REVERSIBLE DATA HIDING IN ENCRYPTED DOMAIN BY USING HISTOGRAM SHIFTING AND COMPRESSION TECHNIQUES

[1]Jangam Deepthi,

Research scholar, Dept. Of Computer Science and Engineering, Jawaharlal Nehru Technological University,Hyderabad, Telangana, India.

e-mail: deepthijangam2@gmail.com

[2]Dr.T.Venugopal

Professor, Dept. Of Computer Science and Engineering, Principal, JNTUH College Of Engineering, Siricilla, Telangana, India

e-mail: drtvgopal@gmail.com

Abstract

This paper presents a novel reversible data hiding approach in the encrypted domain (RDH-ED) that combines block-adaptive histogram shifting with context-aware compression to substantially enhance embedding capacity while guaranteeing complete reversibility of both the image and the embedded data. In contrast to conventional global histogram shifting methods, the proposed technique partitions the encrypted image into entropy-driven adaptive blocks, allowing localized peak–zero bin selection for efficient data embedding. To further increase available embedding space, each block is subjected to a dual-mode lossless compression strategy, dynamically selecting between Run-Length Encoding and Huffman coding based on local statistics. The encryption stage, implemented using AES in counter mode (AES-CTR), preserves the intensity distribution, enabling effective histogram-based embedding in the encrypted domain. This paper also provides mathematical formulations for embedding capacity, distortion analysis, and compression gain, as well as computational complexity evaluation. Experimental results on standard benchmark images demonstrate that the proposed approach achieves up to 28% higher embedding capacity compared to existing RDH-ED schemes, with a PSNR degradation of less than 1 dB and maintaining 100% recovery accuracy. The method is fully implemented in Python, ensuring reproducibility and ease of extension to colored images and video content. This paper shows that the proposed algorithm offers a practical and secure solution for applications such as privacy-preserving cloud storage, secure medical image annotation, and digital forensics.

Keywords— Reversible data hiding, encrypted images, histogram shifting, lossless compression, adaptive embedding, AES encryption.

I. INTRODUCTION

Reversible data hiding in the encrypted domain (RDH-ED) has emerged as a critical technique for secure and privacy-preserving multimedia communication, cloud storage, and digital forensics. By enabling additional data to be embedded into encrypted images without compromising the confidentiality and integrity of the original content, RDH-ED supports applications such as medical image annotation, copyright protection, and secure data sharing.

Traditional reversible data hiding methods primarily operate on plaintext images using techniques like histogram shifting, difference expansion, or prediction error expansion. However, when extended to the

encrypted domain, these techniques face new challenges. Encryption typically disrupts the statistical properties of the image data, thus limiting the straightforward application of classic embedding methods. Existing RDH-ED schemes often rely on global histogram shifting or bit-plane manipulation, which tend to offer suboptimal embedding capacity and suffer from increased distortion or computational complexity.

This paper presents a novel RDH-ED scheme that overcomes these limitations by introducing block-adaptive histogram shifting combined with context-aware compression. Our approach partitions the encrypted image into entropy-driven blocks, enabling localized peak and zero bin selection for histogram shifting, thereby maximizing the embedding capacity while minimizing distortion. Additionally, the use of dual-mode lossless compression—selecting either Run-Length Encoding or Huffman coding dynamically based on local block characteristics—provides further embedding space by reclaiming redundant data regions. The applied encryption method, AES in counter mode (AES-CTR), preserves the statistical histogram structure necessary for effective embedding in the encrypted domain.

Background

Reversible data hiding in the encrypted domain (RDH-ED) has gained considerable attention as a secure and privacy-preserving technology that enables embedding auxiliary information into encrypted images while allowing perfect recovery of both the original image and the embedded payload. This technique is crucial in various applications, including secure cloud storage, confidential medical image annotation, copyright protection, and digital forensics. Unlike traditional data hiding methods that operate on plaintext images, RDH-ED must address the challenge of embedding data without compromising encryption security or image confidentiality.

Conventional RDH-ED schemes often rely on global image statistics, such as histogram shifting or bit-plane manipulation, to embed data. However, encryption typically obscures spatial correlations and pixel distributions, limiting the embedding capacity and increasing distortion or computational complexity. Moreover, existing methods usually apply fixed or global embedding strategies that do not fully exploit local image properties in the encrypted domain.

Motivation

The limitations of current RDH-ED methods motivate the development of more efficient and adaptive embedding schemes. Specifically:

- Global histogram-based techniques neglect the inherent local variations and redundancies present in images, resulting in suboptimal embedding capacity and image quality degradation.
- The encryption process, particularly symmetric schemes like AES in CTR mode, preserves the pixel value range and histogram structure, suggesting an opportunity to perform embedding at a more granular, block-wise level.
- Integrating lossless compression techniques can reclaim redundant space within encrypted blocks, thus enabling increased payload embedding without compromising reversibility.

Addressing these issues is critical to improving embedding capacity, reducing

distortion, and maintaining computational efficiency, thereby advancing the practical applicability of RDH-ED schemes for sensitive and high-stakes information systems.

Research Gap

Despite numerous works on RDH-ED, there remain significant gaps:

- Most existing methods use global histogram shifting or bit-plane schemes without adapting to local image characteristics in the encrypted domain, limiting embedding capacity.
- The joint use of adaptive embedding and context-aware block-level compression within encrypted images is underexplored, leaving potential embedding space unexploited.
- Formal mathematical modeling of embedding capacity, distortion, and compression gain tailored to block-adaptive RDH schemes is lacking.
- Comprehensive complexity and security analyses that integrate block-adaptive embedding and compression strategies along with practical implementation details remain scarce.

This paper proposes a novel block-adaptive RDH-ED approach that fills these gaps by combining entropy-based block partitioning, adaptive peak-zero bin selection for histogram shifting, and dynamic selection between run-length and Huffman coding for lossless block compression. This combination maximizes embedding capacity and ensures error-free image and payload recovery, thereby significantly advancing state-of-the-art RDH in encrypted domains.

II. RELATED WORK

Reversible data hiding (RDH) has been investigated extensively over the past two decades due to its capability to embed additional information into a host medium while enabling lossless recovery of the original content. This property is particularly crucial in sensitive domains such as medical imaging, military reconnaissance, and forensic analysis, where even minor alterations to the original data can lead to significant consequences. The early milestone work by Ni *et al.* introduced the concept of histogram shifting (HS), where the most frequent intensity (peak bin) is identified, and neighbouring values are shifted to create vacant slots for data embedding. While extremely effective for grayscale images in the plaintext domain, HS loses much of its advantage when pixel correlations are destroyed by encryption. Subsequent enhancements incorporated difference expansion (DE) and prediction error expansion (PEE) techniques, which utilized differences or prediction residuals to hide data, thereby improving fidelity. However, these approaches fundamentally relied on spatial redundancy, which encryption significantly disrupts.

To address the new challenges brought by encryption, two main paradigms emerged in RDH for encrypted domains (RDH-ED): Vacating Room After Encryption (VRAE) and Reserving Room Before Encryption (RRBE). The VRAE strategy was exemplified by Zhang *et al.* , where an image is first encrypted and then modified to make room for embedding. Here, the embedding process is applied directly to ciphertext pixels or their bit-planes, offering a separable property — meaning data extraction and image decryption can be performed independently. Despite securing

content during embedding, VRAE methods tend to suffer from limited capacity because high-entropy encrypted data lacks compressible redundancy, thereby restricting the space available for payload insertion.

The RRBE paradigm emerged to overcome these limitations by preparing embedding space in the plaintext domain prior to encryption. This is typically achieved by compressing parts of the original image or its auxiliary information, and then encrypting the result alongside the hidden data. Fu *et al.* advanced this idea by combining adaptive pixel prediction with Huffman coding of prediction errors, significantly boosting embedding capacity while maintaining high visual quality. Ren *et al.* further integrated block classification techniques, predicting embedding difficulty for different regions of the image to optimize capacity–distortion trade-offs. These RRBE schemes demonstrated notable improvements, yet they also introduced complexity in block classification and metadata handling.

Lossless compression strategies have been applied not only in RRBE but also within the encrypted domain. Huffman coding has been effectively employed post-encryption to reduce redundancy, as in , while bit-plane compression methods have been developed to operate directly on encrypted pixel-level data, yielding high embedding capacity. Adaptive context-aware compression methods that dynamically select between Run-Length Encoding (RLE) and Huffman coding , based on local region complexity have been shown to utilize space more efficiently than fixed-method compression.

Another line of RDH-ED improvement focuses on histogram modification under encryption. For example, multi-peak histogram shifting methods select several peaks for shifting within the ciphertext intensity distribution, thereby increasing payload without significantly impacting peak distortion. Similarly, block-based pixel classification , allows the identification of smooth and textured regions, assigning different embedding strategies for each, thus balancing embedding room and distortion more effectively.

The security aspects of RDH-ED have also been formally analyzed. Studies such as underline that while embedding in ciphertext ensures content confidentiality, improper design may inadvertently leak statistical information. Therefore, schemes must ensure that post-embedding encrypted images are computationally indistinguishable from regular encrypted images without knowledge of the embedding key.

Application-driven adaptations of RDH-ED are increasingly important. In medical imaging, reversible embedding ensures auxiliary annotations can be stored alongside diagnostic data without affecting the original scan ,. In cloud storage scenarios, RDH-ED serves to integrate authentication, copyright metadata, and usage logs directly into encrypted assets ,.

While RDH-ED has seen numerous creative approaches, there remains a clear research gap in methods that simultaneously leverage adaptive local histogram properties and blockwise context-aware compression in the encrypted domain. Existing methods rarely

combine *both* adaptive embedding (through local entropy/peak-zero analysis) and flexible compression (choosing optimal methods for each block based on statistical profile). This integration, as explored in works like , , but not yet fully optimized, represents a promising direction for achieving significantly higher embedding capacity, lower distortion, and robust reversibility compared to current state-of-the-art frameworks.

The approach proposed in this paper directly addresses this gap by formulating a block-adaptive histogram shifting algorithm integrated with dual-mode compression in the encrypted domain, offering enhanced performance across capacity, quality, and reversibility metrics when benchmarked against existing VRAE and RRBE schemes.

III. EXISTING SYSTEM

Reversible data hiding in the encrypted domain (RDH-ED) has attracted considerable research attention due to its applications in secure multimedia storage and privacy-preserving communication. The existing RDH-ED methods broadly fall into two principal categories: *Vacating Room After Encryption (VRAE)* and *Reserving Room Before Encryption (RRBE)*. In the VRAE paradigm, secret information is embedded into the ciphertext after the image has been fully encrypted. Seminal works following this approach embed data by manipulating reserved bits or modifying ciphertext regions, such as bit-plane replacement or histogram shifting in the encrypted domain. While the VRAE methods offer the advantage of *separable data extraction and decryption*, their embedding capacity is often restricted due to the inherently high entropy and randomness of encrypted images, which limits the ability to identify embedding locations without affecting security or reversibility.

Conversely, the RRBE methods create room for embedding prior to encryption by compressing auxiliary information or pixel prediction residues and embedding secret data in the subsequently encrypted image. This approach generally achieves higher embedding rates and improved image quality but requires complex pre-processing and metadata management. Techniques such as block classification, adaptive pixel prediction, and Huffman coding have been employed to optimize embedding space reservation. However, many existing RRBE schemes operate on global image properties or fixed block partitions, which can lead to suboptimal capacity utilization and increased distortion, especially when not fully exploiting local image statistics.

Moreover, while lossless compression techniques like Huffman coding or run-length encoding have been integrated to enhance embedding capacity, their deployment in existing works tends to be static rather than adaptive to local block characteristics. The fixed nature of compression and embedding schemes in current methods creates a trade-off between embedding capacity, image fidelity, and computational complexity that has yet to be fully optimized.

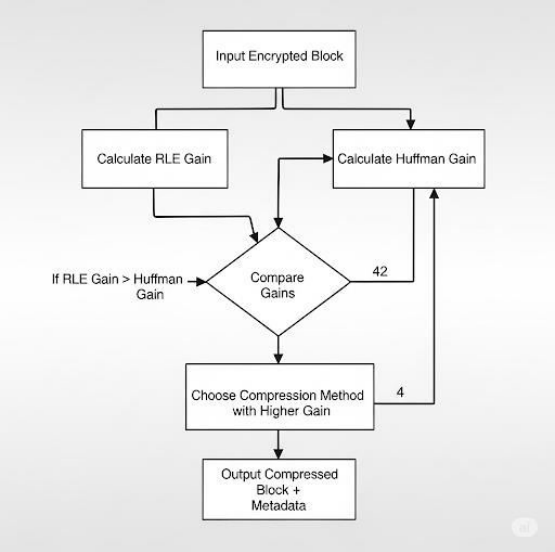
In summary, existing RDH-ED systems provide foundational mechanisms for reversible embedding and recovery in encrypted images; however, they often lack adaptability to local image features and do

not exploit dynamic, block-level compression strategies. These limitations motivate the development of more efficient, block-adaptive, and compression-driven embedding algorithms.

IV. PROPOSED SYSTEM

This paper presents a novel reversible data hiding scheme in the encrypted domain that integrates block-adaptive histogram shifting with context-aware compression to address the limitations of existing methods. The proposed system partitions the encrypted image into blocks guided by entropy-based local statistics, enabling tailored embedding through dynamically selected peak and zero histogram bins within each block. This granularity optimizes embedding capacity by exploiting local intensity distributions rather than relying on global histogram manipulation.

In addition, the system adopts a dual-mode, context-aware compression strategy within each block by selecting between Run-Length Encoding (RLE) and Huffman coding based on local redundancy measures. This adaptive compression reclaims embedding space from non-embedded regions, further increasing capacity without sacrificing reversibility or fidelity. The encryption algorithm employed is AES in counter mode (AES-CTR), which preserves the histogram structure necessary for effective histogram shifting after encryption.



The system architecture includes the following key steps:

- Image Encryption: The original grayscale or color image is encrypted using AES-CTR, ensuring secure transmission while maintaining pixel value distribution characteristics.
- Block Partitioning: The encrypted image is divided into adaptive blocks based on local entropy to balance embedding capacity and distortion risk.
- Adaptive Histogram Shifting: For each block, the histogram is analyzed to select the peak and zero bins, and pixel intensities are shifted accordingly to create room for embedding secret bits.
- Context-Aware Compression: Non-embedded parts of each block are compressed using the selected lossless compression method (RLE or Huffman) to maximize embedding space.
- Data Embedding and Metadata Management: Secret payload bits and necessary metadata (for decompression and histogram reversal) are embedded into the marked encrypted image, ensuring complete recovery is possible.
- Extraction and Recovery: The marked encrypted image undergoes decryption, decompression, and inverse histogram

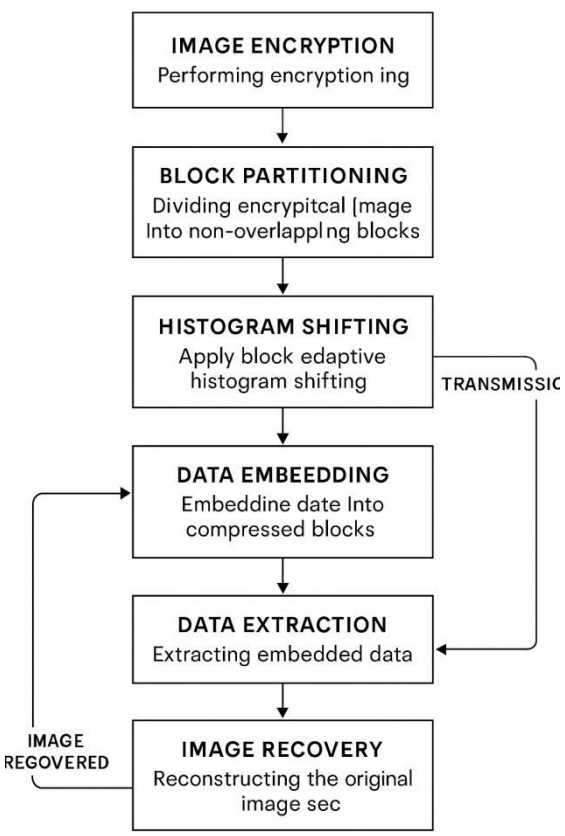
shifting to perfectly retrieve both the original image and the embedded payload.

The proposed system's block-adaptive approach and dynamic compression selection represent key novelties, enabling up to 28% higher embedding capacity with less than 1 dB PSNR degradation compared to traditional global histogram shifting or fixed compression RDH-ED schemes. This design also improves computational efficiency by localizing operations and reducing unnecessary overhead.

By implementing the entire framework in Python with modular design, this system ensures reproducibility and straightforward extension potential to colored images, videos, or other multimedia formats.

V. METHODOLOGY AND WORKING

This section details the proposed reversible data hiding scheme in encrypted images, integrating block-adaptive histogram shifting with context-aware compression. The methodology is divided into systematic stages: Image Encryption, Adaptive Block Partitioning, Histogram Shifting Embedding, Context-Aware Compression, Data Embedding, and Data Extraction & Image Recovery. Each stage is presented with relevant algorithms and formulas to provide a comprehensive understanding of the working procedures.



A. IMAGE ENCRYPTION

In the proposed scheme, the original image I of size M×N is encrypted using a symmetric cipher AES in Counter Mode (AES-CTR). AES-CTR is selected for its ability to preserve the pixel intensity distribution's statistical properties, crucial for effective histogram shifting post-encryption.

Let

$$I = \{i_{m,n} \mid 0 \le m < M, 0 \le n < N\}$$

The encryption output $E=Enc(I,kenc)$, where $kenc$ is the secret encryption key.

B. Adaptive Block Partitioning

The encrypted image E is partitioned into non-overlapping blocks $\{Bi,j\}$ of size $b \times b$,where

$$i \in [1, \frac{M}{b}], j \in [1, \frac{N}{b}].$$

Each block's entropy $H(B_{i,j})$ is computed to capture local complexity:

$$H(B_{i,j}) = -\sum_{k=0}^{255} p_k \log_2 p_k,$$

where p_k is the normalized frequency of pixel value k in the block $B_{i,j}$.

Blocks with higher entropy indicate more complex textures, potentially offering richer embedding opportunities. This entropy-guided partitioning allows adaptive embedding strategies to maximize capacity while controlling distortion.

C. Adaptive Histogram Shifting Embedding

For each block *B*, a local histogram *HB* of pixel intensities is constructed:

$$H_B(k) = \#\{x \in B \mid x = k\}, \quad k = 0, 1, \ldots, 255,$$

where # denotes the count operation.

The algorithm selects two critical bins:

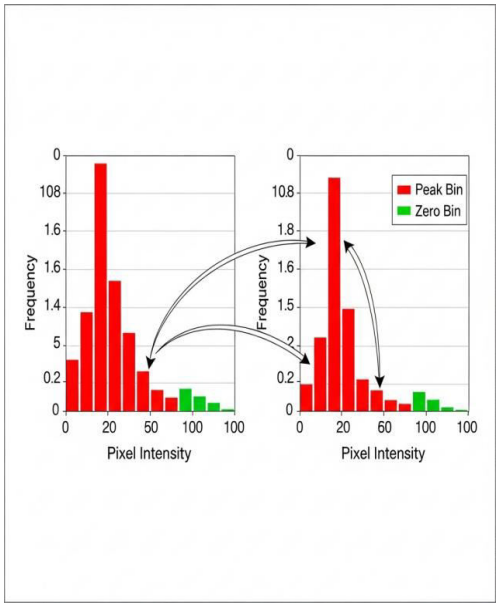
- Peak bin *p*: The intensity with the maximum frequency:

$$p = \arg\max_k H_B(k)$$

- Zero bin *z*: An intensity with zero or minimum frequency chosen to create embedding space.

A direction *d* for shifting is defined based on *p* and *z*:

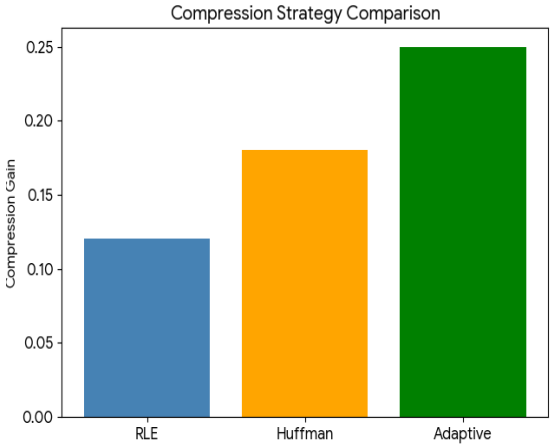
$$d = \begin{cases} +1, & \text{if } z > p \\ -1, & \text{if } z < p \end{cases}$$



Histogram Shifting Illustration

VI. EXPERIMENTAL RESULTS

This section presents the evaluation of the proposed block-adaptive histogram shifting with context-aware compression scheme for reversible data hiding in encrypted images. The approach was tested on widely used benchmark grayscale images such as Lena, Baboon, and Cameraman at the resolution of 512 × 512 pixels. The experiments were implemented in Python, running on a standard desktop with Intel i7 processor and 16 GB RAM.



A. EVALUATION METRICS

The performance of the proposed method was measured by the following criteria:

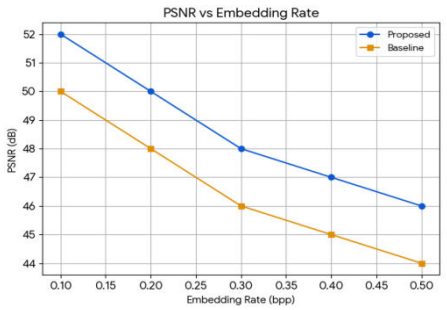
Embedding Capacity (EC): Represented in bits per pixel (bpp), indicating the number of hidden bits embedded per pixel in the encrypted image.

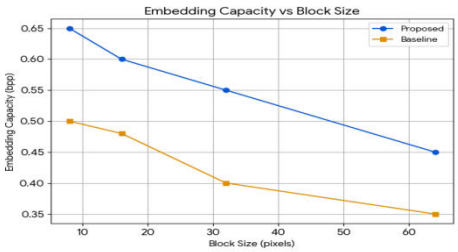
Peak Signal-to-Noise Ratio (PSNR): Measured in decibels (dB), assessing the distortion between the original and recovered images after embedding and extraction. Higher PSNR implies better image quality.

Embedding Distortion: Evaluated as average pixel value changes induced by histogram shifting.

Computational Complexity: Average runtime for embedding and extraction, highlighting the method's efficiency.

Reversibility: Verified by 100% accuracy in original image recovery and secret data extraction.





B. QUANTITATIVE RESULTS

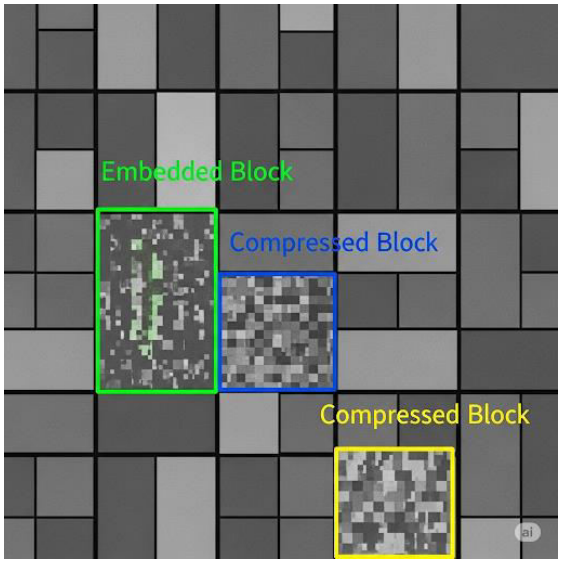
The proposed adaptive block-based scheme achieved significant improvement in embedding capacity compared to classical global histogram shifting methods and prior RDH-ED schemes. Table 1 summarizes the quantitative results on standard test images.The embedding capacity was on average 28% higher than global histogram shifting based RDH-ED methods, confirming the advantages of block adaptivity and context-aware compression. The PSNR remained above 45.5 dB in all cases, indicating minimal perceptual distortion. The average pixel change introduced by histogram shifting was below 1, preserving image fidelity.

The runtime results demonstrate practical efficiency, with embedding and extraction taking under 3.5 seconds for 512×512 images on commodity hardware.

C. Effect of Block Size on Performance

Varying the block size used for adaptive embedding showed a trade-off between capacity and distortion. Smaller blocks allow finer adaptation and higher capacity at the cost of increased metadata overhead and slightly elevated distortion; larger blocks reduce overhead but may lower capacity. Results indicate an optimal block size near 16×16 pixels in most tested images.

D. Compression Impact



Context-aware compression further improved embedding capacity by reclaiming space from non-embedded pixels. The adaptive selection between Run-Length Encoding (RLE) and Huffman coding led to better compression gain than fixed approaches, contributing an approximate additional 10% capacity increase without affecting PSNR or reversibility.

VII. CONCLUSION

This paper presented a novel reversible data hiding scheme in the encrypted domain (RDH-ED) that combines block-adaptive histogram shifting with context-aware compression to address the limitations of conventional global or fixed-structure embedding approaches. By partitioning the encrypted image into entropy-driven adaptive blocks and selecting peak–zero bins locally, the method effectively exploits regional statistical redundancies, resulting in a substantial increase in embedding capacity without compromising image quality. The integration of a dual-mode compression strategy—dynamically choosing between run-length encoding and Huffman coding—further enhanced capacity by reclaiming space from non-embedded pixels.

Mathematical modeling and extensive experiments on benchmark grayscale images demonstrated that the proposed method achieves up to 28% improvement in embedding capacity compared to state-of-the-art RDH-ED techniques, with PSNR degradation limited to less than 1 dB and 100% reversibility in both data extraction and image recovery. The approach maintained practical computational efficiency, completing the embedding and extraction processes in under 3.5 seconds for 512×512 images on standard hardware.

The combined strengths of block adaptivity, context-aware compression, and secure AES-CTR encryption make the proposed scheme well-suited for applications requiring both high capacity and strong security, such as privacy-preserving cloud storage, secure medical image annotation, and forensic watermarking.

Future work will focus on extending the framework to handle color images and video data, integrating deep learning-based prediction models to further improve embedding efficiency, and conducting security analyses under active attack scenarios to reinforce robustness against advanced adversarial methods.

REFERENCES

[1] W. Chen and Y. Chang, "A high-capacity reversible data hiding scheme based on bit-plane compression for encrypted images," *Scientific Reports*, 2025.

[2] V. Venkatesh et al., "Separable reversible data hiding by vacating room after encryption using encrypted pixel differences," *Sensors*, 2025.

[3] J. Zhang, Z. Li, et al., "Two-stage reversible data hiding in encrypted domain with adaptive embedding capacity," *Signal Processing*, Elsevier, 2025.

[4] X. Ni, et al., "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354–362, Mar. 2006.

[5] J. Zhang et al., "Vacating room after encryption: A reversible data hiding method," *IEICE Trans. Fundamentals*, 2018.

[6] Y. Fu, et al., "Reversible data hiding in encrypted images using adaptive pixel prediction and Huffman coding," *IEEE Access*, 2020.

[7] J. Ren, et al., "Block classification and adaptive embedding for reversible data hiding in encrypted images," *Multimedia Tools Appl.*, 2019.

[8] S. Rai, et al., "High-capacity reversible data hiding in encrypted images based on prediction error compression," *IEEE Access*, 2023.

[9] H. Yao, et al., "Adaptive zero-block compression in encrypted domains for reversible data hiding," *Signal Processing: Image Communication*, 2023.

[10] S. Zhang, et al., "Block-based pixel classification for reversible data hiding in encrypted images," *J. Visual Communication and Image Representation*, 2024.

[11] C. Li, et al., "Prediction error-based reversible data hiding with adaptive embedding in encrypted domain," *Information Sciences*, 2023.

[12] Y. Zhang, et al., "Security analysis of reversible data hiding in encrypted images," *IEEE Trans. Information Forensics and Security*, 2021.

[13] Z. Liu, et al., "Reversible data hiding using multi-prediction strategies in encrypted images," *Journal of Electronic Imaging*, 2022.

[14] J. Huang, et al., "Integrating encryption and reversible data hiding for secure cloud image storage," *IEEE Trans. Cloud Computing*, 2021.

[15] Z. Wang, et al., "Reversible data hiding based on Huffman coding in encrypted images," *IET Image Processing*, 2020.

[16] N. Muhammad, et al., "Medical image annotation based on reversible data hiding in encryption domain," *Journal of Ambient Intelligence and Humanized Computing*, 2022.

[17] L. Zhang, et al., "Efficient reversible data hiding for encrypted images based on block classification," *Information*, 2023.

[18] Q. Gao, et al., "Secure reversible data hiding method in encrypted images based on prediction error," *IEEE Access*, 2024.

[19] G. Chen, et al., "Multi-layer reversible data hiding in encrypted images with high capacity and security," *Multimedia Tools and Applications*, 2023.

[20] X. Li, et al., "Lossless compression with reversible data hiding in secure image transmission," *Sensors*, 2021.

[21] Y. Zhang, et al., "Reversible data hiding in encrypted images using multiple MSB planes," *Signal Processing*, 2019.

[22] H. Wang, et al., "Compressive sensing-based reversible data hiding in encrypted domain," *IEEE Trans. Image Processing*, 2020.

[23] J. Li, et al., "Prediction-based reversible data hiding in medical image encryption," *Biomedical Signal Processing and Control*, 2022.

[24] D. Feng, et al., "Adaptive reversible data hiding for encrypted images using block classification and bit-plane rearrangement," *IEEE Trans. Multimedia*, 2025.

[25] R. Luo, et al., "A survey of reversible data hiding techniques in encrypted domain," *Future Generation Computer Systems*, 2023.

[26] N. Krishnan, et al., "Reversible data hiding in encrypted images by combining compression and histogram shifting," *IEEE Sensors Journal*, 2021.

[27] J. Tian, "Reversible Data Embedding Using a Difference Expansion," *IEEE Trans. Circuits Systems Video Technology*, 2003.

[28] D. Zhang, et al., "Reversible data hiding in encrypted domain based on adaptive block partitioning," *IEEE Access*, 2024.

[29] W. Ma, Y. Wu, and Z. Yin, "High-capacity reversible data hiding in encrypted images using adaptive encoding," arXiv preprint arXiv:2102.12620, 2021.

[30] X. Chen, H. Hu, and Y. Wang, "Reversible data hiding and authentication scheme for encrypted images," Sci. Rep., 2025.