Taylor & Francis
Taylor & Francis Group

Automatika

Journal for Control, Measurement, Electronics, Computing and Communications

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/taut20

Enhancing medical image security through machine learning and dual watermarking-based technique

Kumari Suniti Singh & Harsh Vikram Singh

To cite this article: Kumari Suniti Singh & Harsh Vikram Singh (2024) Enhancing medical image security through machine learning and dual watermarking-based technique, Automatika, 65:4, 1579-1592, DOI: 10.1080/00051144.2024.2348907

To link to this article: https://doi.org/10.1080/00051144.2024.2348907

© 2024 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group.

Published online: 01 Oct 2024.

Submit your article to this journal

Article views: 584

View related articles

View Crossmark data

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=taut20

AUTOMATIKA
2024, VOL. 65, NO. 4, 1579–1592
https://doi.org/10.1080/00051144.2024.2348907

OPEN ACCESS

Enhancing medical image security through machine learning and dual watermarking-based technique

Kumari Suniti Singh and Harsh Vikram Singh

Department of Electronics Engineering, KNIT, Sultanpur, India

ABSTRACT

As the world becomes increasingly digital, healthcare is no exception. With the ease of sharing e-healthcare records over open networks, smart healthcare systems have become a popular way to manage patient information. But as the popularity of these systems has grown, so has the concern for their security. That's where image security techniques come in. In this paper we have developed a new approach to secure e-patient records like DICOM images. By combining the redundant discrete wavelets transform (RDWT), Hessenberg Decomposition (HD), and randomized singular value decomposition (RSVD). We developed a robust and dual watermarking scheme. This scheme uses multiple watermarks, including Electronic Patient Record (EPR) as text and images, to ensure high-level authentication. In order to attain a balance between imperceptibility and robustness, a PSO-based optimization of scale factor is employed and Turbo code is utilized to encode the EPR and minimize channel noise. Additionally, the marked image undergoes encryption using a 3D chaotic-based encryption technique, and the extracted watermark is denoised through a deep neural network. The result shows that the proposed scheme is both secure and reliable. With this dual watermarking scheme, we have made great strides in securing e-patient records.

ARTICLE HISTORY
Received 10 December 2023
Accepted 24 April 2024

KEYWORDS
CT-scan images; dual watermarking; RDWT; HD; RSVD; image security; chaotic encryption; PSO optimization; DNN based denoising

1. Introduction

As the internet advances and more e-patient records need to be transmitted, security concerns have become increasingly important, especially in the wake of the global health emergency caused by the Coronavirus [1,2]. While there are many standards and guidelines for securing medical records, none have fully addressed all the security issues [3–5]. Various organizations issue multiple standards and guidelines to guarantee the security of medical records [6]. To address these concerns, many medical image watermarking techniques are being used, such as nature-based optimization [7,8] and chaos-based encryption [9,10] techniques. Despite this, there are only a few techniques that can simultaneously enhance robustness and imperceptibility, while also ensuring good embedding capacity and security. Meanwhile, each technique has its pros and cons. The main concern is that securing e-patient records during the transfer process is critical to ensuring their integrity and authenticity, especially during a pandemic. This paper proposes a dual watermarking solution to enhance the authenticity of medical data. In this paper, the EPR is encoded with the Turbo code to minimize channel noise errors [11] and also an image watermark is used and embedded with EPR to generate a final watermark image. A hybrid of RDWT-HD-RSVD [7,11] is employed to conceal dual watermarks within the host image, as it possesses all the attributes of DWT, is shift invariant and offers greater embedding capacity. Additionally, the HD decomposition produces accurate components that enhance robustness [7], while the RSVD technique decreases computational complexity [12]. A PSO-based optimization has been used to manage robustness through the optimized scale factor while maintaining acceptable imperceptibility [7]. To enhance the security further, the watermarked image is encrypted using a 3D chaos-based encryption scheme with low computational complexity [9,10]. Lastly, to enhance the robustness of the extracted watermark image and make it more similar to the original watermark image, a noise removal approach based on DNN is employed [12]. Various research contributions provide an effective and efficient way of securing e-patient records during the transfer process. The remaining parts of the paper are listed as follows: Section 2 of the paper highlights different watermarking schemes used in healthcare. The paper then presents its innovative methodology in Section 3.

CONTACT Kumari Suniti Singh suniti.singh.2287@knit.ac.in Department of Electronics Engineering, KNIT, Sultanpur 228118, India

© 2024 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group.
This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

Section 4 provides an in-depth analysis of the results of the proposed scheme, and Section 5 wraps up with concluding remarks. This structured approach ensures that readers are taken on an engaging journey that provides insights into the different watermarking schemes and the proposed scheme.

2. Literature review

As healthcare is the main focus of this paper, Section 2 provides a brief overview of various watermarking schemes that have been used in the field. This section serves as a valuable resource for readers who want to understand the various watermarking techniques used in healthcare and the strengths and weaknesses of each approach. One notable framework discussed in [11] is a Paillier cryptosystem-based approach for securing healthcare records. The method uses a step space-filling curve and turbo code to encode the image and character mark, respectively, resulting in improved security and robustness. The framework also leverages homomorphic properties for efficient watermarking, but it comes at a high computational cost. Liu et al. [7] presented an optimization-based approach that uses fruit fly optimization inspired by nature for watermarking medical images. This method achieves acceptable imperceptibility while maintaining robustness. Ali et al. [8] have come up with an ingenious solution for efficiently transmitting images over networks through redistributed invariant DWT and SVD. The authors used artificial bee colony (ABC) optimization to embed the watermark into the host image in an optimized manner, resulting in robust and imperceptible watermarking. In respect of this, works of [7,11,12] present several sturdy watermarking techniques that rely on DWT and SVD. False positives are a significant concern in SVD-based watermarking techniques but can be resolved by implementing encryption operations. In particular, chaotic systems are employed to encrypt the SVD components, thus ensuring the watermarking method exhibits robust security performance by mitigating the false positive issue. In the pursuit of safeguarding healthcare records, researchers have explored a variety of approaches to embed secure watermarks. In [12], the authors described a dual marking algorithm that makes use of the redistributed invariant DWT and SVD to hide watermarks in the original host image. They utilized a turbo coder on the text mark to minimize channel noise, and compression before encryption to ensure enhanced security during transmission. Thakur et al. [13] developed an effective watermarking technique by incorporating multiple watermark embedding and chaotic-based encryption. With such diverse approaches, researchers are making headway in securing healthcare records with effective watermarking techniques. In the quest for more secure and robust watermarking techniques for healthcare records, researchers have employed various strategies, including dual watermarking and the use of hybrid DWT-SVD methods. In one such technique, the Hamming code is used for the healthcare records before embedding dual watermarks in the original image. This paper [10] introduces a novel encryption technique that utilizes non-linear 3D chaos for position permutation and value transformation. This is the first time that 3D chaos has been used for these specific purposes in encryption. To further enhance security, the marked image is encrypted using 3D chaotic encryption instead of 2D chaotic-based encryption. In this paper [14] a PSO optimization-based chaotic encryption scheme is employed to identify a factor that can improve the quality and robustness of the technique [14,15]. The suggested algorithm involves several stages, including the selection of the key, preprocessing of chaotic sequences, block scrambling, expansion, confusion and diffusion. To select the key, they used particle swarm optimization (PSO) and incorporated it into the chaotic map. In the paper [15], the authors proposed a hybrid algorithm called HFPSO, which combines the strengths of both firefly and particle swarm optimization mechanisms. By leveraging the advantages of these two approaches, HFPSO can achieve improved performance compared to using either method alone. Specifically, HFPSO utilizes the previous global best fitness values to determine the start of the local search process, resulting in a more effective optimization technique. Numerous image encryption algorithms have been developed using chaotic maps, such as the logistic map [9,10]. However, higher-dimensional chaotic functions are considered more secure against cryptanalytic attacks [10]. Ansari et al. [16] implemented a method based on DWT-SVD and LSB to secure the image and tamper localization. Despite significant advancements in watermarking techniques, many existing methods struggle to balance robustness and visual quality, leading to limited embedding capacity. While the hidden mark can be extracted effectively, these schemes often suffer from security vulnerabilities, making them less reliable for protecting sensitive healthcare data. Table 1 shows the comparison of existing methods as discussed in the literature review.

3. Proposed watermarking scheme

This section implements an efficient watermarking scheme that can effectively embed and recover watermarks with optimized robustness and visual quality. Our proposed scheme is achieved through four phases, each designed to ensure maximum efficiency. First, we generated the watermark, followed by embedding and recovery using an optimized scale factor obtained through PSO optimization then encrypted the marked image using a 3D chaotic encryption scheme for added

Table 1. Comparison of existing methods.

Authors	Objectives	Methods	Evaluation matrix	Limitations
Anand et al. [11]	Paillier cryptosystem-based approach for securing healthcare records.	Step space filling curve and turbo code	PSNR, BER, SSIM	High computational cost.
Liu et al. [7]	An aim to ensure security of client data through watermarking	DWT-HD-SVD and Fruit fly optimization	PSNR, SSIM, NC	Results are evaluated only for non-medical images
Anand et al. [12]	To provide an improved watermarking technique	DWT-SVD and compression	PSNR, SSIM, NC,CR,BER	Time consuming
Wang et al. [14]	Provides an image encryption scheme	PSO and chaotic based scheme	NPCR,UACI	Key has no correlation with plaintext images
Gangadhar et al. [16]	Providing programming approach for securing medical images	DWT-SVD and PSO	PSNR, NC	Less parameters are taken into consideration for performance evaluation

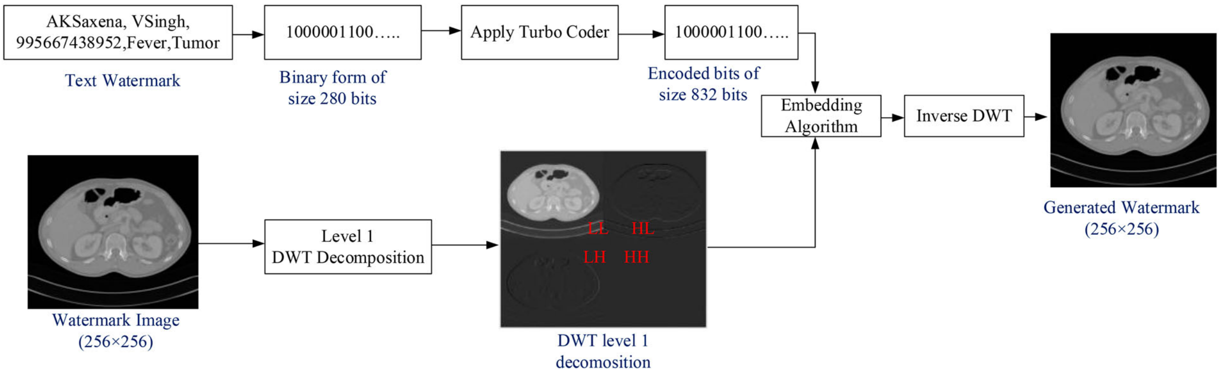

AKSaxena, VSingh, 995667438952,Fever,Tumor
Text Watermark
1000001100…..
Binary form of size 280 bits
Apply Turbo Coder
1000001100…..
Encoded bits of size 832 bits
Embedding Algorithm
Inverse DWT
Generated Watermark (256×256)
Watermark Image (256×256)
Level 1 DWT Decomposition
LL
HL
LH
HH
DWT level 1 decomosition

Figure 1. Watermark generation process.

security. Sections 3.1—3.4 offer a comprehensive explanation of the four stages of our approach, accompanied by Algorithms 1—4.

3.1. Watermark generation

The implemented method takes image watermarking to the next level by combining a text watermark with the image watermark resulting in a single watermark, which is a highly secure generated watermark image as shown in Figure 1. The character watermark includes vital information such as the doctor's and patient's names, Identity card number (ID) and symptoms, making it an EPR watermark (see Figure 1). The ASCII format of the EPR is then encoded using the turbo code to mitigate the effects of channel noise. After encoding, the bits are embedded into the image watermark through DWT, creating the final watermark image as given in Algorithm 1.

Algorithm 1. Watermark Generation (Watermark_text (W_T), Watermark_image (W_I), scale factor (alpha))

```
Start
text_binary ← dec2bin ($W_T$);
text_encoded ← Turbo (text_binary);
for i = 1: size (text_encoded) do
    if text_encoded [i] = = 0
        text_encoded [i] ← −1;
    end if
end for
length ← Length (text_encoded);
if $W_I$ is colour image
    $W_I$ ← rgb2gray ($W_I$);
end if
[$LL_1$, $HL_1$, $LH_1$, $HH_1$] ← DWT ($W_I$);
Watermarked_$HH_1$ ← Embed ($HH_1$, text_encoded, alpha,length);
Generated_watermark ← iDWT ($LL_1$, $HL_1$, $LH_1$, Watermarked_$HH_1$);
return Generated_watermark($W_G$)
```

3.2. Watermark embedding and extraction procedure

In this work, a technique has been proposed to securely embed a watermark into the DICOM host images. The watermarking process is divided into two stages: embedding and extraction. First, the watermark is generated using Algorithm 1. Further, the embedding process uses DWT-based transform to decompose the image into sub-bands. The selected component is transformed using RDWT and then subjected to HD on the specific band of the host image. The HD matrix obtained is further decomposed using RSVD, and the embedding factor obtained through PSO is identified to embed the watermark into the original SVD image. Finally, inverse SVD, HD and DWT have been applied to get the watermarked image. Extraction of the watermark is similar to embedding of the watermark and the whole process of embedding is explained in Algorithm 2, which ensures that the watermark can be securely embedded and extracted from the image. The flow diagram for embedding and extraction of the proposed scheme is shown in Figures 2 and 3, respectively. Later we apply encryption on watermarked images to further enhance the proposed scheme. Extracting the watermark from an image can sometimes result in a

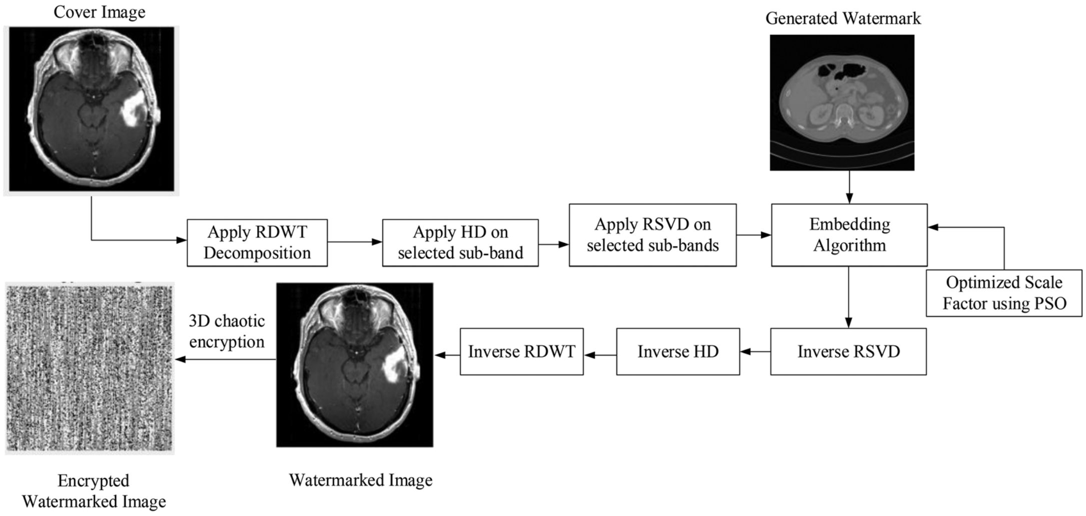


Figure 2. Shows the embedding process.

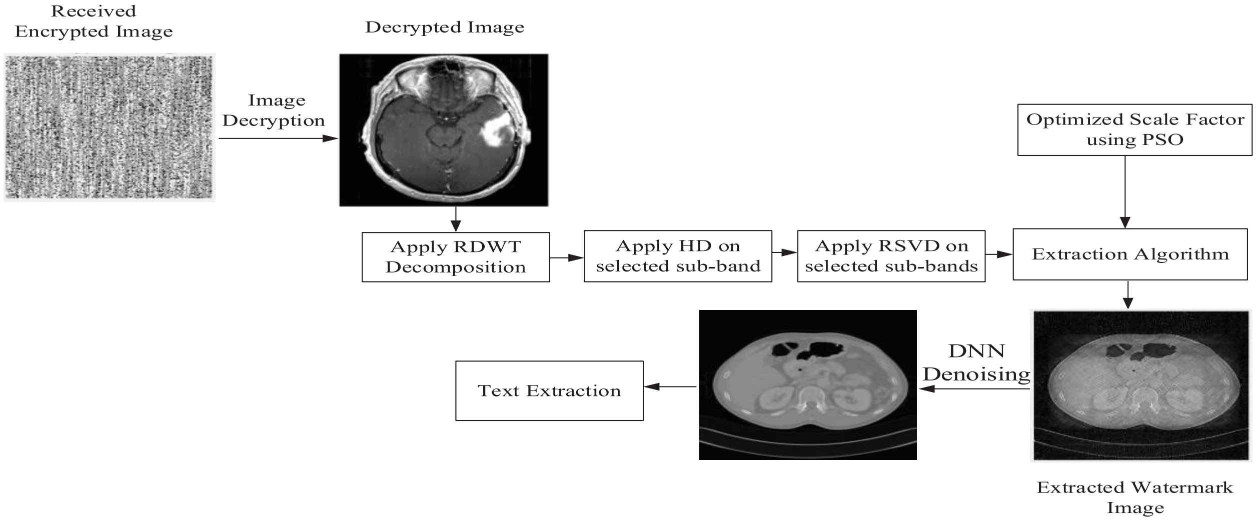


Figure 3. Shows the extraction process.

noisy and distorted mark image, making it difficult to read or use. To tackle this issue, a deep neural network (DNN) is employed during extraction to improve the visual quality of the extracted mark. By denoising the image using advanced algorithms, the extracted watermark becomes clearer and more legible, making it easier to analyse and utilize. The improved quality of the extracted mark enhances the accuracy and reliability of the watermarking scheme, ensuring the authenticity and security of the marked data. Figure 4 shows the data utilized for experimental analysis of proposed schemes in detail.

Algorithm 2: Watermark_Embedding (Host_image (H_I), Generated_watermark (W_G), opt_ScaleFactor(SF))

```
Start
M = length(Host_image);
N = length(Generated_watermark);
R = $\log_2(M/N)$;
[ $RLL_I$, $RHL_I$, $RLH_I$, $RHH_I$] ← RDWT ($H_I$, 'Haar');
[$RP_I$, $RH_I$] ← Hessenberg ($RLL_I$);
[U, S, V] ← RSVD ($RH_I$);
opt_ScaleFactor ← Optimizing_ScalingFactor (S);
$W_G$ ← U × w_S × $V^T$;
w_H ← S + opt_ScaleFactor × w_S;
w_RLL ← $RP_I$ × w_H ×$RP_I^T$;
watermarked_image ← IRDWT (w_RLL, $RHL_I$, $RLH_I$, $RHH_I$);
return watermarked_image($^{H}{}_{I}*$)
```

3.3. PSO-based scale factor optimization

Achieving the appropriate balance between robustness and imperceptibility in a watermarking technique is not an easy task. As the watermark's robustness strengthens, the quality of the marked image is often compromised. That is where nature-inspired optimization techniques come into the picture; they can produce a scaling factor that optimizes both robustness and imperceptibility. To do this, we have used PSO-based

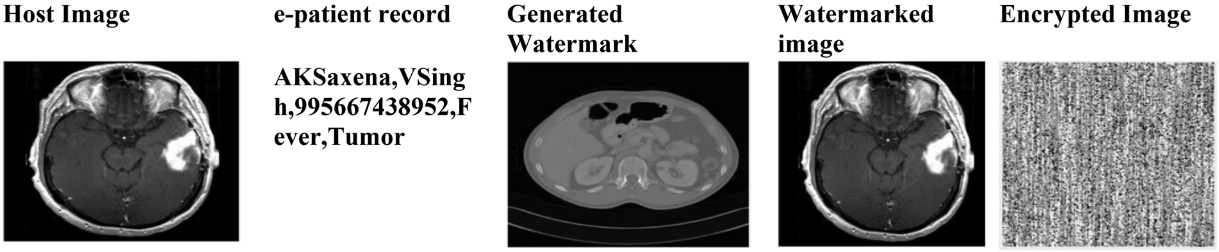


Figure 4. Shows the data utilized for experimental analysis.

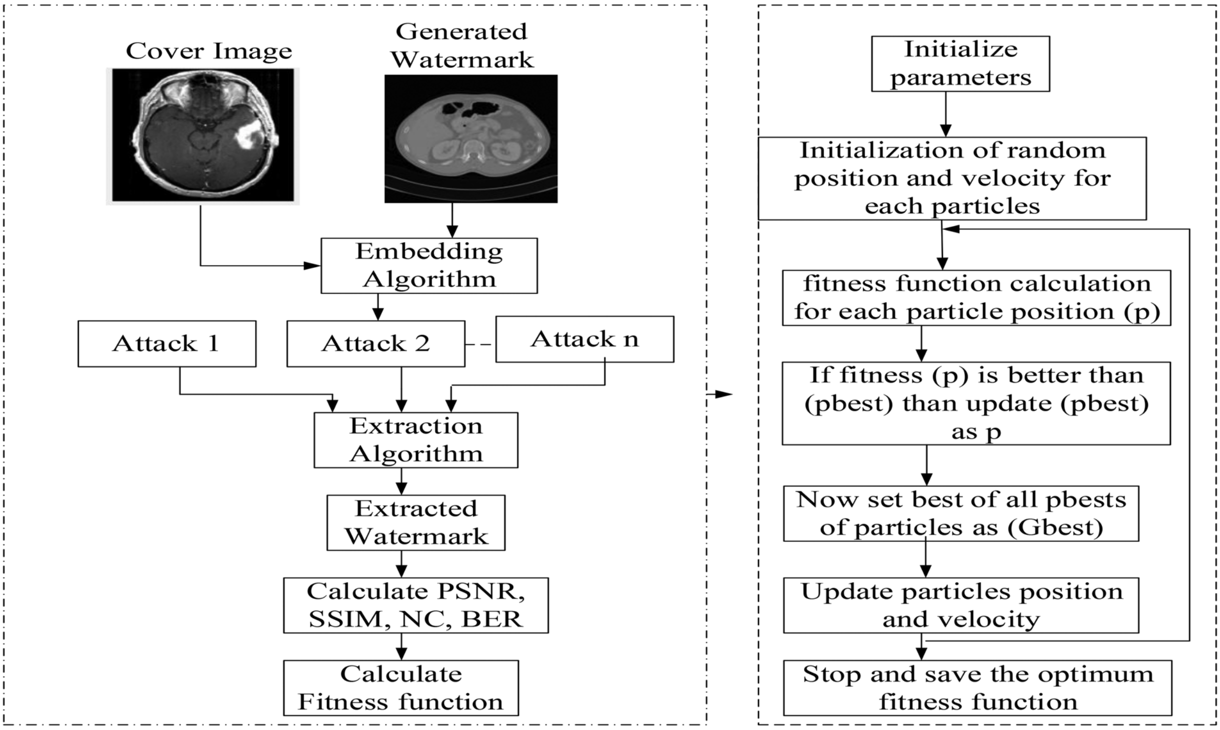

Cover Image
Generated Watermark
Embedding Algorithm
Attack 1
Attack 2
Attack n
Extraction Algorithm
Extracted Watermark
Calculate PSNR, SSIM, NC, BER
Calculate Fitness function
Initialize parameters
Initialization of random position and velocity for each particles
fitness function calculation for each particle position (p)
If fitness (p) is better than (pbest) than update (pbest) as p
Now set best of all pbests of particles as (Gbest)
Update particles position and velocity
Stop and save the optimum fitness function

Figure 5. Flow chart of PSO optimization.

optimization, as detailed in Algorithm 3. PSO is a type of swarm intelligence algorithm that involves swarms working together to locate the optimal solution or "food". Members of the swarm change their searching patterns based on their personal experiences as well as those of other members [14,15,17]. Figure 5 shows the block diagram of the complete PSO-based optimization process. Algorithm 3 gives the details about the PSO-based optimized scale factor in our scheme.

Algorithm 3. Optimization of Scaling Factor (SF)

```
Start
[psnr1, ssim1, nc1, ber1] $\leftarrow$ Embedding_algorithm
   (Host_image, Generated_watermark,
SF);
total $\leftarrow$ Count(attacks);
for i $\leftarrow$ total do
    [ssim[i], nc[i], ber[i]] $\leftarrow$ Embedding_algorithm
       (Host_image, Generated_watermark,
    SF, attack[i]);
end for
fitness_value $\leftarrow$ Fitness ((psnr1, ssim1, nc1, ber1), (ssim[1],
   nc [1], ber [1]) .........(ssim [total], nc [total], ber [total]));
optimized_ScaleFactor $\leftarrow$ PSO (fitness_value)
return optimized_SF
```

The PSO algorithm begins by initializing the solution of each optimization problem through a collection of random particles. These particles then explore the D-dimensional space, and their current position is evaluated using the fitness function. During the search process, the particles adjust their speed based on their own flying experience as well as that of their companions. Let there be m particles in the D-dimensional space, and the position and velocity of the ith particle can be denoted as $x_i = (x_{i1}, x_{i2}, \ldots, x_{iD})$, $v_i = (v_{i1}, v_{i2}, \ldots, v_{iD})$, $1 \le i \le m$, $1 \le d \le D$. The ith particle's search for individual extremum and the entire particle swarm's search for global extremum are represented as $p_i = (p_{i1}, p_{i2}, \ldots, p_{iD})$ and $p_{gbest} = (p_{g1}, p_{g2}, \ldots, p_{gD})$, respectively. The d-dimensional velocity and position update equations for particle i are as follows:

$$v_{id}^{k+1} = w_t(k) * v_{id}^{k} + l_1 r_1 (p_{id}^{k} - x_{id}^{k}) + l_2 r_2 (p_{gd}^{k} - x_{id}^{k}) \quad (1)$$

$$x_{id}^{k+1} = x_{id}^{k} + v_{id}^{k+1} \quad (2)$$

Table 2. PSO-based optimization parameters.

Parameter	m	w_t	T	l_1	l_2
Value	60	0.7	100	2	2

The velocity and position vectors of the particle i at the kth iteration are represented by $v^{k}{}_{id}$ and x_{id}^{k}, respectively. The learning factors are denoted as l_1, l_2, while r_1, r_2 represent a random number between 0 and 1 that enhances search randomness. The value of the inertia weight is represented by w_t in the PSO process. Table 2 provides the values for the number of particles m, inertia weight w, maximum number of iterations T, and learning factors l1 and l2 that are used in the PSO algorithm. Additionally, the fitness function is defined below as [7]

$$\begin{aligned}\text{fitness function}(\alpha_i, c_i) \\ &= c_1 \text{PSNR}(H_I, H_I^*) \\ &\quad + c_2\,\text{SSIM}(H_I, H_I^*) + c_3 \frac{\sum_{i=1}^{j} NC(G_W, G_W^*)}{j} \\ &\quad + c_4 \frac{\sum_{i=1}^{j} \text{BER}}{j}\end{aligned}$$

where H_I^* is the watermarked host image; G_W^* is the extracted watermark; α_i is the scale factor array; c_1, c_2, c_3, c_4 are proportion coefficients that directly reflect the proportion of invisibility and robustness and j gives the different amounts of attacks applied on the watermarked image.

3.4. Watermarked image encryption

The marked image, which is the product of Algorithm 2, undergoes another level of security by employing a chaotic-based encryption and decryption technique. The encryption technique, introduced in [9,10], utilizes a chaotic-based encryption to produce a cipher image. In [18–20] authors used different types of chaotic map-based encryption techniques to enhance the security. In this proposed scheme generally, two distinct categories of image encryption are used such as position permutation and value transformation. Position permutation techniques involve rearranging the position of image pixels without modifying the pixel values, while value transformation techniques alter pixel values by replacing them with other values, leaving pixel positions intact. The XOR operation is a frequently utilized value transformation technique that produces linear independence between two or more variables. The XOR encryption method is based on the notion that reversing the operation is impossible without the knowledge of one of the two initial arguments. Pixel shuffling is a commonly utilized method to enhance the performance of encryption algorithms. This method involves shuffling the positions of pixels in the original image and subsequently modifying the greyscale values of the shuffled pixels.

This paper proposes an improved encryption technique that utilizes both pixel rotation and XOR-based encryption as detailed in Sections 3.4.1—3.4.5, which employs 3D chaos to enhance the security of multimedia communication. The simulation results demonstrate the effectiveness of our approach against various types of attacks. Figure 6 shows the flowchart of the hybrid encryption technique where $x(0)$, $y(0)$, $z(0)$, α, β, γ , Q1, Q2, Q3, Q4, Q5, Q6 are the keys.

3.4.1. Chaos generation

The logistic map, which is the most basic chaotic process generator, can be expressed as the following equation:

$$x_{n+1} = \mu x_n(1 - x_n) \tag{4}$$

The equation can be made chaotic by satisfying the condition that $0 < x_n < 1$, $\mu = 4$, where x_{n+1} represents the chaotic sequence and μ is the bifurcation factor. The 2D version can be extended by the 3D version as follows:

$$x_{n+1} = \gamma\, x_n(1 - x_n) + \beta y_n^2 x_n + \alpha z_n^3 \tag{5}$$

$$y_{n+1} = \gamma\, y_n(1 - y_n) + \beta z_n^2 y_n + \alpha x_n^3 \tag{6}$$

$$z_{n+1} = \gamma\, z_n(1 - x_n) + \beta x_n^2 x_n + \alpha y_n^3 \tag{7}$$

The above equations behave chaotically for $0 < \alpha < 0.015$, $0 < \beta < 0.0021$, $3.53 < \gamma < 3.82$ and the initial value of x, y, and z is in between 0 and 1.

3.4.2. Chaos histogram equalization

To provide high security we need to equalize the histogram. If the image size is $M \times M$ we can apply the following formula to equalize the histogram:

$$x = (\text{integer}(x \times \text{Q2})) \bmod M \tag{8}$$

$$y = (\text{integer}(y \times \text{Q4})) \bmod M \tag{9}$$

$$z = (\text{integer}(z \times \text{Q6})) \bmod M \tag{10}$$

3.4.3. Row rotation

To enhance the security of image encryption, the new approach involves the rotation of rows and columns of a grey image, resembling a combination lock. To encrypt a row of a grey image, a user selects an M number of chaos sequences and a large random number Q1. Starting from index Q1, the chaos sequence "x" from Equation (5) is used to rotate the row. To enhance security, the chaos is rotated right if it is even.

3.4.4. Column rotation

Column rotation is similar to the rotation of rows, and a user selects M number of chaos sequences and a large

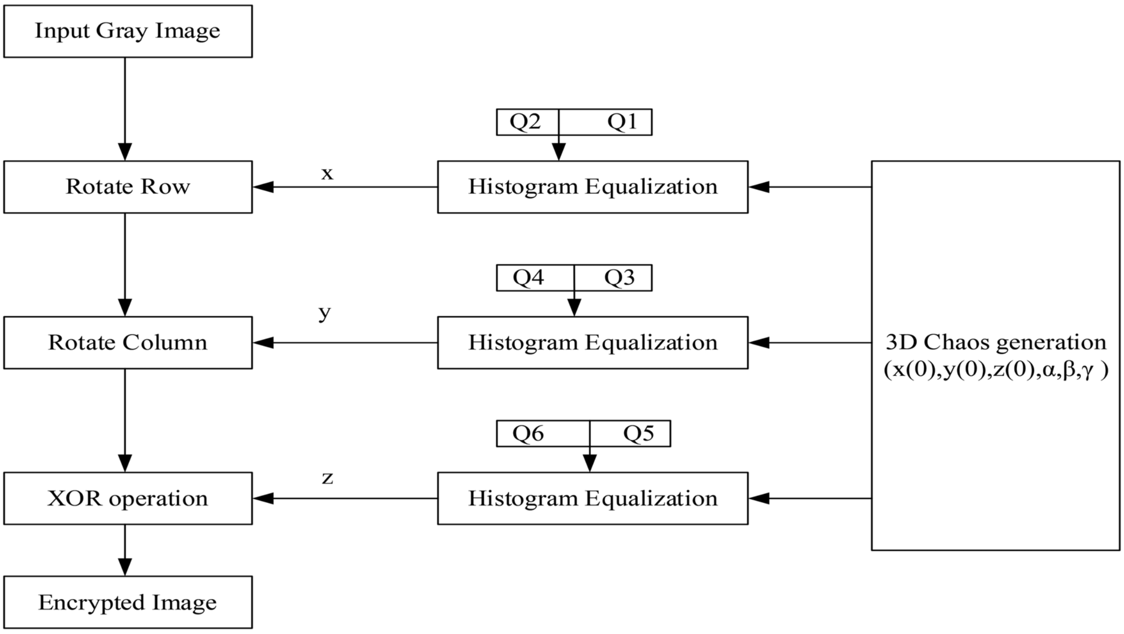


Figure 6. Demonstrate the encryption process using 3D chaos.

random number Q3. Starting from index Q3, the chaos sequence "y" from Equation (6) is used to rotate the column. Encrypting the image through the rotation of rows and columns is vulnerable to a histogram attack. To resolve this issue, an additional step is implemented that modifies the pixel values of the image.

Algorithm 4. Image encryption (watermarked_image, chaotic sequence, key)

```
Start
3D chaos generation using above Equations (5)–(7).
Histogram equalization and preparation for use as given in
  Equations (8)–(10).
x = ceil(mod((x*Q2),image_height));
y = ceil(mod((y*Q4),image_height));
z = ceil(mod((z*Q6),image_height));
Initialize the value of the rotation
for j = 1:1:row
    k(j) = x(j+n);
    l(j) = y(j+p);
End
for i = 1:1:row
k(i) = x(i+n);
End
for j = 1:1:col
    l(j) = y(j+p);
End
for j = 1:1:col*row
    m(j) = z(j+q);
End
If k is even right shift row else left shift row
If l is even shift up column else down shift column
total_length = row*col;
column_image = reshape(shift_column,1,total_length);
for i = 1:1:total_length
xorr1(1,i) = bitxor(column_image(i),m(j));
End
y = reshape(xorr1,row,col);
    return encrypted_image
```

3.4.5. XOR operation

The last step involves an XOR operation that modifies the pixel values of the image. The decryption process involves reversing the rotation without knowing the chaos sequence, generating a large random number Q5 and using the XOR operation to obtain the original image. Histogram equalization can be used to improve the quality of the encrypted image.

3.5. DNN-based image denoising

The papers [21–24] highlight the necessity of DNNs in addressing the complex challenges associated with securing medical images, including segmentation, feature extraction, robustness against attacks, adaptability to chaotic systems, and integration with encryption and compression techniques. DNNs play a crucial role in advancing image security methods and ensuring the confidentiality, integrity and authenticity of medical data. First, we need to choose a pretrained deep neural network for image denoising: There are several popular deep neural networks that have been trained on large datasets of noisy images for image denoising like DnCNN, further, load the pretrained model using a deep learning framework and now load the noisy image as input to it after preprocessing. Now pass the image into the network for image denoising. After image denoising postprocess has been applied on the image and finally save to disk for further process. A DNN-based framework has been given in Figure 7.

4. Experimental results and analysis

The algorithm was implemented on a system with Windows 10 operating system, an i7 processor clocked at 2.50 GHz and 8 GB of RAM. The implementation was done using MATLAB version R2020a-64 bits. The performance of the algorithm has been evaluated based on several parameters as listed in Table 3.

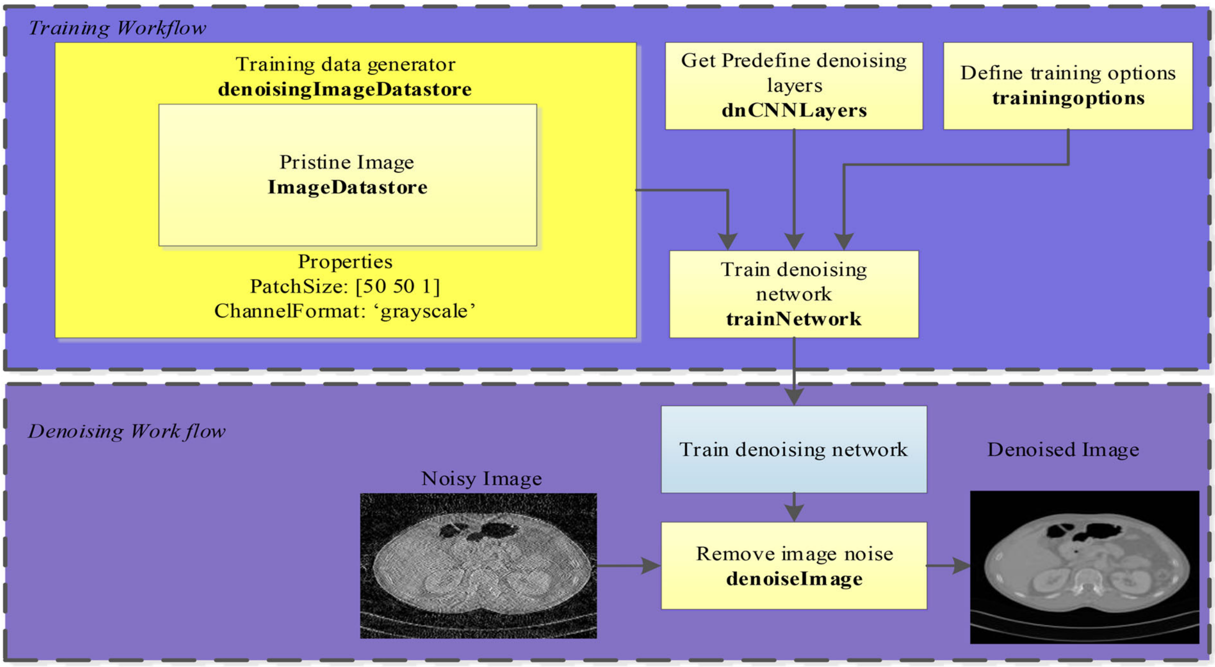


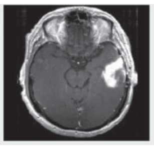
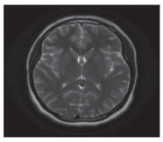
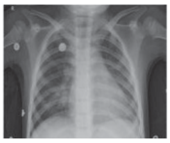
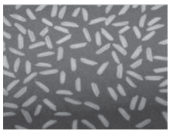
Figure 7. DNN based denoising framework.

Table 3. List of the performance matrices that were utilized in this work.

Performance matrices	Formula	Utilization
Peak signal-to-noise ratio (PSNR) [13,16,25]	$\mathrm{PSNR} = 10\log\frac{H_{I_{\max}}^2}{\mathrm{MSE}}$ where $H_{I_{\max}}^2$ is the maximum possible pixel value of the image (usually 255 for an 8-bit grayscale image), and MSE is the mean squared error between the original image and the marked image.	It measures the quality of the watermarked image by comparing it with the original, un-watermarked image.
Structural Similarity Index (SSIM)	$\mathrm{SSIM} = \frac{\mu_{H_I}\mu_{H_I^*}+c_1}{\mu_{H_I}^2\mu_{H_I^*}^2+c_1}\cdot\frac{\sigma_{H_IH_I^*}+c_2}{\sigma_{H_I}^2+\sigma_{H_I^*}^2+c_2}$ where μ_{H_I} and $\mu_{H_I^*}$ are average of H_I and H_I^*, $\sigma_{H_I}^2$ and $\sigma_{H_I^*}^2$ are variance, c_1 and c_2 are two variables used to stabilize the division in respect to weak denominator.	Used to evaluate the quality of the watermarked image and to ensure that the watermark is imperceptible to the human eye.
Correlation Coefficient (NC)	$\mathrm{NC} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{M} G_{W_{i,j}} G_{W_{i,j}}^*}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{M} G_{W_{i,j}}^2}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{M} G_{W_{i,j}^*}^2}}$	It measures the correlation between the original watermark and the extracted watermark.
Bit Error Rate (BER)	$\mathrm{BER} =$ No. of incorrectly decoded bits/Total no. of bits	It is used to measure the accuracy of the extracted watermark compared to the original watermark.
Number of changing Pixel Rate (NPCR)	$\mathrm{NPCR}(C1, C2) = \frac{\sum_{i,j} D(i,j)}{M\times N}$	Measures the percentage of pixels in the encrypted image that have changed from their original values.
Unified Averaged Changed Intensity (UACI)	$\mathrm{UACI}(C1, C2) = \sum_{i,j}\frac{\lvert C1(i,j)-C2(i,j)\rvert}{255}$ where C1 and C2 are two cipher images before and after pixel change. $D(i,j)$is given as $D(i,j) = \begin{Bmatrix} 1 \; if \; C1(i,j) \neq C2(i,j) \\ 0 \; if \; C1(i,j) = C2(i,j) \end{Bmatrix}$	It calculates the average pixel intensity difference between the original and encrypted images after normalization.

To evaluate the performance of the proposed technique, the experimental parameters include a host DICOM image of size 512×512. An EPR size of 280 bits, and a watermark image size of 256×256 is used to generate the final watermark as illustrated in Figure 4. The 3D chaotic-based encryption scheme is used to encrypt and decrypt the marked image for enhanced security followed by a DNN-based denoising of the extracted watermark. Also, this scheme uses a PSO-based optimization technique to optimize the scale factor. The different evaluation matrices used and their respective roles are listed in Table 2. The proposed approach was evaluated for imperceptibility, robustness and security through multiple experiments. The versatility of the proposed technique was tested on several DICOM images, as shown in Table 3. Furthermore, the technique was also evaluated on various other medical and non-medical images to demonstrate its adaptability and effectiveness. In image processing, achieving both imperceptibility and robustness in a watermarking technique can be a tough task. But the proposed algorithm not only achieves high robustness but also maintains excellent image quality. Furthermore, the technique is versatile enough to be applied to 200 CT scan images of patients and various other medical and non-medical images [26,27]. The extraction of

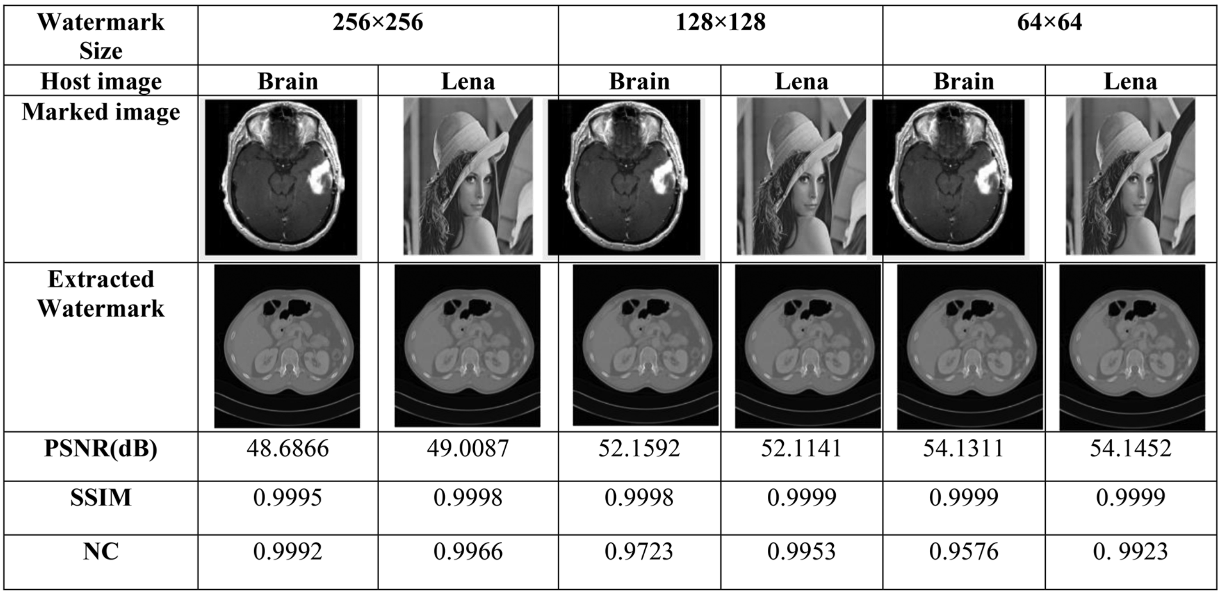
Table 4. Performance analysis using several types of images.

Host images	PSNR (dB)	SSIM	NC	BER
	48.6866	0.9995	0.9992	0
	49.4382	0.9997	0.9997	0
	49.6761	0.9998	0.9937	0
	49.0087	0.9998	0.9966	0
	49.1185	0.9998	0.9974	0
	49.4120	0.9998	0.9963	0
	48.8004	0.9995	0.9962	0
	49.2536	0.9998	0.9982	0
	48.6579	0.9997	0.9336	0
	48.5858	0.9998	0.9794	0
Average of 200 CT scan DICOM images	**48.0853**	**0.9998**	**0.9960**	**0**

e-patient records, up to 346 bits, is entirely possible from the cover image as given in Table 4. The robustness of the technique is put to the test against various signal processing attacks, and the results are impressive, with an acceptable NC value against all attacks. The visual quality of the extracted watermark was subjectively measured against various attacks, and the results confirmed that the proposed approach extracted the mark with high quality. False positive tests were also conducted to validate the proposed technique, thereby making it a reliable watermarking solution for image security.

4.1. Invisibility analysis

In this section, the proposed algorithm's transparency and invisibility are discussed using the PSNR and SSIM. First, the watermark image is embedded into various



Watermark Size	256×256		128×128		64×64	
Host image	Brain	Lena	Brain	Lena	Brain	Lena
Marked image						
Extracted Watermark						
PSNR(dB)	48.6866	49.0087	52.1592	52.1141	54.1311	54.1452
SSIM	0.9995	0.9998	0.9998	0.9999	0.9999	0.9999
NC	0.9992	0.9966	0.9723	0.9953	0.9576	0. 9923

Figure 8. The invisibility performance of the proposed scheme evaluated by using different watermark size and their corresponding extracted watermarks from watermarked image based on metrics such as PSNRs, SSIMs and NCs.

Table 5. Performance at several sizes of e-patient data.

Text size (bits)	PSNR	SSIM	NC	BER (text)
52	43.5382	0.99962	0.9949	0
95	44.6245	0.99975	0.9937	0
120	45.3142	0.99983	0.9931	0
185	46.8696	0.99987	0.9928	0
280	48.6866	0.99987	0.9992	0
305	48.6879	0.99987	0.9942	0.1315
346	48.6880	0.99987	0.9942	0.2184

host images as per Algorithm 2. Then their corresponding PSNR and SSIM values are calculated as given in Figure 8. PSNR is an objective metric that measures image distortion. A higher PSNR value indicates greater similarity between two images. The standard benchmark is 30 dB, and images with PSNR $<$ 30 dB exhibit more noticeable degradation. In general, when PSNR $>$ 30 dB, the image quality is good, and human eyes cannot be able to perceive the modification in the image. The results in Table 4 show that the PSNR between the marked image and the host image is greater than 48 dB and SSIM $>$ 0.9995 in individual cases, indicating that the algorithm has excellent invisibility. Also, the invisibility of the host image has been tested on different sizes of watermarks as given in Figure 8. With a PSNR of 48.6866 dB, SSIM of 0.9995 and NC of 0.9992, the technique proves its worth in head CT scans. This scheme is also tested for several sizes of EPR data and the results are given in Table 5. The value of BER is zero for almost each host image and up to size 346 bits it can be easily extracted from the host image.

4.2. *Robustness analysis*

Different attacks are applied to the embedded watermarked images and again the watermark is extracted from them as shown in Figure 9. The NC between the extracted and original watermark is calculated as given in Table 6. A higher value of NC close to 1 indicates the strong ability of the algorithm to withstand the attacks, whereas weaker robustness is indicated by a lower NC value. The implemented algorithm demonstrates strong robustness against most attacks tested on different images with a maximum NC value of 0.9990, particularly against JPEG compression, cropping and rotation attacks. Although the NC value is not very high in case of motion blur and sharpen attacks still it can be recognized. Additionally, Figure 9 displays the CT scan watermarked image after being attacked and the extracted watermark. As shown in Figure 9, even severely degraded images can yield a clear watermark. Based on the analysis, the proposed algorithm satisfies the robustness requirement, with most attacks producing clear and recognizable watermarks.

4.3. *Security analysis*

The NPCR and UACI values as given in Table 7 illustrate the satisfactory performance of the proposed encryption algorithm as detailed in Algorithm 4. The proposed algorithm has been put through a false positive test. Results given in Figure 11 demonstrate that the algorithm is highly resistant to false positive tests. However, this also results in a poorer NC score due to the random watermark. The key sensitivity analysis of the 3D encryption scheme is validated by modifying random values of the original key, as shown in Figure 10. It is apparent that slight modifications to the key can cause a completely different decrypted image to be generated. If multiple key values are incorrect, the decrypted output would be even more distorted.

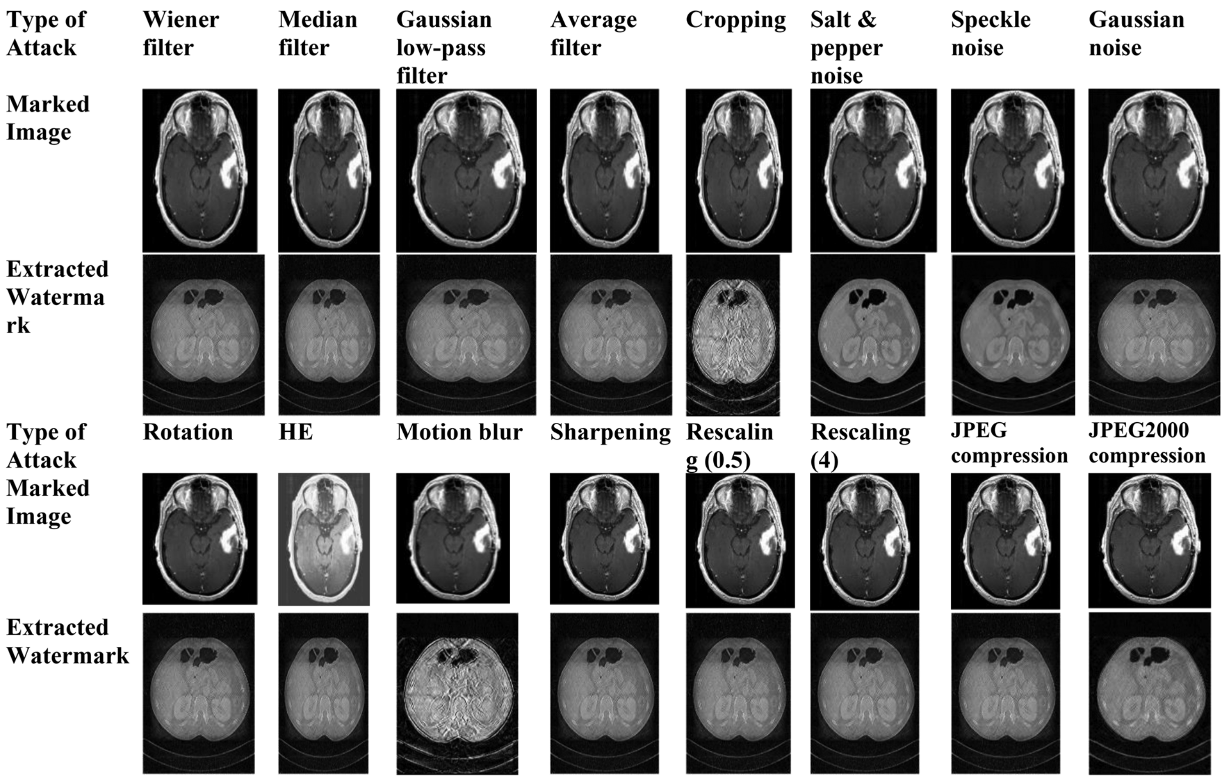


Figure 9. Displays a set of images, consists of an attacked marked image and an extracted watermark image of size 256×256, obtained through various attacks.

Table 6. Robustness analysis of the proposed scheme by applying different attacks on marked image.

Attacks	Specification	NC (image)	BER (text)
No attack	–	0.9992	0
Salt & pepper noise	0.001	0.9985	0
	0.0001	0.9990	0
Gaussian noise	0.001	0.9970	0
	0.0001	0.9987	0
Speckle noise	0.001	0.9984	0
Wiener filter	[2 2]	0.9826	0
	[3 3]	0.9658	0
Median filter	[2 2]	0.9855	0
	[3 3]	0.9676	0
Gaussian low-pass filter	[2 2]	0.9786	0
	[3 3]	0.9962	0
Average filter	[3 3]	0.9458	0
Cropping	[20 20 400 480]	0.9683	40.3462
	2%	0.9829	42.3851
Rotation	2 degree	0.9246	40.5640
	1 degree	0.9287	40.5623
Histogram Equalization (HE)	-	0.9938	0
Motion blur	Theta-4, len-7	0.7313	
Sharpening	0.1	0.9616	0
	0.8	0.9934	0
Rescaling	0.5	0.7853	0
	2	0.9535	0
	4	0.9982	0
JPEG compression	Quality factor = 10	0.9748	0
	Quality factor = 50	0.9938	0
JPEG2000 compression	CR = 10	0.9986	0
PSNR	48.6866	–	
SSIM	0.9995	–	
Optimized Scale factor	0.0283	–	

4.4. Capacity analysis

As we know after the second level of DWT, the second-level sub-band size will be 128×128 for the 512×512 host image and the watermark image is embedded into the sub-bands. For watermark embedding, a level 1 DWT is used resulting in a maximum embedding watermark size of 256×256. The watermarking algorithm capacity is measured by the ratio of watermark pixels to host image pixels. In this case, the capacity of the algorithm is (256×256)/ (512×512) = 0.25, indicating a high capacity scheme.

4.5. Comparative analysis of the proposed scheme with other existing schemes

This section highlights the comparison of our scheme with other existing schemes through analytical examination as given in Table 8 and robustness comparison in Table 9. Also, a capacity comparison has been given in Table 9. The proposed scheme compared using the different bio-inspired optimization algorithms as given in [7] uses a fruit fly and artificial bee colony [8] [25]. The comparison of robustness is shown in Table 8 when the size of the host image and watermark image is 512×512 and 256×256. Table 7 shows that the PSNR and SSIM values of the proposed scheme are more than the existing schemes. Table 8 shows that for filtering attacks (median, Gaussian, average) NC values are more than other schemes, whereas NC values are less for Wiener filtering attacks compared to [7,25]. However,

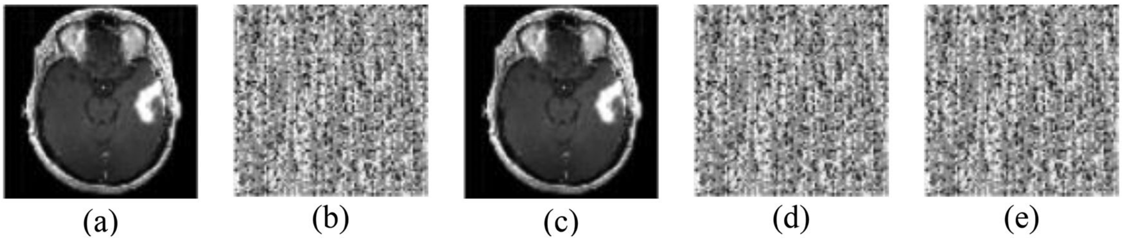


Figure 10. Illustrates the sensitivity analysis of the chaotic-based encryption key: (a) marked image, (b) encrypted image using the original key, (c) decrypted image, (d) decrypted image after modifying one value of the original key and (e) decrypted image after modifying two values of the original key.

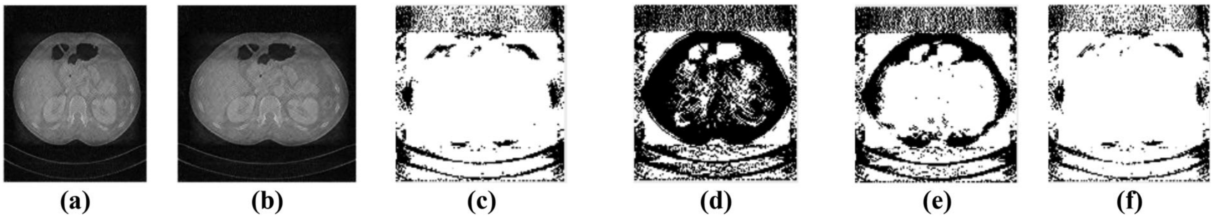


Figure 11. FPP result analysis: (a) original watermark, (b) extracted watermark using correct parameters (x_1, α, y_1, β, z_1, γ) with NC = 0.9992, (c) extracted watermark using correct parameters (y_1, β, z_1, γ) and wrong parameter (x_1, α) with NC = 0.5054, (c) extracted watermark using correct parameters (x_1, α, z_1, γ) and wrong parameter (y_1, β) with NC = 0.7054, (d) extracted watermark using correct parameters (x_1, α, y_1, β) and wrong parameter (z_1, γ) with NC = 0.5934 and (e) extracted watermark using wrong parameters (x_1, α, y_1, β, z_1, γ) with NC = 0.5013.

Table 7. Performance evaluation of the used encryption method.

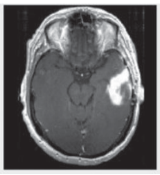
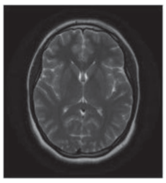
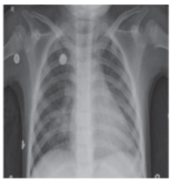
DICOM CT scan images					
NPCR	0.9956	0.9962	0.9943	0.9972	0.9967
UACI	0.2341	0.2354	0.2432	0.2482	0.2364

Table 8. A comparative analysis of the proposed scheme with other existing schemes conducted through analytical examination.

Specification	[7]	[8]	[13]	[17]	[25]	Proposed scheme
Type of Transform	RDWT-HD-RSVD	RIDWT-SVD	DWT-SVD	RDWT-RSVD	DWT-SVD	RDWT-HD-RSVD
Optimization algorithm	Fruit fly	ABC	–	PSO and Firefly	ABC	PSO
Scheme Type	Non-blind	Non-blind	Non-blind	Non-blind	Non-blind	Non-blind
Host Image size	512×512	512×512	512×512	512×512	512×512	512×512
Watermark image size	256×256, 128×128, 64×64	32×32	256×256	256×256	128×128	256×256, 128×128, 64×64
Host image Type	Non-medical	Non-medical	Medical images	Medical images and non-medical	Medical and non-medical	Medical and non-medical
False positive test	Yes	–	–	–	Yes	Yes
Robustness	Robust	Robust	Robust	Robust	Robust	Robust
PSNR (dB)	38.1621	45.5844	38.3571	46.5888	> 40	48.6866
SSIM	0.9992	–	–	0.9964	–	0.9995

NC values are better in the case of sharpening (0.1, 0.8), rescaling (2) and JPEG compression (QF = 50) attacks compared to [7] [13]. Also, the NC values given in Table 8 for Gaussian noise, Salt & Pepper noise and Speckle noise at noise density 0.001 are superior to other schemes. At theta 4 and length 7, our scheme suffers a motion blur attack compared to [7,25] with a low NC value of 0.7313. In most scenarios, the proposed watermarking technique performs well and outperforms the approaches presented in references [7,8,13,25]. Moreover, it demonstrates exceptional resilience against JPEG compression attacks, cropping attacks, filtering and sharpening attacks. Additionally, by utilizing PSO, the proposed watermarking method uses an optimal scaling factor to enhance the robustness of the algorithm. The capacity and time complexity comparison has been given in Table 10. As per Section 4.4 the capacity of our algorithm is 0.25, which is similar to [7,13]. Our algorithm, capacity is 16 times greater than the capacity of the algorithms presented in [8,25], which is 0.015. However, potential shortcomings include computational complexity, vulnerability to advanced attacks, challenges in balancing imperceptibility and robustness, dependence on quality

Table 9. Illustrates the robustness comparison of the proposed scheme with other existing schemes.

Attacks	Specification	[7]	[8]	[13]	[17]	[25]	Proposed Scheme
No attack	–	1.0000	0.9988	0.9986	0.9985	0.9931	0.9992
Salt & pepper noise	0.001	0.9985	–	0.8761	0.9981	–	0.9985
	0.0001	–	–	0.9975	–	–	0.9990
Gaussian noise	0.001	0.9864	0.9830	–	0.992	0.8679	0.9970
	0.0001	–	–	0.9785	–	–	0.9987
Speckle noise	0.001	0.9981	–	0.9947	0.9995	0.9492	0.9984
Wiener filter	[2 2]	–	–	–	–	–	0.9826
	[3 3]	0.9682	–	–	–	0.9794	0.9658
Median filter	[2 2]	–	0.9076	0.9099	0.7549	–	0.9855
	[3 3]	0.9685	–	0.9290	0.7341	0.9818	0.9676
Gaussian low-pass filter	[2 2]		–	–	–	–	0.9786
	[3 3]	0.9864	–	–	–	0.9913	0.9962
Average filter	[3 3]	0.9294	–	–	–	0.8548	0.9458
Cropping	[10 10 200 200]	–	–	0.9009	–	–	0.9683
	2%	0.9823	–	–	–	–	0.9829
Rotation	2 degree	0.9496	–	–	–	–	0.9246
	1 degree	–	–	0.9308	–	–	0.9287
HE	–	0.9924	0.9982	0.6624	0.565	–	0.9938
Motion blur	Theta-4, len-7	0.8322	–	–	–	0.9357	0.7313
Sharpening	0.1	–	–	0.8042	0.8716	–	0.9616
	0.8	1.0000	–	–	–	0.9836	0.9934
Rescaling	0.5	–	–	–	–	–	0.7853
	2	–	0.9134	0.8242	–	–	0.9535
	4	0.9999	–	–	–	0.9923	0.9982
JPEG compression	Quality factor = 10	–	–	0.8994	–	–	0.9748
	Quality factor = 50	0.9998	–	0.9626	0.9825	0.9671	0.9938
JPEG2000 compression	CR = 12	0.9997	–	–	–	0.9785	0.9986

Table 10. Illustrates the capacity and time complexity comparison of the proposed scheme with other existing schemes.

Schemes	[7]	[8]	[13]	[17]	[25]	Proposed scheme
Capacity (bit/pixel)	0.25	0.015	0.25	0.25	0.015	0.25
Time Complexity	Embedding	–	–	0.2576 s	–	0.2348 s
	Encryption	–	–	1.3122 s	–	1.2522 s
	Decryption	–	–	0.3397 s	–	0.2395 s
	Extraction	–	–	0.1588 s	–	0.1390 s

training data for deep learning and key management issues in encryption.

5. Conclusion

In this paper, we implemented a state-of-the-art security scheme that has been specifically designed to protect sensitive DICOM patient data. This robust watermarking technique incorporates a range of advanced features, including watermark generation, turbo coding, and even the embedding of multiple watermarks. To ensure maximum security, the encoded e-patient record is embedded directly into the image watermark using a unique hybrid of RDWT-HD-RSVD techniques. Additionally, a nature-inspired particle swarm optimization (PSO) based optimization technique has been used to optimize the scaling factor. The optimization using PSO gives a better balance between the robustness and invisibility of the proposed algorithm. The watermarked image is encrypted further using a 3D chaotic encryption method to enhance the algorithm, which uses both position and value transformation for image encryption. Further, a noise removal technique based on DNN is utilized to enhance the extracted watermark image and make it less noisy, thus closer to the original watermark image. The proposed technique has undergone extensive testing to evaluate its imperceptibility, robustness and security, and it gives promising results when compared to other schemes. In future studies, it would be worthwhile to test the proposed approach for other applications, such as audio and video watermarking. Furthermore, the implementation of other optimization techniques could potentially enhance the efficiency of the system, especially in healthcare applications. In addition to this the proposed scheme can be used with other encryption schemes and provide more security and robustness to the medical images. In the future we can explore other optimization algorithms, refine the parameters and enhance the robustness of the proposed scheme using targeted deep learning components and the use of blockchain can further enhance the security.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Kumari Suniti Singh http://orcid.org/0000-0002-5957-862X

References

[1] Alarifi A, Sankar S, Altameem T, et al. A novel hybrid cryptosystem for secure streaming of high efficiency H.265 compressed videos in IoT multimedia applications. IEEE Access. 2020;8:128548–128573. doi:10.1109/ACCESS.2020.3008644

[2] Singh AK, Kumar B, Singh G, et al. Medical image watermarking: techniques and applications. Springer International Publishing; 2017.

[3] Salehi S, Abedi A, Balakrishnan S, et al. Coronavirus disease 2019 (COVID-19): a systematic review of imaging findings in 919 patients. Am J Roentgenol. 2020;215(1):87–93. doi:10.2214/AJR.20.23034

[4] Al-Afandy KA, El-Shafai W, El-Rabaie E-SM, et al. Robust hybrid watermarking techniques for different color imaging systems. Multimed Tools Appl. 2018;77(19):25709–25759. doi:10.1007/s11042-018-5814-y

[5] El-Shafai W, El-Rabaie S, El-Halawany MM, et al. Security of 3D-HEVC transmission based on fusion and watermarking techniques. Multimed Tools Appl. 2019;78(19):27211–27244. doi:10.1007/s11042-019-7448-0

[6] Li M, Poovendran R, Narayanan S. Protecting patient privacy against unauthorized release of medical images in a group communication environment. Comput Med Imaging Graph. 2005;29(5):367–383. doi:10.1016/j.compmedimag.2005.02.003

[7] Liu J, Huang J, Luo Y, et al. An optimized image watermarking method based on HD and SVD in DWT domain. IEEE Access. 2019;7:80849–80860. doi:10.1109/ACCESS.2019.2915596

[8] Ali M, Ahn CW, Pant M, et al. An image watermarking scheme in wavelet domain with optimized compensation of singular value decomposition via artificial bee colony. Inf Sci (Ny). 2015;301:44–60. doi:10.1016/j.ins.2014.12.042

[9] Qian X, Yang Q, Li Q, et al. A novel color image encryption algorithm based on three-dimensional chaotic maps and reconstruction techniques. IEEE Access. 2021;9:61334–61345. doi:10.1109/ACCESS.2021.3073514

[10] Momeni Asl A, Broumandnia A, Mirabedini SJ. Scale invariant digital color image encryption using a 3D modular chaotic map. IEEE Access. 2021;9:102433–49. doi:10.1109/ACCESS.2021.3096224

[11] Hossain MB, Rahman MT, Rahman ABMS, et al. A new approach of image encryption using 3D chaotic map to enhance security of multimedia component. International Conference on Informatics, Electronics & Vision (ICIEV), 2014, pp. 1–6.

[12] Anand A, Singh AK. Joint watermarking-encryption ECC for patient record security in wavelet domain. IEEE Multimed. 2020;27(3):66–75. doi:10.1109/MMUL.2020.2985973

[13] Anand A, Singh AK. An improved DWT-SVD domain watermarking for medical information security. Comput Commun. 2020;152:72–80. doi:10.1016/j.comcom.2020.01.038

[14] Thakur S, Singh AK, Kumar B, et al. Improved DWT-SVD-based medical image watermarking through Hamming code and chaotic encryption. Commun Signal Process Lect Notes Electr Eng. 2020;587:897–905. doi:10.1007/978-981-32-9775-3_80

[15] Wang J, Song X, El-Latif AAA. Single-objective particle swarm optimization-based chaotic image encryption scheme. Electronics (Basel). 2022;11(16):26–28.

[16] Aydilek IB. A hybrid firefly and particle swarm optimization algorithm for computationally expensive numerical problems. Appl Soft Comput. 2018;66: 232–249. doi:10.1016/j.asoc.2018.02.025

[17] Gangadhar Y, Akula VG, Reddy PC. An evolutionary programming approach for securing medical images using watermarking scheme in invariant discrete wavelet transformation. Biomed Signal Process Control. 2018;43:31–40. doi:10.1016/j.bspc.2018.02.007

[18] Anand A, Singh AK. Hybrid nature-inspired optimization and encryption-based watermarking for E-healthcare. IEEE Trans Comput Soc Syst.. 2023;10(4): 2033–2040. doi:10.1109/TCSS.2022.3140862

[19] Soualmi A, et al. Multiple blind watermarking framework for security and integrity of medical images in E-health applications. IJCVIP. 2021;11(1):1–16.

[20] Soualmi A, Alti A, Laouamer L. A new blind medical image watermarking based on Weber descriptors and arnold chaotic map. Arab J Sci Eng. 2018;43:7893–7905. doi:10.1007/s13369-018-3246-7

[21] Soualmi A, Alti A, Laouamer L. A novel blind watermarking approach for medical image authentication using MinEigen value features. Multimed Tools Appl. 2021;80:2279–2293. doi:10.1007/s11042-020-09614-x

[22] Amrit *P*, et al. Deep learning-based segmentation for medical data hiding with Galois field. Neural Comput Appl. 2023:1–16. doi:10.1007/s00521-023-09151-2

[23] Singh M, et al. Deep learning-based biometric image feature extraction for securing medical images through data hiding and joint encryption-compression. J Inf Secur Appl. 2023;79:103628.

[24] Singh HK, Singh AK. Using deep learning to embed dual marks with encryption through 3D chaotic map. IEEE Trans Consum Electron. 2024;70(1):3056–3063. doi:10.1109/TCE.2023.3286487

[25] Singh HK, Baranwal N, Singh KN, et al. GAN-based watermarking for encrypted images in healthcare scenarios. Neurocomputing. 2023;560:126853. doi:10.1016/j.neucom.2023.126853

[26] Ansari IA, Pant M. Multipurpose image watermarking in the domain of DWT based on SVD and ABC. Pattern Recognit Lett. 2017;94:228–236. doi:10.1016/j.patrec.2016.12.010

[27] "COVID-19 image data collection." Available from: https://github.com/ieee8023/covidchestxray-dataset.

[28] Available from: https://www.kaggle.com/datasets.