Hindawi
Security and Communication Networks
Volume 2021, Article ID 5514944, 15 pages
https://doi.org/10.1155/2021/5514944

Research Article

Chaotic Reversible Watermarking Method Based on IWT with Tamper Detection for Transferring Electronic Health Record

Mahboubeh Nazari and Arash Maneshi

Department of Computer Engineering, Imam Reza International University, Mashhad, Iran

Correspondence should be addressed to Arash Maneshi; maneshiarash@imamreza.ac.ir

Received 18 February 2021; Accepted 26 April 2021; Published 18 May 2021

Academic Editor: Azeem Irshad

Health IoT deals with sensitive medical information of patients, therefore security concerns need to be addressed. Confidentiality of Electronic Health Record (EHR) and privacy are two important security requirements for IoT based healthcare systems. Recently, watermarking algorithms as an efficient response to these requirements is in the spotlight. Further, as smart city-based applications have to react to real-time situations, efficient computation is a demand for them. In this paper, a secure, lightweight, reversible, and high capacity watermarking algorithm with tamper detection capability is proposed for IoT based healthcare systems. The scheme has applied Integer Wavelet Transform (IWT) and chaotic map for efficiency and increasing security. EHR is encrypted and then embedded into the Least Significant Bits (LSB) of wavelet coefficients of medical images. The proposed method has been extensively tested for various color and grayscale commonly used medical and general images. Investigations on experimental results and criterions such as Peak Signal to Noise Ratio (PSNR) and Bit Error Ratio (BER) above 45.41 dB and 0.04, respectively, for payload of 432,538 bits indicate that the proposed method, besides providing security, being reversible, tamper detection capability, and high embedding capacity, has high imperceptibility and adequate resistance against different types of attacks.

1. Introduction

Nowadays, exchanging sensitive data through insecure Internet channels is inevitable. Moreover, the Internet of Things (IoT) is a revolutionary technology that prepares a reliable infrastructure for actuators and sensors to collaborate and exchange data with each other. By using IoT opportunities, the healthcare system will be revolutionized. IoT based healthcare systems with the capability of collecting patient's real-time health data have attracted many researchers' attention [1].

Patient healthcare data which was collected by equipment and sensors of IoT based healthcare system is used to create Electronic Health Record (EHR) for each patient. EHR, including medical images, Electronic Patient Record (EPR), etc., plays an important role in the diagnosis process of a patient. Thus, any manipulation and tampering in such reports may cause fatal diagnosis to the patient. EHR are exchanged among hospitals, doctors, and insurance companies; therefore preserving the confidentiality of EHR and privacy of patients are the most important security requirements. On the other side, an IoT driven healthcare system must be capable of handling the real-time situation. Therefore, data transferring and computational overhead in such a system have to be efficient. In this scope, researchers are looking for alternative solutions that are proper for resource-constrained IoT devices.

The information hiding techniques are an adequate solution to address these challenges. Information hiding is classified mainly into steganography and watermarking. In both of them, secret data is embedded in the cover data such as text, voice, and pictures with different goals. In the steganography, data hiding in digital media should be done in such a way that the existence of secret data in the host media is unnoticeable. In these algorithms, the cover could be unrelated to the secret data, and only transferring the

hidden secret data and imperceptibility are important. But in watermarking algorithms, the secret data is dependent on the cover to preserve its security through manipulations. In some watermarking applications, information on cover media is hidden inside of cover media for copyright protection or content authentication purposes.

There are two spatial and transform domains for applying steganography and watermarking algorithms. In the spatial domain, the secret message is embedded directly into the cover image by manipulating pixel values. Spatial domain-based algorithms have less computational overhead and less resistance to different types of attacks. In the transform domain, at first, the cover image is transformed by using various transform operations such as Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Discrete Wavelet Transform (DWT), and then a secret message is embedded into coefficients [2]. Transform domain-based algorithms have more computational overhead and more resistance against different types of attacks. For designing a practical scheme for smart city applications, a trade-off between computational complexity and security must be considered.

The main requirements for all watermarking and steganography algorithms are imperceptibility, robustness, and payload capacity. Imperceptibility refers to the amount of deterioration that has been made to the cover media and robustness indicates how much a watermark can resist against different attacks. Corresponding to the application, a different level of robustness is required. Payload capacity also refers to the amount of data embedded inside of a cover media. For some watermarking applications, reversibility is a requirement which means that, after the extraction of the secret messages, host media have to be recoverable [3–5]. In irreversible techniques host media do not need to be restored after extraction of secret message. Considering applications, reversibility is not a requirement for all steganography techniques which could bring more payload capacity [6–8]. Reversible information hiding finds applications in e-healthcare, military communication, and smart cities, etc., where host media need to be recovered after the extraction phase [9].

As already mentioned, low computational complexity while keeping a high amount of payload is highly desirable feature for real-time situations like IoT based electronic healthcare systems and smart city applications. Many high capacity information hiding schemes have been suggested for image [9–14]. Most of them have used the interpolation concept to generate a resized version of the original image before embedding. These techniques estimate pixels values of the resized image by using several algebraic equations which increase computational complexity.

In this paper, we have tried to address these challenges. To provide confidentiality, EHR is encrypted by using a chaotic sequence that is unpredictable for an adversary. To tamper detection, an Integrity Check Code (ICC) is calculated. Moreover, computational complexity is reduced while keeping high capacity. The encrypted EHR and ICC are embedded in two Least Significant Bits (LSB) of cover image's Integer Wavelet Transform (IWT), being a fast and lossless transform. Therefore, the confidentiality of EHR and patient privacy are preserved during transmission.

The important contributions of the proposed method are as follows:

(1) Designing an efficient reversible watermarking algorithm with high capacity and tamper detection, providing EHR confidentiality, and preserving patient privacy for IoT based healthcare system for both grayscale and color images.

(2) Providing a high level of security by using the chaotic sequence as an efficient tool intelligently in host coefficients selection, encryption process, and structure of the symmetric key.

(3) Keeping quality of the cover image high and reducing computational complexity significantly in comparison to the state-of-the-art Pixel Repetition Method (PRM), Neighbor Mean Interpolation (NMI), and Interpolation Neighboring Pixels (INP) techniques.

The rest of the paper is organized as follows. In Section 2, a literature review is presented. Preliminaries are discussed in Section 3. Section 4 also describes the proposed method in detail, and Section 5 provides detailed experimental results and discussion. The conclusion of the paper is in Section 6.

2. Literature Review

In recent years, because of prominent advancements and expansion of IoT and prepared infrastructure for deploying IoT in real life, researchers have tried to take advantage of IoT potentials in real-life scenarios. One of the most attractive topics in this area is using IoT potentials to present smarter healthcare services. Healthcare systems always look for reducing costs and providing better quality in healthcare services. Therefore, many approaches have been introduced in this area. An extensive survey for applications of IoT for healthcare systems, IoT based technologies for healthcare, IoT security including security requirements and attacks classification, and taxonomy have been reported in [1, 15, 16]. Constraints of IoT sensors are also discussed in [17].

Various schemes have been proposed for home healthcare monitoring and telemonitoring. These schemes are based on Wireless Sensor Networks (WSN), Near Field Communication (NFC), and Radio Frequency Identification (RFID). Using IoT components based on these technologies, techniques for fall detection and seizure detection were introduced in [18–21]. In [20], a system was proposed which detects the risk of bedsores by using sensors. Furthermore, applications of IoT based wearable devices for monitoring Parkinson's gait disturbance and cardiac and neurological disorders are reported in [21]. These systems make it possible for caregivers to prevent dangerous situations by taking immediate action and providing better treatment.

Although the above schemes have proposed architectures for mHealth/eHealth, a seamless method for securing patient's EHR has not been reported [9]. Since EHR

contains patient's vital health data, designing a method that provides confidentiality for EHR, preserves patient's privacy, and applies to resource-constrained IoT devices for real-time scenarios in the smart city is highly desirable. Considering requirements and challenges, information hiding techniques seem to be an adequate option to design and develop such a system. Unlike conventional cryptography, information hiding techniques hide information inside of a cover medium intelligently, instead of encrypting information by using costly algorithms. A survey of applications of information hiding techniques in medical and healthcare systems has been presented in [22]. In order to increase capacity for hiding more amount of data, various information hiding techniques based on interpolation have been introduced. Neighbor Mean Interpolation has been introduced by [23]. The average PSNR of this scheme is 35 dB for a payload of 1.622 BPP. Chin Feng Lee and Yu-Lin Huang [24] proposed Interpolation by Neighboring Pixels (INP) to improve the performance of the data hiding scheme proposed by [23]. The payload of this method is up to 2.28 BPP. In [9], a reversible information hiding method based on interpolation has been proposed. This method at first resizes the original image with a size of $M \times N$ into $M/2 \times N/2$. Then using an algorithm called Pixel Repetition Method (PRM) creates a cover image from the resized image by repeating pixels from the original image. Then EHR is embedded into the cover image. However, the interpolation-based method can increase embedding capacity but the calculating number of algebraic equations and operations such as upscaling and downscaling for creating the cover image from the original image increases computational complexity and decreases the original image quality.

A watermarking scheme for the security of medical and nonmedical images based on 2-level Singular Value Decomposition (2-D SVD) has been proposed by [25]. A digital signature is embedded into the cover image for tamper detection purposes; however, watermark is needed for this test. A blind watermarking approach for medical image protection was proposed by [26]. This method uses combination of DWT and SVD for embedding data into the cover image. SVD increases computational complexity significantly and is not a suitable choice for resource-constrained IoT devices and real-time scenarios.

Table 1 summarizes the articles that have been mentioned in literature review section in chronological order of year.

3. Preliminaries

3.1. Integer Wavelet Transform (IWT). Wavelets are basis functions used to represent signals. Integer Wavelet Transforms (IWT) are the wavelet transforms that map integers to integers [27]. The procedure of calculating IWT using lifting technique is illustrated in Figure 1 and described as follows.

Step 1. The image matrix is separated odd and even columns. Frequency subbands, HF (high-frequency components), and LF (low-frequency components) are calculated using the following equations:

$$\begin{aligned} \mathrm{HF} &= \mathrm{odd}(i, j) - \mathrm{even}(i, j), \\ \mathrm{LF} &= \mathrm{even}(i, j) + \frac{\mathrm{HF}}{2}. \end{aligned} \tag{1}$$

Step 2. $\mathrm{LF}_{\mathrm{even}}$ and $\mathrm{LF}_{\mathrm{odd}}$ show the even and odd rows of LF. $\mathrm{HF}_{\mathrm{even}}$ and $\mathrm{HF}_{\mathrm{odd}}$ are also even and odd rows of HF. First level decomposition of the image is calculated as follows:

$$\begin{aligned} \mathrm{HH} &= \mathrm{HF}_{\mathrm{odd}} - \mathrm{HF}_{\mathrm{even}}, \\ \mathrm{HL} &= \mathrm{HF}_{\mathrm{even}} + \frac{\mathrm{HH}}{2}, \end{aligned} \tag{2}$$

$$\mathrm{LH} = \mathrm{LF}_{\mathrm{odd}} - \mathrm{LF}_{\mathrm{even}}.$$

$$\mathrm{LL} = \mathrm{LF}_{\mathrm{even}} + \frac{\mathrm{LH}}{2}. \tag{3}$$

3.2. Logistic-Sine Map. Chaotic map is a mathematical concept which is equal to evolution function. These functions are extremely sensitive to their initial conditions and exhibit chaotic behavior that means a small change in input parameter leads to an unpredictable change in output. Logistic-Sine map (LS) is introduced in [28] as an intensive chaotic map defined as follows:

$$\begin{aligned} x_{n+1} &= \left(r.x_n(1 - x_n) + \frac{(4 - r)\sin(\pi x_n)}{4} \right) \mathrm{mod} 1 r \in (0, 4] \\ x_n &\in [0, 1]. \end{aligned} \tag{4}$$

The analyses of bifurcation diagram and Lyapunov exponent prove that the chaotic behaviors of the LS map exist in the whole range of parameter settings and its chaotic sequences have a uniform distribution within [0, 1] [28]. These properties of LS make it impossible for an adversary to predict the chaotic sequence. In other words, regenerating chaotic sequence without having the key (concatenation of r and x_n parameters) is not possible which makes LS a proper option to increase the security of the proposed method significantly.

4. Proposed Method

The proposed method can be divided into two main phases, embedding and extraction phase, which take place, respectively, on the sender and receiver side. An overview of the proposed method has been shown in Figure 2. At the sender side, the patient's medical image and EHR are obtained as inputs from which the Integrity Check Code (ICC) is calculated. Then EHR and ICC are encrypted using a chaotic sequence generated by LS map. IWT is applied to the medical image as a cover image, and then four frequency subbands are produced and picked to embed encrypted ICC

Table 1: Summary of articles in chronological order of year.

Article	Description	Year
[23]	Data hiding method based on interpolation	2009
[24]	Data hiding method based on interpolation	2012
[20]	Health status monitoring (monitoring the risk of bedsores)	2015
[18]	Health status monitoring (fall detection)	2017
[19]	Health status monitoring (home care systems)	2017
[21]	Health status monitoring (applications of wearable technologies)	2017
[9]	Reversible data hiding method based on interpolation	2018
[25]	Watermarking scheme with digital signature based on SVD	2019
[26]	Watermarking scheme with embedded hash based on SVD	2021

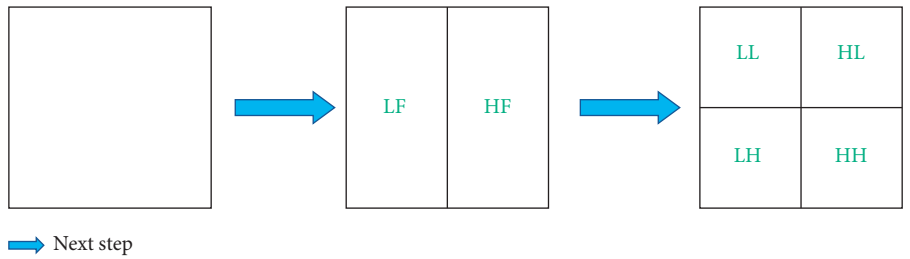

Figure 1: IWT calculation.

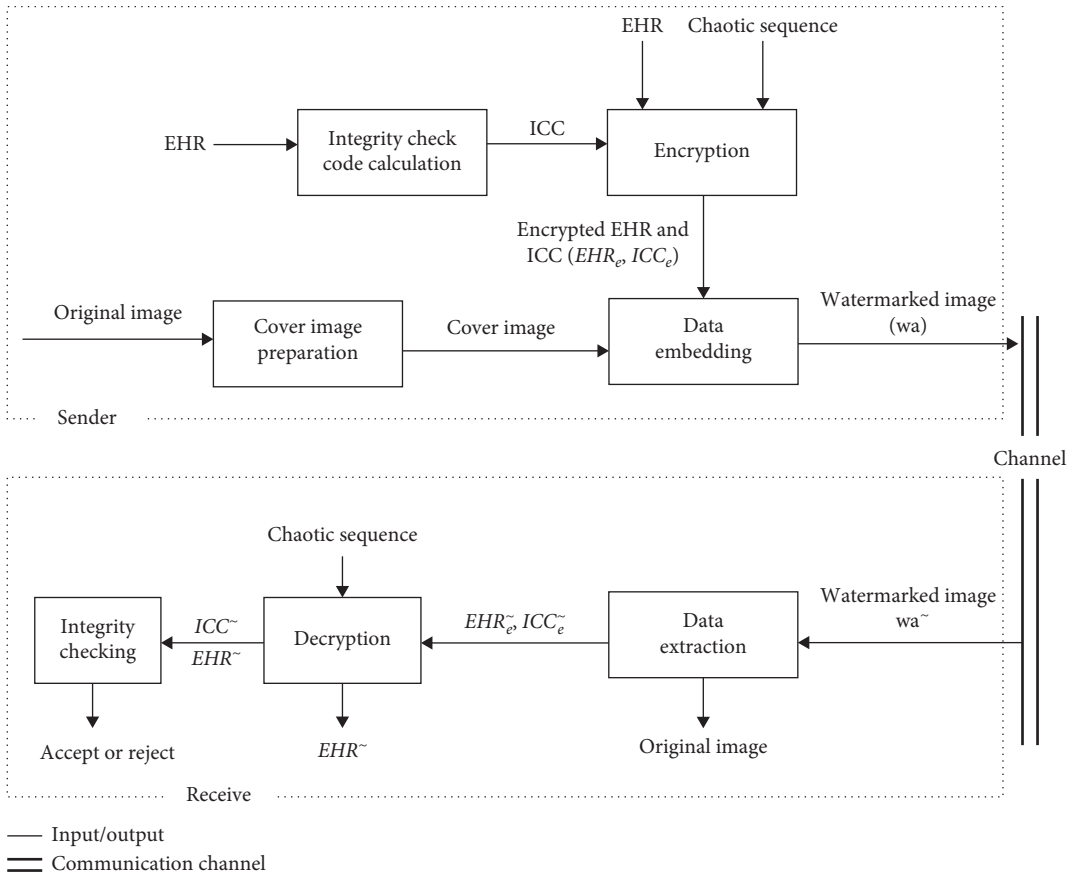

Figure 2: An overview of the proposed method.

and EHR into the LSB of coefficients. The data embedding procedure is described in Section 4.1 in detail. At the receiver side, the watermarked image is obtained and inverse IWT is applied to it. The four frequency subbands are picked to extract encrypted EHR and ICC from pixels LSB. The receiver regenerates chaotic sequence by using an agreed key

and then decrypts EHR and ICC which gives EHR′ and ICC′. Receiver recalculates ICC from EHR′, names it ICC″, and compares it to the ICC′ which was extracted and decrypted from the watermarked image. If ICC″ = ICC′ then the watermarked image is verified. The extraction procedure is described in Section 4.2 in detail.

4.1. Data Embedding Procedure. Data embedding procedure contains five subsections: cover image preparation, chaotic sequence generation, ICC calculation, EHR and ICC encryption, and data embedding, which are described in detail. Overview of data embedding is illustrated in Figures 3 and 4 .

4.1.1. Cover Image Preparation. To prepare the cover image, IWT is applied to the patient's medical image which produces 4 frequency subbands: LL, HL, LH, and HH. The following steps are taken to prepare the cover image:

(1) IWT is applied to the original image which produces LL, HL, LH, and HH frequency subbands

(2) HL, LH, and HH subbands are picked for EHR embedding

(3) LL subband is picked for ICC embedding

4.1.2. Chaotic Sequence (CS) Generation. To generate a chaotic sequence (CS), a key is needed. Concatenation of LS map parameters, x_0 and r, creates the key. Using this key, a chaotic sequence is generated, and the initial value effect can be faded by generating a sequence with a length three times bigger than that needed and picking the last segment. This sequence is used for encrypting EHR and ICC. The order of choosing subbands and pixels of each subband as host positions is based on the chaotic sequence. This leads to high confusion and diffusion which are the result of chaotic sequence features that make them appropriate for security aspects. The following steps are taken to generate CS:

(1) Choosing values for x_0 and r as the key

(2) Using the key as initial values of LS map to generate chaotic sequence (CS) with the size of $3n$, where $n = \text{size}(\text{EHR}||\text{ICC})$ is the length of the needed sequence

4.1.3. ICC Calculation. To detect tampering on a watermarked image, an Integrity Check Code (ICC) is calculated and embedded into the cover image.

The ASCII form of EHR is considered as sequence $W = p_1, p_2, p_3, p_4, p_5, \ldots, p_n$ where each p_n is an ASCII code of a letter. We divide this code into segments with length of five letters. The i^{th} segment of W is denoted by w_i, where $1 \le i \le (n/5)$. It should be noticed that if n is not the multiple of five, we add some padding. Corresponding to each segment $w_i = p_1p_2p_3p_4p_5$ which contains 40 bits, a four-bit code is produced by comparing each element of w_i with the central element p_3 as follows:

$$b_i = \begin{cases} 0, & p_j < p_3, \\ 1, & p_j > p_3, \end{cases} \quad 1 \le j \le 5. \tag{5}$$

All b_i come together to create B which is a compressed Integrity Check Code (ICC).

4.1.4. EHR and ICC Encryption. The CS that has been generated in step 4.1.2 is divided into two parts, CS_1 and CS_2, with the binary size of EHR and ICC, respectively. Then these parts are used to encrypt EHR and ICC to improve security. The encryption process consists of two stages:

(1) Scrambling: the order of the bits of EHR and ICC is changed based on new indices obtained from the sorted subsequences CS_1 and CS_2.

(2) Applying XOR operation: the binary forms of EHR and ICC are XOR with binary form of CS_1 and CS_2, respectively.

The following equations define encrypted EHR and ICC denoted by EHR_e and ICC_e, respectively.

$$\begin{aligned} \text{EHR}_e &= \text{EHR} \oplus \text{CS}_1, \\ \text{ICC}_e &= \text{ICC} \oplus \text{CS}_2. \end{aligned} \tag{6}$$

4.1.5. Data Embedding. The cover image was prepared in 4.1.1 subsection and ready to use for embedding. EHR_e is embedded into LSBs of coefficients in HL, LH, and HH. Moreover, LSBs of coefficients in LL band are hosts of bits in ICC_e. The order of choosing frequency subbands and coefficients for embedding EHR_e and ICC_e is based on chaotic sequence (CS). This technique makes it impossible for an attacker to recognize the host positions without having CS. At the end of this subsection, EHR_e is embedded into the cover image, and the cover image is watermarked with ICC_e. Then inverse IWT is applied to the watermarked image and the result will be sent. In summary for data embedding the following steps are taken:

(1) EHR_e bits are embedded into two LSBs of HL, LH, and HH coefficients of the cover image

(2) ICC_e bits are embedded into two LSBs of LL coefficients of cover image which produces the watermarked image

(3) Inverse IWT is applied to the watermarked image

4.2. Data Extraction Procedure. On the receiver side, at first, EHR is extracted from the watermarked image and then the integrity checking is done to ensure whether the watermarked image has been tampered or not. The data extraction process has been shown in Figures 5 and 6 . EHR and ICC extraction and integrity checking subsections are going to be described.

4.2.1. EHR and ICC Extraction. The receiver regenerates CS using the agreed key between the sender and the receiver which is the concatenation of x_0 and r. IWT applies to the

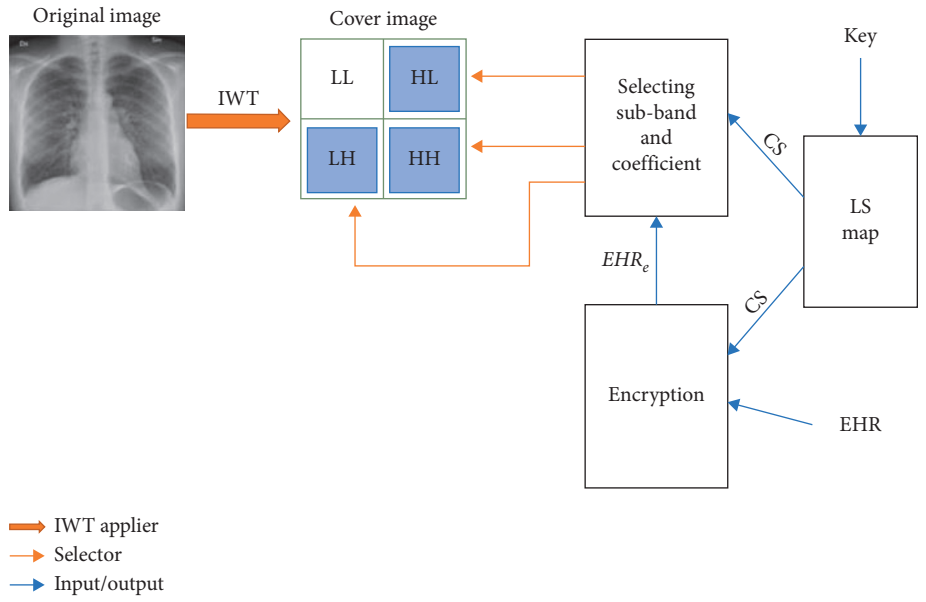

Figure 3: Preparing the cover image and embedding EHR into it.

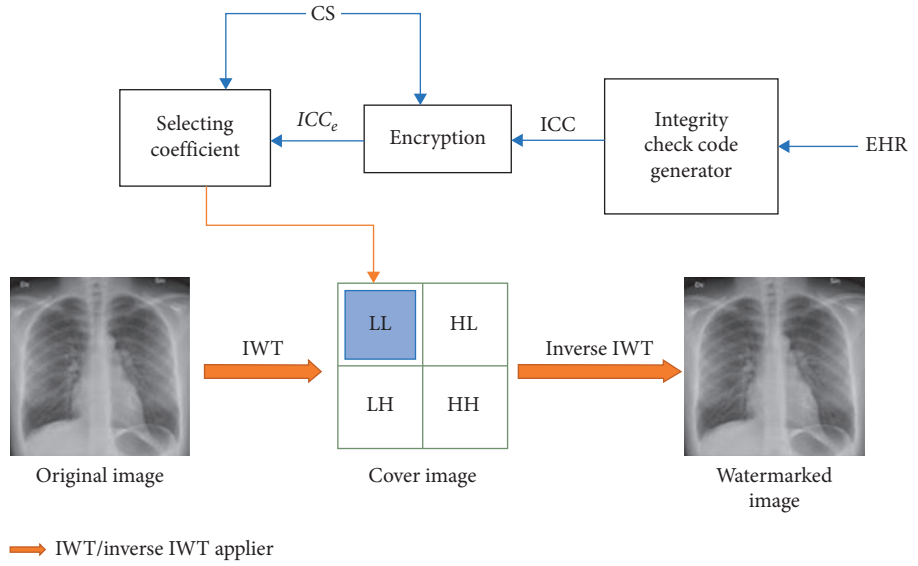

Figure 4: Calculating ICC and embedding it into the cover image.

watermarked image to produce LL, HL, LH, and HH sub-bands. According to the CS, similar to the sender side, the receiver can determine the selection order of host positions and extracts $EHR_e^{\sim}$ and $ICC_e^{\sim}$ from two LSBs of coefficients.

Regenerated CS is also used for decrypting $EHR_e^{\sim}$ and $ICC_e^{\sim}$ by equations $EHR^{\sim} = EHR_e^{\sim} \oplus CS_1$ and $ICC^{\sim} = ICC_e^{\sim} \oplus CS_2$ and then returning the scrambled bits to their first positions.

4.2.2. Integrity Checking. The ASCII code of $EHR^{\sim}$ is put in W and the receiver recalculates the ICC by using the same algorithm as described in 4.1.3 subsection. The integrity checking process has been demonstrated in Figure 6. The receiver compares recalculated ICC to $ICC^{\sim}$; if $ICC = ICC^{\sim}$ this means the watermarked image is valid, and otherwise, it is rejected. After checking the validity of the received watermarked image, inverse IWT is applied to the cover image to recover the patient's medical image. At this point, the receiver has both EHR and the medical image of the patient. Integrity checking is done by taking the following steps:

(1) ICC is calculated

(2) If $ICC = ICC^{\sim}$ then the received watermarked image and EHR are both valid

(3) If $ICC \neq ICC^{\sim}$ then the received watermarked image is rejected

(4) Inverse IWT is applied to the received watermarked image to recover the patient's medical image

5. Results and Discussion

In this section, a comprehensive investigation has been made on the proposed method in terms of performance and security analysis. The experiments have been carried out using MATLAB R2019a [29] on a Windows 10 PC with Intel® Core™ i7-2670QM CPU and 4 GB RAM. Various metrics such as Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Matrix (SSIM), Mean Square Error (MSE), Normalized Cross-correlation (NCC), Mean Absolute Error (MAE), and Bit Error Rate (BER) are measured to evaluate the performance of the proposed method. PSNR and SSIM are used to measure the quality of an image while MSE, NCC, MAE, and BER are used to evaluate the error in extracted secret data bits. All experimental results are reported for both grayscale and color medical/general test images.

5.1. Metrics Explanation. A brief explanation and mathematical definition for each criterion is given in the following.

5.1.1. Peak Signal to Noise Ratio (PSNR). PSNR is a measure of the ratio of signal to noise power. This criterion is used to evaluate the imperceptibility of a watermarked image. PSNR is defined by the following equation [30]:

$$\text{PSNR} = 10\log_{10}\frac{255^2}{\text{MSE}}. \tag{7}$$

5.1.2. Structural Similarity Index Matrix (SSIM). SSIM is a measure for evaluating the similarity of two images related to perceptual quality in terms of the human visual system. SSIM is defined by the following equation:

$$\text{SSIM}(X,Y) = \frac{(2\mu_X\mu_Y + C_1)(2\sigma_{XY} + C_2)}{(\mu_X^2 + \mu_Y^2 + C_1)(\sigma_X^2 + \sigma_Y^2 + C_2)}, \tag{8}$$

where μ_X and μ_Y are averages of pixels values of X and Y, respectively. Moreover, σ_X^2 and σ_Y^2 are variances of X and Y and σ_{XY} is the covariance of X and Y. $C_1 = (K_1\ L)^2$ and $C_2 = (K_2 L)^2$ are two variables to stabilize the division with a weak denominator. Variable L is the dynamic range of pixel values and variables K_1 and K_2 are 0.01 and 0.03 by default [31].

5.1.3. Normalized Cross-Correlation (NCC). NCC measures the degree of similarity between the cover image and the watermarked image [32]. The range of NCC is [1, −1]. When two images are completely the same, NCC is equal to 1, and NCC will be −1 if they are completely opposite. If NCC is equal to 0, this means two images are uncorrelated. Assume $X(i, j)$ and $Y(i, j)$ represent a cover image and a watermarked image, respectively. NCC is defined by the following equation:

$$\text{NCC} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[X(i,j) - \mu_X][Y(i,j) - \mu_Y]}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}\left[(X(i,j) - \mu_X)^2\right]}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}\left[(Y(i,j) - \mu_Y)^2\right]}}, \tag{9}$$

where μ_X and μ_Y are averages of matrices X and Y, respectively.

5.1.4. Mean Absolute Error (MAE). This criterion measures the average absolute errors between the cover image and the watermarked image. Assuming X and Y are cover image and watermarked image, respectively, for a grayscale image, MAE is defined by the following equation [33]:

$$\text{MAE} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}|X(i,j) - Y(i,j)|}{M \times N}. \tag{10}$$

5.1.5. Bit Error Ratio (BER). When data is transmitting over a communication channel, during transmission data could get damaged or altered intentionally by an attacker or unintentionally by noise. The number of damaged bits is divided by the total number of transmitted bits to calculate the ratio of bit error. BER is defined by the following equation [34]:

$$\text{BER} = \frac{n_e}{n_s}, \tag{11}$$

where n_e is the number of damaged bits and n_s is the total number of transmitted bits.

5.2. Imperceptibility Analysis. The changes that are made to cover image must be imperceptible for the human visual system (HVS). A watermark is completely imperceptible if humans cannot distinguish the original image from the watermarked image when they are laid side by side [35].

The proposed method has been tested on various color and grayscale medical and commonly used images with a size of 512 × 512 pixels. All testing images and corresponding watermarked images are shown in Figure 7. The proposed method has been simulated for two modes, such that two and three LSBs of each coefficient of the cover image are

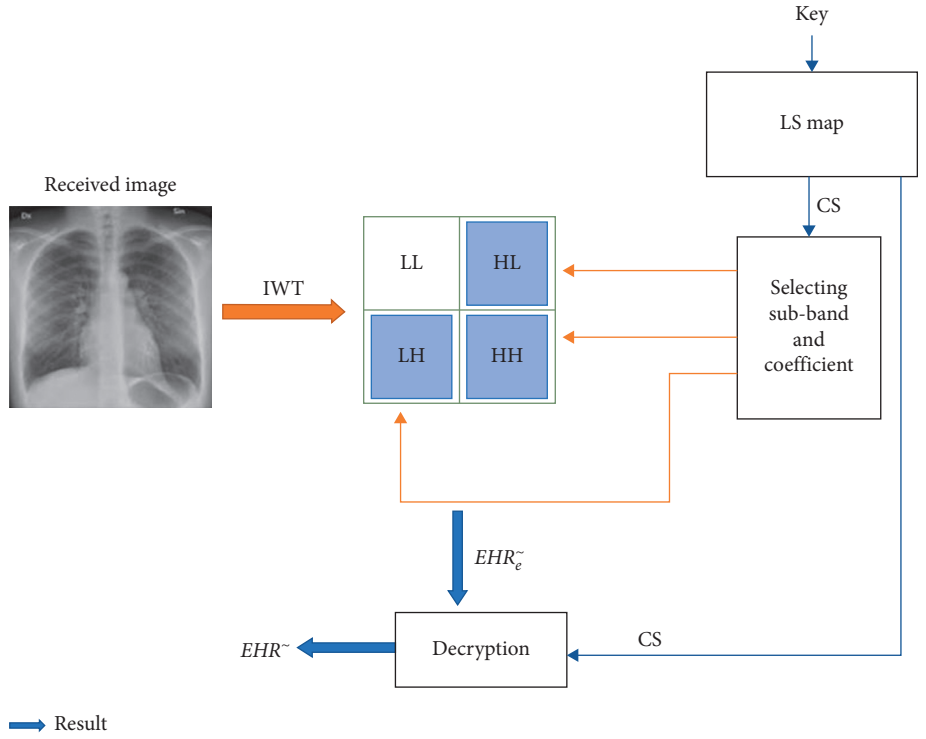

Figure 5: Extracting EHR from the watermarked image.

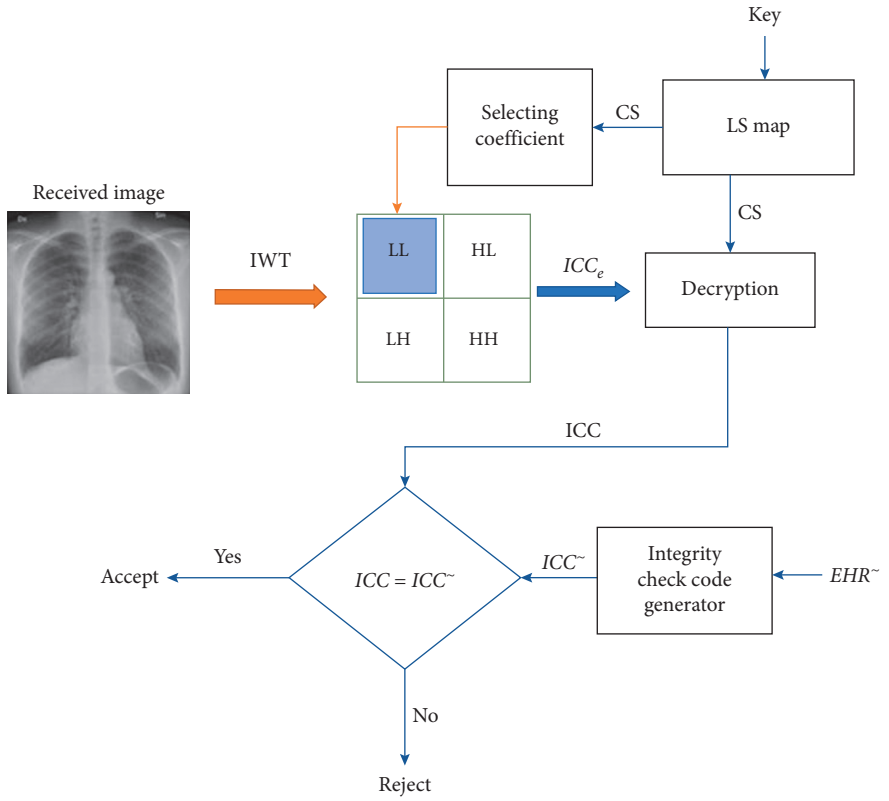

Figure 6: Integrity check test.

selected for embedding secret message in first and second mode, respectively. For grayscale images, the capacities are 432,538 bits (393,216 bits for EHR_e and 39,322 bits for ICC_e) and 648,808 bits (589,824 bits for EHR_e and 58,984 bits for ICC_e), respectively, for the first and second mode. Color images consist of three layers, Red, Green, and Blue (RGB);

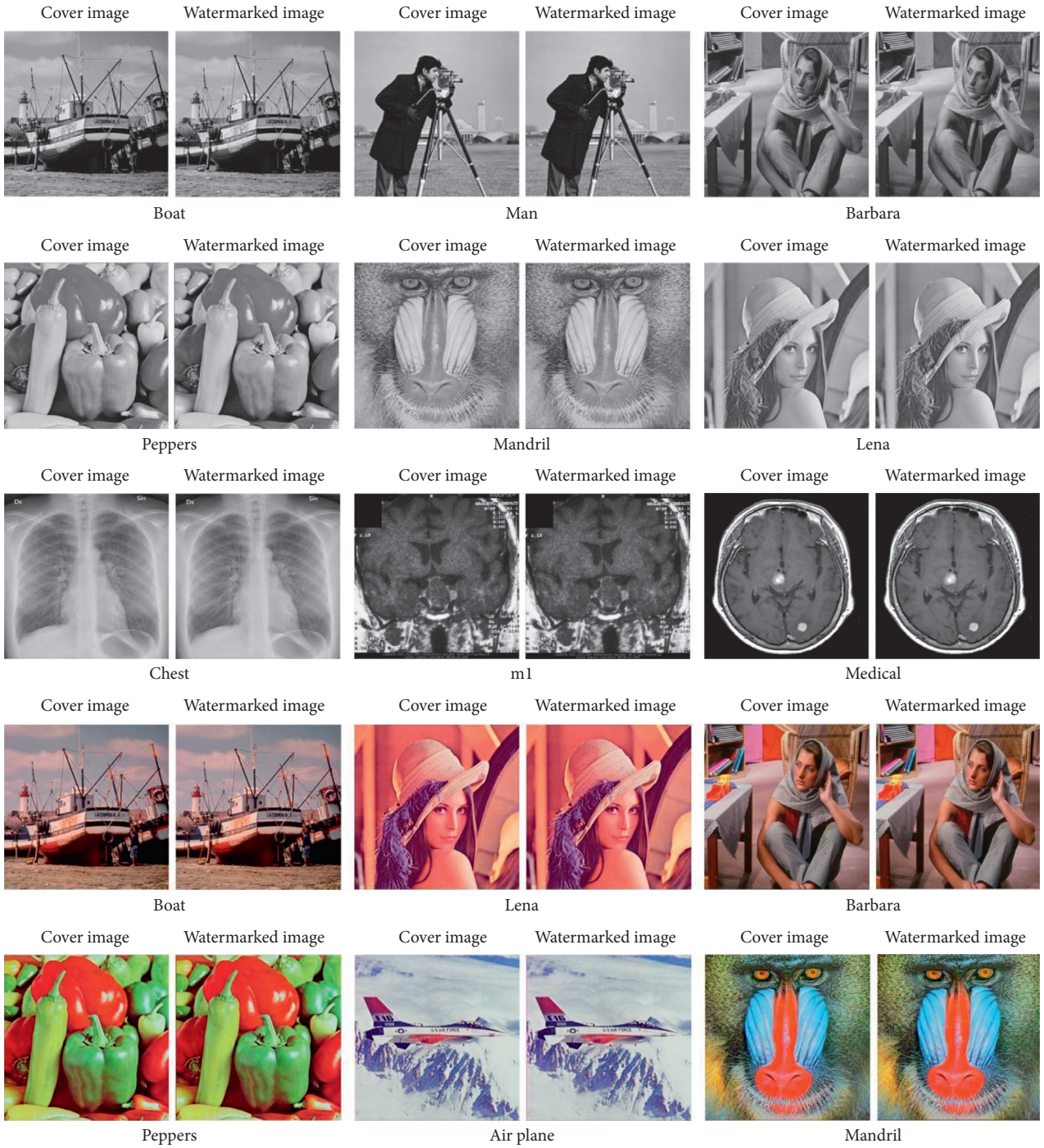

Figure 7: Test and watermarked images.

thus the capacities are 1,297,613 bits (1,179,648 bits for EHR_e and 117,965 bits for ICC_e) and 1,946,424 bits (1,769,472 bits for EHR_e and 176,952 for ICC_e), respectively. Since the length of ICC_e is equal to (1/10) of the length of EHR_e, the full capacity of LL is not occupied and could be used for other purposes. The results of PSNR, SSIM, NCC, and MAE metrics are reported for payloads of 432,538 and 1,297,613 bits (first mode) for grayscale and color images in Tables 2 and 3 , respectively.

PSNR values above 45 dB, MAE values close to zero, and NCC values close to 1 besides outstanding SSIM results indicate that the proposed method is capable of providing imperceptible and high quality watermarked images. PSNR, SSIM, NCC, and MAE results for second mode are given in Tables 4 and 5 for grayscale and color images, respectively. In second mode, the capacity for grayscale images is 648,808 bits (589,824 bits for EHR_e and 58,984 bits for ICC_e) and for color images the capacity is 1,946,424 bits (1,769,472 bits for

Table 2: Criterions results for grayscale images (432,538 bits' payload).

Cover image	PSNR	SSIM	MSE	NAE	NCC
Lena	45.41571356	0.98529705	0.93436050	0.00377006	0.99959233
Peppers	45.40055233	0.98616943	0.94027328	0.00388811	0.99967717
Mandrill	45.37948723	0.99539030	0.94287109	0.00371620	0.99950085
Barbara	45.37739511	0.98971939	0.94022369	0.00401877	0.99968409
Boat	45.28194767	0.98932682	0.96976089	0.00363709	0.99955803
Man	45.40891853	0.98356864	0.94287109	0.00392399	0.99975098
Chest	45.39985440	0.97885607	0.93158340	0.00357256	0.99944428
Medical	44.93731418	0.97929658	0.66186523	0.01098185	0.99970931
M1	45.35225447	0.98161973	1.01231002	0.00653188	0.99968356

Table 3: Criterions results for color images (1,297,613 bits' payload).

Cover image	PSNR	SSIM	MSE	NAE	NCC
Lena	45.39667538	0.99919942	0.31209437	0.00393097	0.99948778
Peppers	45.31623951	0.99911326	0.33829159	0.00450784	0.99962612
Barbara	45.40010469	0.99749971	0.31376139	0.00436215	0.99963265
Boat	45.35461716	0.99125248	0.33135774	0.00368493	0.99972065
Mandrill	45.39058876	0.99861759	0.31411319	0.00372696	0.99966761
Airplane	45.36217708	0.98705524	0.31885867	0.00256708	0.99942052

Table 4: Criterions results for grayscale images (648,808 bits' payload).

Cover image	PSNR	SSIM	MSE	NAE	NCC
Lena	39.16776366	0.94241805	3.92137145	0.00795723	0.99828481
Peppers	39.15785072	0.94528910	3.96346664	0.00817899	0.99864270
Mandrill	39.16214677	0.98142495	3.93774414	0.00781284	0.99791707
Barbara	39.17000866	0.95986360	3.92034149	0.00839860	0.99868275
Boat	39.15454443	0.95880376	3.83931350	0.00778576	0.99819215
Man	39.15081530	0.93682292	3.96741104	0.00830203	0.99894934
Chest	39.16677934	0.92011517	3.88083267	0.00753641	0.99767058
Medical	38.38476078	0.90927220	2.82612609	0.02433453	0.99871588
M1	39.02895827	0.93090727	4.45757293	0.01355195	0.99864375

Table 5: Criterions results for color images (1,946,424 bits' payload).

Cover image	PSNR	SSIM	MSE	NAE	NCC
Lena	39.16788707	0.99666985	1.30826441	0.00825880	0.99785790
Peppers	39.04715772	0.99621930	1.45020294	0.00942305	0.99842121
Barbara	39.17016370	0.98975923	1.31314341	0.00916486	0.99846046
Boat	39.08809440	0.96543779	1.43398072	0.00762411	0.99881913
Mandrill	39.15882182	0.99425752	1.31775029	0.00783808	0.99860516
Airplane	39.15136430	0.94956322	1.33884726	0.00535757	0.99759740

EHR_e and 176,952 bits for ICC_e). Similar to first mode, full capacity of LL subband is not occupied; thus, it could be used for other purposes.

The proposed method has been compared to several state-of-the-art techniques and results are reported in Tables 6 and 7 to show that the proposed method outperforms other schemes under comparison. Although the capacity of the proposed method is higher compared to other techniques, the results are showing significantly better performance of the proposed scheme in terms of PSNR, MAE, NCC, and SSIM. This is because of taking advantage of IWT which is a lossless transform and does not deteriorate cover image at all. In Figure 8, PSNR metric for different test images is compared to the other state-of-the-art methods and BPP is abbreviation of Bits Per Pixel.

5.3. Reversibility. As already mentioned, reversibility is a requirement for IoT based healthcare system. Therefore, we proposed a reversible technique in this paper. Usually, the capacity of irreversible techniques is more in comparison to the reversible techniques. On the other side, increasing capacity decreases imperceptibility. Thus, we tried to establish a trade-off between capacity and imperceptibility while providing reversibility in the proposed scheme. The procedure of extracting secret data from the cover image and

Table 6: PSNR, SSIM, NCC, and NAE criterions comparison.

Cover image	[10] payload: 327,680 bits				The proposed method payload: 432,538 bits			
	PSNR	SSIM	NCC	NAE	PSNR	SSIM	NCC	NAE
Lena	43.8838	0.97572	1	0.0100	45.4157	0.98529	1	0.0037
Mandrill	43.9171	0.98761	1	0.0098	45.3794	0.99539	1	0.0037
Peppers	43.8796	0.97559	1	0.0104	45.4005	0.98616	1	0.0038
Chest	43.8909	0.96547	1	0.0088	45.3998	0.97885	1	0.0035
Average	43.8935	0.97964	1	0.0100	45.3985	0.98894	1	0.0037

Table 7: Comparing the proposed method to the other state-of-the-art schemes.

Cover image	Method	Capacity	PSNR (dB)
Lena	[36]	196,608	46.3661
	[10]	327,680	43.8838
	Proposed	432,538	45.4157
Mandrill	[36]	196,608	46.3725
	[10]	327,680	43.9171
	Proposed	432,538	45.3794
Chest	[37]	10,882	48.4208
	[38]	36,060	48.9464
	[39] (GA scheme)	38,700	49.0119
	[39] (PSO scheme)	38,390	49.0047
	[36]	196,608	46.3685
	[10]	327,680	43.8909
	Proposed	432,538	45.3998

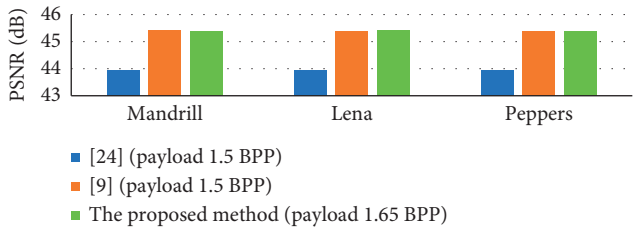

Figure 8: PSNR comparison.

recovering the patient's medical image has been described in Section 4.2 step by step. Test cover images and their corresponding watermarked images in Figure 7 are almost identical, and results of criterions such as SSIM, NCC, and MAE for these images prove their similarity. Because of close similarity, the watermarked image is reusable on the receiver side completely. Since LSBs of the cover image are used for embedding into, high quality of the patient's medical image is preserved.

5.4. Computational Complexity Analysis. As already mentioned, computational complexity is an important factor for IoT based healthcare system. One of the most important features of the proposed method is a low computational overhead which leads to less time and energy consumption. The cover image generation and data embedding stages of the proposed method are compared to cover image generation and data embedding of other state-of-the-art techniques in Figures 9 and 10, respectively. Cover image preparation is considerably faster in the proposed method

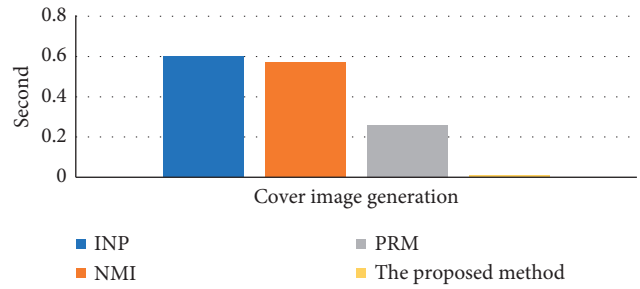

Figure 9: Required time comparison for CIG.

comparing to other schemes, because of taking advantage of IWT instead of calculating several equations in other state-of-the-art techniques. Using various algebraic equations for generating a cover image from the original image is more time consuming and complex than IWT. The data embedding stage of the proposed method is done by embedding secret data directly into LSBs of cover image pixels which does not require any calculation; therefore it is faster in comparison to other state-of-the-art schemes.

5.5. Security Analysis. One of the main goals of this paper is to address security challenges. For this purpose, several security levels are designed and included in the proposed method. In summary, the following steps are taken to ensure the proposed method meets security requirements:

(1) Choosing the order of pixels for embedding is based on a chaotic sequence (CS) which is impossible to regenerate without knowing the agreed key between the sender and the receiver.

(2) Secret data (EHR) is first encrypted and then embedded into the cover image.

(3) A fragile watermark is calculated and encrypted and then embedded into the cover image in order to detect any tampering or altering.

(4) Both encrypted EHR and the watermark are embedded into the transformed layer of the original image using IWT which brings noticeably more resistance against different attacks.

The proposed scheme has been tested against various signal processing and geometric attacks and BER (%) results are presented in Table 8 for payload of 432,538 bits and 1,297,613 bits for grayscale and color images, respectively. Moreover, obtained security analysis results are compared to [10] in Figure 11. It is evident from Figure 11 that the proposed

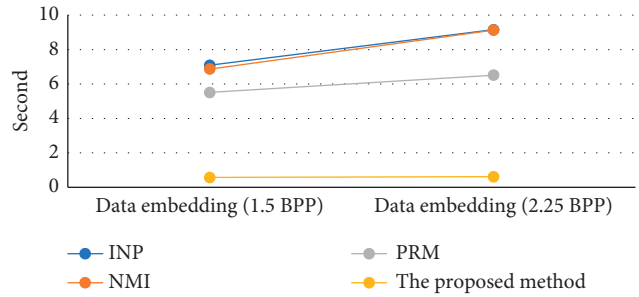

Figure 10: Required time for DE.

Table 8: BER results after performing various attacks for payload of 432,538 and 1,297,613 bits.

Attack	Lena (grayscale)	Mandrill (grayscale)	Lena (color)	Mandrill (color)	Tampering
Salt and pepper (0.1)	0.055	0.085	0.104	0.089	Detected
Gaussian noise (0.02)	0.277	0.165	4.893	2.592	Detected
Median filter	0.328	0.256	0.202	0.245	Detected
Low pass filtering	0.035	0.008	0.214	0.610	Detected
Sharping	0.059	0.236	0.199	0.233	Detected
Histogram equalization	0.041	0.128	0.084	0.215	Detected

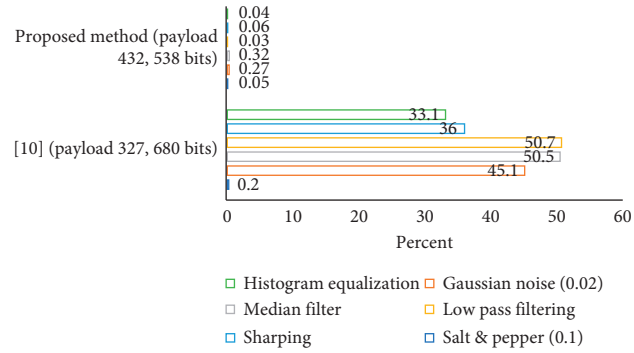

Figure 11: BER comparison for lena.

Table 9: Comparison of the main features of the proposed method and the other state-of-the-art schemes.

Method	Imperceptibility	Capacity	Computational cost	Tamper detection
[40]	Low	Medium	Medium	No
[39]	Low	Low	High	No
[36]	High	Low	Low	Yes
[10]	High	High	Low	Yes
[9]	High	High	Low	No
Proposed	High	High	Low	Yes

method, because of taking advantage of IWT, has impressive resistance against various attacks. Tamper detection analysis is also included in Table 8 to demonstrate the functionality of the fragile watermark. The results prove that the fragile watermark can detect any kind of tampering and altering. All security tests have been done for both grayscale and color images.

In Table 9, the proposed method is compared to other state-of-the-art schemes in terms of the main features.

5.6. Histogram Analysis. Histogram analysis is performed on watermarked images by adversaries with the intension to find a clue about what has been embedded. Histogram analysis is done by comparing the histograms of the cover image and watermarked image with each other. To withstand this attack, histograms of the cover image and watermarked image must be similar to each other closely. In Figure 12 histograms of various cover images (12(a), 12(c),

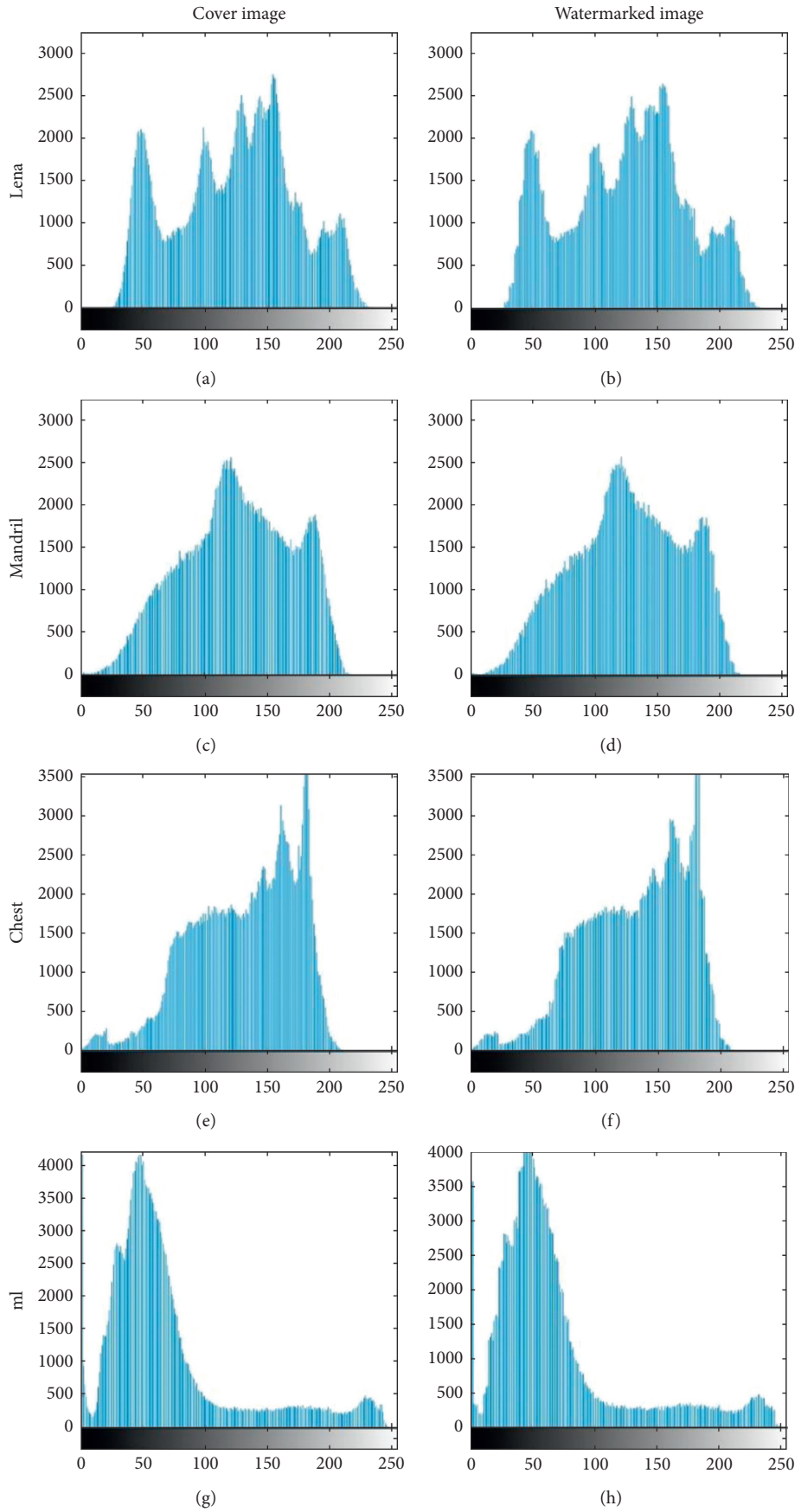

Figure 12: Histograms of cover and watermarked images.

12(e), and 12(g)) and corresponding watermarked images (12(b), 12(d), 12(f), and 12(h)) are presented for a payload of 432,538 bits. It is evident from Figure 12 that the proposed method can resist this attack since the histograms are nearly the same.

6. Conclusion

In this paper, considering security and IoT requirements, a secure, reversible, lightweight watermarking method with the capability of tamper detection has been introduced for IoT based healthcare systems. Usually, the capacity of reversible techniques is less than irreversible ones. Thus, we tried to establish a trade-off between capacity and preserving image quality to introduce a high capacity reversible scheme. In the proposed method for preparing a cover image, IWT was employed which is a fast and lossless transform with low computational complexity. EHR firstly is encrypted by a chaotic sequence and then embedded into LSBs of IWT subbands coefficients. A fragile watermark is calculated and embedded for tamper detection capability. Comprehensive investigations and analyses that have been made to the experimental results demonstrate high performance in terms of imperceptibility and image quality. The proposed method reduces the computational complexity significantly in comparison to the other state-of-the-art techniques by taking advantage of IWT. Security analyses in Section 5.5 prove that the proposed method is noticeably resistant against various signal processing attacks and the tamper detection feature is working properly.

Data Availability

All of the image samples and underlying data that support the results of our study are given in the paper.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

Special thanks are due to Iman Dorostkar Ahmadi who helped us by implementing this work.

References

[1] H. Ahmadi, G. Arji, L. Shahmoradi, R. Safdari, M. Nilashi, and M. Alizadeh, "The application of internet of things in healthcare: a systematic literature review and classification," *Universal Access in the Information Society*, vol. 18, no. 4, pp. 837–869, 2019.

[2] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: techniques, Evaluations, and trends in future research," *Neurocomputing*, vol. 335, pp. 299–326, 2019.

[3] Y. Qiu, H. Duan, J. Sun, and H. Gu, "Rich-information reversible watermarking scheme of vector maps," *Multimedia Tools and Applications*, vol. 78, no. 17, pp. 24955–24977, 2019.

[4] M. Turuk and A. Dhande, "A novel reversible multiple medical image watermarking for health information system," *Journal of Medical Systems*, vol. 40, no. 12, pp. 1–13, 2016.

[5] W. Wang and J. Zhao, "Hiding depth information in compressed 2D image/video using reversible watermarking," *Multimedia Tools and Applications*, vol. 75, no. 8, pp. 4285–4303, 2016.

[6] I. J. Kadhim, P. Premaratne, and P. J. Vial, "High capacity adaptive image steganography with cover region selection using dual-tree complex wavelet transform," *Cognitive Systems Research*, vol. 60, pp. 20–32, 2020.

[7] T. Rabie, M. Baziyad, and I. Kamel, "Enhanced high capacity image steganography using discrete wavelet transform and the Laplacian pyramid," *Multimedia Tools and Applications*, vol. 77, no. 18, pp. 23673–23698, 2018.

[8] D. K. Sarmah and A. J. Kulkarni, "Improved Cohort Intelligence-A high capacity, swift and secure approach on JPEG image steganography," *Journal of Information Security and Applications*, vol. 45, pp. 90–106, 2019.

[9] S. A. Parah, J. A. Sheikh, J. A. Akhoon, and N. A. Loan, "Electronic Health Record hiding in Images for smart city applications: a computationally efficient and reversible information hiding technique for secure communication," *Future Generation Computer Systems*, vol. 108, pp. 935–949, 2020.

[10] J. A. Kaw, N. A. Loan, S. A. Parah, K. Muhammad, J. A. Sheikh, and G. M. Bhat, "A reversible and secure patient information hiding system for IoT driven e-health," *International Journal of Information Management*, vol. 45, pp. 262–275, 2019.

[11] K.-H. Jung, "A survey of interpolation-based reversible data hiding methods," *Multimedia Tools and Applications*, vol. 77, no. 7, pp. 7795–7810, 2018.

[12] A. Malik, G. Sikka, and H. K. Verma, "Image interpolation based high capacity reversible data hiding scheme," *Multimedia Tools and Applications*, vol. 76, no. 22, pp. 24107–24123, 2017.

[13] A. A. Mohammad, A. Al-Haj, and M. Farfoura, "An improved capacity data hiding technique based on image interpolation," *Multimedia Tools and Applications*, vol. 78, no. 6, pp. 7181–7205, 2019.

[14] A. Shaik and V. Thanikaiselvan, "High capacity reversible data hiding using 2D parabolic interpolation," *Multimedia Tools and Applications*, vol. 78, no. 8, pp. 9717–9735, 2019.

[15] E. K. Naeini, I. Azimi, A. M. Rahmani, P. Liljeberg, and N. Dutt, "A real-time PPG quality assessment approach for healthcare Internet-of-Things," *Procedia Computer Science*, vol. 151, pp. 551–558, 2019.

[16] H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, and H. Karimipour, "A survey on internet of things security: requirements, challenges, and solutions," *Internet of Things*, vol. 2019, Article ID 100129, 2019.

[17] W. A. Kassab and K. A. Darabkh, "A-Z survey of Internet of Things: architectures, protocols, applications, recent advances, future directions and recommendations," *Journal of Network and Computer Applications*, vol. 163, Article ID 102663, 2020.

[18] C. C.-H. Hsu, M. Y.-C. Wang, H. C. Shen, R. H.-C. Chiang, and C. H. Wen, "FallCare+: an IoT surveillance system for fall detection," in *Proceedings of the 2017 International Conference on Applied System Innovation (ICASI)*, pp. 921-922, IEEE, Sapporo, Japan, May 2017.

[19] Y. Zhuang, "Query customization and trigger optimization on home care systems," in *Proceedings of the 2017 International*

Conference on Applied System Innovation (ICASI), pp. 668–671, IEEE, Sapporo, Japan, May 2017.

[20] R. Zgheib, R. Bastide, and E. Conchon, "A semantic web-of-things architecture for monitoring the risk of bedsores," in *Proceedings of the 2015 International Conference on Computational Science and Computational Intelligence (CSCI)*, pp. 318–323, IEEE, Las Vegas, NV, USA, December 2015.

[21] D. Wilson, "An overview of the application of wearable technology to nursing practice," *Nursing Forum*, Wiley Online Library, vol. 52, no. 2, pp. 124–132, 2017.

[22] H. Sajedi, "Applications of data hiding techniques in medical and healthcare systems: a survey," *Network Modeling Analysis in Health Informatics and Bioinformatics*, vol. 7, no. 1, pp. 1–28, 2018.

[23] K.-H. Jung and K.-Y. Yoo, "Data hiding method using image interpolation," *Computer Standards & Interfaces*, vol. 31, no. 2, pp. 465–470, 2009.

[24] C.-F. Lee and Y.-L. Huang, "An efficient image interpolation increasing payload in reversible data hiding," *Expert Systems with Applications*, vol. 39, no. 8, pp. 6712–6719, 2012.

[25] T. K. Araghi and A. A. Manaf, "An enhanced hybrid image watermarking scheme for security of medical and non-medical images based on DWT and 2-D SVD," *Future Generation Computer Systems*, vol. 101, pp. 1223–1246, 2019.

[26] N. Zermi, A. Khaldi, R. Kafi, F. Kahlessenane, and S. Euschi, "A DWT-SVD based robust digital watermarking for medical image security," *Forensic Science International*, vol. 320, Article ID 110691, 2021.

[27] V. Thanikaiselvan, P. Arulmozhivarman et al., "Comparative analysis of (5/3) and haar IVVT based steganography," *Information Technology Journal*, vol. 13, no. 16, pp. 2534–2543, 2014.

[28] Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," *Signal Processing*, vol. 97, pp. 172–182, 2014.

[29] T. Jack, *MATLAB. 9.6.0.1072779 (R2019a)*, The MathWorks Inc., Natik, MA, USA, 2019.

[30] M. Saidi, H. Hermassi, R. Rhouma, and S. Belghith, "A new adaptive image steganography scheme based on DCT and chaotic map," *Multimedia Tools and Applications*, vol. 76, no. 11, pp. 13493–13510, 2017.

[31] M. Nazari and I. Dorostkar Ahmadi, "A novel chaotic steganography method with three approaches for color and grayscale images based on FIS and DCT with flexible capacity," *Multimedia Tools and Applications*, vol. 79, no. 19-20, pp. 13693–13724, 2020.

[32] K. Muhammad, J. Ahmad, N. U. Rehman, Z. Jan, and M. Sajjad, "CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method," *Multimedia Tools and Applications*, vol. 76, no. 6, pp. 8597–8626, 2017.

[33] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. S. Ho, and K.-H. Jung, "Image steganography in spatial domain: a survey," *Signal Processing: Image Communication*, vol. 65, pp. 46–66, 2018.

[34] S. A. El_Rahman, "A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information," *Computers & Electrical Engineering*, vol. 70, pp. 380–399, 2018.

[35] M. Staring, "Analysis of quantization based watermarking," *Compare*, vol. 500, no. 2, pp. 3–15, 2002.

[36] S. A. Parah, F. Ahad, J. A. Sheikh, and G. M. Bhat, "Hiding clinical information in medical images: a new high capacity and reversible data hiding technique," *Journal of Biomedical Informatics*, vol. 66, pp. 214–230, 2017.

[37] S. Lee, C. D. Yoo, and T. Kalker, "Reversible image watermarking based on integer-to-integer wavelet transform," *Institute of Electrical and Electronics Engineers Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 321–330, 2007.

[38] L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong, "Reversible image watermarking using interpolation technique," *Institute of Electrical and Electronics Engineers Transactions on Information Forensics and Security*, vol. 5, no. 1, pp. 187–193, 2009.

[39] T. Naheed, I. Usman, T. M. Khan, A. H. Dar, and M. F. Shafique, "Intelligent reversible watermarking technique in medical images using GA and PSO," *Optik*, vol. 125, no. 11, pp. 2515–2525, 2014.

[40] J. Hu and T. Li, "Reversible steganography using extended image interpolation technique," *Computers & Electrical Engineering*, vol. 46, pp. 447–455, 2015.