RESEARCH PAPER

Hybrid Approach Integrating Controlled Pixel Modification, Histogram Shifting, And Aes Approaches

Jangam Deepthi[1], Dr. T. Venugopal[2]

[1] Research Scholar, Department Of Computer Science And Engineering, Jawaharlal Nehru Technological University, Hyderabad, Telangana, India. Email: deepthijangam2@gmail.com

[2] Professor, Department Of Computer Science And Engineering, Principal, Jntuh College Of Engineering, Siricilla, Telangana, India. Email: drtvgopal@gmail.com

Received: 20th Feb, 2026; **Revised:** 4th Mar, 2026; **Accepted:** 25th Mar, 2026; **Available Online:** 10th Apr, 2026

Abstract

Reversible data hiding in encrypted domain (rdh-ed) plays an important role in transmitting the image securely in which both the original image and embedded information can be recovered without any loss. This paper presents a novel rdh-ed framework that utilizes reserving room before encryption (rrbe) approach, followed by a dual-stage data embedding approaches as controlled pixel modification (cpm) and histogram shifting (hs). Unlike conventional methods that embed data after encryption, our proposed approach securely embed the visible an invisible information prior to encryption there by ensuring recovering perfect recovery of image data. First, the space is reserved in the original image by using reserving room before encryption (rrbe) approach by not introducing the significant visual distortion. Next, the visible watermark is embedded within the reserved space by using cpm method in order to ensure ownership and the additional secret data is embedded through the hs approach exploiting the pixel intensities within the reserved regions. This dual embedding process ensures the high capacity and perceptibility by maintaining the reversibility. After embedding, the image is encrypted by using advanced encryption standard (aes) algorithm in order to ensure confidentiality throughout the transmission. Extraction process involves decrypting the encrypted image using appropriate aes key thus extracts both the visible watermark and additional secret data. Subsequently, the original image is perfectly recovered without any loss. In order to validate the performance of the proposed system, quality metrics such as peak signal-to-noise ratio (psnr), structural similarity index measure (ssim) and mean squared error (mse) are computed. Experimental results states that the proposed system achieves high visual quality and lossless recovery thus making it suitable for applications such as secure multimedia communication, medical imaging and copyright protection.

Keywords: Rdh, Rrbe, Vrae, Rdh-Ed, Aes, Cpm, Hs.

How To Cite This Article: Deepthi J, Venugopal T. Hybrid Approach Integrating Controlled Pixel Modification, Histogram Shifting, And Aes Approaches. Int J Drug Deliv Technol. 2026;16(26s):243-248. Doi: 10.25258/ijddt.16.26s.24

1. Introduction

In today's world of digital communication, integrity protection, confidentiality and authenticity of multimedia information has been the major concern. Digital images are widely transmitted and shared through the communication channels which are not secure, making them vulnerable to unauthorized access, tampering and copyright violations. To address these challenges, Reversible Data Hiding(RDH) has emerged as an important technique that not only allows embedding of additional information into an image but also guarantees lossless recovery of the original content after additional data has been extracted. When the RDH integrated with image encryption , forms the basis for Reversible Data Hiding in Encrypted Domain(RDH -ED) thus ensuring both the data security and full reversibility.

Basically, RDH approaches are categorized into two types: Vacating Room After Encryption(VRAE) and Reserving Room Before Encryption(RRBE).

In Vacating Room After Encryption(VRAE), Space is reserved after encryption in order to embed the additional message .Due to the difficulty in modifying encrypted data in order to embed additional data , the distortion is

introduced as well as embedding capacity is decreased.

In Reserve Room Before Encryption approach, Space is reserved before the encryption in order to embed additional data. In this, large amount of data can be accommodated within the reserved space without any difficulty in modifying the pixel data. Therefore, this approach results in maximum embedding capacity and also also supports more controlled an distortion-free embedding of additional data than compared with VRBE approach.

In this paper, we propose a novel RRBE -based RDH -ED method that combines both the Controlled Pixel Modification (CPM) and Histogram Shifting (HS) techniques to embed both a visible watermark and additional secret data before encryption within the reserved space which is created by using RRBE approach. CPM is applied to embed a visible watermark in reserved regions while preserving the structural properties of the image. Subsequently, HS is used to embed a secret message by exploiting the pixel intensities of the histogram. Therefore, this combined approach ensures the high embedding capacity as well as minimal perceptual distortion. Once the watermark and additional data are embedded, the modified image is encrypted by using the Advanced Encryption Standard(AES) algorithm in order to ensure secure transmission through the communication channel. At the receiver's side, the embedded watermark and additional text message are extracted accurately then the original image is perfectly obtained without any loss thus ensuring lossless recovery of the original image.

2. Related Work

In the context of unencrypted images, Reversible data hiding is widely used in which the Difference Expansion(DE),Histogram Shifting(HS) and Prediction Error Expansion(PEE) techniques are most effective[1][2]. However, the integration of encryption with reversible data hiding introduces new challenges in preserving image quality and maintaining exact recovery[3][4][5].

Earlier works such as Zhang's VARE(Vacating Room After Encryption) method explored the possibility of RDH in encrypted images but often suffered from limited embedding capacity and distortion due to direct modification of encrypted pixels[3]. To overcome this, RRBE(Reserving Room Before Encryption) approaches were used that enables better control over embedding distortion and capacity[5][6].However, many existing RRBE -based techniques neglect visible watermarking and lack embedding capacity[7].

Recent studies combine AES encryption with RDH, where Histogram-based[8][14][15] and LSB -based[11] embedding methods are used in encrypted domain. In Controlled Pixel Modification, when the bit to be embedded is '1', the MSB of the pixels are flipped this causes controlled distortion while ensuring reversibility, when bit to be embedded is '0', no change in the MSB position. Therefore, in Controlled Pixel Modification (CPM) approach, the obtained PSNR value is 35.27 dB which is less that results in high distortion in the recovered image ,SSIM value is 19.33, MSE value is 099959 and Maximum Embedding capacity is 22, 278 bits for 512x512 size images which results in limited embedding capacity and low distortion in structured regions[17].

However, recent advances such as block-based secret sharing and adaptive block-wise histogram shifting [18] approaches, the pixel intensity histogram is computed as per peak and zero points. Based on the embedded bit either 1 or 0, the histogram is shifted by one position between zero and peak points, otherwise that histogram remains at the same position respectively. In histogram shifting, the obtained performance metrics are PSNR as 46.74 dB, MSE as 1.3780, SSIM as 0.9995 and Maximum Embedding Capacity as 32, 768 bits for 512x512 images that results in visible distortion and lower embedding capacity. In most of the cases, histogram causes overflow and underflow issues.

Therefore, the integration of both visible watermark and addition text message embedding with secure encryption and full recovery remains an active research challenge.The combination of CPM for visible watermark embedding and HS for additional text message embedding, followed by AES encryption, motivating the comprehensive approach proposed in this paper.

3. Proposed Methodology

The proposed framework utilizes reversible data hiding system in the encrypted domain approach as well as Reserve Room Before Encryption(RRBE) strategy. It consists of four main stages: room reservation, dual-stage embedding, encryption, and recovery.

3.1 Room Reservation:

First, color image or gray scale image is considered as an input. The input image is divided recursively into non-overlapping 2x2 blocks. The Room is Reserved in this blocks in order to embed both visible watermark and additional text messages by using Reserve Room Before Encryption(RRBE) approach.

3.2 Dual-Stage Data Embedding:

- Visible Watermark Embedding using CPM: The visible watermark such as text is embedded into the reserved blocks using Controlled Pixel Modification(CPM) algorithm in a controlled manner.
- Secret Data Embedding using Histogram Shifting: Histogram Shifting is applied to the intensity distribution of reserved regions. Peak and Zero points are identified. These peak and zero points are used to shift pixel values and embed the binary representation of the secret message depending on whether the embedded bit to be 1 or 0 respectively.

3.3 AES Encryption:

The image with embedded visible watermark and additional data is encrypted using the Advanced Encryption Standard (AES) algorithm to ensure authentication and secure transmission.

3.4 Decryption, Data Extraction, and Image Recovery:

- The image is decrypted using the correct AES key.
- The embedded message and watermark are extracted by applying the inverse operations of CPM and HS .
- The original image is restored losslessly .

4. Block diagram of proposed methodology:

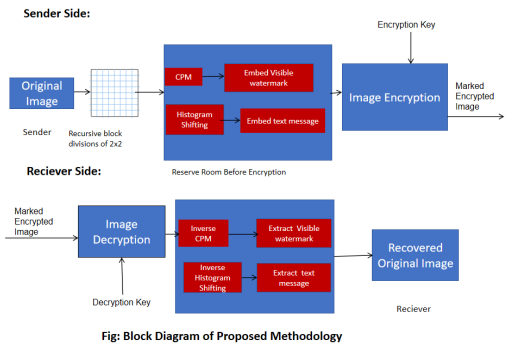

Fig: Block Diagram of Proposed Methodology

The above diagram illustrates the block diagram of the proposed methodology that accepts original image as an input at the sender side.

The original image is divided recursively into 2x2 blocks , and space is reserved within these blocks by using RRBE strategy in order to accommodate visible watermark and additional text message. Visible watermark embedded by using CPM algorithm and additional text message such as secret message is embedded within the reserved blocks by using histogram shifting approach that results in the embedded image. This embedded image is encrypted by using AES algorithm with the help of an encryption key that generates the marked encrypted image which can be securely transmitted through the communication channel in order to provide authentication and confidentiality.

From the above diagram, at receiver side , marked encrypted image which contain both the visible watermark and additional text message is received as an input to image decryption phase, that decrypts marked encrypted image by using appropriate decryption key generated embedded image which in similar to the image that was generated prior to encryption. For this generated embedded image, inverse CPM operation is applied in order to extract visible watermark and inverse histogram shifting operation is applied in order to extract additional text message, thereby finally recovering the original image without any distortion ensuring full reversibility.

Algorithm 1: Controlled Pixel Modification

Input:

Image I of size R × C

Secret message D (in binary)

Key K to generate pseudo-random matrix M

Output:

Final image E' (encrypted + embedded)

Steps:

1. **Generate matrix** M of size R × C with pseudo-random values in range [0, 255] using key K.
2. **Encrypt** the image:

E = I ⊕ M (bitwise XOR of image and matrix)

3. **Initialize** a 2D array E' of size R × C filled with zeros.
4. Set x = 1, y = 1, k = 1
5. while x≤ R-B-1 do

while y≤C-1 do

// Extract block T of size bx2 starting at (x,y)

T = block of E from rows x.. x+B-1 and columns y..y+1

M=1
S=D[k] // Kth secret bit
if S=1 then
// Map pixels in first column of T using predefined rule
While m≤ B do
P=T[m,1]
if p≤ 128 then
P'=P+128
else
P'=P-128
end if
T[m,1]=P'
m=m+1
End while
End if

6. //Put modified block back
Replace block in E' at rows x.. x+B-1, columns y..y+1 with T
7. x=x+B
8. k=k+1
9. Y=y+2
10. End while
11. End while
12. Return E'

The above algorithm scans the encrypted image in small, non-overlapping blocks and use those blocks to embed secret bits. Starting from top-left corner, it takes a block of size Bx2 pixels at position (x,y). For each such block, the secret bit is embedded in the first column of each block .

If the secret bit to be embedded is 1, the first column of the block is modified using simple rule that for a pixel value 'P', if p≤ 128, then adds 128 otherwise subtracts 128. This process effectively flips the MSB of the pixel by keeping the value in the allowable range 0-255 .

If the secret bit to be embedded is '0' , the block is left unchanged.

After processing all the blocks of 2x2 size in the first column , the process moves down to the next blocks and repeat the same process till all blocks in the image are completed. Finally, all these modified blocks are placed back in the original image.

Algorithm 2 : HIstogram Shifting(HS)

1. Compute histogram of pixel values in original image
2. Find a peak bin i.e., most frequent bin and a zero bin i.e., empty value.
3. Shift all pixel values between peak and zero by +1 or-1 to create an empty space next to the peak.
4. Scan all elements that are equal to peak:

If the secret bit to be embedded is '0', leave the peak value as it is.

If the secret bit to be embedded is '1', shift the value by +1 in order to move toward the zero bin.

5. By restoring all these modified pixel values in the original image, form the marked embedded image.

The above algorithm first computes the histogram of pixel values in an image. Then, it finds the peak point and zero pint in histogram. All the pixel values in the histogram are shifted between peak and zero point depending on whether the bit to be embedded is either '0' or '1'. First, we need to identify all peak points. If the bit to be embedded is '1', then the pixel value shifted by '+1' in order to create a space toward zero bin. If the bit to be embedded is '0', no need shift the pixel by one position forward. This process continues until all pixels are computed. Finally, all these modified pixels are placed in image there by forming the marked embedded image.

6. Performance Evaluation:

The performance of the proposed system is evaluated by using the following measures such as

a) Mean Squared Error (MSE)

The Mean Squared Error (MSE) measures the average squared difference between the pixel intensities of the original and recovered image.

$$MSE=\frac{1}{MN}\sum_{1=1}^{M}\sum_{j=1}^{N}[I(i,j)-I^{'}(i,j)]^{2}$$

Where,

M and N are image dimensions(for e.g,8x8=64 pixels)

I(i,j) is the intensity of the original image at pixel (i, j),

I′(i,j) is the intensity of the watermarked or recovered image,

b) Peak Signal to Noise Ratio(PSNR):

The Peak Signal-to-Noise Ratio (PSNR) is a widely used quantitative measure that evaluates the similarity between the original image and the recovered image. It is derived from the Mean Squared Error (MSE) and is expressed in decibels (dB).

$$PSNR=10x log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

Where ,

MAX_I is the maximum possible pixel value of the image , usually 255 for 8-bit grayscale images

MSE is the Mean Squared Error between the original and recovered image.

Lower MSE values indicate higher image quality and better preservation of original details.Since MSE is inversely related to PSNR, minimizing MSE improves the perceptual similarity.

c) Structural Similarity Index Measure (SSIM)

The Structural Similarity Index Measure (SSIM) is a perceptual metric that evaluates image similarity based on luminance, contrast, and structural information. It provides a more human-vision-based assessment compared to PSNR.

$$SSIM(x,y) = \frac{(2\mu_x \mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}$$

Where,

- μ_x, μ_y = average pixel values of x, y
- σ_x^2, σ_y^2 = variances
- σ_{xy} = covariance between x and y
- C_1 , C_2 = small constants to stabilize division (e.g., $C_1=(0.01x\ L)^2$, $C_2= (0.03x\ L)^2$, where L=255)

SSIM ranges between 0 and 1. Values close to 1 indicate high visual quality.It is more sensitive to human visual perception than MSE or PSNR.

In the Proposed Framework, the SSIM metric was used to validate the structural content of the image that was not affected by watermark embedding, encryption, or recovery.

d) **Maximum Embedding Capacity (MEC)**

Maximum Embedding Capacity (MEC) measures the total amount of data i.e.,watermark and additional data that can be embedded in an image without causing visible degradation. It is expressed in bits.

$$\text{Maximum Embedding capacity}_{bits} = \left[\frac{H}{block\ size(verical)}\right] \times \left[\frac{W}{block\ size(horizontal)}\right]$$

A higher embedding capacity indicates that more data can be hidden while maintaining acceptable image quality.However, increasing embedding capacity may slightly reduce PSNR due to greater pixel modification.The goal is to maximize capacity while maintaining high PSNR and SSIM.

7. Experimental Results

Experiments were conducted on standard test images such as Lena, Baboon, Peppers, boat , barbara and Airplane . PSNR, SSIM, and MSE were used to evaluate quality.

For Gray Scale Images:

Image/Metrics	PSNR	MSE	SSIM	MEC
Lena	67.84 dB	0.010693	0.9999	32768 bits
Barbara	67.78 dB	0.010834	1.0000	21252 bits
Pepper	67.99 dB	0.010332	1.0000	44793 bits
Boat	67.82 dB	0.010732	0.9999	27489 bits
Airplane	67.85 dB	0.010671	0.9999	32768 bits
Baboon	67.91 dB	0.010523	0.9999	30735 bits

For Gray Scale Images:

Image/Metrics	PSNR	MSE	SSIM	MEC
Lena	58.77 dB	0.086268	0.9999	32768 bits
Barbara	59.70 dB	0.069629	1.0000	21252 bits
Pepper	72.61 dB	0.003563	1.0000	44793 bits
Boat	55.48 dB	0.184132	0.9999	27489 bits
Airplane	51.14 dB	0.499663	0.9999	32768 bits
Baboon	55.39 dB	0.187981	0.9999	30735 bits

Visual analysis showed clear watermark visibility and perfect recovery with minimal visual difference.

8. Conclusion and Future Work

This paper presented a robust RDH-ED framework integrating Controlled Pixel Modification and Histogram Shifting, followed by AES encryption. By reserving room before encryption, the method enables effective embedding of a visible watermark and hidden message while allowing full recovery of the original image. Experimental evaluation using PSNR, SSIM, and MSE confirmed high visual quality and fidelity.

Future work includes extending the framework to video, medical imaging, and region-based adaptive embedding using AI models for dynamic capacity optimization.

9.References

1. J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding—New paradigm in digital watermarking," *EURASIP Journal on Advances in Signal Processing*, vol. 2002, no. 2, pp. 185–196, 2002.

2. Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354–362, Mar. 2006.

3. X. Zhang, "Reversible data hiding in encrypted image," *IEEE Signal Processing Letters*, vol. 18, no. 4, pp. 255–258, Apr. 2011.

4. W. Hong, T.-S. Chen, and H.-Y. Wu, "An improved reversible data hiding in encrypted images using side match," *IEEE Signal Processing Letters*, vol. 19, no. 4, pp. 199–202, Apr. 2012.

5. K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 3, pp. 553–562, Mar. 2013.

6. L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong, "Reversible image watermarking using interpolation technique," *IEEE Transactions on*

Information Forensics and Security, vol. 5, no. 1, pp. 187–193, Mar. 2010.

7. Y. Q. Shi, X. Li, X. Zhang, H. T. Wu, and B. Ma, "Reversible data hiding: Advances in the past two decades," *IEEE Access*, vol. 4, pp. 3210–3237, 2016.

9. W. Zhang, X. Hu, X. Li, and N. Yu, "Recursive histogram modification: Establishing equivalency between reversible data hiding and lossless data compression," *IEEE Transactions on Image Processing*, vol. 22, no. 7, pp. 2775–2785, July 2013.

10. D. Kundur and D. Hatzinakos, "Digital watermarking using multiresolution wavelet decomposition," *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Seattle, WA, USA, 1998, pp. 2969–2972.

11. R. Chandramouli, N. Memon, "Analysis of LSB based image steganography techniques," *Proceedings of the International Conference on Image Processing (ICIP)*, Rochester, NY, USA, 2002, pp. 1019–1022.

12. National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES)," *FIPS Publication 197*, Nov. 2001. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

13. J. Zou, W. Cao, S. Yi, Y. Zheng, and Z. Hua, "Reversible Data Hiding over Encrypted Images via Intrinsic Correlation in Block-Based Secret Sharing," *arXiv*, Feb. 2025 arxiv.org.

14. A. Arham and H. A. Nugroho, "Enhanced reversible data hiding using difference expansion and modulus function with selective bit blocks in images," *Cybersecurity*, vol. 7, Art. 61, Nov. 2024 cybersecurity.springeropen.com.

15. Z. Pang, H. Li, Z. Xiao, and L. Sui, "Reversible Data Hiding in Encrypted Images Based on an Adaptive Recognition Strategy for Blocks," *Symmetry*, vol. 15, Art. 524, 2023 reddit.com+15mdpi.com+15dl.acm.org+15.

16. "Reversible Data Hiding in Encrypted Images With Asymmetric Coding and Bit-Plane Block Compression," *IEEE Trans. on Multimedia*, vol. 26, 2024 dl.acm.org.

17. "Reversible Data Hiding Scheme in Encrypted Images by Controlled Pixel Modification", 2020 IEEE 4th Conference on Information & Communication Technology (CICT)

18. Reversible Data Hiding in Encrypted Images Using Difference Expansion and Histogram Shifting, 2024 by Namitha R.Shetty, Yogish Naik G.R.,Vidyasagar K.B, journal of Electrical Systems 20-10s(2024): 4732-4743

Author Biography:

Jangam Deepthi is a dedicated research scholar in the Department of Computer Science and Engineering(ECE) at University College Of Engineering and Technology For Women(UCE&TW), Kakatiya University,Warangal.

She is academic journey began with a Bachelor's degree in Engineering from KU College of Engineering and Technology, Kakatiya University in 2013. Following her undergraduate studies, she pursued a Master of Technology in Computer Science and Engineering at JNTUH College of Engineering, Jagitial graduating in 2015. Her

current research focuses on advancing reversible data hiding techniques in encrypted domain. Her academic background and ongoing research reflect a strong commitment to contributing to the fields of Computer Science and Engineering, particularly in improving medical imaging technologies and processing methods.

Dr. T. Venugopal is currently working as a **Professor of CSE & Principal I/c at JNTUH University College of Engineering Rajanna Sircilla, Sircilla** District, Telangana, India. His interesting areas include image processing, data mining, cryptography and file-systems. **Under his guidance 13 students have obtained Ph.D., 2 students have submitted their thesis and about 10 students are pursuing Ph.D**. He has published more than 70 research papers in various International Journals. He participated and presented research papers in International and National Conferences.