cryptography

MDPI

Article

Reversible Data Hiding for DICOM Image Using Lifting and Companding

Amit Phadikar [1,*], Poulami Jana [2] and Himadri Mandal [3]

[1] Department of Information Technology, MCKV Institute of Engineering, Liluah, Howrah 711204, India
[2] Department of Electronics & Telecommunication Engineering, Bengal Institute of Polytechnic, Birbhum 731124, India
[3] Department of Electronics and Communication Engineering, Calcutta Institute of Technology, Uluberia, Howrah 711316, India
* Correspondence: amitphadikar@rediffmail.com; Tel.: +91-(33)-2654-9315

Received: 31 May 2019; Accepted: 14 August 2019; Published: 19 August 2019

Abstract: In this work, a reversible watermarking technique is proposed for DICOM (Digital Imaging and Communications in Medicine) image that offers high embedding capacity (payload), security and fidelity of the watermarked image. The goal is achieved by embedding watermark based on companding in lifting based discrete wavelet transform (DWT) domain. In the embedding process, the companding technique is used to increase the data hiding capacity. On the other hand, a simple linear function is used in companding to make the scheme easy to implement, and content dependant watermark is used to make the scheme robust to collusion operation. Moreover, unlike previously proposed reversible watermarking techniques, this novel approach does not embed the location map in the host image that ultimately helps to achieve high fidelity of the watermarked image. The advantage of the proposed scheme is demonstrated by simulation results and also compared with selected other related schemes.

Keywords: DICOM image; reversible watermarking; lifting; companding; collusion

1. Introduction

Rapid advancement in digital techniques had transformed the style of storage and transmission of multimedia data. With the availability of the communication network and the World Wide Web (WWW), digital data can travel from one source to an endless range of destination in any part of the globe. Notwithstanding these advantages, the digital domain representation of data also has a downside. The artworks in the form of a digital image can be used illegally, tampered with, and copied with an eye to copyright violation. This property of digital technology has encouraged thieves and discouraged the creator and the owner of digital artworks. Digital data hiding (watermarking) becomes a potential solution to address the above problems. Data hiding is a method of inserting an auxiliary message within the original data satisfying a few essential requirements [1,2]. However, it is very difficult to meet all these requirements simultaneously with the highest degree of accuracy. The design of data hiding techniques governed by widely diverse factors such as character and availability of the cover data, visibility/non-visibility of metadata, choice of embedding space and location, degree of resiliency against unintentional or intentional attacks on the data, etc. The watermark can be embedded in the spatial domain or frequency domain depending on the desired application. It is seen that the frequency domain methods are more robust than the spatial domain techniques [3].

The large numbers of data hiding techniques modify the cover media in order to embed the watermark information. The modification is very small and imperceptible to human visual systems (HVS). However, the original cover media cannot be restored entirely. In other words, those schemes

are irreversible data hiding techniques. But the irreversibility is not permissible to some applications, such as legal, forensic image archiving, and medical imaging [4]. Medical images are normally collected in hospitals or research centers due to the nature of the specialized equipment [5]. There are standard means like DICOM (Digital Imaging and Communications in Medicine) that enable the management, storage, and impression of medical images in standard formats [6]. For medical imaging applications, reversible data hiding is used to extract the embedded information as well as to restore the original host signal. In other words, reversible watermarking schemes are also often known to as lossless, invertible, or distortion-free, data hiding technique, and it is a very prominent research area in the last few years [4].

The idea of a reversible watermarking technique initially proposed and patented by Eastman Kodak [7]. Xuan et al. [4] embed watermark information into the high-frequency wavelet coefficients by companding technique. The Laplacian-like distribution of integer wavelet coefficients helps to select the compression and expansion functions. Tang et al. [8] develop a novel encryption scheme to serve the purpose of data hiding in the reversible domain. Their scheme improves the embedding capacity with a minimum computational burden. Tian [9] described a reversible watermarking scheme based on difference expansion (DE). This scheme uses location map to embed watermark. The term 'location map' is the selected positions of the pixels or the coefficients. The method selects the pixels or the coefficients from the location map to modulate during the process of watermark embedding. The major drawback of this scheme is the lack of capacity control due to insertion of the compressed location map in conjunction with the true payload. Hence the system will suffer from low embedding rate and also the lack of visual quality of the watermarked image. Jinna and Ganesan [10] proposed a reversible data hiding scheme using bit-plane coding and wavelet transform based on lifting. The performance of the scheme for several types of noise and attacks is tested. However, it is seen that when the noise level is high and also affecting the major part of the image, the watermark is extracted wrongly.

Xiaolong et al. [11] proposed the prediction-error expansion (PEE) technique for reversible watermarking, which embeds data uniformly. The scheme adaptively embeds one (1) or two (2) bits into the expandable pixel, based on local complexity. Lee et al. [12] proposed a data hiding scheme that divides the host image into non-overlapping blocks. The scheme then embeds a watermark into the high-frequency wavelet coefficients of the above blocks. Authors argue that the scheme offers superior embedding capacity, and also the embedding distortion is maintained at a lesser level. Sachnev et al. [13] present a reversible data hiding scheme for images without using the location map. The scheme uses prediction errors to embed data into the host image. A sorting technique is used to trace the prediction errors depending on the amount of its local variance. A reversible data embedding technique is proposed based on integer wavelet transform by Weng et al. [14]. Data insertion is done by increasing the differences between one pixel and each of its three adjacent pixels. Liu et al. [15] combine data hiding and image encryption to provide integrity/security in the cloud computing environment. The scheme uses block compressive sensing (BCS) technique to compress and encrypt the image. Then hidden data bits are embedded into the least significant nibble. The main feats of the scheme are improved compression, data-loss prevention, and embedding capacity.

Most of the current solutions found in the literature compromise between the quality of the reproduced medical image and the numbers of effective watermark bits inserted, which are indicators of the strength of the authentication and originality mechanisms of solution. Moreover, due to the reduced number of effective inserted bits, the strength of the current solutions is highly vulnerable, and it can be broken with simple security algorithms or brute force attacks [16,17]. Lastly, the schemes proposed in ([4,9]) embed location map as side information for restoration of the host image. That ultimately reduces the effective embedding capacity of a scheme.

Li et al. [18] proposed a prediction error expansion (PEE) based reversible watermarking technique where multiple histogram modification mechanism is used for better embedding performance. The method performs better than conventional PEE methods in terms of watermarked image quality, but it has limited embedding capacity. An improved implementation of pixel value ordering (IPVO)

system is reported by Ou et al [19]. The method has better embedding performance than other IPVO based reversible watermarking technique but the time and space complexity of the system are high. Recently, another improved pixel value ordering (IPVO) technique is proposed by Weng et al [20]. The system uses dynamic IPVO technique which offers better embedding performance with good visual quality.

To resolve the problems stated above, we proposed a novel reversible data hiding (watermarking) scheme that combining lifting based DWT with companding. The multi-resolution signal decomposition by wavelets transform reflects the anisotropic properties of the human visual system more exactly and helps to design data hiding scheme with high fidelity of the watermarked image [21,22]. Because of the small changes in wavelet coefficients distort the image very less. Moreover, unlike previously proposed reversible watermarking techniques [9], this novel approach does not use any location map. So the scheme does not require to embed the location map in the host image that ultimately helps to achieve high fidelity and greater payload capacity of the watermarked image. The proposed data hiding encoder select all the coefficients of high-High (*HH*) frequency sub-band to embed the watermark bits, whereas the decoder selects the same frequency sub-band to retrieve the embedded watermark bits. In other words, the data embedding technique modulates all the high-High (*HH*) sub-band co-efficient. So the proposed scheme does not require any location information but use the particular sub-band i.e., *HH* sub-band to decode the watermark bits. Hence the scheme does not require transmitting location map with the host data. This proposed location map free technique gives better payload capacity with good visual quality. The significant contributions are performance study in various lifting based DWT, Rayleigh fading wireless channel, and collusion attacks. The scheme can also unambiguously distinguish parties involved in collusion operation and innocent users. The simulation results demonstrated the performance efficiency of the proposed scheme. Side by side, the results are compared with related data hiding methods.

The rest of the paper is structured as follows: Section 2 describes the key features of the DICOM file format. Section 3 focuses on lifting based DWT transform. Section 4 discusses the basic of companding technique. Section 5 explores the algorithm for embedding and extracting the watermark. Section 6 presents the experimental results to show the effectiveness of the proposed data hiding method, and Section 7 describes conclusions and the scope of future work.

2. Key Features of DICOM File Format

Digital Imaging and Communications in Medicine (DICOM) is the international standard for formatting, exchanging, and storing medical images and related data for clinical use. It also includes a network communications protocol that uses TCP/IP to communicate between systems [23]. DICOM files can be interchanged between two persons that are capable of receiving images and patient information in DICOM file format. Digital medical images could be generated form diagnostic modalities such as Ultrasound, Nuclear Medicine, digital radiography, X-ray and hospital information system, etc. [24]. Nowadays, DICOM is used in radiology, cardiology imaging, radiotherapy device, ophthalmology, and dentistry. In other words, DICOM is widely used in most of the healthcare messaging standards in the world [24]. The digital watermarking techniques should employ necessary steps so that the quality of medical images are not degraded and are still conform with Digital Imaging and Communication in Medicine (DICOM) format. Any degradation of the medical image's quality could lead to misdiagnosis, and that is somewhat unacceptable. However, in the case of natural images, there is no such hard restriction about the quality of the watermarked natural image.

Each DICOM file has a header which contains the patient's name, type of scan, patient demographic information, acquisition parameters, practitioner & operator identifiers, and image dimensions, etc. The remaining portion of the DICOM file contains the image data. Because they often contain multiple high-resolution images, DICOM files tend to be large and are frequently compressed before storage and transfer [25]. An illustration of the basic file structure is shown in Figure 1. The header consists of a 128 byte File Preamble, followed by a 4-byte DICOM prefix. A Data Set represents an instance of

a real-world Information Object. A Data Set is constructed of Data Element. Data Elements contain the encoded values of attributes of that object. Figure 2 shows the DICOM data set and data element structures. The Data Element structure consists of the following fields: Tag, Value Representation, Value Length, and the Value [26].

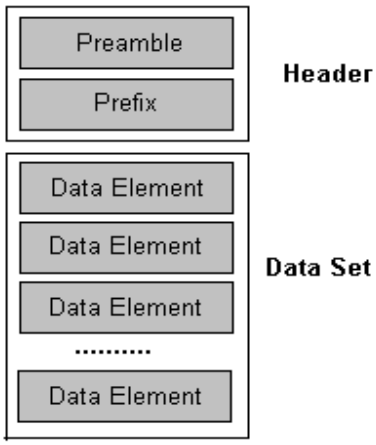


Figure 1. Basic file structure of DICOM image.

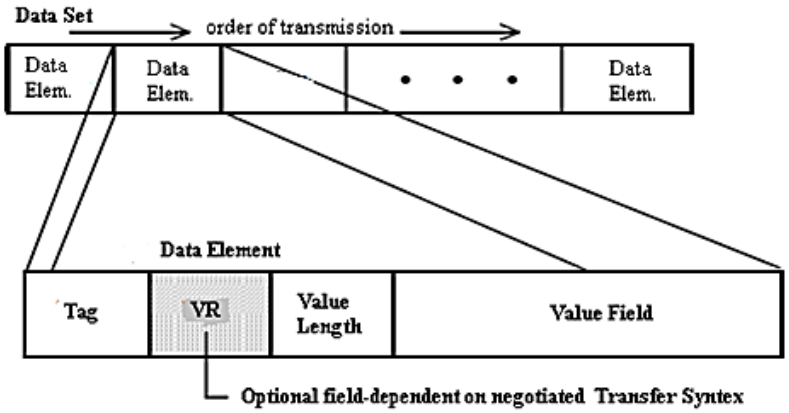


Figure 2. Detail of DICOM data set and data element structures. Source (Abd-Eldayem [26]).

(a) **Tag:** The identifier of the data element; it consists of 32 bits unsigned integer, 16 bits for the Group Number, and 16 bits of the Element Number.
(b) **Value Representation:** It specifies the data type of the value field (byte, integer, character).
(c) **Value Length:** It specifies the length of the value field (number of bytes).
(d) **Value:** It represents the data value of this data element.

3. Lifting Based DWT Transform

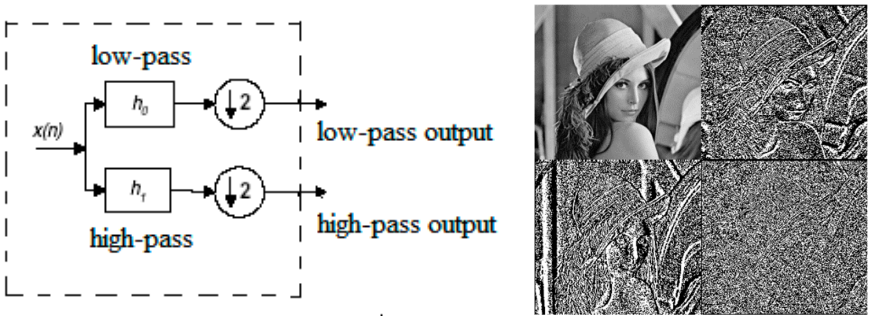
The lifting scheme is a technique for both designing fast wavelets and performing the discrete wavelet transform. The technique was introduced by Wim Sweldens. Lifting-based filtering consists of a sequence of very simple filtering operations for which alternately odd sample values of the signal are updated with a weighted sum of even sample values, and even sample values are updated with a weighted sum of odd sample values as described by Equations (1) and (2) [27,28].

$$y(2n+1) = X_{ext}(2n+1) - \frac{X_{ext}(2n) + X_{ext}(2n+2)}{2} \quad (1)$$

$$y(2n) = X_{ext}(2n) + \frac{y(2n-1) + y(2n+1) + 2}{4} \quad (2)$$

where, the notation X_{ext} representsas extended input. The notation y is the output signal and a indicates the largest integer not extending 'a'. The lifting based DWT is done by filtering operation on the row and column of the host image. It uses both high-pass and low-pass filter. It is seen that the process results in double the number of samples. So, the output from each filter is then down sampled by two that keeps the sample rate constant [29].

From Equations (1) and (2) it is also cleared that lifting based DWT creates correlation among the sample values. To validate the above argument, we calculate the entropy of different sub-bands for both traditional DWT and lifting based coefficients [30]. The average entropy values for different sub-bands of lifting based DWT are LL = 7.26, HL = 5.24, LH = 5.42, HH = 5.40, and for normal DWT, the values are LL = 10.41, LL = 8.30, LH = 6.78, HH= 8.62. The lesser values of entropy for lifting show that there exists a large correlation between the wavelets coefficients. In other words, there is low randomness and high similarity in the lifting based wavelets coefficients. Data hiding scheme takes the advantages of this redundancy to embed a large number of watermark bits for a given embedding distortion that helps in designing a better reversible process [30]. Moreover, lifting provides integer coefficients after transformation that ultimately results in the complete elimination of watermark bits at decoder compared to traditional DWT. For more information regarding various benefits of lifting operation over conventional DWT, interested readers may consult [31]. The lifting based DWT structure is shown in Figure 3a [30]. The number of levels of wavelet decomposition is application dependent. One level of decomposition is demonstrated in the present experimentation. The lifting based DWT decomposition using 'harr' transform is shown in Figure 3b.



(**a**) (**b**)

Figure 3. (**a**) The lifting based DWT structure; (**b**) 2-level lifting based DWT (haar) of the 8-bit Lena image. Source (Phadikar and Maity [30]).

4. Overview of Companding

Companding is a technique that is commonly used to implement nonuniform quantization in speech communications to achieve high signal-noise-ratio (SNR). The technique is based on compression (C) and expansion (E) function [32]. Commonly, the technique first compresses a signal and then expands it [4]. Here, compression does not mean to say data compression. Instead, compression here represents the change in a dynamic range of the original signal to a narrower range and after the expansion of the compressed signal; the expanded signal would be close to the original signal. Now, for a signal x, C and E correlate as follows:

$$E(C(x)) = x \tag{3}$$

If Equation (3) is satisfied, this technique can be effectively used in reversible data hiding [4]. However, in the case of the digital signal, C_Q and E_Q, respectively represent the quantized versions of C and E, where Q denotes quantization function [14]. The quantization function (C_Q) is represented as:

$$X_Q = C_Q(X) \tag{4}$$

$$C_Q(\mathrm{x}) = sign(x) \times \left(\frac{|x|}{2}\right) \tag{5}$$

where sign(·) is the sign function. The expansion function (E_Q) is represented as:

$$E_Q(\mathrm{x}) = sign(x) \times 2x \tag{6}$$

The value of companding error (r) is calculated as [14]:

$$r = |x| - \left|E_Q\left(C_Q(X)\right)\right| \tag{7}$$

Though there is a companding error (r) in the digital case, the present scheme neither does nor requires the information 'r', to loss lessly restore the image, unlike other techniques found in the literature. So in the present scheme, the effective capacity is equal to the size of the payload. It is also to be noted here that due to integer coefficients of lifting based DWT, companding technique would return low loss in watermarked image fidelity (due to floor function used in Equation (5)) than the traditional DWT that returns fractional value of coefficients after transformation.

Assume we have value x = 250, we would like to embed one bit W = 1. First, the value 'x' is divided by two based on Equation (5.) i.e., $C_Q(x) = \mathrm{sign}(x) \times \left(\frac{|250|}{2}\right) = 125$. Next, we represent the quantized value $C_Q(x)$ into its binary representation i.e., $C_Q(x) = 125 = (01111101)_2$. Then we append 'W' into the binary representation of $C_Q(x)$ after the least significant bit (LSB), the new modified value $C'_Q(x)$ will be $(01111101\mathrm{W})_2 = (011111011)_2$. Mathematically, this is equivalent to $2 \times 125 + 1 = 251$, which is considered as a watermarked coefficient. From the embedded coefficients, we can extract the embedded bit and restore the original coefficients. The watermark bits are extracted by investigating the least significant bit (LSB) of the watermarked signal.

5. Proposed Algorithm

The proposed reversible watermarking scheme consists of two main modules, namely, data encoding and data decoding. The encoding module hides a watermark into the cover image. On the other hand, the decoding scheme extracts the embedded watermark and also recovered the original host signal. The block diagrams of the proposed encoding and decoding process are described in Figures 4 and 5, respectively.

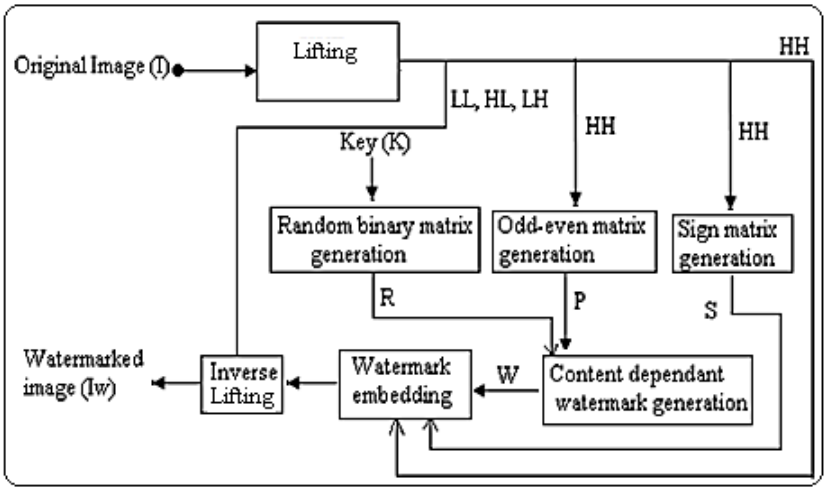


Figure 4. Data encoding.

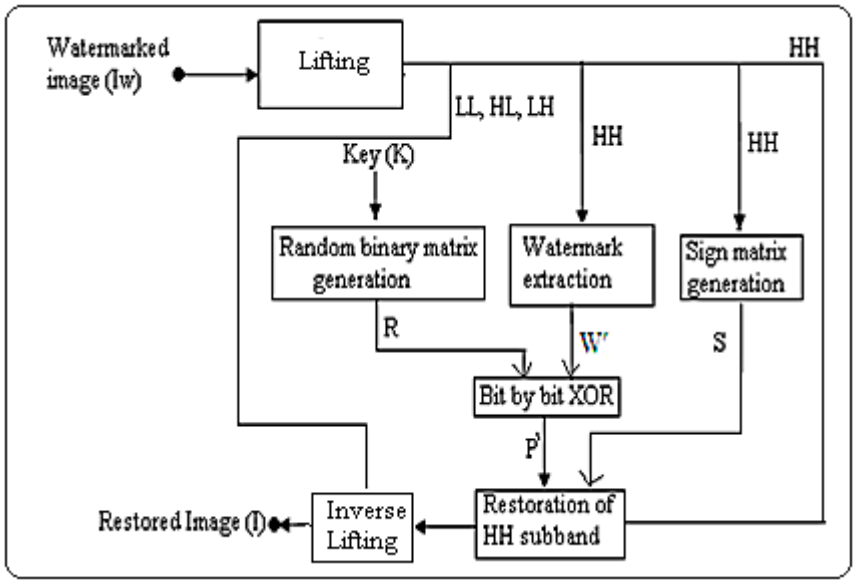


Figure 5. Data decoding.

5.1. Data Encoding

Step 1: Image transformation: Original host image (I) is decomposed into four sub-bands, i.e., low-low (LL), low-high (LH), high-low (HL), and high-high (*HH*) using lifting based DWT. One may use a higher level of decomposition for batter results.

Step 2: Selection of wavelets coefficients for watermark embedding: The scheme selects *HH* sub-bands, as this component contains both the characteristics of horizontal and vertical edge components. Moreover, the choice of embedding the watermark information into the *HH* sub-bands was motivated by experimental tests, as this one offers the best compromise between robustness and invisibility. Moreover, in the case of scalable decoding, if only the high-energy sub-bands are sent to the decoder, the watermark can be detected efficiently from those sub-bands without waiting for the others [30]. It is also to be noted here that if other sub-bands are used, then capacity will also be increased.

Step 3: Generation of the odd-even matrix: The odd-even matrix (*P*) is generated from *HH* sub-band according to the following rule.

$$P(x_i, y_i) = 1\ if HH(x_i, y_i) is odd.\ i = \{0, 1, ...n\} \tag{8}$$

$$P(x_i, y_i) = \ 0\ if HH(x_i, y_i)\ is even \tag{9}$$

It is to be pointed out that the size of *P* and *HH* are the same.

Step 4: Generation of sign matrix: A sign matrix (*S*) is generated from *HH* sub-band according to the following rule.

$$S(x_i, y_i) = \ 1\ if HH(x_i, y_i) is negative \tag{10}$$

$$S(x_i, y_i) = 0\ if HH(x_i, y_i) is positive \tag{11}$$

It is also to be pointed out that the size of *S* and *HH* are the same.

Step 5: Generation of random binary matrix based on user-defined key: A binary pseudorandom matrix (*R*)is created depending on the secret key (K) supplied by the owner.

Step 6: Generation of watermark bit: The straightforward countermeasure against the collusion (average) attack is done by designing the watermark that depends on the host signal. A content dependent watermark (*W*) is produced depending on *P*&*R*, according to the following rule.

$$W(x_i, y_i) = P(x_i, y_i) \oplus R(x_i, y_i) \tag{12}$$

The symbol '$\oplus$' represents bit by bit XOR operation.

Step 7: Change of dynamic range: The coefficients of *HH* bands are divided by two. This is analogous to compression operation as the above division operation changes the dynamic range of wavelet coefficient for the original host signal to a smaller range [4]. This operation will prevent overflow/underflow after data embedding.

$$HH_n(x_i, y_i) = floor(abs(HH(x_i, y_i))/2) \tag{13}$$

The symbol HH_n represents the high-high sub-band after the change of dynamic range. The function abs (.) returns the absolute value of a signal.

Step 8: Watermark bit embedding: Then the watermark bits are embedded into the *HH* sub-band according to the following rule:

$$HH_w(x_i, y_i) = 2 \times HH_n(x_i, y_i) + W(x_i, y_i) \tag{14}$$

The symbol HH_w represents the watermarked coefficients. Then the sign matrix(S) is multiplied with HH_w, to get the final watermarked *HH* sub-band.

Step 9: Inverse image transformation: Then, inverse lifting operation is done, and the watermarked image (I_w) is created.

5.2. Data Decoding

Step 1: Image transformation: Decompose the watermarked image (I_w) into 4-subbands, i.e., low-low (LL), high-low (HL), low-high (LH), and high-high (*HH*), using lifting.

Step 2: Watermark information (bit) extraction: The watermark bits (W') are extracted by investigating the least significant bit (LSB) of *HH* sub-bands.

Step 3: Generation of random binary matrix based on user-defined key: A binary pseudorandom matrix (R) is created depending on the secret key (K) supplied by the owner that was used at watermark embedding time.

Step 4: Extraction of odd-even matrix pattern: Then odd-even matrix pattern (P') is generated based on the extracted watermark W'.

$$P'(x_i, y_i) = W'(x_i, y_i) \oplus R(x_i, y_i) \tag{15}$$

Step 5: Generation of sign matrix: A sign matrix (S) is generated from *HH* sub-band, according to Equations (10) and (11).

Step 6: Restoration of HH sub-band of watermarked image: The watermarked *HH* sub-band is restored to its original form according to the following rule.

$$HH_R(x_i, y_i) = HH_w(x_i, y_i) + 1 \; if \; P'(x_i, y_i) = odd \; \& W'(x_i, y_i) = 0 \tag{16}$$

$$HH_R(x_i, y_i) = HH_w(x_i, y_i) - 1 \; if \; P'(x_i, y_i) = even \; \& W'(x_i, y_i) = 1 \tag{17}$$

$$HH_R(x_i, y_i) = HH_w(x_i, y_i) \; otherwise \tag{18}$$

The symbol HH_R represents the restored *HH* sub-band. Then inverse lifting operation is done to reconstruct the original host image (I).

6. Performance Evaluation

The performance of the proposed reversible watermarking scheme is evaluated over various DICOM medical images having diverse image features and characteristics. The test medical images are

of size (512 × 512). All experimentations are evaluated in Pentium 4, with 512 MB RAM and 2.80 GHz processor, by MATLAB 7.

The present study uses Mean-Structure-Similarity-Index-Measure (MSSIM) [33] and Peak–Signal-to-Noise-Ratio (PSNR) as distortion measures for the watermarked image. On the other hand, the relative entropy distance (Kullback Leibler distance (KLD)) [3] is used to quantify the security (K) of the proposed scheme. The large Peak–Signal-to-Noise-Ratio (PSNR) and Mean-Structure-Similarity-Index-Measure (MSSIM) values and low-security values of the watermarked medical image represent better imperceptibility and security of the hidden data, respectively [34]. PSNR is defined as:

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{\mathrm{MAX}^2}{\mathrm{MSE}}\right) \tag{19}$$

The symbol MAX represents the maximum gray value of pixel for the DICOM medical image. Mean Square Error (MSE) is represented as:

$$\mathrm{MSE} = \frac{1}{\mathrm{MN}}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[X(i,j) - x'(i,j)]^2 \tag{20}$$

where, the symbol 'X' is the gray value of the pixel for the original DICOM host image and 'X'' is the gray value of pixel for the watermarked DICOMimage. The symbol 'M' and 'N' are the height and width of the host image, respectively. MSSIM [33] is defined as:

$$\mathrm{MSSIM}\left(P,\overline{P}\right) = \frac{1}{M'}\sum_{j'=1}^{M'} SSIM\left(P_{j'},\overline{P_{j'}}\right) \tag{21}$$

where,

$$SSIM\left(P,\overline{P}\right) = \left[lu\left(P,\overline{P}\right)\right]^{\alpha}.\left[co\left(P,\overline{P}\right)\right]^{\beta}.\left[st\left(P,\overline{P}\right)\right]^{\gamma} \tag{22}$$

where the symbol 'P' and '$\overline{P}$' are the original and the distorted DICOM image signals, respectively. The symbol 'M'' represents the number of local windows in the DICOM image. The symbol 'Pj,' and '$\overline{P}_{j'}$' are the image information at the j'-th local window. The functions $\mathrm{lu}\left(P,\overline{P}\right)$, $\mathrm{co}\left(P,\overline{P}\right)$ and $\mathrm{st}\left(P,\overline{P}\right)$ are the luminance, contrast, and structure comparison functions respectively. The symbols α, β, and γ {where $\alpha > 0$, $\beta > 0$, $\gamma > 0$} are the parameters used to control the relative weight of the above components. The KLD (D(a||b)) is represented as [3]:

$$D(a||b) = \sum_{x\in X} a(x)\log\frac{a(x)}{b(x)} = E_a\log\frac{a(X)}{b(X)} \tag{23}$$

$$\text{with } 0\log\frac{0}{b} = 0, \text{ a } \log\frac{a}{0} = \infty$$

where the symbol $a(x)$ and $b(x)$ representsthe probability distribution functions (PDF) of the random variables R (i.e., original host image) and S (i.e., watermarked image), respectively. The symbol E_a represents the expectation concerning the joint distribution 'a'. If $a(X) = b(X)$ the security value is always non-negative or zero. On the other hand, the security value may be assumed to be 'K' if $D(a||b) \leq K$ [3]. In the proposed scheme, the normalized cross-correlation (NCC) is used to quantify the quality of the extracted watermark [34]. The NCC value between the original watermark image (W) and the extracted watermark image (W') is represented as:

$$\mathrm{NCC} = \frac{\sum_{\mathrm{i}}\sum_{\mathrm{j}} W_{ij}W'_{ij}}{\sum_{\mathrm{i}}\sum_{\mathrm{j}}\left(W_{ij}\right)^2} \tag{24}$$

Figure 6 shows the test images. Figure 7 shows the few decomposed images using lifting. Figures 8 and 9 show the watermarked images along with PSNR, MSSIM, and '*K*' values and also the restored images, respectively. From Figures 8 and 9, it is cleared that the watermark is embedded in the DICOM host image without decreasing the fidelity/quality of the image. Moreover, the image is restored completely by the proposed scheme.

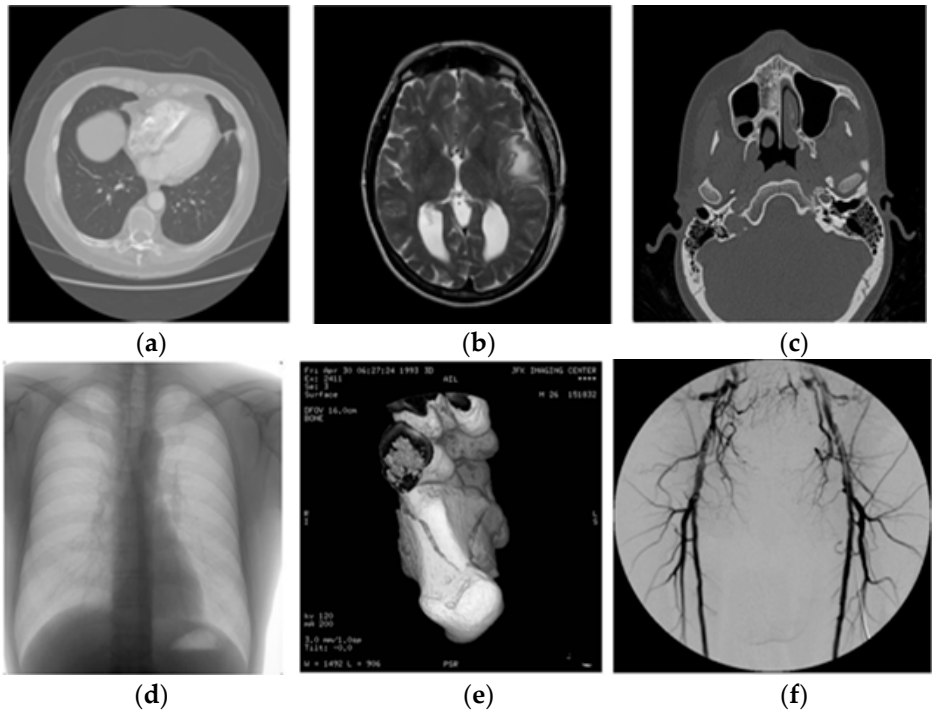


Figure 6. Original host image: (**a**) Lung, (**b**) MRI-1, (**c**) MRI-2, (**d**) Chest, (**e**) Ankle, (**f**) Retina.

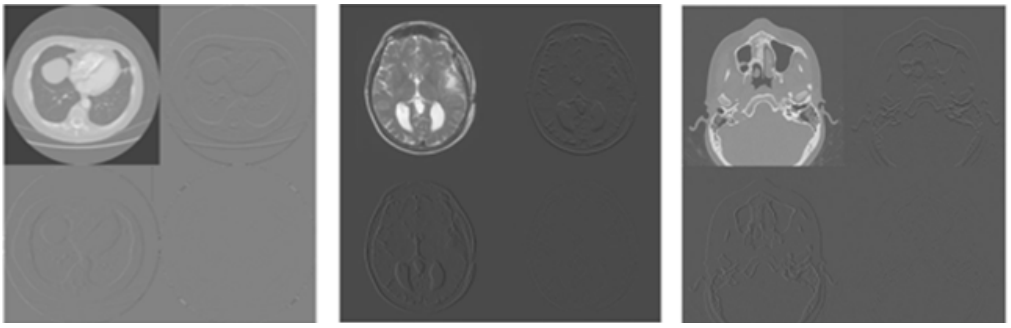


Figure 7. Decomposed host images using lifting based DWT: (**a**) Lung, (**b**) MRI-1, (**c**) MRI-2.

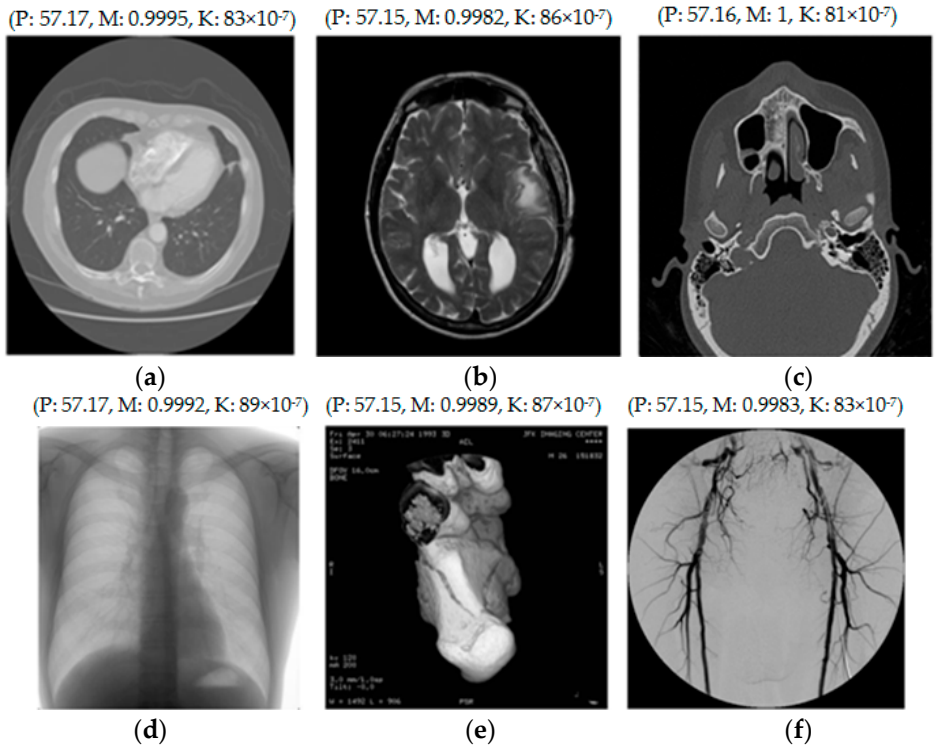


Figure 8. Watermarked image: (**a**) Lung, (**b**) MRI-1, (**c**) MRI-2, (**d**) Chest, (**e**) Ankle, (**f**) Retina. (P, M, K) above each image represents the PSNR (in dB), MSSIM and security values of the watermarked image.

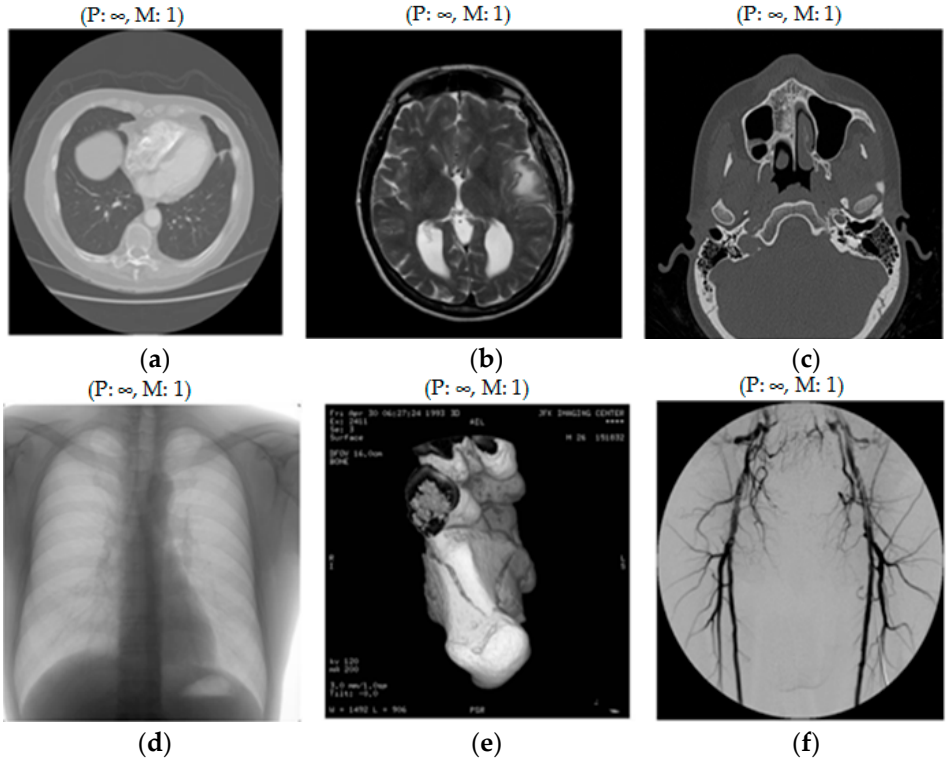


Figure 9. Reconstructed image: (**a**) Lung, (**b**) MRI-1, (**c**) MRI-2, (**d**) Chest, (**e**) Ankle, (**f**) Retina. (P, M) above each image represents the PSNR (in dB), MSSIM of the recovered image).

Table 1 shows the variation of PSNR, MSSIM, and KLD values for the images shown in Figure 6. As expected with the increase in payload size, the quality in term of PSNR (dB) of the watermarked

image is decreased. It is also seen that due to the increase of payload size, there is no such deviation in structural values of watermarked images. It is quite interesting to see that for MRI-2 image, and there is no change in structural value even if the payload size is increased to 65,536 bits. It is also to be noted that with the increase in payload size, the value of KLD is also increased. However, till the KLD value is very low and approaching to zero (0). That ensures that the scheme is secured. The performance of different lifting based wavelets on the test images is shown in Table 2. It is seen that 'haar', 'db1' and 'bior1.1' offers better performance than the other wavelets. On the other hand, the performance of various wavelets and their image security value for a fixed payload of 65,536 bits is shown in Table 3. It is seen that in all test cases, the KLD values are very less and approaching to zero (0). That ensures that the scheme is secured for all type of lifting based wavelets. Table 4 shows the variation of PSNR, MSSIM for different payload size (for Lung image), and wavelets. It is seen that 'Haar', 'db1' and 'bior1.1' offers better performance than the others wavelets even if the payload is increased to 65,536 bits.

Table 1. Variation of PSNR (dB), MSSIM and KLD values for different payload size using lifting based 'Haar' wavelets.

Images	Payload (in Bits)	2500	10,000	40,000	62,500	65,536
Lung	PSNR (dB)	71.42	65.31	59.33	57.40	57.17
	MSSIM	1	0.9998	0.9997	0.9996	0.9995
	KLD	4×10^{-7}	27×10^{-7}	69×10^{-7}	80×10^{-7}	83×10^{-7}
MRI-1	PSNR (dB)	71.33	65.42	59.29	57.37	57.15
	MSSIM	0.9999	0.9995	0.9989	0.9983	0.9982
	KLD	14×10^{-7}	37×10^{-7}	60×10^{-7}	83×10^{-7}	86×10^{-7}
MRI-2	PSNR (dB)	71.23	65.38	59.33	57.35	57.16
	MSSIM	1	1	1	1	1
	KLD	3×10^{-7}	25×10^{-7}	49×10^{-7}	78×10^{-7}	81×10^{-7}
Chest	PSNR (dB)	71.35	65.22	59.28	57.36	57.17
	MSSIM	1	0.9999	0.9995	0.9993	0.9992
	KLD	12×10^{-7}	30×10^{-7}	52×10^{-7}	84×10^{-7}	89×10^{-7}
Ankle	PSNR (dB)	71.42	65.29	59.31	57.37	57.15
	MSSIM	1	0.9999	0.9994	0.9989	0.9989
	KLD	9×10^{-7}	28×10^{-7}	49×10^{-7}	79×10^{-7}	87×10^{-7}
Retina	PSNR (dB)	71.31	65.36	59.33	57.38	57.15
	MSSIM	0.9999	0.9997	0.9991	0.9985	0.9983
	KLD	11×10^{-7}	25×10^{-7}	65×10^{-7}	81×10^{-7}	83×10^{-7}

Table 2. Performance evaluation of various lifting based wavelets in term of PSNR (dB), and MSSIM for the payload of 65,536 bits. (A) Lung, (B) MRI-1, (C) MRI-2, (D) Chest, (E) Ankle, (F) Retina. M: MSSIM; P: PSNR (in dB).

Wavelet Type	Images											
	A		B		C		D		E		F	
	M	P	M	P	M	P	M	P	M	P	M	P
haar	0.9995	57.17	0.9982	57.15	1	57.16	0.9992	57.17	0.9989	57.15	0.9983	57.15
db1	0.9950	57.14	0.9982	57.17	1	57.14	0.9942	57.12	0.9989	57.15	0.9983	57.14
sym2	0.9994	54.54	0.9978	55.05	1	54.11	0.9944	54.00	0.9981	54.15	0.9975	54.72
cdf1.1	0.9995	57.13	0.9982	57.16	1	57.15	0.9988	56.67	0.7349	40.86	0.9983	57.17
bior1.1	0.9995	57.16	0.9982	57.12	1	57.16	0.9992	57.14	0.9989	57.18	0.9983	57.17
rbio1.1	0.9979	51.15	0.9955	51.14	0.9999	51.14	0.9968	51.15	0.9948	51.11	0.9950	51.15
bs3	0.9990	53.15	0.9977	54.77	1	53.00	0.9985	54.05	0.9989	54.53	0.9972	53.94
coif1	0.9931	46.96	0.9942	49.10	0.9999	47.31	0.9932	47.73	0.9760	44.93	0.9916	48.60
rbs3	0.9947	47.92	0.9939	49.05	0.9999	47.96	0.9921	48.92	0.9858	45.94	0.9914	48.39
9.7	0.9970	47.95	0.9253	44.52	0.9999	48.04	0.9531	46.32	0.9955	49.77	0.9457	45.55
r9.7	0.9981	50.29	0.9940	50.34	0.9999	49.95	0.9924	50.12	0.9961	51.24	0.9937	50.26

Table 3. Performance measure of various lifting based wavelets in term of image security value (in KLD) for payload of 65,536 bits. (A) Lung, (B) MRI-1, (C) MRI-2, (D) Chest, (E) Ankle, (F) Retina.

Wavelet Type	Images					
	A	B	C	D	E	F
haar	83×10^{-7}	86×10^{-7}	81×10^{-7}	89×10^{-7}	87×10^{-7}	83×10^{-7}
db1	48×10^{-7}	7×10^{-7}	80×10^{-7}	65×10^{-7}	93×10^{-7}	86×10^{-7}
sym2	9×10^{-7}	1×10^{-6}	99×10^{-7}	27×10^{-7}	12×10^{-7}	3×10^{-6}
cdf1.1	5×10^{-7}	47×10^{-6}	48×10^{-7}	17×10^{-7}	163×10^{-7}	23×10^{-7}
bior1.1	15×10^{-7}	4×10^{-7}	38×10^{-4}	14×10^{-7}	1×10^{-10}	7×10^{-4}
rbio1.1	24×10^{-7}	1×10^{-4}	71×10^{-7}	6×10^{-7}	2×10^{-10}	24×10^{-7}
bs3	1×10^{-4}	6×10^{-4}	71×10^{-7}	15×10^{-8}	1×10^{-10}	39×10^{-4}
coif1	3×10^{-4}	4×10^{-4}	73×10^{-7}	19×10^{-8}	80×10^{-10}	5×10^{-4}
rbs3	55×10^{-7}	34×10^{-6}	10×10^{-7}	25×10^{-7}	62×10^{-72}	78×10^{-7}
9.7	44×10^{-6}	87×10^{-6}	7×10^{-7}	24×10^{-6}	8×10^{-6}	21×10^{-6}
r9.7	36×10^{-6}	51×10^{-7}	12×10^{-6}	51×10^{-6}	22×10^{-6}	2×10^{-7}

Table 4. Performance of various lifting based wavelets and variation of PSNR (dB), MSSIM for different payload size (Lung image). M: MSSIM; P: PSNR (in dB).

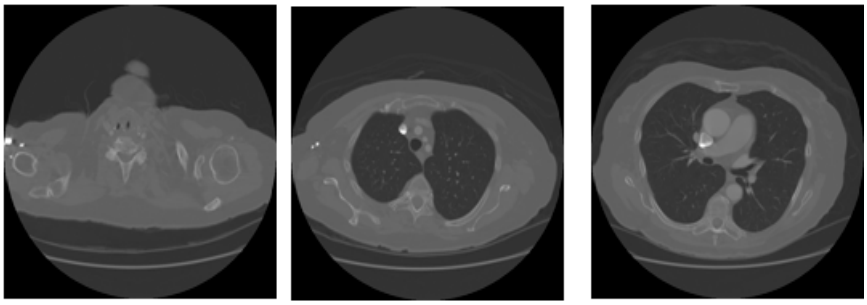
Wavelet Type	Payload (in Bits)									
	2500		10,000		40,000		62,500		65,536	
	M	P	M	P	M	P	M	P	M	P
haar	1	71.42	0.9998	65.31	0.9997	59.33	0.9996	57.40	0.9995	57.17
db1	1	71.33	0.9998	65.36	0.9997	59.33	0.9996	57.35	0.9995	57.17
sym2	1	70.25	0.9998	63.52	0.9996	56.57	0.9994	54.70	0.9994	54.56
cdf1.1	1	71.29	0.9998	65.33	0.9997	59.27	0.9996	57.34	0.9995	57.16
bior1.1	1	71.35	0.9998	65.33	0.9997	59.28	0.9996	57.32	0.9995	57.18
rbio1.1	0.9998	65.34	0.9993	59.31	0.9988	53.29	0.9981	51.34	0.9979	51.11
bs3	0.9999	67.26	0.9997	61.21	0.9994	55.25	0.9991	53.29	0.9990	53.09
coif1	0.9994	60.79	0.9976	54.53	0.9962	49.23	0.9939	47.21	0.9931	46.95
rbs3	0.9995	60.14	0.9981	54.49	0.9970	49.20	0.9952	47.24	0.9947	47.02
9.7	0.9998	63.17	0.9990	56.61	0.9981	50.06	0.9972	48.20	0.9970	48.01
r9.7	0.9998	65.22	0.9994	59.02	0.9988	52.36	0.9983	50.50	0.9982	50.35

To study the performance for collusion operation, we simulate fading like operation on watermarked DICOM image. We call this operation as a fading based collusion operation. Commonly, when collusion attack occurs on a continuous multimedia signal such as audio, video and DICOM images, the evaluation of time-varying weights (TVW) become vital which is equivalent to different gains in fading channels. Fading in communication channel means random deviation in received signal strength. This occurs as multiple copies of the same message signal are received over variable path lengths [35,36]. A robust Multi-Carrier-Code-Division-Multiple-Access (MC-CDMA) based fingerprinting scheme against time-varying collusion attack, which is analogous to fading, is proposed in [37]. The algorithm uses multicarrier approach for codeword generation (i.e., Hadamard-Walsh codes), time-varying channel response for colluder weight evaluation, and the Maximal Ratio Combining (MRC) detector [36]. It is quite reasonable to accept fading operation as collusion-like as colluders would develop an average watermarked DICOM frame through variable weights instead of equal weight to remove their identities.

To simulate collusion operations, five different watermarks (each watermark (W_i) is a pseudo-random binary sequence generated based on secret Key (K)) are embedded in host DICOM images and five different watermarked images are obtained. In the present scheme, we have tested the anti-collusion performance of the proposed reversible watermarking algorithm by transmitting first (in fact it is a random choice from the total set) four (e.g.) watermarked DICOM frame using MC-CDMA [35] through Rayleigh fading wireless channel. Transmission is done at different Signal-to-Noise-Ratio (SNR) values changing from 50 dB to 100 dB. In the present test, we keep SNR value to very high as DICOM images are very sensitive to noise than traditional images. The resultant received watermarked

DICOM frames are then averaged. Transmission of watermarked DICOM frames through Rayleigh fading channel followed by the averaging operation is one way of implementing collusion operation. In the mobile radio communication system, the low value of SNR suggests that the channel is under deep fade. On the other hand, the high value of SNR represents the opposite. In the present scenario, high and low SNR values represent light and heavy collusion operations, respectively [29]. We also test the anti-collusion performance of the proposed scheme by directly averaging watermarked DICOM frame, but without channel fading. This operation is called a non-fading based collusion operation.

Figure 10 shows a few frames from 'Lung' DICOM image database. Figure 11a shows a watermarked frame after non-fading based collusion operation. Figure 11b–f show watermarked DICOM frames after time-varying collusion attacks with different SNR (transmitting each watermarked DICOM frames through fading channel at different SNR values) and then averaged. Table 5 shows the BER (bit error rate) values for different watermarks extracted from the colluded average images. Low BER values indicate that the scheme is robust to fading like collusion operation. It is also seen that the BER values for *columns* 2–5 are quite low compared to the BER values in *column 6*. The low values of BER clearly indicate that the parties having watermarks, i.e., W_1, W_2, W_3, W_4, are identified as colluders. It is also quite clear from the numerical values of BER that parties involved in collusion operation would unambiguously be identified from the innocent users (W_5). Similar results are also obtained if different combinations of watermarked images in the set are used in collusion operations. Table 6 shows the average results for non-fading based collusion operation. High NCC values in Table 6 indicate that the scheme is also robust to non-fading based collusion operation. Table 7 shows the average value of the colluder identification performance of the proposed scheme.



(**a**)Frame 1 (**b**)Frame 25 (**c**)Frame 50

Figure 10. Lung DICOM image database.

Table 5. BER value of the extracted watermark for fading channel.

Watermarks	**W_1**	**W_2**	**W_3**	**W_4**	**W_5**
	Parties Involved in Collusion Operation				**Innocent Users**
SNR 50	0.0258	0.0287	0.0301	0.0267	0.412
SNR 60	0.0256	0.0283	0.0262	0.0263	0.521
SNR 75	0.0253	0.0271	0.0251	0.0251	0.432
SNR 85	0.0249	0.0262	0.0241	0.0242	0.665
SNR 100	0.0248	0.0258	0.0232	0.0238	0.612

Table 6. NCC values against non-fading based collusion attack.

No. of Averaged Frames	**2**	**4**	**6**	**8**
NCC	0.88	0.82	0.78	0.72

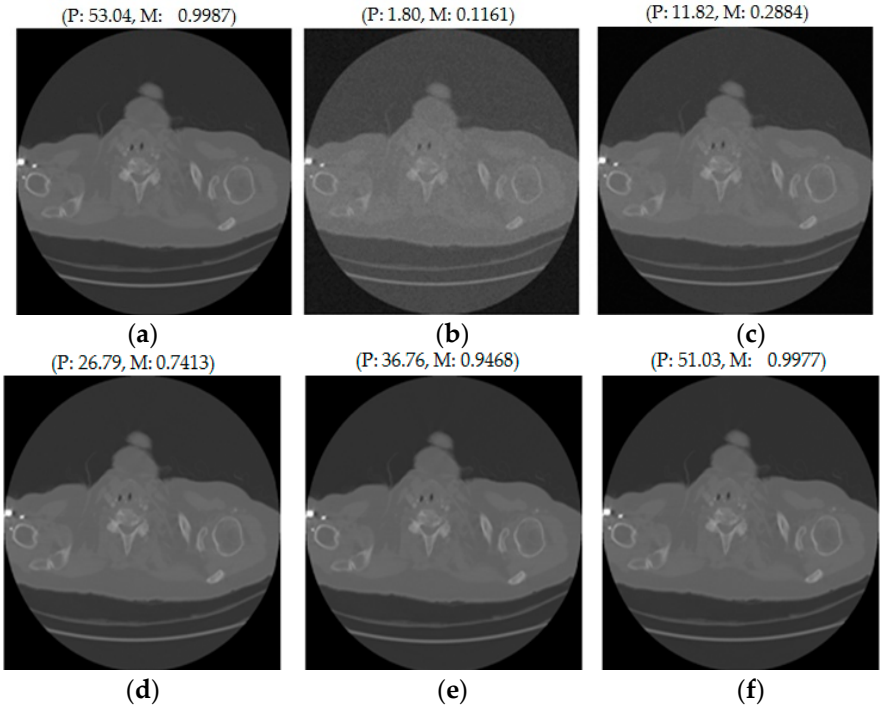


Figure 11. Results for collusion attack (Frame 1 of Lung DICOM image):(**a**) Averaged image without fading, (**b**–**f**): Results for different channel SNR, (**b**): SNR = 50 dB, (**c**): SNR = 60 dB, (**d**): SNR = 75 dB, (**e**): SNR = 85 dB, (**f**): SNR = 100 dB. (P, M) above each image represents the PSNR (in dB), and MSSIM values of the image.

Table 7. Colluder identification performance.

No. of Colluders	3	5	7	10
	No. of Identified Colluders			
Fading based (SNR 85)	3	5	6	7
Non-fading based	3	5	7	9

The collusion performance of the proposed method is also compared with previously reported works [18–20,38,39] to demonstrate the performance comparison. In the time of comparison of our system with the previously proposed ones, we have used reference implementations provided by the authors. It is observed from the results of Figure 12 that the proposed method offers better gain in term of NCC than the others. This is because the present scheme uses the content dependent watermark to resist the collusion attack. As expected, in Figure 12, we have seen that as the number of frames being combined increases, the NCC value decreases. It is also seen that there is a dip in the curve for [38] in Figure 12. This is due to the fact that in their experimentation, every 5thframe was extracted to form the actual set of test frames. So for every 5thframe, there is a valley in the graph.

The evaluation performance of the proposed reversible watermarking scheme is compared with the existing related works. Figure 13 shows the comparative performance in term of embedding capacity (in bpp) versus distortion in PSNR (dB). As expected, with the increase in the embedding capacity (payload), the PSNR (in dB) value decreases. As shown in the figure, the scheme proposed by [10] offers small PSNR (in dB) compared to other reversible watermarking schemes. In the other schemes, like difference-expansion (DE) proposed by [9,11–13] the tradeoff between capacity and image quality is possible and relatively high PSNR can be achieved. However, as shown in the figure, the proposed scheme offers higher embedding capacity with lower distortion than the other schemes [18–20]. This is due to the joint use of lifting and companding technique.

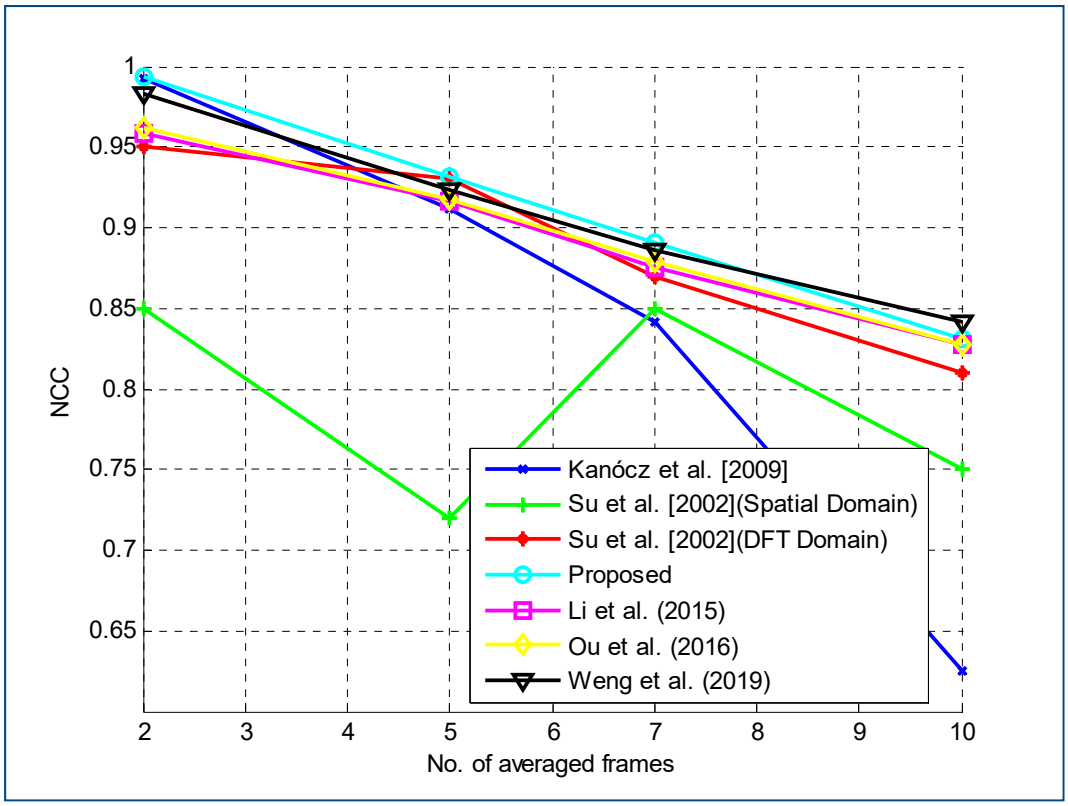


Figure 12. Comparative performance against collusion attack.

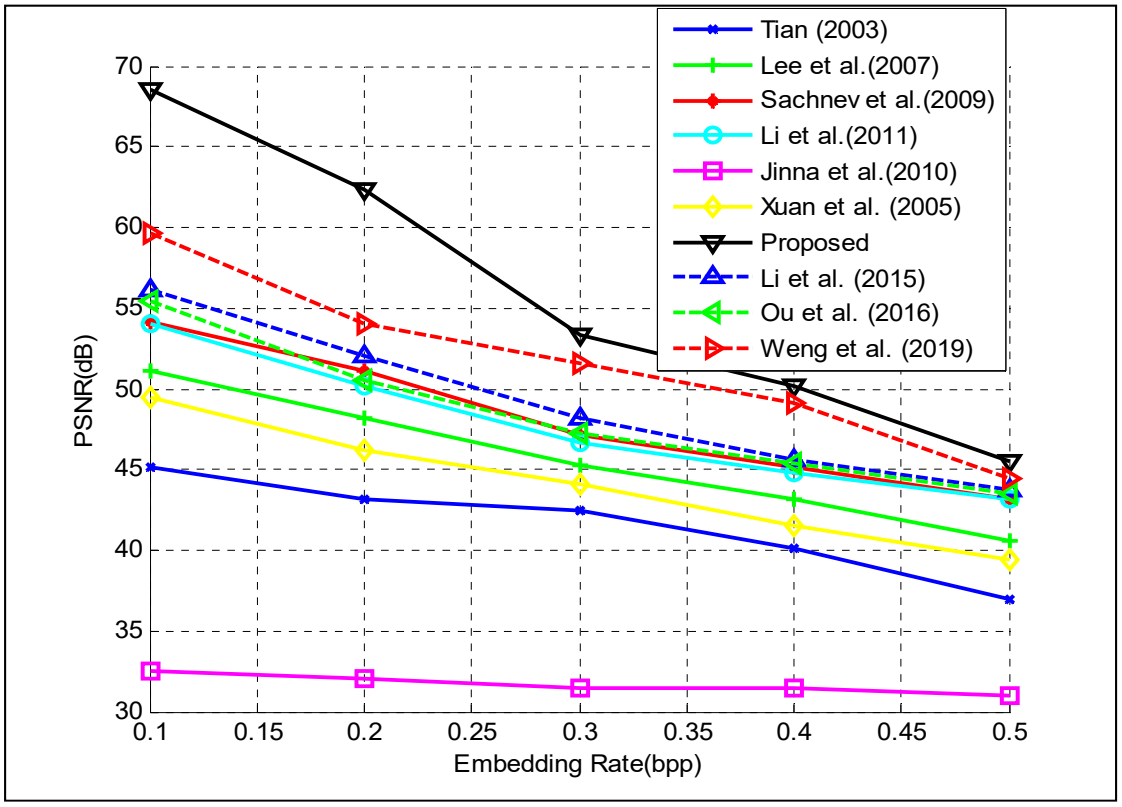


Figure 13. Capacity vs. distortion comparison.

The execution time required to run the whole procedure as a measure of the computational load is also computed. The scheme takes on an average of 1.3543 s. We have also tested the same procedure for traditional DWT. It is seen that the average execution time is 2.1086 s. This result clearly shows that the proposed scheme is much faster than convention DWT based scheme.

7. Conclusions

In this study, a reversible watermarking technique is proposed based on lifting and companding for DICOM image. The investigation results show that the proposed watermarking scheme offers high embedding capacity with no compromise in watermarked image fidelity and security. Moreover, the scheme is also robust to fading and non-fading based collusion attacks. It is seen that the proposed scheme is cost-effective, simple, and easy to implement and can be used as a possible solution for hospital data management (HDM). Future work can be done on further performance enhancement of the proposed scheme using anti-collusion code and channel coding. Lastly, hardware implementation of the proposed scheme based on SPARTAN-3 *FPGA–development* kit is also to be done as future work.

Author Contributions: A.P. and P.J. designed the experiments and performed the implementation; A.P., P.J. and H.M. analyzed the data and wrote the paper.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Qasim, A.F.; Meziane, F.; Aspin, R. Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review. *Comput. Sci. Rev.* **2018**, *27*, 45–60. [CrossRef]
2. Agarwal, N.; Singh, A.K.; Singh, P.K. Survey of robust and imperceptible watermarking. *Multimed. Tools Appl.* **2019**, *78*, 8603–8633. [CrossRef]
3. Maity, S.P.; Kundu, M.K.; Nandi, P.; Das, T.S. Robust image watermarking using multiresolution analysis. In Proceedings of the IEEE INDICON 2004 First India Annual Conference, Kharagpur, India, 20–22 December 2004; pp. 174–179.
4. Xuan, G.; Yang, C.; Zhen, Y.; Shi, Y.Q.; Ni, Z. Reversible data hiding using integer wavelet transform and companding technique. In *International Workshop Digital Watermarking*; Springer: Berlin/Heidelberg, Germany, 2005; Volume 3304, pp. 115–124.
5. Juhola, M.; Joutsijoki, H.; Aalto, H.; Hirvone, T.P. On classification in the case of a medical data set with a complicated distribution. *Appl. Comput. Inform.* **2014**, *10*, 52–67. [CrossRef]
6. Bidgood, S.W.D.; Horii, C.; Prior, F.W.; Van Syckle, D.E. Understanding and using DICOM, the data interchange standard for biomedical imaging. *JAMIA Open* **1997**, *4*, 199–212.
7. Honsinger, C.W.; Jones, P.; Rabbani, M.; Stoffel, J.C. Lossless Recovery of an Original Image Containing Embedded Data. U.S. Patent 6,278,791, 21 August 2001.
8. Tang, Z.; Xu, S.; Yao, H.; Qin, C.; Zhang, X. Reversible data hiding with differential compression in encrypted image. *Multimed. Tools Appl.* **2018**, *78*, 9691–9715. [CrossRef]
9. Tian, J. Reversible data embedding using a difference expansion. *IEEE Trans. Circuits Syst. Video Technol.* **2003**, *13*, 890–896. [CrossRef]
10. Jinna, S.K.; Ganesan, L. Analysis of reversible image watermarking using bit plane coding and lifting wavelet transform with attacks. In Proceedings of the IEEE International Conference on Communication Control and Computing Technologies, Ramanathapuram, India, 7–9 October 2010; pp. 628–636.
11. Xiaolong, L.; Yang, B.; Zeng, T. Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection. *IEEE Trans. Image Process.* **2011**, *20*, 3524–3533. [CrossRef] [PubMed]
12. Lee, S.; Yoo, C.D.; Kalker, T. Reversible image watermarking based on integer-to-integer wavelet transform. *IEEE Trans. Inf. Forensics Secur.* **2007**, *2*, 321–331. [CrossRef]
13. Sachnev, V.; Kim, H.J.; Nam, J.; Suresh, S.; Shi, Y.Q. Reversible watermarking algorithm using sorting and prediction. *IEEE Trans. Circuits Syst. Video Technol.* **2009**, *19*, 989–999. [CrossRef]

14. Weng, S.; Zhao, Y.; Pan, J.; Ni, R. A novel reversible watermarking based on an integer transform. In Proceedings of the IEEE International Conference on Image Processing, San Antonio, TX, USA, 16 September–19 October 2007; pp. 241–244.
15. Liu, L.; Wang, L.; Shi, Y.Q.; Chang, C.C. Separable data-hiding scheme for encrypted image to protect privacy of user in cloud. *Symmetry* **2019**, *11*, 82. [CrossRef]
16. Das, M.L.; Samdaria, N. On the security of SSL/TLS-enabled applications. *Appl. Comput. Inform.* **2014**, *10*, 68–81. [CrossRef]
17. Vigila, S.M.C. A new elliptic curve cryptosystem for securing sensitive data applications. *Int. J. Electron. Secur. Digit. Forensics* **2013**, *5*, 11–24. [CrossRef]
18. Li, X.; Zhang, W.; Gui, X.; Yang, B. Efficient reversible data hiding based on multiple histograms modification. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 2016–2027.
19. Ou, B.; Li, X.; Wang, J. Improved PVO-based reversible data hiding: A new implementation based on multiple histograms modification. *J. Vis. Commun. Image Represent.* **2016**, *38*, 328–339. [CrossRef]
20. Weng, S.; Shi, Y.; Hong, W.; Yao, Y. Dynamic improved pixel value ordering reversible data hiding. *Inf. Sci.* **2019**, *489*, 136–154. [CrossRef]
21. Phadikar, A.; Maity, S.P.; Mandal, M.K. QIM data hiding for tamper detection and correction in digital images using wavelet transform. In Proceedings of the 22nd IEEE Canadian Conference on Electrical and Computer Engineering, Calgary, AB, Canada, 2–5 May 2010; pp. 1–5.
22. Jana, P.; Phadikar, A.; Maity, S.P.; Chakraborty, D.P. Reversible data hiding using wavelet transform and companding for DICOM image. In Proceedings of the 1st International Conference on Industrial Engineering Science and Applications, Durgapur, India, 2–4 April 2014; pp. 197–201.
23. Lu, X.; Zhang, M.; Yang, L.; Zhao, Y.; Liu, J. Research and implementation of medical images management system based on DICOM standard. In Proceedings of the International Conference on Biological and Biomedical Sciences Advances in Biomedical Engineering, Bangkok, Thailand, 7–8 April 2012; pp. 140–146.
24. Genereaux, B.W.; Dennison, D.K.; Ho, K.; Horn, R.; Silver, E.L.; O'Donnell, K.; Kahn, C.E. DICOMweb™: Background and application of the web standard for medical imaging. *J. Digit. Imaging* **2018**, *31*, 321–326. [CrossRef]
25. Standard. *Digital Imaging and Communications in Medicine (DICOM)*; Part 5: Data Structures and Encoding; National Electrical Manufacturers Association: Rosslyn, VA, USA, 2004; pp. 1–106.
26. Abd-Eldayem, M.M. A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine. *Egypt. Inform. J.* **2013**, *14*, 1–13. [CrossRef]
27. Boliek, M.; Christopoulos, C.; Majani, E. JPEG 2000 Part I Final Draft International Standard. (ISO/IEC FDIS15444-1), ISO/IEC JTC1/SC29/WG1 N1855. 2000. Available online: https://pdfs.semanticscholar.org/1be5/a1b60ce2f9fecfd816edf8263ae35b61d17c.pdf (accessed on 18 August 2000).
28. Adams, M.D.; Kossentini, F. Reversible integer-to-integer wavelet transforms for image compression: Performance evaluation and analysis. *IEEE Trans. Image Process.* **2000**, *9*, 1010–1024. [CrossRef]
29. Phadikar, A.; Maity, S.P.; Delpha, C. Image error concealment and quality access control based on data hiding and cryptography. *Int. J. Telecommun. Syst.* **2012**, *49*, 239–254. [CrossRef]
30. Phadikar, A.; Maity, S.P. Data hiding based quality access control of digital images using adaptive QIM and lifting. *J. Signal Process. Image Commun.* **2011**, *26*, 646–661. [CrossRef]
31. Uytterhoeven, G.; Roose, D.; Bultheel, A. *Wavelet Transforms Using Lifting Scheme*; Technical Report ITA-Wavelets Report; Department of Computer Science, Katholieke Universiteit Leuven: Leuven, Belgium, 1997.
32. Sklar, B. *Digital Communications: Fundamentals and Applications*; PTR Prentice Hall: Englewood Cliffs, NJ, USA, 2017.
33. Wang, Z.; Bovik, A.C.; Sheikh, H.R.; Simoncelli, E.P. Image quality assessment: From error measurement to structural similarity. *IEEE Trans. Image Process.* **2004**, *13*, 1–14. [CrossRef]
34. Phadikar, A.; Maity, S.P. Multibit QIM watermarking using M-ary modulation and lifting. In Proceedings of the 2010 International Conference on Signal Processing and Communications, Bangalore, India, 18–21 July 2010; pp. 1–5.
35. Maity, S.P.; Mukherjee, M. Subcarrier PIC scheme for high capacity CI/MC-CDMA system with variable data rates. In Proceedings of the IEEE Mobile WiMAX'09, Napa Valley, CA, USA, 9–10 July 2009; pp. 135–140.
36. Maity, S.P.; Kundu, M.K. Perceptually adaptive spread transform image watermarking scheme using Hadamard transform. *Inf. Sci.* **2011**, *181*, 450–465. [CrossRef]

37. Cha, B.H.; Jay Kuo, C.C. Robust MC-CDMA-based fingerprinting against time-varying collusion attacks. *IEEE Trans. Inf. Forensics Secur.* **2009**, *4*, 302–317. [CrossRef]
38. Su, K.; Kundur, D.; Hatzinakos, D. A novel approach to collusion-resistant video watermarking. In Proceedings of the SPIE Security and Watermarking of Multimedia Contents, San Jose, CA, USA, 29 April 2002; pp. 491–502.
39. Kanocz, T.; Tokar, T.; Levicky, D. Robust frame by frame video watermarking resistant against collusion attacks. In Proceedings of the IEEE International Conference on Radioelektronika, Bratislava, Slovakia, 22–23 April 2009; pp. 99–102.