Medical Image Authentication by Combining Hash Signature and Watermarking Based on Frequency Domains

Amira K. Jabbar, Ashwaq T. Hashim, Qussay F. Hassan
1,2,3 Control and Systems Eng. Dept. University of Technology-Iraq, Baghdad, Iraq
* Corresponding author’s Email: 60766@student.uotechnology.edu.iq

Abstract—Medical images are transmitted to other remote places through the E-healthcare system. The protection of medical images is very crucial. Medical images need to be protected against any modification which the attacker may do through the unsecured channel. It is necessary for inspecting the integrity of the ROI (Region of Interest) of the received medical image prior to the adoption of any diagnostic decision to avoid a misdiagnosis. This paper aimed to confirm the integrity and authenticity of medical images by combining the hash signature with the watermarking technique based on the frequency domains. At first, the medical image is divided into ROI and RONI (Region of Non-Interest). The SLT and DCT transformations are employed together to extract the essential features set from ROI and then combined with EPR (Electronic Patient Registration) to produce a watermark, and then it is encoded by a chaotic map with a secret key to provide a signature. On the other hand, the RONI is mapping into randomly subblocks based on the linear system, and then the Signature is embedded in the chosen block using DWT. The hash code of the recovered image and EPR will be compared with the extracted watermark for integrity and authenticity. The experimental results demonstrate the watermark's robustness against many of the more aggressive and geometric signal processing distortions without affecting the quality of the original medical image. In particular, compared with state-of-the-art technology, the proposed algorithm improves the average NC value larger than 0.90 under all types of attacks.

Index Terms—Authenticity, Chaotic map, DCT, DWT, Hashing, Integrity, Medical image, SLT, Watermarking.

I. INTRODUCTION

MAGING technology has assumed a critical function in the improvement of the medical services area. Checking medical imaging is an essential source for important membership data [1]. To convey the medical images securely, some security requirements should be met. These necessities are secrecy, legitimacy, and integrity [2]. For the exchange of electronic patient records (EPR) between hospitals, a dedicated communication standard known as digital imaging and communications in medicine (DICOM) is used. The header is attached to the medical image files DICOM in this format, containing valuable patient information. The header may be lost, targeted, or other header files disordered. A good solution to those problems and problems may be found with the digital watermarking of medical images [3]. Watermarking techniques are used to add binary signatures (watermarks) directly to image content. Numerous
watermarking approaches do not address the problem of recognition of material. The image quality relies on much of the built-in watermarks. The details about the medical examinations, tests, and procedures of patients may be double blacked out to protect patients' privacy. Well-organized arrangement of confidential information in the healthcare management system seeks to provide good treatment opportunities based upon the right information to right position at the right time [4, 5].

As a compact representation of the original contents is a perceptual hash value, it can be used for robust content authentication. The benefit of perceptive hash algorithms is that they can accommodate the consistency and format variations compared to traditional cryptographic hash algorithms [6]. Binary representation is no longer necessary and still maps the same content at the same hash value. For the multimedia domain, this is especially useful.

We suggested an original checking method based on both hashing and watermarking principles in this paper. The authentication of image content is analyzed by providing a new algorithm that involves a perceptual hashing scheme for digital images with chaos. The interest was to find an acceptable imaging space with robust features that could create an image hash for digital imagery authentication.

The main contributions of this paper are as follows:

1. A new algorithm for extracting features of medical volume data based on human visual characteristics is proposed. This algorithm divide the image the subblock then take the SLT all subblock and then apply DCT on the LL subbands for theses blocks in order to contribute all bytes of image in hash code compared with other works that take only the LL suband of whole image only. This algorithm effectively protects the integrity of the medical image and meets the strict requirements of medical volume data for diagnosis.

2. The watermark encryption uses the Chaotic Shift Keying techniques (CSK), which has richer initial conditions and is extremely sensitive to the initial value, thus enhancing the security of watermarking. The watermark becomes chaotic and it is not possible to obtain effective information from it, hence it is highly concealed. If the watermark is modified to the wrong initial parameters of the CSK, it cannot be extracted correctly.

3. The watermark embedding and extraction algorithm design combines the features of perceptual hash and the block mapping based on secret key in order to provide an extra security level. The watermark embedding algorithm provides more durability under various attacks, and such noise affects the random pixels so that the whole image is not affected. Thus the embedded EPR and hash code are not destroyed.

The rest of the work is organized as follows: Section 2 presented the related works; Section 3 describes the proposed system with details; Section 4 shows some experiment results; Section 5 concludes the work.

II. RELATED WORKS

Recently various approaches are available that are guaranteed the security and integrity of medical images. These approaches comprise ciphering [7-9], watermarking[10-12], image signature or hash [13], the ciphering guaranteed the protection of images. Still, the deciphering will lose safety, whereas the watermarking and hashing can discover if the image has tampered and then the integrity is at risk. Tataru [14] offered an image hashing scheme based on a rugged collection of features extracted using a powerful, chaotic framework from joined DCT-DWT domains. Robustness analysis involves compression, noise, filtering, and geometric transforms. Cedillo-Hernandez et al. [15] proposed, along with the use of digital diagrams and correspondence through normal medical metadata, an extensive watermarking method for medical images, to prohibit the isolation of the relevant EPR data into the watermark. The watermark has been incorporated into the magnitude of the middle frequencies with the high quality of the watermarked images, a discrete transformation of the original medical image in Fourier. The suggested system used three
of the most common metrics to test watermarked images: peak signal-to-noise, structural similarity, and visual detail fidelity. The author proposed a tamper-proofing method for digital images using the digital watermarking technique in [16]. The mechanism presented here describes a method for detecting illegally modified regions in the image. Sharma [17] presented a watermarking method based on two common transform domain techniques, discreet DWT and discrete cosine transformation. The cover medical image is divided into two separate parts in the embedding process: the region of interest (ROI) and the non-region of interest (NROI). Several photographs and text watermarks are combined with the ROI and NROI parts of the same media cover item to authenticate the identity. Before embedding, Rivest-Shamir-Adleman (RSA) ’s encryption technique is applied to a text watermark to boost the text watermark protection and the encrypted EPR data is inserted into the NROI part of medical image coverage. The conversion method for pixels to blocks (PTB) used by Parah et al. [18], used in order to ensure the reversion of medical images, as an effective and computational solution for interpolations. A fragile watermark and the Block Checksum were inserted into the cover image in order to enable tamper detection and tamper position and therefore contents authentication at the recipient. The EPR, watermarks, and control data were embedded using Intermediate Significant Bit Substitution to avoid widely used LSB removal/replacement attacks (ISBS). The author [19] introduced two separate algorithms in the field of transformation for watermarking medical images. The first technological framework in the two regions: Area of Interest (ROI) and region of non-interest was integrated into digital watermarks and Electronic Patient Records (EPRs) (RONI). The Regions of Interest (ROI) are preserved in the second system for telediagnostics and the Non-Interest Region (NIR) is used to mask the digital watermark and EPR. The watermark/EPR is chosen and their size compared with embedding for each of the two DCT coefficients. Due to the performance of two strategies for different attacks, the proposed algorithms can prove useful in an E-health system. Rakhmawati et al. [20] addressed the concepts and characteristics of a fragile watermarking algorithm. The principal contribution of this paper survey is that it summarizes established procedures for choosing, producing and adding watermarks, detection sites, tampering and recovery processes. A comparison of several watermarking methods are analysed and presented in tabular form with an experimental evaluation of four watermarking schemes in several graphs to demonstrate the efficacy of the auto-embodiing fragile watermarking framework. A medical image watermarking (MIW) approach for telemedicine applications is proposed at Khare [21]. The method is effectively utilized in the creation of a watermarking mechanism by transformation by homomorphic transformation (HT), redundant discrete wavelet transformation (RDWT), and singular value decomposition (SVD). The reflecting part of the medical host image is obtained by HT, which includes RDWT and SVD. The RDWT and SVD process the medical watermark image. In order to insert the image of the watermark into the host image, single values (Svs) have been used. The chaotic 2-D Arnold Transform (AT) is used to crypt the watermark image to provide the watermark image with additional security. Moreover, the proposed technique would also test many wavelet families. The robustness and imperceptibility of the proposed technology are increased, as demonstrated in experimental results in various attacks. Swaraja is achieved [22] by hiding dual watermarks in the medical image blocks in the non-interest field, tamper identification and genuineness (RONI). The Human Visual System's (HVS) characteristics are chosen for these blocks, along with the Discrete Wavelet Transformation (DWT) and Schur Transform integration and the algorithm PCS. The lossless compression algorithm Lempel-Ziv-Welch (LZW) compresses two watermarks to improve payload power. Simulation results on different medical image types show that the proposed scheme shows superior clarity and robustness against signal and compression attacks compared to related hybrid optimized algorithms.

III. THE PROPOSED SYSTEM

In this system, a mechanism based on a hybrid frequency domain is used for assuring the integrity and verification level while the encoding is used to maintain authenticity. This methodology is run on two levels. Those are signature generation and watermarking method. Fig. 1 shows the block diagram of the proposed system.
A. **Image localization of ROI and RONI**

Thresholding is one of the most potent techniques for image localization. The OTSU algorithm is used to generate the threshold value for brain medical image binarization. Detecting the connected region can ensure the bounding box of the central brain region called ROI. The size of the ROI is extended to the multiple of two because of the DWT usage. Fig. 2 depicts the localization process of ROI and RONI in brain medical images.

![Block diagram of the proposed system.](image1)

**Fig. 1.** Block diagram of the proposed system.

![Samples of brain images.](image2)

**Fig. 2.** Samples of brain images.

B. **Signature Generation**

In the proposed system the ROI is reshaped for obtaining a squared sub-image of size $m \times m$, and then it is divided into $k \times k$ pixels sub-blocks. Hash code is generated by calculating the signatures of each sub-block. The SLT and DCT are employed together to extract the essential features set. The SLT first level decomposition confirms the sub-block information's isolation in frequency sub-bands $LL_1$, $HL_1$, $LH_1$, and $HH_1$. The $LL_1$ sub-band holds most of the information from each sub-block. Therefore, we take into
consideration the LL_1 sub-band for the feature extraction method. When decomposing to the n-level, the LL_n sub-band is obtained, and the LL_n offers a square array that preserves most of the correlation from each block. According to the DCT distribution, the block top-left corner holds the high frequencies while the bottom-right holds the low significant frequencies. Each block has a DC term, i.e. the (0,0) frequency, which includes the most block significant information part. This term is taken from each DCT block and is used to form the hash code.

A feature vector of DC’s is obtained for all computed DCT blocks from the LL_n sub-band. Subsequently, the feature vector is binarized, and this is accomplished by comparing each feature set component with the overall set of feature average. Binary 0 is employed to state DC values below the average, and binary one is used to state the DC values exceeding average. Consequently, a binary hash code is obtained for the digital image, as shown in Fig. 3. The hash code is combined with EPR to produce a watermark. A quadratic chaotic map is employed to encode the watermark with a secret key to sign it. Algorithm 1 lists the steps of generating the Signature.

Algorithm 1: Signature Generation

Input:
- ROIimg, // Region of interest image
- W, H // Width and Height
- n, // Number of level
- k, // block size
- m // The new size of image

Output:
- S // Signature

Step1: The gray image ROI_{img} is resized to m×m dimensions by the bicubic interpolation.
\[
\text{ROI}_{img}(x, y) = \text{BicubicResize}(\text{ROI}_{img}(H, W, [m, m]))
\]

if \( H \) or \( W < 256 \) \hspace{1cm} (1)

Step2: Split ROI_{img} into the non-overlapping k×k sub-block.

Step3: Apply 2D SlantLet Transformation (SLT) with n level for each sub-block.

Step4: Apply the DCT transform on the n LL sub-band for each sub-block.

Step5: The DC terms are collected from DCT of each LL sub-band to construct features vector V of the ROI_{img}.

Step6: Compute the mean value \( m_{dc} \) for the features vector V.

Step7: Binarized, the features vector V, to get binary features vector BV using the following formula:

\[
BV_i = \begin{cases} 
0 & \text{if } V_i < m_{dc} \\
1 & \text{if } V_i \geq m_{dc}
\end{cases}
\]

Fig. 3. Hash code generation.
V=(Vi) and BV=(BVi) where i=1,..., l.

**Step8:** Convert the ASCII for the EPR of length 44 bytes to binary to generate BEPR.

**Step9:** Encode the BEPR and BV using a Quadratic Chaotic map [23]. The following formula generates the random signal:

\[ X_{n+1} = a - x_n^2 \quad \text{for} \quad 0 < a < 2 \]  

Where \(0 < a < 2\) and \(x_n\)

Then the two random sequence signals \(x_0\) and \(x_1\) are the inverted version of each other \((x_0(t) = -x_1(t))\). The transmitted signal can then be written as:

\[
S(t) = \begin{cases} 
  x_1 & \text{symbol 1 is transmitted} \\
  x_0 & \text{symbol 0 is transmitted} 
\end{cases}
\]

**C. Hiding Signature**

The embedding procedure attempts to insert the Signature bits, including the encoded hash code and EPR, in the RONI. The RONI is split into 2×2 non-overlapping blocks. In the embedding watermark schematic, block mapping is performed before the Signature inserting process. The proposed mapping method included the block mapping phase and block remapping phase. Details about the two phases of our proposed algorithm are described below.

**D. Block Mapping Phase**

The proposed block mapping is based on using a set of linear equations with \(n=2\), \(k=2\). By the linear transformation presented in Eq. (5), a High pixel correlation can be detached.

\[
\begin{bmatrix} 
  x' \\
  y'
\end{bmatrix} = A \begin{bmatrix} 
  x \\
  y
\end{bmatrix} \mod N = \begin{bmatrix} 
  K_1 & K_2 \\
  K_3 & K_4
\end{bmatrix} \times \begin{bmatrix} 
  x \\
  y
\end{bmatrix} \mod N
\]

Where \((x,y)\) is the original pixel position, \((x', y')\) is the transformation pixel position and \((x',y'), (x,y) \in [1,N] \times [1,N]\). The N is the number of sub-blocks in the image, and the \(K_1, K_2, \text{and } K_3\) are prime secret keys while \(K_4\) is even. This selection of the keys is to ensure that all generating indices are odd.

In the mapping phase, at first, the RONI is rearranged in a symmetric matrix that its size computed from the following substeps:

1. Compute the numbers of bytes in RONI by the following formula:

\[
TS = (R \times C) - (K \times L)
\]

Where \(R\) and \(C\) are the numbers of rows and columns of the original medical image. At the same time, \(K\) and \(L\) are the ROI length and width.

2. Take the square root of \(TS\) to construct the square matrix for RONI:

\[
N = \sqrt{TS}
\]

If \(N < \text{int}(T)\)

\[
N = \text{int}(N)+1
\]

Endif
3. The size of the RN matrix is then $N \times N$.

Fig.4 shows the ROI and RONI regions.

![ROI and RONI](image)

**Fig. 4.** The ROI and RONI.

Besides using linear equations, modular algebra is employed to control the overall index size's increasing size. According to Equation (5), the range of indices values $[x', y']$ is $[0... N]$. Eq.(5) might be rewritten as follows:

$$
\begin{bmatrix}
K_1 & K_2 \\
K_3 & K_4
\end{bmatrix} \times
\begin{bmatrix}
x \\
y
\end{bmatrix} \mod N\times
\begin{bmatrix}
x' + p_i \\
y' + p_i
\end{bmatrix}
$$

(7)

$p_i$ is an integer whose value will not be recorded as part of the index values. During the retrieval phase its values will be compensated according to specific integer division rules.

![Block mapping process](image)

**Fig. 5.** Block mapping process.

**E. Embedding Signature**

The domain transformation method offers the potential of embedding more information and stronger resistance to many common attacks. Each bit is embedded in a block of RONI. Their indices are computed from the block indices mapping phase and consider the supposition that the length of a watermark is less than the number of sub-blocks in RONI.

After the mapping phase on RONI blocks is completed, one LWT level is applied to get four subbands (LL, LH, HL, HH) for each block. High frequencies may be lost by compression or scaling; therefore, the watermark will be embedded in the lower frequency by updating its value according to Eq. (9). In addition, a quantization parameter ($Q_s$) can be used to achieve better performance in terms of robustness. Herein we use the LL subband to embed the watermark. LL sub-band first is quantized by a scaling factor ($Q_s$) as in the following Equation:
\[ q = \text{floor}\left(\frac{LL}{Qs}\right) \]  

(8)

Qs is a scaling factor.

Then embed bits of Signature as in the Eq. (9):

\[
LL = \begin{cases} 
(q * Qs) + \left(\frac{Qs}{2}\right) & \text{if } \text{mod}(q, 2) = W(idx) \\
((q + 1) * Qs) + \left(\frac{Qs}{2}\right) & \text{otherwise}
\end{cases}
\]

(9)

\( \text{for } idx = 1 \text{ to length}(W) \)

After embedding the bit in LL, apply the inverse of LWT on the current block. Finally, when all bits are
embedded reconstruct the RONI blocks to get watermarked RONI and then merge ROI with watermarked
RONI to get the watermarked medical image. Algorithm (2) shows the steps of the embedding process.

**Algorithm 2: Embedding Signature**

**Input:**
- ROI and RONI.
- Sig // The signature

**Output:**
- WMI // Watermarked Medical Image

**Step1:** Partition the RONI into non-overlapping sub-blocks of size 2×2 pixels.

**Step2:** Repeating step 3.1 to step 3.5 for each bit Signature Sig until all signature bits are embedded.

**Step2.1:** Each bit in the Sig is embedded in a block of RONI whose number is selected randomly
using the eq. (1).

**Step2.2:** Apply LWT on the selected block (the result is LL, HL, LH, and HH).

**Step 2.3:** Make quantization to LL by using Equation (2).

**Step 2.4:** Embed one Sig bit in the sub-bands (LL) of each mapping block using Equation (3):

**Step 3.5:** Applying inverse of LWT on the watermarked block.

**Step5:** Reconstruct the blocks of RONI to get watermarked RONI.

**Step6:** Merge ROI with watermarked RONI to get WMI.

After embedding the bits of Signature in RONI, the remapping is done then rearranges the square
matrix of RONI to its original location in the medical image. The watermarked medical images send to the
receiver via the internet in a secure manner.

**F. Block Remapping Phase**

In this phase, the blocks are remapping to their original locations in the RONI by applying the revealing
operations performed by algorithm 3.

**Algorithm 3: Block Remapping**

**Input:**
- \(\begin{bmatrix} x' \\ y' \end{bmatrix}\) //Mapping indices
- A // prime keys array of 2×2

**Output:**
- \(\begin{bmatrix} x \\ y \end{bmatrix}\)

**Step1:** Construct two linear equations set.
Step2: Create the coefficients matrix, $A'(\cdot)$, of the corresponding linear equations, that is;

$$a'_{ml} = a_{m,l}$$  \hspace{1cm} (10)

Where $a'_{ml} \in A'$, $a_{m,l} \in A$, $m=1,2$ and $l=1,2$

Step3: Determine the determinant value of $A$ (i.e., $D=\text{det}(A)$), and the corresponding complementary matrix $C$; such that for all values of $j$ the following condition is satisfied:

$$\sum_{l=1}^{2} a_{ij} C_{ij} = \sum_{j=1}^{2} a_{ij} C_{ij} = D$$  \hspace{1cm} (11)

Here, the matrix element $C_{ij}$ is equal to the determinant of the reduced matrix $C$ (whose $i^{th}$ row and $j^{th}$ column are removed) multiplied by the factor $(-1)^{i+j}$.

Step4: The values of the retrieved secret indices $\{V'_j | j=1...2\}$ could be determined using:

$$V'_j = \frac{1}{D} \left\{ \left( \sum_{l=1}^{2} C_{ij} S_{n_l} \right) + w_j \right\}$$  \hspace{1cm} (12)

Where $w_j$ is an integer number, whose value is multiples of N, such that:

$$w_j = N \sum_{l=1}^{2} C_{ij} p_l$$  \hspace{1cm} (13)

G. Extraction Signature

Firstly, to extract the Signature from RONI, it is divided into non-overlapping blocks of 2 × 2 pixels and performed mapping for sub-blocks. Then bits of the Signature are extracted from RONI blocks by applying one level of LWT on the selected blocks and making quantization to the resulted LL using Eq. (6).

Finally, the bits of extracted Signature are obtained from the result of the quantization of LL ($q$) using Eq. (14):

$$\text{Extracted_watermark}(i) = \text{mod}(q,2)$$  \hspace{1cm} (14)

Where $i$ represented the index of the extracted watermark. Algorithm (4) shows the steps of extraction operation:

Algorithm (4): Extraction Process

Input:  
$WMI$ // Watermarked Medical Image

Output:  
$\text{Encrypted\_Sign}$ // The Encrypted Signature

Step1: Segment the $WMI$ into ROI and RONI.

Step2: Partition the RONI into non-overlapping sub-blocks of size 2 × 2 pixels.

Step3: repeat step3.1 to step 3.5 until all watermark bits are extracted.

Step3.1: Mapping the sub-blocks using equation 6.

Step3.2: Each bit in the Signature is extracted from a sub-block of RONI after mapping.

Step 3.3: Make quantization to LL (by using Equation (6))

Step 3.4: Extract one encrypted signature bit from the sub-bands (LL) of each subblock by using Eq. (17).
After the watermark is extracted represented by an encrypted signature, a deciphering is performed. The decoding of the chaotic map with the same key for enciphering is applied, and then the Hash and EPR is reconstructed.

VI. EXPERIMENTAL RESULTS

A set of samples of EPR and generated hash code by the proposed hashing method are used as a signature for testing, as displayed in Figs. 7 and 8. And also, the performance of the proposed watermarking system is verified in terms of imperceptibility and robustness on 8 bits grayscale of MRI brain medical image of size 512×512 for 1000 images.

Different parameters are set during the simulations for the proposed hash method like the resized image dimension \(m, n\)–level for the SLT transformation, and the size of block \(k\times k\) for the DCT transformation. The performance of the algorithm is tested under the subsequent parameters: \(n=1, k=32, m=512\). The bit error rate (BER) is used as a metric to measure the distance between hash values and it is defined as:

\[
d_{xy} = \frac{1}{N} \sum_{i=0}^{N-1} |x_i - y_i|
\]

Where \(x\) and \(y\) are two \(N\) length binary vectors.

A successful algorithm against legitimate distortion is robust. Some distortions – JPEG compression, scaling, medium smoothing, wiener filtering, rotation, and sharpening – are considered legitimate. In practice, they are typically found. It is expected that the hash value is not susceptible to these operations. We measure the average hash distance for each pair of the original image and its distorted version. Table 1 displays the results.

| Attacks     | Proposed Method | Ref. 24 | Ref. 25 | Ref. 26 | Ref. 27 |
|-------------|-----------------|---------|---------|---------|---------|
| Wiener Filtering | 0               | -       | -       | -       | 0.00    |
|              |                  |         |         |         | 39      |
The proposed hash code generation results are acceptable in most types of attacks compared with some related researches. The table shows that the proposed scheme provides more durability under mean, median, rotation noise because this type of noise affects the random pixels so that the whole image is not affected. Thus the embedded EPR data is not destroyed. Nevertheless, the approaches demonstrated a vulnerable to geometric manipulations such as rotations.

### A. Security Analysis of Chaotic Encryption

To increase the security and robustness of the proposed system, the watermarks are encoded using a chaotic method.

The quadratic map is used to generate a chaotic sequence by using Eq.(3). The sequence is very sensitive to a change in an initial value, where a very small difference in the initial values can cause a large impact on the next values. As illustrated in Fig. 9 two signals are generated with initial condition (x0= 0.5 and x0= 0.50000000000001) from quadric chaotic generator. Fig. 10 presented the auto and cross correlations between these signals. As we see, the cross and auto correlation characteristics look like those of random white noise, even though their initial conditions are somewhat different. It can be concluded that the Quadrate map can generate uncorrelated sequences and exhibit good autocorrelation properties making a call for using in security applications.

| Method               | Median Filtering | Sharpening | Sample Down | JPEG Compression | Rotation 10° | Scale 40% | Discrimination |
|----------------------|------------------|------------|-------------|------------------|--------------|-----------|----------------|
|                      | 0.0125           | 0.0121     | 0.0542      | 0.0365           | 0.0367       | 0          | 0.487          |
|                      | -                | -          | 0.12        | 0.18             | 0.12         | 0         | -              |
|                      | -                | -          | 0.09        | 0.03             | 0.06         | 0         | -              |
|                      | -                | -          | 0.0         | 0.13             | 0.14         | 0         | -              |
|                      | -                | -          | -           | 0.78             | 0.65         | -         | 63             |
|                      | -                | -          | -           | -                | -            | 0         | -              |

![Fig. 8. Sensitivity to initial conditions.](image)
**Figure. 9.** Auto and cross correlation performance for Quadric chaos generator.

Fig. 11 depicts the coded Signature in Fig. 9 after applying eq. 4, while Fig. 12 depicts the cross correlation between the encrypted Signature and the original Signature.

From Fig. 12, it is noticed that the characteristics of outputs look like those of random AWGN (Additive White Gaussian Noise).

**B. Testing the Fidelity Measures of Proposed Watermarking Method**

The watermarking algorithm embeds a signature included an encoded hash code of the sender (doctor) of length 256 bits and EPR of length 512 bits, and then the size of the total length of Signature is 768 bits. The PSNR is used to evaluate the fidelity of the embedding scheme Fig. 13 shows the original and watermarked images with their PSNR values for a sample of images. And the PSNR equation is given by Eq. (15) [28]:

\[
\text{PSNR} = 10 \log_{10} \left( \frac{R^2}{\text{MSE}} \right)
\]  

(16)

Can calculate MSE by Eq. (17)

\[
\text{MSE} = \frac{1}{MP} \sum_{i=0}^{M-1} \sum_{j=0}^{P-1} [\text{OMI}(i,j) - \text{RMI}(i,j)]^2
\]  

(17)

Where R is the maximum fluctuation in the input image data type, Mean Square Error (MSE), PSNR (Peak signal to Noise Ratio), M, P are the sizes of the original medical image (OMI) and the retrieved medical images (RMI), respectively.
The PSNR values are changed according to various factors such as data payload (watermark size), scaling factor and RONI size used in the proposed embedding algorithm. The size of the watermark is fixed, but the RONI size is changeable and the value of scaling factor = 2.

C. Robustness Measures of Proposed Watermarking Method against Attacks

The robustness of the system is measured with several kinds of attacks. The BER is used to calculate the difference between the extracted hash code and the hash code generated from the received brain image to check the integrity of ROI. If the integrity of ROI is verified, it means that the region is not tempered, and then the patient information is decrypted. To define the degree of robustness of the proposed embedding method, Normalized Correlation (NC) is calculated between the original and the extracted patient information using the following Equation [29]:

\[
NC = \frac{\sum_{m=1}^{M} \sum_{n=1}^{N} W_m W_n'}{\sqrt{\sum_{m=1}^{M} \sum_{n=1}^{N} W_m^2} \times \sqrt{\sum_{m=1}^{M} \sum_{n=1}^{N} W'_n^2}}
\]  

(18)

Where W is original watermark and W' is recovered watermark with zero mean value each.

By calculating the bit error rate (BER) using Eq. (15). Table 2 shows the results acceptable in most types of attacks. The table shows that the proposed scheme provides more durability under these attacks,
and such noise affects the random pixels so that the whole image is not affected. Thus the embedded EPR data is not destroyed.

**TABLE 2** HD and NC after subjecting several attacks on the watermarked image

| Type of attack | HD%  | NC   |
|---------------|------|------|
| No attack     | 0    | 1    |
| Salt & pepper with different density of noise | 0.01 | 0.0329 | 0.9905 |
| Gaussian (mean =0), variance =0.00001) | 0.07 | 0.0349 | 0.9689 |
| Gaussian (mean =0), variance =0.00002) | 0.1  | 0.03587 | 0.9578 |
| Speckle (variance=0.001) | 0.05 | 0.0343 | 0.9771 |
| Speckle (variance=0.002) | 0.07 | 0.0349 | 0.9689 |
| Cropping | 0.07 | 0.0349 | 0.9689 |
| Brightness +50 | 0.07156 | 0.9902 |
| Brightness +80 | 0.0400 | 0.9764 |

To assess the robustness of the presented scheme against several attack attempts, such as mean, median, share. the PSNR is calculated and compared with other related works, and the consequences are arranged in Table 4.

**TABLE 3** PSNR values under various attacks

| Type of attack | Proposed system | REF. [30] | REF. [31] | REF. [32] |
|---------------|-----------------|-----------|-----------|-----------|
| Salt and pepper noise 10% | 42.15 | 41.43 | - | - |
| Gaussian (mean =0), variance =0.00001) | 13.01 | 12.53 | 12.32 |
| Cropping 5% | 41.51 | 40.62 | - | - |
| Cropping10% | 39.60 | 38.45 | - | - |
| Brightness +5 | 16.69 | - | - | - |
| Brightness +10 | 16.69 | - | - | - |
| Median attack | 22.40 | - | 21.85 | 21.85 |
| Rotation attack | 12.50 | - | 12.45 | 12.38 |
| Noise attack | 35.65 | - | - | 12.38 |
| Contrast-enhanced | 15.06 | - | - | - |
| Local modification | 13.817 | - | - | - |

Table 4 shows the time consuming for each step in the proposed system.

**TABLE 4** Time consuming for the proposed system.
V. CONCLUSIONS

To verify the integrity and authenticity of medical image, this paper proposed a method which is combined the hash signature with the watermarking technique based on the frequency domains. The hash code is extracted from ROI by hybrid the SLT and DCT transformations by employing the good features of them to generate robustness hash code then it combined with EPR to form a watermark. To increase the security and robustness of the proposed system, the watermark is encoded by a chaotic map with a secret key to generate a signature. The transformation domain method offers the potential of embedding More knowledge and better attack resistance. The block mapping approach provides extra level of security and high pixel correlation can be detached. The proposed approach demonstrated high image quality as regards robustness in the experimental findings. Furthermore, the proposed approach was shown to be very stable against addition of noise and JPEG compression. Good output has been demonstrated for geometric distortions including scaling, rotation, translation and shearing.

REFERENCES

[1] Elhoseny M, Shankar K. Optimal bilateral filter and convolutional neural network based denoising method of medical image measurements. Measurement. 2019;143:125-135.
[2] Somaraj S, Hussain MA. Securing medical images by image encryption using key image. Int J Comput Appl. 2014;104(3):30-34.
[3] Rose-Mharie Åhlfeldt. Information Security in Distributed Healthcare, Exploring the Needs for Achieving Patient Safety and Patient Privacy. PhD Thesis, DSV Report Series No. 08-003, ISBN 978-91-7155-73-1, Stockholm, 2008.
[4] R. Åhlfeldt. Information Security in Home Healthcare Personal Integrity and Secrecy” Ph.D thesis, Skövde, SWEDEN, 2001.
[5] Weng L, Preneel B. A secure perceptual hash algorithm for image content authentication. In: IFIP International Conference on Communications and Multimedia Security. Springer; 2011:108-121.
[6] Menezes AJ, Van Oorschot PC, Vanstone SA. Handbook of Applied Cryptography. CRC press; 2018.
[7] Mahmood AB, Dony RD. Segmentation based encryption method for medical images. In: 2011 International Conference for Internet Technology and Secured Transactions. IEEE; 2011:596-601.
[8] Laouamer L, Al Shaikh M, Nana LT, Pascu AC. Informed symmetric encryption algorithm for DICOM medical image based on N-grams. In: 2013 Science and Information Conference. IEEE; 2013:353-357.
[9] Dai Y, Wang X. Medical image encryption based on a composition of logistic maps and chebyshev maps. In: 2012 IEEE International Conference on Information and Automation. IEEE; 2012:210-214.
[10] Bouslimi D, Coatrieux G, Cozic M, Roux C. A joint encryption/watermarking system for verifying the reliability of medical images. IEEE Trans Inf Technol Biomed. 2012;16(5):891-899.
[11] Singh AK, Dave M, Mohan A. Hybrid technique for robust and imperceptible image watermarking in DWT–DCT–SVD domain. Natl Acad Sci Lett. 2014;37(4):351-358.
[12] Singh AK, Dave M, Mohan A. Hybrid technique for robust and imperceptible multiple watermarking using medical images. Multimed Tools Appl. 2016;75(14):8381-8401.
[13] Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. John wiley & sons; 2007.
[14] Tataru RL. Secure Image Verification in Jointed Frequency Domains. IJCSA. 2015;12(2):99-119.
[15] Cedillo-Hernandez M, Garcia-Ugalde F, Nakano-Miyatake M, Perez-Meana H. Robust watermarking method in DFT domain for effective management of medical imaging. Signal, Image Video Process.
2015;9(5):1163-1178.

[16] Abraham J. A Blind Watermarking Scheme for Tamper Detection in Digital Images. *ICTACT J Image Video Process.* 2015;6(2):1133-1136.

[17] Sharma A, Singh AK, Ohrera SP. Secure hybrid robust watermarking technique for medical images. *Procedia Comput Sci.* 2015;70:778-784.

[18] Parah SA, Ahad F, Sheikh JA, Bhat GM. Hiding clinical information in medical images: a new high capacity and reversible data hiding technique. *J Biomed Inform.* 2017;66:214-230.

[19] Parah SA, Sheikh JA, Ahad F, Loan NA, Bhat GM. Information hiding in medical images: a robust medical image watermarking system for E-healthcare. *Multimed Tools Appl.* 2017;76(8):10599-10633.

[20] Rakhamwati L, Wirawan W, Suwadi S. A recent survey of self-embedding fragile watermarking scheme for image authentication with recovery capability. *EURASIP J Image Video Process.* 2019;2019(1):61.

[21] Khare P, Srivastava VK. A secured and robust medical image watermarking approach for protecting integrity of medical images. *Trans Emerg Telecommun Technol.* Published online 2020.

[22] Swaraja K, Meenakshi K, Kora P. An optimized blind dual medical image watermarking framework for tamper localization and content authentication in secured telemedicine. *Biomed Signal Process Control.* 2020;55:101665.

[23] Mohammed, R. S., & Sadkhan, S. B., “Speech scrambler based on proposed random chaotic maps,” IEEE International Conference on Multidisciplinary in IT and Communication Science and Applications, Baghdad, pp.1–6, 2016.

[24] R. A. P. Hernandez, M. N. Miyatake, and B. M. Kurkoski, “Robust image hashing using image normalization and SVD decomposition,” in *2011 IEEE 54th International Midwest Symposium on Circuits and Systems (MWSCAS)*, 2011, pp. 1–4.

[25] S. S. Kozat, R. Venkatesan, and M. K. Mihčak, “Robust perceptual image hashing via matrix invariants,” in *2004 International Conference on Image Processing, 2004. ICIP’04.*, 2004, vol. 5, pp. 3443–3446.

[26] R.-L. Tataru, “Image hashing secured with chaotic sequences,” in *2014 Federated Conference on Computer Science and Information Systems*, 2014, pp. 735–740.

[27] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, “Image quality assessment: from error measurement to structural similarity,” *IEEE Trans. image Process.*, vol. 13, no. 1, 2004.

[28] Fatma E, Hikal NA, Abou-Chadi FEZ. Secret medical image sharing and EPR data embedding scheme over cloud computing environment. *Int J Comput Appl.* 2013;69(11).

[29] Jadhav S, Bhalchandra A. Robust digital image-adaptive watermarking using BSS based extraction technique. *Int J Image Process.* 2010;4(1):77.

[30] Puvvadi Aparna, Polurie Venkata Vijay Kishore, An Efficient Medical Image Watermarking Technique in E-healthcare Application Using Hybridization of Compression and Cryptography Algorithm, *Journal of Intelligent Systems*, 27(1), 115-133 - September 2017 https://doi.org/10.1515/jisys-2017-0266

[31] J. Liu, J. Ma, J. Li, M. Huang, N. Sadiq and Y. Ai, "Robust Watermarking Algorithm for Medical Volume Data in Internet of Medical Things," in *IEEE Access*, vol. 8, pp. 93939-93961, 2020, doi: 10.1109/ACCESS.2020.2995015.

[32] Jing Liu, Jingbing Li, Jixin Ma, Naveed Sadiq, Uzair Aslam Bhatti, Yang Ai, “A Robust Multi-Watermarking Algorithm for Medical Images Based on DTCWT-DCT and Henon Map”, *Appl. Sci. 2019, 9, 700; doi:10.3390/app9040700*