International Information and Engineering Technology Association
Advancing the World of Information and Engineering

International Journal of Safety and Security Engineering
Vol. 14, No. 5, October, 2024, pp. 1487-1493
Journal homepage: http://iieta.org/journals/ijsse

Medical Image Authentication Using Statistical Correlations

Haranahalli Rajannaa Chennamma[1*], Basanth Kumar Halaguru Basavarajappa[2], Madhushree Basavaraju[1], Kyatanahalli Nanjappa Sowmya[3], Appusamy Venkataraman Senthil Kumar[4]

[1] Department of Computer Applications, JSS Science and Technology University, Mysuru 570006, India
[2] Maharaja Institute of Technology Thandavapura, Department of MCA, NH 766, Nanjanagudu Taluk, Mysuru 571302, India
[3] Department of Information Science and Engineering, JSS Academy of Technical Education, Bengaluru 560059, India
[4] Department of Computer Applications, Hindusthan College of Arts and Science, Coimbatore 641028, India

Corresponding Author Email: hrchennamma@jssstuniv.in

https://doi.org/10.18280/ijsse.140516

Received: 17 February 2024
Revised: 1 June 2024
Accepted: 22 June 2024
Available online: 31 October 2024

Keywords:
gray level co-occurrence matrices (GLCM), least significant bits (LSB), reversible watermarking, statistical measures

ABSTRACT

Ensuring the integrity and confidentiality of patient information is crucial since it contains sensitive information. Normally the source or owners' information is used as watermark which is susceptible to illegal manipulations. This research work proposes an imperceptible and reversible watermarking algorithm designed to embed image content-based information for detecting illegal alterations in medical images. The algorithm operates by first normalizing the medical image within the range 0 to 255 and dividing it logically into 4×4 equal blocks. Subsequently, for each block, a Gray-level Co-occurrence Matrix is computed, enabling the derivation of statistical correlations such as contrast, correlation, energy, and homogeneity. These statistical measures collectively form a unique signature, which serves as the watermark to embed in the least significant bits of the pixels of the cover image. Further, in order to verify its integrity, a watermark can be extracted and compared with the original. The proposed watermarking method accelerates the accurate recovery of medical images by retaining their originality and also facilitates the efficient detection of unauthorized manipulations. Experimental results demonstrate the superior imperceptibility achieved by the proposed approach. The proposed method can be used with medical imaging modalities such as X-rays, CT scans, MRI scans, ultrasound scans, etc.

1. INTRODUCTION

The usage of computer graphics in healthcare applications helps doctors for proper diagnoses of patients as well as for effective treatment. Telemedicine or e-medicine has accelerated the online examination of patients' medical scans that are generated through X-rays, magnetic resonance imaging (MRI), computerized tomography (CT), and other modalities. These medical scans are susceptible to illegal manipulations when they undergo various hospital workflows which pose a significant threat to healthcare systems. Consequently, maintaining confidentiality and integrity is a primary concern in safeguarding medical images from unauthorized access.

Digital Imaging and Communication in Medicine (DICOM) is the commonly used standard file format in medical applications. The DICOM standard ensures the possibility of data exchange even if such medical data or images are produced by different equipment, hospitals, or companies. The header of every DICOM file contains acquisition parameters, and picture dimensions and patient's demographics; the remaining space of the DICOM file contains image data. This DICOM format provides both picture data and header information together.

Digital watermarking turns out as an efficient approach to assure the authenticity and integrity of medical images.

The method presented by Guo et al. [1] uses an identifier in an electronic patient record as a watermark, and a method presented by Liu et al. [2] uses the hospital logo as a watermark. The aforementioned techniques use watermarks, which are information-dependent. A unique signature is required, which is generated based on the image contents and used as a watermark for the authenticity and integrity verification of medical images.

The Gray-Level Co-occurrence matrix (GLCM) plays a crucial role in diagnosis and treatment. It analyzes spatial relationship between pixel intensity values to yield qualitative measure which aid in the characterization of tissue qualities like smoothness, homogeneity, and roughness. As a result, we use GLCM in our research work to produce distinct signatures.

This paper introduces a reversible watermarking scheme designed to detect unauthorized alterations done with medical images. Firstly, the image is normalized between the range 0 and 255 then divided into four equal sub-blocks, further a distinctive signature is generated for each sub-block using GLCM (Gray-Level Co-occurrence Matrix). This signature serves as a watermark and least significant bit (LSB) of the pixels are used to embed such a watermark in the cover image. In order to verify the integrity of image content, the embedded watermark will be extracted and compared with the original generated signature. The proposed approach demonstrates the capability to accurately recover images in their original state and efficiently detects any unauthorized manipulations. The paper introduces a straightforward yet an efficient method to uniquely represent with signature for each medical image. Notably, the proposed technique, which utilizes texture features for signature generation, represents a pioneering approach in utilizing such signatures as watermarks to enhance the security of medical images. When the watermark is compromised or fails, it can lead to false information, content fabrication, and patient misdiagnosis.

The paper makes two key contributions:

- To create a content-based signature that is unique in nature and used as a watermark.
- To verify the integrity of medical images based on the LSB substitution technique.

The subsequent sections are structured as follows: Section 2 provides an overview of the techniques employed to guarantee the integrity of medical images. Section 3 presents a comprehensive description of the method for verifying the medical image content for its originality. Section 4 presents experimental findings, and the paper is concluded in Section 5.

2. RELATED WORKS

Medical images represent the patient's medical condition and help in diagnosis and treatment of patient assisting as evidence to doctors and patients. Diagnostic centers share the medical images across the network and security, patient privacy is a matter of concern. Tampering of medical images has been increasing to claim false insurance, malign personalities affecting the faith of the people over the medical world. Protection of medical images to ensure CIA triad is accomplished with watermark at spatial level [3-11] and through medical image transformations [12-20].

2.1 Spatial domain-based watermarking of medical images

Spatial Watermark involves altering the intensity and color value associated with the pixel of an image. Least Significant Bit substitution (LSB) [3, 4] and Difference Expansion (DE) [3-8, 12, 13] are the popular approaches adopted for embedding a watermark in literature.

Zain and Fauzi [3] focused on local manipulation detection. The watermark method involved four concepts: block-based, separation of authentication and recovery bits with hierarchical average intensity as an image feature. It uses simple operations like parity checks and comparison between average intensities, and can detect image tampering with recovery for tampered images. Further, they improved this method in recovery and reconstruction rates for medical images. Image quality is improved in the ROI with change of 2 bits maximum per 4 pixels by locating recovery bits outside the ROI, and enhances reconstructed image quality using 2×2 pixels [4]. The lossless watermarking scheme proposed by Guo and Zhuang [1] employs difference expansion of adjacent pixel values and a polygon region to prevent distortion in ROI. It also includes a digital signature for image integrity and an identifier from the electronic patient record for authenticity. Al-Qershi and Khoo [5] considered a fragile method involving DE and its modified version to overcome drawbacks of existing schemes. It uses a combination of two DE techniques, embedding the first watermark with *'Patient Data'* and ROI hash message MD5. It is then included with recovery data into RONI along with the original. Further, Al-Qershi and Khoo [6] proposed a two-dimensional DE technique with high embedding capacity; the original DICOM image is partitioned into non-overlapping blocks and is transformed using Haar wavelet transform into frequency domains. 16 bits were concealed to hide patient data, authenticate ROI, localize tampered areas, and recover them. Al-Qershi and Khoo [7] further introduced an improvement over the DE technique to improve the hiding capacity for medical images. The intended technique used a high embedding capacity approach for the smooth region and original DE technique to a non-smooth region after dividing the image into regions as smooth and non-smooth. Tan et al. [8] proposed a dual-layer watermark by embedding patient metadata and source information into medical images using a reversible scheme, to ensure authenticity and integrity. The method incorporates public-key encryption and tamper detection features. Das and Kundu [9] used two different fragile watermarking methods for enforcing the integrity, authenticity, and confidentiality of medical-information in medical data management. The last LSB-planes of the medical image are modality and task independent providing high security were used for the embedding purpose. It preserves the visual/information quality and diagnostic value of medical data and conforms to strict specifications and requirements. Naseem et al. [12] proposed a reversible and fragile watermarking scheme by introducing the Residue Number System and chaotic key in medical images. The chaotic key is used to generate a 256-bit hash for the entire image, and is then embedded in the RONI. At the receiving side, a watermark is extracted and compared with the un-watermarked image's hash to check tampering. The scheme is blind, eliminating the need for the original medical image. Eswaraiah and Reddy [13] proposed a novel medical image watermarking technique to avoid distortion, verify ROI integrity, detect tampered blocks, and recover original ROI without loss. The technique segments medical images into ROI, RONI, and border pixels, embeds authentication and ROI information in border pixels, and recovers ROI without loss. Shehab et al. [10] developed a SVD-based fragile watermarking scheme for tamper localization and self-recovery in medical applications. It uses two codes, one containing block information and the other containing block authentication information. The Arnold transform is used to hide neighboring pixel information, improving self-recovery. The scheme also improves the PSNR ratio through neighborhood block-based recovery. Qasim et al. [11] proposed an amalgam of active and passive forensics through blind reversible watermarking approach to detect intentional and unintentional changes in brain Magnetic Resonance (MR) images. The MRI image is segmented into ROI and RONI. Watermark data is included into a ROI using the DE technique. The method has attained better imperceptibility with low degradation.

2.2 Transform domain-based watermarking of medical images

In the transform domain, the DICOM image data from the spatial domain is transformed using mathematical transformations. Integer wavelet transform (IWT), discrete wavelet transform (DWT), discrete cosine transform (DCT) and Slantlet transform (SLT) are few such transformations.

Woo et al. [14] created a fragile annotated watermark using patient data for annotation and digitally signed data through the general practitioner is embedded in a frame pattern at the borders of the image. The central region of the image contains the binary fragile watermark distributed using the LSB approach. Intentional compressions, noise, and copy-move forgery attacks are effectively detected with distorted watermark patterns. Wu et al. [15] proposed an additive watermark over the preprocessed medical image leading to no flips in pixels and the steganography technique was near-lossless in nature. The recovery method was ROI-based in each block and the authentication failure on the whole image could be narrowed down to the tampered block. With the extraction of scattered JPEG bit-strings the ROI is recovered. The areas prone to micro-calcification should be selectively chosen for ROI. Arsalan et al. [16] proposed a block-based fragile watermarking scheme, utilizing an intelligent computation of compounding thresholds in the IWT domain. The reversible property of the watermarking scheme is improved and avoids round-off errors. The approach uses binary GA for integer value-based optimization, allowing for the selection of local optimum thresholds and effective trade-off between watermark payload and imperceptibility, particularly in medical imagery. Gadhiya et al. [17] used a discrete wavelet transform for detection and locating forgery in digital medical images. Hash representation of DWT helps to identify tampering and its direction effectively. The method is sensitive enough to detect even the smallest changes and resilient against harmless alterations. Liu et al. [2] generated a Watermark with a combination of authenticity related data and integrity data. Authenticity data is the 160-bit hash value of a hospital logo and integrity data includes tamper detection information of the whole medical image generated using the SHA-1 hash function. Localization of tampered regions is carried out using CRC-16 and recovery information with IWT. It is then embedded into the image using SLT, SVD and recursive dither modulation to provide robustness and reduce faults in diagnosis. Swaraja et al. [18] exploited visual and edge entropy for concealing information in medical images to detect malicious tampering and authenticate medical images. HVS model determines RONI blocks suitable for watermark insertion along with DWT, Schur transforms and PSBFO integration. The HVS model ensures discernibility during watermark insertion and Lempel-Ziv-Welch (LZW) compression is carried out over the dual watermarks to increase payload capacity. Blind watermarks with chaotic sequences are generated using IWT, LSB and ILC proposed by Nazari and Mehrabian [19]. Depending on the core diagnosis area of focus the medical image is classified into ROI and RONI. IWT sub-bands at the first and second levels are utilized for watermark insertion in the middle frequency of the RONI. Third level sub-band of IWT is used for verifying authenticity by embedding the doctor's signature. Sayah et al. [20] ensures integrity through blind watermarking using frequency content. Schur-transformed data is applied over the mid-frequency sub-bands and the hash value is replaced with the upper triangular matrix values. Copyright of medical images can be effectively managed with this scheme. Pal et al. [21] presented an efficient authentication scheme for digital image watermarking on medical images using Support Vector Machine (SVM) and Lifting Wavelet Transform (LWT). SVM separates the Region of Interest (ROI) and NROI in the image, while LWT embeds watermark information within the NROI part. A shared secret key enhances robustness.

From the relevant literature, we find that most of the watermarking schemes use patient information for generating watermarks and suffer from low imperceptibility. In this work, distinct signatures based on texture statistical properties of medical image content are proposed. The unique signature is then included as a watermark for integrity verification of medical images. To the best of our knowledge, the method of generating distinct signatures based on textural statistical measures is the first of its kind in the literature.

3. PROPOSED METHOD

Computer generated images contain complex information and high visual quality. The advantage of the reversible watermarking over conventional watermarking is that, embedding and extracting watermark information by preserving its integrity and quality of the cover data.

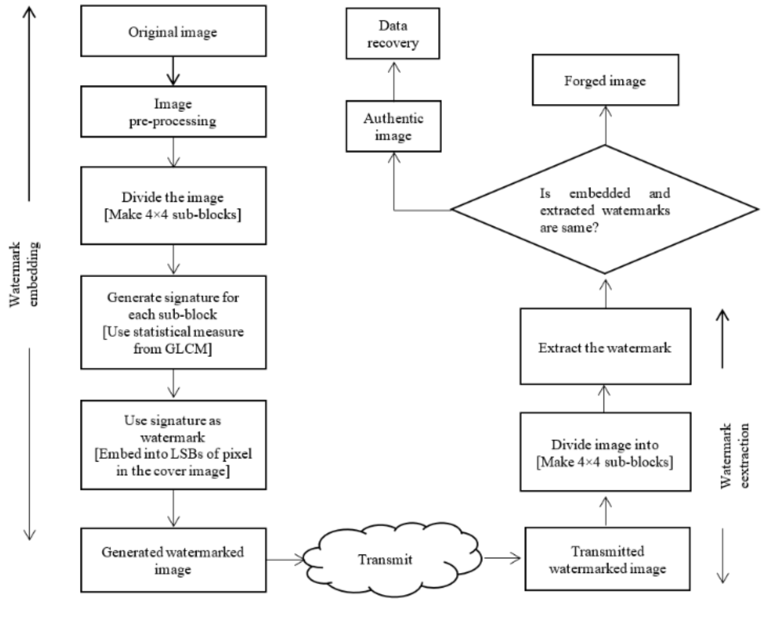

Original image
Image pre-processing
Divide the image [Make 4×4 sub-blocks]
Generate signature for each sub-block [Use statistical measure from GLCM]
Use signature as watermark [Embed into LSBs of pixel in the cover image]
Generated watermarked image
Transmit
Transmitted watermarked image
Divide image into [Make 4×4 sub-blocks]
Extract the watermark
Is embedded and extracted watermarks are same?
Authentic image
Data recovery
Forged image
Watermark embedding
Watermark eextraction

Figure 1. Schematic diagram of reversible watermarking scheme for medical image authentication and integrity verification

To generate a distinct signature based on image contents and to maintain good visual quality in computer-generated imagery post-insertion, we present a reversible watermarking approach that divides an image into 4×4 blocks. Then, using statistical measures derived from gray-level co-occurrence matrices (GLCM), a distinct signature is generated for each block. Subsequently, this distinct signature serves as a watermark and is embedded in the least significant bits of the picture elements in the cover image. Then, the watermark is extracted from the watermarked counterpart and compared with the embedded one to verify its integrity. If they are identical, the image is declared authentic and recovers the data. Otherwise, the image is flagged as forged. Figure 1 presents a reversible watermarking approach designed for tampering detection with computer-generated imagery.

The proposed approach involves four stages: signature/watermark creation, watermark encoding, watermark extraction, and recovery of data.

3.1 Signature/watermark creation

The given Image denoted by I, is transformed into a grayscale and its picture elements are normalized in the range [0-255] and is described by Eq. (1).

$$\mathrm{Norm_I} = \frac{(y_i - (\min(y))}{(\max(y) - (\min(y))} \times 255 \qquad (1)$$

where, y_i in Eq. (1) represents pixel intensity of normalized image, min(y) and max(y) denotes minimum and maximum values of the normalized image.

The normalized image $\mathrm{Norm_I}$ is segmented into 4×4 blocks (refer to Figure 2), each block comprising 128×128 pixels.

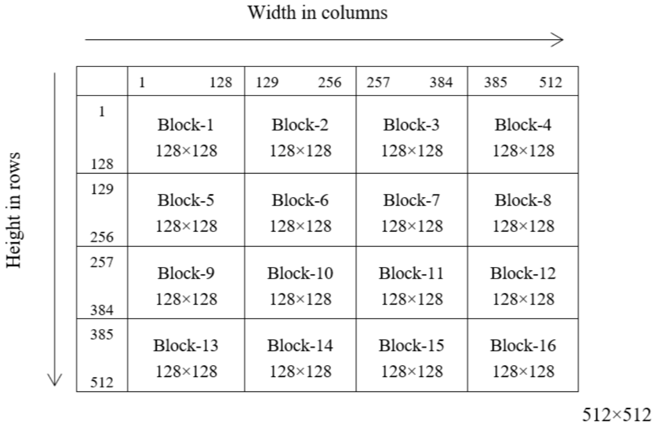


Figure 2. Illustration of normalized image segmented into 4×4 blocks

Table 1. Statistical properties deduced from GLCM

Property	Formula
Contrast	$\sum_{m,n} \lvert m-n \rvert^2 \; l(m,n)$
Correlation	$\sum_{m,n} \frac{(m-\mu_m)(n-\mu_n)l(m,n)}{\sigma_m \sigma_n}$
Energy	$\sum_{m,n} l(m,n)^2$
Homogeneity	$\sum_{m,n} \frac{l(m,n)}{1+\lvert m-n \rvert}$

For each block, GLCM [22] is computed with the parameters d=1 and Θ=0 respectively. Consequently, statistical properties, including contrast, correlation, energy, and homogeneity (refer to Table 1) are computed from the GLCM. The resulting values are multiplied by 100 then rounded off to the nearest integer, transformed into characters, resulting in four characters per block. This process yields a string of sixty-four characters for an image.

Here, the notations l(m, n) signifies the value at (m, n) location in the GLCM, with μ and σ representing the mean and standard deviation, respectively.

3.2 Watermark embedding

In the watermark embedding phase, the least significant bit substitution (LSB) technique is employed to embed a watermark into the cover image. It uses the Ex-OR operation, which modifies the value of picture elements by either zero or one, based on the LSB value of the pixel and the watermark bits. The algorithm for embedding the watermark into a cover image is outlined in Algorithm 1.

```
Algorithm 1:  Watermark Embedding
Input:        Normalized image – $N_I$
Output:       Watermarked image – $I_W$
Step 1:       Convert the watermark into binary
Step 2:       for i ← 1 to 4 do
              for j ← 1 to 4 do
                  input ← $N_I$block(i, j)
                  output ← input
                  k ← 1
              for x ← 1 to 128 do
              for y ← 1 to 128 do
               if k <= 32 then
              begin
              lsb ← input(x, y) % 2
                          t ← lsb ⊕ $W_b$(k)
                           output(x, y) ← input(x, y) + t
                          k ← k + 1
              end
              end
              end
              $I_w$(i, j) ← output
              end
              end
```

3.3 Watermark extraction

The algorithm for extracting the watermark from the watermarked version of the image is given in Algorithm 2.

```
Algorithm 2:  Watermark Extraction
Input:        Watermarked image – $I_w$
Output:       Watermark – W
Step 1:       Read $I_w$
Step 2:       Divide $I_w$into 4×4 blocks
Step 3:       k ← 1
Step 4:       fori ← 1 to 4 do
              for j ← 1 to 4 do
              if k <= 32 then
              begin
                          $\mathrm{bits}(k, 1) \leftarrow I_{W_{i,j}}$ % 2
                      k ← k + 1
              end
              end
              end
Step 5:       Transform the extracted bits into a string
              (W)
```

3.4 Recovery of data

The final step involves ascertaining whether the watermarked image has suffered any illegal alterations. This is accomplished by comparing the extracted watermark with the embedded one; if they match, the image is recovered using the Eq. (2). Conversely, if two watermarks are inconsistent, declare the image as fabricated.

$$W_i(x, y) = \text{LSB of beginning 32 pixels of } W_{m,n} \oplus S_B \tag{2}$$

where, m=1, 2, 3, 4; n=1, 2, 3, 4; B=1, 2, …, 32; $W_{m,n}$ represent the watermarked image and S_B corresponds to the secret information bits.

Illustration of watermark encoding, retrieval and restoration of data

Consider decimal value 80, its binary equivalent is 01010000, and watermark bit (W_b) is 1.

I. Watermark encoding

Watermarked data=01010000⊕1=01010001

II. Watermark retrieval

Extracted watermark=Watermarked data % 2=81 % 2=1

III. Data restoration

Watermarked data=81 and its binary equivalent is 01010001, and W_b=1

Data restore=watermarked data⊕W_b

Data restore=01010001⊕1=01010000

4. EXPERIMENTS

Forty CT lung original medical images in DICOM format, each with 512×512 picture elements, were randomly chosen from the dataset described by Mirsky et al. [23] to assess the effectiveness of the proposed technique. MATLAB R 2018a has been used for the experiment on a Windows 10 Pro platform with an Intel Core i3 processor and 8GB RAM. Since DICOM medical images contain negative pixel values, they were normalized in the range of 0 to 255 and transformed to grayscale. Each image was split into 4×4 subblocks to calculate GLCM. Statistical measures obtained from GLCM, as shown in Table 1, were then computed to provide a unique signature with a string of text containing 64 characters.

4.1 Evaluation measures for watermarked version of medical image

Evaluating the visual quality of watermarked medical images is essential because the introduction of the watermark in the image causes distortion, impacting the overall image quality. Evaluation criteria, including mean square error (MSE), peak signal-to-noise ratio (PSNR), and structural similarity index (SSIM) were utilized in our study. "The cover image and its watermarked counterpart were used for evaluation."

Let C_i represent the cover image and W_i represent the watermarked counterpart, both with a size of P×Q. The aforementioned evaluation criteria are described as follows:

$$\text{MSE} = \frac{1}{R_s\, C_s} \sum_{P=1}^{R_s-1} \sum_{Q=1}^{C_s-1} (\text{C}(\text{P}, \text{Q}) - \text{W}(\text{P}, \text{Q}))^2 \tag{3}$$

The R_s and C_s related to their respective row and column numbers. While C and W represent the original and watermarked counterpart at position (P, Q).

$$\text{PSNR} = 10 \log_{10} \frac{L^2}{\text{MSE}} \text{ decibel} \tag{4}$$

$$\text{SSIM}(O_i, W_i) = [l(C_i, W_i)]^{\alpha} * [C(C_i, W_i)]^{\beta} * [S(C_i, W_i)]^{\delta} \tag{5}$$

$$l(C_i, W_i) = \frac{2\, \mu_{C_i} \mu_{W_i} + C_1}{\mu^2{}_{C_i} + \mu^2{}_{W_i} + C_1} \tag{6}$$

$$C(C_i, W_i) = \frac{2\, \sigma_{C_i} \sigma_{W_i} + C_2}{\sigma^2{}_{C_i} + \sigma^2{}_{W_i} + C_2} \tag{7}$$

$$S(C_i, W_i) = \frac{\sigma_{C_i W_i} + C_3}{\sigma_{C_i} \sigma_{W_i} + C_3} \tag{8}$$

In summary, the overall index is given by:

$$\text{SSIM}(C_i, W_i) = \frac{\left(2\, \mu_{C_i} \mu_{W_i} + C_1\right)\left(2\sigma_{C_i W_i} + C_2\right)}{(\mu^2{}_{C_i} + \mu^2{}_{W_i} + C_1)\, (\sigma^2{}_{C_i} + \sigma^2{}_{W_i} + C_2)} \tag{9}$$

When α=β=γ=1 and C_3=$C_{2/2}$.

where, C_1=$(0.01*L)^2$, C_2=$(0.03*L)^2$, and L=255.

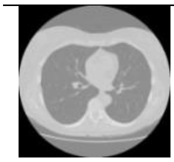
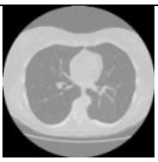
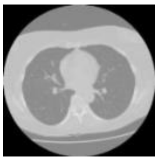
The results of the performance metrics used to evaluate the watermarked versions of the medical images are tabulated in Table 2. As seen from Table 2, it can be seen that the proposed technique has attained better imperceptibility. Figure 3 exhibits the reversibility of the content-based watermarking approach by pixel-by-pixel comparison between the cover image and the restored image, which shows no numerical difference between those images.

Further, the efficacy of the proposed approach in detecting unauthorized manipulations was tested by deliberately modifying some of the watermarked versions of medical images. Table 3 presents the comparison of visual quality between the combinations of cover (C_I), watermarked (W_I), restored (R_I), and forged images (F_I). As seen from Table 3, it can be found that the increase in PSNR value yields good imperceptibility, and a low PSNR value indicates changes in the watermark contents, resulting in an image that has been tampered with or forged. Further, to verify whether a large or small area of an image has been manipulated, MSE was adopted. A large value of MSE indicates a broader area has been manipulated, and a value beyond 0.0001 indicates a small area has been manipulated. Furthermore, identical values were found between (W_I, F_I) and (C_I, F_I) due to the low embedding capacity of the proposed watermarking approach. Further, a SSIM value of 0.99 was observed between (C_I, R_I), (W_I, F_I), and (C_I, F_I). From the experimental study, we found that performance metrics PSNR and MSE are found to be effective in verifying the integrity of medical images compared to SSIM.

Table 2. Visual quality of watermarked counterparts of medical images

Image Name	MSE	PSNR	SSIM	Image Name	MSE	PSNR	SSIM
1531_69	0.000896	78.6	1	2925_78	0.000900	78.58	1
1531_76	0.000938	78.4	1	2960_98	0.000938	78.4	1
1563_238	0.000965	78.28	1	2960_112	0.000965	78.28	1
1563_287	0.000870	78.73	1	3341_70	0.000961	78.3	1
1610_74	0.000919	78.49	1	3341_84	0.000908	78.55	1
1610_83	0.000954	78.33	1	3361_154	0.000973	78.25	1
1632_127	0.000957	78.31	1	3361_174	0.000946	78.37	1
1632_144	0.000847	78.85	1	4474_58	0.000938	78.4	1
1779_78	0.000904	78.56	1	4474_67	0.000965	78.28	1
1779_80	0.000919	78.49	1	4474_76	0.000923	78.47	1
1779_89	0.000885	78.66	1	4474_82	0.000893	78.62	1
1779_93	0.000946	78.37	1	6080_141	0.000923	78.47	1
1840_61	0.000874	78.71	1	6080_176	0.000923	78.47	1
1840_78	0.000950	78.35	1	6644_51	0.000889	78.64	1
2104_72	0.000900	78.58	1	6644_68	0.000851	78.83	1
2104_77	0.000900	78.58	1	C_1045_103	0.000835	78.91	1
2366_68	0.000954	78.33	1	C_1546_159	0.000854	78.81	1
2366_80	0.000950	78.35	1	C_1871_149	0.000935	78.42	1
2925_59	0.000908	78.55	1	C_1871_156	0.000908	78.55	1
2925_70	0.000889	78.64	1	C_1871_207	0.000912	78.53	1

Table 3. Comparison of visual quality between cover, watermarked, restored and forged images

Cover Image (C_I)	Watermarked image (W_I)	Restored Image (R_I)	Forged Image (F_I)	Image Type	Evaluation Metrics		
					PSNR(In dB)	MSE	SSIM
				C_I, W_I	78.60	0.0896	1.00
				C_I, R_I	73.84	0.0027	0.99
				W_I, F_I	**33.59**	**28.42**	**0.97**
				C_I, F_I	**33.59**	**28.42**	**0.97**
				C_I, W_I	78.28	0.0965	1.00
				C_I, R_I	73.60	0.0028	0.99
				W_I, F_I	**44.72**	**2.19**	**0.99**
				C_I, F_I	**44.72**	**2.19**	**0.99**

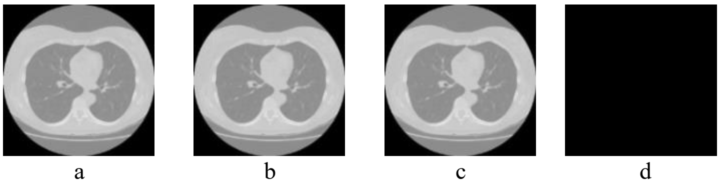


Figure 3. (a) Cover image, (b) Watermarked version of cover image with PSNR value 78.6 dB, (c) Restored image with PSNR value 73.84 dB, and (d) No numerical difference can be found out/identified between the host and recovered image

5. CONCLUSIONS

Medical data handling and sharing among professionals involve a combination of technical safeguards, organizational policies, and legal frameworks to ensure the confidentiality, integrity, and privacy of patient information while facilitating collaboration and quality patient care. The watermarking of medical images enhances their integrity and authenticity. There are also complicated ethical issues to address in relation to patient privacy, informed consent, data integrity, risk of misunderstanding, and regulatory compliance. Healthcare professionals must balance the potential benefits of watermarking against the requirement to safeguard patient privacy and ensure that medical data is handled ethically.

This paper introduces a content-based reversible watermarking system designed for verifying the authenticity of medical images. The system employs a GLCM texture descriptor to generate unique signatures based on the content of the images, which are then embedded into the LSBs of pixels in the original image. Later, these signatures can be extracted to confirm the integrity of the medical images. The effectiveness of the proposed method is evaluated using a dataset of 40 CT lung images. Experimental results demonstrate that the proposed watermarking scheme achieves high imperceptibility, effectively identifies unauthorized alterations, and can restore the original image content if it remains unaltered. One notable advantage of this scheme is its simplicity and cost-effectiveness. However, it is important to note some limitations, including its relatively low embedding capacity and its compatibility solely with DICOM images of dimensions 512×512.

While implementing a watermarking system for medical images entails significant upfront costs, the long-term benefits to healthcare providers include enhanced data integrity, improved regulatory compliance, efficiency gains, and ultimately, better patient care outcomes.

REFERENCES

[1] Guo, X., Zhuang, T.G. (2009). A region-based lossless watermarking scheme for enhancing security of medical data. Journal of Digital Imaging, 22: 53-64. https://doi.org/10.1007/s10278-007-9043-6

[2] Liu, X., Lou, J., Fang, H., Chen, Y., Ouyang, P., Wang, Y., Wang, L. (2019). A novel robust reversible watermarking scheme for protecting authenticity and integrity of medical images. IEEE Access, 7: 76580-76598. https://doi.org/10.1109/ACCESS.2019.2921894

[3] Zain, J.M., Fauzi, A.R. (2006). Medical image watermarking with tamper detection and recovery. In 2006 International Conference of the IEEE Engineering in Medicine and Biology Society, New York, NY, USA, pp. 3270-3273. https://doi.org/10.1109/IEMBS.2006.260767

[4] Zain, J.M., Fauzi, A.R. (2007). Evaluation of medical image watermarking with tamper detection and recovery (AW-TDR). In 2007 29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Lyon, France, pp. 5661-5664. https://doi.org/10.1109/IEMBS.2007.4353631

[5] Al-Qershi, O.M., Khoo, B.E. (2009). Authentication and data hiding using a reversible ROI-based watermarking scheme for DICOM images. Journal of Digital Imaging, 24: 114-125. https://doi.org/10.1007/s10278-009-9253-1

[6] Al-Qershi, O.M., Khoo, B.E. (2010). ROI-based tamper detection and recovery for medical images using reversible watermarking technique. In 2010 IEEE International Conference on Information Theory and Information Security, Beijing, China, pp. 151-155. https://doi.org/10.1109/ICITIS.2010.5688743

[7] Al-Qershi, O.M., Khoo, B.E. (2011). High capacity data hiding schemes for medical images based on difference expansion. Journal of Systems and Software, 84(1): 105-112. https://doi.org/10.1016/j.jss.2010.08.055

[8] Tan, C.K., Ng, J.C., Xu, X., Poh, C.L., Guan, Y.L., Sheah, K. (2011). Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability. Journal of Digital Imaging, 24: 528-540. https://doi.org/10.1007/s10278-010-9295-4

[9] Das, S., Kundu, M.K. (2013). Effective management of medical information through ROI-lossless fragile image watermarking technique. Computer Methods and Programs in Biomedicine, 111(3): 662-675. https://doi.org/10.1016/j.cmpb.2013.05.027

[10] Shehab, A., Elhoseny, M., Muhammad, K., Sangaiah, A. K., Yang, P., Huang, H., Hou, G. (2018). Secure and robust fragile watermarking scheme for medical images. IEEE Access, 6: 10269-10278. https://doi.org/10.1109/ACCESS.2018.2799240

[11] Qasim, A.F., Aspin, R., Meziane, F., Hogg, P. (2019). ROI-based reversible watermarking scheme for ensuring the integrity and authenticity of DICOM MR images. Multimedia Tools and Applications, 78: 16433-16463. https://doi.org/10.1007/s11042-018-7029-7

[12] Naseem, M.T., Qureshi, I.M., Cheema, T.A., Rahman, A. (2013). Hash based medical image authentication and recovery using chaos and residue number system. Journal of Basic and Applied Scientific Research, 3(6): 488-495.

[13] Eswaraiah, R., Reddy, E.S. (2014). Medical image watermarking technique for accurate tamper detection in ROI and exact recovery of ROI. International Journal of Telemedicine and Applications, 2014: 1-10. https://doi.org/10.1155/2014/984646

[14] Woo, C.S., Du, J., Pham, B. (2005). Multiple watermark method for privacy control and tamper detection in medical images. In Workshop Proceedings: WDIC 2005 APRS Workshop on Digital Image Computing, pp. 43-48.

[15] Wu, J.H., Chang, R.F., Chen, C.J., Wang, C.L., Kuo, T.H., Moon, W.K., Chen, D.R. (2008). Tamper detection and recovery for medical images using near-lossless information hiding technique. Journal of Digital Imaging, 21: 59-76. https://doi.org/10.1007/s10278-007-9011-1

[16] Arsalan, M., Malik, S.A., Khan, A. (2012). Intelligent reversible watermarking in integer wavelet domain for medical images. Journal of Systems and Software, 85(4): 883-894. https://doi.org/10.1016/j.jss.2011.11.005

[17] Gadhiya, T.D., Roy, A.K., Mitra, S.K., Mall, V. (2017). Use of discrete wavelet transform method for detection and localization of tampering in a digital medical image. In 2017 IEEE Region 10 Symposium (TENSYMP), Cochin, India, pp. 1-5. https://doi.org/10.1109/TENCONSpring.2017.8070082

[18] Swaraja, K., Meenakshi, K., Kora, P. (2020). An optimized blind dual medical image watermarking framework for tamper localization and content authentication in secured telemedicine. Biomedical Signal Processing and Control, 55: 101665. https://doi.org/10.1016/j.bspc.2019.101665

[19] Nazari, M., Mehrabian, M. (2021). A novel chaotic IWT-LSB blind watermarking approach with flexible capacity for secure transmission of authenticated medical images. Multimedia Tools and Applications, 80(7): 10615-10655. https://doi.org/10.1007/s11042-020-10032-2

[20] Sayah, M.M., Redouane, K.M., Amine, K. (2022). Secure transmission and integrity verification for color medical images in telemedicine applications. Multimedia Tools and Applications, 81(30): 43613-43638. https://doi.org/10.1007/s11042-021-11791-2

[21] Pal, P., Chowdhuri, P., Si, T. (2023). A novel watermarking scheme for medical image using support vector machine and lifting wavelet transform. Multimedia Tools and Applications, 82(26): 41187-41206. https://doi.org/10.1007/s11042-023-15144-z

[22] Haralick, R.M., Shanmugam, K., Dinstein, I.H. (1973). Textural features for image classification. IEEE Transactions on Systems, Man, and Cybernetics, SMC-3(6): 610-621. https://doi.org/10.1109/TSMC.1973.4309314

[23] Mirsky, Y., Mahler, T., Shelef, I., Elovici, Y. (2019). CT-GAN: Malicious tampering of 3d medical imagery using deep learning. In 28th USENIX Security Symposium (USENIX Security 19), Santa Clara, CA, USA, pp. 461-478.