electronics

Article

A Robust Medical Image Watermarking Scheme Based on Nature-Inspired Optimization for Telemedicine Applications

Vijay Krishna Pallaw [1,†], Kamred Udham Singh [1,2,*,†], Ankit Kumar [3,†], Teekam Singh [4,†], Chetan Swarup [5,*,†] and Anjali Goswami [6]

[1] School of Computing, Graphic Era Hill University, Dehradun 248002, India
[2] Department of Computer Science and Information Engineering, National Cheng Kung University, Tainan 701, Taiwan
[3] Department of Computer Engineering and Application, GLA University, Mathura 281406, India
[4] School of Computer Science, University of Petroleum and Energy Studies, Dehradun 248007, India
[5] Department of Basic Science, College of Science and Theoretical Studies, Saudi Electronic University, Riyadh-Male Campus, Riyadh 13316, Saudi Arabia
[6] Department of Basic Sciences, College of Science & Theoretical Studies, Saudi Electronic University, Riyadh Female Campus, Riyadh 13316, Saudi Arabia
* Correspondence: 11004033@gs.ncku.edu.tw (K.U.S.); c.swarup@seu.edu.sa (C.S.)
† These authors contributed equally to this work.

Abstract: Medical images and patient information are routinely transmitted to a remote radiologist to assist in diagnosis. It is critical in e-healthcare systems to ensure that data are accurately transmitted. Medical images of a person's body can be used against them in many ways, including by transmitting them. Copyright and intellectual property laws prohibit the unauthorized use of medical images. Digital watermarking is used to prove the authenticity of the medical images before diagnosis. In this paper, we proposed a hybrid watermarking scheme using the Slantlet transform, randomized-singular value decomposition, and optimization techniques inspired by nature (Firefly algorithm). The watermark image is encrypted using the XOR encryption technique. Extensive testing reveals that our innovative approach outperforms the existing methods based on the NC, SSIM, and PSNR. The SSIM and NC values of watermarked image and extracted watermark are close to or equal to 1 at a scaling factor of 0.06, and the PSNR of the proposed scheme lies between 58 dB and 59 dB, which shows the better performance of the scheme.

Keywords: slantlet transform; RSVD; firefly algorithm; medical image watermarking

check for updates

Citation: Pallaw, V.K.; Singh, K.U.; Kumar, A.; Singh, T.; Swarup, C.; Goswami, A. A Robust Medical Image Watermarking Scheme Based on Nature-Inspired Optimization for Telemedicine Applications. *Electronics* **2023**, *12*, 334. https://doi.org/10.3390/electronics12020334

Academic Editor: Dong-Joo Kim

Received: 23 November 2022
Revised: 19 December 2022
Accepted: 27 December 2022
Published: 9 January 2023

1. Introduction

Patients, healthcare staff, businesses, and the development of a healthy society in smart cities will all benefit from the recent rise in popularity of electronic healthcare, which has gained a lot of support from the medical community over the past few years. With the growth of the Internet and other related technologies, it is easy to share audio-visual content such as music and video clips. With the expansion of computing, medical images are finding more and more uses. Academics use medical images for several things, including patient diagnosis and research into illness avoidance and treatment. When medical images are used in any form, including transfer, they are vulnerable to attack by unwanted parties [1]. Copyright and intellectual property can both be effectively safeguarded through the use of digital watermarking [2]. Diagnostic treatments such as X-ray, magnetic resonance imaging (MRI), computed tomography (CT), and ultrasound imaging, to name a few, use digital imaging technology in a big way and without permission. As a result, these medical images are widely circulated within the hospital intranet as well as online [3,4].

A powerful watermarking solution should be able to handle a lot of weighty problems and compelling requirements. Many other kinds of deficiencies can occur, such as those related to security, robustness, invisibility, capacity, and complexity [5]. Watermarks only work if the thing they are put on cannot be used to find out where the watermarked image came from. Based on this, watermarks are expected to be indecipherable to the human senses. Robustness in the context of watermarking means being able to find a watermark even when known attacks are happening. Ideally, a secure watermarking system would make it impossible to detect, remove, or alter the watermark [6]. The capacity of a material is the total quantity of data that can be hidden inside it. How challenging a watermarking technique is depends on how easy it is to insert or extract the watermark. In this context, using a watermarking methodology to ensure the content's integrity, protect it, and provide measuring tools for electronic health information can become a feasible solution [7]. Encryption-based watermarking is also becoming more popular as a way to make digital copies of medical content safer. Notably, the primary goal of the watermarking algorithm is to improve performance in terms of imperceptibility, watermark capacity, and robustness [8]. It is difficult to strike a balance between the competing demands that these three performance metrics place on the algorithm. To solve this problem, nature-based meta-heuristic schemes have been developed; one such scheme offers an excellent link between invisibility and robustness in an effective manner [9,10].

Yang [11] has recently developed a novel optimization method that he has coined the firefly algorithm. This algorithm is unique compared to others, such as the genetic algorithm (GA) and particle swarm optimization (PSO), as well as a few nature-inspired algorithms (NIAs). Numerous studies such as [10,12–15] have shown that the Firefly algorithm (FA) is superior to other NIAs, which was made possible by the widespread application of the FA across a variety of business sectors. The FA was used for the process of picture registration by Zhang et al. [11], who demonstrated that, in comparison to GA, PSO, and ABC, FA-based techniques offer the most accurate solution for the spatial transformation parameters [16]. Hassanzadeh et al. [13] segmented images using FA as an application in their research method. Based on the results of their study, an FA-based method is not only much better than Otsu's method but also much better than recursive Otsu [13]. Kanimozhi and Latha [14] have implemented the FA into the procedure for retrieving intelligent photos. The retrieval performance shows that the FA-based technique offers superior average precision and recall compared to other methods such as PSO, GA, support vector machine, and query point movement. This is demonstrated by the fact that the FA-based method produces superior results and has better retrieval performance. When it comes to the use of the FA in photo watermarking, the research that Ali and Ahn [17] and Mishra et al. [18] have carried out can be characterized as having an exploratory tone due to the nature of the questions it seeks to answer. Because of this, it is very important to find out if there are any other benefits to using the FA in photo watermarking.

The above study found that several image watermarking studies used NIAs and decomposition-based watermarking schemes have been used. Basically, these NIAs are used during the watermark embedding process to optimize the scaling factor. We have opted for the FA among the various available NIAs because of the number of individuals in the population, the number of iterations in a run, and the number of runs that were kept constant [11]. Moreover, SLT has superior smoothness and localization and can control two zeros in discrete time, and RSVD reduces computing complexity. Singular matrix alterations have little effect on invisibility performance, making it suitable for embedding [19]. To secure the watermark image, XOR encryption has been used. Major contributions of the proposed technique are as follows:

- The use of SLT and RSVD reduces the computational complexity and improves the robustness.
- The use of XOR encryption improves the security of inserted watermark.
- The FA provides a better optimized scaling factor in the least number of populations and iterations.

- We used the PSNR, SSIM, and NC values to design the fitness function for the FA, which improves the quality of both the embedded watermarked image and the extracted watermark.

The proposed approach comprises several significant new advances, which may be summarized in the following order: Section 2 provides an overview of watermarking schemes or techniques, setting the stage for our next work and providing context for the conversation that follows. Section 4 explains the suggested research agenda for watermark embedding and extraction. In Section 5, we will discuss the results. Section 6 contains the conclusion-related information.

2. Background and Motivation

Various watermarking techniques have been designed to add a watermark to patient images and may be found in the literature. The discussion will focus on state-of-the-art watermarking solutions that are based on optimization.

The watermarking method developed by Chaturvedi and Shukla is based on DWT, antagonistic grasshopper optimization, and sanitization encryption [20]. The cover image is optimized, and a method for encrypting images is utilized to transform the hidden image into bits for it to be accessible. The encryption process is currently determining the embedding position in the cover image. The utilization of the redistributed wavelet transform and singular value decomposition (SVD) in the watermarking method that was described by Ali et al. [17] makes it possible for the media data to be efficiently transmitted over the channel. The watermarking method turns this theoretical possibility into a practical one. After optimization, the approach embeds the sensitive data with the cover image. The provided method optimization is carried out using a scaling factor. Ahmadi et al. [21] utilized both PSO and singular value decomposition to create a technique for watermarking.

Pandey et al. suggested a copy protection method that operates in the lifting wavelet-SVD domain in their article [22]. The scrambling and optimization method is used in this technique to make it more secure and reliable. The Firefly algorithm is at the core of the watermarking system that Agarwal et al. have developed [18]. The system is able to covertly embed the watermark data into the cover image. It makes use of the optimum scaling factor. The authors describe the steps needed to make a watermarking method that works in the invariant wavelet-SVD domain. A PSO analysis has also been done to see how likely it is that a balance can be found between the system's robustness and its ability to stay out of sight. SVD is still afflicted by exorbitant prices, even though it has extensive usage in the industry that deals with watermarking [23]. The RSVD algorithm is utilized as the watermarking approach to cut costs without compromising on the quality of the end product [19].

Anand et al. [19] suggested a workable solution to the issue of how to keep confidential medical information hidden. As part of this method in the RDWT-RSVD domain, confidential marks are first hidden by being embedded in the host image, and then they are cloaked. In addition, compression is performed before encryption to overcome the authentication problem. Furthermore, Anand and Singh [24] have created a risk-free watermarking method that can be used to authenticate digital content related to medical care. This method can be utilized to certify medical-related websites and documents. If you use wavelet domain watermarking and then make a dual watermark, you can put an encoded media access control (MAC) address inside the watermarked image. A scaling factor is used by this cloud-based solution to add the final watermark to the host image. In addition to a hybrid of the integer wavelet transform (IWT) and the Schur-RSVD, a fuzzy inference method is used to compute the best scaling factor. This is done to keep the level of robustness high and reduce visual distortion as much as possible at the same time. Lastly, chaotic encryption is added to the image that has been flagged to make it safer while it is being sent over an open network. A watermarking method of copy protection was developed by Singh and Singh [25] in the transformation domain.

There are different transform domains, such as the lifting wavelet transform (LWT), the Hessenberg decomposition (HD), and the regularized singular value decomposition (RSVD), that are utilized for the transformation of host images. The watermarking embedding options and level of security are significantly constrained as a result. Watermarking technology has made some important strides in recent years, but this is still the case. Additionally, many processes do not do a good job of balancing the strength of their individual parts with the beauty of the things they make. This is problematic because, to maximize efficiency, an ideal balance is required.

3. Preliminaries

This section discusses the theories used in the proposed watermarking technique.

3.1. Slantlet Transform

The Slantlet transform (SLT) gives better localization and smoothness properties. It has the ability to control two zeros along with discrete time. To iterate, it does not use filter banks which results in better time localization banks. A parallel structure is implemented as a solution for the SLT of the filter bank [26]. The length of the SLT filter is much smaller compared to discrete wavelets. The length of the SLT filter is directly proportional to i when analyzing the signals of the SLT filter on the scale of i.

SThe LT filter bank uses $\theta_i(k)$, $\phi_i(k)$, and $\psi_i(k)$ banks use filters to construct their filter banks. The filter bank of the SLT has twice the number of channels concerning the filter bank. $Theta_i(k)$ is the adjacent filter to the low-pass filter. Down-sampling is used in a time-reversed manner for all filters, and the rest of the filters are done in the same way. The parameters $\alpha_{0,0}$, $\alpha_{0,1}$, $\alpha_{1,0}$, and $alpha_1, 1$, which are used to describe the filter $\phi_i(k)$, are as follows:

$$\theta_i(k) = \begin{cases} \alpha_{0,0} + \alpha_{0,1} n & for \text{ n} = 0, \cdots, 2^i - 1 \\ \alpha_{1,0} + \alpha_{1,1}(n-2) & for \text{ n} = 2^i, \cdots, 2^{i+1} - 1 \end{cases} \quad (1)$$

8 parameters are used to describe the $\phi_i(k)$, and $\psi_i(k)$ filters:

$$\phi_i(k) = \begin{cases} \beta_{0,0} + \beta_{0,1} n & for \text{ n} = 0, \cdots, 2^i - 1 \\ \beta_{1,0} + \beta_{1,1}(n-2) & for \text{ n} = 2^i, \cdots, 2^{i+1} - 1 \end{cases} \quad (2)$$

$$\psi_i(k) = \begin{cases} \gamma_{0,0} + \gamma_{0,1} n & for \text{ n} = 0, \cdots, 2^i - 1 \\ \gamma_{1,0} + \gamma_{1,1}(n-2) & for \text{ n} = 2^i, \cdots, 2^{i+1} - 1 \end{cases} \quad (3)$$

3.2. Firefly Algorithm

The Firefly Algorithm (FA) was first developed by [11] at Cambridge University. This is a new swarm intelligence optimization technique and is inspired by the flashing light of fireflies. Two basic functions of the flashlight are to attract mating partners and to attract potential prey. The FA is based on the assumption that the solution of an optimization problem can be perceived as fireflies whose "brightness" is proportional to the value of its objective function within a given problem space. In the FA, there are three idealized rules:

1. All fireflies are unisexual, so one firefly will be attracted to other fireflies regardless of their sex.
2. Attractiveness is proportional to their brightness; thus, for any two flashing fireflies, the less bright one will move.
3. If there are no fireflies brighter than a particular firefly, it will move randomly toward the brighter one.

In formulating the FA there are two important issues: the variation of light intensity and the formulation of the attractiveness. The attractiveness of a firefly is determined by its brightness which is proportional to the encoded objective function (Algorithm 1).

For maximization, the brightness of a firefly at a particular location x is proportional to the objective function. However, the attractiveness β is relative, it will vary with the distance r_{ij}, between the firefly i and firefly j. It also varies with the degree of light absorption by the medium.

Yang in [11] used a Cartesian distance $r_{i,j}$ where i and j are two individual fireflies at location x_i and x_j, respectively, as given by Equation (4)

$$r_{ij} = \|x_i - x_j\| = \sqrt{\sum_{k=1}^{c} \left(x_{i,k} - x_{j,k}\right)^2} \tag{4}$$

where $x_{i,k}$ is the kth component of the spatial coordinate x_i of ith firefly. The attractiveness β of a firefly is determined by using Equation (5)

$$\beta \leftarrow \beta_0 e^{-\gamma r_{ij}} \tag{5}$$

where β_0 is the attractiveness at $r_{i,j} = 0$ and γ is the light absorption coefficient of the medium. The movement of a firefly i is attracted to another more brighter firefly j and is given by Equation (6)

$$x_i \leftarrow x_i + \beta_0 e^{-\gamma r_{ij}} \left(x_i - x_j\right)^2 + \alpha u_i \tag{6}$$

where the random walk parameter u_i is evaluated by Equation (7).

$$u_i = \left(rnd1 - \frac{1}{2}\right) \tag{7}$$

If there are no fireflies brighter than a particular firefly i with maximum objective value then i will move randomly according to the Equation (8).

$$x_{i^{max}} \leftarrow x_{i^{max}} + \alpha u_{i^{max}} \tag{8}$$

In this case the random walk parameter $u_{i^{max}}$ is evaluated by (9)

$$u_{i^{max}} = \left(rnd2 - \frac{1}{2}\right) \tag{9}$$

where $rnd1 \approx U(0,1)$ and $rnd2 \approx U(0,1)$ are random numbers obtained from uniform distribution. The objective function $f(x)$ (Equation (12)) influences or determines the brightness of the firefly. The perceptual quality of an image is measured using the peak signal-to-noise ratio (PSNR) (Equation (13)), the structural similarity index measure (SSIM) (Equation (15)), and the normalized correlation (NC) (Equation (14)). In our case, the PSNR is used to measure the perceptual quality of a watermarked image, whereas the SSIM and NC are used to measure the perceptual quality of an extracted watermark. The value $\alpha = 0.013$ is used as a balancing parameter to improve perceptual quality. The output of the fitness function is used as an input parameter ($\Delta = 0.02$) when the embedding and extraction process is performed.

$$fitness = \frac{(PSNR \times SSIM)}{\alpha} + \frac{NC}{\alpha} \tag{10}$$

Algorithm 1: Firefly algorithm to optimize MSF.

```
Input: An objective function
Input: Firefly initial population
Output: Optimized value of MSF ($\Delta$)
BEGIN:
while max population size
    for i = 1 to length of firefly population
        for j = 1 to length of firefly population
            move $j$th $\leftarrow$ $i$th if $j$th firefly is more attractive
            than $i$th
            update objective function and the value of $\Delta$
        end for
    end for
    get current global best solution.
end while
END
```

3.3. Randomized Singular Value Decomposition (RSVD)

Randomized singular value decomposition was presented by Zhang et al. [27] to perform lossless compression, reformation, classification, and target detection with hyperspectral data. The mathematical definition of RSVD is given in Equation (11).

$$\hat{Z} = \hat{X}\hat{\sum}\hat{Y}^T \tag{11}$$

where $\hat{X}$ and $\hat{Y}$ are orthonormal matrices and $\hat{\sum}$ is column vector of orthonormal matrices. The RSVD examines approximate matrix factorization using random projections (Equation (11)) by dividing the process into two phases. In the first step, random sampling is used to generate a reduced matrix whose range approaches the range of Z. The final phase involves the factorization of the reduced matrix. Using the initial stage on matrix Z, the orthonormal column matrix Q ($Q^T Z \epsilon R^{l \times m}$) is determined

$$Y = Z\Omega \tag{12}$$

where Ω is an identically distributed randomized matrix.

4. Proposed Work

In the current work, the following SLT-RSVD-based watermarking technique is employed to investigate the impact of the scaling factor on PSNR. The images are assessed for visual quality using the PSNR given in Equation (13), the NC (Equation (15)), and the SSIM given in Equation (16).

4.1. Watermark Entrenching Scheme

In this subsection, we discussed the watermark entrenching procedure (shown in Figure 1). The step-wise process to entrench the watermark is given in Algorithm 2. In the first step of the watermark embedding process, the cover image is transformed using an SLT. The watermark image is embedded in a lower-frequency sub-band. In the second step, the coefficients of the lower-frequency sub-band are converted into blocks of size 3 × 3. In the third step, each block undergoes the RSVD putrefaction process to obtain the U, S, and V matrices, where U and V are unitary matrices and S is a singular matrix. In the fourth step, the watermark bits are encrypted using the XOR encryption technique. The watermark bits are entrenched into the singular matrix in the fifth step using an additive quantization mechanism (given in step 9) and scaling factor Δ. The value of Δ is obtained using the Firefly algorithm. In the sixth step, inverse RSVD putrefaction is implied to obtain the blocks. Finally, in the seventh step, the inverse Slantlet transform is employed to get the watermarked image.

Algorithm 2: The step-wise process to entrench the watermark

```
Input: $h\_image$ (Cover/Host Image), $w\_image$ (Watermark Image), an
    encryption key (k), and the optimized value of $\Delta$.
Output: Watermarked image ($h\_image''$)
BEGIN:
    coef = slt($h\_image$)
    block = getBlock(coef, blockNumber, blockSize)
    $[U,S,V]$ = rsvd(block)
    encrypted = $w\_image \oplus$ k
    $S' = S + \Delta * W_i$
    $block'$ = irsvd($U$, $S'$, $V$)
    $h\_image'$ = islt(blocks)
    $h\_image''$ = reshape($h\_image'$)
END
```

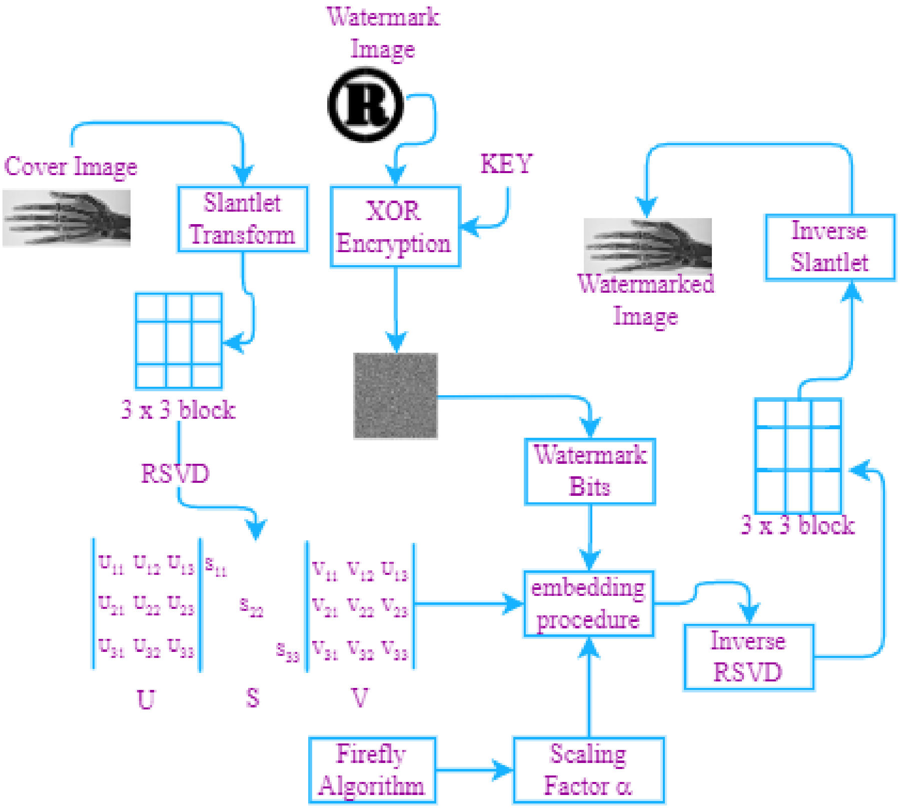


Figure 1. Block diagram: watermark entrenching process.

4.2. Watermark Extraction Scheme

This section describes the watermark extraction technique. Figure 2 depicts the watermark extraction process. In Algorithm 2, the technique for embedding the watermark is outlined in detail. Algorithm 3 takes h'_image, the encryption key, and the multi-valued scaling factor (MSF) as input and outputs a watermark image. In step one of the watermark extraction process, the watermarked image is transformed using SLT to obtain the coefficients of the lower-frequency sub-band. In step two, the coefficients of the lower-frequency sub-band are transformed into blocks of size 3 × 3. Each block proceeds through the RSVD putrefaction process in the third phase to produce U', S', and V'. Step four involves utilizing the equation given in step eight to retrieve the watermark bits. Finally, in step six, the watermark bits are deciphered to get the extracted watermark.

Algorithm 3: The step-wise process to extract the watermark

```
Input: $h'\_image$ (Watermarked Image), an encryption key (k), and
    the optimized value of $\Delta$.
Output: W′ (Extracted Watermark Image)
BEGIN:
    coef = slt($h'\_image$)
    block = getBlock(coef, blockNumber, blockSize)
    $[U', S', V']$ = rsvd(block)
    $W' = \begin{cases} 1, & \text{if } S' + \Delta \leq \lambda \\ 0, & \text{Otherwise} \end{cases}$
    $W''$ = $W'$ $\oplus$ $k$
    Obtain extracted watermark as ($W''$)
END
```

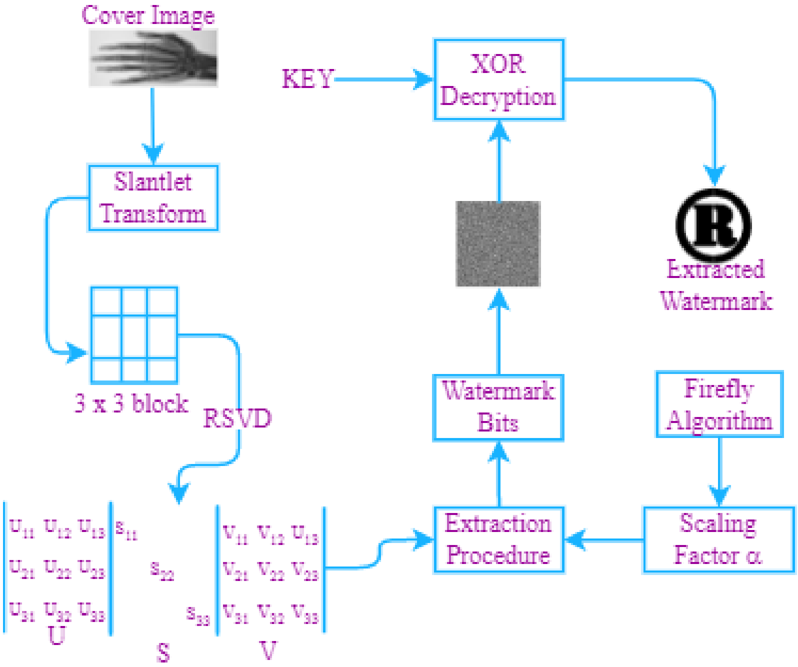


Figure 2. Block diagram: watermark extraction process.

4.3. Analysis of Imperceptibility Based on SSF

The effectiveness of watermarking is determined by a number of parameters, two of which are particularly important: imperceptibility and resilience. On the other hand, both of these ideas are incompatible. To put it another way, the robustness of anything decreases its imperceptibility, and vice versa [28]. In this investigation, a method based on SLT-RSVD is proposed for determining the single-valued scaling factor (SSF) to strike a balance between the two ideas being discussed.

An SSF may be inappropriate for perturbing all of the cover image's coefficients in the transform domain. This is because various spectrum components may have varying levels of tolerance for the alteration that is being generated. To integrate the watermark energy into the cover image, they advise using an MSF rather than an SSF. They added that the nature and intensity of the image might affect how MSFs are determined [28].

Moreover, a crucial part of watermarking success is the scaling factor Δ, which is used to modify the value of the second element in the first column of the S matrix during the embedding phase. Selecting a very small scaling factor increases imperceptibility but reduces robustness. Another possible explanation is that a higher scaling factor leads to a higher ratio of image deterioration while watermarking [29]. Therefore, finding the best scaling factor based on the standard deviation is important. The proposed method uses the threshold values stored in each firefly as a scaling factor during the embedding stage.

The parameters of the proposed scheme are initially established during the optimization stage. The population size is set to 10, and β_0 and γ are in between 0 and 1. The watermarking system's imperceptibility and robustness are considered when establishing numerous scaling factors. The PSNR, SSIM, and NC are used to gauge the imperceptibility of an image. These are the most used distortion measures [30].

$$\mathrm{PSNR} = 10 \ \times \log_{10}\left(\frac{255^2}{MSE}\right) \tag{13}$$

$$MSE = \frac{1}{M \times N}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}(C(x,y) - CW(x,y))^2 \tag{14}$$

where C stands for the image in its unaltered, unmodified form and CW stands for the image in its altered, watermarked form.

$$\mathrm{NC} = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N} \mathrm{w(x,y)\ x\ w'(x,\ y)}}{\sum_{x=1}^{M}\sum_{y=1}^{N} w^2(x,y)} \tag{15}$$

where w stands for original watermark and w' stand for extracted watermark.

$$SSIM = \frac{(2\mu_w\mu_{w'} + C_1)(2\sigma_{ww'} + C_2)}{(\mu_w^2 + \mu_{w'}^2 + C_1)(\sigma_w^2 + \sigma_{w'}^2 + C_1)} \tag{16}$$

where σ_w and σ_w' represent the covariance of the original watermark and the extracted watermark, respectively, and C_1 and C_2 are constants. μ_w corresponds to the mean of the original watermark, and $\mu_{w'}$ corresponds to the mean of the recovered watermark.

Before assessing the effects of MSF over the robustness and imperceptibility on watermarked images with different image processing attacks.

We studied the effects of the SF on the PSNR and SSIM to assess the robustness and imperceptibility. In order to assess the imperceptibility of watermarked images, PSNR is used. The plot in Figure 3 depicts the effect of the SF on the PSNR. In this plot, the scaling factor Δ ranges from 0.01 to 0.06. In this figure, we can observe almost straight lines in the PSNR with respect to the SF, except for the Gaussian filter attack which largely influences the PSNR value. Salt and pepper noise is the second most influencing attack that can be observed in this plot. The least influencing attacks are JPEG and sharpening since the almost straight line can be seen in the plot. Therefore, we can consequently state that the PSNR and Δ have an inverse relationship for the watermarked image. Furthermore, the PSNR is constant with respect to Δ for all attacked images.

The observed mean PSNR value from the experiment is shown in Table 1. A small change in the PSNR can be seen in this table. With regard to SF (Δ), the PSNR value is primarily influenced by the Gaussian filter, whereas JPEG compression and sharpening attack have the least impact.

The SSIM is used to examine the resilience of extracted watermarks. The graph in Figure 4 illustrates the impact of Δ on the SSIM. In this plot, the SF significantly impacts the SSIM at a certain point in time, but afterward, the value becomes stabilized. This is true for all attacks without any exception. Therefore, the range of SF is an adequate range for determining MSFs based on the type and severity of the considered attack for the attacks employed in this simulation.

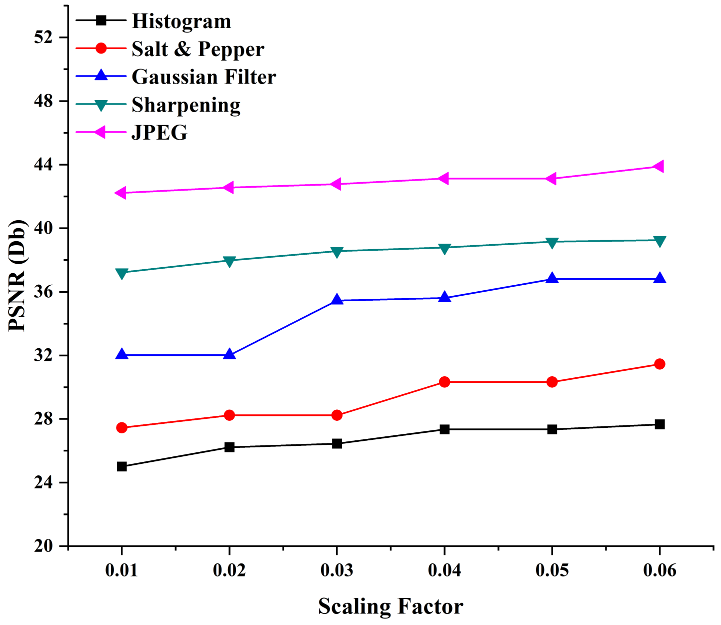


Figure 3. Effect of SF (Δ) on the PSNR.

Table 1. Effect of SF (Δ) on the PSNR.

SF	Histogram	Salt and Pepper	Gaussian Filter	Sharpening	JPEG
0.01	25.0125	27.4512	32.0125	37.2235	42.2234
0.02	26.2323	28.2356	32.0126	37.9815	42.5678
0.03	26.4512	28.2365	35.4589	38.5642	42.7787
0.04	27.3521	30.3312	35.6201	38.7886	43.1256
0.05	273528	30.3312	36.8011	39.1563	43.1187
0.06	27.6621	31.4589	36.8011	39.2563	43.8920

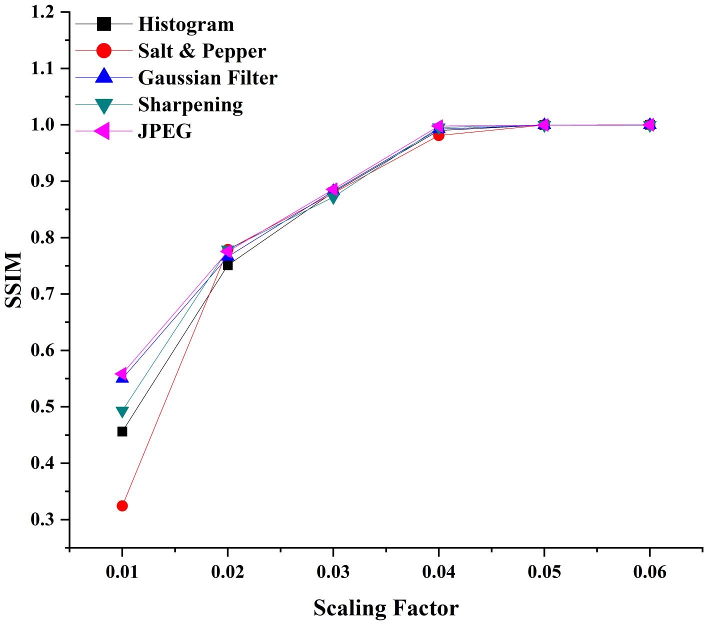


Figure 4. Effect of SF (Δ) on the SSIM.

Table 2 presents the mean SSIM of all the X-ray images used in our simulation. In this table, the observed SSIM values are presented with respect to the range of the SF on various assaults employed in our experiment. The SF has a significant and equal impact on SSIM on all image processing assaults.

Table 2. Effect of SF (Δ) on the SSIM.

SF	Histogram	Salt and Pepper	Gaussian Filter	Sharpening	JPEG
0.01	0.4563	0.3245	0.5501	0.4933	0.5586
0.02	0.7512	0.7789	0.7663	0.7789	0.7756
0.03	0.8809	0.8791	0.8828	0.8719	0.8856
0.04	0.9901	0.9812	0.9923	0.9956	0.9979
0.05	0.9998	0.9998	0.9996	0.9998	0.9997
0.06	1.0000	1.0000	0.9997	0.9999	1.0000

In the above study of the SSF, we found that the SF inversely affects the imperceptibility of the cover image and directly affects the robustness of the extracted image in the given range of the SF. The above observation shows that the objective function used to embed the watermark has to consider the PSNR and SSIM to optimize the values of the SF. Consequently, this objective function is applied to optimize the value of MSFs (Δ) to achieve the best results. Therefore, we used this range for the SF in all calculations. Thus, our findings are consistent as reported in [28]. In Table 3, we used the PSNR, SSIM, and NC to analyze the watermarked image and the SSIM and NC of extracted watermarks. The PSNR value is between 58 dB and 59 dB, indicating that the suggested method outperformed at MSF 0.06. The parameters NC and SSIM are close to or equal to 1 for the watermarked image, indicating that the proposed technique has better imperceptibility. We have also calculated the NC and SSIM of the extracted watermark, which are close to or equal to 1, meaning the quality of extracted watermark is significant.

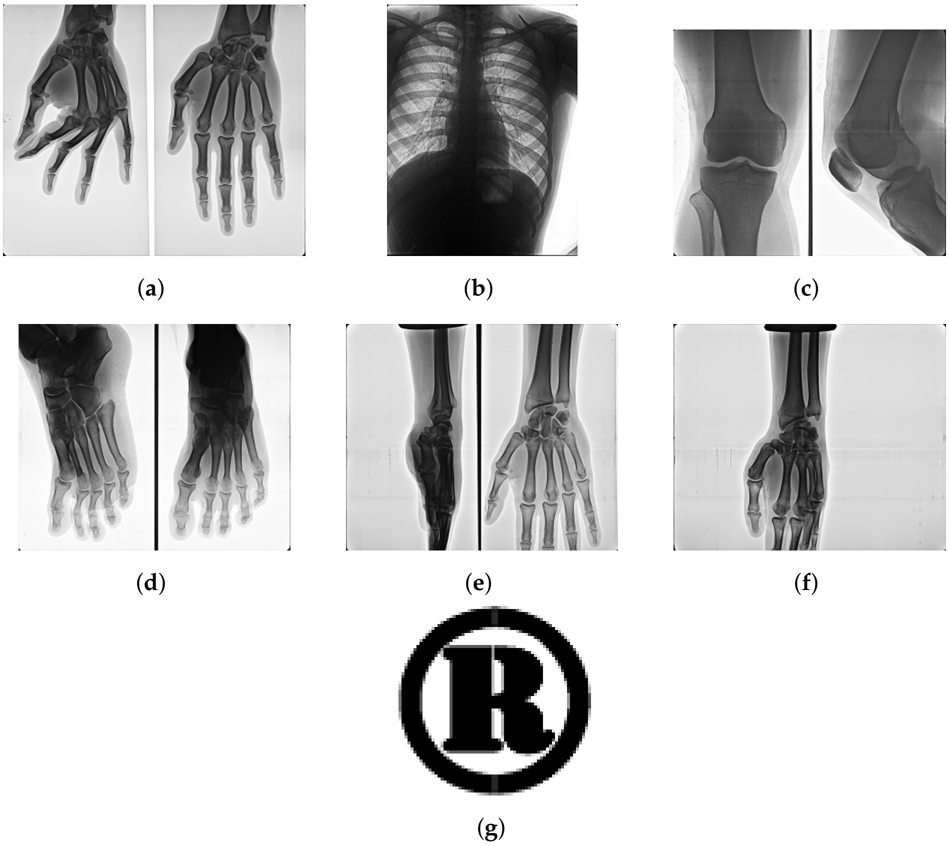
Table 3. Quality evaluation parameters of the watermarked image and the extracted watermark.

Evaluation Matrics	(a)	(b)	(c)	(d)	(e)	(f)	(g)
Watermarked Image	PSNR	58.6123	58.6122	58.6122	58.6118	58.6121	58.6121
	SSIM	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
	NC	0.9991	0.9991	0.9992	0.9991	0.9993	0.9991
Extracted Watermark	SSIM	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
	NC	0.9988	0.9989	0.9987	0.9988	0.9986	0.9987

5. Results and Discussion

This section examines the anticipated work and discusses the expected outcome. Various X-ray image types and binary watermark images were employed to evaluate the effectiveness of the suggested approach. In the proposed layout, the selected cover medical image dimensions are 700 × 600 pixels and 64 × 64 pixels for the watermark image. The X-ray medical images employed in this experiment are accessible to the public domain (The National Library of Medicine presents MedPix). The experimental versions of the medical images can be seen in Figure 5a–f, and the watermark image can be seen in Figure 5g. The information on the patient has been purposefully removed to protect their confidentiality and safety.

Moreover, this section also offers experimental data demonstrating the performance of the proposed technique in terms of a variety of watermarking features, including imperceptibility, robustness, security, and payload. Experiments were carried out on Intel(R) Core (TM) i5-8300H CPU running at 2.30 GHz, a 64-bit processor, 8.00 GB of RAM, and the Windows 10 operating system. As their primary instrument for conducting experiments, we utilized MATLAB R2015b. These trials were carried out to demonstrate how efficiently the watermarking scheme works.



(**a**) (**b**) (**c**)

(**d**) (**e**) (**f**)

(**g**)

Figure 5. Watermark Images used for experiment. (**a**–**f**) The experimental versions of the medical images, (**g**) the watermark image.

The PSNR and SSIM values of the watermarked images that were extracted from the watermark are listed in Table 3. The maximum values of PSNR and SSIM that could be calculated were 58.6123 and 1.00, respectively. This demonstrates the extreme degree of secrecy that a watermark exhibits within an image that has been watermarked, as the watermark is virtually undetectable. In addition to this, the process of removing the watermark is successful in its application. This is demonstrated by the non-watermarked versions of the images' NC values after the watermarks have been removed. The fact that the NC values are reasonably near to one is a strong indicator that the extraction method is functioning appropriately.

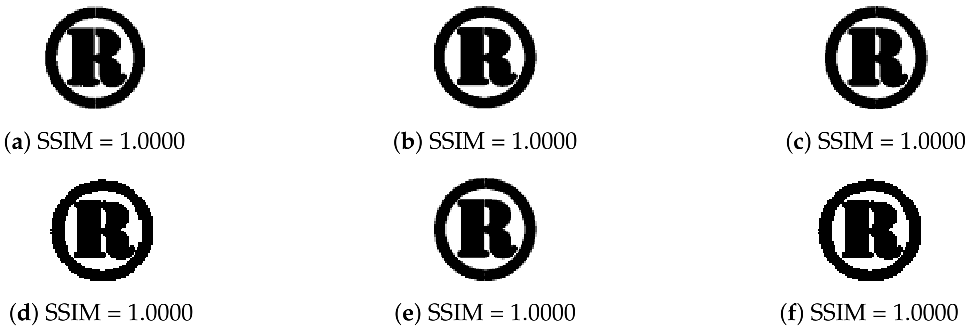
5.1. Robustness Analysis

Additionally, we outline below a number of tests that were carried out and their outcomes to evaluate the effectiveness of the multi-objective FA-SLT-RSVD-based watermarking system. After using a histogram equalization image processing attack, Table 4 demonstrates the SSIM values of retrieved watermarks from all of the cover medical X-ray pictures used in our experiment. This table makes it evident that the extracted watermark is significantly impacted when the Δ ranges from 0.01 to 0.03, while the range of Δ between 0.04 and 0.06 has the least impact on the extracted watermark. Therefore, we can conclude that our algorithm gives better results robustness.

The extracted watermark from a deformed watermarked image (shown in Figure 6) is illustrated in Table 5 by adding noise. The salt and pepper attack is also a common image distortion attack (shown in Figure 7). The SSIM values presented in the table below are largely affected when the MSF is 0.01. The range of the SSIM is from 0.3235 to 0.3298, while the range of the SSIM is from 0.7783 to 0.7799 when the MSF is 0.01 and 0.02, respectively. It shows that the quality of the extracted watermark is much more distorted when the MSF is low and better when MSF is high. Thus, we can say that the results gained from the anticipated watermarking scheme described the robustness against noise attacks.

Table 4. The SSIM values of the extracted watermark after a histogram equalization attack.

	Image Name					
SF	**(a)**	**(b)**	**(c)**	**(d)**	**(e)**	**(f)**
0.01	0.4563	0.4553	0.4563	0.4534	0.4566	0.4566
0.02	0.7512	0.7512	0.7522	0.7532	0.7522	0.7512
0.03	08809	0.8811	0.8809	0.8811	0.8809	0.8809
0.04	0.9901	0.9901	0.9901	0.9901	0.9901	0.9901
0.05	0.9998	0.9998	0.9998	0.9998	0.9998	0.9998
0.06	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000



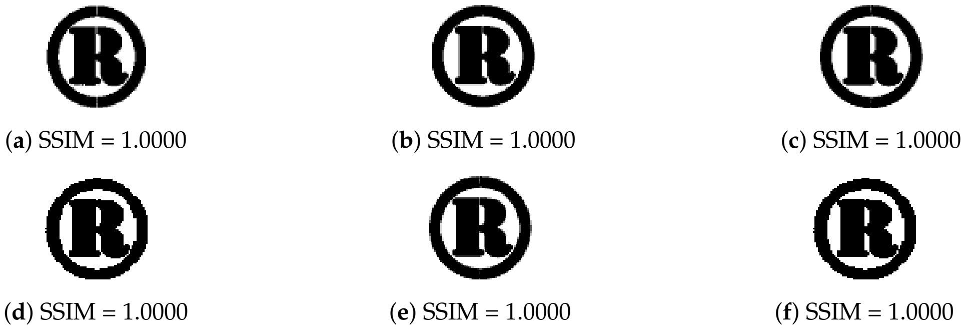
(**a**) SSIM = 1.0000 (**b**) SSIM = 1.0000 (**c**) SSIM = 1.0000

(**d**) SSIM = 1.0000 (**e**) SSIM = 1.0000 (**f**) SSIM = 1.0000

Figure 6. Extracted watermark after a histogram equalization attack.

Table 5. The SSIM values of the extracted watermark after a salt and pepper attack.

	Image Name					
SF	**(a)**	**(b)**	**(c)**	**(d)**	**(e)**	**(f)**
0.01	0.3245	0.3234	0.3242	0.3298	0.3245	0.3235
0.02	0.7789	0.7799	0.7783	0.7789	0.7799	0.7788
0.03	0.8791	0.8796	0.8789	0.8795	0.8797	0.8792
0.04	0.9812	0.9823	0.9823	0.9825	0.9823	0.9812
0.05	0.9998	0.9998	0.9998	0.9998	0.9998	0.9998
0.06	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000



(**a**) SSIM = 1.0000 (**b**) SSIM = 1.0000 (**c**) SSIM = 1.0000

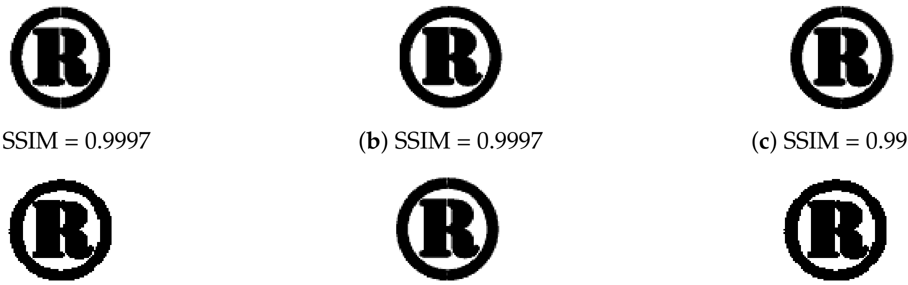
(**d**) SSIM = 1.0000 (**e**) SSIM = 1.0000 (**f**) SSIM = 1.0000

Figure 7. Extracted watermark after a salt and pepper attack.

The image is distorted because of the signals in the transmission channels. The watermark image is also interpolated to prevent attacks based on distortion or signal processing. The term filter attack refers to a specific type of attack in the realm of image processing. As part of our experiment, we launched a filtering attack to test how well the proposed watermarking scheme works. The SSIM values of the extracted watermark (shown in Figure 8) when employing a filtering attack are shown below in Table 6. The quality of the extracted watermark can be assessed by observing the SSIM values for different ranges of Δ. The SSIM values are least affected by the MSF.

Table 6. The SSIM values of the extracted watermark after a Gaussian filter attack.

	Image Name					
SF	**(a)**	**(b)**	**(c)**	**(d)**	**(e)**	**(f)**
0.01	0.5501	0.5501	0.5501	0.5501	0.5501	0.5501
0.02	0.7663	0.7663	0.7663	0.7663	0.7663	0.7663
0.03	0.8828	0.8828	0.8828	0.8828	0.8828	0.8828
0.04	0.9923	0.9923	0.9923	0.9923	0.9923	0.9923
0.05	0.9996	0.9996	0.9996	0.9996	0.9996	0.9996
0.06	0.9997	0.9997	0.9997	0.9997	0.9997	0.9997



(**a**) SSIM = 0.9997 (**b**) SSIM = 0.9997 (**c**) SSIM = 0.9997

(**d**) SSIM = 0.9997 (**e**) SSIM = 0.9997 (**f**) SSIM = 0.9997

Figure 8. Extracted watermark after a Gaussian filter attack.

Patients were diagnosed online during the epidemic. Consequently, medical images were regularly sent from one source to another via various communication routes. For all intents and purposes, this procedure involved the compression and format conversion of medical photographs. The quality of converted medical images is always lower than the original. As a result, JPEG compression has emerged as a standard and indispensable tool in image processing. Therefore, the image compression attack becomes essential to test the robustness of our proposed watermarking system. Table 7 exhibits the SSIM values of the extracted watermark from all six X-ray medical images after employing a JPEG compression attack. The SSIM values for each extracted watermark range from 0.55 to 1.0 for all values of Δ. For MSFs ranging from 0.03 to 0.04, the SSIM values of the extracted watermark are from 0.9969 to 0.9997. The SSIM values closer to 1 show that the watermark is completely extracted from the watermark image when employing JPEG attacks (as shown in Figure 9a–f). This shows the robustness of our watermarking system.

Table 7. The SSIM values of extracted watermark after a JPEG compression attack.

	Image Name					
SF	**(a)**	**(b)**	**(c)**	**(d)**	**(e)**	**(f)**
0.01	0.5586	0.5591	0.5587	0.5586	0.5586	0.5588
0.02	0.7756	0.7759	0.7756	0.7751	0.7756	0.7758
0.03	0.8856	0.8855	0.8857	0.8851	0.8856	0.8856
0.04	0.9979	0.9971	0.9969	0.9979	0.9969	0.9979
0.05	0.9997	0.9997	0.9997	0.9997	0.9997	0.9997
0.06	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000

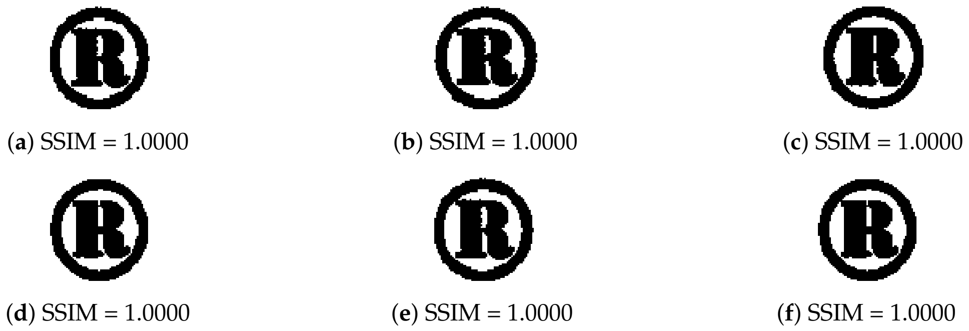

(**a**) SSIM = 1.0000 (**b**) SSIM = 1.0000 (**c**) SSIM = 1.0000
(**d**) SSIM = 1.0000 (**e**) SSIM = 1.0000 (**f**) SSIM = 1.0000

Figure 9. Extracted watermark after a JPEG compression attack.

5.2. Comparison of Proposed Scheme with Existing Schemes

We have carried out a number of experiments to evaluate the practicability of the method that has been outlined above. To evaluate the performance of the proposed scheme we have presented a comparison of the SSIM and NC values with existing similar approaches presented in [7,10,31,32] of the extracted watermark without any image processing attacks (shown in Table 8). The FA-SLT-RSVD gives a more optimal solution considering various optimization in watermarking techniques. The proposed scheme ensures higher imperceptibility of the extracted watermark. The SSIM values obtained by our scheme are much better than the scheme proposed in [7]. Additionally, the NC value is higher than all the existing schemes except [10], which shows the better performance of the watermarking technique.

Table 8. The NC and SSIM values of the extracted watermark.

	Proposed Work	[7]	[10]	[31]	[32]
SSIM	1.0000	0.9961	-	-	-
NC	0.9988	0.9985	0.9993	0.9869	1.0000

To evaluate the comparative performance of the technique under several image processing attacks with existing similar approaches [7,10,31,32], a comparison table has also been presented in Table 9. The SSIM values obtained by the proposed work under histogram equalization attack, salt and pepper attack, Gaussian noise attack, and JPEG compression attack are 1, 1, 0.9997, and 1, respectively, which is higher compared to other schemes. The higher SSIM values show robustness against image distortion. The proposed scheme achieves better performance when the NC values are compared with existing schemes. The NC values obtained by our scheme under histogram equalization attack, salt and pepper attack, Gaussian noise attack, and JPEG compression attack are 0.6221, 0.9879, 0.9889, and 0.9941, respectively. The NC value obtained shows good imperceptibility against all attacks except [10,32] in a histogram equalization attack. On the basis of the above comparison and analysis, it has been observed that our scheme performs better than existing schemes.

Table 9. Comparative analysis of the proposed scheme.

Attack	**Proposed Work**		[7]		[10]		[31]		[32]	
	SSIM	**NC**	**SSIM**	**NC**	**SSIM**	**NC**	**SSIM**	**NC**	**SSIM**	**NC**
Histogram Equalization	1.0000	0.6221	0.9961	0.5650	-	0.7223	-	-	-	-
Salt and Pepper	1.0000	0.9879	0.9923	0.9981	-	09251	-	0.9938	0.9260	0.9997
Gaussian Noise	0.9997	0.9889	0.9816	0.9920	-	0.5918	-	0.9738	0.9314	0.9997
JPEG Compression	1.0000	0.9941	0.9910	0.9825	-	-	-	-	0.9314	0.9997

6. Conclusions

The proposed watermarking scheme uses the Slantlet transform, randomized-singular value decomposition, and nature-inspired optimization method. It successfully enhanced the authenticity of X-ray images. A series of evaluation tests are conducted, and the results are compared to predetermined standards to ascertain the system's imperceptibility and robustness. Our research demonstrates that the suggested watermarking procedure achieves lower distortion than the most cutting-edge methods. The proposed watermarking method produces high NC, PSNR, and SSIM values of watermarked images, making it suitable for medical images. The SSIM and NC values of extracted watermark are close to or equal to 1 at a scaling factor of 0.06, which shows the better performance of the scheme. The watermark is successfully retrieved after several image processing attacks (i.e., JPEG compression, salt and pepper noise, Gaussian filtering, or histogram equalization).

The scope of this research is limited to grayscale medical images. It is essential to carry out operational trials prior to implementing the watermark system in a fully working e-healthcare system. In the future, more NIAs will be employed, and our method will also be evaluated on different medical image formats.

Author Contributions: Methodology, K.U.S.; Software, V.K.P.; Validation, A.K. and C.S.; Investigation, T.S. Data curation, A.G.; Writing—review & editing, A.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

SVD	Singular Value Decomposition
SLT	Slantlet Transform
RSVD	Randomized-Singular Value Decomposition
FA	Firefly Algorithm
MRI	Magnetic Resonance Imaging
CT	Computed Tomography
DICOM	Digital Imaging and Communications in Medicine
JPEG	Joint Photographic Experts Group
SSIM	Structural Similarity Index Metric
PSNR	Peak Signal-to-Noise Ratio
NC	Normalized Correlation
NIA	Nature Inspired Algirthm
MSF	Multi-Valued Scaling Factor
SSF	Single-Valued Scaling Factor
LWT	Lifting Wavelet Transform
IWT	Integer Wavelet Transform
PSO	Particle Swarm Optimization
MRI	Magnetic Resonance Imaging
GA	Genetic Algorithm
ABC	Artificial Bee Colony Algorithm
DWT	Discrete Wavelet Transform
MAC	Media Access Control
HD	Hessenberg Decomposition

References

1. Kumar, L.; Singh, K.U. Color Ultrasound Image Watermarking Scheme Using FRT and Hessenberg Decomposition for Telemedicine Applications. *JUCS J. Univers. Comput. Sci.* **2022**, *28*, 882–897. [CrossRef]
2. Altay, Ş.Y.; Ulutaş, G. Self-adaptive step firefly algorithm based robust watermarking method in DWT-SVD domain. *Multimed. Tools Appl.* **2021**, *80*, 23457–23484. [CrossRef]
3. Favorskaya, M.; Savchina, E.; Gusev, K. Feature-based synchronization correction for multilevel watermarking of medical images. *Procedia Comput. Sci.* **2019**, *159*, 1267–1276. [CrossRef]
4. Liu, X.; Lou, J.; Fang, H.; Chen, Y.; Ouyang, P.; Wang, Y.; Zou, B.; Wang, L. A Novel Robust Reversible Watermarking Scheme for Protecting Authenticity and Integrity of Medical Images. *IEEE Access* **2019**, *7*, 76580–76598. [CrossRef]
5. Mousavi, S.M.; Naghsh, A.; Abu-Bakar, S.A.R. Watermarking techniques used in medical images: a survey. *J. Digit. Imaging* **2014**, *27*, 714–729. [CrossRef]
6. Qasim, A.F.; Meziane, F.; Aspin, R. Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review. *Comput. Sci. Rev.* **2018**, *27*, 45–60. [CrossRef]
7. Anand, A.; Singh, A.K. Hybrid Nature-Inspired Optimization and Encryption-Based Watermarking for E-Healthcare. *IEEE Trans. Comput. Soc. Syst.* **2022**, 1–8. [CrossRef]
8. Anand, A.; Singh, A.K. Watermarking techniques for medical data authentication: A survey. *Multimed. Tools Appl.* **2021**, *80*, 30165–30197. [CrossRef]
9. Ali, M.; Ahn, C.W.; Pant, M.; Siarry, P. An image watermarking scheme in wavelet domain with optimized compensation of singular value decomposition via artificial bee colony. *Inf. Sci.* **2015**, *301*, 44–60. [CrossRef]
10. Anand, A.; Singh, A.K. RDWT-SVD-Firefly Based Dual Watermarking Technique for Medical Images (Workshop Paper). In Proceedings of the 2020 IEEE Sixth International Conference on Multimedia Big Data (BigMM), New Delhi, India, 24–26 September 2020; pp. 366–372. [CrossRef]
11. Yang, X.S. *Nature-Inspired Metaheuristic Algorithms*; Luniver Press: Frome, UK, 2008.
12. Zhang, Y.; Wu, L. Rigid Image Registration based on Normalized Cross Correlation and Chaotic Firefly Algorithm. *Int. J. Digit. Content Technol. Its Appl.* **2012**, *6*, 129–140.
13. Hassanzadeh, T.; Vojodi, H.; Moghadam, A.M.E. An image segmentation approach based on maximum variance Intra-cluster method and Firefly algorithm. In Proceedings of the 2011 Seventh International Conference on Natural Computation, Shanghai, China, 26–28 July 2011; Volume 3, pp. 1817–1821. [CrossRef]
14. Kanimozhi, T.; Latha, K. An integrated approach to region based image retrieval using firefly algorithm and support vector machine. *Neurocomputing* **2015**, *151*, 1099–1111. [CrossRef]
15. Sharma, A.; Chaturvedi, R.; Bhargava, A. A novel opposition based improved firefly algorithm for multilevel image segmentation. *Multimed. Tools Appl.* **2022**, *81*, 15521–15544. [CrossRef]
16. Draa, A.; Benayad, Z.; Djenna, F.Z. An opposition-based firefly algorithm for medical image contrast enhancement. *Int. J. Inf. Commun. Technol.* **2015**, *7*, 385–405. [CrossRef]
17. Ali, M.; Ahn, C.W. Comments on "Optimized gray-scale image watermarking using DWT-SVD and firefly algorithm". *Expert Syst. Appl.* **2015**, *42*, 2392–2394. [CrossRef]
18. Mishra, A.; Agarwal, C.; Sharma, A.; Bedi, P. Optimized gray-scale image watermarking using DWT–SVD and Firefly Algorithm. *Expert Syst. Appl.* **2014**, *41*, 7858–7867. [CrossRef]
19. Anand, A.; Singh, A.K.; Lv, Z.; Bhatnagar, G. Compression-Then-Encryption-Based Secure Watermarking Technique for Smart Healthcare System. *IEEE Multimed.* **2020**, *27*, 133–143. [CrossRef]
20. Chaturvedi, A.K.; Shukla, P.K. Effective watermarking technique using optimal discrete wavelet transform and sanitization technique. *Multimed. Tools Appl.* **2020**, *79*, 13161–13177. [CrossRef]
21. Baba Ahmadi, S.B.; Zhang, G.; Jelodar, H. A robust hybrid SVD-based image watermarking scheme for color images. In Proceedings of the 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 17–19 October 2019; pp. 0682–0688. [CrossRef]
22. Pandey, M.K.; Parmar, G.; Gupta, R.; Sikander, A. Lossless robust color image watermarking using lifting scheme and GWO. *Int. J. Syst. Assur. Eng. Manag.* **2020**, *11*, 320–331. [CrossRef]
23. Lai, C.C.; Tsai, C.C. Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition. *IEEE Trans. Instrum. Meas.* **2010**, *59*, 3060–3063. [CrossRef]
24. Anand, A.; Singh, A.K. Cloud based secure watermarking using IWT-Schur-RSVD with fuzzy inference system for smart healthcare applications. *Sustain. Cities Soc.* **2021**, *75*, 103398. [CrossRef]
25. Xu, D. Commutative Encryption and Data Hiding in HEVC Video Compression. *IEEE Access* **2019**, *7*, 66028–66041. [CrossRef]
26. Selesnick, I. The slantlet transform. *IEEE Trans. Signal Process.* **1999**, *47*, 1304–1313. [CrossRef]
27. Zhang, J.; Erway, J.; Hu, X.; Zhang, Q.; Plemmons, R. Randomized SVD Methods in Hyperspectral Imaging. *J. Electr. Comput. Eng.* **2012**, *2012*, 409357. [CrossRef]
28. Cox, I.; Kilian, J.; Leighton, F.; Shamoon, T. Secure spread spectrum watermarking for multimedia. *IEEE Trans. Image Process.* **1997**, *6*, 1673–1687. [CrossRef] [PubMed]
29. Loukhaoukha, K. Optimal Image Watermarking Algorithm Based on LWT-SVD via Multi-objective Ant Colony Optimization. *J. Inf. Hiding Multimed. Signal Process.* **2011**, *2*, 303–319.

30. Wang, Z.; Bovik, A.C.; Sheikh, H.R. Structural similarity based image quality assessment. In *Digital Video Image Quality and Perceptual Coding*; CRC Press: Boca Raton, FL, USA, 2017; pp. 225–242.
31. Thakur, S.; Singh, A.K.; Kumar, B.; Ghrera, S.P. Improved DWT-SVD-Based Medical Image Watermarking Through Hamming Code and Chaotic Encryption. In *Proceedings of the Advances in VLSI, Communication, and Signal Processing*; Dutta, D., Kar, H., Kumar, C., Bhadauria, V., Eds.; Springer: Singapore, 2020; pp. 897–905.
32. Guo, Y.; Li, B.Z.; Goel, N. Optimised blind image watermarking method based on firefly algorithm in DWT-QR transform domain. *IET Image Process.* **2017**, *11*, 406–415. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.