Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 47 (2026), No. 6, pp. 2223–2244
DOI : 10.47974/JIOS-2119

A novel reversible digital image watermarking algorithm to protect medical image and patient record authenticity

Prasanta Kumar Sahoo *
School of Computer Sciences
Odisha University of Technology and Research
Bhubaneswar 751029
Odisha
India

and

Department of Computer Application
Siksha 'O' Anusandhan (Deemed to be University)
Bhubaneswar 751030
Odisha
India

Debasis Gountia †
Ranjan Kumar Dash §
School of Computer Sciences
Odisha University of Technology and Research
Bhubaneswar 751029
Odisha
India

Abstract

Due to the growing quantity of medical images, the patient data recognition is the important one for treatment clinical institutions. So, digital image watermarking has widespread importance at the time of sharing of medical images among treatment clinical institutions. But in watermarking the extraction of the patient data and preserving image quality are the major important factors, after sharing of medical images. In this paper, a

* *E-mail:* **mrprasantasahoo@gmail.com; (Corresponding Author)**
prasantasahoo@soa.ac.in
† *E-mail:* **dgountia@outr.ac.in**
§ *E-mail:* **rkdash@outr.ac.in**

novel spatial domain-based reversible digital image watermarking scheme proposed on medical images to ensure authenticity, integrity, and confidentiality. In this scheme, the input ground truth image (or cover image) is divided into 4 X 4 block sizes. The watermark image is embedded with the original ground truth image by performing L-level Quantization. The watermark image is quick response (QR) code of patient information. The compression applied to the remainder part of the cover ground truth image using the mean arithmetic method to make the process most robust. The reversible watermarking scheme applied over watermarked images by performing inverse L-level Quantization and decompression. The proposed scheme is compared with Reza et al. existing scheme: "An Image Watermarking Algorithm for Medical Computerized Tomography Images". The proposed scheme has better experimental results compared to the existing scheme in terms of Peak Signal-to-noise ratio (PSNR), Mean Square Error (MSE), and Structural Similarity Index (SSIM). The PSNR, MSE, and SSIM metrics are used to evaluate the robustness of the proposed scheme for extracting cover images and QR code of patient information (in terms of watermark images) from watermarked images. In addition, the Similarity (SIM) and the correlation coefficient (CRC) are used to evaluate how well the suggested approach for patient data and cover ground truth medical image extraction holds up robustness. The experimental numerical values of metrics achieved in the proposed scheme have better performance for compression and decompression watermarking medical images.

Subject Classification: *08A70, 68P30, 54H30.*

Keywords: *Medical image, Watermarking, Reversible watermarking, Spatial domain, Scalar quantization, Compression, Decompression, QR code.*

1. Introductıon

Digital medical images can now be exchanged globally for telemedicine, tele rdiology, telediagnosis, and teleconsultation services due to the widespread adoption of the internet and electronic medical record management. The importance of effectively sharing patient data among specialists in different hospitals is underscored by the significant societal and economic benefits of early diagnosis and understanding of diseases, as well as the reduction of misdiagnoses. A primary objective in managing medical imaging is to safeguard patient records from unauthorized manipulation. Therefore, establishing a standard method to ensure the integrity and validity of medical images is a critical aim of the current electronic medical system: Kuang, Zhang, and Han [1].

Consequently, using digital watermarking is one way to address the aforementioned problem. Put differently, watermarking can improve the security of medical images by discreetly adding unique information, sometimes known as hidden data or a watermark, to the image. Typically, watermark data is added to the host image's pixel value in a binary format. Afterward, this data can be accessed to verify if the medical image is distributed from the real source (authenticity) or if the patient is the right one (integrity): Sahoo, Nanda, and Jahangeer [2], Bhatnagar and Jonathan [3], Pan et al. [4], Zain and Clarke [5], Wu and Hwang [6].

The watermark data is directly inserted in the host or cover image's pixel value in the spatial domain. These techniques offer a great capacity for watermark embedding while being quick and easy to use. While spatial domain approaches have the potential to overcome cropping attacks and offer certain advantages, their primary vulnerability to noise or lossy compression attacks remains. Furthermore, embedded watermarks are easily modifiable by a third party once they find out the technique: Wu and Hwang [6], Heylena and Dams [7]. But, the watermarked image is obtained in the transform domain by applying the watermark to the original image after it has been transformed: Mohanty, Ramakrishnan, and kankanhalli [8]. The sections that follow include a description of some of these transformations as well as an analysis of their advantages and disadvantages.

Watermarking techniques can be classified as visible or invisible based on how humans perceive them. Logos are a common example of visible approaches; they are used to protect content or copyright and are placed in the corners of image or videos. However, applications like copyright protection, integrity verification, and identification can benefit from the usage of invisible watermarks. It is occasionally possible to utilize both visible and invisible watermarking at the same time, which is called as dual watermarking method: Sahoo et al. [9]. So, the invisible watermark in this instance might be thought of as a fallback for the visible one.

There are four categories of invisible watermarking techniques exist: robust, hybrid, fragile, and semi-fragile: Gaikwad, Gowda, and Athavale [10], Jabade and Gengaje [11]. The watermark is quickly destroyed by even the smallest adjustments because of its easy approach. This type of watermarking is only useful for integrity checking and authentication. Although the semi-fragile approach is robust against unintentional attacks, it's still vulnerable to malicious ones. The powerful watermarking technique, which is typically employed to safeguard copyright, needs to be impervious to numerous types of attacks. By using various attacks on the watermarked images and comparing the embedded and extracted watermarks using various benchmarks, the strength of these techniques may be evaluated. Ultimately, hybrid watermarking combines a variety of strong and weak methods to offer concurrent copyright protection, integrity verification, and authentication: Memon and Gilani [12].

Apart from the aforementioned classifications, another crucial element in watermarking is reversibility, which is often referred to as lossless or invertible watermarking. Reversible data concealing, in contrast to typical watermarking systems, precisely restores both the watermark and the original multimedia, an essential need for military and medical applications. Reversible techniques are characterized primarily by their capacity to restore the original image in its original form without distortion following the extraction of watermark segments, in addition to provide identification and tamper proofing. Medical officers can precisely recover both the concealed information and the image itself by integrating patient information and diagnostic data into the medical image using a reversible data hiding technique. Numerous researchers have put out several numbers of reversible watermarking techniques. Reversible watermarking

systems have often been evaluated using a variety of criteria, such as perceptual, distortion-free cover data, PSNR, and watermark embedding capacity: Kaur and Kaur [13].

Reversible watermarking is a form of image restoration because it allows the exact recovery of both the original image and the hidden image, resulting in a watermarked image. This feature specifically designates a unique data-hiding technique that reverses all modifications made during the embedding process. These processes encompass three distinct stages of conceptualization.

i. *Embedding process:*

The watermark, i.e., secret information about patient data in medical images, is embedded into the cover image by modifying pixel values or transforming coefficients. To ensure reversibility, the modified pixel values or compressed original data are also embedded.

ii. *Extraction or Verification:*

At the receiver's side, the watermark is extracted using the reverse process of the embedded algorithm. The extracted watermarked image is used for verification of authentication or tamper detection.

iii. *Restoration:*

The original cover image was perfectly reconstructed by reversing the specific process or extracting auxiliary data. The extracted data is an identical bit-by-bit copy of the cover image, which remains free from any degradation.

1.1 *A Data Security System Overview*

The concepts of steganography and cryptography are strongly linked to watermarking. These topics are included in the category of data security systems. A secure communication can be sent using cryptography, which only an authorized recipient can decode and read. We refer to this as a "secret writing." The primary drawback of cryptography approaches when compared to watermarking is that, although an encrypted message may be safeguarded during transmission, it loses its protection once it is decrypted. Moreover, the majority of cryptographic techniques are complicated and offer only poor copyright protection.

The Greek words "steganos" and "graphei," which translate to "covered" and "writing," respectively, are the origin of the word steganography. Although steganography and watermarking share certain similarities, they also differ in a few ways, as will be discussed below:

- The objective of steganography is to embed a secret message that is unrelated to the cover work, while the objective of watermarking is to establish a connection between the embedded information and the cover work.

- The embedded information in watermarking can be either visible or invisible. In contrast, steganography is designed so that the message remains invisible.
- The main goal of watermarking is to embed data within cover data in a manner that makes it difficult for an attacker to remove or replace it. In contrast, the primary aim of steganography is to hide the message so that it goes undetected by any intruder.

These benefits and drawbacks lead one to the conclusion that watermarking is the best option for maintaining a digital image's security. As an additional degree of security, the data can also be encrypted prior to the watermark being embedded.

1.2 *The Different Components of A Standard Watermarking System.*

The process of adding information i.e. a watermark on a host image so that authorized users may identify the watermark image or data and use it to verify the authenticity of the object is known as digital watermarking . The watermark can be any sort of image, logo, serial number, owner's ID, name, or other information that proves ownership of the host signal, whereas the host signal can be any kind of image, audio, video, or 3D mesh. Normally, these characteristics are first transformed into a binary sequence and then included in the host signal. The usual protocol for the watermarking process is as follows. A brief explanation of each component is provided, and Figure 1 depicts a typical watermarking system.

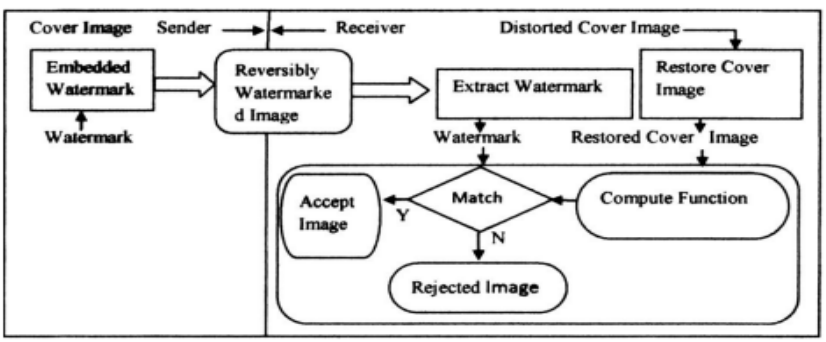

Figure 1
Architecture of Typical Water marking System

The remaining sections of this work are structured as follows: Section 2 evaluates the fundamental aspects of various domain knowledge pertaining to reversible digital image watermarking, including a review of previously published methodologies. Section 3 addresses the significant facts, highlighted gaps, and proposed methods. Section 4 delineates the design and implementation of algorithms. Section 5 looks at the discussion of results pertaining to the

proposed model, while Section 6 finishes with observations and recommendations for future activities regarding the model.

2. Revıew of Exıstıng Methodology

Many studies have proposed and refined watermarking and reverse watermarking methods for medical images. This includes medical image watermarking. Zain et al. proposed spatial domain watermarking for ultrasound (US) DICOM pictures: Zain and Clarke [14]. Their plan has four steps. Starting with a rectangle shape, the ROI is extracted from the noninterest zone. Next, the hash function calculates the image's hash value. Finally, RONI's least significant bits include the hash value. For DICOM pictures, suggested a hybrid ROI-based watermarking method for authentication and data concealing: Al-Qershi and Khoo [15]. Their method separates the cover DICOM image ROI and RONI regions. Next, ROI regions are embedded with patient data using a reversible difference expansion approach. Tamper detection and recovery data are integrated into RONI regions using a reliable DWT transform approach. The RONI regions: Movahed, Rezaeian, and Ghasemi [16] models feature a patient data and authentication watermark. SVD decomposition and the DWT transform (DWT-SVD) comprise their embedding method.

On the other hand, the reversible watermarking scheme discusses the many methods currently in use for data extraction from embedded media and data concealment.

No earlier example of reversible data embedding was found than the 1994 Barton patent. His method compresses a bit string inside a data block and adds overplayed bits. The original image can be recovered without loss by rebuilding the payload from an embedded image and subtracting it: Honsinger et al. [17]. creating a large-capacity, reversible data-embedding method using embedded message status on pixels. Two reversible methods for data-embedding JPEG lossy image formats: Fridrich and Goljan [18] and theoretical capacity limits based on lossless data compression: Perry, MacIntosh, and Cushman [20] and a viable code architecture: Kalker and Willems [19] are also provided. quantization residue compression data-embedding that is reversible, high-capability, and low-distortion: Celik et al. [21].

Many reversible watermarking methods have been introduced recently. All of them extract sections of an image block to apply the watermark by lossless compressing them. A difference expansion: Tian [22], this technique identifies expandable coefficients, which are subsequently given an extra bit. Haar wavelet transform method: Wakekar et al. [23], Tian [24], this method creates an unidentifiable watermarked image with faultless recovery. Watermark bits are included in a vector of pixels using the difference expansion of an extended integer wavelet transform: Alattar [25], this method has low embedding capacity.

Reversible watermarking is a unique type of digital watermarking that has gained a lot of attention in recent years. By adding the designated watermark to the original image, it not only offers copyright protection, but it also has the

ability to extract the original from the allegedly tampered with image. Through a comparison between the assigned and retrieved watermarks, ownership can be ascertained. Reversible watermarking methods, like conventional ones, must be resilient to both purposeful and inadvertent attacks. They also need to be undetectable to prevent attacks and value loss. Consequently, all requirements of conventional watermarking, including robustness, imperceptibility, and ease of embedding and retrieval, must also be met by reversible watermarking: Mallat [26].

Additionally, the associated work is separated into three categories, which are domains that are spatial, encrypted and compressed.

2.1 *Spatıal Domaın*

Tian [27] presented a technique that modifies pixel pairs based on their differences to incorporate hidden data bits. A threshold value is used to calculate the embedding capacity. Issues with overflow and underflow could arise during the embedding step. Alattar [28] introduced a method for embedding reversible features through the difference expansion of quads, that achieves minimal image distortion. Triplets of bits are concealed by this approach in the difference expansion of quads of nearby pixels. The outcomes demonstrate that, in terms of embedding capacity, it performs better than Tian [27] approach. An approach utilizing reduced difference expansion in the spatial domain and a multiple-layer data hiding strategy was developed by Lou, Hu, and Liu [29]. In order to lower the difference expansion's value, they also devised the transformation function approach. This could result in the modified difference expansion's value being quite similar to the cover image. Additionally, at the same level of image quality, their method offers more embedding capacity than Tian's difference expansion method. Fallahpour, Megias, and Ghanbar [30] shifting histogram-based algorithm was developed. This method involves the author first dividing the image into separate tiles, after which their histogram is moved between the frequency's maximum and minimum ranges. Subsequently, the writer integrated the information at the pixel level with the highest frequency. The author improved the quality of the images and the data hiding capacity by employing this method.

2.2 *Encrypted Domaın*

To address the issue of tamper detection and localization, checksum bits are generated. They embedded EPR, checksum, and watermark data using intermediate significant bit substitution (ISBS). For block-encrypted images, an alternative approach that works was provided by Tai, Yeh, and Chang [31]. The original image is encrypted by the sender using the encryption key and block cipher technique before data is sent to a remote server. Histogram shifting and difference expansion are two techniques that Puech, Chaumont, and Strauss [32] suggested be used in order to extract the original image and biomedical information. The open key of the Pascalier cryptosystem algorithm encodes each pixel. The image in the encrypted domain's histogram is expanded via

homomorphic multiplication. In the encrypted domain, the histogram is shifted based on the difference between neighbouring pixels and homomorphic addition. The message is incorporated into the pixel differences of the host image. On the receiving end, the recipient uses his private key to decrypt the encrypted image containing extra data. In order to conceal sensitive information, Rani and Lakshmanan [33] proposed a system that precisely employs the four least significant portions of the original image. Before the embedding operation, the cover image is scrambled using a mapping technique known as logistic mapping. A block-based matching technique was presented by Aydogan and Bayilms [34] and is used to include diagnosis-related data. The author presented eight distinct scanning orders, six of which are newly designed, and it will also aid in enhancing the image quality.

2.3 *Compressed Domaın*

An approach based on spatial additive watermarking was presented by Wu et al. [35]. It is further integrated with the modulo-addition method. Authenticity and image protection are provided by the aforementioned technique. The aforementioned strategy only took into account one square region of interest (ROI). In this study, Rani and Lakshmanan [36] introduces a run length encoding (RLE) compression method. Phase one of the algorithm, when data is to be hidden, is split into three parts. The second phase involves compressing the image, and the third phase involves decompressing the image to get the secret data. A strategy based on bipolar multiple-base conversion was presented by Chao, Hsu, and Miaou [37]. It permits many forms of electronic patient record (EPR) data to be concealed under one mark. In essence, the aforementioned method offers integration, security, privacy, validation, processing time complexity, and key change frequency. A run length encoding technique was presented by Rani and Lakshmanan [33] to compress the medical image. There are three stages to this procedure. The first involves hiding text data within the medical image. The stego images are compressed in the second step, and the hidden data is extracted in the third phase through decompression. A JPEG bit stream encryption technique was presented by Chang, Lu, and Wu [38]. He developed a technique called "reserving room before encryption," wherein the cover JPEG bit-stream is intended to be slightly distorted in order to create enough reserve space for further data embedding before the modified JPEG is intended for encryption: Adnam et al. [39].

3. Problem Statement

Though still in the early stages of development, reversible watermarking schemes offer enormous potential. Reversible watermarking is especially well suited for uses requiring high-quality images, like military and medical applications. To increase robustness, more useful spatial techniques like reversible watermarking are applied. Reversible watermarking is a method for performing distortion-free watermarking. The patient data in this paper has been transformed to Quick Response (QR) code in our proposed model. Any portion of the cover image can be embedded with the QR code, which is used as a

watermark image. This paper uses L-level scalar quantization in the Compress domain of the reverse watermarking paradigm. Using the algebraic mean Compression method, L-level scalar quantization is used for image embedding and compression. The original cover image and patient data in the form of a QR code have been extracted by applying reverse L-level scalar quantization to the watermarked image after it is decompressed.

4. Proposed Methodlogy

A revised and suggested framework developed for reversible digital image watermarking in the spatial domain. This method divides the input image into 4X4 blocks. Watermarks and other images can be included in a cover image using L-level Scalar Quantization technique. Compressed the remaining portion of the ground truth image by applying the mean algebraic method to strengthen the covered ground truth image.

The proposed model includes an appropriate algorithm for watermarking digital images in a reversible manner using the JPEG 2000 compression standard. The sub-modules of the reversible watermarking architecture were identified, and the design requirements for reversible watermarking are established. Using MATLAB and JAVA programming, a software reference model for reversible watermarking sub-modules is created based on the stated architecture and algorithm. The simulation of the reversible watermarking top module yields the desired results. Following diagram shows the execution flow process of sub-module for proposed reversible digital image watermarking: Sahoo and Nanda [40], Sahoo et al. [41].

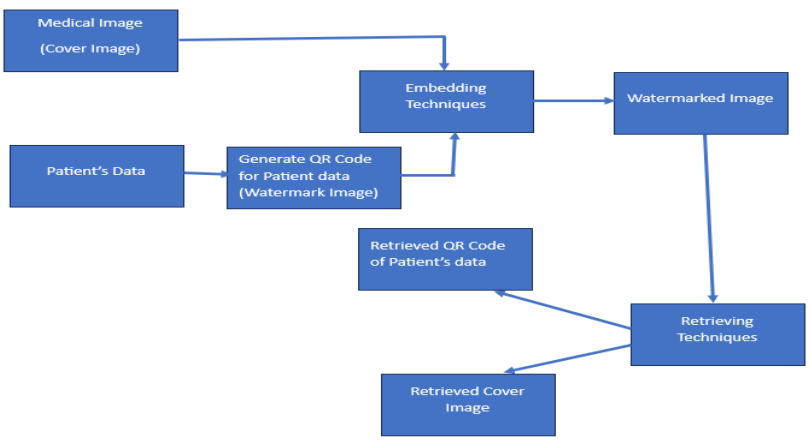

Figure 2
Execution flow diagram of Proposed Reversible Digital Image Watermarking Model.

Figure 2 displays the execution flow diagram of the proposed methodology. In Figure 2, the cover image represents the original ground truth

image. The patient's name, age, disease name, and department are converted into a QR code. The QR code behaves as a watermark. The watermark is embedded with the cover image using the algebraic mean compression (AMC) algorithm to form the watermarked image. The AMC algorithm has been applied in reverse to retrieve the watermark and cover image. The retrieved watermark image and cover image have been compared with the original watermark image and cover image for calculation of the performance of the proposed model in terms of performance matrices MSE, PSNR, SSIM, CRC, etc.

4.1 *Proposed Method Algorıthms*

The proposed method consists of two algorithms. The algorithm-1 is the conversion of Patient's data into QR code and the algorithm-2 is the embedding QR code to the cover image in order to form watermarked image and retrieval of QR code and cover image from watermarked image for ownership identification. What follows is a detailed explanation of both stages of the suggested procedure, is given below.

Algorithm 1: QR code Generation

1. Store patient's details i.e. Patient Name, Department, Gender and Age in a .txt file.
2. Create object(s) for following classes

   File fin1=new File("data.txt");

   FileReader fr1=new FileReader(fin1);

   BufferedReader br1=new BufferedReader(fr1);

   String str1;
3. Convert .txt file to .png image file

   while((str=br1.readLine())!=null)

   {

   String data[]=str.split("\t");

   String qrdata="Department: "+data[0]+"\n"+" Patient Name: "+data [1]]+"\n"+"Gender: "+data [2];+"\n"+"Age: "+data [3];

   String path = data[0]+"_QR.png";

   String charset = "UTF-8"; //Encoding charset to be used

   Map<Encode_HintType, Error_Correction_Level> hashMap = new Hash_Map<Encode_HintType, Error_Correction_Level>();

   hashMap.put(Encode_HintType.ERROR_CORRECTION, Error_Correction_Level.);

generate_QRcode(qrdata, path, charset, hash_Map, 200, 200);//increase or decrease height and width accordingly

System.out.println(data[0]+"_QR Code created successfully."); //prints if the QR code is generated

}

4. Invoke fr.close(); method to close all classes.

Diagrammatical Representation of Proposed Method Algorithm 1:

Figure 3
QR code Generation Output

Figure 3 shows the generation of Quick Response (QR) Code of patient data. The QR code is the image file form of patient information text file.

Algorithm 2: Embedding Process

Embedding Process:

1. Get the grayscale ground truth cover image $c(i,j)$and use it as input.
2. Make 4 X 4 blocks of equal sections out of the entire cover image $c(i,j)$.
3. Calculate the quotient matrix $Q_L(x)$ and remainder matrix $R_L(x)$for each pixel in terms of a 4×4 matrix by applying L-level scalar quantization to each pixel value x. For these, the formula is as follows:

$$Q_L(x) = \lfloor x/L \rfloor \; and \; R_L(x) = x\%L$$

4. Apply compression to the remainder matrix $R_L(x)$. Carrying out an algebraic mean operation on neighbouring elements of each column with respect to the floor function gets the matrix into the 3×4 dimension. For these, the formula is as follows:

$R_{comp}(x) = \lfloor (x+y)/2 \rfloor, where\ (x,y)$

$are\ the\ adjucent\ pixel\ belongs\ to\ same\ column\ C_i$

5. To reform 4 × 4 matrix from 3 × 4 matrix, embed QR code as watermark in $R_{comp}(x)$ matrix. The reformed 4 × 4 matrix say $R_{embd}(x)$.

6. Perform reversely L-level Scalar quantization to obtained watermarked image $w(i,j)$ over quotient matrix $Q_L(x)$, L-level Scalar Quantization L and embedded matrix $R_{embd}(x)$. For these the formula is as follows:

$$w(i,j) = L \times Q_L(x) + R_{embd}(x)$$

Diagrammatical Representation of Proposed Method Algorithm 2:

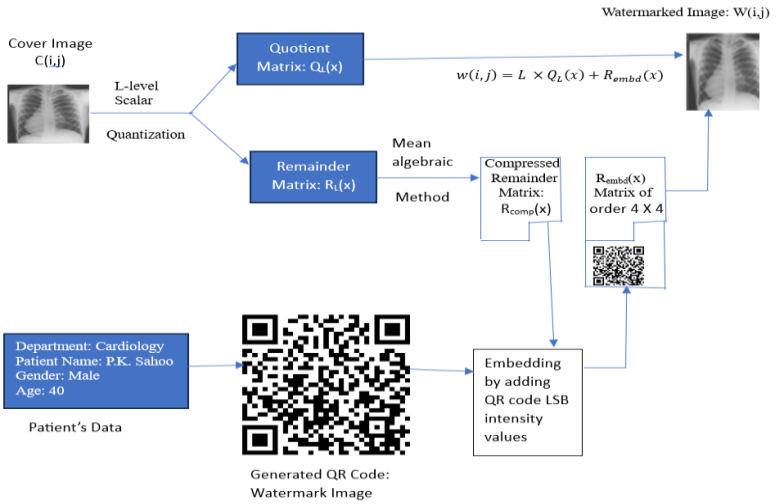

Figure 4
Embedding Process Diagram

Figure 4 shows embedding process of watermark image with ground truth cover image, in order to produce watermarked image.

Algorithm 3: Retrieving process

1. Consider Watermarked image $w(i,j)$ which was obtained from the embedding procedure, and utilize it as the input.
2. Calculate the quotient matrix $Q_{Lr}(x)$ and remainder matrix $R_{Lr}(x)$for each pixel in terms of a 4×4 matrix by applying L-level scalar quantization to each pixel value x of watermarked image $w(i,j)$. For these, the formula is as follows:

$$Q_{Lr}(x) = \lfloor x/L \rfloor \; and \; R_{Lr}(x) = x\%L$$

3. To extract QR code or reverse watermark image$w_r(i,j)$ and from $R_{Lr}(x)$, decompress the $R_{Lr}(x)$. For these, the formula is as follows:

$R_{Dcomp}(x) = \lfloor (x+y)/2 \rfloor, where\ (x,y)$
$are\ the\ adjucent\ pixel\ belongs\ to\ same\ column\ C_i$
of w(i, j). and $w_r(i,j) = \sum_{i=0}^{L-1} L^i \times R_{Lr}(x)$, here $R_{Lr}(x)$ is a matrix of order 1×4

4. To extract reverse cover image $c_r(i,j)$ perform the process as $c_r(i,j) = L \times Q_{Lr}(x) + R_{Dcomp}(x)$

Diagrammatical Representation of Proposed Method Algorithm 3:

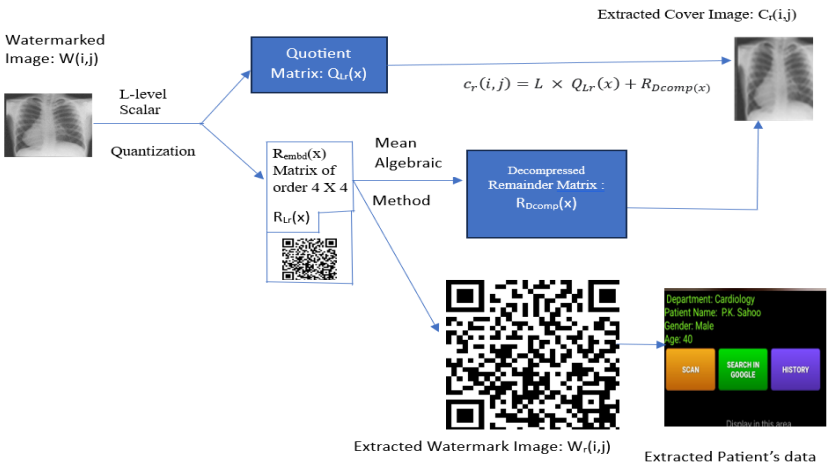

Figure 5
Extracting Process Diagram

Figure 5 shows the extracting process of watermark image and ground truth cover image from watermarked image.

Algorithm 4: Generation of $R_{embd}(x)$ matrix

The process of creating a 4 × 4 $R_{embd}(x)$ matrix from a 3 × 4 $R_{comp}(x)$ matrix using the List Significant Bit (LSB) filtration method is as follows.

Augmented process:

1. Read the cover image $w(i,j)$ having size M × N and resize it into 256 ×256 pixels.
2. calculate height and width of the watermark image w(i, j) as height=size (M, 1) and width=size (N, 2).
3. Count the number of embedded bits as follows and initialize embed_count=1, length= M × N.

   for← i=1 to height

   for ← j=1 to width

   if (embed_count <= length)

   LSB= mod$(w(i,j), 2)$;

   temp= LSB ⊕ embed_count;

   $R_{embd}(x) \leftarrow R_{comp}(x)$+ temp;

   embed_count++;

   end

end
end

Diagrammatical Representation of Proposed Method Algorithm 4:

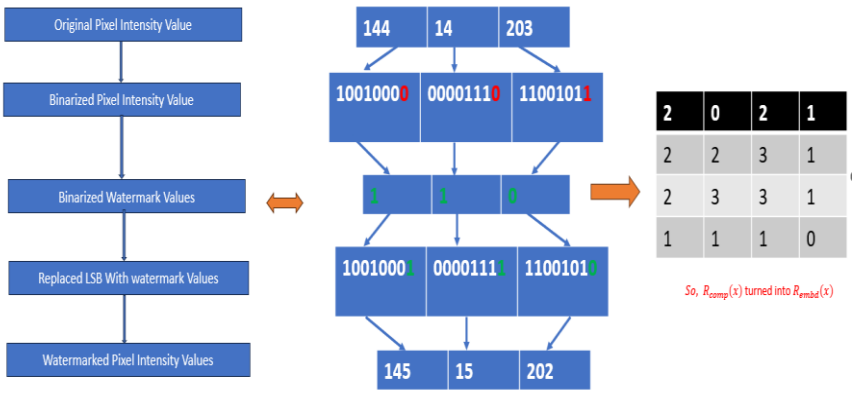

Figure 6
Augmented Process Diagram

Figure 6 shows the derivation of 4 × 4 $R_{embd}(x)$ matrix from a 3 × 4 $R_{comp}(x)$ matrix.

5. Dataset And Implementation Details

Validation and testing of the proposed method are carried out with the help of CT medical images obtained from the MURAV1.1 dataset of Stanford University Medical School, California, USA. Eighty images are included in it. They are obtained from many parts of the human body, such as the brain, chest, and the pelvic region. There are different images having different pixels, out of them we have taken only 128×128 pixels images that make up the resolution of the selected image. Every image contains a patient's data that conveys the patient's admitted department, name, gender, and age: Sahoo, Gountia, and Dash [42], Batra, Narwal, and Mohapatra [43].

The suggested approach and its related simulations are conducted using a Desktop equipped with an Intel(R) Core (TM) i3-10110U CPU @ 2.10GHz 2.50 GHz and 8 GB of RAM. All experiments and techniques are carried by using the MATLAB R2020a program and java programming languages.

5.1 *Performance Metrics*

This study evaluates the efficacy of the proposed methodology using two categories of evaluation criteria. The first set of metrics includes SSIM, PSNR, and MSE, which evaluate the picture watermark's imperceptibility. The following formulas can be used to calculate Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR):

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [C(i,j) - W(i,j)]^2 \quad (1)$$

and

$$PSNR = 10 \times log_{10} \left(\frac{MAX_I^2}{MSE} \right)$$
$$= 20 \times log_{10} \left(\frac{MAX_I}{\sqrt{MSE}} \right)$$
$$= 20 \times log_{10}(MAX_I) - 10 \times log_{10}(MSE) \quad (2)$$

Here,
$C(i,j) =$ Is the Original ground truth Cover image
$W(i,j) =$ Is the processing (or embedding) watermarked image
$M \times N =$ Is the size of the image having M-rows and N-columns.

As a measure of how similar two images are to one another, the Structural Similarity Index (SSIM) metric is defined as follows:

$$SSIM(C,W) = \frac{(2\mu_c\mu_w + c_1)(2\sigma_{c,w} + c_2)}{(\mu_c^2 + \mu_w^2 + c_1)(\sigma_c^2 + \sigma_w^2 + c_2)} \quad (3)$$
$$\begin{cases} c_1 = (k_1 L)^2 \; k_1 = 0.01 \\ c_2 = (k_2 L)^2 \; k_2 = 0.03 \end{cases}$$

Here,
μ_c=Mean intensity values of cover image $C(i,j)$
μ_w= Mean intensity values of embedding watermarked image $W(i,j)$
σ_c=Variance in intensity values of cover image $C(i,j)$
σ_w= Variance in intensity values of embedding watermarked image $W(i,j)$
$\sigma_{c,w}$=covariance in intensity values between $C(i,j)$ and $W(i,j)$
L=L-level Quantization and is defined as
$L = 2^n - 1, where\ n\ is\ the\ number\ of\ bits\ per\ pixel$

c_1 and c_2 are two variables used for calming the division with denominator.

The watermarking scheme's robustness is evaluated in the second set. In simpler terms, these measures assess how well the extracted image matches the original watermark image as well as original cover image. Specifically, CRC and SIM are the following metrics that make up this group:

$$CRC = \frac{\sum_i \sum_j w(i,j) w_r(i,j)}{\sqrt{\sum_i \sum_j w(i,j)^2 \times \sum_i \sum_j w_r(i,j)^2}} \quad (4)$$

and

$$SIM = \frac{\sum_i \sum_j w(i,j) w_r(i,j)}{\sum_i \sum_j w_r(i,j)^2} \quad (5)$$

Here, w(i,j)= Is the watermark image and
w_r(i,j)=Is the extracted watermark image

5.2 *Experimental Result Analysis and Discussion*

In this section, the experimental results of proposed methods are discussed. The input images for proposed methods are CT medical images of sizes 512 X 512 pixels, 256 X 256 pixels and 128 X 128 pixels. But for performance analysis comparison of proposed model with traditional models like Singular Value Decomposition (SVD) based method, Discrete Wavelet Transform (DWT) based method, and Reza et al. existing watermark scheme, the input images are taken 128 X 128 pixels CT images are only used. The numerical results are shown in following tables: Noruzi et al. [44], Zouilekh and Bouroubi [45].

Table 1

Performance metrics numerical results comparisons between Proposed scheme and Existing Reza et al. schemes & other traditional watermarking Schemes.

Srl. No.	Metrices / Approaches	MSE	PSNR (dB)	SSIM (Mean ±Std)
1	Proposed Scheme	0.022	58.871 dB	1.5 ± 0.045
2	Reza et al. Scheme	0.035	55.46 dB	0.93 ± 0.04
3	SVD Scheme	1.40	53.51 dB	0.84 ± 0.10
4	DWT Scheme	5.56	30.67 dB	0.58 ± 0.26
5	SVD-DWT Scheme	20.49	41.28 dB	0.71 ± 0.24

Table 1 simulation results show the proposed scheme has a lower MSE value and higher PSNR and SSIM (in mean and standard deviation) values compared to Reza et al. scheme and other traditional watermark schemes as mentioned in the Table 2.

Table 2

Performance metrics numerical results of extracted image and original watermark image comparisons between Proposed scheme and Existing Reza et al. schemes & other traditional Schemes

Srl. No.	Metrices / Approaches	CRC (Mean ±Std)	SIM (Mean ±Std)
1	Proposed Scheme	0.9781 ± 0.001	0.999 ± 0.002
2	Reza et al. Scheme	0.9982 ± 0.001	0.9989 ± 0.001
3	SVD Scheme	0.9701 ± 0.002	0.9814 ± 0.003
4	DWT Scheme	0.9458 ± 0.001	0.9672 ± 0.001
5	SVD-DWT Scheme	0.9852 ± 0.001	0.9952 ± 0.001

The simulation results in Table 2. indicate that the CRC value of the proposed scheme is very close to that of Reza et al. scheme, while the SIM value of the proposed scheme is higher than both Reza et al. scheme and other traditional watermarking schemes. Therefore the proposed method has better performance in similarity accuracy to preserve the originality of the image.

5.2 *Graphical Representation*

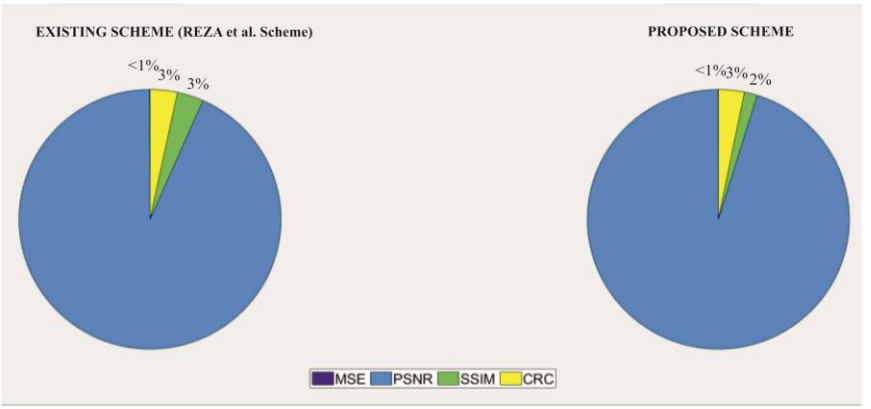

Figure 7
Pie Chart represantation on Performance Metrices MSE, PSNR, SSIM & CRC between Existing Scheme and Psoposed Scheme

Figure 7 shows graphical representation of performance metrices such as Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Structural Similarity (SSIM) and Corelation Coefficients (CRC) between Existing Reza et al. Scheme and Proposed Scheme. From This representation we observed that PSNR value (95% dB) of proposed scheme is better than PSNR value of Existing Scheme (93% dB). Better PSNR value has better clarity in visual quality, although the existing scheme has better CRC value than proposed scheme.

6. Conclusıon And Future Work

In this work, a modified reversible watermarking technique is presented over CT medical images. This technique is totally new and simple approach in spatial domain. It is evaluated using clinical computed tomography (CT) images obtained from different parts of the human body. Based on the results of experiments, the suggested technique outperforms conventional DWT-based, traditional SVD-based, and DWT-SVD-based watermarking techniques for CT medical images regarding security, invisibility, and robustness.

After this study, a concise comparison of image watermarking approaches is also proposed here to aid with future studies in this field. Such as, the extend watermarking approach encrypting the transmitted image with Advanced Encryption Standard (AES) for better and safer transmission. Advantages of the proposed approach include reducing image size and encrypting watermarked images before transmission to safeguard patient data. The suggested method offers resistance to geometry and signal attacks due to its LSB embedding mechanism along with AES encryption mechanism, which is sensitive to alterations.

Data availability statement

All considered datasets are open-source datasets. We have cited all references of the datasets.

Note on competing interests and obligations

The authors affirm that they do not possess any identifiable conflicting financial interests or personal affiliations that may have influenced the research presented in this scholarly article.

References

[1] L. Q. Kuang, Y. Zhang, and X. Han, "A Medical Image Authentication System Based on Reversible Digital Watermarking," in *Proceedings of the 1st International Conference on Information Science and Engineering (ICISE)*, Nanjing, China, pp. 1047–1050 (2009), doi: 10.1109/ICISE.2009.60.

[2] P. K. Sahoo, M. K. Nanda, and M. Jahangeer, "A Modified Framework for Reversible Digital Image Watermarking," in *Proceedings of the International Conference on Advanced Machine Learning (ICAML)*, Bhubaneswar, India, pp. 228–234 (2019), doi: 10.1109/ICAML48257.2019.00049.

[3] G. Bhatnagar and W. U. Jonathan, "Biometrics inspired watermarking based on a fractional dual tree complex wavelet transform," *Future Generation Computer Systems*, vol. 29, no. 1, pp. 182–195 (2013), doi: 10.1016/j.future.2012.05.021.

[4] W. Pan, G. Coatrieux, N. C. Boulahia, F. Cuppens, and C. Roux, "Medical image integrity control combining digital signature and lossless watermarking," in *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance*, vol. 5959, Lecture Notes in Computer Science (LNCS), Berlin, Germany: Springer, pp. 153–162, (2010), doi: 10.1007/978-3-642-11207-2_12.

[5] J. M. Zain and M. Clarke, "Reversible region of non-interest (RONI) watermarking for authentication of DICOM images," *Intenational Journal of Computer Science and Network Security*, vol. 7, no. 9, pp. 19–28 (2011), doi: 10.48550/arXiv.1101.1603.

[6] N. I. Wu and Hwang, "Data hiding current status and key issues," *International journal of Network Security*, vol. 4, no. 1, pp. 1–9 (2007).

[7] K. Heylen and T. Dams, "An image watermarking tutorial tool using MATLAB," in *Mathematics of Data/Image Pattern Recognition, Compression, and Encryption with Applications XI*, Proc. SPIE 7075, San Diego, CA, USA, Art. no. 70750D (2008), doi: 10.1117/12.793308.

[8] S. P. Mohanty, K. R. Ramakrishnan, and M. Kankanhalli, "A Dual Watermarking Technique for Images," in *Proceedings of the 7th ACM International Conference on Multimedia*, Orlando, FL, USA, pp. 49–5 (1999), doi: 10.1145/319878.319891.

[9] P. K. Sahoo, D. Gountia, R. Dash, and J. Mohammed, "A Technical Analysis of Digital Image and Video Processing," *IETE Technical Review,* vol. 41, no. 4, pp. 420-430 (2024), doi: 10.1080/02564602.2023.2262418

[10] A. S. Gaikwad, V. D. Gowda, and P. A. Athavale, "Enhancing IoT security through encrypted image processing for intelligent surveillance system," *Journal of information and Optimization Sciences*, vol. 46, no. 7, pp. 2363-2374 (2025), doi: 10.47974/JIOS-2133.

[11] V. S. Jabade and S. R. Gengaje, "Literature review of wavelet based digital image watermarking techniques," *International Journal of Computer Application,* vol. 31, no. 1, pp. 28–35 (2011), doi: 10.5120/3838-5334.

[12] N. A. Memon and S. A. M. Gilani, "Watermarking of chest CT scan medical images for content authentication," *International Journal of Computer Mathematics*, vol. 88, no. 22, pp. 265– 280 (2010), doi: 10.1080/00207161003596690.

[13] M. Kaur and R. Kaur, "Reversible watermarking of medical images authentication and recovery-a survey," *Journal of Information and Operations Management*, vol. 3, no. 1,pp. 241– 244 (2012).

[14] J. M. Zain and M. Clarke, "Reversible region of non-interest (RONI) watermarking for authentication of DICOM images," *Int. J. Comput. Sci. Netw. Secur.*, vol. 7, no. 9, pp. 19–28 (2007).

[15] O. M. Al-Qershi and B. E. Khoo, "Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images," *Journal of digital imaging*, vol. 24, no. 1, pp. 114-125 (2011), doi: 10.1007/s10278-009-9253-1.

[16] R. A. Movahed, M. R. Rezaeian, and S. Ghasemi, "An Image Watermarking Algorithm for Medical Computerized Tomography Images," in *Proceedings of the 5th Iranian Conference on Signal Processing and Intelligent Systems (ICSPIS)*, Shahrood, Iran, pp. 1–5 (2019), doi: 10.1109/ICSPIS48872.2019.9066018.

[17] C. W. Honsinger, P. W. Jones, M. Rabbani, and J. C. Stoffel, "Lossless Recovery of an Original Image Containing Embedded Data," U.S. Patent 6,278,791, (Aug. 2001).

[18] J. Fridrich and M. Goljan, "Practical Steganalysis of Digital Images," in *Security and Watermarking of Multimedia Contents IV*, Proc. SPIE 4675, San Jose, CA, USA, pp. 1–13 (2002), doi: 10.1117/12.465263.

[19] T. Kalker and F. M. J. Willems, "Capacity Bounds and Construction for Reversible Data Hiding," in *Proceedings of the 14th International Conference on Digital Signal Processing (DSP 2002)*, Santorini, Greece, vol. 1, pp. 71–76 (2002), doi: 10.1109/ICDSP.2002.1027818.

[20] B. Perry, B. MacIntosh, and D. Cushman, "Digimarc MediaBridge—The Birth of a Consumer Product, from Concept to Commercial Application," *Proceedings of Electronic Imaging Security and Watermarking of Multimedia*, San Jose, California, United States, vol. 4, pp. 118–123 (2002), doi:10.117/12.465267.

[21] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," *IEEE Transactions on Image Processing*, vol. 14, no. 2, pp. 253-266 (2005), doi: 10.1109/TIP.2004.840686.

[22] J. Tian, "Wavelet-Based Reversible Watermarking for Authentication," in *Security and Watermarking of Multimedia Contents IV*, Proc. SPIE 4675, San Jose, CA, USA, pp. 679–690 (2002), doi: 10.1117/12.465329.

[23] A. L. Wakekar, S. Patil, V. K Bhosale, E. Xudaynazarov, N. Tukhtaeva, and S. Karale, "Algebraic geometry approaches to 3D image reconstruction," *Journal of Interdisciplinary Mathematics*, vol. 29, no. 3, pp. 709–717 (2026), doi: 10.47974/JIM-2507.

[24] J. Tian, "High Capacity Reversible Data Embedding and Content Authentication," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2003)*, Hong Kong, China, vol. 3, pp. III-517–III-520 (2003), doi: 10.1109/ICASSP.2003.1199525.

[25] A. M. Alattar, "Reversible Watermark Using the Difference Expansion of a Generalized Integer Transform," *IEEE Transactions on Image Processing*, vol. 13, no. 8, pp. 1147–1156 (2004), doi: 10.1109/TIP.2004.828418.

[26] S. G. Mallat, "Multifrequency Channel Decomposition of Images and Wavelet Models," *IEEE Transactions on Acoustics, Speech, and Signal Processing*, vol. 37, no. 12, pp. 2091–2110 (1989), doi: 10.1109/29.45554.

[27] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Transactions on Circuits and System for Video Technology*, vol. 13, no. 8, pp. 890–896 (2003), doi: 10.1109/TCSVT.2003.815962.

[28] A. M. Alattar, "Reversible Watermark Using Difference Expansion of Quads," in *Proceedings of the IEEE International Conference on Acoustics,*

Speech, and Signal Processing (ICASSP '04), Montreal, QC, Canada, pp. 377–380 (2004), doi: 10.1109/ICASSP.2004.1326560.

[29] D.-C. Lou, M.-C. Hu, and J.-L. Liu, "Multiple layer data hiding scheme for medical images," *Computer Standards & Interfaces*, vol. 31, no. 2, pp. 329–335 (Feb. 2009), doi: 10.1016/j.csi.2008.05.009.

[30] M. Fallahpour, D. Megías, and M. Ghanbari, "Reversible and High-Capacity Data Hiding in Medical Images," *IET Image Processing*, vol. 5, no. 1, pp. 190–197 (2011), doi: 10.1049/iet-ipr.2009.0226.

[31] W.-L. Tai, C.-M. Yeh, and C.-C. Chang, "Reversible Data Hiding Based on Histogram Modification of Pixel Differences," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 19, no. 6, pp. 906–910 (2009), doi: 10.1109/TCSVT.2009.2017409.

[32] W. Puech, M. Chaumont, and O. Strauss, "A Reversible Data Hiding Method for Encrypted Images," in *Security, Forensics, Steganography, and Watermarking of Multimedia Contents X*, Proc. SPIE 6819, San Jose, CA, USA, 68191E, (2008), doi: 10.1117/12.766754.

[33] M. S. Rani and S. Lakshmanan, "A Novel Method of Data Hiding and Image Compression for Medical Images," *International Journal of Advanced Information Technology*, vol. 6, no. 1, pp. 43–51 (Feb. 2016), doi: 10.5121/ijait.2016.6104.

[34] T. Aydogan and C. Bayilmis, "A new efficient block matching data hiding method based on scanning order selection in medical images," *Turkish Journal of Electrical Engineering & Computer Sciences*, vol. 25, no. 1, pp. 461-473 (2017), doi: 10.3906/elk-1506-189.

[35] J. Wu, R. Chang, C. Chen, C. Wang, T. Kuo, W. N. Moo, and D. Chen, "Tamper detection and recovery for medical images using nearlossless information hiding technique," *Journal of Digital Imaging*, vol. 21, no. 1, pp. 59-76 (2007), doi: 10.1007/s10278-007-9011-1.

[36] M. M. Rani and S. Lakshmanan, "An Integrated Method of Data Hiding and Compression of Medical Images," *International Journal of Advanced Information Technology*, vol. 6, no. 1, pp. 43-51 (2016), doi: 10.5281/zenodo.5771904.

[37] H. Chao, C. Hsu, and S. Miaou, "A data-hiding technique with authentication, integration, and confidentiality for electronic patient records," *IEEE Transactions on Information Technology in Biomedical*, vol. 6, no. 1, pp. 46-53 (2002), doi: 10.1109/4233.992161.

[38] J. Chang, Y. Lu, and H. Wu, "A separable reversible data hiding scheme for encrypted JPEG bitstreams," signal processing vol. 133, no. 3, pp. 135-14 (2017), doi: 10.1016/j.sigpro.2016.11.003.

[39] W. A. W. Adnam, S. Hitarn, S. A. –Karim, and M. R. TamJis, "A review of image watermarking," *Proceedings Student Conference*, Putrajaya, Malaysia, pp. 381–384, doi: 10.1109/SCORED.2003.1459727.

[40] P. K. Sahoo and M. K. Nanda, "A modified partitioning algorithm for classification of e-waste," *Journal of Statistics and Management Systems*, vol. 26, no. 1, pp. 53-65 (2023), doi: 10.47974/JSMS-947.

[41] P. K. Sahoo, D. Gountia, R. Dash, S. Behera, and M. K. Nanda, "An Extension Application of 1D Wavelet Denoising Method for Image Denoising," In: Lanka, S., Sarasa-Cabezuelo, A., Tugui, A. (eds) *Trends in Sustainable Computing and Machine Intelligence*., ictsm 2023, *Algorithms for Intelligent Systems*. Springer, Singapore, vol. 1, no. 1, pp. 87-105 (2024), doi: 10.1007/978-981-99-9436-6_7.

[42] P. K. Sahoo, D. Gountia, and R. K. Dash, "Combine Application of Reversible Watermarking Technique and RSA Algorithm to Verify Ownership of Digital Images: A Hybrid Image Restoration Approach," *Journal of Dalian University of Technology*, vol. 33, no. 3, pp. 286-302 (2026), doi: 10.5281/zenodo.18999399.

[43] S. Batra, B. Narwal, and A. K. Mohapatra, " JLSAIoMT : Justifiable lightweight and secure mutual authentication scheme for Internet of Medical Things," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 29, no. 3, pp. 1151–1180 (2026), doi: 10.47974/JDMSC-2189.

[44] A. Noruzi, N. Nazeri, S. J. Baghiabadi, R. Farshid, A. S. A. Mirkabad, and A. Asnafi, "Analysis of scientific productions regarding knowledge management with the open innovation approach," *COLLNET Journal of Scientometrics and Information Management*, vol. 19, no. 2, pp. 229–253 (2025), doi: 10.47974/CJSIM-2025-03005.

[45] B. Zouilekh and S. Bouroubi, "Optimizing minimum dominating set using an enhanced binary whale algorithm," *Journal of Information and Optimization Sciences*, vol. 47, no. 3, pp. 887–905 (2026), doi: 10.47974/JIOS-1583.

Received March, 2025