International Journal of Advanced Computer Technology
ISSN: 2319-7900 www.ijact.org Volume 14, Issue 2, April 2025

Enhanced Reversible Data Hiding for Encrypted Image Based on Block Mean Difference Histogram Shifting and BPHST

Jigisha Mehra, Amit Jha, Kamini Maheshwar
Computer Science and Engineering Department
University Institute of Technology, Barkatullah University, Bhopal (M.P.), India
mehrajigisha@gmail.com, amitkumarjha40@gmail.com, kaminimaheshwar@gmail.com

Abstract - This paper proposes an improved reversible data hiding method for encrypted images, utilizing Block Prediction Histogram Shifting Technique (BPHST). Reversible data hiding (RDH) ensures both secure data embedding and complete recovery of the original image post-extraction. Our proposed BPHST approach is based on bit-level shifting and histogram manipulation of block mean differences within encrypted image segments. The method extracts the mean difference from encrypted blocks and constructs a histogram using additive homomorphic properties, allowing precise data embedding via histogram shifting. This technique ensures that data extraction is separable from image decryption by preserving the difference prediction before and after encryption. Compared to previous methods relying on sorting, prediction, and histogram adjustment, BPHST achieves better error rate management, enhanced robustness, and secure data embedding. The proposed method effectively balances high data security, imperceptibility, and reversibility, making it suitable for sensitive multimedia applications. Furthermore, BPHST demonstrates improved Peak Signal-to-Noise Ratio (PSNR) and lower Mean Squared Error (MSE), ensuring high fidelity in image recovery. This makes BPHST a promising technique for secure, reversible information hiding in encrypted images.

Keywords: - Reversible Data Hiding (RDH), Encrypted Image, Histogram Shifting, Block Mean Difference, Bit Pattern Shifting Technique (BPHST), Image Recovery.

I. INTRODUCTION

Reversible processes involving information storage and secure data hiding in images refer to strategies that conceal information within digital images, followed by anonymous communication. It is a method of embedding additional messages into cover media with a reversible approach, such that the original image and the hidden content can be fully recovered after data extraction. Traditionally, image data hiding has been used for secret communication. In certain important applications, the embedded carriers or images are further encrypted to prevent the carrier or image from being analysed and revealing the presence of embedded data. Other applications arise when the owner of the carrier image does not want any third party, including the data hiding, to be aware of the image content before data hiding is performed, as in the case of military or confidential medical images.

A growing amount of confidential data is being stored on cloud servers for efficient processing, owing to the development of cloud computing technology. However, this trend also introduces concerns about data privacy and security. To ensure the confidentiality of sensitive images, it is

now common for users to encrypt images before uploading them to the server. However, processing encrypted images places constraints on the server's capabilities. To address the challenge of authenticating and managing encrypted images on the cloud server, the technique of Reversible Data Hiding in Encrypted Images (RDHEI) has been proposed, which enables data to be hidden and extracted losslessly from encrypted images.

Data hiding is now considered a promising method for ensuring data security within the broader vision of responsible AI. Typically, it involves concealing information in a particular form within another type of media. It can take various forms, such as embedding confidential information into a text file or inserting audio signals into digital images. As digital assets become increasingly diverse and widespread, the significance and applications of data hiding are expected to expand continuously [1].

In today's digital age, with the increasing prevalence of digital communication and multimedia data, data hiding has become critically important. Ensuring responsible AI, such as machine learning as a service, requires secure communication across all channels, and the accountability of responsible AI (e.g., digital intellectual property) requires protection against misuse and theft. Conventionally, data-hiding techniques are divided into three categories: watermarking, steganography, and cryptography [2].

Data hiding is the art and science of embedding secret information into appropriate multimedia carriers such as images, audio, and video. Digital steganography and watermarking are two major types of data hiding. Reversible data hiding can be defined as an approach where data is hidden in a host medium, such as a cover image, in such a way that the original content can be fully recovered after the data is extracted. Reversible data embedding, also known as lossless data embedding, involves embedding invisible data (called the payload) into a digital image in a way that allows complete recovery of the original image. A basic requirement for such techniques is that the quality degradation of the image after data embedding should be minimal. One of the most attractive features of reversible data embedding is its reversibility, i.e., the ability to remove the embedded data and restore the original image completely. Data hiding techniques embed information into cover media such as audio, image, and video files and are used in applications like copyright protection, media annotation, integrity verification, and covert communication. Most data-hiding approaches modify only the least significant portions of the cover media, such as the least significant bits of an image, to generate a marked version that retains perceptual transparency. However, this typically introduces permanent distortion to the original content, making it unrecoverable. In sensitive applications such as medical imaging, military operations, and legal forensics, any degradation of the original image is unacceptable. Therefore, a specialised category known as reversible data hiding (RDH) or lossless data hiding is required, which allows the original image to be fully restored after the embedded message is extracted. The block diagram of RDH illustrates how reversible steganography or watermarking techniques can retrieve the original carrier with no distortion or only negligible distortion after the hidden data has been extracted. Consequently, reversible data hiding is gaining popularity. As shown in Fig. 1.1, reversible data hiding is founded on the requirement that image quality degradation after data embedding must remain low. Its key advantage is the ability to restore the image to its pristine form after data removal. From an

information-hiding perspective, reversible data embedding involves concealing information in a digital image so that an authorised entity can both decode the embedded data and restore the original image. An information-hiding system is typically characterised by four aspects: capacity, security, perceptibility, and robustness [3].

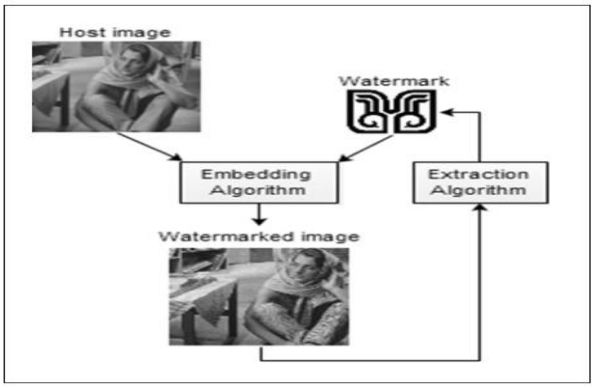

Fig.1: RIEDH in process

II. RELATED WORK

Reversible data hiding has been actively studied over the past few years. Several important techniques are discussed here. This section aims to classify existing Reversible Data Hiding in Encrypted Images (RDHEI) techniques based on the underlying image processing mechanisms. J. Huang et al. [7] observed that conventional algorithms for embedding secret data in the clear domain are not applicable in the encrypted domain [37]. Traditional encryption methods fail to preserve pixel correlation without compromising security. The authors introduced a new encryption strategy allowing conventional data-hiding algorithms originally designed for unencrypted images to be applied to encrypted images. In this method, the original image is divided into non-overlapping blocks. Within each block, all pixels are encrypted using an XOR operation with a pseudo-randomly generated byte, and the blocks are then pseudo-randomly permuted. Notably, pixels within each block are not scrambled. Only the order of blocks changes. This approach preserves the statistical properties of the original image, particularly the histogram of pixel differences or prediction errors, making it feasible to apply conventional data-hiding algorithms in the encrypted domain. However, the embedding capacity remains limited due to underflow/overflow handling. Yan Chen et al. [8] proposed a novel RDHEI method using a single-level embedding approach involving three parties: an image owner, a data hider, and a recipient. The image owner encrypts the original image into ciphertext by dividing it into blocks, pseudo-randomly permuting them with a permutation key, and then encrypting each block's content using a stream cipher (where pixels share the same stream bytes). Once the encrypted image is uploaded to the server, the data hider embeds additional messages by selecting peak pixels from each block using an embedding key and applying histogram shifting. At the recipient's side, the hidden message can be extracted using the embedding key, while the original image can be losslessly recovered using both the permutation and encryption keys. They further extended this into a multi-level approach, where iterative embedding creates marked encrypted images. Compared to existing methods, their approach provides better embedding efficiency and error-free recovery. Yanping Xiang et al. [9] introduced a separable RDH scheme based on Pixel Value Ordering (PVO) in the encrypted domain. The image is encrypted using homomorphic encryption by the content owner, and the secret data is embedded in each block using PVO. Additive homomorphism ensures that performance in the encrypted domain closely matches that in the plaintext domain. The encryption does not cause data expansion, which improves the payload. Depending on the available keys, as with the data hiding key only, the receiver can extract the hidden data. With only the encryption key, a decrypted image resembling the original can be recovered. With both keys, the

original image and the embedded data can be perfectly restored. Ranging Wang et al. [10] emphasised the need for secure image processing in cloud environments, where encrypted image storage is standard. For content annotation or tamper detection, additional data must be embedded directly in encrypted images. They proposed a separable and error-free RDH scheme utilising interpolation. Sample pixels are encrypted using a stream cipher, and a specific mode is designed to encrypt the interpolation error of non-sample pixels. The data hider embeds information into the interpolation error using modified histogram shifting and different expansion techniques without knowing the original content. Their scheme supports both encrypted-domain and decrypted-domain data extraction and ensures real reversibility. Experiments confirmed their feasibility and efficiency. Jiang-Yi et al. [11] designed a Bit-Plane Block Embedding (BPBE) algorithm to embed messages in binary images and later extended it to encrypted images. The method embeds parts of the Least Significant Bit (LSB) planes into the Most Significant Bit (MSB) planes before encryption. This reserves room for data embedding into the LSBs post-encryption. If only the data hiding key is available, the receiver can extract the hidden data; with only the encryption key, the original image can be reconstructed; and with both keys, perfect data extraction and image recovery are achieved. Experimental results showed a higher embedding rate compared to other methods while maintaining acceptable image quality. W. H. Tsai et al. [12] proposed an image transformation method that selects a target image similar to the secret image and replaces each block in the target with a similar block from the secret image. A mapping between secret and target blocks is embedded to form an encrypted version of the secret image. A greedy search is used to find the most similar blocks. However, the method's effectiveness is limited to scenarios where the target image is visually similar to the secret image, and the visual quality of the encrypted image remains suboptimal. Y. L. Lee et al. [13] improved Tsai's method by enabling the transformation of the secret image into a randomly selected target image, removing the need for a similar image database. In this method, each block of the secret image is transformed using a reversible colour transformation, and recovery parameters (e.g., indexes, parameters) are added to the transformed blocks to generate the encrypted image. Although this improves encrypted image quality, the transformation is not fully reversible, meaning the original image cannot be losslessly reconstructed. Xianquan Zhang et al. [14] addressed payload limitations in RDHEI methods by proposing a technique based on hierarchical embedding. Their contributions include a hierarchical label map generation strategy for bit-planes in plaintext images using prediction techniques. The label map is compressed and embedded into the encrypted image. A hierarchical embedding mechanism categorising prediction errors into small-, medium-, and large-magnitude types. Unlike traditional approaches, secret bits are embedded even in large-magnitude errors, significantly increasing the payload. Experiments on benchmark datasets showed the method provides high image quality and a superior embedding rate. W. Zhang et al. [15] were the first to propose a Reverse Room Before Encryption (RRBE) method, diverging from previous RDHEI techniques. The original image is divided into blocks. Pixel correlation is evaluated using a fluctuation function, and blocks are classified into Group A (textured) and Group B (smooth). Group A blocks are placed at the beginning of the image, followed by Group B. To reserve space for secret embedding, the LSB plane of Group A is embedded into pixels of Group B using histogram shifting. The resulting image is encrypted using a stream cipher, and the number of embeddable pixels is stored in

the first few LSBs. The actual embedding is performed by substituting the LSBs of pixels in Group A. Up to three LSBs per pixel can be used. Xin Wu et al. [16] proposed a novel RDHEI method based on block mean difference histogram shifting. The data owner partitions the cover image into non-overlapping 2×2 blocks and computes the block mean difference. These values are then encrypted using the Paillier cryptosystem, exploiting its additive homomorphic property to bind the block mean difference to each encrypted block. During embedding, the data hider calculates block mean differences in histograms and uses histogram shifting to embed the data, resulting in a marked encrypted image. Thanks to Paillier's properties, the receiver can extract the hidden data and reconstruct the original image from either the encrypted or decrypted domain. Experiments confirm that the proposed method achieves high image quality and superior PSNR and embedding rate compared to existing techniques.

III. BACKGROUND ON REVERSIBLE DATA HIDING METHODS (RDHM)

Reversible data hiding has existed for several years. Researchers have proposed various methods for reversible data hiding. The following are different techniques that have been introduced over the years. Circular Visual Cryptography was introduced in 2005. In this scheme, a circular shadow image can hide two or more confidential datasets in circular images and display them in both the inner and outer regions of the circular images. However, it can only produce a circular shadow image without the central part, resulting in low resolution in the inner portion, as shown in Figure 4. It encrypts data into two ringed shadow images, allowing two confidential datasets to be hidden simultaneously.

1. Histogram Block Shift-Based Technique.

Histogram-shifting-based reversible data hiding schemes embed data by shifting the histogram in a fixed direction. There are two key points in these schemes: the peak point and the zero point. The peak point corresponds to the grayscale value with the maximum number of pixels in the histogram of the given image. The zero point is typically a grayscale value where the pixel count is zero. The zero point with the fewest number of pixels is selected to increase the embedding capacity. In histogram-shifting algorithms, the pixels between the peak and zero pairs are modified during the embedding process. The pixel at the peak point is used to carry a bit of the secret message, while other pixels are adjusted without embedding secret data. The data hiding capacity of the histogram-shifting technique equals the number of pixels at the peak points. The larger the number of pixels at the peak point, the higher the hiding capacity. Multiple peaks and zero-point pairs can be used to increase capacity. However, it is often difficult to find multiple pairs, as zero points are not always available [6].

2. Difference Expansion (DE)-Based Technique.

Tian proposed the difference expansion (DE) technique for reversible data hiding [2]. In the DE technique, extra storage space is obtained by utilising the redundancy in image content. The DE method is used to embed a payload into digital images reversibly. Both the payload capacity and the visual quality of the embedded images produced by the DE method are among the best in the literature, along with low computational complexity [5].

3. Least Significant Bit Modification-Based Technique.

One of the earliest methods is the LSB (Least Significant Bit) modification technique. In this well-known method, the LSB of each signal sample is overwritten by a secret data bit. During extraction,

these bits are read in the same scanning order, and the secret data is reconstructed [4].

IV. PROPOSED METHODOLOGY

The proposed methodology introduces an enhanced reversible data hiding technique for encrypted images by integrating Block Mean Difference Histogram Shifting (BMDHST) with a novel Bit Pattern Histogram Shifting Technique (BPHST). This approach is aimed at increasing embedding capacity, reducing image distortion, and ensuring the complete recovery of both embedded data and the original image without loss. The process begins with image encryption, where the original image is partitioned into non-overlapping 2×2 blocks. For each block, the mean intensity value is calculated to capture block-wise pixel distribution. Encryption is then applied using a block-wise XOR operation with a pseudo-random key, ensuring both confidentiality and compatibility with histogram-based embedding techniques. Next, the block means difference calculation stage computes the difference between each pixel and its corresponding block mean. These values form a Block Mean Difference Histogram, which is used as the primary embedding domain.

The histogram construction and shifting phase analyse this histogram to identify peak points (values with the highest frequency) and zero points (values with minimal or zero frequency). These points guide the embedding of secret bits. Each bit of the message is embedded by modifying pixels corresponding to the peak point, while surrounding values are adjusted to maintain reversibility and data integrity. To further improve embedding efficiency and robustness, the Bit Pattern Histogram Shifting Technique (BPHST) is introduced. Unlike conventional histogram shifting methods, BPHST exploits the internal bit pattern distribution within each block. This strategy allows the identification of optimal embedding positions while preserving the pixel prediction error distribution. It also leverages the repetitive structure of specific bit patterns, thereby enabling higher embedding payloads without significant visual distortion. The modified encrypted image, known as the marked image, retains its statistical properties, facilitating reversible data extraction. During the data extraction and image recovery stage, the recipient utilises the embedding key to identify and reverse the histogram modifications. The encryption key is then used to decrypt the image blocks, after which the original pixel values are reconstructed using inverse block mean operations. This ensures the lossless retrieval of both the embedded message and the original image. The proposed BPHST method offers several distinct advantages. It achieves a high Peak Signal-to-Noise Ratio (PSNR) by minimising pixel alterations, and it results in low Mean Squared Error (MSE) due to localised histogram shifts.

Additionally, it enhances robustness, making the system resilient to noise and manipulation. The separable architecture of the scheme allows for flexible access control, enabling data extraction or image recovery depending on the availability of keys. Overall, this methodology successfully combines the strengths of statistical and pattern-based embedding in the encrypted domain, making it applicable to secure scenarios such as medical image storage, military communications, and encrypted cloud data management.

V. EXPERIMENTAL SETUP AND SIMULATION TOOL

To evaluate and compare the proposed BPHST-based reversible data hiding technique with existing methods such as BMDHST, a series of experiments were conducted in a controlled simulation environment. The experimental setup was implemented using MATLAB Version 14 (R2008a) on a system configured with an Intel Dual-Core processor, 80 GB hard disk, and Windows 7 Ultimate operating system. MATLAB

was chosen due to its robust numerical computing capabilities, efficient matrix operations, and high-level programming features that are well-suited for image processing tasks. The Just-In-Time (JIT) compilation technology of MATLAB ensures optimised execution speeds comparable to conventional programming languages. It also provides multi-threaded support for linear algebra and numerical functions, thereby leveraging multi-core and multiprocessor systems to accelerate computation. The simulations were carried out using a variety of test images, including colour (RGB), grayscale, and binary formats, across commonly used file types such as JPG and PNG. The proposed technique was tested for key performance metrics such as Peak Signal-to-Noise Ratio (PSNR) and Mean Squared Error (MSE), both of which are critical for assessing image quality and distortion after embedding. The MATLAB environment enabled the design, implementation, visualisation, and debugging of the reversible data-hiding algorithms. It provided built-in functions for tasks such as histogram analysis, block processing, and statistical computation, which were extensively utilised during experimentation.

Table 1: Result Analysis of PSNR and MSE on Operation Sindoor Image

Technique	MSE (dB)	PSNR (dB)
BMDHST	0.0893	25.4376
BPHST	0.0059	52.5671

Additionally, MATLAB facilitated a graphical representation of results through histogram plots, PSNR/MSE comparison graphs, and detailed tabulated results. The use of MATLAB also allowed seamless integration with Simulink for potential future extensions involving neural networks or real-time data flow simulation. Overall, the MATLAB platform offered a comprehensive and flexible environment for testing the performance, accuracy, and robustness of the proposed reversible data-hiding methodology in encrypted images.

VI. RESULTS AND PERFORMANCE ANALYSIS

The effectiveness of the proposed Bit Pattern Histogram Shifting Technique (BPHST) was evaluated through a series of experiments conducted on several types of images and compared against traditional methods, particularly the Block Mean Difference Histogram Shifting Technique (BMDHST). The performance was assessed based on two standard metrics in image quality analysis: Peak Signal-to-Noise Ratio (PSNR) and Mean Squared Error (MSE). PSNR provides a measure of the peak error and is inversely proportional to the logarithmic scale of the MSE. A higher PSNR value indicates better image quality, while a lower MSE suggests reduced distortion during the data embedding and recovery process. In the first set of experiments, the “Operation Sindoor” image and its corresponding “OS-Logo” variant were utilised to evaluate the performance of the proposed method. Both images were analysed in terms of their histograms and pixel integrity post-embedding. The proposed BPHST technique demonstrated superior results by achieving a PSNR of 52.5671 dB and an MSE of only 0.0059, as compared to the BMDHST method, which yielded a PSNR of 25.4376 dB and an MSE of 0.0893. These findings are summarised in Table 1.

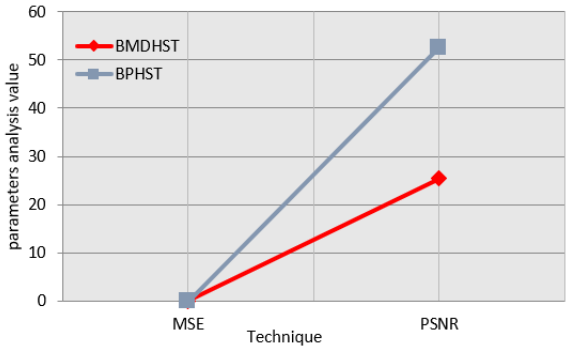

Fig. 2 Comparison between BMDHST and BPHST on operation Sindoor

These results confirm that the BPHST method introduces minimal distortion during the embedding process, making it suitable for applications requiring high visual fidelity. The histogram analysis also confirmed that the proposed method maintains the statistical distribution of the image more effectively than existing techniques, which is essential for achieving reversible data hiding in the encrypted domain.

In addition to the Operation Sindoor image, another test case involving the "BrahMos Missile" image and the "BrahMos Logo" image was carried out. Similar to the previous analysis, the main parameters under consideration were PSNR and MSE, along with the image formats (e.g., JPG, PNG) and colour types (RGB, grayscale, and binary).

Table 2: Result Analysis of PSNR and MSE on BrahMos Missile Image

Technique	MSE (dB)	PSNR (dB)
BMDHST	0.0258	36.4984
ARDIEM	0.0011	67.9248

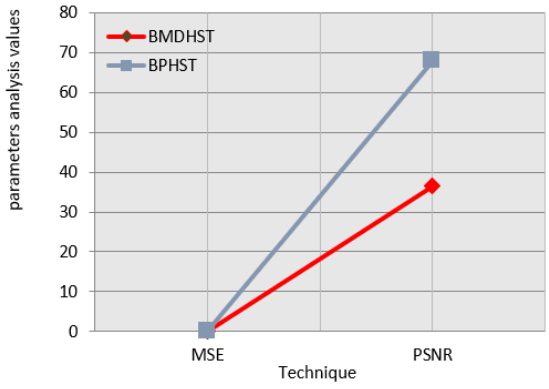

Fig. 3 Comparison between BMDHST and BPHST on Brahmos missile image

The results obtained from this experiment further validated the robustness and efficiency of the proposed technique. The BPHST-based method, referred to in the results as ARDIEM (Advanced Reversible Data Hiding using Encrypted Mechanism), achieved an exceptionally high PSNR of 67.9248 dB and a remarkably low MSE of 0.0011. In contrast, the BMDHST method recorded a PSNR of 36.4984 dB with an MSE of 0.0258. These comparative values are reported in Table 2. These findings clearly highlight the advantages of incorporating bit-pattern-based analysis and adaptive histogram shifting to preserve image quality while enhancing embedding capacity.

The graphical analysis, as represented in Figures 2 and 3, further underscores the substantial improvements introduced by BPHST over traditional histogram-based methods. In both the Operation Sindoor and BrahMos Missile image evaluations, BPHST consistently outperformed the baseline BMDHST technique. The improvement in PSNR indicates that the embedded images are visually closer to the original ones. At the same time, the significant reduction in MSE implies that pixel-level modifications are minimal and precisely controlled. This is crucial in applications like medical imaging or military communication, where even minor alterations in image content could result in critical misinterpretations. One of the standout features of the BPHST methodology is its ability to exploit repetitive bit patterns within image blocks. By leveraging the frequency of predictable patterns, the embedding strategy minimises abrupt changes in pixel values, which are the primary contributors to perceptual degradation in steganographic and watermarking techniques. Furthermore, the localised histogram shifting approach used in BPHST ensures that changes are confined to targeted regions, enhancing both the robustness and reversibility of the method.

Overall, the results from the experimental evaluations confirm that the proposed BPHST-based reversible data hiding scheme significantly improves upon existing techniques in terms of embedding efficiency, image quality preservation,

and data security. With higher PSNR and lower MSE across multiple image formats and content types, BPHST proves to be a highly effective technique for secure and reversible data embedding in encrypted images, making it especially valuable in cloud storage, sensitive surveillance, and secure communication environments.

V. CONCLUSION AND FUTURE WORK

An improved reversible data hiding technique for encrypted images has been proposed based on Block Mean Difference Histogram Shifting (BMDHST) and the novel Bit Pattern Histogram Shifting Technique (BPHST). Reversible data hiding (RDH) in encrypted images is essential for ensuring data confidentiality, especially in sensitive domains such as medical imaging and military communication. The proposed strategy (BPHST) leverages bit pattern-based histogram shifting to enhance embedding capacity, improve visual quality, and ensure complete recovery of both the original image and embedded data. This paper has explored and compared various RDH techniques, including Least Significant Bit (LSB) substitution, Difference Expansion (DE), and Histogram Modification. However, the primary focus lies in the comparative analysis between BPHST and traditional BMDHST methods. While all methods offer certain advantages and disadvantages, the proposed BPHST demonstrates superior performance in terms of payload capacity, robustness, and minimal degradation of image quality. Techniques based purely on histogram shifting often suffer from image clarity loss, inefficient data compression, and issues in the decoding process.

In contrast, BPHST enables a reversible transformation of the encrypted image by embedding data with minimal distortion, ensuring high visual quality and secure information retrieval. Our approach supports the concept of reversible image transformation, allowing a secret image to be encrypted into a visually distinct but statistically consistent image. This ensures that the hidden content remains protected and the original image can be restored without any loss. The proposed BPHST method is particularly effective because it integrates block-wise analysis and pattern-based data embedding while preserving image integrity through histogram-controlled shifts. The research confirms the feasibility and utility of executing RDH in encrypted images. This field holds substantial promise for enhancing digital security, especially where trade-offs between embedding capacity, reconstructed image quality, and data robustness must be optimised. The study also explores encryption strategies where the data hider may not have access to the original image content, yet can embed secret information reliably by modifying selected portions of the encrypted data. Experimental results confirm that the BPHST method achieves a high Peak Signal-to-Noise Ratio (PSNR), low Mean Squared Error (MSE), and enhanced robustness and security of the encrypted image. These outcomes affirm the reliability and effectiveness of the proposed methodology. The entire implementation has been successfully simulated using the MATLAB environment, demonstrating its practicality for real-world deployment. In the future, the proposed method can be extended to support colour image encryption, real-time video frames, and optimised embedding for cloud-based secure data storage. Further improvements may include adaptive thresholding for block selection, integration with deep learning-based prediction models, and application in blockchain-secured communication systems.

REFERENCES

[1]. I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, Digital watermarking and steganography. Morgan Kaufmann, 2007.

[2]. W. Bender, W. Butera, D. Gruhl, R. Hwang, F. J. Paiz, and S. Pogreb, "Applications for data hiding," IBM Systems Journal, vol. 39, no. 3.4, pp. 547–568, 2000.

[3]. Huang, Fangjun, Jiwu Huang, and Yun-Qing Shi. "New framework for reversible data hiding in the encrypted domain." IEEE Transactions on Information Forensics and Security 11, no. 12: 2777-2789, 2016.

[4]. Chandramouli, Rajarathnam, and Nasir Memon. "Analysis of LSB-based image steganography techniques." In Proceedings 2001 international conference on image processing (Cat. No. 01CH37205), vol. 3, pp. 1019-1022. IEEE, 2001.

[5]. Varsaki, Eleni, Vassilis Fotopoulos, and A. N. Skodras. "A reversible data hiding technique embedded in the image histogram." Hellenic Open University Journal of Informatics 1, no. 2, 2006.

[6]. Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Transactions on Circuits and Systems Video Technology, Vol. 16, No.3, 2006, pp. 354–362.

[7]. Huang, F. Huang, Y.-Q. Shi, New framework for reversible data hiding in the encrypted domain, IEEE Transactions on Information Forensics and Security 11, 2777–2789, 2016.

[8]. Ge, Haoli, Yan Chen, Zhenxing Qian, and Jianjun Wang. "A high-capacity multi-level approach for reversible data hiding in encrypted images." IEEE Transactions on Circuits and Systems for Video Technology 29, no. 8: 2285-2295, 2018.

[9]. Xiao, Di, Yanping Xiang, Hongying Zheng, and Yong Wang. "Separable reversible data hiding in encrypted image based on pixel value ordering and additive homomorphism." Journal of Visual Communication and Image Representation 45: 1-10, 2017.

[10]. Xu, Dawen, and Rangding Wang. "Separable and error-free reversible data hiding in encrypted images." Signal Processing 123: 9-21, 2016.

[11]. Lin, Jiang-Yi, Yu Chen, Chin-Chen Chang, and Yu-Chen Hu. "Reversible Data Hiding in Encrypted Images Based on Bit-plane Block Embedding." J. Inf. Hiding Multim. Signal Process. 10, no. 2: 408-421, 2019.

[12]. I.-J. Lai and W.-H. Tsai, "Secret-fragment-visible mosaic image–a new computer art and its application to information hiding," IEEE Trans. Information Forensics and Security, vol. 6, no. 3, pp. 936–945, 2011.

[13]. Y. L. Lee and W.-H. Tsai, "A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible colour transformations," IEEE Trans. Circuits Syst. & Video Technol., vol. 24, no. 4, pp. 695–703, 2014.

[14]. Yu, Chunqiang, Xianquan Zhang, Xinpeng Zhang, Guoxiang Li, and Zhenjun Tang. "Reversible data hiding with hierarchical embedding for encrypted images." IEEE Transactions on Circuits and Systems for Video Technology 32, no. 2: 451-466, 2021.

[15]. K. Ma, W. Zhang, X. Zhao, N. Yu, F. Li, Reversible data hiding in encrypted images by reserving room before encryption, IEEE Transactions on Information Forensics and Security 8, 553–562, 2013.

[16]. Wu, Xin. "Reversible Data Hiding for Encrypted Image Based on Block Mean Difference Histogram Shifting." In 2024 4th International Conference on Neural Networks, Information and Communication (NNICE), pp. 320-324. IEEE, 2024.

[17]. Chen, Kaimeng, Chin-Chen Chang, and C. C. Chang. "High-capacity reversible data hiding in encrypted images based on two-phase histogram shifting." Mathematical

Biosciences and Engineering 16, no. 5: 3947-3964, 2019.

[18]. Mohammadi, Ammar, and Mohammad Ali Akhaee. “Reversible data hiding in encrypted images using histogram modification and MSBs integration.” Multimedia Tools and Applications 83, no. 2: 5229-5249, 2024.

[19]. Xu, D., Chen, K., Wang, R., & Su, S. (2018). Separable reversible data hiding in encrypted images based on two-dimensional histogram modification. Security and Communication Networks, (1), 1734961, 2018.

[20]. Tang, Zhenjun, Shijie Xu, Dengpan Ye, Jinyan Wang, Xianquan Zhang, and Chuanqiang Yu. “Real-time reversible data hiding with shifting block histogram of pixel differences in encrypted image.” Journal of Real-Time Image Processing 16: 709-724, 2019.