https://doi.org/10.31436/iiumej.v24i1.2597

ROBUST AND IMPERCEPTIBLE WATERMARKING ON MEDICAL IMAGES USING COEFFICIENT PAIR MODIFICATION

LEDYA NOVAMIZANTI[1,3*], ANDRIYAN BAYU SUKSMONO[2], DONNY DANUDIRDJO[2], GELAR BUDIMAN[3]

[1]*Electrical Engineering and Informatics, School of Electrical Engineering and Informatics, Institut Teknologi Bandung, Bandung, Jawa Barat, Indonesia*
[2]*School of Electrical Engineering and Informatics, Institut Teknologi Bandung, Bandung, Jawa Barat, Indonesia*
[3]*School of Electrical Engineering, Telkom University, Bandung, Jawa Barat, Indonesia*

**Corresponding author: ledyaldn@telkomuniversity.ac.id*

*(Received: 7th September 2022; Accepted: 3rd October 2022; Published on-line: ** *** 2023)*

ABSTRACT: Sensitive data including medical images and electronic patient records (EPR) have potential value in the era of big data and telemedicine applications. Distribution of medical images and EPR over public networks requires a high level of privacy and security. Robust and imperceptible watermarking techniques are needed to provide copyright preservation for medical images and protect patient information security. This paper improves the technique of Coltuc *et al.* by modifying the discrete cosine transform (DCT) coefficient pairs in the watermark embedding formula. Our proposed formula ensures that the difference between the two coefficients is at least ζ. If the difference between the two coefficients is less than ζ, then the new pixels are modified so that the difference is equal to ζ. The proposed method was evaluated on a variety of medical images, including X-ray, CT, US, MRI, and Colonoscopy, and compared to numerous robust watermarking techniques of the recent time. The experimental results demonstrate that the suggested method outperforms contemporary robust watermarking techniques in terms of imperceptibility, robustness, and security. The peak signal noise ratio (PSNR) for all modalities of watermarked medical images exceeds 54 dB, and the average PSNR is approximately 56 dB. The proposed method is outstanding compared to Coltuc's method due to a 93% and 14% increase in bit error rate (BER) and normalized correlation (NC), respectively. Our work is superior to various state-of-the-art robust watermarking techniques, allowing it to be employed effectively in medical applications.

ABSTRAK: Data sensitif termasuk imej perubatan dan rekod pesakit elektronik (EPR) mempunyai potensi nilai dalam era aplikasi data besar dan teleperubatan. Pengedaran imej perubatan dan EPR melalui rangkaian awam memerlukan tahap privasi dan keselamatan yang tinggi. Teknik penanda air yang mantap dan tidak dapat dilihat diperlukan untuk menyediakan pemeliharaan hak cipta untuk imej perubatan dan melindungi keselamatan maklumat pesakit. Kertas kerja ini menambah baik teknik Coltuc *et al.* dengan mengubah suai pasangan pekali transformasi kosinus diskret (DCT) dalam formula pembenaman tera air. Formula yang dicadangkan kami memastikan bahawa perbezaan antara dua pekali adalah sekurang-kurangnya ζ. Jika perbezaan antara dua pekali kurang daripada ζ, maka piksel baharu diubah suai supaya perbezaannya sama dengan ζ. Kaedah yang dicadangkan telah dinilai pada pelbagai imej perubatan, termasuk X-ray, CT, US, MRI, dan Kolonoskopi, dan dibandingkan dengan banyak teknik penanda air yang mantap pada masa terkini. Keputusan eksperimen menunjukkan bahawa kaedah yang dicadangkan mengatasi teknik penanda air teguh kontemporari dari segi ketidakjelasan, keteguhan dan keselamatan. Nilai PSNR untuk semua

https://doi.org/10.31436/iiumej.v24i1.2597

modalitas imej perubatan bertanda air melebihi 54 dB, dan nilai purata PSNR adalah lebih kurang 56 dB. Kaedah yang dicadangkan adalah cemerlang daripada kaedah Coltuc kerana masing-masing peningkatan 93% dan 14% dalam BER dan NC. Kerja kami lebih unggul daripada pelbagai teknik penanda air teguh terkini, membolehkan ia digunakan dengan berkesan dalam aplikasi perubatan.

KEY WORDS: *DCT, Imperceptible, Medical Image, Robust, Watermarking.*

1. INTRODUCTION

Information and communication technology (ICT) is essential to all sectors of society, including government, banking, education, health, agriculture, and transportation. ICT integrates computer systems, digital data, communication devices, and the internet into one unified system. An important use of ICT for effective quality health care is the electronic storage of medical data. The information in the electronic medical data storage, including: patient identities, diagnosis reports, doctor's consultations, hospital information where the image was created, and other helpful information, can be used anywhere and anytime [1]–[3]. Medical data is susceptible and has great potential value in the era of big data because it is the most important basis for diagnosis in determining diagnostic methods and results [4], [5]. Through public networks like the internet, medical professionals frequently exchange digitally created medical images of patients created using various modalities. Radiologists and doctors in the same field share these images for clinical interpretation [6].

Medical professionals use telemedicine applications to remotely diagnose, evaluate, and treat patients via electronic communications. The program facilitates the transmission of medical images between two healthcare providers for improved diagnosis. However, medical image and EPR delivery over public networks demand a high level of security [7]. Modified, manipulated, or distorted medical data can cause incorrect diagnoses and severe health issues for everyone. In addition, the destruction and theft of medical images and identities can give rise to various legal and ethical concerns, including image retention and fraud, piracy, and illegal handling [1]. In contrast to financial institutions, which have robust data protection methods through two-factor authentication, medical records in healthcare systems are poorly protected. Medical facilities must secure data from illegal actions such as hacking and virus intrusion, staff negligence, and the theft of medical records on purpose [3]. The transfer of data in an intelligent healthcare system while preserving privacy, integrity, authority, and security is a complex topic that requires additional consideration [4].

Digital watermarking is a common approach for concealing digital information by masking signals [8] due to its additional qualities of robustness and imperceptibility. Digital watermarking technology is becoming crucial for various fields since it offers a variety of compact solutions for numerous approaches and applications, such as cloud computing, electronic health, and the Internet of Things [2], [11]. Watermarking of digital images is allowed in two domains, i.e., the spatial domain and the frequency domain. In the spatial domain of watermarking technology, personal information is integrated directly into the cover image by modifying the pixel values [3], [9]. In frequency domain watermarking, the cover image is first translated into the frequency domain, and then the hidden data is embedded by modifying the frequency coefficient value [3], [9]. Watermarking is also categorized based on the method of watermark extraction. Non-blind techniques require both the host and the watermark image to extract the watermark. A semi-blind watermark requires a secret key and a watermarked image to extract the watermark. If only the secret key is required to extract the

https://doi.org/10.31436/iiumej.v24i1.2597

watermark, the approach is known as blind watermarking [10]. Based on the application, watermarking techniques can be classified as either robust or fragile [1], [5].

The robustness of confidential information, and how the encoded information can withstand attacks conducted by attackers during data transmission, is the primary goal of robust watermarking [9]. Robust watermarking is therefore widely used to preserve digital data's copyright. However, fragile watermarking [1] is used to identify the invader-damaged portions of the watermarked image, i.e., those regions of the image that were damaged during transmission. The integrity of digital data material is therefore verified using fragile watermarking. Processing time for spatial domain-based watermarking is lower than for methods that embed data in the transformation domain. However, compared to transformation-based strategies, spatial domain-based approaches are less resistant to attacks [7]. Two key requirements for creating effective watermarking methods are imperceptibility and robustness [6].

Compared to watermarking in the spatial domain, watermarking in the frequency domain offers additional benefits. That is why many researchers use frequency domain watermarking techniques. DCT is one of the widespread transformations and is often chosen in frequency domain watermarking techniques [6] because of its lower computational cost, high robustness and high compression [11]. In [12], [13], the watermark was embedded by Coltuc and Chassery using the DCT domain watermarking method. The image is divided into 8×8 blocks. Next, DCT for each block is determined. One bit of information entered into each block depends on the difference between the two coefficients of the mid-band frequency. For example, bit "1" is encoded if the difference is negative, and a bit "0" otherwise. If the relative size of each coefficient does not match the bit to be encoded, the coefficients are swapped. The interchange of these coefficients does not considerably alter the watermarked image because the mid-frequency DCT coefficients have almost identical magnitudes. However, this method can cause errors due to the rounding case of DCT. As a result, not all watermarks can be extracted properly.

Coltuc's method is improved by modifying the DCT coefficient pairs in the watermark embedding formula. Our proposed formula ensures that the difference between the two coefficients is at least ζ. If the difference between the two coefficients is less than ζ, then the new pixels are modified so that the difference is ζ. The new watermarking system on medical images based on the modification of DCT coefficient pairs is proposed to achieve the following objectives: (1) to achieve good imperceptibility from watermarked images; (2) to provide intellectual property protection for medical images; (3) to preserve the safety of patient data [6].

This paper is additionally organized as follows: Section 2 discusses the most recent medical image watermarking approaches appropriate to the proposed methodology. Section 3 explains the fundamentals of DCT and the methods proposed by Coltuc *et al.* The procedure for watermark insertion and extraction is described in Section 4. Section 5 covers the experimental outcomes and analysis. In the last section, conclusions and future research are offered.

2. RELATED WORKS

The discrete cosine transform (DCT), which has energy compaction features, is frequently employed in watermarking approaches. DCT can convert an image into a frequency band, which can be inverted to transform it back into the original image. Following the DCT process, the image pixels are turned into coefficients. Direct current (DC) is represented by the first

https://doi.org/10.31436/iiumej.v24i1.2597

coefficient DCT in the base array function's upper left corner, while the remaining coefficients represent alternating current (AC). Since the AC is so crucial to an image, any modifications to the AC can significantly affect the image. On the other hand, slight adjustments to the image have little impact on the AC.

Thanki *et al.* [14] developed a watermarking technique for medical images based on fast discrete curvelet transform (FDCuT) and DCT. The block-wise DCT is applied to the medical image's high-frequency curvelet coefficient. A white Gaussian noise (WGN) order is added to the original image's mid-band frequency coefficient in compliance with the watermark bit to create a watermarked medical image. Images from X-rays, ultrasounds, MRIs, and computed tomography (CT) scans were utilized to evaluate how the suggested watermarking technique worked. The study results show that watermarks are more invisible in all types of medical images with PSNR above 45 dB. However, two uncorrelated WGN sequences generated during the embedding process are required to recover the watermark. Therefore, only binary watermarks may be embedded using this technique; text-based EPR data cannot be. Another drawback is that the resulting watermark image always contains noise.

Novamizanti *et al.* [15] introduced the singular value decomposition (SVD) method to medical image watermarking techniques based on FDCuT and DCT. Watermark embedding by exchanging the singular value of the watermark and the host image result from the FDCuT and DCT transformations. The proposed algorithm has good imperceptibility with interval PSNR values [53, 54]. However, this watermarking scheme is semi-blind, where it is necessary to output SVD results from the original watermark image at the extraction stage. This method is not resistant to blurring and geometry attacks.

Lei *et al.* [16] reported a robust image watermarking algorithm based on DCT domain and QIM. The host signal's medium and low-frequency DCT coefficient is divided into two regions. Then the watermark bit is embedded by quantizing the ratio of the two halves. According to experimental findings, this method is only superior against attacks of the common type. This algorithm has limited capacity, where a 512×512 image host can only accommodate a 128-bit watermark. Then, the optimal parameter for each image is obtained as PSNR of 41 dB.

Zhu *et al.* [17] presented a robust image steganography algorithm for JPEG compression. Firstly, a candidate DCT coefficient unaffected by JPEG compression is chosen. Second, the proposed distortion function gives each potential DCT coefficient a cost. The error correction code and the Syndrome Trellis Code help the method become even more robust and invisible. This algorithm's embedding capacity remains restricted to payloads between 0.01 and 0.1 bpnzAC. For 512×512 image hosts, the proposed algorithm only produces PSNR values at the [42, 47] dB interval.

Rachmawanto *et al.* [18] designed an image watermarking algorithm using block-based DCT, where the DC coefficient is chosen to keep the watermark resistance included. The Beaufort cipher is used for the encryption process and the watermark distribution when inserted. The goal is to improve watermark security and imperceptibility aspects. Generally, the spread spectrum watermarking technique uses PN Sequence for watermark deployment. However, the proposed method is non-blind, where the cover image is still required for the watermark extraction process.

An image watermarking technique based on DCT was researched by Byun *et al.* [19]. First, the DCT coefficient for the specified location is determined. Next, the variation value is calculated to adjust the coefficient under the embedding bit and quantization step. Finally, the watermark bit is inserted directly into the pixel value without using a full-frame DCT. According to the findings, the suggested watermarking technology offers less computing

https://doi.org/10.31436/iiumej.v24i1.2597

complexity and ensures robustness. A color host image with a size of 512×512 can only accommodate a watermark of 1024 bits, indicating that the embedding capacity of this technique is still constrained. The proposed method's average PSNR is about 42 dB.

Ko *et al.* [20] reported a watermarking method based on the correlation of DCT coefficients between blocks. The coefficient variance in the two blocks of DCT is calculated and changed depending on the watermark bits to adjust this difference to a specified range. The level of the DCT coefficient's modification is based on the DC coefficient and the median of the alternating current (AC) coefficient, which is ordered in zigzag order. The experimental findings demonstrate the robustness of the suggested technique against several single and combined attacks. For the Lena watermarked image, only 41.6 dB PSNR is obtained. In addition, the resistance is weak against types of noise attacks, including BER is 17.06 for salt-and-pepper noise and 9.98 for Gaussian noise.

A robust watermarking technique based on DCT, speeded up robust features (SURF), and perceptual hashing was proposed by Nawaz *et al.* [21]. The watermark image is preprocessed to enhance its security using affine transformation with feature matrix and chaotic encryption technology. SURF feature points are utilized to choose the DCT region and extract scalable watermarks after geometric rectification during the extraction process. Studies reveal that the algorithm efficiently defends against geometric and conventional attacks and can effectively maintain the security of images with an NC value higher than 90%. However, this paper does not report the PSNR results from the watermarked images without attack. This technique utilizes a correlation function to confirm the similarity of the derived watermarks. Hence scrambled data from the original watermark is still required at the watermark extraction stage.

Kumar *et al.* [22] presented a secure watermarking framework on medical images by applying IntDCT and SVD. The differential evolution technique was used to determine suitable scaling factors by randomizing the watermark with the step space fill curve. In addition to the watermarked image, the $U_W, S,$ and V_W values during insertion are also required for the watermark extraction process. The experimental findings demonstrate that the designed framework is robust to geometric attacks.

Fares *et al.* [23] introduced watermarking approaches based on DCT and Schur decomposition to protect medical images. Integration is performed at the intermediate frequencies. According to the findings, the designed algorithm produces acceptable imperceptibility with PSNR values at intervals [47, 49]. However, capacity is limited, where a 1024×1024 image host can only accommodate a 1024-bit watermark. The suggested method is robust under some conventional attacks but, it is not resistant to geometric attacks, such as cropping and scaling.

3. PRELIMINARY

In this section, the DCT technique and the method of Coltuc et al. are presented and used in the proposed watermarking method. The energy compaction and redundancy removal properties of DCT make this transformation popular in image processing, especially image watermarking. However, DCT-based watermarking is prone to rounding errors. When this DCT is applied to the Coltuc et al. method, which exchanges two DCT coefficients to embed a watermark into the host image, the watermarking method is challenging in developing watermarking techniques, especially in medical images.

3.1. Discrete cosine transform

https://doi.org/10.31436/iiumej.v24i1.2597

As one of the prominent transformation techniques, DCT works by changing the image from the spatial to the frequency domain [13]. This technique has been used extensively in image processing. Some of the outstanding properties of DCT in image processing applications [24], [25] include:

1. Decorrelation can eliminate redundancy between neighboring pixels.
2. DCT offers better energy compaction for correlated images.
3. Separability and symmetry: Transformation matrices can be computed offline, thus providing computational efficiency.
4. Orthogonality: This property makes some reduction in pre-computing complexity.

Generally, the image is segmented into 8×8 pixel blocks. Then, each of those blocks is subjected to a 2D-DCT. Mathematically, the 2D-DCT transformation and the 2D-DCT inverse for a block size of 8×8 can be seen in Eq. (1) and (2), respectively, as follows:

$$F(u,v) = \frac{1}{4}C(u)C(v)\sum_{x=0}^{7}\sum_{y=0}^{7} f(x,y)\ cos\left(\frac{(2x+1)u\pi}{16}\right) cos\left(\frac{(2y+1)v\pi}{16}\right) \quad (1)$$

$$f(x,y) = \frac{1}{4}C(u)C(v)\sum_{u=0}^{7}\sum_{v=0}^{7} F(u,v)\ cos\left(\frac{(2x+1)u\pi}{16}\right) cos\left(\frac{(2y+1)v\pi}{16}\right) \quad (2)$$

with $C(\omega) = \frac{1}{\sqrt{2}}$ for $\omega = 0$, and $C(\omega) = 1$, for otherwise ; $F(u,v)$ is the DCT coefficient; $f(x,y)$ is the pixel value in the spatial domain.

There are two ways to apply DCT to images: block-wise and without block-wise. DCT separates the image into three frequency sub-bands, i.e., low (LF), middle/ mid (MF), and high (HF), in a block-wise approach. Fig. 1 shows the position of the DCT coefficient with blocks of size (8×8) pixels. The 8×8 pixel block transformation yields 64 DCT coefficients. The position of the upper left corner of the DCT coefficient, $F(0,0)$, is the DC component, and the other 63 coefficients are the AC component. The DC component represents the average color of the entire frequency-transformed region. Thus, embedding data in DC components can cause visual artifacts that are visible to the normal human eye. Embedding data is done in the MF coefficient region, because this region carries relatively less important image information than the HF and LF regions, and is less significant in perception. Thus, data embedding in the MF region does not significantly affect image quality or communication performance [14], [26].

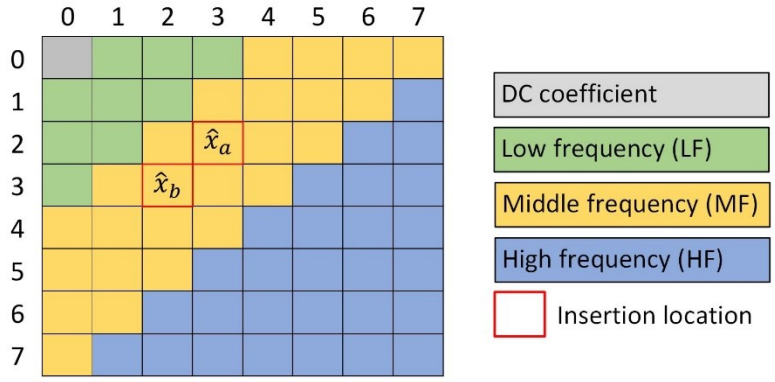


Fig. 1. The 2D Discrete cosine transform (DCT) coefficients with blocks of size (8×8) pixels.

3.2. Coltuc's Method

https://doi.org/10.31436/iiumej.v24i1.2597

Coltuc and Chassery [12], [13] applied the DCT domain in the robust watermarking stage. Firstly, the cover image X is segmented into 8×8 blocks. Next, DCT is applied to each block. The two MF coefficients $\hat{x}_a$ and $\hat{x}_b$ in each DCT block are chosen to insert one watermark bit $w \in \{0,1\}$, as follows [27]:

$$(\hat{x}'_a, \hat{x}'_b) = \begin{cases} (\hat{x}_a, \hat{x}_b), & if\ \hat{x}_a - \hat{x}_b > 0 \text{ and } w = 1 \\ (\hat{x}_b, \hat{x}_a), & if\ \hat{x}_a - \hat{x}_b \leq 0 \text{ and } w = 1 \\ (\hat{x}_a, \hat{x}_b), & if\ \hat{x}_a - \hat{x}_b \leq 0 \text{ and } w = 0 \\ (\hat{x}_b, \hat{x}_a), & if\ \hat{x}_a - \hat{x}_b > 0 \text{ and } w = 0 \end{cases} \quad (3)$$

with a and b being the two AC channel indexes. The index is the coordinates of the pixels. Thus, the AC channel index represents the coordinates of the DCT coefficients located in the AC component. For example, a=(2,3) and b=(3,2) are the selected AC channel indexes, so the two MF coefficients $\hat{x}_{(2,3)}$ and $\hat{x}_{(3,2)}$ are used to insert a watermark bit, as shown in Fig. 1.

By replacing $\hat{x}'_a$ and $\hat{x}'_b$ for the appropriate coefficients, the DCT coefficients for Y are obtained. The watermarked image Y is then created by applying the inverse DCT. For the decoding process, Y is segmented into 8×8 blocks. Next, each block is converted using the DCT technique. The embedded watermark for a coefficient pair of $\hat{y}_a$ and $\hat{y}_b$ is recovered as: if $\hat{y}_a - \hat{y}_b > 0$, then the bit watermark is 1, and 0 otherwise.

One bit of information is entered into each block depending on the difference between the two coefficients of MF. The new coefficient value does not change if the difference is positive and the bit is "1", or the difference is negative, and the bit is "0". However, for other conditions, the positions of the two MF coefficients are swapped. The exchange of these coefficients does not change the watermarked image significantly because the MF of DCT coefficients generally have almost the same magnitude. However, this condition is prone to extraction errors due to the rounding factor of DCT, as shown in Fig. 2(a). As a result, not all watermarks can be extracted properly. One solution is to select two MF coefficients $\hat{x}_a$ and $\hat{x}_b$ to embed a robust watermark. However, this method becomes impractical.

4. PROPOSED METHOD: WATERMARKING IMAGES VIA MODIFYING DCT COEFFICIENT PAIR

In this section, the modification of the insertion formula in Coltuc's method is described in subsection 4.1. The watermarking embedding step is presented in subsection 4.2., and the watermarking extraction step is presented in subsection 4.3. The watermarking framework for medical images is generally shown in Fig. 3. First, a watermark in the form of an EPR is hidden into a medical image, resulting in a Y watermarked image, and then sent through a communication channel. During transmission, the watermarked image undergoes various attacks, resulting in a medical image that is attacked as $\hat{Y}$. The attacks can be in the form of noise and intentional and unintentional modifications. In the extraction process, only Y (for noise-free channel) or Y (for noise channel) is needed to restore the original watermark. Thus, it can preserve medical images with copyright and maintain patient data security.

This paper enhances the robust watermarking method Coltuc *et al.* by modifying the DCT coefficient pairs in the watermark embedding formula. The proposed formula ensures that the difference between the two coefficients is at least as much as ζ. If the difference between the two coefficients is less than ζ, then the new pixels are modified so that the difference is equal to ζ. This new watermarking system on medical images based on modifying the DCT coefficient pair is suggested to obtain acceptable imperceptibility of watermarked images, impart data confidentiality of medical images, and preserve patient information privacy.

https://doi.org/10.31436/iiumej.v24i1.2597

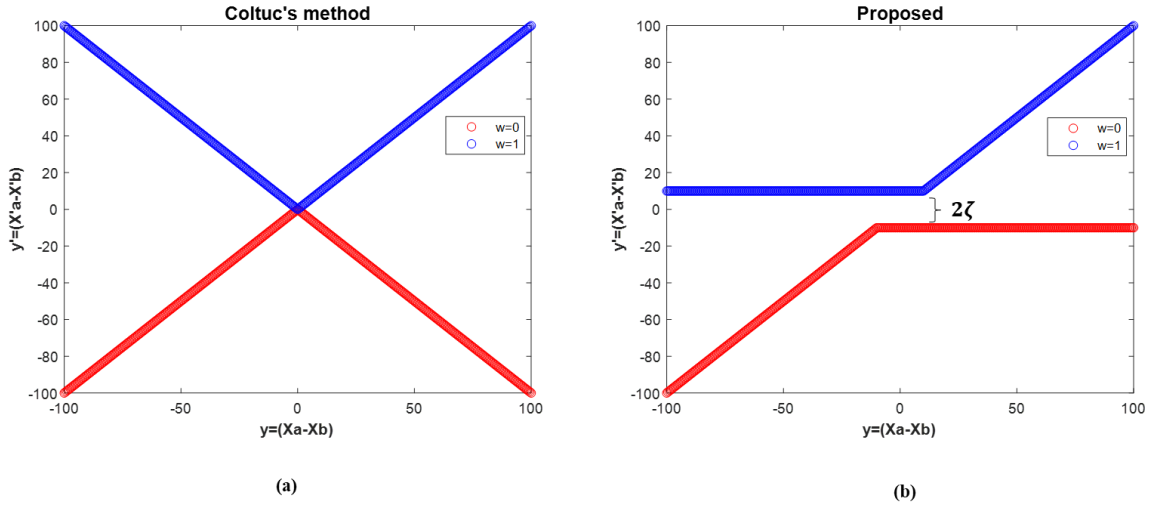


Fig. 2. Illustration of watermark embedding formula (a) Coltuc's method, (b) Proposed.

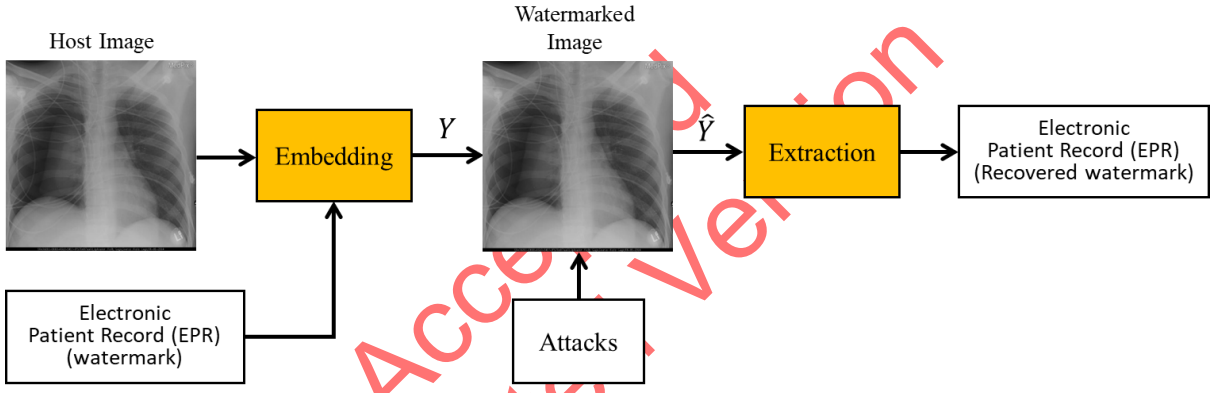


Fig. 3. The framework of medical image watermarking.

4.1. Modification of the Watermark Embedding Formula in Coltuc's Method

The value of the MF coefficient of the DCT generally has the same magnitude. After rounding operations to produce watermarked images and entering the decoding process, not all watermarks can be extracted correctly. We modified Eq. (3) so that the watermarked host image has high imperceptibility, protects the copyright (watermark) embedded in medical images, and maintains the privacy of patient information.

$$(\hat{x}'_a, \hat{x}'_b) = \begin{cases} (\hat{x}_a, \hat{x}_b), & if\ \hat{x}_a - \hat{x}_b > \zeta \text{ and } w = 1 \\ \left(\bar{x} + \frac{\zeta}{2}, \bar{x} - \frac{\zeta}{2}\right) & if\ |\hat{x}_a - \hat{x}_b| \le \zeta \text{ and } w = 1 \\ \left(\bar{x} + \frac{\zeta}{2}, \bar{x} - \frac{\zeta}{2}\right) & if\ \hat{x}_a - \hat{x}_b < -\zeta \text{ and } w = 1 \\ (\hat{x}_a, \hat{x}_b), & if\ \hat{x}_a - \hat{x}_b < -\zeta \text{ and } w = 0 \\ \left(\bar{x} - \frac{\zeta}{2}, \bar{x} + \frac{\zeta}{2}\right), & if\ |\hat{x}_a - \hat{x}_b| \le \zeta \text{ and } w = 0 \\ \left(\bar{x} - \frac{\zeta}{2}, \bar{x} + \frac{\zeta}{2}\right), & if\ \hat{x}_a - \hat{x}_b > \zeta \text{ and } w = 0 \end{cases} \quad (4)$$

https://doi.org/10.31436/iiumej.v24i1.2597

The proposed formula ensures that the difference between the two MF coefficients, namely $\hat{x}_a$ and $\hat{x}_b$, is at least as much as ζ. If the distance between the two MF coefficients is less than ζ, then the new pixel is modified so that the difference in distance is as significant as ζ. Modification of the insertion formula of Coltuc's method through the DCT coefficient pair can be seen in Eq. (4) and then simplified to Eq. (5). Fig. 2(b) presents the illustration of the proposed formula

$$(\hat{x}'_a, \hat{x}'_b) = \begin{cases} (\hat{x}_a, \hat{x}_b), & \text{if } (\hat{x}_a - \hat{x}_b < -\zeta \text{ and } w = 0) \text{ or } (\hat{x}_a - \hat{x}_b > \zeta \text{ and } w = 1) \\ \left(\frac{\hat{x}_a + \hat{x}_b + (2w-1)\zeta}{2}, \frac{\hat{x}_a + \hat{x}_b - (2w-1)\zeta}{2}\right), & \text{otherwise} \end{cases} \quad (5)$$

with $\bar{x}$ is the average of the two MF coefficients of the DCT, namely $\hat{x}_a$ dan $\hat{x}_b$.

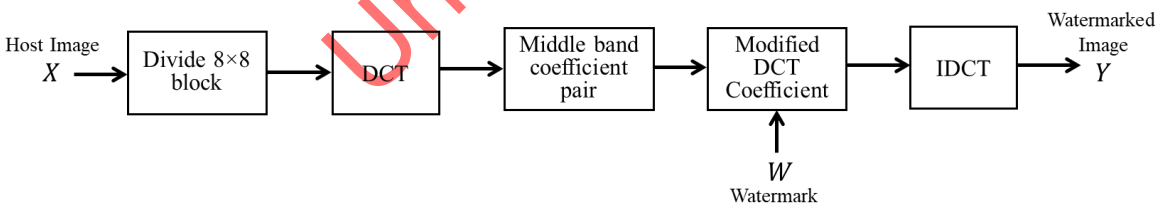
4.2. Embedding Stage

The input of the watermarking embedding stage is a medical image X as the host, and the output is a watermarked host image Y. The sizes of X and Y are M × M, while the size of W is N × N. Fig. 4(a) presents the watermarking embedding stage, and the detailed embedding steps are described as follows.

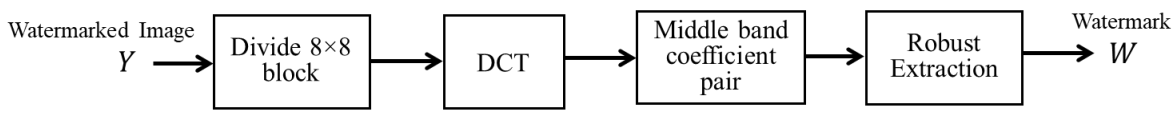
1. Split X into 8×8 non-overlapping blocks.
2. For each block, apply DCT using Eq. (1) so that it produces $\hat{X}$.
3. In each DCT block, the two MF coefficients $\hat{x}_a$ and $\hat{x}_b$ are decisive in embedding one-bit watermark $w \epsilon \{0,1\}$. The robust watermark embedding formula is expressed in Eq. (5).
4. The DCT coefficient of Y is done as follows:

$$\hat{y}_i = \begin{cases} \hat{x}'_i, & if\ i \epsilon \{a, b\} \\ \hat{x}_i, & \text{otherwise} \end{cases} \quad (6)$$

5. Process the inverse DCT using Eq. (2), and a watermarked image is obtained.



(a)



(b)

Fig. 4. The proposed watermarking method using DCT coefficient pair (a) embedding stage (b) extraction stage.

https://doi.org/10.31436/iiumej.v24i1.2597

4.3. Extraction Stage

The input of the watermarking extraction stage is the Y watermarked host image, and the output is the extracted watermark W^*. While, Y and W^* sizes are M × M, and N × N, respectively. Fig. 4(b) presents the watermarking extraction stage, and the extraction steps in detail are described as follows.

1. Split Y into 8×8 non-overlapping blocks.
2. Apply DCT to each block using Eq. (1) so that it produces $\hat{Y}$.
3. In each DCT block, the two MF coefficients $\hat{y}_a$ and $\hat{y}_b$ become determinants in extracting the one-bit watermark $w\epsilon\{0,1\}$. The robust watermark extraction formula is stated as follows.

$$W^* = \begin{cases} 1, & \text{if } \hat{y}_a - \hat{y}_b > 0 \\ 0, & \text{otherwise} \end{cases} \tag{7}$$

At the transmission is without noise, W^* equals W.

5. RESULT AND DISCUSSIONS

This section evaluates the effectiveness of the suggested robust and imperceptible watermarking technique. Subjective visual observation and objective quantitative analysis are used to evaluate the proposed method. Numerous attacks with varying parameters were performed to assess robustness further. Finally, the proposed method's imperceptibility and robustness are compared to state-of-the-art works.

This experiment uses the grayscale format and image sizes 512×512 of the host medical image. A total of five medical images from different modality types were used as test data, including MRI, X-Ray, Computed Tomography (CT), Ultrasound (US), and colonoscopy. Medical images were retrieved from the MedPixTM medical image database [26] and CVC-ClinicDB database [28]. The host medical image modality used in the experiment is shown in Fig. 5(a-e). Meanwhile, the watermark is a random binary image whose size depends on the block size discussed in the previous section. For an 8×8 block, the amount of watermarks embedded into the original host medical image is (512×512)/(8×8)=4096 bits. In other words, blocks measuring 8×8 yield a watermark of size 64×64.

The efficiency of the proposed method is thoroughly evaluated on two watermarking criteria, including imperceptibility and robustness. The performance metric for imperceptibility criteria uses peak signal noise ratio (PSNR) [9]. The watermarked host image must be invisible to humans to guarantee information security. Therefore, imperceptibility/ invisibility criteria are essential metrics in watermarking techniques. The PSNR measures how visually similar the watermarked image and the original host are. Both images should look the same, so there is no significant difference between the two. The similarity between the two images increases with increasing PSNR values and vice versa. Generally, the watermarked image is acceptable if the PSNR is more than 37 dB and the watermark is not discernible to the human visual system [29]. Here, X is the original host image, Y is the watermarked host image, and M×M is the host image size. Mathematically, PSNR (in dB) is formulated as follows [11], [15].

$$PSNR = 10 \times log \frac{255^2 \times \mathrm{M} \times \mathrm{M}}{\sum_{i=1}^{\mathrm{M}} \sum_{j=1}^{\mathrm{M}} (\boldsymbol{X}_{i,j} - \boldsymbol{Y}_{i,j})^2} \tag{8}$$

The bit error rate (BER) and normalized correlation (NC) are the performance metric to evaluate a watermarking technique's robustness criteria. Technically, BER measures the erroneous bit rate after the watermark extraction process. If the BER value is close to 0, then a

https://doi.org/10.31436/iiumej.v24i1.2597

few messages are lost, and vice versa. Ideally, the value of BER should be 0. If EB is the amount of incorrectly decoded bits, and TB is the number of watermark bits, then BER can be calculated [14], [27] as EB/TB.

Fig. 5. Five modalities of original medical image and a watermark (a) X-ray , (b) CT, (c) US, (d) MRI, (e) Colonoscopy, (f) watermark.

Principally, the NC measures the similarity between the original and extracted watermark images. The NC can be described mathematically by Eq. (9). If the NC value is near 1, then the watermarking method is very robust.

$$NC = \frac{\sum_{i=1}^{N}\sum_{i-1}^{N} W_{i,j}\, W_{i,j}^{*}}{\sum_{i=1}^{N}\sum_{i-1}^{N} W_{i,j}^{2}} \tag{9}$$

where W and W^{*} are the original watermark and extracted watermark images, respectively. N × N is the watermark image's size [14]. After applying the embedding and extraction processes, the proposed scheme's imperceptibility and robustness tests are carried out for varied medical images.

5.1. ζ Parameter Evaluation

The proposed watermark embedding formula ensures that the difference between the two MF coefficients, namely $\hat{x}_a$ and $\hat{x}_b$, is at least ζ. If the distance between the two MF coefficients is less than ζ, then the new pixels are modified so that the distance difference is ζ. We changed the value of the ζ parameter in the watermark embedding formula to get the PSNR and expected robustness level. Experiments were carried out on five types of medical images, i.e., X-ray, CT, US, MRI, and Colonoscopy. Fig. 6 presents the effect of the ζ parameter on PSNR and BER. Figure 6(a) shows the relationship between ζ and BER.

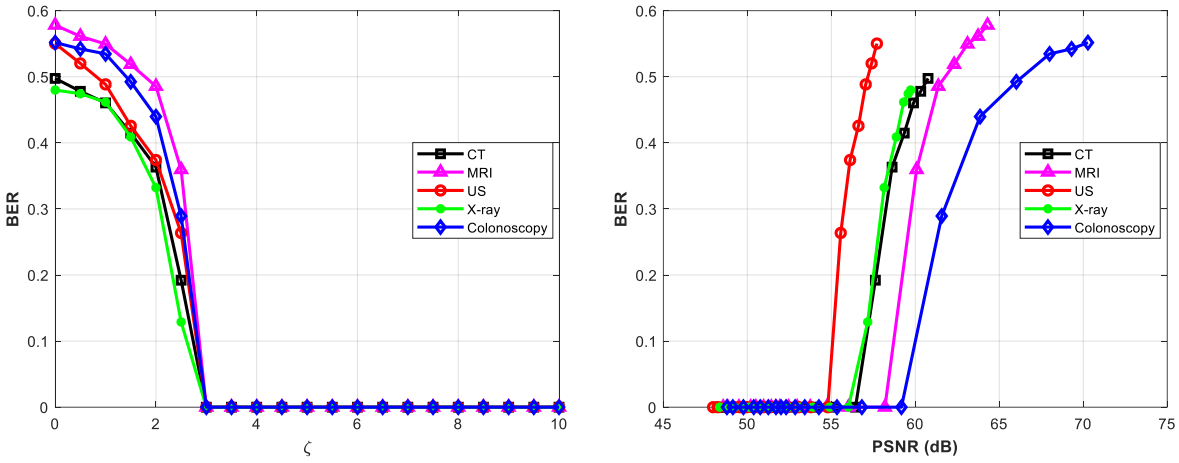
Higher ζ results in lower BER. The criterion BER is 0 when $\zeta \geq 3$. It means that the extracted watermark can be recovered very well. BER of 0 means there are no bit errors in watermark extraction. While Fig. 6(b) shows the relationship between BER and PSNR over ζ, which corresponds to Fig. 6(a). The higher the ζ value, the higher the resistance, but the lower the PSNR. When the resistance condition is ideal, namely BER is 0, the PSNR value ranges around [48, 59] dB for the range of ζ is 3 to 10. Thus, ζ determines the imperceptibility and robustness of the watermark embedding into the host medical image.

5.2. Imperceptibility Analysis

For integrity and ensuring information security, watermarked host medical images must be imperceptible/ invisible to humans. Fig. 7 shows a watermarked host X-ray image when not under attack and the extracted watermark. The experiment was carried out when ζ = 3. The PSNR, BER, and NC results of each corresponding image are also shown in Fig. 7. The watermarked image is acceptable because the PSNR is more than 37 dB, and the watermark is not discernible to the human visual system [30].

Early Access Date: 4 November 2022

https://doi.org/10.31436/iiumej.v24i1.2597



(a) (b)

Fig. 6. Evaluation of ζ (a) The BER of extracted watermark (b) The trade-off between PSNR and BER.

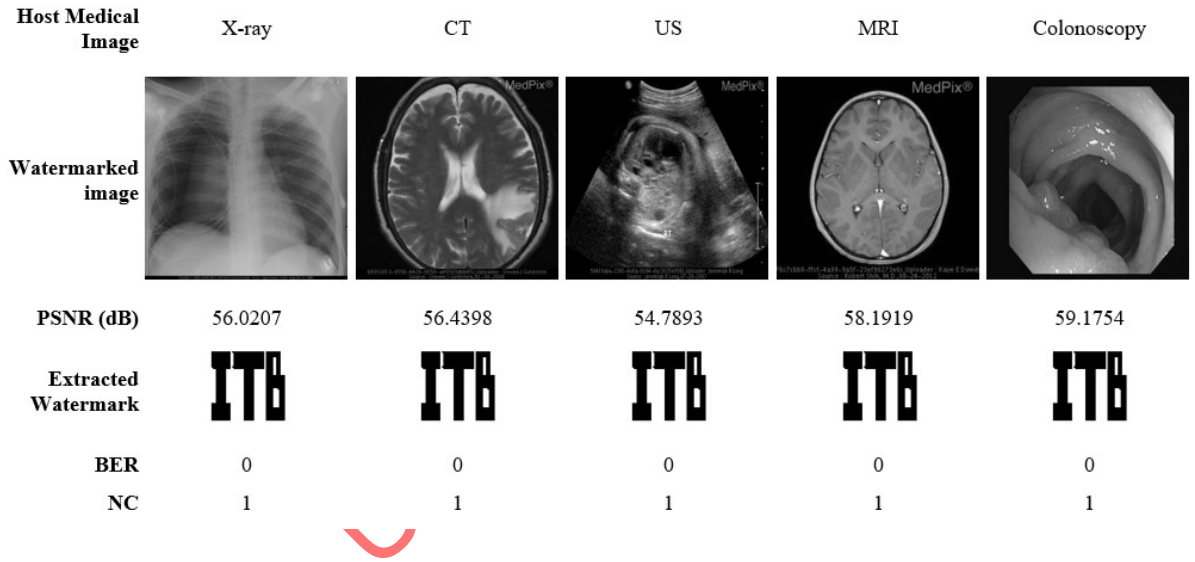


Fig. 7. Imperceptibility and robustness performance. Rows represent the extracted watermarked image and watermark along with their corresponding PSNR, NC, and BER. Columns represent type medical images, i.e., X-ray, CT, US, MRI, and Colonoscopy.

Based on Fig. 7, the imperceptibility criterion of the suggested method is that all PSNR of each watermarked medical image is greater than 54 dB. The average PSNR generated for the five watermarked medical image modalities is 56.3604 dB. Then, all extracted watermarks yielded BER is 0 and NC is 1 when the watermarked host image was not subjected to attack. It demonstrates that the method of watermarking is imperceptible. Furthermore, the suggested approach satisfies both the subjective and objective standards for watermarking invisibility. When the watermarked host image is not subjected to an assault, extracted watermarks have a BER of 0 and an NC of 1. Therefore, the process of watermarking has a high level of imperceptibility. Thus, the suggested method satisfies both the subjective and objective requirements for watermarking invisibility.

https://doi.org/10.31436/iiumej.v24i1.2597

5.3. Robustness Analysis

Various watermarking attacks were applied to watermarked medical images to examine the robustness criteria of the proposed method. Table 1 represents different attacks with parameter specifications used in the experiment. These attacks include compression, filtering, noise, histogram equalization, sharpening, and motion blur. In particular, compression attacks include JPEG and JPEG2000. JPEG compression parameters with quality factor (QF) 80 and JPEG2000 compression with compression ratio (CR) = 4 and 8. Filter attacks consist of median, Gaussian, average, and lowpass filters. The parameters in the filtering attack use a filter with a window size of 3×3. Noise attacks include Gaussian, salt & pepper, and speckle. The parameters in the noise addition attack are set by the variance or noise density of 0.001. Parameters of motion blur attack with linear motion of the camera with pixels Len = 7, with angle degrees Theta = 4. At the same time, histogram equalization and sharpening use default parameters.

Table 1: Various Attacks with Parameter Specifications in Experiments

Attack	Parameter Specifications
JPEG compression (JC)	QF = 80, 90
JPEG2000 compression (J2k)	CR = 8, 12
Median filter (MF)	3×3
Gaussian filter (GF)	3×3
Average filter (AF)	3×3
LPF	3×3
Gaussian noise (GN)	Mean = 0, Variance = 0.001
Salt & peppers noise (SP)	Noice density = 0.001
Speckle noise (SN)	Mean = 0, Variance = 0.001
Histogram equalization (HE)	-
Sharpening (SH)	-
Motion blur (MB)	Len = 7, Theta = 4

In the extraction stage, if the extracted watermark can recover from damaged watermarked images, then the watermarking method is said to be robust and secure. Here, BER and NC performance metrics examine the robustness of the proposed method under various watermarking attacks. In addition, the result of the suggested scheme is compared with the existing techniques [15]–[17] for the same medical image dataset. The BER of extracted watermark on numerous watermarked medical images is shown in Fig. 8. Meanwhile, Fig. 9 presents the results of the extracted watermark from the attacked watermarked X-ray along with corresponding BER and NC.

Various attacks are rendered on watermarked medical images. These medical images include X-ray, CT, US, MRI, and Colonoscopy. On the extraction side, the extracted watermark image is expected to be recovered from the damaged watermarked medical image. Based on Fig. 8, JPEG compresses images without significantly altering their appearance. Medical images with watermarks are compressed with JPEG using varying quality factors. Then, the proposed method is used to extract the watermarked image. The experiments indicated that the proposed method performs well for all the medical images we tested on JPEG compression with QF > 80 and JPEG2000 compression with CR < 12. The extracted watermark can still be interpreted visually if BER < 0.3 [30]. On X-ray, CT, and Colonoscopy images, watermarks can be extracted well even at JPEG compression with QF = 90 and JPEG2000 compression

https://doi.org/10.31436/iiumej.v24i1.2597

with CR = 12. Remarkably, watermarks can be best extracted, with BER is 0 for all compression parameters given in watermarked Colonoscopy image. Based on Fig. 9, watermarks can be extracted well with BER of 0 and NC of 1 for JPEG compression attacks with QF = 90 and JPEG2000 with CR = 8, and 12 given to the attacked watermarked X-ray images.

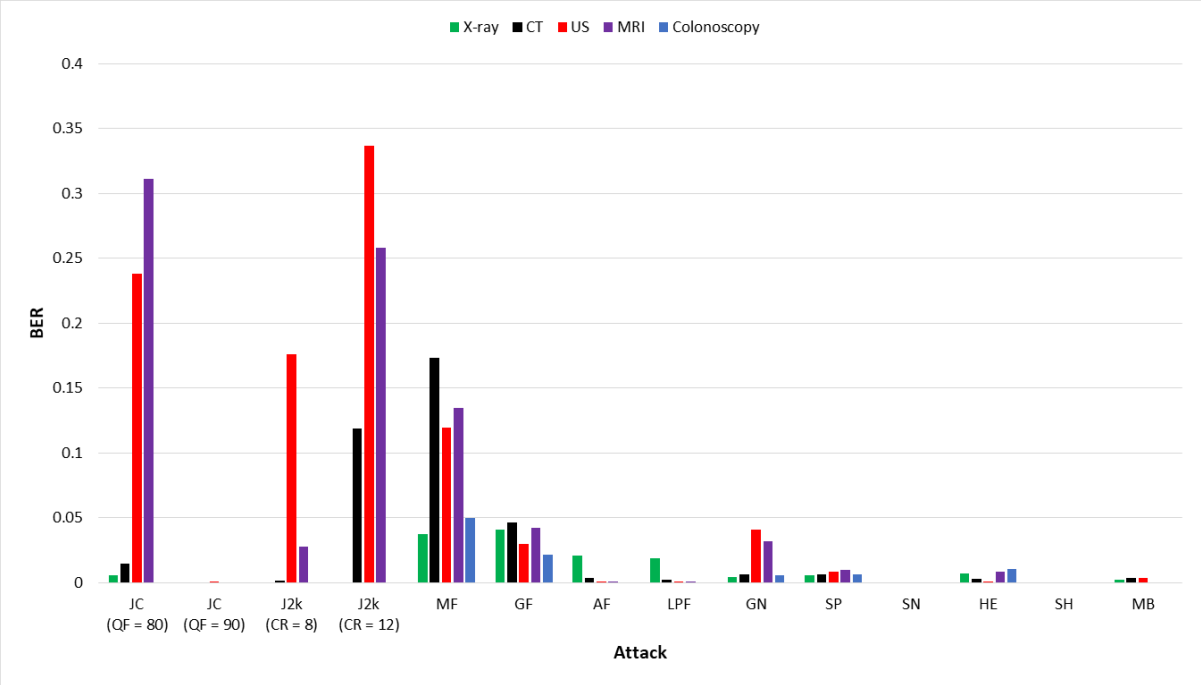


Fig. 8. The BER of extracted watermarks when condition with attack.

Attack	JPEG (QF = 80)	JPEG (QF = 90)	J2k (CR = 8)	J2k (CR = 12)	MF (3×3)	GF (3×3)	AF (3×3)
Extracted watermark							
BER	0.0056	0	0	0	0.0374	0.0405	0.0208
NC	0.9888	1	1	1	0.9221	0.9172	0.9563

Attack	LPF 3×3	GN (0.001)	SP (0.001)	SN (0.001)	HE	SH	MB
Extracted watermark							
BER	0.0190	0.0042	0.0054	0	0.0068	0	0.0022
NC	0.9598	0.9950	0.9982	1	0.9863	1	0.9956

Fig. 9. The BERs and NCs of extracted watermarks from watermarked X-rays attacked.

Four filters, including the median, Gaussian, average, and low pass, and three different noises, such as Gaussian, salt & pepper, and speckle, are applied to watermarked medical images. Afterward, the watermark image is extracted using the proposed method. The experiment results (Fig. 8 and Fig. 9) prove that the proposed method performs well for all medical images provided a filtering attack. Remarkably, watermarks can be extracted very well with BER 0 for watermarked Colonoscopy medical images subjected to average filter and LPF attacks. The experiment results also prove that the proposed scheme performs well for all

medical images under the noise attack. Remarkably, watermarks can be successfully extracted with a BER of 0 for all watermarked medical images subjected to speckle noise attacks.

A series of other attacks, such as histogram equalization, sharpening, and motion blur are also applied to watermarked medical images for endurance testing. Based on the experiment results (Fig. 8 and Fig. 9), the proposed scheme performs well for all medical images given the three attacks. Impressively, watermarks can be well extracted with a BER of 0 for all watermarked medical images given a sharpening attack. Watermarks can also be extracted with a BER of 0 for motion blur attacks rendered in watermarked MRI and Colonoscopy images.

5.4 Comparison of the Proposed Method with State-of-the-Art Work

In Fig. 10, the imperceptibility performance of the proposed method is compared with Coltuc's method [13] and the recently developed watermarking method [14], [15] for medical image identity protection. The watermark payload under the same conditions, which is 1 bit for every 64 pixels of the host medical image. The PSNR value of the proposed method is compared with the related work. The methods are compared using $\zeta = 3$ and without watermarking attacks. The proposed scheme offers superior performance to the three existing schemes [13]–[15]. In the proposed method, the average PSNR value of watermarked medical images is 56.3604 dB. Meanwhile, the mean of PSNR for watermarked medical images from the [13]–[15] scheme are 50.5647 dB, 48.3150 dB, and 53.6184 dB, respectively. It means that the insertion of watermark bits does not influence the watermarked medical image of the proposed method. The proposed method produces high imperceptibility over the the state-of-the-art works [13]–[15].

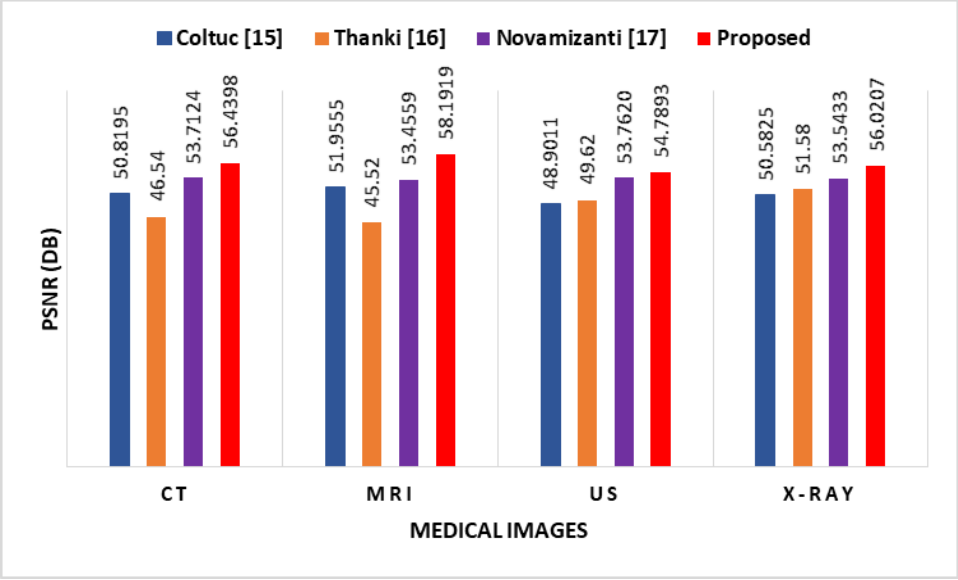


Fig. 10. Comparison under different medical images and methods.

Specifically, Table 2 summarizes the robustness performance of the proposed method compared to Coltuc's method [13] to evaluate how much contribution the proposed watermarking method makes. The host image used as test data is an X-ray. The suggested method performs well compared to the previous method against all types of watermarking attacks. In fact, the watermark can be extracted perfectly in a JPEG compression attack with QF = 90, JPEG2000 with CR = 8 and 12, speckle noise, and sharpening. The proposed method is outstanding from Coltuc's method [13], with the increase in BER and NC being 93% and 14%, respectively.

https://doi.org/10.31436/iiumej.v24i1.2597

Table 2: Comparison of BERs and NCs of the Proposed Method to the Coltuc's Method [15] in Attacked Watermarked X-Ray

Attack	BER		NC	
	[13]	Proposed	[13]	Proposed
JPEG (QF=80)	0.2488	**0.0056**	0.8491	**0.9888**
JPEG (QF=90)	0.2493	**0**	0.8523	**1**
J2k (CR=8)	0.1177	**0**	0.9605	**1**
J2k (CR=12)	0.1626	**0**	0.9337	**1**
MF [3×3]	0.2842	**0.0374**	0.4059	**0.9221**
GF [3×3]	0.1492	**0.0405**	0.6942	**0.9172**
AF [3×3]	0.0615	**0.0208**	0.8693	**0.9563**
LPF [3×3]	0.0625	**0.0190**	0.8673	**0.9598**
GN (0.001)	0.2261	**0.0042**	0.8644	**0.9950**
SP (0.001)	0.0173	**0.0054**	0.9877	**0.9982**
SN (0.001)	0.2146	**0**	0.8652	**1**
HE	0.1060	**0.0068**	0.9237	**0.9863**
SH	0.0225	**0**	0.9843	**1**
MB	0.0603	**0.0022**	0.9706	**0.9956**

Table 3: NCs Comparison of the Proposed Method to the State-of-the-Art [14], [15] in Attacked Watermarked X-Ray

Attack	Thanki [14]	Novamizanti [15]	Proposed
JPEG (QF=80)	0.9282	0.8769	**0.9888**
JPEG (QF=90)	0.9806	0.8973	1
GN (0.001)	0.6377	0.9970	0.9950
SP (0.001)	0.7532	0.9473	**0.9982**
HE	0.9708	0.8909	**0.9863**
SH	0.9674	0.9890	**1**

The proposed method is also compared with the recently developed watermarking methods [14], [15] to maintain the privacy and protection of the EPR as a watermark. Host X-ray images were used as test data for all compared methods. Watermarking in both techniques [14], [15] was performed in the FDCuT and DCT domains. The extraction process of both methods is semi-blind. The difference is the insertion of the watermarking technique [16] using the correlation sequence method. While in [17], the watermarking embedding technique uses the SVD method. Compared with the state-of-the-art works [14], [15], the proposed method is superior in terms of resistance to JPEG compression attacks, sharpening, histogram equalization, and sharpening. In addition, on a JPEG compression attack with QF = 90 and sharpening, the watermark can be extracted perfectly. The proposed method modifies the DCT coefficient pairs to embed a robust watermark. Thus, the average result demonstrates that the suggested method outperforms the present scheme regarding imperceptibility, robustness, and security. The proposed approach can be part of a robust reversible watermarking scheme [31] due to the blind extraction stage of the proposed watermarking method.

6. CONCLUSION

This paper proposes a modification of the DCT coefficient pair in the watermark embedding process. The proposed formula ensures that the difference between the two

coefficients is at least as ζ. If the difference between the two coefficients is less than ζ, then the new pixels are modified so that the difference is equal to ζ. This simple watermarking technique based on modifying DCT coefficient pairs is offered to achieve high imperceptibility, provide intellectual property protection for medical images, and ensure patient data security. The suggested method was evaluated on different types of medical images, including X-ray, CT, US, MRI, and Colonoscopy, and compared to numerous robust watermarking techniques of the current work. The experimental results indicate that the suggested method outperforms various contemporary watermarking techniques regarding imperceptibility, robustness, and security. The PSNR value for all categories of watermarked medical images exceeds 54 dB, and the average PSNR value is approximately 56 dB. In terms of resistance to JPEG compression attacks, histogram equalization, and sharpening, the suggested method is superior to numerous state-of-the-art robust watermarking methods. Future research could apply the presented technology to a robust reversible watermarking strategy and medical image protection for telemedicine applications.

ACKNOWLEDGEMENT

This research is part of L. Novamizanti's dissertation research funded by the Doctoral Dissertation Research Grant from the Ministry of Research and Technology of the Republic of Indonesia, file numbers: 083/E5/PG.02.00.PT/2022 and 343/IT1.B07.1/SPP- LPPM/V/2022. The Indonesian Endowment Fund for Education (LPDP) Scholarship and Telkom University also partially funded this research.

REFERENCES

[1] Memon, NA. Alzahrani A. (2020) Prediction-based reversible watermarking of CT scan images for content authentication and copyright protection. IEEE Access, 8: 75448-75462. doi: 10.1109/ACCESS.2020.2989175.
[2] Sajedi H, Rahbar S. (2020) Information hiding methods for E –Healthcare. Smart Health, 15: 100104. doi: 10.1016/j.smhl.2019.100104.
[3] Ahmad GI, Singla J, Giri KJ. (2021). Security and Privacy of E-health Data. In Multimedia Security, Springer Singapore, (pp. 199–214).
[4] Lanxiang C, Wutong BAI, Zhiqiang YAO. (2020) A Secure and Privacy-Preserving Watermark Based Medical Image Sharing Method. Chinese J. Electron., 29(5): 819–825. doi: 10.1049/cje.2020.07.003.
[5] Magdy M, Hosny KM. (2022) Security of medical images for telemedicine : a systematic review. Multimed. Tools Appl., 81: 25101–25145. doi: 10.1007/s11042-022-11956-7
[6] Alzahrani A, Memon NA. (2021) Blind and Robust Watermarking Scheme in Hybrid Domain for Copyright Protection of Medical Images. IEEE Access, 9: 113714–113734). doi: 10.1109/ACCESS.2021.3104985.
[7] Thakur S, Singh AK, Ghrera SP, Mohan A. (2020) Chaotic based secure watermarking approach for medical images. Multimed. Tools Appl., 79: 4263–4276. doi: 10.1007/s11042-018-6691-0
[8] Hassan B, Ahmed R, Li BO, Hassan O. (2019) An Imperceptible Medical Image Watermarking Framework for Automated Diagnosis of Retinal Pathologies in an eHealth Arrangement. IEEE Access, 7: 69758–69775, doi: 10.1109/ACCESS.2019.2919381.
[9] Anand A, Singh AK. (2021) Watermarking techniques for medical data authentication : a survey. Multimed. Tools Appl., 80: 30165–30197.doi: 10.1007/s11042-020-08801-0
[10] Evsutin O, Dzhanashia K. (2022) Watermarking schemes for digital images : Robustness overview. Signal Process. Image Commun., 100: 116523. doi: 10.1016/j.image.2021.116523.
[11] Saini D, Ali M. (2020) A robust medical image watermarking framework based on SVD and DE In Integer DCT domain (Workshop Paper) (pp. 373–378). doi: 10.1109/BigMM50055.2020.00064.

[12] Coltuc D, Chassery JM. (2007) Distortion-free robust watermarking: a case study. Secur. Steganography, Watermarking Multimed. Contents IX, 6505: 65051N, doi: 10.1117/12.702445.
[13] Coltuc D. (2007) Towards distortion-free robust image authentication. J. Phys. Conf. Ser., 77(1). doi: 10.1088/1742-6596/77/1/012005.
[14] Thanki R, Borra S, Dwivedi V, Borisagar K. (2017) An efficient medical image watermarking scheme based on FDCuT–DCT. Eng. Sci. Technol. an Int. J., 20(4): 1366–1379. doi: 10.1016/j.jestch.2017.06.001.
[15] Novamizanti L, Wahidah I, Wardana NPDP. (2020) A Robust Medical Images Watermarking Using FDCuT-DCT-SVD. Int. J. Intell. Eng. Syst., 13(6): 266–278. doi: 10.22266/ijies2020.1231.24
[16] Lei M, Liu X, Wang M, Yang Y, Qu Z. (2018) Robust image watermarking based on quantization index modulation in the DCT domain. J. Internet Technol., 19(2): 507–514. doi: 10.3966/160792642018031902019.
[17] Zhu Z, Zheng N, Qiao T, Xu M. (2019) Robust steganography by modifying sign of DCT coefficients. IEEE Access, 7: 168613–168628. doi: 10.1109/ACCESS.2019.2953504.
[18] Rachmawanto EH, Setiadi DRIM, Sari CA, Rijati N. (2019) Imperceptible and secure image watermarking using DCT and random spread technique. Telkomnika (Telecommunication Comput. Electron. Control., 17(4): 1750–1757. doi: 10.12928/TELKOMNIKA.v17i4.9227.
[19] Byun SW, Son HS, Lee SP. (2019) Fast and Robust Watermarking Method Based on DCT Specific Location. IEEE Access, 7: 100706–100718. doi: 10.1109/ACCESS.2019.2931039.
[20] Ko HJ, Huang CT, Horng G, WANG SJ. (2020) Robust and blind image watermarking in DCT domain using inter-block coefficient correlation. Inf. Sci. (NY)., 517: 128–147. doi: 10.1016/j.ins.2019.11.005.
[21] Nawaz SA, Li J, Bhatti UA, Mehmood A, Shoukat MU, Bhatti MA (2020) Advance hybrid medical watermarking algorithm using speeded up robust features and discrete cosine transform. PLoS One, 15(6): 1–21. doi: 10.1371/journal.pone.0232902.
[22] Kumar S, Jha RK. (2019) FD-based detector for medical image watermarking. IET Image Processing, 13(10): 1773-1782 2019. doi: 10.1049/iet-ipr.2018.5485.
[23] Fares K, Khaldi A, Redouane K, Salah E. (2021) DCT & DWT based watermarking scheme for medical information security. Biomed. Signal Process. Control, 66: 102403. doi: 10.1016/j.bspc.2020.102403.
[24] Khayam SA. (2003) The Discrete Cosine Transform (DCT): Theory and Application. In Information Theory and Coding, Michigan State University (pp. 1–13).
[25] Hamidi M, Haziti ME, Cherifi H, Hassouni ME. (2018) Hybrid blind robust image watermarking technique based on DFT-DCT and Arnold transform. Multimed. Tools Appl., 77(20): 27181–27214. doi: 10.1007/s11042-018-5913-9.
[26] Hernandez JR, Amado M, Perez-Gonzalez F. (2000) DCT-domain watermarking techniques for still images: detector performance analysis and a new structure. IEEE Trans. Image Process.,9(1): 55–68, doi: 10.1109/83.817598.
[27] Wang X, Li X, Pei Q. (2020) Independent Embedding Domain Based Two-Stage Robust Reversible Watermarking. IEEE Trans. Circuits Syst. Video Technol., 30(8): 2406–2417. doi: 10.1109/TCSVT.2019.2915116.
[28] Rahim T, Novamizanti L, Ramatryana INA, Shin SY. (2021) Compressed medical imaging based on average sparsity model and reweighted analysis of multiple basis pursuit. Comput. Med. Imaging Graph., 90: 101927. doi: 10.1016/j.compmedimag.2021.101927.
[29] Guo Y, Li BZ., Goel N (2017) Optimised blind image watermarking method based on firefly algorithm in DWT-QR transform domain. IET Image Process, 11(6): 406–415. Doi: 10.1049/iet-ipr.2016.0515
[30] Budiman G, Suksmono AB, Danudirdjo D. (2020) Compressive Sampling with Multiple Bit Spread Spectrum-Based Data Hiding. Appl. Sci., 10(12): 1–21. doi: 10.3390/app10124338.
[31] Novamizanti L, Suksmono AB, Danudirdjo D, Budiman G. (2022) Robust Reversible Watermarking using Stationary Wavelet Transform and Multibit Spread Spectrum in Medical Images. Int. J. Intell. Eng. Syst., 15(3): 343–354, doi: 10.22266/ijies2022.0630.29.