IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 8 October 2023, accepted 7 November 2023, date of publication 20 November 2023,
date of current version 6 December 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3335172

RESEARCH ARTICLE

Robust and Secure Medical Image Watermarking for Edge-Enabled e-Healthcare

PRIYANKA SINGH[1], K. JYOTHSNA DEVI[2], HIREN KUMAR THAKKAR[3], MUHAMMAD BILAL[4], (Senior Member, IEEE), ANAND NAYYAR[5], (Senior Member, IEEE), AND DAEHAN KWAK[6], (Member, IEEE)

[1]Department of Computer Science and Engineering, SRM University AP, Guntur, Andhra Pradesh 522502, India
[2]Department of Computer Science and Engineering, PVPSIT, Vijayawada, Andhra Pradesh 520008, India
[3]Department of Computer Engineering, Pandit Deendayal Energy University, Gujarat 382007, India
[4]School of Computing and Communications, Lancaster University, LA1 4WA Lancaster, U.K.
[5]School of Computer Science, Faculty of Information Technology, Duy Tan University, Danang 550000, Vietnam
[6]Department of Computer Science and Technology, Kean University, Union, NJ 07083, USA

Corresponding author: Daehan Kwak (dkwak@kean.edu)

ABSTRACT Advancements in networking technologies have enabled doctors to remotely diagnose and monitor patients using the Internet of Medical Things (IoMT), telemedicine, and edge-enabled healthcare. In e-healthcare, medical reports and patient records are typically outsourced to a server, which can make them vulnerable to unauthorized access and tampering. Therefore, it is crucial to ensure the authorization, security, confidentiality, and integrity of medical data. To address these challenges, this paper proposes a novel reversible watermarking approach with a high payload and low computational cost. First, the input medical image is divided into a Border region (BR) and a Non-Border region (NBR). The NBR region is upscaled using Neighbour Mean Interpolation (NMI) to ensure reversibility. The Electronic Patient Record (EPR) is encrypted using a pseudorandom key, which is generated adaptively from the host medical image and the Enigma machine. The encrypted EPR is then embedded in the medical image using NMI. Two levels of tamper detection (global and local) are performed at the receiver's end for higher accuracy. A Global Integrity Code is generated and embedded in BR using LSB embedding technique for global tamper detection. The experimental results show that the visual quality and robustness are both high (Avg. PSNR = 41.03 dB and Avg. SSIM = 0.99, NC = 0.99, and BER = 0.0019 calculated for 100 images). The subjective and objective experimental analysis indicates that the proposed scheme is highly secure and the computational cost is also low. The average embedding and extraction time (including embedding, encryption and decryption, extraction process respectively) is 0.88 s and 0.83 s. It is resistant to various image processing attacks. A comparison with some of the most recent popular schemes confirms the scheme's effectiveness.

INDEX TERMS e-healthcare, edge-enabled healthcare, interpolation, IoMT, medical image watermarking, pseudorandom key, reversible data hiding, reversible watermarking scheme.

I. INTRODUCTION

In the past decade, e-healthcare and mobile healthcare solutions have become integral components of efficient healthcare service delivery worldwide. Numerous "smart healthcare" solutions have been designed to support real-time and continuous healthcare services. With easy and affordable access to Internet services, an increasing number of hospitals and healthcare centers are now interconnected for instant and rapid transmission of healthcare data [1]. The recent pandemic has mandated both developed and developing countries to innovate the exchange of data and maintain efficient healthcare delivery without compromising the standards of healthcare service. However, the electronic exchange of patients' healthcare data is subject to external attacks and may expose crucial patient health-related information to

The associate editor coordinating the review of this manuscript and approving it for publication was Larbi Boubchir.

third parties [2]. In several countries, healthcare services are highly distributed, with different entities providing different health services. For instance, diagnostic laboratories only generate the reports such as X-rays, CT scans, MRIs, and the hospitals provide the treatment based on the health reports [3]. In such circumstances, patients' health reports are transferred electronically from diagnostic laboratories to hospitals via a public network. The typical distributed healthcare infrastructure is shown in Figure. 1. Let N be the number of diagnostic laboratories defined as $D = \{d_1, d_2, \ldots., d_N\}$ and M be the number of hospitals defined as $H = \{h_1, h_2, \ldots, h_M\}$ in a given city. It is assumed that each diagnostic laboratory $d_i \in D$ and hospital $h_j \in H$ comprise numerous edge devices and a corresponding edge server e_i and e_j, respectively. Diagnostic laboratories connect to hospitals via cloud data centers using 5G public communication networks, where data transferred by diagnostic laboratories are stored in the cloud data centers and retrieved by hospitals on an as-needed basis. Any data transfer from diagnostic laboratories to the cloud data center, and from the cloud data center to hospitals, takes place via 5G public networks, which are highly unreliable. In contrast, health data transfer within the hospital/diagnostic laboratory is more secure since it is on a private network [4], [5], [6]. It is assumed that diagnostic laboratories and hospitals are equipped with several edge devices, such as X-ray machines, CT scans, CCTV cameras, and edge servers. Without loss of generality, it is considered that the edge devices have the least computational power and are a primary source of data generation, edge servers have adequate computational power, and cloud data servers have abundant computational power [7]. Moreover, edge devices have the least data storage capacity, edge servers have adequate storage capacity, and cloud data servers have theoretically infinite storage capacity.

The Electronic Patient Record (EPR) and medical images carry valuable patient information, and their secure transmission over public networks is highly essential and an integral part of overall healthcare delivery. However, public networks are susceptible to external attacks, and attackers may tamper with and manipulate crucial health information, leading to an inaccurate diagnosis and subsequent incorrect medical treatment, risking the patient's life. To protect the identity of patients and detect potential tampering of medical images, medical image watermarking (MIW) and data encoding techniques are employed. However, most existing MIW and encoding techniques are either computationally intensive or unsuitable for the medical image domain [8], [9], [10], [11]. The proposed scheme offers a two-fold solution: 1) a low-cost and highly secured watermark embedding cum encryption scheme that supports the computational powers of edge devices and edge servers, and 2) higher accuracy in tamper detection and recovery at a low computational cost. The secured transmission of healthcare information over the public healthcare infrastructure is illustrated in Figure 1.

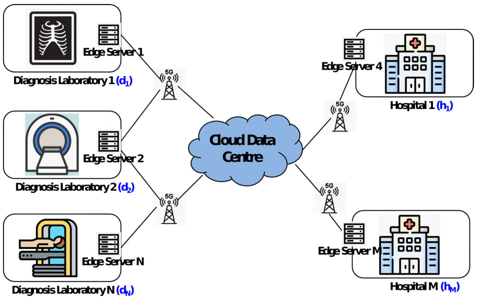


FIGURE 1. Edge-enabled healthcare infrastructure.

A. OBJECTIVES OF THE PAPER

1) To conduct the background study with regard to the secure medical image transmission in e-healthcare applications like IoMT. And also to identify image transmission issues through cloud servers.
2) To propose a novel methodology, 'Robust and Secure Medical Image Watermarking for Edge-Enabled E-Healthcare,' to resolve the image transmission issues over cloud servers via edge-servers and minimize computational cost.
3) To test and validate the proposed methodology using various performance metrics such as PSNR, SSIM, NC, BER, CC, entropy, computational time, and embedding capacity.
4) To compare the performance of the proposed methodology with existing techniques such as Gull et al. [33], Bhardwaj [34], Geetha and Geetha [35], Huang et al. [36], Showkat et al. [38], Parah et al. [39], Bamal and Kasana [54], and Bamal and Kasana [55].

B. ORGANIZATION OF THE PAPER

Section II presents a literature review. Section III elucidates the proposed scheme. Section IV focuses on experimentation, results, and discussion. Finally, Section V concludes the paper and discusses future scope.

II. LITERATURE REVIEW

Cloud and edge computing have revolutionized the medical healthcare arena. Now, medical data, including medical images and Electronic Patient Records (EPR), can be securely transmitted through edge devices to edge servers and from edge servers to cloud servers. Medical image watermarking is widely used for the secure transmission of medical data. It ensures the authentication, confidentiality, integrity, and security of medical data. Many researchers have investigated the role of MIW, yielding substantial results. Schemes proposed in [12], [13], [20], and [22] explored conventional transform domain watermarking schemes for high imperceptibility and robustness in medical image transmission [14], [18], [19], [21]. Generally, transform domain watermarking schemes have a high computational cost. But, for real-time e-healthcare applications like IoMT, edge, cloud-based communications, computational cost is the major concern.

Some researchers have suggested reversible watermarking schemes for medical images in both the spatial and transform domains [23], [24], [25], [26], [27], [28], [30], [31], [32], [33], [34], [36], [38], [39]. Reversible watermarking schemes (RWS) allow for the lossless restoration of medical images while mitigating security risks. Additionally, they provide high imperceptibility, robustness, embedding capacity, and lossless recovery of medical images.

RWS are generally performed using histogram shifting [25], [26], [36], [38], compression [27], [33], pixel value difference (PVD) expansion [34], [35], [39], [44], and transform techniques [28], [30], [31], [32]. Various histogram shifting techniques, such as median histogram shifting [36], contrast stretching [38], zero or minimum points of the histogram [25], and local histogram shifting [26], have been explored by researchers for RWS. Histogram shifting recovers the original image but requires extra data for lossless recovery, resulting in increased computational overhead for lossless recovery. Schemes proposed in [33] and [27] use compression techniques to reduce file size and increase data transfer rate over the internet, but they have significant computational drawbacks, such as latency and dictionary overhead. Also, RWS that use compression provide reversibility to only a portion of the medical image (ROI), where medical images are divided into Region of Interest (ROI) and Region of Non-Interest (RONI) segments [40]. The schemes proposed in [24], [34], [35], [39], and [44] utilize PVD for lossless recovery with low computational cost. A weighted interpolation process was proposed in [24], and pixel adjustment was suggested to avoid overflow and underflow conditions during embedding [34]. Rhombus mean interpolation technique was used by [35]. The Left Data Mapping (LDM) and Pixel Repetition Method (PRM) approaches are used in [39]. Modified neighbour mean interpolation (MNMI) is proposed in [44] for embedding. RWS in [28], [30], [31], and [32] had achieved high robustness and imperceptibility, by using transforms for reversibility such as IWT [28], [29], SLT transform [30], DWT [31], and DCT+DWT+SVD [32] making it computationally expensive. It is observed that interpolation based RWS have comparatively less computational cost.

One of the most important requirements for medical image transmission is integrity (tamper detection and recovery), which ensures that the receiver has received an intact medical image. The schemes proposed in [13], [15], [16], [24], [25], [26], [28], [30], [31], [32], [33], [34], [36], and [37] had achieved high imperceptibility but fall short in ensuring integrity. Localized tamper detection and recovery techniques had been implemented in [12], [23], [27], and [35] to ensure integrity. However, improvement is required in terms of tamper detection and recovery accuracy. Schemes proposed in [12], [23], [27], [35], [38], and [39] embed tamper detection, localization, and recovery information in medical images. These schemes improve imperceptibility and embedding capacity at the expense of robustness and high computational cost. EPR watermark confidentiality and security are also important for applications such as e-healthcare, IoMT, and Telemedicine services. However, watermark security is undervalued in the majority of MIW schemes. The schemes presented in [24], [25], [26], [27], [28], [30], [31], [32], and [33] are less focused on watermark security. A chaotic map was used for watermark security in [13] and [17], but the chaotic map had a problem with the hyper-tuning parameter. Despite the fact that the schemes presented in [13], [34], and [39] have achieved high imperceptibility and security, they had a high computational cost.

A. MOTIVATION AND CONTRIBUTION OF THE PROPOSED SCHEME

According to the literature review, there has been a significant amount of research on using the MIW technique for the secure transmission of medical images over the Internet. However, there are several issues that must be addressed, such as EPR security, achieving a good balance between watermarking characteristics (imperceptibility, robustness, embedding capacity) and integrity, with low computational cost.

B. MAJOR CONTRIBUTIONS OF THE PROPOSED SCHEME

This paper proposes a novel region-based lossless RWS scheme for medical images in the spatial domain that employs interpolation and MIW techniques to provide high EPR security and integrity at a low computational cost.

1) LOW COMPUTATIONAL COST

The proposed scheme ensures low computational time by employing embedding in the spatial domain through interpolation and EPR encryption using the Enigma machine and arithmetic operations. Additionally, the scheme proposes a two-level tamper detection approach consisting of global followed by local tamper detection, which helps to reduce the computational burden.

2) HIGH SECURITY

It ensures EPR security by encrypting and decrypting it using a strong and unique Pseudo-random Key ($\mathcal{PR}_{Key}$), which is adaptively generated from the host image and difficult to crack. The encrypted EPR (EPR') is then embedded in the Non-Border Region using interpolation to prevent EPR detachment.

3) HIGH TAMPER DETECTION AND RECOVERY ACCURACY

An ingenious block checksum computation mechanism is implemented for internal tamper detection, localization, and recovery in a 3 × 3 NBR block. The proposed scheme has achieved more than 99% accuracy in tamper detection and preserves the perceptual quality of the watermarked and recovered medical images.

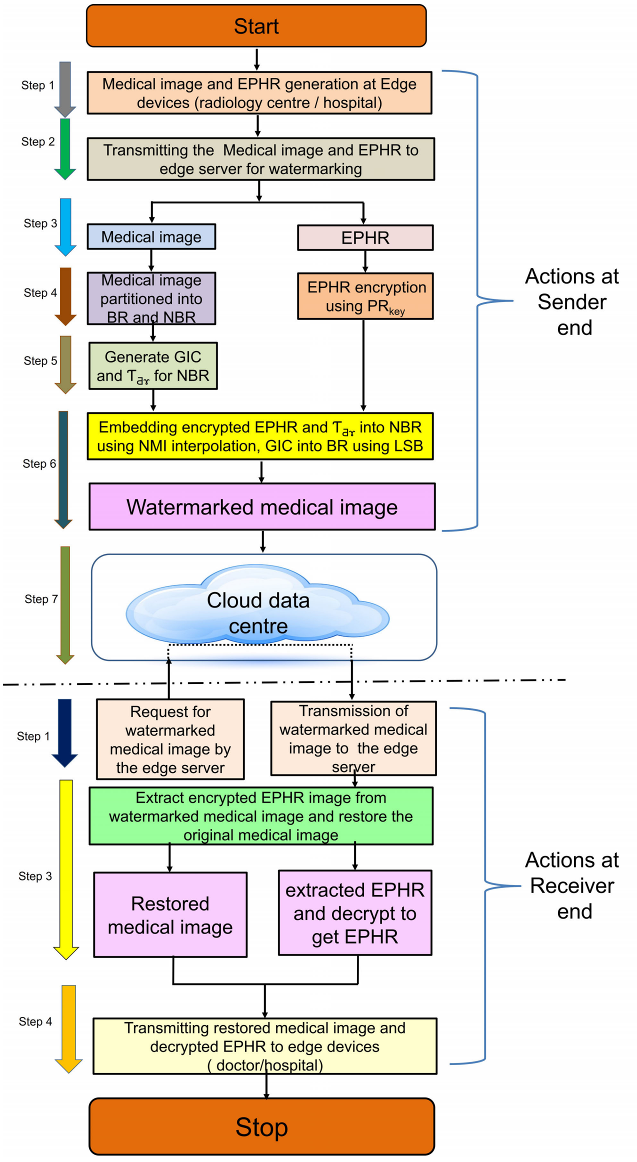

Start
Step 1
Medical image and EPHR generation at Edge devices (radiology centre / hospital)
Step 2
Transmitting the Medical image and EPHR to edge server for watermarking
Step 3
Medical image
EPHR
Step 4
Medical image partitioned into BR and NBR
EPHR encryption using PR_{key}
Step 5
Generate GIC and $T_{\partial\gamma}$ for NBR
Step 6
Embedding encrypted EPHR and $T_{\partial\gamma}$ into NBR using NMI interpolation, GIC into BR using LSB
Watermarked medical image
Actions at Sender end
Step 7
Cloud data centre
Step 1
Request for watermarked medical image by the edge server
Transmission of watermarked medical image to the edge server
Step 3
Extract encrypted EPHR image from watermarked medical image and restore the original medical image
Restored medical image
extracted EPHR and decrypt to get EPHR
Actions at Receiver end
Step 4
Transmitting restored medical image and decrypted EPHR to edge devices (doctor/hospital)
Stop

FIGURE 2. Flow graph of the proposed edge-enabled scheme.

4) HIGH EMBEDDING CAPACITY

The proposed scheme has a high embedding capacity of 2 bpp and an average PSNR of approximately 40 dB, while preserving the reversibility of the host medical image.

III. PROPOSED SCHEME

This paper proposes a region-based reversible MIW technique to ensure medical image authentication, integrity, confidentiality, and security with high imperceptibility and robustness. The medical host image ($\mathcal{H}_{img}$) of size $\mathcal{A} \times \mathcal{B}$ is first partitioned into the Border Region (BR) and the Non-Border Region (NBR). After medical image partitioning, a Global Integrity Code (GIC) is generated for the NBR and embedded in the BR pixels' Least Significant Bit (LSB) position. The flow graph of the proposed scheme is shown in Figure 2.

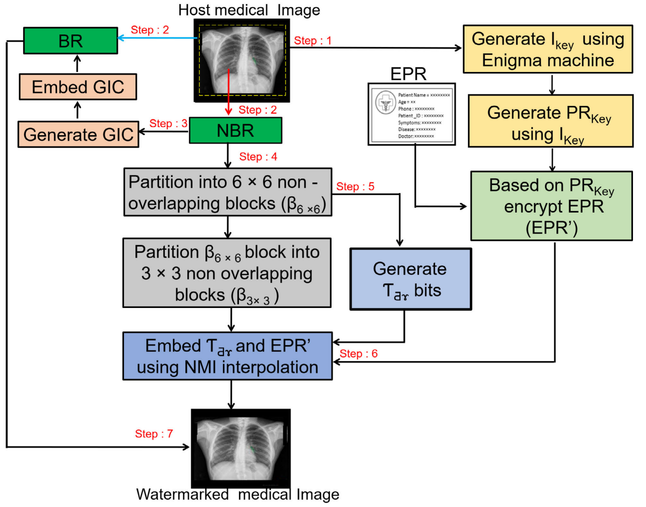

Host medical Image
BR
Step : 2
Step : 1
Generate I_{key} using Enigma machine
Embed GIC
EPR
Generate PR_{Key} using I_{Key}
Generate GIC
Step : 3
NBR
Step : 2
Step : 4
Partition into 6 × 6 non - overlapping blocks ($\beta_{6\times6}$)
Step : 5
Based on PR_{Key} encrypt EPR (EPR')
Partition $\beta_{6\times6}$ block into 3 × 3 non overlapping blocks ($\beta_{3\times3}$)
Generate $T_{\partial\gamma}$ bits
Embed $T_{\partial\gamma}$ and EPR' using NMI interpolation
Step : 6
Step : 7
Watermarked medical Image

FIGURE 3. Block diagram of the proposed embedding process.

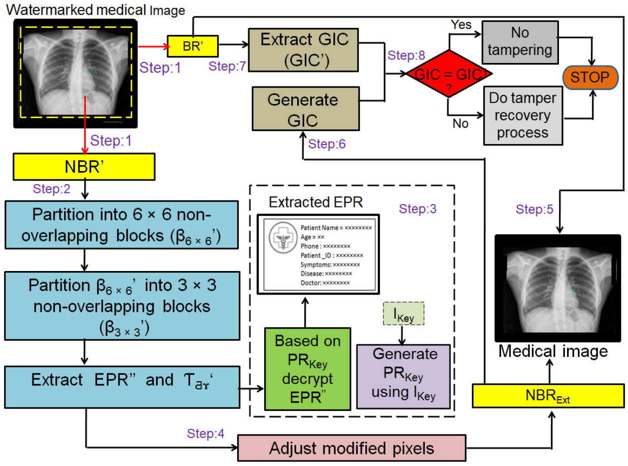

Watermarked medical Image
BR'
Step:1
Step:7
Extract GIC (GIC')
Step:8
GIC = GIC' ?
Yes
No tampering
STOP
No
Do tamper recovery process
Generate GIC
Step:6
Step:1
NBR'
Step:2
Partition into 6 × 6 non-overlapping blocks ($\beta_{6\times6}$')
Partition $\beta_{6\times6}$' into 3 × 3 non-overlapping blocks ($\beta_{3\times3}$')
Extract EPR'' and $T_{\partial\gamma}$'
Extracted EPR
Step:3
I_{Key}
Based on PR_{Key} decrypt EPR''
Generate PR_{Key} using I_{Key}
Step:5
Medical image
NBR_{Ext}
Step:4
Adjust modified pixels

FIGURE 4. Block diagram of the proposed extraction process.

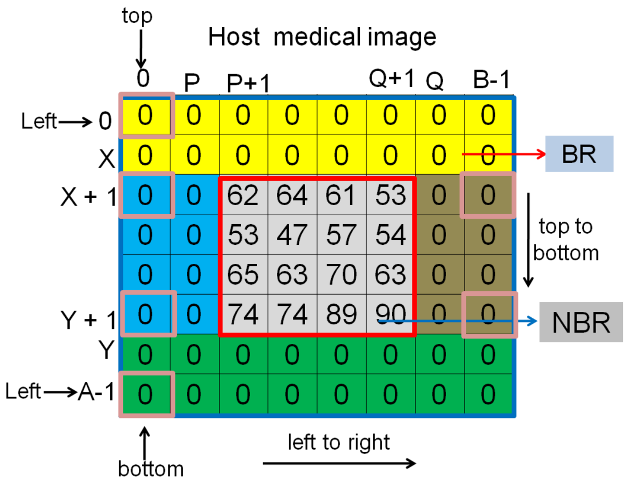
Then, the EPR' of size $\mathcal{C} \times \mathcal{D}$ and block-wise tamper detection and recovery bits ($\mathcal{T}\mathfrak{d}\gamma$) are embedded in the interpolated 3×3 NBR block using Neighbor Mean Interpolation (NMI). The watermarked NBR and BR are combined to produce the watermarked medical image ($\mathcal{H}_{img}'$). The watermarks are extracted from $\mathcal{H}_{img}'$ for authentication, tamper detection, and recovery. Block diagrams of the proposed watermark embedding and extraction process (for BR and NBR) are shown in Figures 3 and 4, respectively. The proposed scheme is described as follows:

A. BR AND NBR PARTITIONING

In region-based MIW, most researchers have suggested automated or manual partitioning of $\mathcal{H}img$ into ROI and RONI [42], [43]. However, automated partitioning methods are computationally expensive, modality-specific, and less accurate, while manual partitioning requires human effort. Additionally, some medical images, such as ultrasounds,

TABLE 1. Acronym used in this paper and corresponding meaning.

Acronym	Meaning	Acronym	Meaning
$\mathcal{H}_{img}$	Medical host image	GIC	Global Integrity Code
$\mathcal{A} \times \mathcal{B}$	Size of $\mathcal{H}_{img}$	I_{key}	Intermediate key
BR	Border region of $\mathcal{H}_{img}$	$(\mathcal{PR}_{Key})$	Pseudorandom key
NBR	Non border region of $\mathcal{H}_{img}$	NBR'	Watermarked NBR
EPR'	Patient Healthcare Record	IBL	3 × 3 Interpolated block
$\mathcal{C} \times \mathcal{D}$	Size of EPR	NBR_{Ext}	Recovered NBR at receiver end
$\mathcal{T}\mathfrak{d}\gamma$	Block wise tamper detection and recovery bits	GIC''	Generated GIC from NBR_{Ext}
NMI	Neighbor mean interpolation	GIC'	extracted GIC from watermarked BR
$\mathcal{H}_{img}'$	Watermarked medical image	$\beta_{3\times3}$	NBR 3 × 3 non-overlapping block



	0	P	P+1			Q+1	Q	B-1
0	0	0	0	0	0	0	0	0
X	0	0	0	0	0	0	0	0
X + 1	0	0	62	64	61	53	0	0
	0	0	53	47	57	54	0	0
	0	0	65	63	70	63	0	0
Y + 1	0	0	74	74	89	90	0	0
Y	0	0	0	0	0	0	0	0
A-1	0	0	0	0	0	0	0	0

FIGURE 5. BR and NBR partitioning.

X-rays, and CT images, have a larger ROI compared to RONI. Region-based approaches usually fail to embed watermarks in such types of images. Determining the precise ROI boundaries is also a challenge in region-based MIW. Handling multiple ROIs is not feasible using the latter approach. To address these issues, the proposed scheme partitions $\mathcal{H}img$ into BR and NBR parts, as shown in Figure 3.

Steps for partitioning $\mathcal{H}_{img}$ into BR and NBR:

1) TOP BORDER

Scan $\mathcal{H}img$ from the top-left corner pixel (0,0) to the top-right corner pixel in a raster fashion. Add the rows that have all zero-intensity pixels to the BR until a non-zero pixel is encountered. If a non-zero pixel is encountered in row $X + 1$, then stop scanning, and consider rows from 0 to X as the top border region.

2) BOTTOM BORDER

Scan $\mathcal{H}img$ starting from the bottom-left corner pixel to the bottom right-most pixel in a bottom-to-top fashion. Add rows with all zero-intensity pixels to the BR until a non-zero pixel is encountered. If a non-zero pixel is encountered in row $Y+1$, then stop scanning, and consider rows from Y to $A - 1$ as the bottom border.

3) LEFT BORDER

Scan columns from the pixel position $(X + 1, 0)$ to $(Y + 1, 0)$ in a top-to-bottom fashion. Similarly, scan columns from left to right. Add the columns having all pixel intensities as zero to the left border. If a non-zero pixel is encountered in column $P + 1$, then stop scanning and consider columns 0 to P as the left border.

4) RIGHT BORDER

Scan columns from $(X + 1, B - 1)$ to $(Y + 1, B - 1)$ pixel in a top-to-bottom fashion. Similarly, scan columns from right to left. Add the columns having all pixel intensities as zero to the right border. If a non-zero pixel is encountered in column $Q + 1$, then stop scanning and consider columns Q to $B - 1$ as the right border.

The partitioning of BR and NBR from $\mathcal{H}_{img}$ using the above steps is shown in Figure 5. The proposed approach for BR and NBR partitioning has the advantage of not requiring any ROI selection procedure or side information regarding ROI coordinates, making it easy to handle multiple ROIs. This approach can be applied to a wide range of image modalities, regardless of whether they have a larger ROI or not. After the partitioning of the medical host image, the GIC is generated as detailed in the following subsection.

B. GLOBAL INTEGRITY CODE (GIC) GENERATION

In the proposed scheme, the GIC is used for global tamper detection in the NBR. To generate the GIC, the NBR is divided into 4 × 4 non-overlapping blocks. If the size of the last NBR block is less than 4 × 4, zero padding is applied to the block to make its size 4 × 4. The pixel values in these 4 × 4 non-overlapping blocks represent the gray intensity level, ranging from 0 to 255. For each block, the summation of pixels (S) is calculated. A modulus operation is performed on S of each block so that the S value falls within the range of 0 to 255. This is followed by conversion into the equivalent binary format (8-bit integer). Furthermore, this 8-bit binary number is converted to its 2's complement, and its decimal equivalent is calculated. The cumulative sum (CS) of Dec for all 4 × 4 non-overlapping NBR blocks is computed. Then, CS is converted to the equivalent 32-bit binary format. The resulting 32-bit binary number is the GIC. To facilitate global tamper detection at the receiver, a 32-bit GIC is generated for

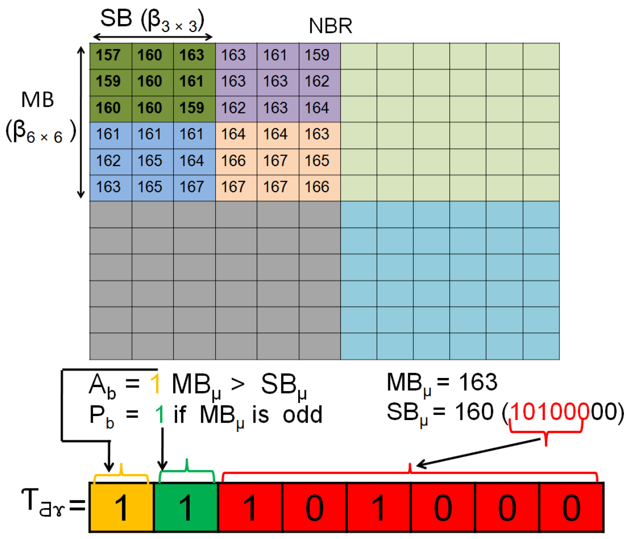


FIGURE 6. 8-bit $\mathcal{T}_{\eth\gamma}$ generation.

the NBR and then embedded into the BR. The algorithmic steps for generating the 32-bit GIC are shown in Algorithm 1.

```
Algorithm 1 Global Integrity Code (GIC) Generation:
Require: NBR
Ensure: GIC of size 32 bits
  Partition the NBR into 4 × 4 non-overlapping blocks.
  for each 4 × 4 non-overlapping NBR blocks do
      Calculate sum of pixel values of each 4 × 4 block (S).
      $M = (S\%255)_2$
      $Bin$ = 2's complement of $M$
      $Dec = (Bin)_{10}$
  end for
  Take cumulative sum (CS) of D for all
  4 × 4 non-overlapping NBR blocks.
  Convert CS to equivalent 32-bit binary format to get final GIC.
```

C. TAMPER DETECTION AND RECOVERY BITS ($\mathcal{T}_{\mathfrak{D}\gamma}$) GENERATION

In the proposed scheme, $\mathcal{T}_{\eth\gamma}$ bits are used for tamper localization and recovery of NBR. To generate $\mathcal{T}_{\eth\gamma}$, NBR is divided into 6×6 non-overlapping blocks called Main Block (MB) which is further divided into 3×3 non-overlapping blocks called Sub Block (SB). For each of the 3×3 SB, 8-bit $\mathcal{T}_{\eth\gamma}$ is generated using Algorithm 2, and the process is elucidated in Figure 6.

D. INTERMEDIATE KEY (I_{KEY}) AND PSEUDO RANDOM KEY ($\mathcal{PR}_{KEY}$) GENERATION

The I_{key} acts as the secret key between the sender and receiver for generating the $\mathcal{PR}_{Key}$. To generate the I_{key}, the $\mathcal{H}_{img}$ is partitioned into 4×4 non-overlapping blocks ($\beta_{\mathcal{H}}$). Block-wise mean of pixel intensity (β_μ) for each $\beta_{\mathcal{H}}$ is calculated using Eq 3 and stored in a vector β_μ.

$$\beta_\mu = \left\lceil \frac{\sum_{i=1}^{4}\sum_{j=1}^{4} \beta_{\mathcal{H}}(i,j)}{16} \right\rceil \tag{3}$$

Further the vector having β_μ is divided into bins, where each bin contains β_μ of 8 consecutive $\beta_{\mathcal{H}}$. 4^{th} positioned value is taken from randomly selected 16 bins by using Linear Congruential Method (LCG) pseudo-random number generator [52]. These 16 values are converted into corresponding ASCII characters and fed into Enigma machine. The Enigma machine uses a series of electro-mechanical rotors in order to generate cipher text, which is further converted into binary to generate a strong 128-bit $\mathcal{I}_{key}$ which is difficult to crack [45], [46]. For experimentation, the Enigma machine is simulated on the MATLAB environment [41], [47]. $\mathcal{PR}_{Key}$ is generated from I_{key} using the algorithmic steps presented in Algorithm 3. The size of $\mathcal{PR}_{Key}$ is equal to the size of EPR.

```
Algorithm 2 $\mathcal{T}_{\eth\gamma}$ Generation
Require: MB of size 6 × 6 , SB of size 3 × 3.
Ensure: $\mathcal{T}_{\eth\gamma}$
  Find mean of MB using the following relation:
      $MB_\mu = \left\lceil \left( \frac{\sum_{i=1}^{6}\sum_{j=1}^{6} MB(i,j)}{6 \times 6} \right) \right\rceil$
  Find mean of SB using the following relation.
      $SB_\mu = \left\lceil \left( \frac{\sum_{i=1}^{3}\sum_{j=1}^{3} SB(i,j)}{3 \times 3} \right) \right\rceil$
  Generate authentication ($A_b$) and parity ($P_b$) bits for
  each SB from $SB_\mu$ and $MB_\mu$ using Eq 1, Eq 2.
      $P_b = \begin{cases} 1 & if\ MB_\mu\ is\ odd \\ 0 & otherwise \end{cases}$   (1)
      $A_b = \begin{cases} 1 & if\ MB_\mu > SB_\mu \\ 0 & otherwise \end{cases}$   (2)
  Extract 6 MSB bits from $SB_\mu$. Then append $A_b$ and $P_b$
  bits to form a 8-bit $\mathcal{T}_{\eth\gamma}$.
```

E. EPR ENCRYPTION AND DECRYPTION

In the proposed scheme, a symmetric cryptographic approach is used for EPR encryption/decryption to provide high EPR security. An XOR operation is performed between EPR pixels and the corresponding value in $\mathcal{PR}_{Key}$ to obtain the encrypted EPR (EPR'). EPR decryption is the inverse of EPR encryption. EPR' is extracted from the watermarked NBR. $\mathcal{PR}_{key}$ is generated from the secret key I_{key} received from

Algorithm 3 $\mathcal{PR}_{key}$ Generation From I_{key}

```
Require: 128-bit $I_{key}$
Ensure: $\mathcal{PR}_{key}$ of size $\mathcal{C} \times \mathcal{D}$
  Divide 128-bits of $I_{key}$ into 16 groups ($G_1, G_2 \ldots\ldots G_{16}$) such that each group contains 8 consecutive bits.
  Select 1 to 8 bits in each group individually, and generate M and N vectors of size 128 bits using the following relations:
      $S_i = G_1(i) \mid\mid G_2(i) \mid\mid \ldots \mid\mid G_{16}(i)$
  where $i = [1, 2, 3, 4, 5, 6, 7, 8]$, || is the concatenation operation.
  $M = S_1 \mid\mid S_2 \mid\mid \ldots . \mid\mid S_8$
  Reverse the M vector to get 128 bit N.
  Initialize SK of size $\mathcal{C} \times 128$
  SK(1)=$I_{key}$
  for i=1 to $\mathcal{C} \times \mathcal{D}$ do
  for j=1 to 128 do
  O(j) = SK(i,j) $\bigoplus$ M(j),   P(j) = O(j) $\bigoplus$ N(j)
  R(j) = O(j) $\bigoplus$ P(j),   SK(i+1,j) = R(j)
  $\mathcal{PR}_{key}$ (i)=R(j)
  end i
  end j
  where ($\bigoplus \ldots \bigoplus$) is the XOR operation.
  Convert $\mathcal{PR}_{key}$ vector into $\mathcal{PR}_{key}$ 2D matrix form of size $\mathcal{C} \times \mathcal{D}$
```

the certified authority/sender. Then, EPR' is decrypted by performing XOR operation according to $\mathcal{PR}_{key}$.

F. WATERMARK EMBEDDING AND EXTRACTION

In the proposed scheme, BR and NBR are watermarked in the spatial domain. $\mathcal{T}_{\eth\gamma}$ and EPR' are embedded in NBR using the Neighbour Mean Interpolation (NMI) approach [44] because it provides lossless reversible embedding while ensuring high embedding capacity and security. Researchers have presented a variety of interpolation methods such as Bi-linear interpolation, Nearest neighbour interpolation, NMI, Bi-cubic interpolation, Basic-splines (B-spline), Lanczos interpolation, etc. The NMI approach has been chosen in the proposed scheme for embedding $\mathcal{T}_{\eth\gamma}$ and EPR' in the NBR due to its comparatively low computational time [44]. This approach helps to achieve a low computational cost, which is one of the important requirements in smart healthcare and IoMT applications [44]. Algorithm 4 presents the steps for the NBR embedding process.

NBR extraction is the reverse process of NBR embedding. The encrypted EPR (EPR'') and block-wise tamper detection and recovery bits ($\mathcal{T}_{\eth\gamma}'$) are extracted from NBR'. The algorithmic steps for NBR' extraction are provided in Algorithm 5. NBR embedding and extraction are illustrated in Figure 7, considering an example where $EPR' = 00$ and $\mathcal{T}_{\eth\gamma} = 00100111$. The equivalent decimal values for $EPR' = 0$ and $\mathcal{T}_{\eth\gamma} = 0{,}2{,}1{,}3$ are embedded in 3×3 IBL block to get 3×3 NBR' block. To extract the embedded watermark, the corner pixel values are considered to obtain $\beta_{2\times2}{}'$, as shown in Figure 7.

Algorithm 4 NBR Embedding Process:

```
Require: NBR, encrypted EPR ($EPR'$)
Ensure: $NBR'$
  Remove pixel intensity values 253, 254 and 255 from NBR (to avoid addition overflow) and save their corresponding row and column indices in $\mathcal{XY}$ matrix with two columns $\mathcal{X}$ and $\mathcal{Y}$ respectively. The values of $\mathcal{X}$ and $\mathcal{Y}$ are image dependent. The general range between $\mathcal{X}$ falls under $0 \leq \mathcal{X} < \mathcal{A}$ and $\mathcal{Y}$ is in between $0 \leq \mathcal{Y} < \mathcal{B}$. Resulting NBR ($NBR^1$) is used for the embedding process.
  Partition the $NBR^1$ into $6 \times 6$ non-overlapping blocks ($\beta_{6\times6}$), and further divide into $3 \times 3$ non-overlapping blocks ($\beta_{3\times3}$).
  Generate 8-bit $\mathcal{T}_{\eth\gamma}$ for each $\beta_{3\times3}$ sub block using Algorithm 2.
  For each of $\beta_{3\times3}$, select 4 corner pixels and convert it into $2 \times 2$ block ($\beta_{2\times2}$).
  Apply NMI on $\beta_{2\times2}$ to convert it into $3 \times 3$ interpolated block (IBL).
  Divide 8-bit $\mathcal{T}_{\eth\gamma}$ into four groups each having 2 consecutive bits and convert it into the equivalent decimal value to obtain $\mathcal{T}_{\eth\gamma 2}$, $\mathcal{T}_{\eth\gamma 4}$, $\mathcal{T}_{\eth\gamma 6}$, $\mathcal{T}_{\eth\gamma 8}$ using the following relation:
      $\mathcal{T}_{\eth\gamma_x} = bTod(\mathcal{T}_{\eth\gamma}(x-1), \mathcal{T}_{\eth\gamma}(x))$   (4)
  where $x = [2, 4, 6, 8]$ and bTod(.) is binary to decimal conversion.
  Similarly, select 2 bits at a time from $EPR'$ and convert it into equivalent decimal value ($EPR^D$).
  Embed $EPR^D$ and $\mathcal{T}_{\eth\gamma_x}$ in $IBL$ using the following relations:
      $IBL'(2,2) = IBL(2,2) + EPR^D$   (5)
      $IBL'(1,2) = IBL(1,2) + \mathcal{T}_{\eth\gamma 2}$   (6)
      $IBL'(2,1) = IBL(2,1) + \mathcal{T}_{\eth\gamma 4}$   (7)
      $IBL'(2,3) = IBL(2,3) + \mathcal{T}_{\eth\gamma 6}$   (8)
      $IBL'(3,2) = IBL(3,2) + \mathcal{T}_{\eth\gamma 8}$   (9)
  Finally, replace removed intensity pixel values 253, 254 and 255 to get watermarked $NBR'$.
```

G. TAMPER DETECTION AND RECOVERY

In the proposed scheme, the integrity of NBR is verified at two levels (global and block-wise) to achieve high tamper detection and recovery accuracy at low computational cost. First, global NBR integrity verification is done using GIC. At the receiver end, GIC'' is generated from NBR_{Ext} using Algorithm 1. GIC' is extracted from watermarked BR.

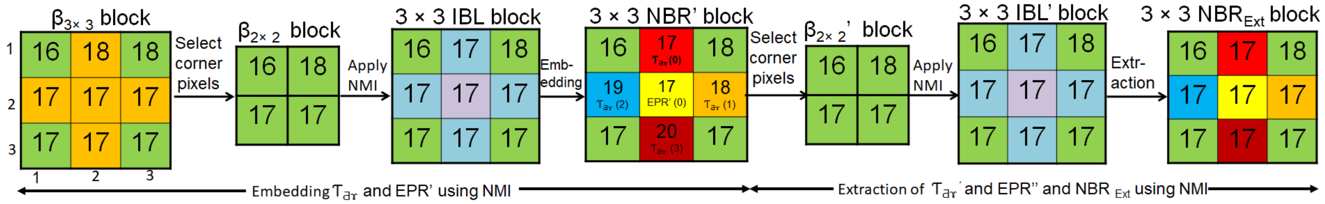


FIGURE 7. Embedding and extraction of $\mathcal{T}_{\partial\gamma}$ and *EPR′* using NMI.

Algorithm 5 NBR Extraction Process:

```
Require: $NBR'$, $\mathcal{XY}$
Ensure: $NBR_{Ext}$, extracted encrypted EPR ($EPR''$),
        Block-wise tamper detection and recovery bits ($\mathcal{T}_{\partial\gamma}'$)
Remove pixel intensities (253, 254 and 255) from the position according to the matrix $\mathcal{XY}$ (received as side information). The resulting NBR ($NBR'^{1}$) is used for extraction process.
Partition $NBR'^{1}$ into $6 \times 6$ non-overlapping blocks ($\beta_{6\times6}'$), and further partition these resultant blocks into $3 \times 3$ non-overlapping blocks ($\beta_{3\times3}'$).
Select 4 corner pixels of $\beta_{3\times3}'$, and convert to $2 \times 2$ ($\beta_{2\times2}'$) block.
Apply NMI on $\beta_{2\times2}'$ to convert $3 \times 3$ interpolated block ($IBL'$).
Extract $EPR''$ and $\mathcal{T}_{\partial\gamma}'$ bits from $IBL'$ using the following relations:
    $EPR^{D'} = \beta_{3\times3}'(2,2) - IBL'(2,2) \quad (10)$
    $\mathcal{T}_{\partial\gamma_2}^{D'} = \beta_{3\times3}'(1,2) - IBL'(1,2) \quad (11)$
    $\mathcal{T}_{\partial\gamma_4}^{D'} = \beta_{3\times3}'(2,1) - IBL'(2,1) \quad (12)$
    $\mathcal{T}_{\partial\gamma_6}^{D'} = \beta_{3\times3}'(2,3) - IBL'(2,3) \quad (13)$
    $\mathcal{T}_{\partial\gamma_8}^{D'} = \beta_{3\times3}'(3,2) - IBL'(3,2) \quad (14)$
    where $\mathcal{T}_{\partial\gamma_2}^{D'}$ contains first 1, 2 bits, $\mathcal{T}_{\partial\gamma_4}^{D'}$ contains 3, 4 bits, $\mathcal{T}_{\partial\gamma_6}^{D'}$ contains 5, 6 bits and $\mathcal{T}_{\partial\gamma_8}^{D'}$ contains 7, 8 bits of $\mathcal{T}_{\partial\gamma}'$ for corresponding $\beta_{3\times3}'$.
Convert $EPR^{D'}$, $\mathcal{T}_{\partial\gamma_2}^{D'}$, $\mathcal{T}_{\partial\gamma_4}^{D'}$, $\mathcal{T}_{\partial\gamma_6}^{D'}$ and $\mathcal{T}_{\partial\gamma_8}^{D'}$ into equivalent 4 binary value to get final $EPR''$, $\mathcal{T}_{\partial\gamma}'$.
Adjust modified pixels using the following relations:
    $\beta_{3\times3}(2,2) = \beta_{3\times3}'(2,2) - EPR^{D'} \quad (15)$
    $\beta_{3\times3}(1,2) = \beta_{3\times3}'(1,2) - \mathcal{T}_{\partial\gamma_2}^{D'} \quad (16)$
    $\beta_{3\times3}(2,1) = \beta_{3\times3}'(2,1) - \mathcal{T}_{\partial\gamma_4}^{D'} \quad (17)$
    $\beta_{3\times3}(2,3) = \beta_{3\times3}'(2,3) - \mathcal{T}_{\partial\gamma_6}^{D'} \quad (18)$
    $\beta_{3\times3}(3,2) = \beta_{3\times3}'(3,2) - \mathcal{T}_{\partial\gamma_8}^{D'} \quad (19)$
Finally, restore pixel intensity values 253, 254 and 255 to get extracted NBR ($NBR_{Ext}$).
```

In comparison, if GIC'' and GIC' are equal, then the received NBR is intact (not tampered) and no block-by-block tamper detection is required, thus saving time. Unequal GIC'' and GIC' indicate that the received NBR is tampered. Thus, local block-by-block tamper detection and recovery process, as shown in Figure 8, is carried out for tamper localization and recovery.

For localized tamper detection and recovery, the A_b and P_b bits are calculated for $\beta_{3\times3}$ of NBR_{Ext} using Eq 1, Eq 2 and compared with the extracted A_b' and P_b' from $\mathcal{T}_{\partial\gamma_2}^{D'}$ of $\beta_{3\times3}'$ to detect a tampered NBR block. The process of extracting $\mathcal{T}_{\partial\gamma_2}^{D'}$ is explained in Section III-F. If A_b, P_b and A_b', P_b' are equal, then $\beta_{3\times3}$ of NBR_{Ext} block is not tampered. Otherwise $\beta_{3\times3}$ of NBR_{Ext} is marked as tampered. For tampered blocks, 6 MSB recovery bits are obtained.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

Experiments were performed using MATLAB to assess the performance of the proposed scheme. Color and grayscale test host images were taken from OASIS [48], ADNI [49] and Kaggle [50]. For experimentation, $\mathcal{H}_{img}$ was scaled to 256 pixel resolution, and EPR was adjusted to 74 × 74 pixel resolution. The performance of the proposed scheme was evaluated in terms of imperceptibility, robustness, confidentiality, security, embedding capacity, and computational cost. Experimental results and discussions are presented in this section.

A. IMPERCEPTIBILITY TEST

The higher imperceptibility is one of the major requirements for MIW. The imperceptibility of watermarked medical images is evaluated in terms of the Peak Signal to Noise Ratio (PSNR) and the Structural Similarity Index Metric (SSIM) [33]. The PSNR measures the quality of watermarked medical images with respect to the host medical image. On the other hand, SSIM is used to predict perceived image quality and cinematic image attributes. The imperceptibility performance is evaluated in terms of PSNR and SSIM, and the results are presented in Table 2. As shown in Table 2, the PSNR values for all images are above 40dB, indicating good visual quality of the watermarked medical images [50]. Additionally, the SSIM values for all image modalities are close to the ideal value of 1, affirming that the proposed scheme is suitable for watermarking most medical images. The average PSNR and SSIM values for grayscale medical images are 41.89dB and 0.9883, respectively, while for color medical images they are 42.99dB and 0.9908. It is noteworthy

TABLE 2. PSNR (dB), SSIM,NC, BER for grayscale and color images under zero attack.

Grayscale images					Color images				
Image	**PSNR**	**SSIM**	**NC**	**BER**	**Image**	**PSNR**	**SSIM**	**NC**	**BER**
MRI Chest	41.24	0.9995	1	0	PET Brain	43.25	0.9938	0.9942	0.0083
CT Brain	42.01	0.9916	1	0	MRI arm	42.02	0.9952	0.9970	0.0076
X - ray arm	43.34	0.9923	1	0	Doppler	41.56	0.9860	0.9919	0.0022
Ultrasound	42.85	0.9892	1	0	Retina	44.23	0.9879	1	0
Mammograph	41.01	0.9806	1	0	Skin	45.87	0.9995	0.9999	0.0001
Lena	40.90	0.9764	1	0	Baboon	41.03	0.9823	0.9999	0.0001
Average	41.89	0.9883	1	0	**Average**	42.99	0.9908	0.9971	0.0030

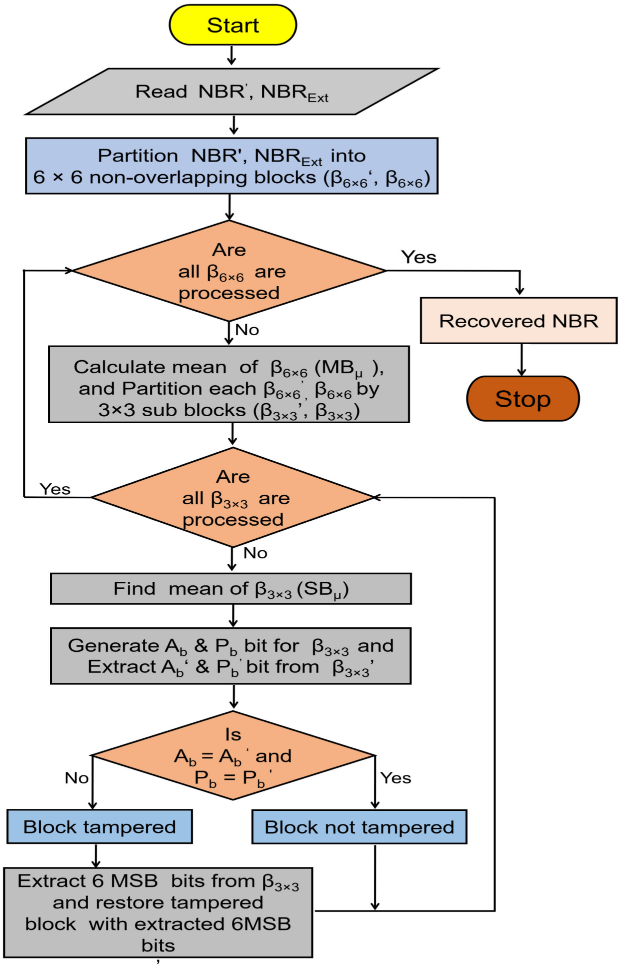

Start
Read NBR', NBR$_{Ext}$
Partition NBR', NBR$_{Ext}$ into 6 × 6 non-overlapping blocks ($\beta_{6\times6}$', $\beta_{6\times6}$)
Are all $\beta_{6\times6}$ are processed
Yes
No
Recovered NBR
Stop
Calculate mean of $\beta_{6\times6}$ (MB$_\mu$), and Partition each $\beta_{6\times6}$', $\beta_{6\times6}$ by 3×3 sub blocks ($\beta_{3\times3}$', $\beta_{3\times3}$)
Yes
Are all $\beta_{3\times3}$ are processed
No
Find mean of $\beta_{3\times3}$ (SB$_\mu$)
Generate A$_b$ & P$_b$ bit for $\beta_{3\times3}$ and Extract A$_b$' & P$_b$' bit from $\beta_{3\times3}$'
Is A$_b$ = A$_b$' and P$_b$ = P$_b$'
No
Yes
Block tampered
Block not tampered
Extract 6 MSB bits from $\beta_{3\times3}$ and restore tampered block with extracted 6MSB bits

FIGURE 8. *NBR$_{Ext}$* blockwise tamper detection and recovery.

that achieving high PSNR and SSIM values with a high embedding capacity of 2bpp is commendable.

B. ROBUSTNESS TEST

The proposed MIW scheme encodes and embeds authentication, authorization, and patient record information as a watermark in the host medical image. As a result, higher watermark resilience is required for MIW to assist in precise diagnosis. The robustness of the proposed scheme is analyzed under various attacks, and the results are quantified in terms of Normalized Correlation (NC) and Bit Error Rate (BER) [51], [52]. NC indicates the degree of similarity between two images, with values ranging from 0 to 1. An NC of 0 indicates low robustness, while an NC of 1 indicates high robustness. This observation is supported by the NC and BER values presented in Table 2. It can be seen that for all grayscale images under zero attack, NC and BER have ideal values. Similarly, for color images, NC ≃ 1 and BER ≃ 0. The average NC and BER for color images are 0.9971 and 0.0030, respectively. The results demonstrated in Table 2 indicate that the suggested scheme is robust for various image modalities under zero attack.

The robustness of the proposed scheme is further tested under different attacks such as noising (Salt & Pepper noise (SP), Gaussian noise (GN), Poisson noise (PN) with varying levels from 0.0002 to 0.02), filtering (Gaussian filter (GF), Median filter (MF), Butterworth filter (BF), Wiener filter (WF), Unmask filter (UF), Histogram equalization (HE), Sharpening with filter sizes of 3 × 3, 5 × 5), compression (JPEG), and geometrical attacks (translate, resize, cropping, row cut, column cut, and rotation). For the purpose of comparison, the NC and BER values for MRI Chest and CT Brain images are presented in Table 3. The proposed scheme exhibits high resistance against GF, MF, BF, WF, Unmask filter, SP, row cut, column cut, and HE attacks, as evidenced by the NC and BER values being close to the ideal value. Additionally, from Table 3, it can be claimed that the proposed scheme is moderately resilient to sharpening, GN, PN, JPEG compression, translation, resizing, rotation, and cropping attacks, as the NC and BER values exceed the threshold values. The scheme's robustness is validated at varying noise levels from 0.0002 to 0.2, as shown in Table 3. For all the noising attacks at all noise levels, the proposed scheme shows an NC above the threshold value of 0.7 [53]. The robustness of the proposed scheme is further evaluated with natural images such as Lena and Baboon, and the results are tabulated in Table 3. The suggested technique exhibits resilience against the majority of attacks for normal images, as per the NC and BER values for EPR presented in Table 3. There is scope for improvement in the performance of the proposed scheme under the resize and cropping attacks, which can be considered as future work. The robustness of the presented scheme is also tested for 30 different medical images under various attacks. In Table 3, the average NC and BER are tabulated. For SP and filtering

TABLE 3. NC, BER under attacks for MRI Chest, CT Brain, Lena, Baboon and average NC, BER for 30 medical images.

Attack	MRI Chest		CT Brain		Lena		Baboon		Average of 30 medical images	
	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER
SP(0.0002)	0.9998	0.0003	0.9999	0	0.9996	0	0.9998	0	0.9994	0.0002
SP(0.002)	0.9995	0.0010	0.9997	0.0002	0.9993	0.0002	0.9995	0.0003	0.9992	0.0006
SP(0.02)	0.9989	0.0035	0.9990	0.0016	0.9988	0.0046	0.9990	0.0014	0.9987	0.0029
GN(0.0002)	0.8327	0.01371	0.7471	0.0103	0.6162	0.0526	0.6692	0.0418	0.8291	0.02915
GN(0.002)	0.8018	0.0160	0.7692	0.0198	0.5960	0.0640	0.6457	0.0587	0.8031	0.0370
GN(0.02)	0.7935	0.0194	0.7583	0.02041	0.5825	0.0652	0.6216	0.0595	0.8002	0.0383
PN	0.8187	0.0345	0.8526	0.0242	0.6174	0.0787	0.6208	0.0780	0.9134	0.0186
Sharpening	0.7509	0.3935	0.8432	0.0615	0.8236	0.0916	0.7894	0.0287	0.8014	0.1432
GF(3×3)	1	0	1	0	1	0	0.9999	0	0.9999	0.0002
GF(5×5)	0.9999	0	0.9999	0	1	0	0.9996	0.0004	0.9997	0.0004
MF(3×3)	0.9998	0 .0008	1	0	1	0	0.9999	0	0.9998	0.0004
MF(5×5)	0.9993	0 .0012	0.9998	0.0002	0.9999	0	0.9997	0.0003	0.9995	0.0012
BF(G=1, F=20)	1	0	1	0	1	0	0.9998	0.0001	0.9999	0.0002
WF(3×3)	1	0	1	0	0.9999	0	0.9998	0	0.9997	0.0006
UF	1	0	1	0	0.9999	0	0.9998	0	0.9994	0.0010
Translate(0.25,0.25)	0.7542	0.0476	0.7646	0.0377	0.7960	0.0858	0.7401	0.0595	0.7637	0.0351
Resize(128,128)	0.6219	0.0619	0.6491	0.0952	0.6580	0.0963	0.5949	0.0628	0.5637	0.0751
Cropping (10%)	0.5623	0.0894	0.4935	0.0962	0.5014	0.0842	0.5577	0.0654	0.5131	0.0893
Row cut (10)	0.9998	0 .0008	0.9997	0.0010	0.9996	0 .0012	0.9992	0.0067	0.9991	0.0025
Column cut (10)	0.9997	0 .0008	0.9996	0.0010	0.9995	0 .0063	0.9984	0.0086	0.9984	0.0032
Rotation (10^0)	0.7936	0.0373	0.8072	0.0285	0.8216	0.0241	0.8372	0.0315	0.7825	0.0316
JPEG (60%)	0.9842	0.0231	0.9741	0.0217	0.9810	0.0481	0.9862	0.0205	0.9782	0.0052
HE	0.9998	0 .0006	0.9997	0.0008	0.9999	0 .0004	0.9997	0.0010	0.9990	0.0174

attacks, the proposed scheme yields an average NC $\simeq 1$ and an average BER $\simeq 0$. Despite the fact that the remaining attacks performed poorly, the average NC and BER values were greater than the threshold values. Simulation results for various attacks from Table 3 show that the proposed scheme is more robust against a number of attacks. It can be inferred from this discussion that the proposed scheme is successful in ensuring high robustness.

C. REVERSIBILITY ANALYSIS

The proposed scheme is a lossless RWS scheme for medical images in the spatial domain, where EPR is extracted, and the medical image is successfully reconstructed from the watermarked image at the receiver end. Here, the reversibility analysis of the proposed scheme is presented. Based on subjective evaluation, it is observed that the difference between the host image and the recovered image is black. Therefore, it can be concluded that the proposed scheme is capable of retrieving the original host medical image.

D. TAMPER DETECTION AND RECOVERY

Effectiveness of the proposed scheme in tamper detection and recovery has been examined in this section. True Positive (TP), True Negative (TN), False Positive (FP), False Negative (FN), True Positive Rate ($\mathcal{TPR}$), False Positive Rate ($\mathcal{FPR}$), and Accuracy rate ($\mathcal{AR}$) in tamper recovery are used as metrics.

Evidently, $TP + FN$ and $FP + TN$ are the number of valid and invalid pixels for tampered area detection, respectively. $\mathcal{AR} \simeq 100\%$, indicates that the image has been recovered successfully. For the experimental study, 10% of the watermarked image pixels are tampered (erased/copy-paste) and TP, TN, FP, FN are tabulated in Table 4

$\mathcal{TPR}$ is more than 94% and 83% for grayscale and color images, respectively. It is also observed from Table 4 that the proposed scheme has a high $\mathcal{TPR}$ and a low $\mathcal{FPR}$ for all images. Generally, high $\mathcal{TPR}$ and low $\mathcal{FPR}$ illustrate better robustness against various attacks and higher tamper localization. Thus, the proposed scheme is able to detect tampered areas effectively. In Table 4, it can be studied that $\mathcal{AR}$ is more than 99% for all images, affirming that the proposed scheme can efficiently detect tampering and, if any tamper is detected, can recover it successfully.

E. SECURITY TEST

In e-healthcare applications, ensuring the confidentiality and security of EPR is of utmost importance. In this section, we evaluate the security of the proposed $\mathcal{PR}_{key}$ encryption approach using the Correlation Coefficient (CC) and entropy metrics. A good encryption technique should remove any correlations between neighboring pixels that are vertically (V), horizontally (H), or diagonally (D) adjacent. Highly correlated pixels have a CC of 1, while uncorrelated pixels have a CC close to 0. Table 5 shows the CC of the original and encrypted images as well as the original and decrypted images. The correlation between the original watermark image and the encrypted watermark image is less than -0.39, while for the decrypted watermark image, the correlation is 1 for all test images as shown in Table 5. Based on the results presented in Table 5, it can be observed that the encrypted images have a negative correlation coefficient, indicating that they are negatively or reversibly correlated. Conversely, the decrypted images have a correlation coefficient of exactly 1,

TABLE 4. TP, TN, FP, FN and $\mathcal{TPR}$, $\mathcal{FPR}$ and $\mathcal{AR}$ of grayscale and color images.

Image	TP	TN	FP	FN	$\mathcal{TPR}$	$\mathcal{FPR}$	$\mathcal{AR}$
Grayscale images							
MRI Chest	1238	64219	24	55	95.74	0.03	99.87
CT Brain	1154	64288	35	59	95.13	0.05	99.85
X - ray arm	1194	64231	43	66	94.76	0.06	99.83
Ultrasound	1195	64258	26	57	95.44	0.01	99.87
Mammograph	1217	64232	28	61	95.15	0.04	99.86
Lena	1221	64219	34	62	95.16	0.04	99.85
Color images							
PET Brain	1063	64164	103	206	83.76	0.16	99.52
MRI arm	1103	64191	85	157	87.53	0.13	99.63
Doppler	1204	64236	32	64	94.95	0.04	99.88
Retina	1209	64224	28	75	94.15	0.04	99.84
Skin	1163	64216	28	75	91.79	0.08	99.84
Baboon	1198	64238	32	68	94.62	0.04	99.84

TABLE 5. CC and Entropy (OI- original image, EI - Encrypted image, DI- Decrypted image, EBE- Entropy before encryption, EAE- Entropy after encryption).

Image	CC b/n OI & EI			CC b/n OI & DI			EBE	EAF
	H	D	V	H	D	V		
EPR	-0.15	-0.19	-0.16	1	1	1	0.3101	0.9964
MRI Chest	-0.38	-0.38	-0.34	1	1	1	0.9522	0.994
Ultrasound	-0.24	-0. 21	-0.28	1	1	1	0.5858	0.9987
Skin	-0.34	-0.31	-0.32	1	1	1	0.8010	0.9972
Lena	-0.34	-0.35	-0.31	1	1	1	0.7240	0.9964

indicating that they are positively correlated with the original images. Therefore, it can be concluded that the proposed scheme is highly secure. In addition, the security performance is evaluated in terms of entropy, which is a widely used metric for assessing the effectiveness of encryption methods. Table 5 shows the entropy of binary images before and after encryption. It can be observed that the entropy of all images before encryption is ≤ 0.95 and ≥ 0.99 after encryption. From Table 5, it can be concluded that the images before encryption are less random as compared to after encryption. Thus, it becomes difficult for an intruder to extract the original image from the encrypted one. Hence, it validates that the proposed scheme has very high and effective watermark security.

F. COMPUTATIONAL COST

The computational cost (Ψ) of the proposed scheme has been determined by considering only the major expensive steps involved in the watermarking process. For a medical host image ($\mathcal{A} \times \mathcal{B}$) and EPR ($\mathcal{C} \times \mathcal{D}$), the ($\Psi$) of major steps involved in the proposed scheme is shown in Table 6. Taking only the most expensive steps into account, the (Ψ) of the proposed scheme is $\mathcal{O}(\mathcal{AB})$. Embedding and extraction time are shown in Table 7. The embedding time (including $\mathcal{PR}_{Key}$ generation and EPR encryption time) is less than 0.85s. Similarly, the extraction time (including $\mathcal{PR}_{Key}$ generation and EPR decryption time) for grayscale and colour images is nearly 0.83s and 0.85s, respectively. Based on the results presented in Table 7, it can be concluded that the proposed scheme has a reasonable computational cost.

TABLE 6. Computational cost of the proposed scheme.

Operation	Ψ	Operation	Ψ
BR, NBR partitioning	$\mathcal{O}(\mathcal{AB})$	$\mathcal{T}_{\mathfrak{d}\gamma}$ generation	$\mathcal{O}(\mathcal{AB})$
NMI process	$\mathcal{O}(\mathcal{AB})$	I_{key} generation	$\mathcal{O}\ (\mathcal{AB})$
GIC generation	$\mathcal{O}(\mathcal{AB})$	$\mathcal{PR}_{Key}$ generation	$\mathcal{O}(\mathcal{CD})$
Embedding process	$\mathcal{O}(\mathcal{CD})$	EPR Encryption	$\mathcal{O}(\mathcal{CD})$
Overall Ψ	$\mathcal{O}(\mathcal{AB})$		

TABLE 7. Embedding time (EMT) and extraction time (EXT) in seconds.

Grayscale images			Color images		
Image	**EMT**	**EXT**	**Image**	**EMT**	**EXT**
MRI Chest	0.8434	0.8049	PET Brain	0.8415	0.8285
CT Brain	0.8317	0.8133	MRI arm	0.8477	0.8052
X-ray arm	0.8486	0.8289	Doppler	0.8413	0.8209
Ultrasound	0.8189	0.8058	Retina	0.8752	0.8575
Mammograph	0.8575	0.8219	Skin	0.8348	0.8045
Lena	0.8352	0.8083	Baboon	0.8607	0.8348

G. COMPARATIVE ANALYSIS

A comparative analysis of the proposed scheme has been conducted with current state-of-the-art schemes, including Gull et al. [33], Bhardwaj [34], Geetha and Geetha [35], Huang et al. [36], Showkat et al. [38], Parah et al. [39], Bamal and Kasana [54] and Bamal and Kasana [55]. Parameters such as imperceptibility, robustness, security, embedding capacity, and computational time were considered for the comparative study. Gull et al. [33] proposed a reversible data hiding (RDH) scheme for IoMT-based networks to ensure a high embedding capacity using Huffman encoding techniques. Bhardwaj [34] also proposed a high embedding capacity RDH scheme in the spatial domain using the pixel adjustment process. Geetha and Geetha [35]] proposed an RDH scheme for tamper detection and recovery, using the rhombus mean interpolation approach for embedding tamper detection and recovery information. Huang et al. [36] proposed a two-tier lossless data hiding scheme with high embedding capacity, using median histogram shifting and prediction error schemes for lossless recovery. Another RDH scheme is proposed by Showkat et al. [38] using contrast stretching to ensure high ROI visual quality. Parah et al. [39] proposed an RDH scheme using left data mapping (LDM) and pixel repetition

TABLE 8. Comparison analysis of proposed scheme with state - of - art schemes. (WA- Watermarking approach, HIS- Host image size, SOE - Size of EPR, EM- Embedding method, TDR- Tamper detection and recover, AIMP (PSNR)- Avg. Imperceptibility, AEMC- Avg. Embedding capacity).

Schemes	WA	HIS	SOE	EM	TDR	Security	AIMP	AEMC (bpp)	Robustness
Gull et al. [33]	RDH	512 × 512	400 × 389	Huffman encoding	No	Yes (low)	44 dB	3.54	Medium
Bhardwaj [34]	RDH	512 × 512	256 × 256	Enhanced RDH	No	Yes (high)	44.46dB	3	Medium
Geetha and Geetha. [35]	RDH	512 × 512	91,600 (bits)	Mean interpolation	Yes	No	42.36 dB	1.5	Low
Huang et al. [36]	RDH	350 × 512	99,633 (bits)	Histogram shifting	No	No	45.62 dB	1.5	Low
Showkat et al. [38]	RDH	256 × 256	32 × 32	Contrast stretching	Yes	No	48.15 dB	1	Low
Parah et al. [39]	RDH	256 × 256	64 × 64	LDM, PRM	Yes	Yes (high)	41.98 dB	2.21	Low
Bamal & Kasana [54]	RDH	512 × 512	61,440 bits	SLT + PSO	Yes	Yes (high)	50.14 dB	1.1225	High
Bamal & Kasana [55]	RDH	512 × 512	66,048 hits	SVD+ FWT + SLT	Yes	Yes (high)	48.89 dB	1.8207	High
Proposed	RDH	256 × 256	74 × 74	NMI	Yes	Yes (high)	42.44 dB	2	High

TABLE 9. Tamper detection and recovery of the schemes in [35], [38], [39] and proposed scheme under attacks for the MRI chest image (TB - Tampered blocks).

Attack /Scheme	Geetha and Geetha. [35]		Showkat et al. [38]		Parah et al. [39]		Proposed	
	No. of TB	BER %	No.of TB	BER %	No.of TB	BER %	No.of TB	BER %
Median Filter (3 × 3)	14,556	41.2 8	18327	38.18	53014	83.314	1238	0.8
Salt and pepper noise (0.002)	11,524	4.78	18327	29.49	21280	19.951	1238	0.3
Gaussian noise (0.002)	11,524	3.05	18327	51.17	64782	98.78	1238	0.16
Histogram equalization	14,556	38.27	18327	69.63	48264	84.57	1238	0.6
JPEG (90%)	14,755	44.11	18327	28.51	53516	85.43	1238	0.21

TABLE 10. Average BER of State-of-art and proposed scheme under zero attacks and various attacks for 30 medical images.

Scheme	Zero attacks	Salt & pepper (0.0002)	Gaussian noise (0.002)	Median filter (3 × 3)	Sharp-ening	JPEG (60%)
[33]	0.0024	0.5047	0.4986	0.4993	0.4999	0.4988
[34]	0.0008	0.5564	0.5381	0.3516	0.4047	0.6482
[35]	0.0085	0.0488	0.4992	0.4130	0.4971	0.4450
[38]	0	0.2489	0.5317	0.3748	0.4453	0.3794
[39]	0	0.2088	0.6358	0.5231	0.4429	0. 5241
[54]	0	0.0691	0.0710	0.06703	0	0.0725
[55]	0	0.0632	0.0645	0.0633	0.0644	0.0644
Proposed	**0**	**0.0002**	**0.0570**	**0.0004**	**0.1432**	**0.0052**

method (PRM) to ensure reversibility, with RC4 used for EPR security. Bamal and Kasana [54] proposed an RDH scheme utilizing both spatial and transformation domains. The Slantlet Transform (SLT) is utilized for the embedding process, and a particle swarm optimization algorithm is used for finding optimal locations in slant blocks for embedding ROI and biometric ID. Before embedding, the watermark is encrypted using LZW, AES, and MD5 techniques. Similarly, Bamal and Kasana [55] also suggested a lossless data hiding scheme in a hybrid SVD + Fast Walsh Transform (FWT) + SLT transform. In this scheme, an artificial neural network is utilized for finding the ROI part. This scheme embeds 4 watermarks such as ROI, patients' personal data, unique biometric ID, and the key of the encryption process. For watermark security, this scheme utilizes AES and LZW processes. The proposed scheme utilizes a cryptography strategy that combines an enigma machine and mathematical theory to generate a pseudo-random key with low computational cost, making it difficult for any attacker to crack and highly secure.

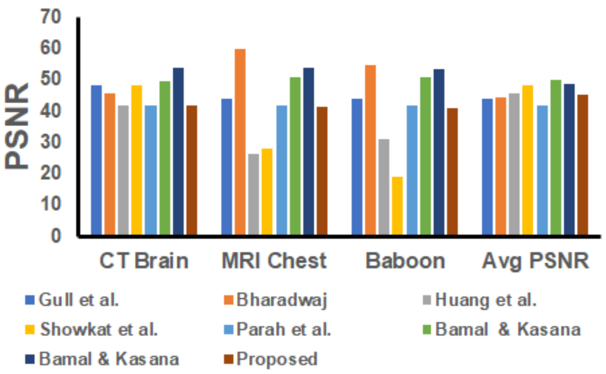


FIGURE 9. PSNR comparison of the proposed scheme and state - of - the -art schemes for CT Brain, MRI Chest, Baboon and Average PSNR of 30 medical images.

The average embedding capacity and PSNR for 30 medical images are shown in Table 8. From Table 8, it can be observed that the proposed scheme has a higher embedding capacity than the schemes proposed in [35], [36], [38], [54], [55]. The imperceptibility performance of the proposed scheme is compared for different types of images (CT Brain, MRI Chest, and Baboon) in terms of PSNR, as shown in Figure 9. The PSNR of the proposed scheme is higher than that of [35], [39], but lower than that of [33], [34], [36], [38], [54], [55]. However, the PSNR of the proposed scheme is above the optimal PSNR value and shows consistent performance for different images. The average PSNR of 30 medical images of the proposed scheme is on par with the schemes in comparison, as shown in Figure 9. The robustness of the proposed scheme is compared with other schemes under different attacks in terms of the average BER of 30 medical images, as shown in Table 10. The average BER value of the proposed scheme is higher than that of the schemes in [33], [34], and [35] and almost equal to that of the schemes in [38], [39], [54], and [55] under zero attack. From Table 10, it can be observed that the performance of the proposed scheme under attacks such as SP, GN, MF, sharpening, and JPEG compression is superior to that of the schemes in [33], [34], [35], [38], [39], [54], and [55]. Hence, the proposed scheme is more robust than the schemes in comparison.

V. CONCLUSION AND FUTURE SCOPE

A Reversible MIW approach is suggested for the secure transmission of medical images and EPR in smart healthcare applications that utilize real-time healthcare services. The encrypted EPR, tamper detection, and tamper recovery bits are inserted in the BR and NBR to ensure the integrity of the medical image, EPR confidentiality, and ownership authentication. The proposed scheme achieves high imperceptibility, robustness, tamper detection and recovery, security, and embedding capacity at a minimal computational cost. It has been tested using a variety of attacks, including filtering, compression, geometric distortions, and noise, demonstrating resistance against the vast majority of them. For effective tamper detection and recovery in the NBR, the proposed tamper detection and recovery algorithm and RWS achieve greater than 99% accuracy. According to the experimental results, the proposed scheme is effective for both grayscale and color medical images with varying textures and modalities. The limited robustness of the proposed scheme against rotation and shear attacks can be seen as a future scope of research.

REFERENCES

[1] M. M. Dhanvijay and S. C. Patil, "Internet of Things: A survey of enabling technologies in healthcare and its applications," *Comput. Netw.*, vol. 153, pp. 113–131, Apr. 2019.

[2] P. P. Ray, D. Dash, and D. De, "Edge computing for Internet of Things: A survey, e-healthcare case study and future direction," *J. Netw. Comput. Appl.*, vol. 140, pp. 1–22, Aug. 2019.

[3] A. El-Saadawy, A. El-Sayed, M. El Bery, and M. Roushdy, "Medical images watermarking schemes—A review," *Int. J. Intell. Comput. Inf. Sci.*, vol. 21, no. 1, pp. 119–131, Feb. 2021.

[4] R. Thabit, "Review of medical image authentication techniques and their recent trends," *Multimedia Tools Appl.*, vol. 80, no. 9, pp. 13439–13473, Apr. 2021.

[5] K. J. Devi, P. Singh, R. K. Yadav, and M. Z. Gafaru, "Reversible and secured image watermarking technique for IoMT healthcare," in *Proc. 12th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT)*, Jul. 2021, pp. 1–6.

[6] Priyanka and S. Maheshkar, "An optimized color image watermarking technique using differential evolution and SVD–DWT domain," in *Proc. 5th Int. Conf. Soft Comput. Problem Solving (SocProS)*, vol. 1. Singapore: Springer, 2016, pp. 105–116.

[7] P. Garg and A. K. Jain, "Digital watermarking techniques and their analysis," in *Smart Systems: Innovations in Computing*. Singapore: Springer, 2022, pp. 41–54.

[8] A. Anand and A. K. Singh, "Watermarking techniques for medical data authentication: A survey," *Multimedia Tools Appl.*, vol. 80, no. 20, pp. 30165–30197, Aug. 2021.

[9] K. Jyothsna Devi, P. Singh, H. K. Thakkar, and N. Kumar, "Robust and secured watermarking using Ja-Fi optimization for digital image transmission in social media," *Appl. Soft Comput.*, vol. 131, Dec. 2022, Art. no. 109781.

[10] P. Singh, K. J. Devi, H. K. Thakkar, and J. Santamaría, "Blind and secured adaptive digital image watermarking approach for high imperceptibility and robustness," *Entropy*, vol. 23, no. 12, p. 1650, Dec. 2021.

[11] K. J. Giri, Z. Jeelani, J. I. Bhat, and R. Bashir, "Survey on reversible watermarking techniques for medical images," in *Multimedia Security*. Singapore: Springer, 2021, pp. 177–198.

[12] D. Ravichandran, P. Praveenkumar, S. Rajagopalan, J. B. B. Rayappan, and R. Amirtharajan, "ROI-based medical image watermarking for accurate tamper detection, localisation and recovery," *Med. Biol. Eng. Comput.*, vol. 59, no. 6, pp. 1355–1372, Jun. 2021.

[13] M. P. Prakash, R. Sreeraj, F. AthishMon and K. Suthendran, "Combined cryptography and digital watermarking for secure transmission of medical images in EHR systems," *Int. J. Pure Appl. Math*, vol. 118, no. 8, pp. 265–269, 2018.

[14] B. Hassan, R. Ahmed, B. Li, and O. Hassan, "An imperceptible medical image watermarking framework for automated diagnosis of retinal pathologies in an eHealth arrangement," *IEEE Access*, vol. 7, pp. 69758–69775, 2019.

[15] P. Khare and V. K. Srivastava, "A secured and robust medical image watermarking approach for protecting integrity of medical images," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 2, p. e3918, Feb. 2021.

[16] M. Z. Konyar and S. Öztürk, "Reed Solomon coding-based medical image data hiding method against salt and pepper noise," *Symmetry*, vol. 12, no. 6, p. 899, Jun. 2020.

[17] S. Kaçar, M. Z. Konyar, and Ü. Çavuşoğlu, "4D chaotic system-based secure data hiding method to improve robustness and embedding capacity of videos," *J. Inf. Secur. Appl.*, vol. 71, Dec. 2022, Art. no. 103369.

[18] K. Swaraja, K. Meenakshi, and P. Kora, "An optimized blind dual medical image watermarking framework for tamper localization and content authentication in secured telemedicine," *Biomed. Signal Process. Control*, vol. 55, Jan. 2020, Art. no. 101665.

[19] D. Liu, Z. Yuan, and Q. Su, "A blind color image watermarking scheme with variable steps based on Schur decomposition," *Multimedia Tools Appl.*, vol. 79, nos. 11–12, pp. 7491–7513, Mar. 2020.

[20] M. Al-Qdah, "Secure watermarking technique for medical images with visual evaluation," *Signal Image Process., Int. J.*, vol. 9, no. 1, pp. 1–9, Feb. 2018.

[21] L. Novamizanti, I. Wahidah, and N. Wardana, "A robust medical images watermarking using FDCuT-DCT-SVD," *Int. J. Intell. Eng. Syst.*, vol. 13, no. 6, pp. 266–278, Dec. 2020.

[22] H. S. Alshanbari, "Medical image watermarking for ownership & tamper detection," *Multimedia Tools Appl.*, vol. 80, no. 11, pp. 16549–16564, May 2021.

[23] X. Deng, Z. Chen, F. Zeng, Y. Zhang, and Y. Mao, "Authentication and recovery of medical diagnostic image using dual reversible digital watermarking," *J. Nanoscience Nanotechnol.*, vol. 13, no. 3, pp. 2099–2107, Mar. 2013.

[24] P. V. S. Govind and M. V. Judy, "A secure framework for remote diagnosis in health care: A high capacity reversible data hiding technique for medical images," *Comput. Electr. Eng.*, vol. 89, Jan. 2021, Art. no. 106933.

[25] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar. 2006.

[26] Z. Pan, S. Hu, X. Ma, and L. Wang, "Reversible data hiding based on local histogram shifting with multilayer embedding," *J. Vis. Commun. Image Represent.*, vol. 31, pp. 64–74, Aug. 2015.

[27] S.-C. Liew, S.-W. Liew, and J. M. Zain, "Tamper localization and lossless recovery watermarking scheme with ROI segmentation and multilevel authentication," *J. Digit. Imag.*, vol. 26, no. 2, pp. 316–325, Apr. 2013.

[28] D. Zou, Y. Q. Shi, Z. Ni, and W. Su, "A semi-fragile lossless digital watermarking scheme based on integer wavelet transform," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 10, pp. 1294–1300, Oct. 2006.

[29] P. Selvam, S. Balachandran, S. P. Iyer, and R. Jayabal, "Hybrid transform based reversible watermarking technique for medical images in telemedicine applications," *Optik-Intell. Light Electron Opt.*, vol. 145, pp. 655–671, Sep. 2017.

[30] R. Thabit and B. E. Khoo, "Robust reversible watermarking scheme using slantlet transform matrix," *J. Syst. Softw.*, vol. 88, pp. 74–86, Feb. 2014.

[31] C.-Y. Weng, "DWT-based reversible information hiding scheme using prediction-error-expansion in multimedia images," *Peer-Peer Netw. Appl.*, vol. 13, no. 2, pp. 514–523, Mar. 2020.

[32] S. Bekkouch and K. M. Faraoun, "Robust and reversible image watermarking scheme using combined DCT-DWT-SVD transforms," *J. Inf. Process. Syst.*, vol. 11, no. 3, pp. 406–420, 2015.

[33] S. Gull, S. A. Parah, and K. Muhammad, "Reversible data hiding exploiting Huffman encoding with dual images for IoMT based healthcare," *Comput. Commun.*, vol. 163, pp. 134–149, Nov. 2020.

[34] R. Bhardwaj, "An improved reversible and secure patient data hiding algorithm for telemedicine applications," *J. Ambient Intell. Humanized Comput.*, vol. 12, no. 2, pp. 2915–2929, Feb. 2021.

[35] R. Geetha and S. Geetha, "Embedding electronic patient information in clinical images: An improved and efficient reversible data hiding technique," *Multimedia Tools Appl.*, vol. 79, nos. 19–20, pp. 12869–12890, May 2020.

[36] L.-C. Huang, S.-F. Chiou, and M.-S. Hwang, "A reversible data hiding based on histogram shifting of prediction errors for two-tier medical images," *Informatica*, vol. 32, no. 1, pp. 69–84, 2021.

[37] F. Sabbane and H. Tairi, "Medical image watermarking technique based on polynomial decomposition," *Multimedia Tools Appl.*, vol. 78, no. 23, pp. 34129–34155, Dec. 2019.

[38] S. Showkat, S. A. Parah, and S. Gull, "Embedding in medical images with contrast enhancement and tamper detection capability," *Multimedia Tools Appl.*, vol. 80, no. 2, pp. 2009–2030, Jan. 2021.

[39] S. A. Parah, J. A. Kaw, P. Bellavista, N. A. Loan, G. M. Bhat, K. Muhammad, and V. H. C. de Albuquerque, "Efficient security and authentication for edge-based Internet of Medical Things," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15652–15662, Nov. 2021.

[40] M. Rathod and J. Khanapuri, "A comparative study of transform domain methods for image resolution enhancement of satellite image," in *Proc. 11th Int. Conf. Intell. Syst. Control (ISCO)*, Coimbatore, India, Jan. 2017, pp. 287–291.

[41] M. Mohanta, D. S. Chablani, and D. Kowsagni, "Securing data in cloud environment using ENIGMA and des combination encryption," *Turkish J. Physiotherapy Rehabil.*, vol. 32, no. 2, p. 2, 2021.

[42] K. K. Roy and A. Phadikar, "Automated medical image segmentation: A survey," *Comput., Commun. Manuf.*, vol. 1, pp. 1–5, Feb. 2014.

[43] D. L. Pham, C. Xu, and J. L. Prince, "Current methods in medical image segmentation," *Annu. Rev. Biomed. Eng.*, vol. 2, no. 1, pp. 315–337, Aug. 2000.

[44] A. Malik, G. Sikka, and H. K. Verma, "A reversible data hiding scheme for interpolated images based on pixel intensity range," *Multimedia Tools Appl.*, vol. 79, nos. 25–26, pp. 18005–18031, Jul. 2020.

[45] K. Prasad and M. Kumari, "A review on mathematical strength and analysis of enigma," 2020, *arXiv:2004.09982*.

[46] K. Bawane, S. Zile, P. Meharkure, S. Barapatre, and S. Kurzadkar, "The enigma machine II," *Int. J. Res. Eng., Sci. Manage.*, vol. 2, no. 2, pp. 1–3, 2019.

[47] J. Roberts. (2021). *Enigma*. [Online]. Available: https://www.mathworks.com/matlabcentral/fileexchange/23367-enigma

[48] *The OASIS Image Database*. Accessed: Sep. 9, 2021. [Online]. Available: https://www.oasis-brains.org/

[49] *The ADNI Image Database*. Accessed: Sep. 9, 2021. [Online]. Available: http://adni.loni.usc.edu/data-samples/access-data/

[50] *The Kaggle Image Database*. Accessed: Sep. 9, 2021. [Online]. Available: https://www.kaggle.com/datasets

[51] M. Moosazadeh and G. Ekbatanifard, "A new DCT-based robust image watermarking method using teaching-learning-based optimization," *J. Inf. Secur. Appl.*, vol. 47, pp. 28–38, Aug. 2019.

[52] P. Singh, K. J. Devi, H. K. Thakkar, and K. Kotecha, "Region-based hybrid medical image watermarking scheme for robust and secured transmission in IoMT," *IEEE Access*, vol. 10, pp. 8974–8993, 2022.

[53] A. Anand and A. K. Singh, "Dual watermarking for security of COVID-19 patient record," *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 1, pp. 859–866, Jan. 2023.

[54] R. Bamal and S. S. Kasana, "Slantlet based hybrid watermarking technique for medical images," *Multimedia Tools Appl.*, vol. 77, no. 10, pp. 12493–12518, May 2018.

[55] R. Bamal and S. S. Kasana, "Dual hybrid medical watermarking using Walsh-slantlet transform," *Multimedia Tools Appl.*, vol. 78, no. 13, pp. 17899–17927, Jul. 2019.

PRIYANKA SINGH received the Ph.D. degree from IIT Dhanbad. She is currently an Assistant Professor with the Department of Computer Science and Engineering, SRM University AP, Guntur, Andhra Pradesh, India. Her research interests include digital image processing, digital image watermarking, image forensics, artificial intelligence, and machine learning.

K. JYOTHSNA DEVI received the Ph.D. degree from SRM University AP, Amaravati, and the M.Tech. degree from JNTU Hyderabad. She is currently an Assistant Professor with the Department of Computer Science and Engineering, PVPSIT, Vijayawada, Andhra Pradesh, India. Her research interests include digital image watermarking, optimization techniques, digital forensics, and machine learning.

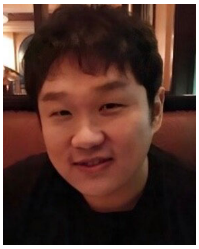
HIREN KUMAR THAKKAR received the M.Tech. degree from IIIT Bhubaneswar, India, in 2012, and the Ph.D. degree from the Department of Computer Science and Information Engineering, Chang Gung University, Taiwan, in 2018. He was a Postdoctoral Research Fellow with the Motor Behavioural Research Laboratory (MBRL), Healthy Aging Research Center, Chang Gung University. He is currently an Assistant Professor with the Department of Computer Science and Engineering, Pandit Deendayal Energy University, Gujarat. His research interests include healthcare data analysis, cloud resource management, opinion mining, and data analytics.

MUHAMMAD BILAL (Senior Member, IEEE) received the Ph.D. degree in information and communication network engineering from the Electronics and Telecommunications Research Institute (ETRI), Korea University of Science and Technology, in 2017.

From 2017 to 2018, he was with Korea University, where he was a Postdoctoral Research Fellow with the Smart Quantum Communication Center. In 2018, he joined the Hankuk University of Foreign Studies, South Korea, where he was an Associate Professor with the Division of Computer and Electronic Systems Engineering. In 2023, he joined Lancaster University, where he is currently a Senior Lecturer (Associate Professor) with the School of Computing and Communications. Throughout his career, he has been actively involved in various research projects, including various funded projects by the Korean Government Institute for Information and Communications Technology Promotion (IITP), the Ministry of Trade, Industry & Energy (MOTIE), South Korea, the BK21 Program, the National Research Foundation of Korea (NRF), and the National Science Foundation China. He is the author/coauthor of more than 140 articles published in renowned journals, including IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, IEEE INTERNET OF THINGS JOURNAL, IEEE SYSTEMS JOURNAL, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, and IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING, one book editorship, seven published proceedings papers, four issued U.S. patents, and six Korean patents. His research interests include network optimization, cyber security, the Internet of Things, vehicular networks, information-centric networking, digital twins, artificial intelligence, and cloud/fog computing.

Dr. Bilal is an Editorial Board Member of IEEE Transactions on Intelligent Transportation Systems, IEEE Internet of Things Journal, IEEE Future Directions in Technology, Policy, and Ethics Newsletter, *Alexandria Engineering Journal* (Elsevier), *Physical Communication* (Elsevier), *Computer Systems Science and Engineering*, *Intelligent Automation & Soft Computing*, *Frontiers in Communications and Networks*, and *Frontiers in the Internet of Things*, and the Co-Editor-in-Chief of the *International Journal of Smart Vehicles and Smart Transportation*. He has served as a Technical Program Committee Member for many international conferences, including the IEEE VTC, the IEEE ICC, ACM SigCom, and the IEEE CCNC.

ANAND NAYYAR (Senior Member, IEEE) received the Ph.D. degree in computer science in the area of wireless sensor networks, swarm intelligence, and network simulation from Desh Bhagat University, in 2017. He is currently with the School of Computer Science, Duy Tan University, Da Nang, Vietnam, as a Professor, a Scientist, the Vice-Chairperson (Research), and the Director of the IoT and Intelligent Systems Laboratory. He is a Certified Professional with more than 125 professional certifications from CISCO, Microsoft, Amazon, EC-Council, Oracle, Google, Beingcert, EXIN, GAQM, Cyberoam, and many more. He has authored/coauthored cum edited more than 50 books on computer science. He has published more than 175 research papers in various high-quality ISI-SCI/SCIE/SSCI Impact Factor-Q1, Q2, Q3, and Q4 journals cum Scopus/ESCI indexed journals, more than 70 papers in international conferences indexed with Springer, IEEE, and ACM Digital Library, more than 60 book chapters in various Scopus/Web of Science indexed books with Springer, CRC Press, Wiley, IET, and Elsevier with more than 12000 citations, H-index: 57, and i-index: 207. He has 18 Australian patents, seven German patents, four Japanese patents, 34 Indian design cum utility patents, eight U.K. patents, one USA patent, three Indian copyrights, and two Canadian copyrights to his credit in the area of wireless communications, artificial intelligence, cloud computing, the IoT, healthcare, drones, robotics, and image processing. He is also researching in the areas of wireless sensor networks, the Internet of Things, swarm intelligence, cloud computing, artificial intelligence, drones, blockchain, cyber security, healthcare informatics, big data, and wireless communications. He is a member of more than 60 associations as a Senior Member and a Life Member, such as a Senior Member of ACM. He is associated with more than 600 international conferences as a program committee/chair/advisory board/review board member. He was awarded 44 awards for the Teaching and Research Young Scientist, the Best Scientist, the Best Senior Scientist, the Asia Top 50 Academicians and Researchers, the Young Researcher Award, the Outstanding Researcher Award, the Excellence in Teaching, Best Senior Scientist Award, the DTU Best Professor and Researcher Award, in 2019, 2020, 2021, and 2022, the Distinguished Scientist Award by the National University of Singapore, Obada Prize 2023, the Lifetime Achievement Award, in 2023, and many more. He is acting as an Associate Editor of *Wireless Networks* (Springer), *Computer Communications* (Elsevier), *International Journal of Sensor Networks* (IJSNET) (Inderscience), *Frontiers in Computer Science*, *PeerJ Computer Science*, *Human-Centric Computing and Information Sciences* (HCIS), *IASC* (Tech Science Press), *Computers Materials and Continua* (CMC), *IET Quantum Communication*, *IET Wireless Sensor Systems*, *IET Networks*, *IJDST*, *IJISP*, *IJCINI*, *IJGC*, and *IJSIR*. He is acting as a Managing Editor of *International Journal of Knowledge and Systems Science* (IJKSS) (IGI-Global Journal, USA) and the Editor-in-Chief of *International Journal of Smart Vehicles and Smart Transportation* (IJSVST) (IGI-Global, USA). He has reviewed more than 2500 articles for diverse Web of Science and Scopus-indexed journals. He is listed among the Top 2% Scientists as per Stanford University, in 2020, 2021, and 2022, Ad Index (Rank No:1 Duy Tan University, Rank No:1 Computer Science in Vietnam), and listed on Research.com (Top Scientist of Computer Science in Vietnam-National Ranking: 2; D-index: 31).



DAEHAN KWAK (Member, IEEE) received the M.S. degree from the Korea Advanced Institute of Science and Technology (KAIST), South Korea, in 2008, and the Ph.D. degree in computer science from Rutgers University, New Brunswick, NJ, USA, in 2017. During his graduate studies, he was affiliated with the Networked Systems and Security (Disco) Laboratory, Rutgers University, and the Telematics and USN Research Division, Electronics and Telecommunications Research Institute (ETRI). He was a Research Staff Member with the UWB Wireless Research Center, Inha University; the Wireless Internet and Networks Laboratory, KAIST; and the Network Management and Optimization Laboratory, Yonsei University. He is currently an Associate Professor with the Department of Computer Science and Technology, Kean University, Union, NJ, USA. His current research interests include intelligent systems, cyber-physical systems, the IoT, systems and networking, wireless and sensor systems, mobile and vehicular computing, smart transportation, and smart health. He is a reviewer of several international journals, conferences, and undergraduate proceedings. He has served as the Guest Editor for journals, such as *Electronics* and *Wireless Communications and Mobile Computing*.