

ORIGINAL RESEARCH

Open access

A Reversible Data Hiding Scheme for Secure Transmission of Encrypted DICOM Images

Kenji Tanaka^{1*}, Yui Kobayashi¹, Takeshi Nakamura²

Abstract

Modern technological innovations and breakthroughs in the medical sector have significantly enhanced life expectancy. While smart healthcare systems are currently being transformed by artificial intelligence (AI) and the Internet of Things (IoT), the confidentiality and security of medical data continue to be a critical challenge. Reversible data hiding (RDH) is extensively investigated within medical environments to facilitate secure information transmission, as well as in fields such as cloud computing and satellite imagery transfer. The transmission of medical images serves as a cornerstone of the smart healthcare industry.

For clinical images, even a marginal distortion during reconstruction can result in diagnostic errors by physicians, thereby endangering patient safety. Consequently, while numerous RDH methods have been developed, a limited number focus specifically on clinical imagery, particularly regarding high-quality DICOM formats.

The introduced AdaBPE RDH framework provides a robust solution for securely sharing patient health reports (PHRs) and other confidential data with medical professionals. This strategy introduces a methodology that establishes an optimal balance between leveraging smooth pixels for maximized intra-block data embedding and ensuring lossless image reconstruction. Within this framework, an encrypted 16-bit DICOM image serves as the host medium to conceal the patient's confidential data. The algorithm divides the cover image into equally sized, non-overlapping blocks, adaptively embedding data into these encrypted sections based on the underlying characteristics of the original pixel values via an MSB prediction error approach.

Performance evaluation is conducted using both 16-bit DICOM and 8-bit natural images. The proposed method successfully meets the core RDH benchmarks of BER = 0, PSNR = ∞ , and SSIM = 1, yielding an average embedding capacity of 5.7067 bpp for premium medical images and 1.6769 bpp for natural scenes. The empirical findings demonstrate substantial advantages, outperforming existing state-of-the-art approaches.

Keywords Reversible Data Hiding (RDH), Medical image security, 16-bit DICOM images, AdaBPE

*Correspondence:

Kenji Tanaka
tanaka.kenji@med.u-tokyo.ac.jp

¹ Department of Medical Image Security and Cryptography, Faculty of Medicine, University of Tokyo, Tokyo, Japan

² Department of Reversible Data Hiding and Telemedicine, Faculty of Medicine, Kyoto University, Kyoto, Japan

Introduction

In recent times, there has been a dramatic escalation in the adoption of e-health and telehealth applications, primarily driven by the Coronavirus disease (COVID-19) crisis. As face-to-face interactions became unfeasible during the pandemic, digital communication infrastructures emerged as vital alternatives, offering crucial support to healthcare

providers, pharmaceutical entities, and patients alike. Virtual communication platforms such as WhatsApp Messenger, Zoom, Google Meet, and Skype became the primary substitutes for direct consultations with medical experts. While these tools offer dependable connectivity, clinical efficacy heavily relies on the precision of the critical details transmitted across them, particularly when exchanging substantial medical data like radiology scans, historical clinical records, and patient health summaries.

Concurrently, paradigms like cloud computing have supplemented traditional content-sharing frameworks by allowing the secure uploading of medical imagery and sensitive patient data [1-3]. For instance, ref. [4] presents an architectural approach designed to elevate the security of medical image datasets during public channel transmission. This enables authenticated medical professionals to retrieve the information, notify the cloud administrator, and consult with the patient. Nevertheless, because an individual patient often accumulates numerous interconnected diagnostic files, the resulting data volumes can become massive and cumbersome to manage. The administrative efficiency of handling this large-scale data can be markedly enhanced by consolidating the diagnostic documentation and the corresponding clinical scans into a single unified file.

Reversible data hiding (RDH) represents a highly effective remedy for this issue. RDH constitutes a methodology where confidential records, such as demographic details, diagnostic reports, or historical health data, are securely embedded into a host medium—such as a computed tomography (CT) scan or a magnetic resonance imaging (MRI) file—enabling the flawless restoration of the original cover image alongside the error-free extraction of the hidden data at the destination [5-7]. Furthermore, reversible data hiding in encrypted images (RDHEI) has garnered significant research attention owing to its extensive utility in safeguarding personal information privacy [8].

Motivation for the proposed research

Existing literature indicates that least significant bit (LSB) methods [9-11] have historically been the dominant focus in the design of RDH models. Nonetheless, detecting the existence of concealed data within an encrypted framework remains inherently challenging, regardless of whether the algorithm utilizes LSB or most significant bit (MSB) strategies. Furthermore, prior to the encryption of the host image, the intense correlation among adjacent pixels renders MSB prediction an exceptionally potent technique for estimating neighboring pixel values. Based on these insights and aiming to maximize the payload capacity, Puteaux and Puech introduced RDH techniques driven by MSB prediction [12].

Specifically, one of the two MSB prediction error-centric RDHEI frameworks detailed in ref. [12] achieves an elevated payload rate approaching 1 bpp. This method leverages an individual MSB plane per pixel to conceal supplemental data while offering complete reversibility. Within this process, the host image is partitioned into segments containing eight pixels. Depending on the computed MSB prediction error, each segment is classified as either embeddable or non-embeddable, a distinction that facilitates the injection of secret data into the encrypted cover.

However, the primary challenge for the receiver lies in accurately identifying which blocks contain embedded data. To assist in the decoding phase, non-embeddable segments are flagged by modifying their preceding and succeeding blocks with a distinctive pattern; specifically, the MSBs of all pixels in the blocks flanking a non-embeddable segment are forced to 1. Nevertheless, an investigation into the cryptographic integrity of this scheme by ref. [13] revealed that this data insertion process lacks true imperceptibility.

Consequently, an adversary could potentially extract structural insights from the encrypted cover image using straightforward analytical methods. Continuous sequences of 1s across the MSBs of the encrypted file reveal the presence of these indicator flags, meaning that the existence of hidden payloads can be uncovered by applying simple histogram analysis to the distribution of 1s in the encrypted domain. Additionally, our observations show that in premium 16-bit DICOM data, the critical diagnostic details are typically restricted to the initial 10–12 bits (LSBs) of each pixel across most samples. This characteristic strongly supports the strategy of exploiting the underutilized MSBs for data hiding purposes.

Research objective and highlights

The primary objective of this investigation is to present an RDHEI framework with enhanced embedding capacity by re-engineering the architectural model from ref. [12] to eliminate the security vulnerabilities identified in ref. [13]. While our approach labels every block, it completely avoids the use of fixed, predefined sequences. This RDHEI algorithm is structured so that the indicator bits are embedded simultaneously with the payload, ensuring streamlined extraction. In this setup, these marker bits fulfill two distinct roles:

1. Verifying whether a particular block can accommodate data.
2. Determining the precise embedding rate allocated to each block.

The presented AdaBPE technique is a high-capacity RDH algorithm for encrypted imagery that dynamically responds to the structural characteristics of the pixels within each segment. In this configuration, one pixel from each non-overlapping block with a side length of A pixels serves as the predictor, while multiple MSBs from the remaining $((A \times A) - 1)$ pixels are leveraged to conceal confidential data.

The performance of this framework is validated across an extensive image repository, aligning perfectly with the idealized metrics of $BER = 0$, $PSNR = \infty$, and $SSIM = 1$. Verification trials cover both high-resolution medical DICOM images and standard natural photos. Additional key features of the proposed AdaBPE model include:

1. The volume of embedded data is uniform among pixels within the same block (intra-block) but can fluctuate across different blocks (inter-block).
2. In contrast to conventional prediction-centric frameworks that typically self-embed a localized map or flag tokens merely to signify a block's embeddability, our technique self-embeds specialized tracking bits. These bits denote not only whether a block is available for data injection but also define the exact payload capacity per pixel within that segment.
3. Maximizing the utilization of homogeneous (smooth) regions across the image enables the algorithm to achieve substantially higher data-hiding capacities, with the overall embedding rate fluctuating based on individual image composition.
4. The end user can extract the concealed private data exclusively using the data decryption key, completely independent of the image decryption key.

The primary technical innovations introduced by the AdaBPE RDHEI framework can be summarized as follows:

1. Formulation of a block-level adaptive methodology specifically tailored for RDHEI applications in clinical imaging.
2. Optimized exploitation of uniform intra-block pixels, avoiding the constraint of restricting all blocks to a fixed, uniform embedding capacity.
3. Leveraged multi-bit MSB prediction to achieve error-free data injection and recovery (utilizing 6 MSBs for 16-bit DICOM files and 3 MSBs for 8-bit natural images).

Related Work

Reversible data hiding (RDH) in images is typically executed across three distinct frameworks. The first approach utilizes a standard natural image to hide confidential data by modifying its original pixel intensities [14-16]. In the second method, the image is first encrypted, and the hidden data is subsequently embedded within this encrypted domain [17]. The final paradigm involves concealing the secret data simultaneously with the encryption phase, a technique known as RDH through encryption. To embed sensitive patient data into a digital medical image, the data hider must allocate sufficient spatial capacity. This allocation process must avoid inflicting irreversible distortions on the host image, ensuring its flawless reconstruction. Space for data insertion can be generated either prior to or following the encryption step.

Contemporary taxonomies of RDH algorithms distinguish between separable [18, 19] and non-separable [20, 21] approaches. Separable RDH architectures allow the extraction of the concealed payload and the restoration of the host image to function as mutually exclusive, independent processes. When standard natural images serve as the host medium, the visual fidelity of the resulting stego image is of paramount importance. An effective equilibrium between embedding payload and the visual integrity of the stego image, utilizing a local binary pattern methodology, is demonstrated in ref. [14]. Typically, augmenting the volume of hidden data proportionally diminishes the visual quality of the stego image. In this specific study, the methodology achieves an average embedding capacity of 1.98 bpp, accompanied by an average peak signal-to-noise ratio (PSNR) of 52.36 DB and a structural similarity index (SSIM) of 0.9977. Additionally, this strategy successfully mitigates underflow and overflow complications.

A framework for non-separable RDH within encrypted images is detailed in ref. [20]. This architecture injects 2 bits of confidential information into intra-block pixels categorized as black. Data insertion is facilitated by linking the 2-bit payload to a one-dimensional pseudo-random permutation matrix containing values spanning [0 – 255]. The restoration of every host block relies on evaluating the specific weights of a corresponding graph derived from that block. This strategy guarantees a consistent embedding capacity of 0.0312 bpp, independent of the underlying image characteristics. Furthermore, ref. [22] introduces an innovative encrypted-domain RDH model that expands the most significant bit (MSB) variance between pixels to open up embedding space. These MSB discrepancies are adjusted to yield an even numerical output while circumventing overflow. This separable architecture supports a payload of up to 1 bpp without degrading the fidelity of the reconstructed image. Another distinct RDH methodology designed to shrink the overall size of the encrypted image is outlined in ref. [2]. By creating a compressed variant using multiple MSBs, the algorithm generates supplementary space, allowing the extra data to be embedded into the encrypted counterpart. This technique reportedly decreases the encrypted file size to between 40% and 91% of the original host image, rendering it highly suitable for cloud computing environments. In ref. [18], an adaptive reversible integer transformation mechanism is introduced to create embedding capacity. Operating as a separable framework, the algorithm first modifies the host image using the integer transformation, generating auxiliary data that is subsequently embedded to free up space. A cloud server can then exploit these evacuated areas to hide secondary data within the encrypted file. Diverging from conventional methods, ref. [11] presents a reversible strategy that embeds payloads across replicated versions of the host image, referred to as shadow images. The intended recipient must possess all three stego images to successfully extract the entirety of the concealed payload. This approach demonstrates robust resilience against steganalysis intrusions. Ref. [23] describes a unique embedding model that safeguards a patient's identification number within the initial row of an encrypted DICOM file. This research leverages the Le Gal 5/3 wavelet transform and the Bülban map to execute image encryption and subsequent identification number insertion. Approved clinical staff can employ this procedure to extract the first row from the secured image and verify the patient ID; upon successful verification, cryptographic keys are utilized to decrypt the remaining pixels and reconstruct the full DICOM scan. This system provides strong defenses against plaintext and brute-force vulnerabilities.

Research in ref. [1] achieves an exceptionally high embedding ratio of 3.43 bits per bit change. This method utilizes an orthogonal projection technique to accurately estimate the substituted MSB, while a matrix encoding algorithm facilitates the insertion of auxiliary data directly into the MSB positions of the host image pixels. This configuration yields an average payload capacity of 0.412 bpp. The uniqueness of the model in ref. [1] lies in its ability to simultaneously elevate embedding efficiency and minimize write-associated costs. In contrast, ref. [24] applies a block-oriented stream cipher to encrypt the host medium, subsequently scrambling the data to obscure the original visual content and thwart complexity-based cryptanalysis. Data insertion is accomplished by categorizing blocks as either non-useable or useable based on localized pixel correlations. These blocks are then reorganized, moving non-useable segments to the terminal positions. To ensure flawless reconstruction of the initial image, the auxiliary metadata embedded via the RDH process must contain the original block sequencing. Building upon the principles of ref. [24], the investigation in ref. [25] applies the Arnold scrambling technique to the encrypted medium. This operation not only bolsters the cryptographic security of the encrypted file but also functions as a mechanism for concealing extra payload. This framework achieves a stable embedding capacity of 0.0547 bpp across all tested images. Subsequent enhancements to the payload capacity were

realized utilizing the Fibonacci transform algorithm, maintaining completely lossless recovery for both the host image and the hidden data [26].

The framework proposed in ref. [21] utilizes a symmetric cryptographic architecture to optimize non-separable, block-oriented RDH operations within encrypted files. Under this model, the encrypted host is processed as a series of uniform blocks. Within each specific block, pixels are grouped into discrete sets dictated by the volume of bits designated for insertion; for instance, accommodating a 2-bit payload requires partitioning the pixels into two corresponding sets. A formalized set of extraction rules dictates the embedding process, which is executed by flipping the 3 LSBs of the targeted pixels. This ensures a bit error rate (BER) of 0 during the reconstruction of the host image for block sizes ≥ 8 , while maintaining a peak signal-to-noise ratio (PSNR) between ≥ 40 and ≤ 60 . RDH strategies rooted in predictive modeling [27, 28] have also been extensively investigated, highlighted by the high-capacity architecture in ref. [29]. Operating on a prediction error mechanism, this approach generates a structured, hierarchical label map that undergoes compression to free up capacity before being embedded into the encrypted medium to aid subsequent recovery. This map explicitly designates the specific bit planes allocated for data concealment. The framework achieves an impressive average capacity of 3.4568 bpp. This significant payload expansion is driven by the categorization of prediction errors into three distinct magnitudes: large, medium, and small. Watermarking serves as a supplementary embedding methodology primarily focused on verifying data authenticity. Ref. [30] details a reversible, fragile watermarking framework engineered to precisely identify tampered zones while offering enhanced resilience, superior visual fidelity in the watermarked output (PSNR exceeding 52 DB), and expanded payload capacities. Standing apart from standard RDH algorithms, ref. [31] introduces a highly resilient RDH model tailored for compressed images, combining a (7,4) Hamming code with block truncation coding. The primary objective of this architecture is to ensure substantial structural robustness alongside premium stego image quality. The block truncation process operates as a lossy compression technique that segments the image into 4×4 grids. Blocks that are designated as smooth, as determined by a predefined threshold, are modified to store 2 bits of data using the Hamming code protocol.

Proposed Scheme

The primary entities within the introduced AdaBPE architecture comprise the data hider, the information sender, and the recipient. This RDH methodology operates by partitioning the original medical image (OMI) into non-overlapping, uniformly sized blocks. In the preliminary phase, the sender processes the OMI to formulate a marker list detailing the viable embedding capacities for each distinct block across the image. The OMI then undergoes encryption via a stream cipher algorithm. Subsequently, the encrypted OMI, the encrypted patient health report (PHR) data, and the corresponding marker list are transferred to the data hider. The data hider is responsible for seamlessly injecting both the encrypted PHR and the marker list into the encrypted OMI, ultimately producing a marked stego image. Conversely, the recipient's role begins with extracting the concealed PHR payload, followed by the lossless restoration of the underlying OMI. The practical viability of the proposed framework is validated through comprehensive testing on standard 8-bit natural images as well as 16-bit DICOM clinical formats.

Figure 1 illustrates the fundamental sequence of operations executed at the sender's end. The algorithm first segments the original medical image (OMI) into discrete, uniformly dimensioned blocks. Prior to the injection of PHR records, a preliminary analytical phase utilizes an MSB prediction error technique across each block to construct the marker list. Both the PHR contents and the OMI are then secured using dedicated encryption keys. To create physical space, a specific number of LSBs—equivalent to the data length of the marker list—are evacuated and stored independently. These isolated LSBs are merged with the encrypted PHR, consolidating into a singular data payload. The newly generated marker list is then inserted into the evacuated LSB positions. Guided by the parameters established in the marker list, the consolidated data payload is subsequently concealed within this updated encrypted image. This final insertion concludes the PHR embedding procedure.

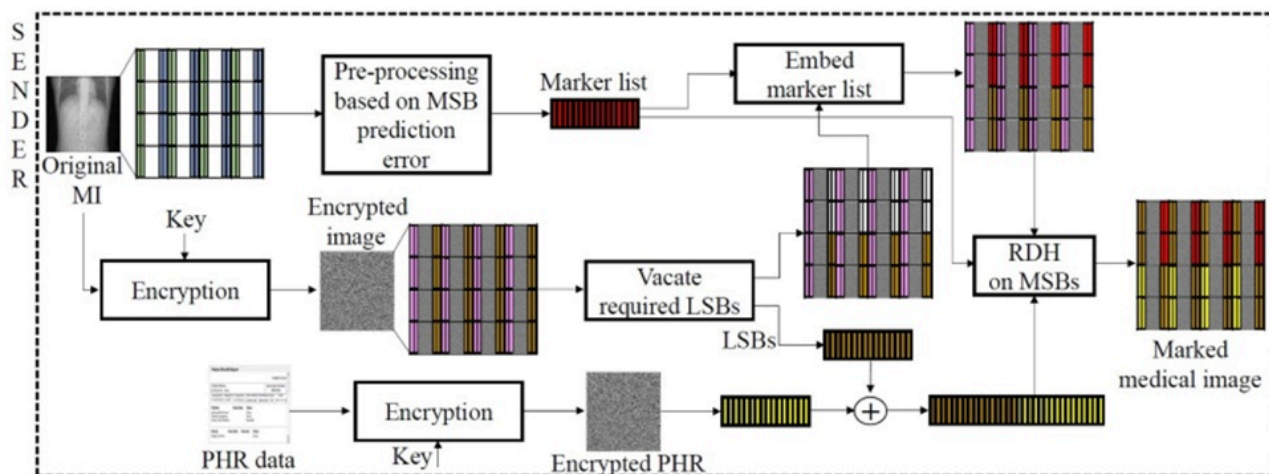


Figure 1. Basic model of sender side activities.

Figure 2 presents an overview of the corresponding processes managed by the recipient. The marked stego image is subdivided into identical, non-overlapping blocks matching the dimensions employed during the sender's routine. The initial extraction phase isolates the marker list from the modified LSBs of the received image. This retrieved marker list serves as a structural guide to securely extract the manipulated MSBs. From these harvested MSBs, the algorithm decouples the displaced original LSBs and the hidden PHR payload. The actual PHR is successfully reconstructed by applying decryption protocols to the isolated PHR segment. Simultaneously, the decoupled original LSBs are reinserted into their exact prior locations, overwriting the extracted marker list. Following this, the marked image is fully decrypted using the appropriate key, and the original pixel values within each block are flawlessly rebuilt using the marker list alongside the MSB prediction error logic. In-depth technical descriptions covering the specific mechanisms of both the extraction and embedding cycles are elaborated upon in the subsequent sections.

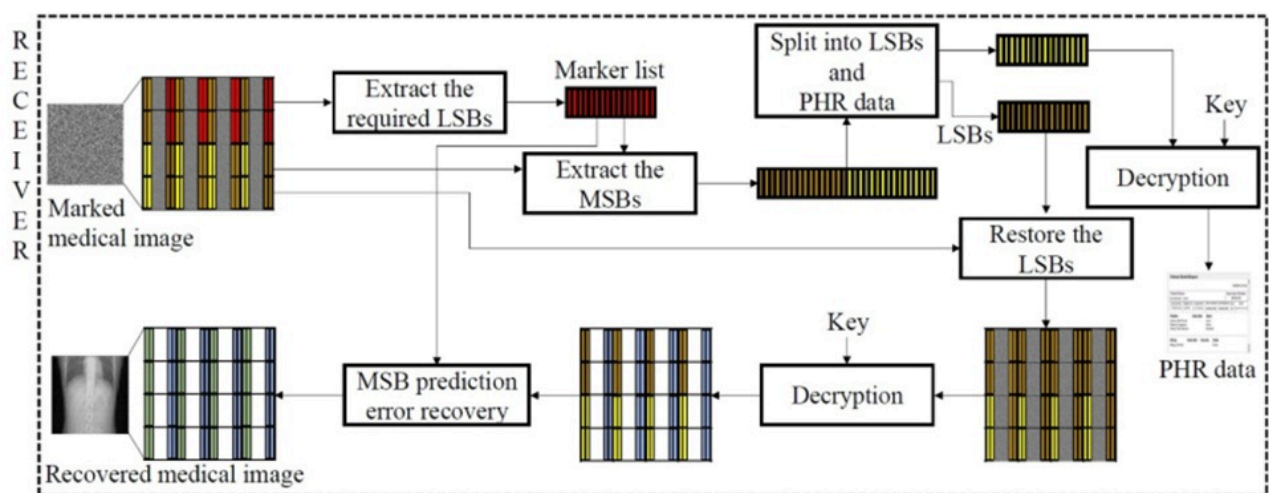


Figure 2. Basic model of receiver side activities.

Hiding the PHR information

The 16-bit DICOM original medical image (OMI) selected for the experimental setup possesses dimensions of $L \times M$ pixels. Therefore, the intensity value of every pixel within the OMI falls in the range $[0, 65535]$. Conversely, the pixel intensities of an 8-bit natural image are confined to $[0, 255]$. Prior to executing any processing steps, the original image is

standardized to a resolution of 512×512 pixels. Subsequent operations on the OMI are performed after partitioning it into non-overlapping blocks G^i of size $A \times A$ pixels, where $i = 1, 2, \dots, T$, $A \in \{2, 4, 8, 16, 32\}$. The total number of blocks is defined as:

$$T = \left\lfloor \frac{L}{A} \right\rfloor \times \left\lfloor \frac{M}{A} \right\rfloor \quad (1)$$

Marker list generation

Each $A \times A$ pixel block of the OMI is evaluated for prediction errors. The pixel located at the top-left corner of each block is designated as the predictor pixel. As illustrated in **Figure 3**, pixel P serves as the predictor, while the remaining pixels within the 4×4 block function as non-predictor pixels, denoted as N_i where $i = 1, 2, \dots, 15$.

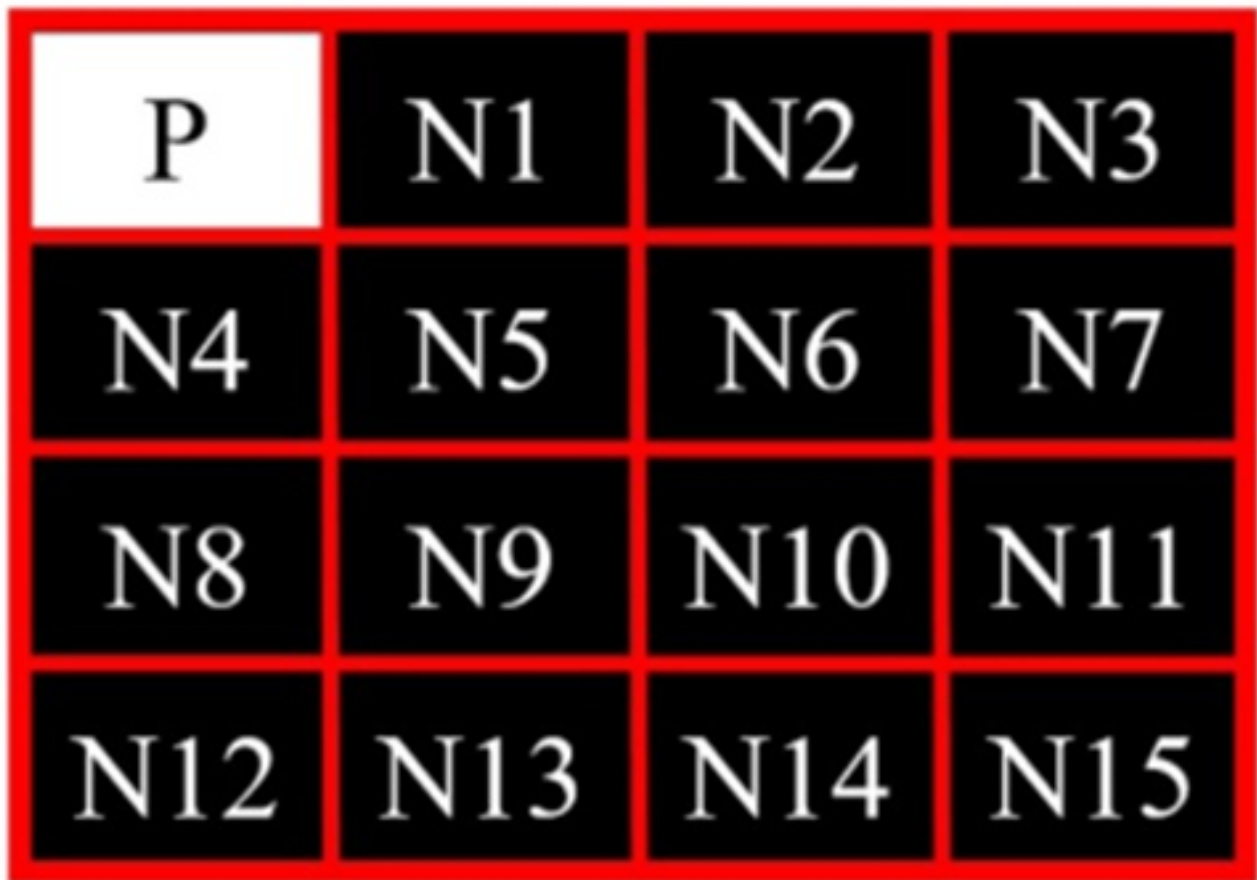


Figure 3. Block showing predictor and non-predictor pixels.

A marker list is constructed as a sequence of bit groups, with each group specifying the volume of data that can be securely embedded into the non-predictor pixels of a corresponding block. Let M_i represent the marker bits allocated to block G^i of the OMI, then:

$$M_i = \begin{cases} \{000, 001, 010, 011, 100, 101, 110\} & \text{if 16-bit DICOM image} \\ \{00, 01, 10, 11\} & \text{if 8-bit Natural image} \end{cases} \quad (2)$$

where $1 \leq i \leq T$. Eq. 2 dictates that a 3-bit marker is generated for every block within an original medical image (OMI), whereas a 2-bit marker is produced for each block in a natural image. The specific embedding capacity—and consequently the exact configuration of M_i —is contingent upon the inherent structural characteristics of the intra-block pixels, which are determined via the MSB prediction error mechanism. This compiled sequence of M_i indicators is formally referred to as the MarkerList.

Computing prediction error

The prediction error associated with a specific non-predictor pixel is determined by evaluating the numerical variance between the predictor pixel and multiple modified states of that non-predictor pixel. For instance, when validating a 1-bit embedding capacity, two distinct states of the non-predictor pixel are evaluated: the unaltered original pixel and a modified version where its MSB has been inverted. The prediction errors are calculated as the absolute differences between the predictor pixel and these two states of the non-predictor pixel. Consequently, the number of evaluated variations for a given non-predictor pixel scales directly with the intended bit-embedding depth. Within the parameters of this proposed framework, a maximum of 6 bits can be embedded into a non-predictor pixel in a DICOM image, and up to 3 bits in a natural image. Let P define the predictor pixel and N_i represent the non-predictor pixel. The binary representation encompasses bit planes $\{N_{i0}, N_{i1}, \dots, N_{iQ}\}$, where $0 \leq x \leq (Q - 1)$ and Q signifies the overall bit-depth of the image. Here,

$$N_{ix} = \left\lfloor \frac{N_i}{2^x} \right\rfloor \bmod 2, \quad 0 \leq x \leq (Q - 1), \quad (3)$$

or

$$N_i = \sum_{j=0}^{Q-1} (2^j \times N_{ij}). \quad (4)$$

The methodology requires that every N_i must be accurately predictable based on P . Furthermore, uniform embedding capacity is mandated across all N_i pixels residing within the same block. Because this specific prediction logic is grounded in MSB replacement, N_i is mathematically modeled as the composite of two distinct segments, where one segment explicitly isolate the MSB replacement mechanics. Thus:

$$N_i = Y_{(Q-1)-k} + Z_k. \quad (5)$$

In this context, k denotes the exact quantity of MSBs targeted for substitution to hold the embedded data. As an example, an embedding capacity of 1 on N_i signifies that the original N_i satisfies the predictability threshold for a 1-MSB replacement. Therefore, when attempting to embed 1 bit into a 16-bit DICOM file, the algorithm evaluates the 1-MSB prediction error. Implementing a k -MSB replacement on N_i produces N_i^X possible variations, where $X = 2^k$ and $k \geq 0$. Consequently, evaluating a 1-bit MSB prediction generates 2 distinct forms of N_i : one instance where the original MSB is forcibly set to 0, and another where it is set to 1. If the absolute difference between the predictor pixel and the unmodified original non-predictor pixel is demonstrably smaller than the differences calculated for all other generated versions of N_i , the system validates that a 1-bit MSB replacement is viable. This evaluation for a 1-bit embedding is formalized by the following equation:

$$Y_{14} = \sum_{j=0}^{14} (2^j \times Ni_j) \text{ and} \quad (6)$$

$$Z_1^1 = \sum_{j=15}^{15} (2^j \times Ni_j), \text{ also} \quad (7)$$

$$Z_1^2 = \sum_{j=15}^{15} (2^j \times (1 - Ni_j)). \quad (8)$$

This yields two specific variations of the non-predictor pixel:

$$\begin{aligned} Ni^1 &= Y_{14} + Z_1^1, \\ Ni^2 &= Y_{14} + Z_1^2. \end{aligned} \quad (9)$$

If $|P - Ni^1| < |P - Ni^2|$, the pixel successfully qualifies for 1-bit information embedding. Applying this logic to a 2-bit embedding scenario requires computing the MSB prediction error across 4 distinct variations of Ni , defined by:

$$Z_2^1 = \sum_{j=14}^{15} (2^j \times Ni_j), \quad (10)$$

$$Z_2^2 = \sum_{j=14}^{15} (2^j \times (1 - Ni_j)), \quad (11)$$

$$Z_2^3 = (2^{15} \times Ni_{15}) + (2^{14} \times (1 - Ni_{14})), \quad (12)$$

$$Z_2^4 = (2^{15} \times (1 - Ni_{15})) + (2^{14} \times Ni_{14}). \quad (13)$$

In this specific instance, the MSB prediction errors are calculated between the predictor pixel and the four aforementioned versions of Ni . If the error magnitude $|P - Ni^1|$ remains smaller than the alternatives, the block is cleared for 2-bit embedding. In these examples, Ni^1 uniformly represents the initial, unaltered non-predictor pixel N . This methodological progression is utilized to establish the maximum permissible embedding rate for any given block. The algorithm initiates testing at a baseline embedding rate of 1 and incrementally advances the rate by one bit, recalculating the prediction errors until it determines the absolute maximum payload capacity that holds true for every non-predictor pixel within that block. As previously established, the upper limit for embedding capacity under this framework is capped at 6 bits for 16-bit DICOM formats and 3 bits for natural imagery.

Embedding the patient health report (PHR)

Assuming a processed block size of $A \times A$ and a total block count of T , the marker list will encompass B bits corresponding to each respective block. We define:

$$B = \begin{cases} 3 & \text{if image is a 16-bit DICOM image} \\ 2 & \text{if image is an 8-bit Natural image.} \end{cases} \quad (14)$$

The marker list itself is defined as:

$$M = \{\{M_i\} \mid 1 \leq i \leq T\}. \quad (15)$$

The aggregate size of the marker list M is denoted by SM :

$$SM = T \times B. \quad (16)$$

Let a block of side-length A contain F non-predictor pixels available for concealing confidential data. Here:

$$F = (A \times A) - 1. \quad (17)$$

Given that individual blocks can accommodate varying volumes of data based on their specific MSB prediction thresholds, the maximum embeddable payload MAX across the entire image is intrinsically tied to the parameters defined within the marker list:

$$MAX = \sum_{i=1}^T ((M_i)_{10} \times F). \quad (18)$$

In the context of medical deployments, the destination party must flawlessly reconstruct the original MI free of any artifacts, while simultaneously executing a lossless extraction of the concealed diagnostic report PHR. To guarantee the cryptographic security of the PHR data, the information undergoes encryption. To enable the lossless reconstruction process, the marker list M is self-embedded alongside the encrypted PHR payload. Consequently, the maximum volume of PHR information $MPHR$ that can be practically embedded is calculated as:

$$MPHR = MAX - SM. \quad (19)$$

The introduced AdaBPE methodology executes data hiding strictly within an encrypted medical image environment. Therefore, a 512×512 pseudo-random matrix, generating intensity values in the range $[0, 65535]$, is employed to encrypt a 16-bit OMI, resulting in the encrypted medical image (EMI). This encryption is executed using an XOR operation. The PHR data is subjected to a parallel encryption process. For natural images, the pseudo-random matrix parameters are adjusted accordingly. The sequential protocol for embedding the $MPHR$ data into the EMI is outlined below:

1. Subdivide the EMI into non-overlapping $A \times A$ pixel blocks to determine the total block count T .
2. Compute the length of the marker list:

$$|M| = T \times B. \quad (20)$$

3. Extract a sequence of LSBs from the EMI pixels, precisely matching the calculated bit size M .

$$LSB = \{ \{ LSB_i \} \mid 1 \leq i \leq |M| \}. \quad (21)$$

4. Substitute these vacated LSB positions with the compiled marker list M .
5. Concatenate the encrypted PHR data D , possessing a size of $MPHR$, with the LSBs isolated in step 3. This combination forms the total payload TI , the size of which equates to MAX (Eq. 18).

$$TI = LSB || D. \quad (22)$$

6. The combined payload is then embedded into each encrypted block via multiple MSB substitutions, explicitly governed by the B-bit instruction defined in the marker list M_i . If N_i represents a non-predictor pixel within a block f belonging to a 16-bit EMI, the substitution logic is:

$$\begin{aligned} N_i &= N_i, & \text{if } M_f &= 000 \\ N_i &= N_i \text{ with 1-bit MSB substituted from } TI, & \text{if } M_f &= 001 \\ N_i &= N_i \text{ with 2-bit MSB substituted from } TI, & \text{if } M_f &= 010 \\ N_i &= N_i \text{ with 3-bit MSB substituted from } TI, & \text{if } M_f &= 011 \\ N_i &= N_i \text{ with 4-bit MSB substituted from } TI, & \text{if } M_f &= 100 \\ N_i &= N_i \text{ with 5-bit MSB substituted from } TI, & \text{if } M_f &= 101 \\ N_i &= N_i \text{ with 6-bit MSB substituted from } TI, & \text{if } M_f &= 110. \end{aligned} \quad (23)$$

When processing an 8-bit natural image, equation 23 is restricted to four conditions for N_i , reflecting the use of a 2-bit marker per block. Ultimately, the marked medical image (MMI), successfully generated by embedding the encrypted PHR payload into the encrypted medical host, is transmitted to the consulting medical specialist via a designated communication pathway for review. A high-level schematic of the proposed RDH architecture executed by the sender is depicted in Figure 1, while the corresponding extraction architecture at the receiver's end is detailed in Figure 2.

Recovering the hidden PHR information

The introduced AdaBPE RDH method provides the receiver with the capability to extract all concealed encrypted PHR data from the MMI without requiring the image decryption key, while also allowing the lossless restoration of the original MI using this key. The procedure for retrieving both the embedded encrypted PHR data and the original medical image (OMI) involves the following steps:

1. The total number of blocks, T , is computed using Eq. 1, contingent upon the processing block dimensions of $A \times A$ pixels.
2. The dimension of the marker list M is dependent on T (Eq. 16).
3. Retrieve the $|M|$ LSBs from the MMI to generate the marker list M .
4. Analyze the extracted bits of M in their retrieval sequence and organize them into clusters of B bits. As an illustration, in a 16-bit medical image, M comprises 3-bit clusters where $M_i \in \{000, 001, 010, 011, 100, 101, 110\}$ and $1 \leq i \leq T$.
5. Evaluate the marked image MMI as non-overlapping $A \times A$ pixel blocks.

$$MMI = \{ MMI_i \} \mid 1 \leq i \leq T. \quad (24)$$

It is important to note that MMI_i has dimensions of $A \times A$ pixels.

6. Retrieve multiple MSBs from the non-predictor pixels within block MMli, relying on the marker list , to assemble the extracted information EI.
7. Partition the extracted information EI into two distinct segments.

$$EI = EI_i || EI_j \text{ with } 1 \leq i \leq |M| \text{ and } |M| + 1 \leq j \leq |EI|. \quad (25)$$

In this context, EIj represents the extracted encrypted PHR data from the marked medical image MMI, while EIi constitutes the bit stream representing the original LSBs of the encrypted medical image EMI.

8. Substitute all LSB locations previously utilized for extraction in step 3 with the retrieved bit stream EIi from step 7, thereby producing the intermediate marked image IMI.
9. Decipher the intermediate marked image IMI applying the designated image decryption key.
10. Execute block recovery via the MSB prediction error technique on every block of the decrypted image, guided by the marker list M, to reconstruct the original medical image OMI.
11. Decipher the extracted encrypted PHR data EIj utilizing the data decryption key to restore the initial embedded PHR information.

Block recovery using MSB prediction error method

Assume a block DMIi originating from the decrypted marked medical image with dimensions $A \times A$ pixels, alongside the embedding information Mi derived from the marker list M, wh $k = (M_i)_{10}$ and $k = \{0, 1, \dots, K\}$, ere $1 \leq i \leq T$.

Within every block DMI_i, there are $((A \times A) - 1)$ non-predictor pixels. Designate P as the solitary predictor pixel and Ni, where $1 \leq i \leq (A \times A) - 1$, as the non-predictor pixels within that block. For a 16-bit medical image, the block marker data is $M_i \in \{000, 001, 010, 011, 100, 101, 110\}$. Consequently, there are 7 distinct block recovery scenarios for a 16-bit medical image, and 4 unique scenarios for an 8-bit natural image. Let,

$$k = (M_i)_{10} \text{ and } k = \{0, 1, \dots, K\}, \quad (26)$$

where,

$$K = \begin{cases} 6 & : \text{image being a 16-bit DICOM image} \\ 3 & : \text{image being an 8-bit Natural image.} \end{cases} \quad (27)$$

Suppose N_{ix} denotes the specific bit-plane values (Eq. 3).

1. When $k = 0$, embedding did not occur; therefore, the non-predictor pixels within the block are unaltered.
2. When $k = 1$, a single-bit MSB substitution was performed by the sender. Consequently, there are two variations of Ni to evaluate during recovery: Ni' and Ni". Here,

$$\begin{aligned} Ni' &= \sum_{j=0}^{Q-1-k} (2^j \times Ni_j), \\ Ni'' &= 32768 + \sum_{j=0}^{Q-1-k} (2^j \times Ni_j), \end{aligned} \quad (28)$$

where Q represents the pixel bit-length of the given image. To restore the authentic non-predictor pixel N_i , the variance between P and both variations of N_i is calculated.

$$N_i = \begin{cases} N_i' & \text{if } |P - N_i'| < |P - N_i''| \\ N_i'' & \text{otherwise.} \end{cases} \quad (29)$$

3. When $k = 2$, two MSBs were replaced to embed two bits of information by the sender. As a result, four distinct versions of N_i must be evaluated for recovery: N_i' , N_i'' , N_i''' , and N_i'''' .

$$\begin{aligned} N_i' &= \sum_{j=0}^{Q-1-k} (2^j \times N_{ij}), \\ N_i'' &= 32768 + \sum_{j=0}^{Q-1-k} (2^j \times N_{ij}), \\ N_i''' &= 16384 + \sum_{j=0}^{Q-1-k} (2^j \times N_{ij}), \\ N_i'''' &= 49152 + \sum_{j=0}^{Q-1-k} (2^j \times N_{ij}). \end{aligned} \quad (30)$$

The absolute difference between P and each of the four N_i variations is determined. The specific version of N_i yielding the smallest difference from the predictor pixel P corresponds to the original non-predictor pixel N_i , as demonstrated in equation 29. Similarly, the restoration of all non-predictor pixels can be executed for $k = \{0, 1, \dots, K\}$.

This described procedure is iterated until every block within the DMI is restored, utilizing the data provided in the marker list M , thereby reconstructing the original medical image OMI.

Visual representations of the embedding and recovery procedures are provided in **Figures 4 and 5**, respectively. To demonstrate this methodology, an 8-bit image measuring 4×4 pixels was utilized and divided into 4 non-overlapping 2×2 pixel blocks. Assuming each block produces 2-bit marker data to track the embedding, the cumulative length of the marker list equals $4 \times 2 = 8$ bits. For clarity, the displayed PHR data reflects the information produced post-encryption.

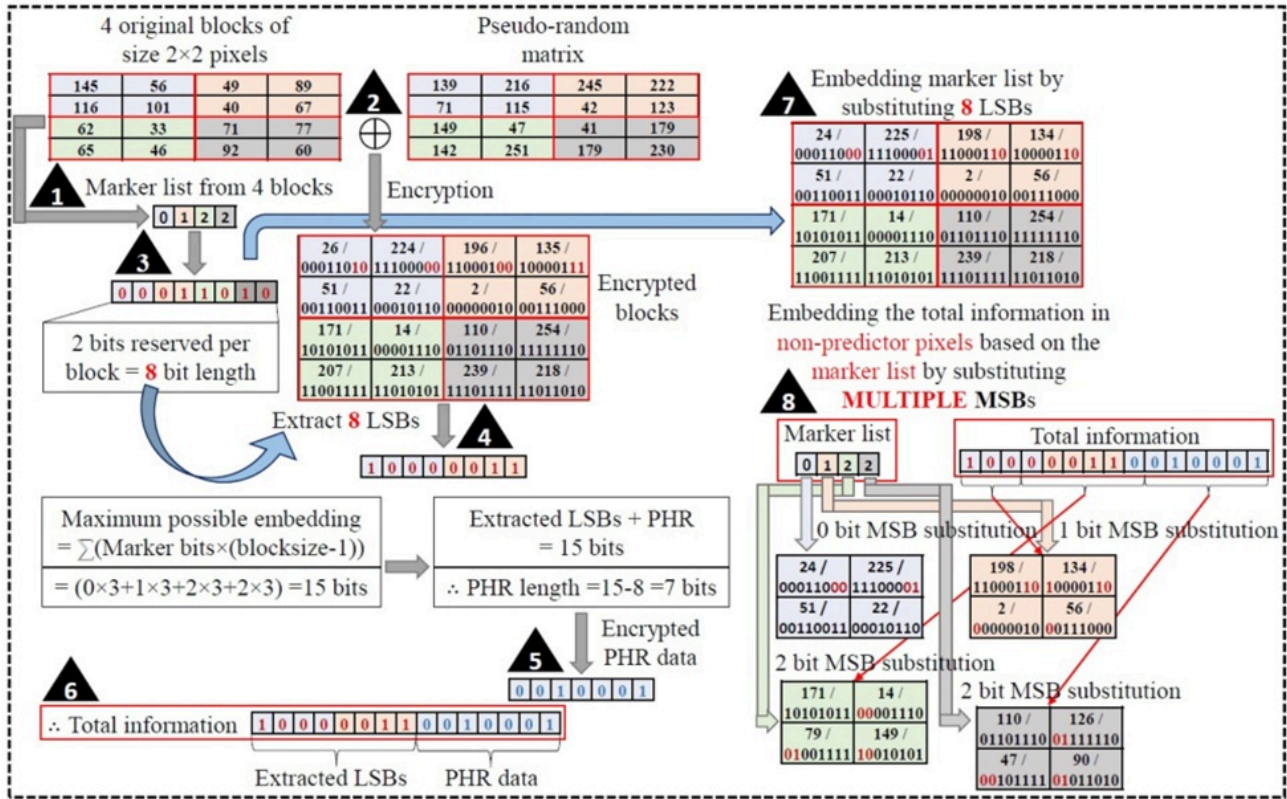


Figure 5. An illustration of PHR and original block recovery in the AdaBPE RDH scheme.

Experimental Results

The AdaBPE methodology was simulated using Matlab R2019a. The software was built and tested on a 64-bit operating system running an x64-based Intel(R) Core(TM) i5-9300H processor at 2.40 GHz with 8 GB of RAM. The experimental dataset incorporated high-quality 16-bit DICOM images, encompassing 497 images across CT, MR, and OT modalities sourced from ref. [32], alongside 100 CT images [33] obtained from the Cancer Imaging Archive [34]. Furthermore, the proposed method was evaluated on 210 natural images taken from the USC-SIPI digital image database [35]. Within this study, the outcomes for specific images depicted in **Figure 6** are prominently featured, while **Figure 7** presents a selection of sample output images generated during the experiments.

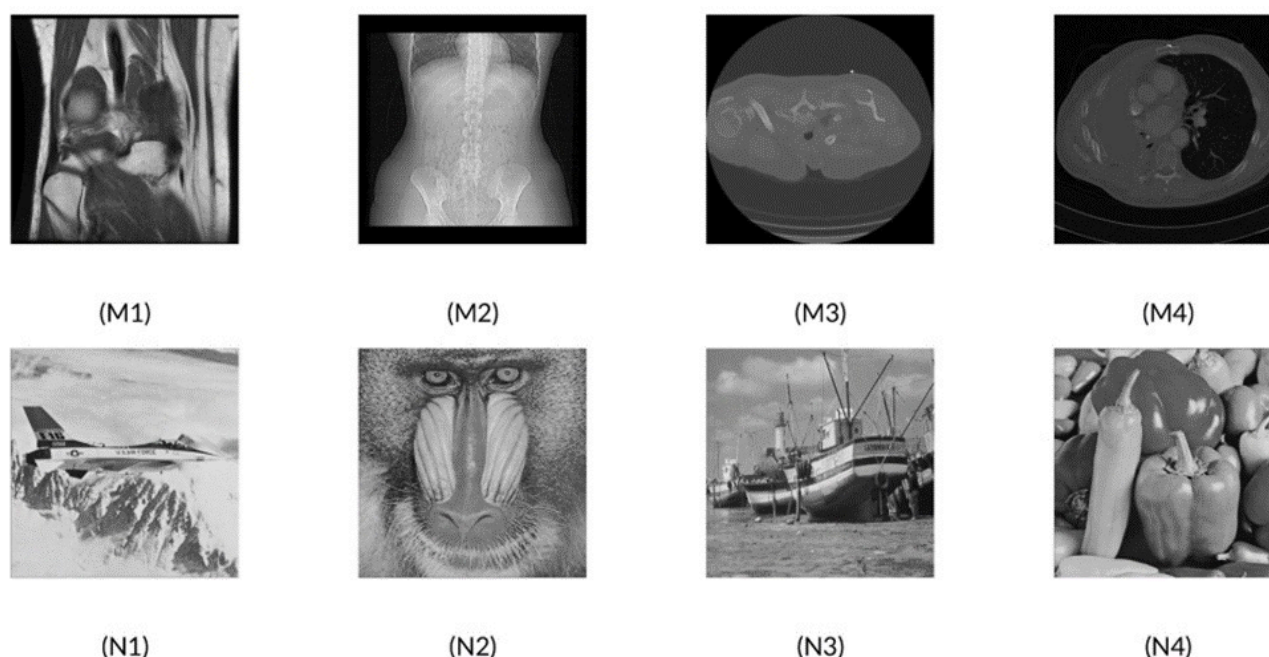


Figure 6. 16-bit sample DICOM images: (M1) Medical Image-1, (M2) Medical Image-2, (M3) Medical Image-3, (M4) Medical Image-4, and Sample natural images: (N1) Airplane, (N2) Baboon, (N3) Boat, and (N4) Peppers.

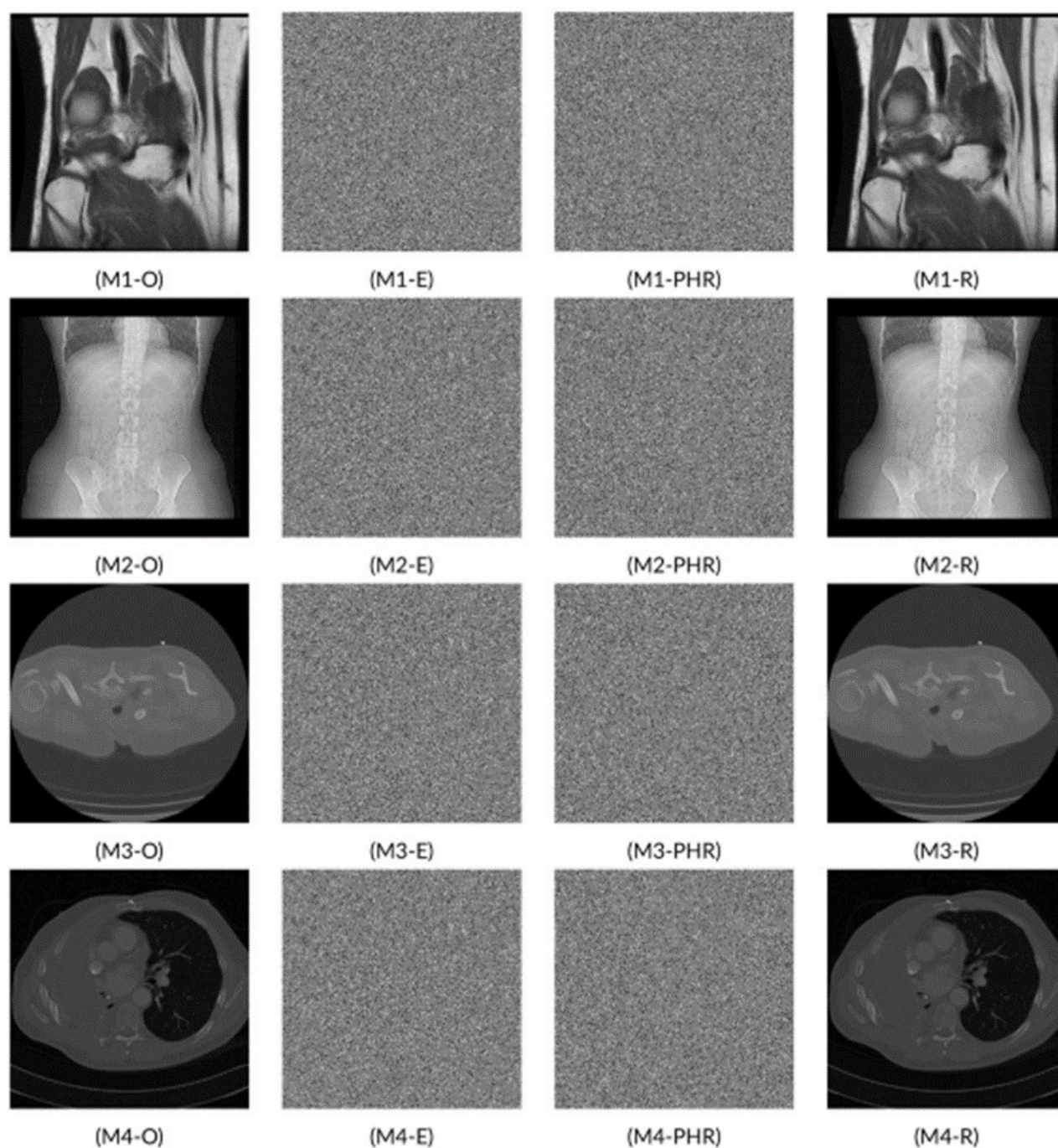


Figure 7 Sample image results from experiment [Figure (M1-O), (M2-O), (M3-O), and (M4-O): Original medical images, Figure (M1-E), (M2-E), (M3-E), and (M4-E): corresponding encrypted images, Figure (M1-PHR), (M2-PHR), (M3-PHR), and (M4-PHR): encrypted and PHR embedded images, and Figure (M1-R), (M2-R), (M3-R), and (M4-R): corresponding recovered images].

Single reference for prediction

In the majority of prediction-oriented techniques, a row, a column, or a mixture of both is typically set aside to forecast the remaining related pixels within a given block. However, in the newly introduced AdaBPE framework, every non-predictor pixel within a block is forecasted utilizing just one designated predictor pixel. Through this strategy, all but one pixel in each block are available for concealing the patient's health report (PHR) data. As a result, within an 8×8 pixel block, 63 out of 64 pixels are exploited to house supplementary information. Consequently, for an image measuring 512×512 pixels, the pixel utilization rate reaches 98.44% when employing a side-length of 8.

Adaptive block embedding

The integration of sensitive patient data varies across individual blocks and is intrinsically linked to the MSB prediction error technique. Every block undergoes independent processing, and a maximum achievable embedding value selected from $\{0, 1, 2, 3, 4.5, 6\}$ is established once prediction errors are factored in. The embedding capacity allocated to a block is constrained to ensure that every non-predictor pixel remains fully recoverable. **Figure 8** illustrates the fluctuations in the embedding rate across 200 randomly chosen blocks from Medical Image-1 utilizing a side-length of 16.

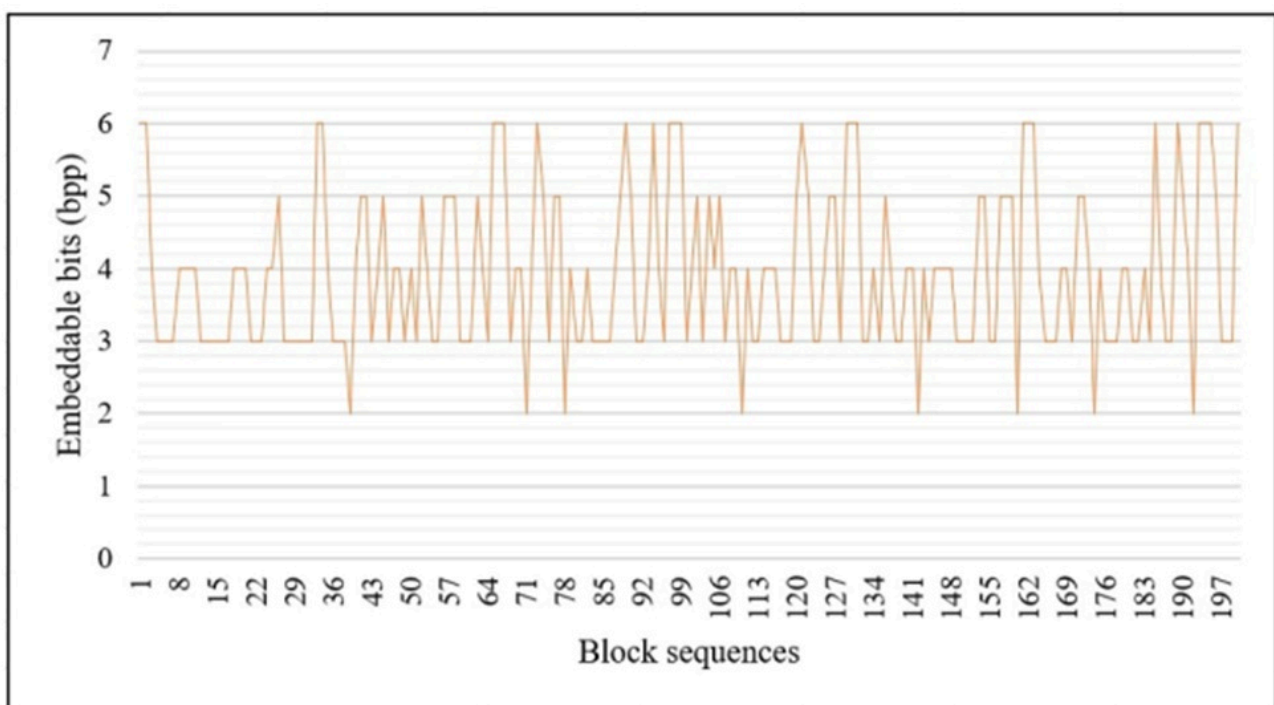


Figure 8. Embedding difference in different blocks of the same image.

Appropriate block selection

Selecting an optimal block size in any RDH framework significantly impacts both the volume of embedded data and the efficacy of the recovery phase. While specific block dimensions promote enhanced embedding rates, they may simultaneously compromise the qualitative restoration of the image. It is important to emphasize that block size does not hinder the retrieval of concealed data or the original image within the presented AdaBPE methodology; however, it directly dictates the embedding rate. **Table 1** catalogs the number of images that reached their peak embedding capacities for varying block sizes. Based on experimental trials involving 597 high-quality 16-bit DICOM images, 380 of these medical images recorded their highest embedding potential with a block side-length of 16. This signifies that 63.65% of the medical images maximized their embedding using 16×16 pixel blocks. Conversely, 68.1% of the evaluated natural images maximized their embedding capacity using 4×4 pixel blocks.

Table 1. Overall image count that accomplished its maximum embedding with respect to block size.

Image Type	Total Images	Block Side-Length →	2	4	8	16	32
Medical Image	597		0	13	201	380	3
Natural Image	210		51	143	15	1	0

Quantity of PHR data embedded

The rate at which PHR data is embedded into an encrypted medical image fluctuates depending on the intrinsic characteristics of the specific image. Within medical imaging, extensive regions are typically black, with pertinent information localized in confined zones. Consequently, this characteristic is leveraged to conceal the maximum possible amount of PHR data using the MSB prediction error technique. The embedding of information is quantified in bits per pixel (bpp). **Tables 2 and 3** detail the embedding metrics for four medical images and four natural images, respectively, evaluated across block side-lengths of $\{2, 4, 8, 16, 32\}$. **Figures 9 and 10** illustrate the variations in embedding rates across the 497 medical images sourced from ref. [32] and the 100 CT images [33] obtained from the Cancer Imaging Archive [34]. The USC-SIPI digital image repository encompasses diverse classifications of natural images, including Aerials, Misc, Sequences, and Textures. **Figure 11** outlines the embedding rate disparities observed across all 210 natural images.

Table 2. Estimation of the embedding information and bit error rate on medical images.

Image	Bit	Embedded	Block
	Error rate	Rate (bpp)	Side-length
Medical Image-1	0	3.635	2
	0	4.806	4
	0	4.599	8
	0	4.016	16
	0	3.454	32
Medical Image-2	0	3.750	2
	0	5.437	4
	0	5.859	8
	0	5.964	16
	0	5.991	32
Medical Image-3	0	3.747	2
	0	5.405	4
	0	5.767	8
	0	5.755	16
	0	5.581	32

Medical Image-4	0	3.738	2
	0	5.368	4
	0	5.688	8
	0	5.602	16
	0	5.241	32

Table 3. Embedding rate and bit error rate on natural images.

Image	Bit error rate	Embedded information (bpp)	SBlock side-length
Airplane	0	1.550	2
	0	2.036	4
	0	1.788	8
	0	1.337	16
	0	0.829	32
Baboon	0	0.954	2
	0	0.964	4
	0	0.626	8
	0	0.336	16
	0	0.134	32
Boat	0	1.472	2
	0	1.779	4
	0	1.362	8
	0	0.814	16
	0	0.376	32
Peppers	0	1.594	2
	0	2.089	4
	0	1.688	8
	0	1.043	16
	0	0.435	32

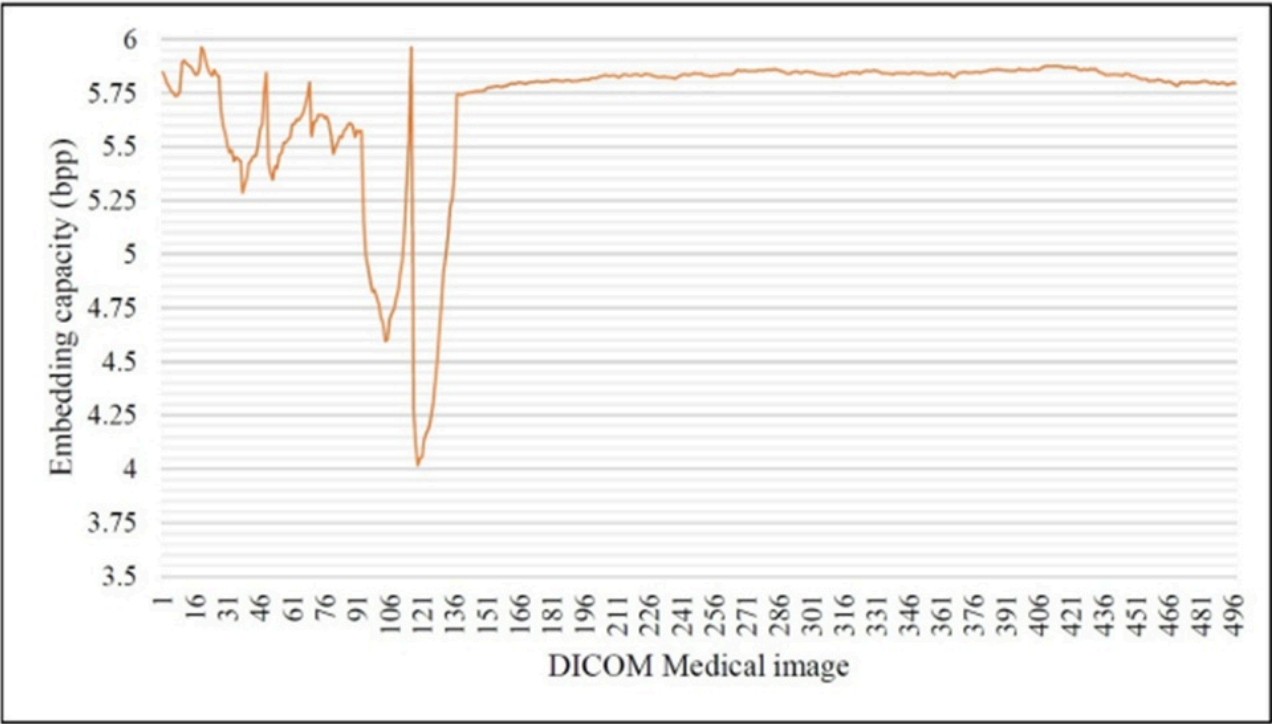


Figure 9. Embedding rate obtained from 497 DICOM medical images.

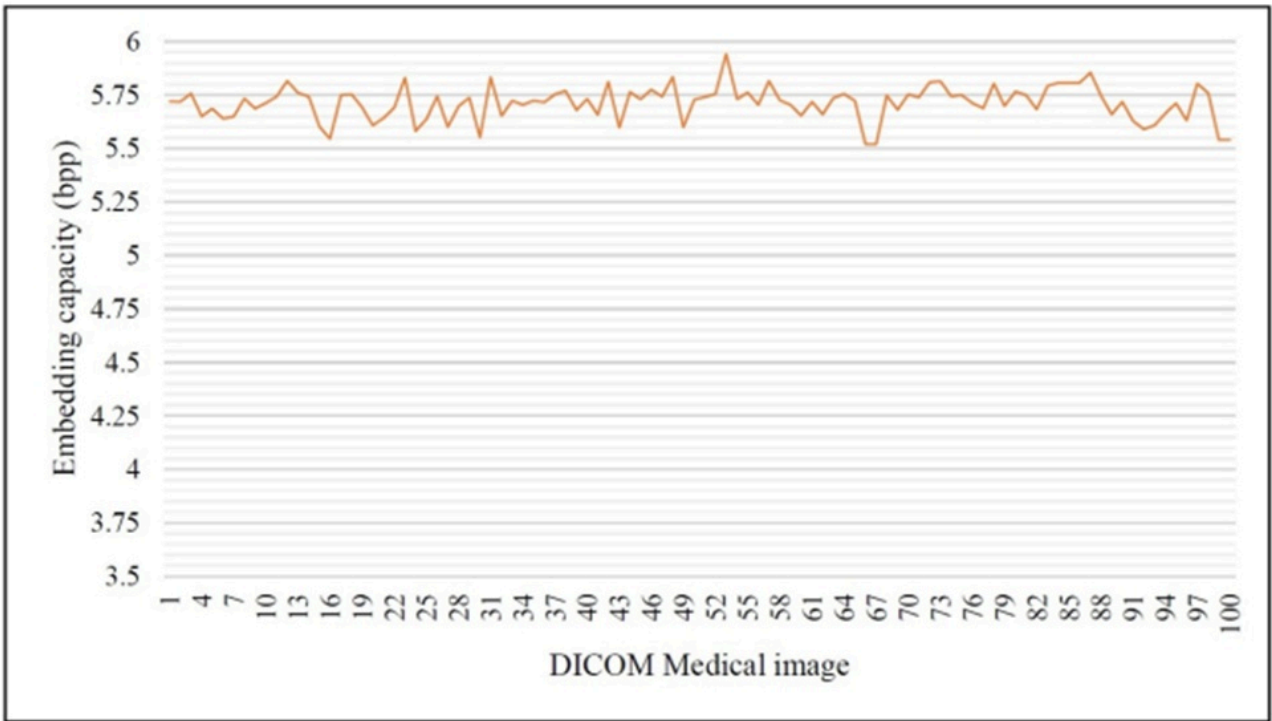


Figure 10. Embedding rate obtained from 100 DICOM medical images.

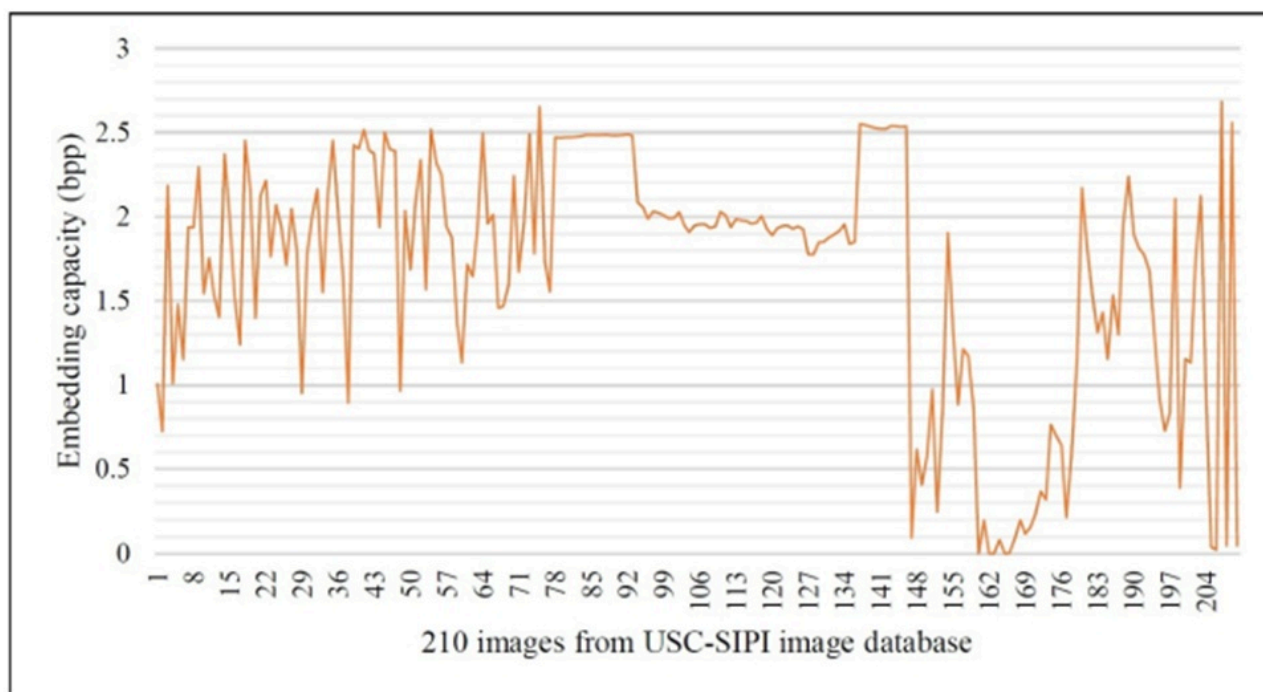


Figure 11. Embedding rate obtained from natural images.

Error in recovering the PHR data

Enhancing the embedding payload in RDH methods often degrades the quality of the restored image. Therefore, an effective RDH framework must strike a balance between data payload and image restoration to maintain the fidelity of the reconstructed image. The introduced AdaBPE methodology achieves excellent embedding efficiency while flawlessly retrieving all confidential patient data upon reception. **Table 2** presents the details of BER across 4 medical images, whereas **Table 3** provides corresponding metrics for 4 natural images evaluated at various side-lengths {2,4,8,16,32}. These tables demonstrate a BER = 0, indicating that the concealed PHR data is fully restored without any data corruption.

Examining through entropy analysis

Images are highly vulnerable to statistical exploits, necessitating robust protective measures, particularly for medical imagery. The presented AdaBPE methodology utilizes premium DICOM images as the carrier medium, embedding confidential patient details, such as medical reports, as supplementary data. Consequently, unauthorized entities must be prevented from extracting any meaningful data from the image. The variance in pixel values plays a crucial role in defending images against statistical breaches. Therefore, we evaluated the entropy of both the ciphered image and the marked image—the image containing the concealed PHR data. Due to the extensive diversification of pixels, adversaries can extract virtually no useful information from the encrypted state. The entropy approaches 8 for an 8-bit encrypted image and approximately 16 for a 16-bit encrypted image. An entropy metric near 16 indicates high pixel randomness, effectively preventing the disclosure of definitive visual data. **Tables 4 and 5** illustrate the entropy measurements for four medical and four natural images, respectively. The metrics recorded for both the encrypted images and the PHR-embedded images closely align with the theoretical ideal. Generally, the entropy of an image I can be computed using the equation:

$$ENTROPY(I) = - \sum_{i=0}^{N-1} P(i) \log_2 P(i) \quad (31)$$

Here N indicates the peak intensity level and P(i) gives the probability of occurrence of the pixel intensity value i.

Table 4. Entropy obtained on medical images.

Image	Entropy recovered image	Entropy after embedding PHR	Entropy after encryption	Entropy original image	Side-length of the block
Medical Image-1	12.007	15.611	15.807	12.007	2
	12.007	15.802	15.807	12.007	4
	12.007	15.808	15.807	12.007	8
	12.007	15.808	15.807	12.007	16
	12.007	15.808	15.807	12.007	32
Medical Image-2	6.400	15.538	15.808	6.400	2
	6.400	15.780	15.808	6.400	4
	6.400	15.807	15.808	6.400	8
	6.400	15.807	15.808	6.400	16
	6.400	15.808	15.808	6.400	32
Medical Image-3	7.660	15.537	15.808	7.660	2
	7.660	15.781	15.808	7.660	4
	7.660	15.806	15.808	7.660	8
	7.660	15.807	15.808	7.660	16
	7.660	15.810	15.808	7.660	32
Medical Image-4	9.395	15.545	15.809	9.395	2
	9.395	15.784	15.809	9.395	4
	9.395	15.807	15.809	9.395	8
	9.395	15.808	15.809	9.395	16
	9.395	15.807	15.809	9.395	32

Table 5. Entropy obtained on four natural images.

Image	Entropy recovered image	Entropy after embedding PHR	Entropy after encryption	Entropy original image	Block side-length
Airplane	6.702	7.924	7.999	6.702	2

	6.702	7.996	7.999	6.702	4
	6.702	7.999	7.999	6.702	8
	6.702	7.999	7.999	6.702	16
	6.702	7.999	7.999	6.702	32
Baboon	7.358	7.991	7.999	7.358	2
	7.358	7.999	7.999	7.358	4
	7.358	7.999	7.999	7.358	8
	7.358	7.999	7.999	7.358	16
	7.358	7.999	7.999	7.358	32
Boat	7.191	7.944	7.999	7.191	2
	7.191	7.998	7.999	7.191	4
	7.191	7.999	7.999	7.191	8
	7.191	7.999	7.999	7.191	16
	7.191	7.999	7.999	7.191	32
Peppers	7.593	7.920	7.999	7.593	2
	7.593	7.997	7.999	7.593	4
	7.593	7.999	7.999	7.593	8
	7.593	7.999	7.999	7.593	16
	7.593	7.999	7.999	7.593	32

Examining through histogram analysis

Image histograms can similarly expose significant details regarding visual content. The distribution of pixel intensities is graphically represented in an image's histogram, allowing potential adversaries to draw concrete conclusions by evaluating the frequency of these intensity bins. Therefore, an image exhibiting a more uniform distribution of pixel intensities offers enhanced security. Prioritizing this uniform spread, a post-encryption histogram appears flat, thereby preventing the image from leaking structural details. Within this framework, we evaluated both the encrypted image and the PHR-embedded image using histogram analysis. **Figure 12** illustrates the histogram outcomes from tests conducted on both medical and natural images. As evidenced by the results, the intensity distributions for both the ciphered images and the PHR-concealed images exhibit a flat profile.

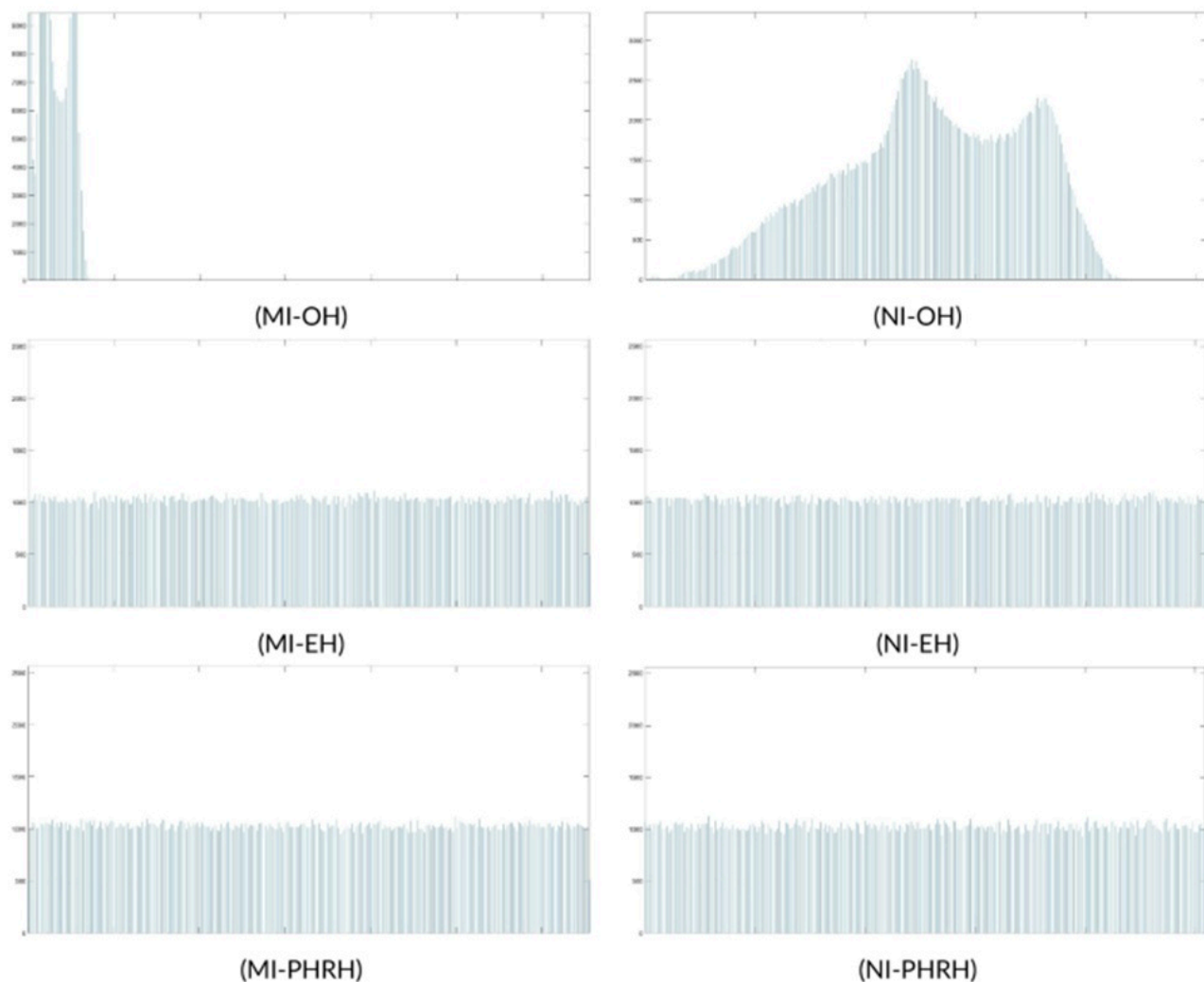


Figure 12. Histogram results of DICOM Medical image-1 (MI-OH, MI-EH, and MI-PHRH) and Natural image - Baboon (NI-OH, NI-EH, and NI-PHRH) [Figure (MI-OH), (NI-OH): histogram of original images, Figure (MI-EH), (NI-EH): histogram of encrypted images, and Figure (MI-PHRH), (NI-PHRH): histogram of images after hiding PHR information].

Correlation of pixels

The visual protection offered by the AdaBPE framework is further assessed by examining the correlation among adjacent pixels. This statistical dependency is quantified by pairing neighboring pixels across both horizontal and vertical dimensions. While the pixels within an unaltered image exhibit significant statistical self-similarity, this characteristic is nullified post-encryption. Consequently, the pixels in the resulting encrypted image are dissimilar. Visual security is assured when the image's pixels exhibit no mutual correlation. We evaluated the image correlations accordingly. **Figures 13 and 14** visually represent this correlation, demonstrating that the original image's pixels cluster toward ideality. Conversely, the pixels in both the ciphered image and the PHR-embedded image are highly dispersed, confirming the intended dissimilarity property.

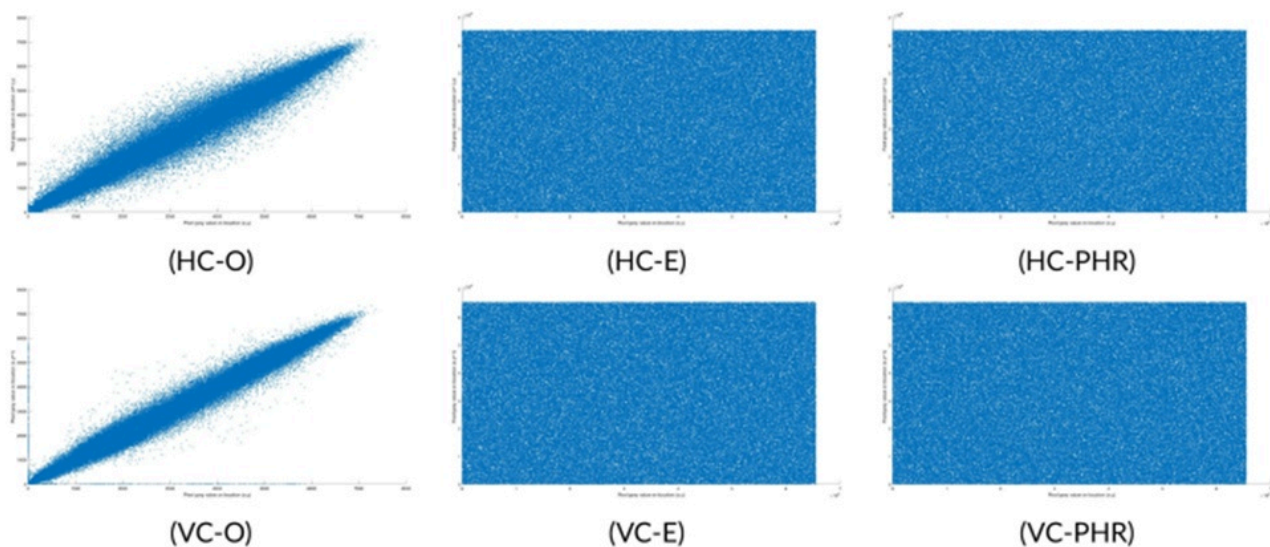


Figure 13. Correlation of adjacent pixels in DICOM Medical Image-1 (HC-O, HC-E, and HC-PHR: Horizontal correlation) and (VC-O, VC-E, and VC-PHR: Vertical correlation) [Figure (HC-O), (VC-O): correlation on original image, Figure (HC-E), (VC-E): correlation on encrypted image, and Figure (HC-PHR), (VC-PHR): correlation on image obtained after hiding PHR information].

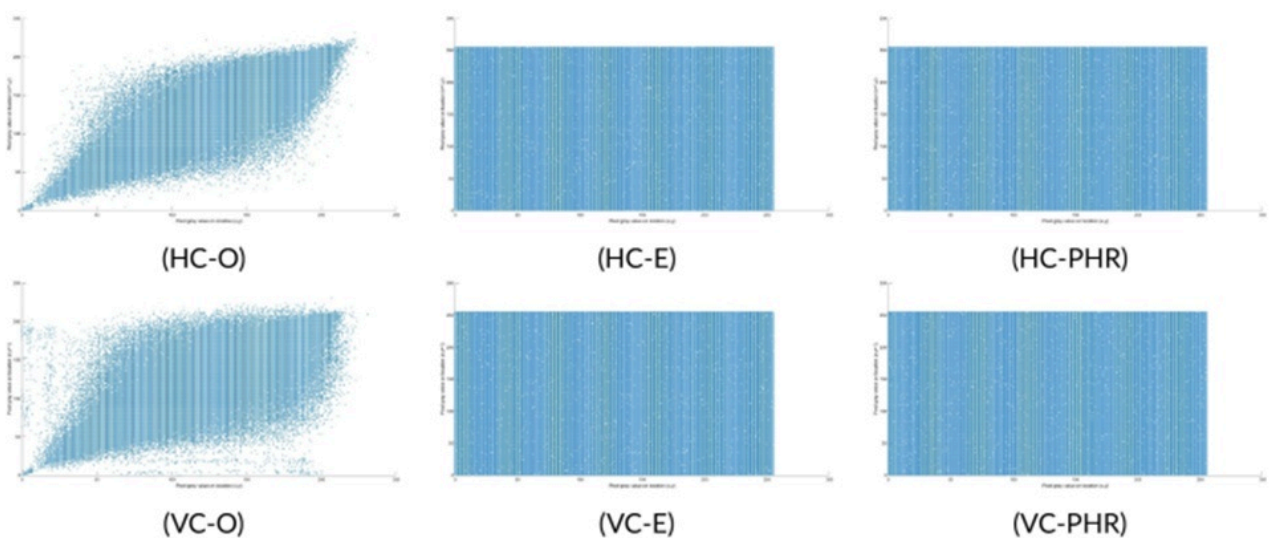


Figure 14. Correlation of adjacent pixels in the natural image - Baboon (HC-O, HC-E, and HC-PHR: Horizontal correlation) and (VC-O, VC-E, and VC-PHR: Vertical correlation) [Figure (HC-O), (VC-O): correlation on original image, Figure (HC-E), (VC-E): correlation on encrypted image, and Figure (HC-PHR), (VC-PHR): correlation on image obtained after hiding PHR information].

Quality of the recovered image

Restoring a medical image to its pristine quality remains a paramount concern in healthcare data transmission. An inaccurate clinical diagnosis could result from a degraded or noisy reconstruction. Therefore, RDH techniques applied to medical imagery must guarantee complete reversibility. The developed method is fully reversible, ensuring zero quality degradation in the reconstructed medical image. Experimental recovery quality is quantified using peak signal-to-noise

ratio (PSNR) and structured similarity index (SSIM). Both evaluation metrics assess the noise introduced into the image relative to the original baseline, making it essential to analyze these factors to verify flawless reversibility.

PSNR and SSIM

PSNR serves as a metric for peak error. It is defined as the ratio between the maximum gray level and the mean square error (MSE) factor. A minimized error factor correlates with superior recovered image fidelity. When the reconstructed image is identical to the original image, the error factor is 0, resulting in a PSNR of ∞ . In contrast to PSNR, SSIM operates as a perception-based quality estimator. The three components considered by SSIM that influence human visual perception are structure, luminance, and contrast. If the reconstructed image structurally matches the original cover image perfectly, the SSIM evaluates to 1. The calculated PSNR and SSIM metrics for four DICOM medical images and four natural images are detailed in [Tables 6 and 7](#), respectively. These figures clearly confirm that the AdaBPE methodology losslessly reconstructs the cover image after the complete embedded PHR data is extracted.

Table 6. PSNR and SSIM measured over four DICOM medical images.

Image	Block side-length	PSNR (dB)	SSIM
Medical Image-1	2	∞	1
	4	∞	1
	8	∞	1
	16	∞	1
	32	∞	1
Medical Image-2	2	∞	1
	4	∞	1
	8	∞	1
	16	∞	1
	32	∞	1
Medical Image-3	2	∞	1
	4	∞	1
	8	∞	1
	16	∞	1
	32	∞	1
Medical Image-4	2	∞	1
	4	∞	1
	8	∞	1
	16	∞	1
	32	∞	1

Table 7. PSNR and SSIM measured over four natural images.

Image	Block side-length	PSNR (dB)	SSIM
Airplane	2	∞	1
	4	∞	1
	8	∞	1
	16	∞	1
	32	∞	1
Baboon	2	∞	1
	4	∞	1
	8	∞	1
	16	∞	1
	32	∞	1
Boat	2	∞	1
	4	∞	1
	8	∞	1
	16	∞	1
	32	∞	1
Peppers	2	∞	1
	4	∞	1
	8	∞	1
	16	∞	1
	32	∞	1

Comparison With Other Similar RDH Schemes

This section provides a comparative analysis between the introduced AdaBPE methodology and other related RDH frameworks. **Table 8** presents a concise overview of these outcomes. Evaluations are conducted against the models detailed in [12, 22, 36-40]. The variable k in **Table 8** denotes the base of secret information. The statistics of **Table 8** demonstrate that the proposed technique is unique, achieving an exceptionally high embedding capacity within encrypted medical imagery. In addition to a substantial embedding rate, the introduced methodology flawlessly retrieves the original cover medical image without any deterioration, yielding a PSNR of infinity.

Table 8. Comparing other schemes on medical images [1].

Image Type	Metric	Proposed AdaBPE Scheme	[40]	[39] [k=3]	[12]	[38]	[22]	[37]	[36]
Medical Image-1	Embedded Information	1,052,883	962,360	786,432	262,144	131,072	262,144	262,144	585,225
	Embedding Rate	4.01	3.67	3	1	0.5	1	1	2.24
	PSNR	∞	∞	∞	∞	∞	∞	∞	∞
Medical Image-2	Embedded Information	1,563,648	1,043,960	786,432	262,144	131,072	262,144	262,144	585,225
	Embedding Rate	5.96	3.98	3	1	0.5	1	1	2.24
	PSNR	∞	∞	∞	∞	∞	∞	∞	∞
Medical Image-3	Embedded Information	1,508,823	1,039,880	786,432	262,144	131,072	262,144	262,144	585,225
	Embedding Rate	5.75	3.97	3	1	0.5	1	1	2.24
	PSNR	∞	∞	∞	∞	∞	∞	∞	∞
Medical Image-4	Embedded Information	1,468,788	1,041,920	786,432	262,144	131,072	262,144	262,144	585,225
	Embedding Rate	5.60	3.97	3	1	0.5	1	1	2.24
	PSNR	∞	∞	∞	∞	∞	∞	∞	∞

• Note: The bold values indicate the results of the proposed technique.

While all the benchmarked frameworks demonstrate strong embedding capabilities—though not on par with the proposed method—they fail to leverage lower-intensity pixels, with the exception of ref. [39]. A primary obstacle when processing extreme-intensity pixels during the data hiding stage is overflow and underflow. Ref. [39] successfully utilized the lowest intensities without encountering underflow issues, resulting in a substantial embedding rate. This scheme possesses high embedding and tamper detection functionality via a fragile watermark; however, the original cover image is interpolated before private information is embedded, which may lead to transmission bandwidth issues. The maximum possible embedding in ref. [37] is 1 bpp, similar to ref. [22], where the difference between MSBs of adjacent pixels is utilized for information hiding. In ref. [22], specific pixels are chosen for MSB difference expansion, which is tracked via a location map. Although this framework is separable and secured through homomorphic encryption, not every pixel is utilized. Its payload capacity can peak at 1 bpp, whereas the actual embedding on medical images documented in ref. [38] is 0.32 bpp. Because the size of the location map varies across different images, the effective payload correspondingly varies. Consequently, we have tabulated the aggregated embedding bits, which remain static across all images [131,072] for ref. [38] in Table 8. The system benefits from reduced computational complexity, as the encryption and embedding procedures rely on addition and subtraction computations. However, the application of a rhombus prediction pattern leaves half the pixels underutilized. In ref. [36], the Paillier cryptosystem mitigates overflow and underflow complications

during the embedding phase. Here, the embedding rate was improved by concealing binary patient data within every pixel of the cover image. Additionally, the scheme utilized fragile watermarking to authenticate the information at the receiver side. Despite the improved embedding, its primary disadvantage is executing the embedding process on an interpolated image, similar to ref. [39], which introduces bandwidth issues from a communication standpoint. Conversely, ref. [40] pre-processes the cover image using varying block dimensions and dual snake scan directions. This strategy enabled the RDH method to generate a substantial payload for each image, as the embedding count fluctuated with the scanning direction. The computational complexity here can be higher because the optimal block size is determined through a pre-processing step that evaluates multiple block sizes alongside a dual scanning process for each size.

The MSB prediction-based RDH scheme in ref. [12] provides a robust payload of 1 bpp; however, its methodology introduces a security flaw, as the runs of 1's utilized to distinguish the embedding block from the non-embedding block are detectable via histogram analysis of the 1's pattern [13]. Furthermore, while ref. [36] documented an impressive payload of 2.24 bpp, it must be noted that this figure is calculated based on the original image, even though the actual embedding is carried out on a scaled-up image. Our methodology diverges from previous techniques by employing all pixels based on prediction error, meaning there can never be an overflow or underflow. We determined that the higher bits of pixels within premium 16-bit DICOM images frequently remain underutilized. Consequently, we calculate the maximum amount of MSBs allowable for embedding within each block, resulting in variable embedding rates across different blocks. This strategy facilitated adaptive embedding and significantly elevated the hiding capacity. On average, we attained an embedding payload of 5.7067 bpp during tests encompassing 597 medical images, which comprised 497 CT, MR, and OT modality images from ref. [32] and 100 CT scans [33] acquired from the Cancer Imaging Archive [34]. **Table 9** outlines a feature comparison among the approaches utilized by various related RDH frameworks.

We further evaluated our methodology against several alternative strategies applied to natural images. **Table 10** summarizes the key comparative findings. As highlighted, the presented framework performs exceptionally well against its peers. The mean embedding capacity achieved through testing on 210 images from the USC-SIPI natural image dataset is 1.6769 bpp. Despite this strong embedding rate, it must be acknowledged that the method is unable to manage good results on highly textured images, as seen in **Figure 11**.

Table 9. Comparison of schemes based on the approaches.

RDH Approach	Separable Scheme	Method	Error in Data Recovery	Error in Image Recovery	Room Reserved
Approach in ref. [41]	No	Homomorphic encryption	No	No	Yes
Approach in ref. [36]	No	Interpolation based	No	No	Yes
Approach in ref. [40]	Yes	MSB prediction	No	No	Yes
Approach in ref. [38]	No	Rhombus prediction	No	No	Yes
Approach in ref. [37]	No	Homomorphic encryption	No	No	Yes
Approach in ref. [22]	Yes	MSB difference expansion	No	No	Yes
Approach in ref. [39]	No	Interpolation based	No	No	Yes
Approach in ref. [42]	Yes	MSB prediction	No	No	Yes
Approach in ref. [24]	Yes	MSB substitution	No	No	Yes

Approach in ref. [12] – CPE	Yes	MSB prediction	No	Yes	Yes
Approach in ref. [12] – EPE	Yes	MSB prediction	No	No	Yes
Approach in ref. [43]	Yes	MSB prediction	No	No	Yes
Approach in ref. [17]	Yes	Pixel difference histogram	No	No	Yes
Proposed AdaBPE Approach	Yes	MSB prediction	No	No	Yes

Table 10. Comparison with other RDH approaches on natural images.

RDH scheme	Peppers	Boat	Baboon	Airplane
Approach in ref. [20]	0.0312	0.0312	0.0312	0.0312
Approach in ref. [12]	0.9930	0.9913	0.8380	0.9926
Approach in ref. [26]	0.0625	0.0625	0.0625	0.0625
Approach in ref. [1]	0.4250	-	0.3650	0.4260
Approach in ref. [43]	0.4252	0.4252	0.4252	0.4252
Approach in ref. [44]	0.9903	0.9849	0.8842	0.9924
Approach in ref. [24]	0.8176	0.7527	0.2282	1.1581
Approach in ref. [42]	1.5111	1.2862	-	2.0230
Approach in ref. [17]	-	0.0989	0.0050	0.1595
Approach in ref. [45]	-	0.0665	0.0453	0.1514
Approach in ref. [46]	1.3595	-	0.9526	1.5691
Approach in ref. [38]	0.4633	0.4994	0.4542	0.4998
Proposed AdaBPE scheme	2.0892	1.7798	0.9641	2.0367

• Note: The bold values indicate the results of the proposed technique.

Analysing capability of recovery

The information receiver (IR) at the destination must regenerate the precise original medical image that was utilized as the cover medium to perform an accurate diagnosis. Therefore, the fidelity of the reconstructed medical imagery is given the highest priority. **Figure 7** illustrates sample visual outcomes, **Table 4** displays the entropy of the restored images, and **Table 6** details the PSNR and SSIM values of the recovered image, consistently reporting infinity and 1, respectively, for all images. These results provide evidence of the flawless reconstruction of the cover image upon reception, giving the AdaBPE methodology a completely reversible tag.

Time complexity analysis

This segment reveals both experimental and theoretical time complexity evaluations.

Experimental time complexity

We measured the processing time required to conceal the PHR payload within a medical image and the subsequent time needed to restore the original cover image by independently extracting the embedded PHR data. **Figure 15** plots the execution times evaluated across 50 randomly chosen DICOM images. It is evident that the duration of the embedding phase is significantly shorter compared to the restoration phase. When tested on 597 DICOM images utilizing a 16×16 pixel processing block, the mean execution times for the embedding and restoration stages were recorded at 0.428 s and 7.922 s, respectively. Naturally, the restoration duration is higher because both the embedded data and the cover image must be reconstructed. This disparity is further amplified because the embedding rate in the majority of the blocks within 16-bit DICOM formats is substantially high.

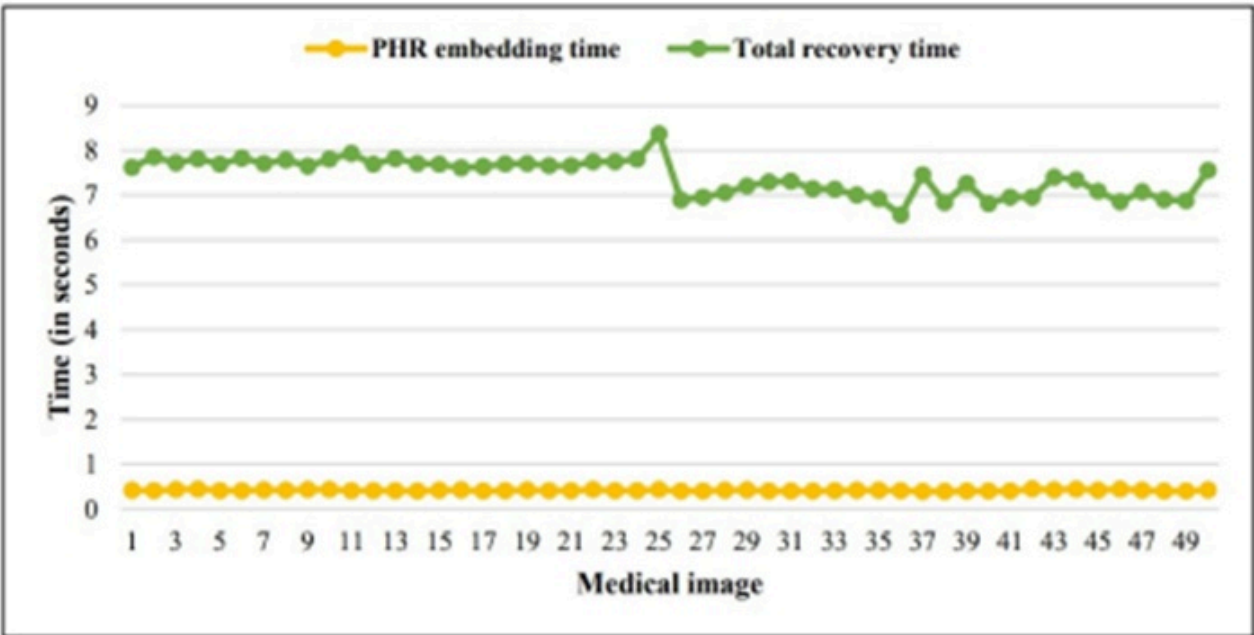


Figure 15. Time incurred during embedding and recovery phases on medical images.

Testing conducted on the USC-SIPI natural image repository yielded an overall mean embedding time of 0.187 s and an average recovery time of 0.726 s. Detailed metrics regarding the average embedding and restoration times across various image categories within the USC-SIPI dataset are provided in **Table 11**. Observations indicate that Textures images required the least processing time, whereas Sequences images consumed the maximum time. This difference stems primarily from the nature of the blocks. In highly textured images, neighboring pixels are not closely correlated; consequently, the MSB prediction error mechanism struggles to locate suitable blocks for embedding. As a result, fewer blocks carry supplementary data, which reduces the receiver-side computation time. Conversely, the pixels in sequence images are mostly smooth and highly correlated. Therefore, the majority of blocks are exploited for data embedding, leading to an increased restoration duration. It is important to note that the processing block dimension utilized for the experimental time evaluation on natural images was 4×4 pixels.

Table 11. Time analysis on USC-SIPI image dataset.

Image category	Recovery time (seconds)	Embedding time (seconds)	Total images
----------------	-------------------------	--------------------------	--------------

Aerials	0.76	0.19	38
Textures	0.44	0.16	64
Miscellaneous	0.85	0.20	39
Sequences	0.90	0.21	69

Theoretical time complexity

Within this subsection, we detail the theoretical time analysis for both the embedding and restoration phases.

The embedding workflow involves several distinct stages: calculating the MSB prediction error, forming a marker list, encrypting the cover image, safeguarding required LSBs, ciphering the supplementary data (PHR), integrating the LSBs with the encrypted PHR, inserting the marker list into the vacated LSBs, and ultimately hiding the preserved LSBs alongside the encrypted PHR data. The cover image is processed in consistently sized, non-overlapping blocks. Assuming the cover image dimensions are $M \times N$ pixels, computing the MSB prediction error requires a time complexity of $O(Z)$, where $Z = M.N$. Subsequent operations—such as generating the marker list, encrypting the image, preserving the LSBs, ciphering the additional information, and executing the data embedding—yield only constant time. Therefore, the total theoretical execution time for the embedding phase equates to $O(Z)$, where $Z = M.N$.

The recovery stage of the proposed framework entails retrieving the LSBs to compile the marker list, extracting the MSBs from the received image using the marker list, splitting the MSBs to isolate the PHR payload, decrypting the PHR data, restoring the correct LSBs, decrypting the image, and ultimately recovering the pixels via MSB prediction guided by the marker list. As evident, with the exception of the cover image recovery via the MSB prediction error methodology, all procedural steps require a constant amount of time. Given the image dimensions of $M \times N$ pixels, recovery via MSB prediction dictates that the entire recovery workflow operates at a theoretical time complexity of $O(Z)$, where $Z = M.N$.

Future Directions

This segment outlines the constraints of the current methodology and suggests avenues for future enhancements. The presented AdaBPE framework assumes an error-free and noiseless communication channel; therefore, it does not evaluate the scheme's versatility across diverse security models. Consequently, a primary future objective is to fortify the approach against noisy channels by addressing vulnerabilities linked to various security threats. Furthermore, the utilized prediction mechanism is inherently dependent on the cover image's MSBs. This reliance gives the methodology a competitive advantage regarding embedding payload in medical imagery, particularly within smoother images. This framework demonstrates optimal efficacy when neighboring pixels share strong correlations, evidenced by 380 DICOM images maximizing their payload using a 16×16 block configuration, compared to the 4×4 configuration required for natural images. Smaller block dimensions contain fewer pixels that generally exhibit high correlation, which facilitated the MSB prediction strategy. However, this restricts the volume of additional data that can be embedded within heavily textured images. Additionally, the current model relies on a single predictor pixel to estimate the remaining pixels within a square block of dimensions $A \times A$. While this design choice was implemented to maximize the embedding rate—proving highly successful for 16-bit DICOM formats—it performs inadequately on textured visuals. Therefore, developing a superior approach capable of handling textured blocks or images featuring continuous boundaries remains a vital area for future exploration.

Conclusion

We introduced an AdaBPE RDH framework for encrypted medical imagery, characterized by its unique property of embedding confidential patient records adaptively based on the nature of pixels within a given block. The embedding rate remains fixed for pixels inside a specific block but fluctuates across different blocks. The methodology relies on the MSB prediction error technique to embed private data and patient health records inside a medical image acting as the cover medium, and it proves its practical viability by losslessly reconstructing the original cover image after fully extracting the hidden data. This private information is embedded by substituting the MSB bits of the image's pixels. The framework's adaptive block-based embedding nature provides a substantial competitive edge, yielding a mean embedding payload of 5.7067 bpp across 597 premium 16-bit DICOM medical images, alongside a 1.6769 bpp average payload on 210 natural images. Consequently, this research introduces a highly capable RDH architecture within the encrypted domain, tailored specifically for high-capacity embedding in premium DICOM imagery. The documented experimental outcomes across multiple parameters establish this methodology as highly competent when evaluated alongside contemporary state-of-the-art approaches.

Acknowledgements

None

Conflict of interest

None

Financial support

This research work is supported by DST-SERB, India (File Number: TAR/2022/000,121), SRM University-AP, Andhra Pradesh, India; MRC, UK (MC_PC_17,171), Royal Society, UK (RP202G0230), the Hope Foundation for Cancer Research, UK (RM60G0680), GCRF, UK (P202PF11), the Sino-UK Industrial Fund, UK (RP202G0289), BHF, UK (AA/18/3/34220), LIAS, UK (P202ED10, P202RE969), the Data Science Enhancement Fund, UK (P202RE237), Fight for Sight, UK (24NN201); Sino-UK Education Fund, UK (OP202006); BBSRC, UK (RM32G0178B8).

Ethics statement

None

Received: 05 Sep 2021

Revised: 29 Oct 2021

Accepted: 22 Nov 2021

Published online: 15 March 2022

Rights and permissions

Open Access The author(s) retain copyright. This article is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. It may be shared and adapted for non-commercial purposes with appropriate attribution, an indication of changes, and distribution of adaptations under the same license. Third-party material may be subject to separate terms identified in its credit line. View the license at <https://creativecommons.org/licenses/by-nc-sa/4.0/>.

References

- Xie XZ, Chang CC, Chen K. A high-embedding efficiency RDH in encrypted image combining MSB prediction and matrix encoding for non-volatile memory-based cloud service. *IEEE Access*. 2020;8:52028-40.
<https://doi.org/10.1109/ACCESS.2020.2980302>.
- Chen F, Yuan Y, He H, Tian M, Tai HM. Multi-MSB compression based reversible data hiding scheme in encrypted images. *IEEE Trans Circuits Syst Video Technol*. 2020;31(3):905-16.
<https://doi.org/10.1109/TCSVT.2020.2992817>.
- Chowdhuri P, Jana B. Hiding data in dual color images reversibly via weighted matrix. *J Inf Secur Appl*. 2020;50:102420.
<https://doi.org/10.1016/j.jisa.2019.102420>.
- Tahiri MA, Bencherqui A, Karmouni H, Amakdouf H, Mirjalili S, Motahhir S, et al. Implementation of a steganography system based on hybrid square quaternion moment compression in IoMT. *J King Saud Univ Comput Inf Sci*. 2023;35(7):101604.
<https://doi.org/10.1016/j.jksuci.2023.101604>.
- Yang Y, Xiao X, Cai X, Zhang W. A secure and privacy-preserving technique based on contrast-enhancement reversible data hiding and plaintext encryption for medical images. *IEEE Signal Process Lett*. 2020;27:256-60.
<https://doi.org/10.1109/LSP.2020.2965826>.
- Panchikil S, Manikandan VM, Zhang Y, Wang S. A multi-directional pixel-swapping approach (MPSA) for entropy-retained reversible data hiding in encrypted images. *Entropy (Basel)*. 2023;25(4):563.
<https://doi.org/10.3390/e25040563>.
- Singh PK, Jana B, Datta K. Superpixel based robust reversible data hiding scheme exploiting Arnold transform with DCT and CA. *J King Saud Univ Comput Inf Sci*. 2022;34(7):4402-20.
<https://doi.org/10.1016/j.jksuci.2020.09.014>.
- Puteaux P, Ong SY, Wong KS, Puech W. A survey of reversible data hiding in encrypted images—the first 12 years. *J Vis Commun Image Represent*. 2021;77:103085.
<https://doi.org/10.1016/j.jvcir.2021.103085>.
- Sahu AK, Swain G. High fidelity based reversible data hiding using modified LSB matching and pixel difference. *J King Saud Univ Comput Inf Sci*. 2022;34(4):1395-409.
- Mondal J, Swain D, Panda DD. A novel LSB-based RDH with dual embedding for encrypted images. *Int J Electron Secur Digit Forensics*. 2019;11(3):281-93.
- Sahu M, Padhy N, Gantayat SS, Sahu AK. Shadow image based reversible data hiding using addition and subtraction logic on the LSB planes. *Sens Imaging*. 2021;22(1):7.
<https://doi.org/10.1007/s11220-020-00328-w>.
- Puteaux P, Puech W. An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images. *IEEE Trans Inf Forensics Secur*. 2018;13(7):1670-81.
- Dragoi IC, Coltuc D. On the security of reversible data hiding in encrypted images by MSB prediction. *IEEE Trans Inf Forensics Secur*. 2020;16:187-9.
- Sahu M, Padhy N, Gantayat SS, Sahu AK. Local binary pattern-based reversible data hiding. *CAAI Trans Intell Technol*. 2022;7(4):695-709.
<https://doi.org/10.1049/cit2.12130>.

Datta K, Jana B, Chakraborty MD. Two-layers robust data hiding scheme for highly compressed image exploiting AMBTC with difference expansion. *J King Saud Univ Comput Inf Sci*. 2022;34(8):5240-60.

Mukherjee S, Jana B. A novel method for high capacity reversible data hiding scheme using difference expansion. *Int J Nat Comput Res*. 2019;8(4):13-27.

Anushiadevi R, Amirtharajan R. Separable reversible data hiding in an encrypted image using the adjacency pixel difference histogram. *J Inf Secur Appl*. 2023;72:103407.
<https://doi.org/10.1016/j.jisa.2022.103407>.

Qiu Y, Qian Z, Zeng H, Lin X, Zhang X. Reversible data hiding in encrypted images using adaptive reversible integer transformation. *Signal Process*. 2020;167:107288.
<https://doi.org/10.1016/j.sigpro.2019.107288>.

Liu L, Wang A, Chang CC. Separable reversible data hiding in encrypted images with high capacity based on median-edge detector prediction. *IEEE Access*. 2020;8:29639-47.
<https://doi.org/10.1109/ACCESS.2020.2972736>.

Panchikkil S, Manikandan V, Zhang YD. A pseudo-random pixel mapping with weighted mesh graph approach for reversible data hiding in encrypted image. *Multimed Tools Appl*. 2022;81(12):1-29.

Bhardwaj R, Aggarwal A. An improved block based joint reversible data hiding in encrypted images by symmetric cryptosystem. *Pattern Recognit Lett*. 2020;139:60-8.

Anushiadevi R, Pravinkumar P, Rayappan JBB, Amirtharajan R. Uncover the cover to recover the hidden secret: a separable reversible data hiding framework. *Multimed Tools Appl*. 2021;80(13):19695-714.

Manikandan V, Amirtharajan R. A simple embed over encryption scheme for DICOM images using Bülban map. *Med Biol Eng Comput*. 2022;60(3):701-17.

Wang Y, Cai Z, He W. High capacity reversible data hiding in encrypted image based on intra-block lossless compression. *IEEE Trans Multimedia*. 2021;23:1466-73.
<https://doi.org/10.1109/TMM.2020.2999187>.

Panchikkil S, Manikandan V, Zhang YD. An efficient spatial transformation-based entropy retained reversible data hiding scheme in encrypted images. *Optik*. 2022;261:169211.

Panchikkil S, Vegesana SP, Manikandan VM, Donta PK, Maddikunta PKR, Gadekallu TR. An ensemble learning approach for reversible data hiding in encrypted images with Fibonacci transform. *Electronics*. 2023;12(2):450.
<https://doi.org/10.3390/electronics12020450>.

Mohammadi A, Nakhkash M, Akhaee MA. A high-capacity reversible data hiding in encrypted images employing local difference predictor. *IEEE Trans Circuits Syst Video Technol*. 2020;30(8):2366-76.
<https://doi.org/10.1109/TCSVT.2020.2990952>.

Malik A, Wang HX, Chen Y, Khan AN. Reversible data hiding in encrypted image based on prediction-error estimation and location map. *Multimed Tools Appl*. 2020;79(17-18):1-24.
<https://doi.org/10.1007/s11042-019-08460-w>.

Yu C, Zhang X, Zhang X, Li G, Tang Z. Reversible data hiding with hierarchical embedding for encrypted images. *IEEE Trans Circuits Syst Video Technol*. 2021;32(2):451-66.
<https://doi.org/10.1109/TCSVT.2021.3062947>.

Sahu AK, Sahu M, Patro P, Sahu G, Nayak SR. Dual image-based reversible fragile watermarking scheme for tamper detection and localization. *Pattern Anal Appl*. 2023;26(2):571-90.

<https://doi.org/10.1007/s10044-022-01104-0>.

Datta K, Jana B, Singh P, Dalui M. Robust data hiding scheme for highly compressed image exploiting BTC with Hamming code. *Multimed Tools Appl*. 2023;83(3):1-38.

<https://doi.org/10.1007/s11042-023-15727-w>.

DICOM. Image database [Internet]. [cited 2022 Apr 1]. Available from: <https://www.dicomlibrary.com/>

Albertina B, Watson M, Holback C, Jarosz R, Kirk S, Lee Y, et al. Radiology data from the Cancer Genome Atlas Lung Adenocarcinoma [TCGA-LUAD] collection. The Cancer Imaging Archive. 2016.

Clark K, Vendt B, Smith K, Freymann J, Kirby J, Koppel P, et al. The Cancer Imaging Archive (TCIA): maintaining and operating a public information repository. *J Digit Imaging*. 2013;26(6):1045-57.

<https://doi.org/10.1007/s10278-013-9622-7>.

USC. Image database [Internet]. [cited 2022 Apr 1]. Available from: <http://sipi.usc.edu/database/>

Bhardwaj R. Enhanced reversible and secure patient data hiding algorithm based on cellular automata. *Multimed Tools Appl*. 2022;81(30):44363-81.

<https://doi.org/10.1007/s11042-022-12501-2>.

Wu X, Chen B, Weng J. Reversible data hiding for encrypted signals by homomorphic encryption and signal energy transfer. *J Vis Commun Image Represent*. 2016;41:58-64.

<https://doi.org/10.1016/j.jvcir.2016.09.005>.

Anushiadevi R, Amirtharajan R. Design and development of reversible data hiding-homomorphic encryption and rhombus pattern prediction approach. *Multimed Tools Appl*. 2023;82(30):1-24.

<https://doi.org/10.1007/s11042-023-15455-1>.

Bhardwaj R. An enhanced reversible patient data hiding algorithm for E-healthcare. *Biomed Signal Process Control*. 2021;64:102276.

<https://doi.org/10.1016/j.bspc.2020.102276>.

Panchikkil S, Manikandan V. A prediction error based reversible data hiding scheme in encrypted image using block marking and cover image pre-processing. *Multimed Tools Appl*. 2024;83(2):1-38.

Chen YC, Shiu CW, Horng G. Encrypted signal-based reversible data hiding with public key cryptosystem. *J Vis Commun Image Represent*. 2014;25(5):1164-70.

Wang Y, He W. High capacity reversible data hiding in encrypted image based on adaptive MSB prediction. *IEEE Trans Multimedia*. 2022;24:1288-98.

Chen K, Chang CC. Real-time error-free reversible data hiding in encrypted images using (7, 4) Hamming code and most significant bit prediction. *Symmetry*. 2019;11(1):51.

Huang D, Wang J. High-capacity reversible data hiding in encrypted image based on specific encryption process. *Signal Process Image Commun*. 2020;80:115632.

<https://doi.org/10.1016/j.image.2019.115632>.

Yang CH, Weng CY, Chen JY. High-fidelity reversible data hiding in encrypted image based on difference-preserving encryption. *Soft Comput*. 2022;26(4):1727-42.

<https://doi.org/10.1007/s00500-022-06745-1>.

Chen KM, Chang CC. High-capacity separable reversible data-hiding method in encrypted images based on block-level encryption and Huffman compression coding. *Connect Sci*. 2021;33(4):975-94.

<https://doi.org/10.1080/09540091.2021.1926930>.