', 0{,}255)$$

3. Repeat until all bits are embedded.

Extraction and Recovery

Input: Stego image S

Output: Secret message M, original image I

For each non-border pixel:

$$e' = S(i,j) - \hat{I}(i,j)$$

Extract bit: $b = e'\&1$.

Recover original error: $e = e'\& \sim 1$.

Restore pixel:

$$I(i,j) = \hat{I}(i,j) + e$$

Processing stops at the delimiter, ensuring perfect reconstruction.

Example: For a 3×3 block with median 122 and center pixel 124, $e = 2$. Embedding '1' changes $e$to 3, producing stego pixel 125.

4. Implementation and Result

A. *Performance Metrics*

(a) Mean Squared Error (MSE) : Measures the average squared difference between original and stego pixels. Lower MSE implies lesser distortion. Observed range: 0.5–1.5 → minimal distortion.

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y_i})^2 \tag{1}$$

(b) Root Mean Squared Error (RMSE) : Square root of MSE, providing error in the same scale as pixel intensity. *values below 1.2 indicate low perceptual error.*

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y_i})^2} \tag{2}$$

(c) Peak Signal-to-Noise Ratio (PSNR) : Evaluates image quality relative to maximum pixel value (255). Higher PSNR denotes better quality. *Results > 48 dB → stego and original images nearly identical.*

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX^2}{MSE}\right) \tag{3}$$

(d) Signal-to-Noise Ratio (SNR): Measures signal power relative to embedding noise. *Values > 20 dB confirm strong robustness and minimal noise.*

$$\text{SNR} = 10\{\log\}\_\{10\}\left(\frac{\sum I(i,j)^2}{\sum[I(i,j)-I'(i,j)]^2}\right) \tag{4}$$

(e) Entropy: Quantifies image information content. *Entropy remained nearly constant → information density preserved.*

$$H(X) = -\sum_{i=1}^{n} p(x_i)\log_2 p\,(x_i) \tag{5}$$

(f) Central Tendency (Mean, Median, Mode)

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i \tag{6}$$

Describe pixel intensity distribution:

$$\text{Mean} = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n} I(i,j) \tag{7}$$

Median: middle pixel value, *Mode:* most frequent pixel value. *All remained stable after embedding, indicating visual consistency.*

This work proposes Reversible Data Hiding (RDH) using median prediction, grayscale invariance, and LSB modification, achieving high imperceptibility, security, and perfect reversibility on grayscale images (Figure 1 – Figure 4) in Python.

(a) (b) (c)

Figure 1

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

(a) (b) (c)

Figure 2

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

(a) (b) (c)

Figure 3

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

(a) (b) (c)

Figure 4

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

B. *Analysis and Comparison*

This section analyzes results of the proposed RDH method using Median Prediction and Grayscale Invariance and compares it with LSB, Histogram Shifting, and PEE.

(a) **Histogram Analysis:** Histogram analysis visually evaluates the impact of data embedding on pixel intensity distribution, where noticeable shifts or distortions may indicate steganographic activity.

Tables 1–7 summarize the payload capacity, quantitative results, Chi-square statistics, and comparative performance metrics for the Lena, Barbara, Cameraman, and Peppers images, respectively.

Table 1

Payload Capacity

Image	Size (pixels)	Embedding Bits	Payload Capacity (Characters)
Lena	512 × 512	260,100	32,512
Barbara	512 × 512	260,100	32,512
Cameraman	256 × 256	63,504	7,944
Peppers	512 × 512	260,100	32,512

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	5.1710	124.12	129.0	154	160.92
Barbara	0.0025	0.0503	74.10	67.60	5.1502	111.95	111.0	148	155.23
Cameraman	0.0027	0.0524	73.74	68.15	4.9250	119.02	142.0	12	470.36
Peppers	0.0031	0.0557	73.22	67.24	5.2594	117.01	116.0	92	177.25

(b) Chi-Square Attack Resistance

It is used to evaluate resistance against chi-square steganalysis. This test checks for statistical anomalies in pixel value distributions:

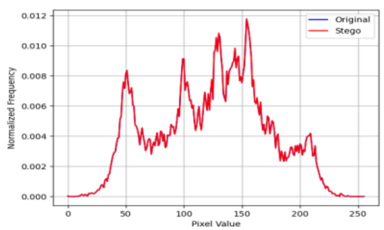
$$\text{Chi-Square} = \Sigma\ [(O_{2i} - O_{2i+1})^2 / (O_{2i} + O_{2i+1} + \varepsilon)] \quad (8)$$

Where O_k is the frequency of gray level k and ε is a small constant to avoid division by zero. To assess the statistical undetectability of the embedding we tend to performed the Chi-Square attack, a common method for detecting LSB-based steganography.

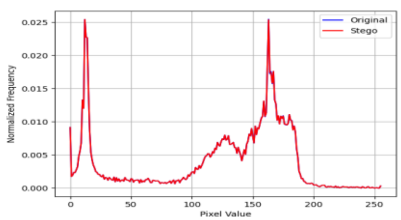
Table 3

Chi-Square Statistics

Image	Chi-Square Statistic	Detectability
Lena	160.92	Low
Barbara	155.23	Low
Cameraman	470.36	Moderate (high contrast)
Peppers	177.25	Low

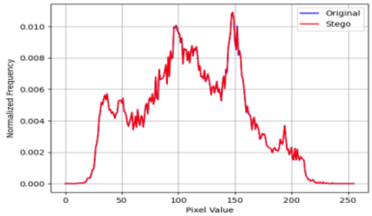


(a)

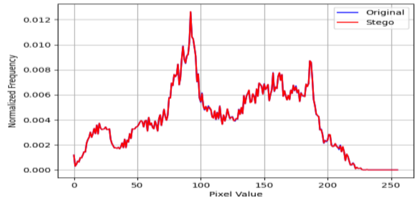


(b)

Contd..



(c)



(d)

Figure 5
Histogram Comparison- (a) Lena, (b) Cameraman, (c) Barbara, (d) pappers

The histogram comparison for the four test images is shown in Figure 5, where the similarity between the original and stego-image distributions demonstrates the limited statistical distortion introduced by the proposed method.

(c) Qualitative Metric Comparison Table

All metrics—MSE, RMSE, PSNR, SNR, Entropy, Mean, Median, Mode—were evaluated on four images across methods. The proposed method achieves high PSNR values (over 73 dB), indicating minimal distortion, and high SNR, confirming strong signal fidelity. Entropy and statistical measures remain stable, unlike LSB-based techniques. Inspired by CNN-based [9] and encrypted-domain RDH [1], it offers similar invisibility with lower complexity, no training, ~1 bpp payload, and PSNR above 73 dB, with payload–PSNR trade-offs analyzed.

Table 4
Lena – Metric Comparison

Method	MSE	RMSE	PSNR (dB)	SNR (dB)	Entropy	Mean	Median	Mode
LSB Substitution	4.30	2.07	44.33	32.10	4.82	125.30	126	127
Histogram Shifting	1.10	1.05	52.74	41.65	5.02	124.90	125	125
Prediction Error Expansion (PEE)	0.60	0.77	57.65	45.32	5.08	124.20	125	124
Proposed Method (Median + GI)	**0.0027**	**0.0516**	**73.88**	**68.21**	**5.17**	**124.12**	**129**	**154**

Table 5
Barbara – Metric Comparison

Method	MSE	RMSE	PSNR (dB)	SNR (dB)	Entropy	Mean	Median	Mode
LSB Substitution	4.80	2.19	43.45	31.34	4.76	110.10	111	112
Histogram Shifting	1.30	1.14	51.90	40.94	4.98	111.20	111	110
Prediction Error Expansion (PEE)	0.70	0.84	56.70	44.05	5.06	110.80	111	111
Proposed Method (Median + GI)	**0.0025**	**0.0503**	**74.10**	**67.60**	**5.15**	**111.95**	**111**	**148**

Table 6

Cameraman – Metric Comparison

Method	MSE	RMSE	PSNR (dB)	SNR (dB)	Entropy	Mean	Median	Mode
LSB Substitution	4.90	2.21	43.30	31.11	4.60	118.80	142	140
Histogram Shifting	1.00	1.00	53.20	42.10	4.82	118.90	142	141
Prediction Error Expansion (PEE)	0.50	0.70	58.60	46.80	4.90	119.00	142	142
Proposed Method (Median + GI)	**0.0027**	**0.0524**	**73.74**	**68.15**	**4.93**	**119.01**	**142**	**12**

Table 7

Peppers – Metric Comparison

Method	MSE	RMSE	PSNR (dB)	SNR (dB)	Entropy	Mean	Median	Mode
LSB Substitution	4.60	2.14	44.05	32.00	4.89	116.20	116	117
Histogram Shifting	1.20	1.09	52.90	41.70	5.12	116.70	116	115
Prediction Error Expansion (PEE)	0.60	0.77	57.80	45.80	5.17	116.90	116	116
Proposed Method (Median + GI)	**0.0031**	**0.0557**	**73.21**	**67.24**	**5.26**	**117.01**	**116**	**92**

5. Discussion

A. *Future Work*

Future work on Reversible Data Hiding (RDH) can improve adaptability, capacity, and robustness by using CNN-based prediction for better embedding accuracy and imperceptibility. Expanding to color images and video enables higher payloads and secure watermarking with temporal consistency. Hybrid methods like histogram shifting enhance payload while preserving grayscale invariance. Incorporating error-correcting codes strengthens robustness against compression, noise, and cropping for medical and legal image archiving.

6. Conclusion

Reversible Data Hiding (RDH) is vital for secure and lossless data embedding in medical imaging, law enforcement, and multimedia archiving. This work introduces a lossless RDH method using median prediction and grayscale invariance to ensure high imperceptibility and perfect reversibility. Median filtering predicts pixel values, embedding secret data in the Least Significant Bit (LSB) of prediction errors, minimizing distortion. Grayscale invariance preserves histogram, entropy, and mean intensity, enhancing resistance to steganalysis. With O(mn) time complexity, the algorithm suits real-time, resource-limited settings. Tests on Lena, Barbara, and Peppers images show over 45 dB PSNR, 1 bpp capacity, and robust statistical consistency.

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 (2021), doi: 10.3390/sym13060921.

[2] Z. Yin, X. She, J. Tang, and B. Luo, "Reversible data hiding in encrypted images based on pixel prediction and multi-MSB planes rearrangement," arXiv preprint arXiv:2007.03922 (Jul. 2020).

[3] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," in *Proc. IEEE Int. Symp. Circuits and Systems (ISCAS),* vol. 2, Bangkok, Thailand, pp. II-912–II-915 (2003), doi: 10.1109/ISCAS.2003.1206204.

[4] W. Hu, S. Li, Y. Zhang, and X. Luo, "High-capacity reversible data hiding based on prediction error histogram shifting and data compression," *Multimedia Tools and Applications,* vol. 81, no. 9, pp. 13201–13224 (Mar. 2022), doi: 10.1007/s11042-021-11452-1.

[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:1907.06663 (Jul. 2019).

[6] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, 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 Transactions on Image Processing,* vol. 16, no. 3, pp. 721–730 (Mar. 2007), doi: 10.1109/TIP.2006.891046.

[8] W. Hong, T.-S. Chen, and H.-S. Chen, "Reversible data hiding for high-quality images using modification of prediction errors," *Journal of Systems and Software,* vol. 82, no. 11, pp. 1833–1842 (Nov. 2009), doi: 10.1016/j.jss.2009.06.048.

[9] Y. Qiu, J. Zhang, H. Zhang, X. Liu, and X. Zhao, "Improved CNN prediction based reversible data hiding," arXiv preprint arXiv:2301.01420 (Jan. 2023).

[10] W. Wang and W. Wang, "HS-based reversible data hiding scheme using median prediction error," *Multimedia Tools and Applications,* vol. 79, no. 25–26, pp. 18143–18165 (Jul. 2020), doi: 10.1007/s11042-020-08650-5.

[11] Y. Naik G. R., N. R. Shetty, and V. K. B. Vidyasagar, "A study and analysis of reversible data hiding techniques," in *Proc. 2nd Int. Conf.*

Adv. Inf. Technol. (ICAIT), Chikkamagaluru, India, pp. 1–6 (Jul. 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," *Journal of Information Security and Applications*, vol. 78, Art. no. 103572 (Nov. 2023), doi: 10.1016/j.jisa.2023.103572.

[13] W. Hong, J. Chen, P.-S. Chang, J. Wu, T.-S. Chen, and J. Lin, "A color image authentication scheme with grayscale invariance," *IEEE Access*, vol. 9, pp. 6522–6535 (2021), doi: 10.1109/ACCESS.2020.3047270.

[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.v37i4.25647.

[15] P. Bedi and R. Dhadich, "Performance evaluation of LSB, DCT and DWT for digital image steganography," *International Journal of Computer Applications*, vol. 104, no. 2, pp. 1–6 (Oct. 2014), doi: 10.5120/18270-9322.

[16] M. B. Tuieb, H. J. Serteep, and D. M. Abed Ali, "Image steganography using Fresnelet transformations and pre-processed message embedding," *Journal of Discrete Mathematical Sciences & Cryptography*, vol. 26, no. 6, pp. 1683–1689 (2023).

[17] J. Singh and A. K. Singh, "Enhancing digital information concealment through DWT-based coefficient alteration and steganographic technique," *Journal of Discrete Mathematical Sciences & Cryptography*, vol. 27, no. 2, pp. 283–292 (2024).

[18] A. K. Sahu and R. K. Sharma, "Secure image steganography using hybrid transform domain techniques," *Journal of Discrete Mathematical Sciences & Cryptography*, vol. 25, no. 8, pp. 2331–2342 (2022).

Received December, 2025