algorithms

MDPI

Article

Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition for Enhanced Imperceptibility and Robustness

Mahbuba Begum [1,2], Sumaita Binte Shorif [2], Mohammad Shorif Uddin [2,*], Jannatul Ferdush [3], Tony Jan [4], Alistair Barros [5] and Md Whaiduzzaman [4,5,*]

[1] Department of Computer Science and Engineering, Mawlana Bhashani Science and Technology University, Tangail 1902, Bangladesh; mahbubacse@mbstu.ac.bd

[2] Department of Computer Science and Engineering, Jahangirnagar University, Dhaka 1342, Bangladesh; sumaita.bs@gmail.com

[3] Department of Computer Science and Engineering, Jashore University of Science and Technology, Jashore 7408, Bangladesh; jannatulferdush@just.edu.bd

[4] Centre for Artificial Intelligence Research and Optimisation (AIRO), Torrens University, Australia; tony.jan@torrens.edu.au

[5] School of Information Systems, Queensland University of Technology, Brisbane, QLD 4000, Australia; alistair.barros@qut.edu.au

* Correspondence: shorifuddin@juniv.edu (M.S.U.); wzaman@juniv.edu (M.W.)

Abstract: Digital multimedia elements such as text, image, audio, and video can be easily manipulated because of the rapid rise of multimedia technology, making data protection a prime concern. Hence, copyright protection, content authentication, and integrity verification are today's new challenging issues. To address these issues, digital image watermarking techniques have been proposed by several researchers. Image watermarking can be conducted through several transformations, such as discrete wavelet transform (DWT), singular value decomposition (SVD), orthogonal matrix Q and upper triangular matrix R (QR) decomposition, and non-subsampled contourlet transform (NSCT). However, a single transformation cannot simultaneously satisfy all the design requirements of image watermarking, which makes a platform to design a hybrid invisible image watermarking technique in this work. The proposed work combines four-level (4L) DWT and two-level (2L) SVD. The Arnold map initially encrypts the watermark image, and 2L SVD is applied to it to extract the s components of the watermark image. A 4L DWT is applied to the host image to extract the LL sub-band, and then 2L SVD is applied to extract s components that are embedded into the host image to generate the watermarked image. The dynamic-sized watermark maintains a balanced visual impact and non-blind watermarking preserves the quality and integrity of the host image. We have evaluated the performance after applying several intentional and unintentional attacks and found high imperceptibility and improved robustness with enhanced security to the system than existing state-of-the-art methods.

Keywords: DWT; SVD; imperceptibility; robustness; arnold map

check for updates

Citation: Begum, M.; Shorif, S.B.; Uddin, M.S.; Ferdush, J.; Jan, T.; Barros, A.; Whaiduzzaman, M. Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition for Enhanced Imperceptibility and Robustness. *Algorithms* **2024**, *17*, 32. https://doi.org/10.3390/a17010032

Academic Editor: Frank Werner

Received: 31 October 2023
Revised: 2 January 2024
Accepted: 3 January 2024
Published: 12 January 2024

1. Introduction

The rapid development of Internet technology makes it easier for intruders to duplicate, manipulate, and distribute digital content illegally. Digital image watermarking is one of the most promising techniques in this regard that can be used as a safeguard for digital content. This technology can be used in several applications, including authentication, broadcast monitoring, integrity verification, copyright protection, and content tracking [1]. In this section, we have described the background and contributions of this work.

1.1. Background

Digital image watermarking technology is basically used passively to protect copyright for authentication and identifies the ownership of digital content. This image watermarking technology embeds an additional image (or watermark) into the original cover or host image and produces the watermarked image in such a way that the hidden watermark can be detected or extracted later from the watermarked image to identify the right owner of the digital content [2].

The general framework of image watermark embedding (or inserting) and extraction are shown in Figure 1 [3]. At first, the watermark embedding algorithm takes the host and watermark images and the secret key. The communication channel is used to pass the watermarked image, which was then attacked in numerous ways. The watermark image is extracted from the watermarked image by the watermark extraction algorithm with the same secret key and reverse algorithm of the watermark embedding.

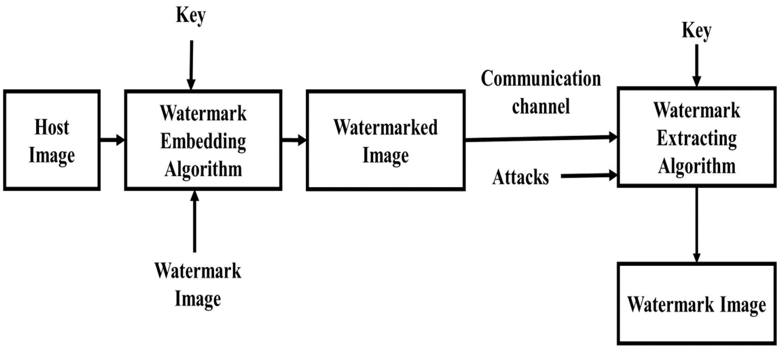

Figure 1. Common framework for inserting and extraction of watermark image.

Inserted watermarking can be visible or indistinguishable to the viewer, but invisible watermarking gains more popularity than visible watermarking in image authentication. Hence, we have designed an invisible image watermarking technique in this work.

An efficient image watermarking system must satisfy four design requirements like imperceptibility, robustness, security, and embedding capacity, simultaneously [4]. It is really a challenging task for researchers to maintain a proper balance among these requirements because of their limited and contradictory qualities [5]. Also, maintaining a proper balance among these design requirements depends on watermarking applications [6–9]. Watermarking can be conducted through spatial or transform domain techniques. But, peak-signal-to-noise-ratio (PSNR) values for spatial domain approaches are lower than those for transform domain methods [10]. Also, they are less robust against attacks, whereas transform domain techniques guarantee improved imperceptibility and high robustness, with improved security to the system. Researchers are now concentrating on hybridizing spatial or two or more transform domain methods, as a single transformation cannot satisfy all of the design requirements simultaneously [3].

1.2. Contributions

Our main contributions are:

- We implement a hybrid image watermarking method that ensures high imperceptibility, improved robustness, enhanced security, and high embedding capacity to the system simultaneously.
- We embed an indistinguishable watermark image into the cover image and we also ensure the security of the watermark image by using the Arnold map.
- We use a dynamically sized watermark image that maintains a balanced visual impact by preventing the watermark from being too small or too large.

The rest of this research is organized as follows: Section 2 describes the related literature with existing research gaps. Some theories about the Arnold map, DWT, and SVD are discussed in Section 3. Section 4 describes our proposed methodology by incorporating watermark embedding and extraction algorithms. The experimental results and comparison with state-of-the-art methods are described in Section 5. Finally, we have concluded our research in Section 6, with a new direction for research.

2. Related Literature and Problem Statement

This section describes the related literature on transform domain and decomposition techniques based on hybrid image watermarking methods. Then, it points out some issues that must be improved.

2.1. Literature Review

There exists a lot of research work on hybrid domain image watermarking methods. A color image watermarking method is designed by Rasti et al., 2017 [11] based on wavelet and QR decomposition. Two-level (2L) DWT, QR decomposition, Chirp Z-Transform (CZT), and SVD are used to embed the watermark image into the cover (or host) image. The method ensures better imperceptibility and high robustness against various attacks like gamma correction, flipping, image blur, contrast enhancement, histogram equalization (HE), Gaussian noise (GN), salt-and-pepper-noise (SPN), and image sharpening. But, this method is less robust against cropping, scaling, and JPEG compression attacks. Moreover, the security of the watermark image and embedding capacity into the host image are not observed. Singh et al. [2] proposed another robust and secure color image watermarking method by combining DWT, SVD, and QR codes. At first, 2L DWT is applied on the color cover or host image prior to dividing it into blocks. Then, SVD is applied to each block and extracted the singular values. Then, the same steps are done to the QR code as a watermark image. After that, the method embeds the singular values of the watermark image into the singular values of the host image. The method is robust against GN, SPN, and median filter (MF) attacks. But, other requirements like imperceptibility, security, and embedding capacity are not analyzed. Also, geometric and other signal-processing attacks are not observed. Therefore, in the scheme Singh et al., 2018 [12], another hybrid domain image watermarking method is proposed that combines NSCT, DCT, and SVD to ensure better imperceptibility and high robustness against geometric and other attacks. NSCT, DCT, and SVD are applied one after another to both host and watermark images. Here, singular values of the watermark image are embedded into the singular values of the host image. The watermarked image is generated after performing inverse transformations. The method is robust against JPEG compression, average filter (AF), Gaussian filter (GF), MF, GN, HE, Gaussian blur, motion blur, SPN, rotation, scaling, and resizing attacks. But, the method does not observe security and calculate the watermark embedding capacity into the host image. Najafi et al. [13] proposed another robust and secure hybrid domain method that combines sharp frequency localized contourlet transform (SFLCT) and SVD. Experimental results show that PSNR is 45.85 dB, which makes the watermarked image less noticeable. Also, the method is robust against Gamma correction, JPEG compression, GN, SPN, SN, sharpening, MF, Wiener filter (WF), HE, scaling, rotation, cropping, copy attack, cutting, and shearing attacks. But, they do not use any security method and compute the host image's capability for watermark embedding. In 2018, Zhou et al. [14] proposed another DWT, all-phase discrete cosine biorthogonal transform (APDCBT), and an SVD-based hybrid image watermarking method. At first, DWT, APDCBT, and SVD are applied to the cover image one after another. Watermark is inserted into the singular values of the host image. The generated watermarked image seems similar to the host image as PSNR is 101.97 dB. The method proves robustness against SPN, JPEG compression, GN, scaling, MF, AF, rotation, contrast enhancement, and brightness adjustment attacks. The method is resistant to hybrid attacks as well, which is an additional feature of this method. The embedding capacity is 2048 bits. But, this method does not consider the false-positive-detection (FPD) problem. Also, any security technique is not used to ensure the security of the watermark image. Liu et al. [15] proposed another hybrid image watermarking method based on DWT, Hessenberg decomposition (HD), and SVD. To ensure that robustness and imperceptibility are properly balanced, the Fruit fly optimization algorithm is used to determine the optimized scaling factor. Experiments found PSNR > 38 dB, which means a better imperceptibility of the watermarked image. The method is robust against WF, MF, low-pass Gaussian filter (LPGF), AF, GN, SN, SPN, JPEG compression, JPEG 2000, rescaling, HE, sharpening, and motion blur attacks. Also, the FPD problem can be solved by this method. But, hybrid attacks and watermark embedding capacity are not observed. Also, they do not use any security technique for ensuring watermark image security. In scheme Dhar et al., 2020 [16], another blind method is proposed based on fan beam transform (FBT) and QR decomposition. At first, FBT is applied to the color host image, and QR decomposition is applied to it. The watermark is inserted into the selected coefficients of the host image. The method results in high imperceptibility, as PSNR > 54 dB. The method is robust against JPEG compression, rotation, SPN, GN, SN, Poisson noise (PN), contrast adjustment, sharpening, WF, and MF attacks. But, the method is less robust against cropping attacks. Also, hybrid attacks, copy attacks, security issues, and embedding capacity are not examined. In 2021, Begum et al. [3] proposed a hybrid method based on discrete cosine transform (DCT), DWT, and SVD. At first, the watermark image is encrypted by the Arnold map. Then, DCT is applied to the encrypted watermark image and afterwards, the DWT prior to SVD is applied to it. The same steps are applied to the host image. The watermark image's singular values are then embedded into the host image's singular values. The method has better imperceptibility as PSNR is 57.63 dB. Also, the method proves robustness against WF, AF, MF, SPN, and rotation attacks. But, GN, SN, PN, cropping, scaling, resizing, hybrid attacks, and watermark embedding capacity are not observed by this method. Another hybrid discrete Fourier transform (DFT) and SVD-based method is proposed by Begum and Uddin [17] in 2021, where the logistic chaotic map is used for security. The method has a PSNR of 50.91 dB, which proves better imperceptibility and is robust against the filter, geometric, hybrid, image sharpening, Gamma correction, HE, and image blur attacks. Also, the watermark embedding capacity is 20,480 bits. But, it shows a weaker performance than other non-DFT-based methods. Another fusion-based blind method DWT-DCT-SVD is proposed in the paper [18]. The Arnold map is employed in this technique to guarantee the security of the watermark image. Experimental results show that PSNR is 44.05 dB, and the method is robust against AF, MF, Gaussian blurring, JPEG compression, JPEG 2000, HE, resizing, and cropping attacks. But, the method is less robust against SPN and GN attacks, and the method has a large computational complexity due to fusion. Also, hybrid, scaling, GF, PN attacks, and embedding capacity are not observed. In the scheme Srivastava et al., 2021 [19], another hybrid DCT-DWT-based watermarking method is proposed. At first, the watermark image is encrypted by the Arnold map. Then, 2L DWT is applied to the host image and extracted from the LH sub-band. Then, LH is divided into blocks, and DCT is applied to each block. Then, the watermark is embedded into the modified DC coefficients of the host image. Experimental results show high PSNR (>69 dB) and strong robustness against cropping, scaling, adaptive filtering, HE, SPN, GN, and sharpening attacks. Also, the method requires less time (0.97 s) to execute without attacks. But, rotation, resizing, MF, AF, LPGF, SN, and hybrid attacks are not observed. Also, the capacity is not calculated. Another decomposition-based fragile image watermarking is proposed by the scheme by Nejati et al., 2021 [20], where the QR technique decomposes the watermark image. Fourier transform (FT) is applied to the host image, and then QR is applied to it. Then, coefficients of the R matrix of the watermark image are embedded into the coefficients of the R matrix of the host image. The method obtains a high PSNR which is greater than 62 dB. As it is a fragile method, the watermark image cannot be extracted if manipulation occurs in the watermarked image. The method is also less resistant to attacks. Thanki et al. [21] proposed another NSCT-redundant DWT (RDWT)-based method for ensuring better imperceptibility and strong robustness. The method guarantees improved imperceptibility (PSNR = 57.06 dB) and strong robustness (normalized correlation, NC = 0.99) against various attacks. At first, 1L NSCT is applied to the host image and selected contourlet sub-bands. Then, RDWT is applied to it. Then, wavelet sub-bands are selected and divided into 8 × 8 blocks. Finally, the watermark bit is inserted into each block of the host image. Thus, the watermarked image is produced after performing a reverse transformation. The method proves robustness against motion cropping, sharpening, HE, MF, LPGF, GN, SN, SPN, GF, MF, JPEG compression, and blurring attacks. But, they do not use any security technique in the watermark image. Additionally, the capacity to insert a watermark is not estimated. In 2021, Yasmeen and Uddin [22] proposed another DWT-SVD-based efficient image watermarking technique. The method has better imperceptibility (PSNR > 36 dB) and is robust against GN, SPN, SN, rotation (45°), cropping, stretching, and HE attacks. FPD problems can be solved by this method. But, it does not show quantitative results for FPD. Also, filter and hybrid attacks are not observed. They do not use any encryption technique to ensure watermark image security. Also, embedding capacity is not calculated. Zeng et al. [23] proposed another blind hybrid NSCT-DWT-SVD-human visual system (HVS) based image watermarking method for ensuring better imperceptibility and robustness. At first, 1L NSCT is applied to the host image to extract low-frequency sub-band, and then 2L DWT is applied to it to extract sub-blocks. SVD is applied to each sub-block, and the best position for embedding the watermark is selected using HVS. The Arnold map encrypts the watermark image that is embedded into the singular values of the host image. Thus, the watermarked image is generated. FPD problems can be avoided by this method. The method ensures better imperceptibility (PSNR = 46.56 dB) and is robust against GN, SN, GF, MF, JPEG compression, cropping, shear center (CC), and scaling attacks. But, the method is less robust against rotation attacks. Also, AF, SPN, resizing, hybrid attacks and embedding capacity are not observed.

2.2. Problem Statement

From the discussions in Section 2.1, we can conclude the following:

- Existing hybrid domain algorithms fail to maintain a proper balance among imperceptibility, robustness, security, and capacity simultaneously.
- Certain algorithms utilize visible images as watermarks, which are unsuitable for identifying authentic recipients.
- Can watermark image be easily applied to new content without any adjustment?
- Some methods lack the incorporation of security techniques for encrypting the watermark image.
- The majority of the methods overlook hybrid attacks and do not calculate the watermark embedding capacity.

These findings highlight the need for developing improved hybrid domain algorithms that address these limitations and provide enhanced imperceptibility, robustness, security, and capacity performance.

3. Theoretical Background

This section describes the preliminary concepts of the Arnold map, Discrete Wavelet Transform (DWT), and Singular Value Decomposition (SVD) techniques.

3.1. Arnold Map

The Arnold map is an encryption technique that iteratively scrambles adjacent pixels [24]. If I is a two-dimensional image with order N, its pixel representation can be written as:

$$P = \{(x, y) \mid x, y = 0, 1, 2, \ldots, N-1\}$$

After scrambling, it can be written as:

$$P' = \{(x', y') \mid x', y' = 0, 1, 2, \ldots, N-1\}$$

The Arnold scrambling transformation can be expressed as follows:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} modN$$

Here, x and y represent the pixel coordinates of the original image, and x' and y' represent the pixel coordinates after performing Arnold scrambling on the original host image. This transformation disperses the host image, ensuring that hidden information remains evenly dispersed even if the original image is corrupted. This criterion enhances the reliability, robustness, and security of the hidden image [24]. In our proposed method, we employ the Arnold map to ensure the security of the watermark image.

3.2. *Discrete Wavelet Transform (DWT)*

The wavelet transform DWT decomposes a signal into wavelets, which are discretely sampled. DWT operates on both frequency and time location, providing an advantage over the Fourier transform [25]. This transformation is commonly used in image compression, signal processing, noise removal, and other applications [26].

DWT transforms the host image into four sub-bands: low-low (LL), low-high (LH), high-low (HL), and high-high (HH). The LL sub-band contains the approximation part, while the other three sub-bands contain detailed information such as the edges and textures of the image. Each sub-band can be further decomposed into four sub-bands, resulting in a multi-level decomposition. The magnitude of DWT coefficients is usually larger in the LL sub-band compared to the other sub-bands. In our proposed method, we have decomposed the host image using a four-level DWT on the LL sub-band. Figure 2 shows the four-level DWT on the LL sub-band.

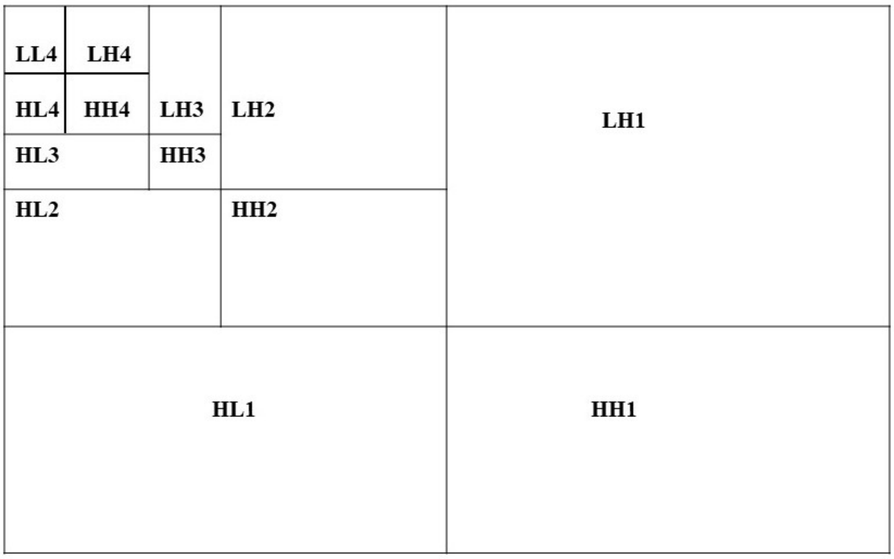

Figure 2. A 4L DWT on LL sub-band.

3.3. *Singular Value Decomposition (SVD)*

SVD is the decomposition of a real or complex matrix. If M is an image with dimension N × N, then, it can be decomposed into two orthogonal matrices (like U and V) and one diagonal matrix S, such that $M = USV^T$[27]. The elements of diagonal matrix S are called singular values. SVD can be widely used in several digital signal processing operations, including image restoration, data compression, power spectrum estimation, and noise reduction [28–30]. This SVD can be used in watermarking effectively, as this decomposition maintains the imperceptibility of the watermarked image properly [31]. Also, unique, singular values of SVD make it more robust against geometric [12] and other attacks. Besides, these singular values contain major information of an image [14]. Also, small changes due to noise cannot affect the singular values significantly [18]. These properties make SVD more attractive to researchers in doing research with image watermarking. Motivated by this, we performed SVD after completing DWT on the host image.

4. Proposed Methodology

The proposed method for embedding the watermark image into the host image is illustrated by Figure 3. It is not an embedding operation of a direct substitution. Rather, we have performed different levels of DWT and SVD operation on both host and watermark images before the embedding operation. At first, the Arnold map is used for encrypting the watermark image to ensure the security of the system. We have applied SVD twice both for LL4 and ew for increasing robustness and security. Watermark embedding with different SVD levels resists the geometric attacks more effectively. Therefore, two-level (2L) SVD is applied to LL4 to extract S components. The method applies 4L DWT to the host image and extracts the LL4 sub-band. After that, 2L SVD is applied to that sub-band and S components are extracted. Then, the method embeds the watermark image's S components into the host image's S components with a scaling factor α that is chosen manually to obtain the best value so that there maintains a better trade-off between the imperceptibility and robustness of the system. In this study, we have used $\alpha = 0.07$. After that, the LL4 sub-band is rebuilt and the inverse DWT (IDWT) is applied to obtain the watermarked image. Watermark extraction is conducted in a reverse way which is shown by Figure 4. Initially, 4L DWT is applied to the watermarked image to extract LL4wmv. Then, 2L SVD is applied to it to extract the Sw component. After that, inverse SVD (ISVD) is applied to Sw to extract the encrypted watermark, ew. Finally, the system applies the inverse Arnold map to ew to obtain the watermark image. We have encrypted the watermark with Arnold mapping; our main focus is to extract the watermark image from the watermarked image.

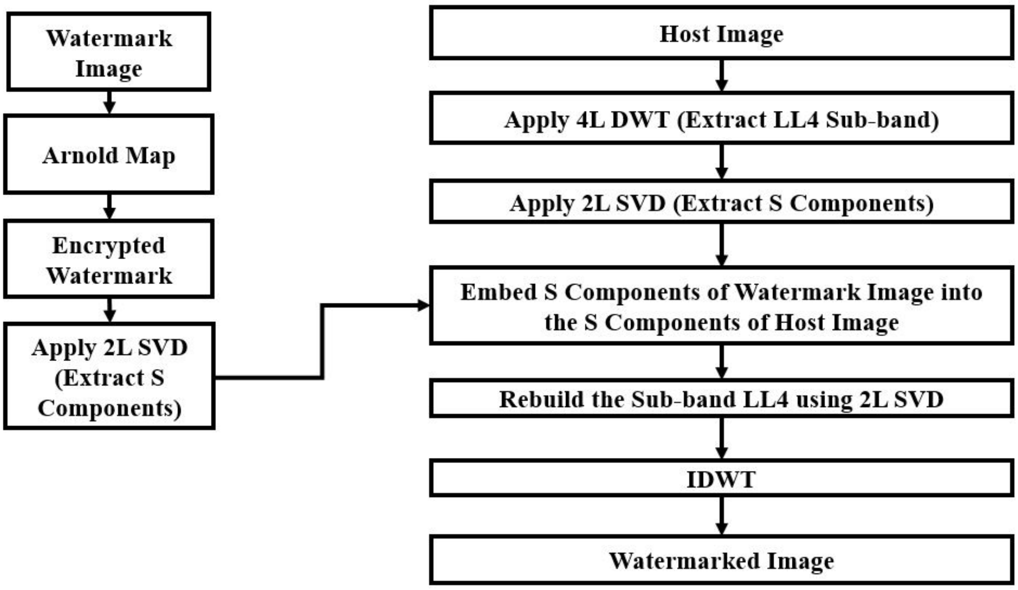
Watermark Image
Arnold Map
Encrypted Watermark
Apply 2L SVD (Extract S Components)
Host Image
Apply 4L DWT (Extract LL4 Sub-band)
Apply 2L SVD (Extract S Components)
Embed S Components of Watermark Image into the S Components of Host Image
Rebuild the Sub-band LL4 using 2L SVD
IDWT
Watermarked Image

Figure 3. Proposed method for watermark embedding.

However, this section describes proposed algorithms for watermark embedding and extraction in Algorithm 1 and Algorithm 2, respectively.

Algorithm 1 Watermark Embedding Algorithm

```
Input: Watermark image, $w$, and host image, $I$, both of size 512 × 512 pixels
Output: Watermarked image, $WI$

Apply 4L DWT to host image;
$DWT(I) = [LL1, HL1, LH1, HH1]$;
$DWT(LL1) = [LL2, HL2, LH2, HH2]$;
$DWT(LL2) = [LL3, HL3, LH3, HH3]$;
$DWT(LL3) = [LL4, HL4, LH4, HH4]$;

Apply 2L SVD on $LL4$;
$SVD(LL4) = [Uy, Sy, Vy]$;
$SVD(Sy) = [U1y, S1y, V1y]$;

Resize the watermark image, $w$, to the size of $LL4$ (32 × 32 pixels);
Apply the Arnold map to encrypt the watermark image:
$ew = ArnoldMap(w)$;
Apply 2L SVD to $ew$;
$SVD(ew) = [Uw, Sw, Vw]$;
$SVD(Sw) = [U1w, S1w, V1w]$;

Insert $S$ components of the watermark image into the $S$ components of the host image with a scaling factor $\alpha$ . The embedding equation is:
$Smark = S1y + \alpha \times S1w$;

Rebuild the sub-band;
$LL4_1 = Uy \times Smark \times V_y^T$;

Apply inverse DWT (IDWT) to obtain $WI$;
$LL3_1 = IDWT(LL4_1, HL4, LH4, HH4)$;
$LL2_1 = IDWT(LL3_1, HL3, LH3, HH3)$;
$LL1_1 = IDWT(LL2_1, HL2, LH2, HH2)$;
$WI = IDWT(LL1_1, HL1, LH1, HH1)$;
```

Algorithm 2 Watermark Extraction Algorithm

```
Input: Watermarked image, $WI$
Output: Watermark image, $w$

Apply 4L DWT to $WI$;
$DWT(WI) = [LL1_{wmv}, HL1, LH1, HH1]$;
$DWT(LL1_{wmv}) = [LL2_{wmv}, HL2, LH2, HH2]$;
$DWT(LL2_{wmv}) = [LL3_{wmv}, HL3, LH3, HH3]$;
$DWT(LL3_{wmv}) = [LL4_{wmv}, HL4, LH4, HH4]$;

Apply SVD to $LL4_{wmv}$;
$SVD(LL4_{wmv}) = [Uy, Smark_{wmv}, Vy]$;

Extract the $S$ component;
$S1wrec = (Smark_{wmv} - S1y)/\alpha$;

Apply ISVD to $Sw$
$ISVD(Swrec) = [U1w \times S1wrec \times V1w^T]$;
$ISVD(ew) = [Uw \times Swrec \times Vw^T]$;

Apply the inverse Arnold map to $ew$ to obtain watermark image, $w$;
$w = Inverse\_Arnold(ew)$;
```

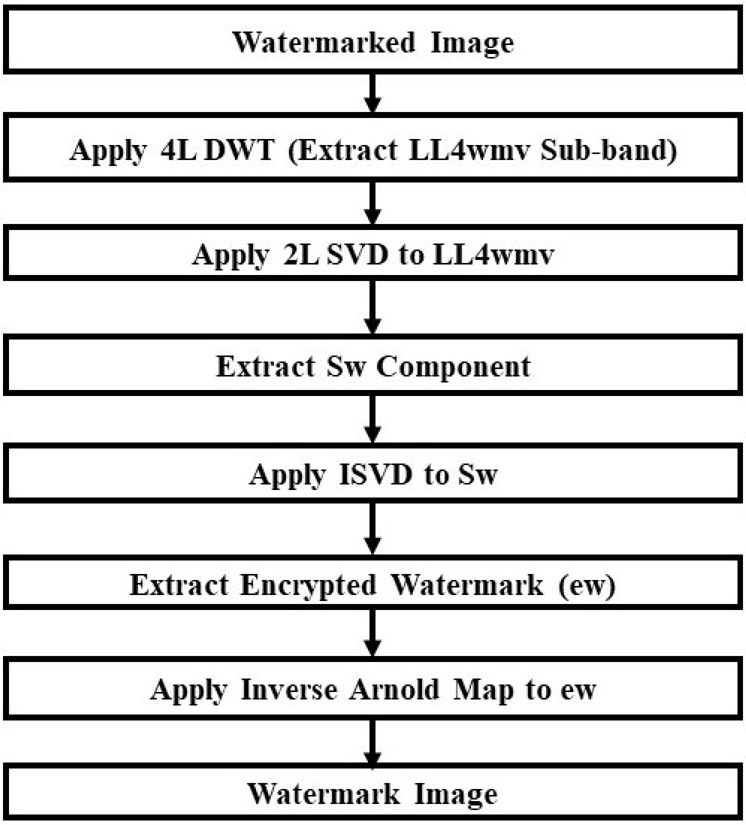
Watermarked Image
Apply 4L DWT (Extract LL4wmv Sub-band)
Apply 2L SVD to LL4wmv
Extract Sw Component
Apply ISVD to Sw
Extract Encrypted Watermark (ew)
Apply Inverse Arnold Map to ew
Watermark Image

Figure 4. Proposed method for watermark extraction.

5. Experimental Results and Analysis

The suggested algorithm was carried out through MATLAB R2016a software. We validated the imperceptibility and robustness of the proposed watermarking through rigorous experimentation with different groups of images like miscellaneous, texture, medical, and underwater images. Our main novelty is the dynamic-sized watermark image that maintains a balanced visual impression. In this experiment, different groups of grayscale 512 × 512 images are taken as hosts and a grayscale copyright image whose size is equal to the size of LL4 is used as a watermark image. Our watermark image size is equal to the size of LL4. Therefore, it depends on the host image size. Our host image size is 512 × 512. Then, our watermark image size will be 64 × 64 after performing LL4. Hence, our watermark image can be easily applied to new content without any adjustment. There is no scope to be the same size of host and watermark images. We have used PSNR, the structural similarity index measure (SSIM), and normalized correlation (NC) to assess the watermarking system's effectiveness. The input images are shown in Figure 5, where (a–j) serve as host images, and (k) serves as a watermark image. Here, (a–c) are miscellaneous images and (d–e) are texture images that are taken from the USC (University of Southern California)-SIPI (Signal and Image Processing Institute) image database [32]. Image (f) is taken from the image database [33]. On the other hand, (g) and (h) are medical images that are taken from chest X-ray images (Pneumonia) [34] and the ECG heartbeat categorization dataset [35], respectively. Finally, (i) and (j) are underwater images that are taken from the fish species image data [36] and the Brackish dataset [37], respectively.

However, this section analyses the system's imperceptibility, robustness, security, and capacity. At the conclusion of this section, a comparison of the imperceptibility and robustness of our suggested method with existing methods is shown.

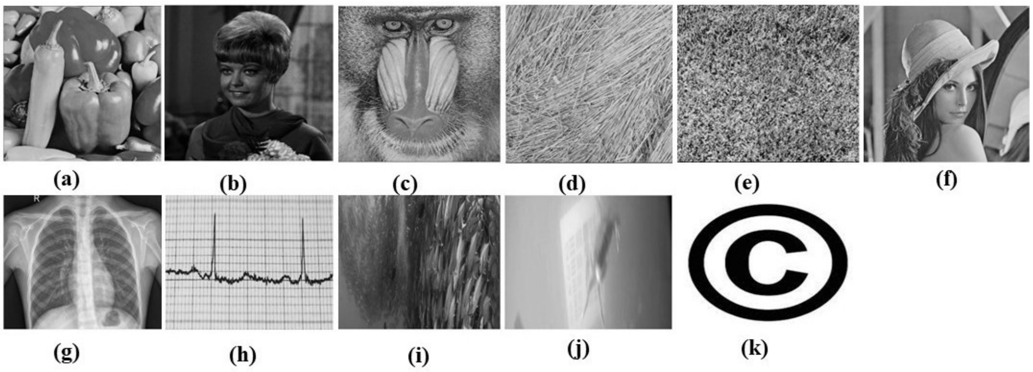

Figure 5. Input images: (**a**) Pepper; (**b**) Female; (**c**) Baboon; (**d**) Straw; (**e**) Grass; (**f**) Lena; (**g**) Chest X-ray; (**h**) ECG; (**i**) Fish Species; (**j**) Marine Animal; (**k**) Copyright (watermark image).

5.1. Imperceptibility Analysis

We have analyzed the imperceptibility of our proposed method for different groups of images by PSNR (dB) and SSIM, which is observed in Table 1. From this Table, we can say that, for different groups of images, the value of PSNR is greater than 48 dB, and the value of SSIM is close to 1. Also, we noticed that for chest X-ray medical images, we found the largest value of PSNR, which is 48.9688 dB. Therefore, we can state that our proposed method ensures improved the imperceptibility for different groups of images. The generated watermarked and extracted watermark images are shown in Figure 6.

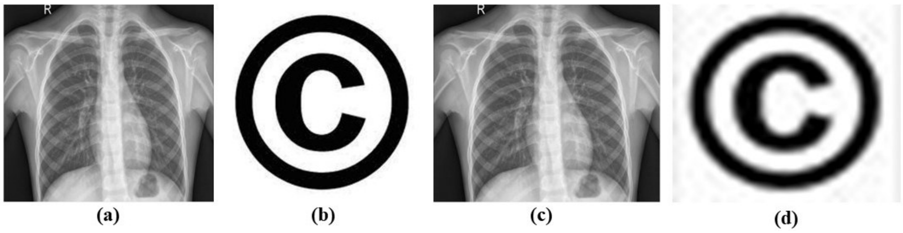

Figure 6. (**a**) Chest X-ray (Host Image); (**b**) Copyright (Watermark Image); (**c**) Watermarked Image; (**d**) Extracted Watermark.

Table 1. Imperceptibility Analysis for Different Groups of Images by PSNR (dB) and SSIM.

Image Type	Image Name	PSNR (dB)	SSIM
Miscellaneous	Pepper	48.9192	0.9997
	Female	48.6165	0.9995
	Baboon	48.7890	0.9999
	Lena	48.6339	0.9998
Texture	Straw	48.8687	0.9999
	Grass	48.8001	1.0000
Medical Image	Chest X-ray	48.9688	0.9997
	ECG signal	48.5490	0.9998
Underwater Image	Fish Species	48.8687	0.9997
	Marine Animal	48.5780	0.9993

5.2. Robustness Analysis

We analyzed noise, filter, geometric, image blur, and hybrid attacks for different groups of images. For all of these images, we found that the values of NC are greater than 0.9, indicating that our method can successfully recover the watermark image.

5.2.1. Noise Attack

Table 2 analyzes speckle noise (SN), Gaussian noise (GN), SPN, and Poisson noise (PN). For the chest X-ray image, the image is very much distorted by the PN attack, since the watermarked image's PSNR (26.9433 dB) is sufficiently low for visualization. But, our system can still extract the watermark image from the generated watermarked image, as NC is close to 1. Figure 7 shows the PSNR (dB) and NC values after the noise attack for the chest X-ray medical image.

Table 2. Robustness Analysis for Noise Attack with Different Groups of Images by NC.

Image Type	Image Name	SN	GN	SPN	PN
Miscellaneous	Pepper	0.9916	0.9911	0.9915	0.9469
	female	0.9905	0.9909	0.9906	0.9313
	Baboon	0.9942	0.9924	0.9944	0.9446
	Lena	0.9933	0.9920	0.9929	0.9674
Texture	Straw	0.9912	0.9922	0.9936	0.9643
	Grass	0.9946	0.9955	0.9954	0.9776
Medical Image	Chest X-ray	0.9941	0.9923	0.9951	0.9707
	ECG signal	0.9957	0.9927	0.9953	0.9640
Underwater Image	Fish Species	0.9944	0.9920	0.9944	0.9744
	Marine Animal	0.9904	0.9908	0.9914	0.9468

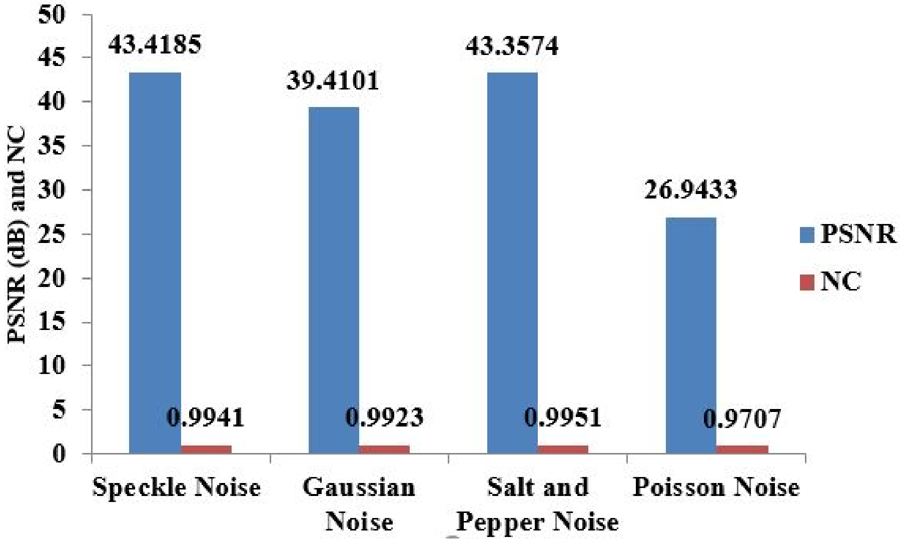

Figure 7. PSNR(dB) and NC values after noise attacks for chest X-ray image.

5.2.2. Filter Attack

Table 3 shows the performance of various filter attacks, like the average filter (AF), median filter (MF), Wiener filter (WF), and low pass Gaussian filter (LPGF), for different groups of images. In Figure 8, for the chest X-ray image, we found the lowest PSNR value (35.3040 dB) after the AF attack. But, still, the NC value is 0.9627, which indicates that the method is capable of removing the watermark from the watermarked image.

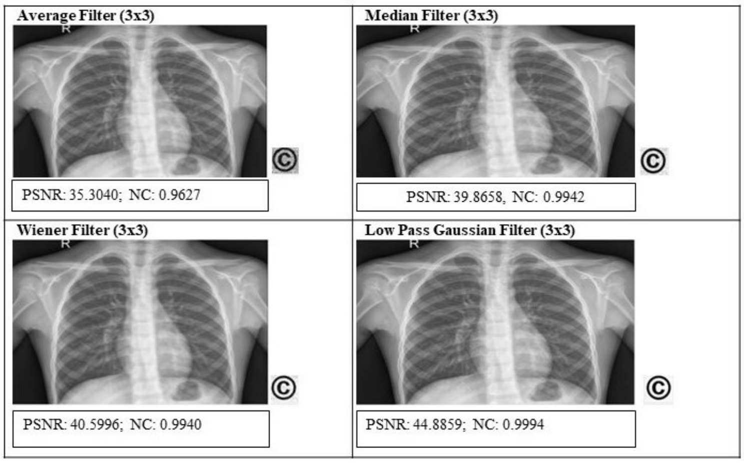
Average Filter (3x3)
PSNR: 35.3040; NC: 0.9627
Median Filter (3x3)
PSNR: 39.8658, NC: 0.9942
Wiener Filter (3x3)
PSNR: 40.5996; NC: 0.9940
Low Pass Gaussian Filter (3x3)
PSNR: 44.8859; NC: 0.9994

Figure 8. PSNR(dB) and NC values after filter attacks for chest X-ray image.

Table 3. Robustness Analysis for Filter Attack with Different Groups of Images by NC.

Image Type	Image Name	AF	MF	WF	LPGF
Miscellaneous	Pepper	0.9431	0.9789	0.9897	0.9978
	Female	0.9576	0.9978	0.9952	0.9993
	Baboon	0.9512	0.8753	0.9652	0.9963
	Lena	0.9713	0.9803	0.9936	0.9983
Texture	Straw	0.9641	0.9520	0.9732	0.9972
	Grass	0.9245	0.9854	0.8967	0.9963
Medical Image	Chest X-ray	0.9627	0.9942	0.9940	0.9994
	ECG signal	0.9233	0.8437	0.9517	0.9954
Underwater Image	Fish Species	0.9849	0.9658	0.9942	0.9989
	Marine Animal	0.9939	0.9997	0.9993	0.9999

5.2.3. Geometric and Blur Attacks

Image blur and geometric attacks like image resize and jpeg compression are highlighted in Table 4. We used the built-in function of Matlab "imresize" for image resizing. This means that the "imresize" function has been used as B = imresize(A, [rows cols]), which resizes image A to image B so that it has the desired size containing a specified number of rows and cols with the Matlab default cubic interpolation method. In Figure 9, for the chest X-ray image, the resultant PSNR and NC values are shown in place of the image resize, jpeg compression, and image blur attacks.

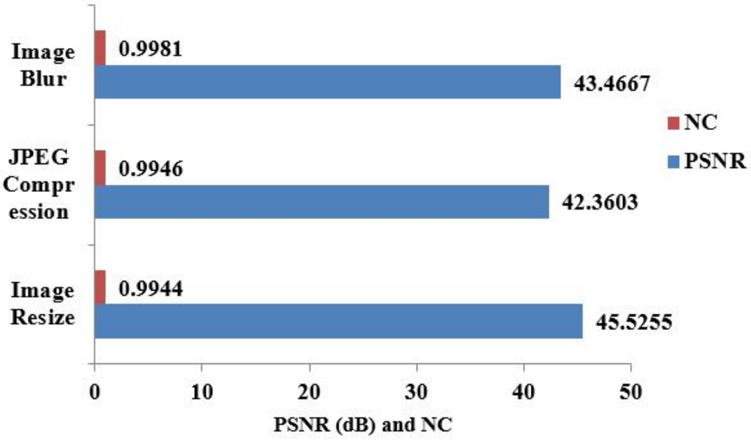

Figure 9. PSNR(dB) and NC values after geometric and blur attacks for chest X-ray image.

Table 4. Robustness Analysis for Geometric (resize and jpeg compression) and Blur Attacks with Different Groups of Images by NC.

Image Type	Image Name	Resize	JPEG Compression	Image Blur
Miscellaneous	Pepper	0.9934	0.9923	0.9974
	female	0.9907	0.9903	0.9978
	Baboon	0.9948	0.9961	0.9970
	Lena	0.9935	0.9943	0.9988
Texture	Straw	0.9936	0.9939	0.9978
	Grass	0.9943	0.9951	0.9969
Medical Image	Chest X-ray	0.9944	0.9946	0.9981
	ECG signal	0.9929	0.9955	0.9952
Underwater Image	Fish Species	0.9950	0.9950	0.9991
	Marine Animal	0.9917	0.9921	0.9995

5.2.4. Hybrid Attacks

We analyzed some hybrid attacks like MF+blur, SPN+WF, WF+GN, SN+MF, and MF+PN in Table 5. In Figure 10, for the chest X-ray image, we found the lowest PSNR (26.7531 dB) for hybrid attack MF+PN. But, still, the method can extract the watermark image successfully, as the NC value is close to 1.

Table 5. Robustness Analysis for Hybrid Attacks with Different Groups of Images by NC.

Image Type	Image Name	MF+Blur	SPN+WF	WF+GN	SN+MF	MF+PN
Miscellaneous	Pepper	0.9656	0.9834	0.9885	0.9750	0.9623
	Female	0.9952	0.9841	0.9934	0.9865	0.9824
	Baboon	0.8657	0.9549	0.9654	0.8772	0.8907
	Lena	0.9718	0.9805	0.9902	0.9730	0.9554
Texture	Straw	0.9412	0.9657	0.9755	0.9469	0.9371
	Grass	0.9834	0.8602	0.8940	0.9840	0.9820
Medical Image	Chest X-ray	0.9906	0.9851	0.9929	0.9802	0.9638
	ECG signal	0.8329	0.9438	0.9493	0.8335	0.8859
Underwater Image	Fish Species	0.9589	0.9907	0.9919	0.9627	0.9417
	Marine Animal	0.9995	0.9910	0.9979	0.9905	0.9269

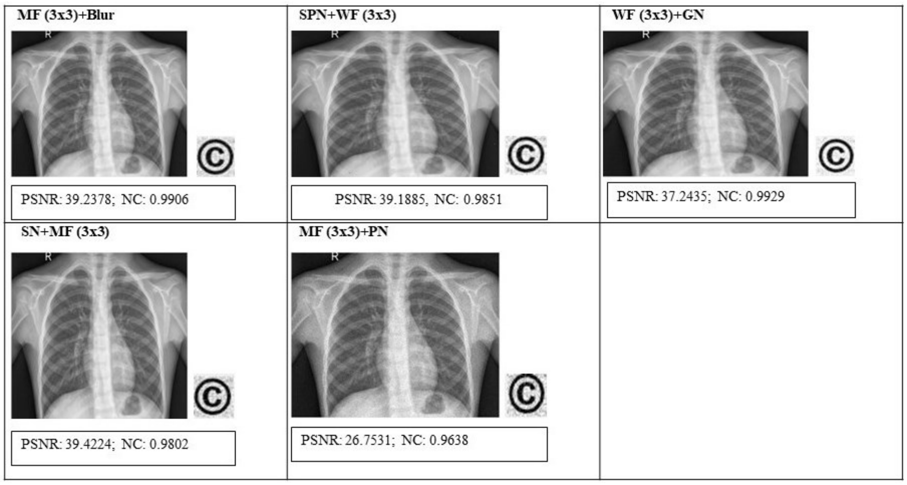
MF (3x3)+Blur
PSNR: 39.2378; NC: 0.9906
SPN+WF (3x3)
PSNR: 39.1885, NC: 0.9851
WF (3x3)+GN
PSNR: 37.2435; NC: 0.9929
SN+MF (3x3)
PSNR: 39.4224; NC: 0.9802
MF (3x3)+PN
PSNR: 26.7531; NC: 0.9638

Figure 10. PSNR(dB) and NC values after hybrid attacks for a chest X-ray image.

5.3. Security Analysis

We enhanced the security of the watermark image with an Arnold map. The Arnold map is highly secure and sensitive for the iteration number (key), which the sender and receiver keep private. The watermark image cannot be retrieved without the key. From Figure 11a, It is shown that the right key (32) is required to extract the watermark image. Otherwise, for Figure 11b, the right watermark image cannot be extracted. For a fake watermark, there is no image correlation between neighboring pixels, which indicates a meaningless image. So, the method we propose is sufficiently secure.

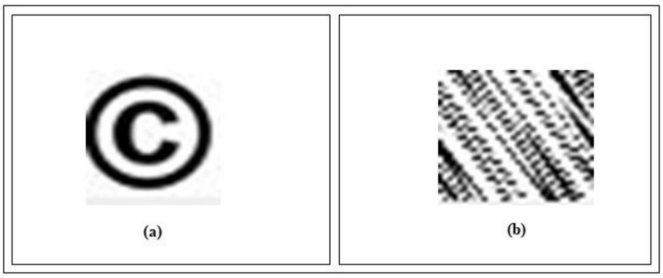

Figure 11. Extracted watermark; (**a**) with right key 32; (**b**) with wrong key.

5.4. Capacity Analysis

In the given scenario, the PSNR and SSIM values are constant for increasing bit depths. PSNR is a metric that measures the quality of an image by comparing it to the original image. Higher PSNR values indicate better quality, and typically, a PSNR value above 30 is considered good. In Table 6, for the pepper image, the PSNR value is 47.5334 dB, which suggests a high level of similarity between the watermarked image and the original host image, indicating a good-quality image.

SSIM is another metric that quantifies the structural similarity between two images. SSIM values range from −1 to 1, where 1 indicates a perfect match. The SSIM value of 0.9984 is close to 1, indicating a high level of similarity between the watermarked image and the original host image.

Table 6. Capacity Analysis by PSNR(dB) and SSIM.

Host Image	Watermark Image	Bit Depth	PSNR (dB)	SSIM
Pepper	Copyright	1024, 512, 256, 128, 64, 32, 16	47.5334	0.9984
		8	48.8636	0.9988
		2, 4	Infinite	1

5.5. Comparison with Existing Methods

Table 7 compares the characteristics of our proposed method with existing recent methods. We used different parameters like method, cover image type, cover image size and color, watermark image type, watermark image size and color, PSNR(dB) and SSIM, security techniques, and application. These parameters reflect the characteristics of our proposed method and compare the characteristics of our proposed method with existing recent methods. From this Table, we can say that the value of PSNR (dB) of the watermarked image of our proposed method is greater than the existing methods [18,21–23]. But, our resultant SSIM is greater than all of the existing methods. However, this section compares the imperceptibility and robustness of our proposed method with other hybrid watermarking methods.

Table 7. Comparison of Characteristics of the Proposed Method with Recent Methods.

Parameter	**Begum et al., 2021** [3]	**Begum et al., 2021** [17]	**Alzahrani et al., 2021** [18]	**Srivastava et al., 2021** [19]	**Nejati et al., 2021** [20]	**Thanki et al., 2021** [21]	**Yasmeen et al., 2021** [22]	**Zeng et al., 2022** [23]	**Proposed Method**
Method	DCT+ DWT+ SVD	DFT+ SVD	DWT+ DCT+ SVD	DWT+ DCT	Fourier transform+ QR decomposition	NSCT + RDWT	DWT+ SVD	NSCT+ DWT+ SVD	DWT+ SVD
Cover Image Type	Lena	Lena	Medical image	Pepper	Lena, Baboon, House, Sailboat	Pepper , medical image	Lena	Lena	Pepper, Lena, Chest X-ray
Cover Image Size and Color	512 × 512, grayscale	512 × 512, grayscale	1024 × 1024, grayscale	512 × 512, grayscale	512 × 512, color	512 × 512, grayscale	512 × 512, grayscale and color	512 × 512, grayscale	512 × 512, grayscale
Watermark Image Type	Panda	Panda	Hospital logo. text watermark	Text image	Pepper	Logo	Logo	Cameraman	Copyright
Watermark Image Size and Color	64 × 64, grayscale	64 × 64, grayscale	32 × 32, 128 × 8 grayscale	64 × 64, grayscale	512 × 512, color	32 × 128, grayscale	256 × 256, grayscale	32 × 32, binary	32 × 32, grayscale
PSNR (dB)	57.63	50.91	44.05	>69	62.74	57.60 (pepper), 40.89 (medical image)	43.84 (grayscale), 34.73 (color)	46.56	Pepper (48.92), Lena (48.63), Chest X-ray (48.97)
SSIM	0.9984	0.9745	0.9800	-	0.9998	0.9991 (pepper), 0.9994 (medical image)	0.9909 (grayscale), 0.9885 (color)	-	Pepper (0.9997), Lena (0.9998), Chest X-ray (0.9997)
Security Technique	Arnold map	Chaotic map	Arnold transform and pseudo random (PN) sequence	Arnold map	-	PN sequence	-	Arnold map	Arnold transform
Applications	Copyright protection	Copyright protection	Copyright protection	Data integrity	Medical image security	Telemedicine	Copyright protection	-	Copyright protection

5.5.1. Imperceptibility Comparison

We compared the PSNR (dB) and SSIM of our proposed method with other methods, which are shown in Figure 12. Figure 12a shows the comparison of PSNR values between our proposed method with popular watermark methods for chest X-ray images. It demonstrates that compared to other approaches, our method obtains the highest PSNR value (48.97 dB). Figure 12b shows the comparison of SSIM between our proposed method with other watermark methods for the Lena image. From this Figure, we observed that the SSIM value of our proposed method (0.9998) is greater than the existing methods.

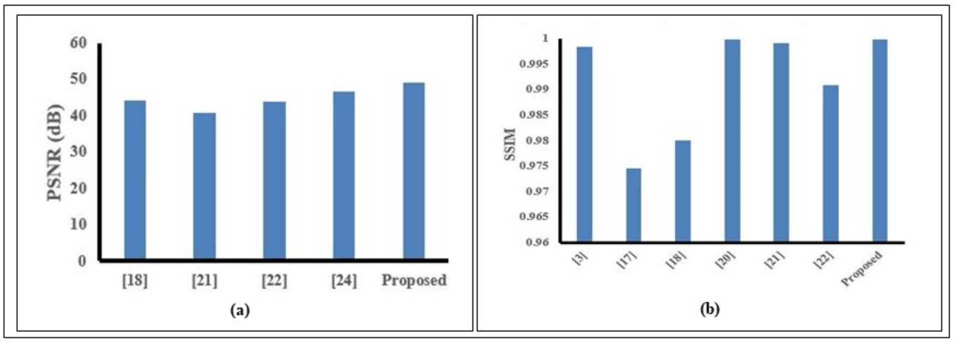

Figure 12. (**a**) PSNR values of various methods; (**b**) SSIM values of various methods.

Hence, our proposed method ensures better imperceptibility (high PSNR and SSIM) than the existing recent methods.

5.5.2. Robustness Comparison

We compared our proposed method for noise, filter, and blur attacks with state-of-the-art methods for chest X-ray images and found promising performance. In Figure 13, we compared SN and GN attacks with other methods. Figure 13a exhibits the highest NC value (0.9941) versus other methods for the SN attack. Moreover, Figure 13b displays the highest NC value (0.9923) versus existing methods for a GN attack. From Table 8, we found the highest NC value for SPN attack versus existing recent methods. We showed our comparison for MF and LPGF attacks in Figure 14. Here, Figure 14a exhibits the highest NC (0.9942) for our method versus others for the MF attack. For the LPGF attack in Figure 14b, our method shows the highest NC (0.9994) versus method [21], where NC = 0.9961. Also, we found a greater NC (0.9981) for our method than method [12], where NC= 0.9780 for the image blur attack.

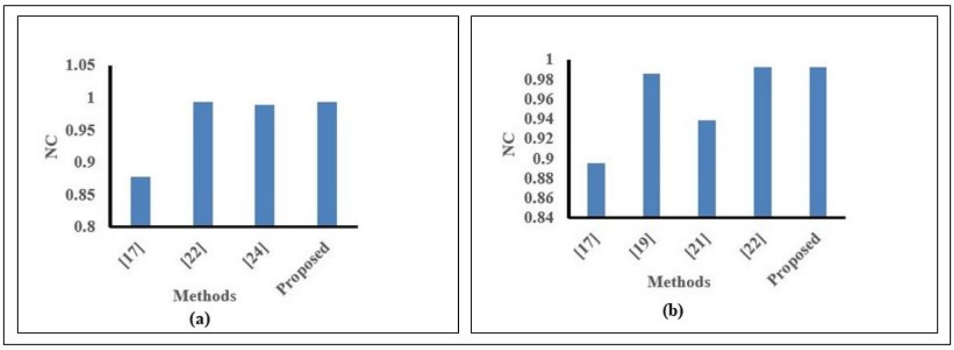

Figure 13. Comparison of Robustness (**a**) for SN attack; (**b**) for GN attack.

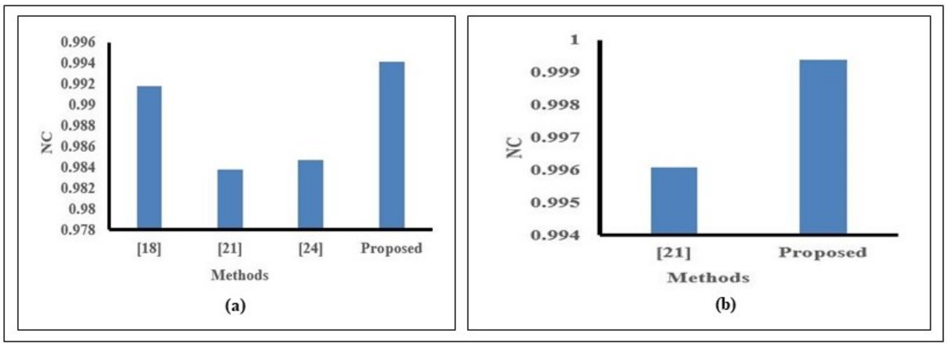

Figure 14. Comparison of Robustness (**a**) for MF attack; (**b**) for LPGF attack.

Table 8. Comparison of Robustness for SPN Attack with recent methods by NC.

Reference	SPN
Begum et al., 2021 [3]	0.9912
Begum et al., 2021 [17]	0.8734
Alzahrani et al., 2021 [18]	0.9846
Srivastava et al., 2021 [19]	0.9855
Thanki et al., 2021 [21]	0.9835
Yasmeen et al., 2021 [22]	0.9932
Zeng et al., 2022 [23]	0.9644
Proposed Method	0.9951

6. Conclusions and Future Work

This paper proposed a hybrid robust invisible image watermarking by combining DWT and SVD. The proposed method is tested on different groups of host images, and the performance is compared with recent methods in the literature. It ensures an effective image authentication as it uses invisible image watermarking. It is observed that the proposed method showed superiority over the existing methods in terms of imperceptibility and robustness. Our proposed method ensures better imperceptibility, which is 48.9688 dB. Compared to the existing advanced methods, the method also provides enhanced robustness against noise, filter, and image blur attacks. For noise attacks, average NC values are close to 1 and greater than other existing methods. For filter attacks, our average NC value is 0.9876, which is greater than the existing methods. For image blur attack, we found higher NC value of 0.9981 than other methods. The Arnold map increases the system's security. The original watermark and decrypted watermark are identical for our method as the SSIM value of these two images is 1. DWT reduces the inserting capacity into the cover or host image and also leads to failure in extracting the watermark image due to its shift variance property. In the future, we will work with redundant DWT to overcome these issues. The FPD problem, however, is a limitation of the suggested technique and is not addressed in this study. In future work, we will address this issue and work with other intentional and unintentional attacks along with removal and brute-force attacks in conjunction with genetic and neural network-based optimization techniques, in order to test the system's robustness and implement our method for any watermark image size, while simultaneously maintaining proper balance among basic design requirements. Also, we will use deep learning and diverse interpolation-based methods for geometric attacks like image resizing, rotation, and cropping. In blind watermarking, the watermark can be accurately extracted from the watermarked image while preserving the quality and integrity of the host image. To achieve a blind watermarking capability is essential for practical applications, as the original image is not always feasible or available. In the future, we will extend our method for blind image watermarking. Secure authentication in the context of the Internet of Things (IoT) is a current open research issue [38]. Moreover, image watermarking using a generative adversarial network provides more robustness against noise interference compared to the existing methods [39]. A photo response non-uniformity-based forgery detection method in image watermarking also proves their effectiveness in detecting forgeries of digital images [40]. User-unaware watermarks can be effectively used in detecting fake profiles of any social network, where the photo response non-uniformity method shows more effectiveness compared to the state-of-the-art methods [41]. In the future, we will work with generative adversarial networks, photo response non-uniformity, or user-unaware watermarks to enhance the robustness of our method. Also, block truncation coding is used to protect multimedia content from unauthorized access [42]. Moreover, the adaptive information hiding technique is currently used to secure embedded information based on the feature extraction method [43]. In the future, we will enhance the security of the system with a block truncation coding framework and IoT or visible light communication-based adaptive security techniques. If we remove the watermark using the same Arnold mapping process that was used to embed it, we might not be able to restore the original unwatermarked image that reflects the reversible image watermarking. In the future, we will work with an optimized scaling factor or adaptive techniques to choose the value of the watermark strength alpha. In addition, we will work with blind reversible image watermarking to reconstruct the original host or the unwatermarked image after watermark extraction. Moreover, we will incorporate RGB color images and other multimedia elements into this hybrid grayscale image watermarking method.

Author Contributions: Conceptualization, M.B. and M.S.U.; Methodology, M.B., S.B.S. and J.F.; Software, M.B., S.B.S. and J.F.; Validation, J.F.; Formal analysis, M.B.; Investigation, M.B., M.S.U. and M.W.; Resources, M.S.U. and T.J.; Data curation, S.B.S. and J.F.; Writing—original draft, M.B.; Writing—review & editing, T.J., A.B. and M.W.; Supervision, M.S.U.; Project administration, M.S.U.; Funding acquisition, A.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research is partially supported by the Australian Research Council Discovery Project: DP210101864.

Data Availability Statement: Data are contained within the article.

Acknowledgments: The authors are thankful to the Information and Communication Technology Division of the Government of the People's Republic of Bangladesh for a Ph.D. fellowship to Mahbuba Begum.

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

References

1. Cox, I.; Miller, M.; Bloom, J.; Fridrich, J.; Kalker, T. *Digital Watermarking and Steganography*; Morgan Kaufmann: San Francisco, CA, USA , 2007.
2. Singh, R.K.; Shaw, D.K.; Sahoo, J. A secure and robust block based DWT-SVD image watermarking approach. *J. Inf. Optim. Sci.* **2017**, *38*, 911–925. [CrossRef]
3. Begum, M.; Ferdush, J.; Uddin, M.S. A Hybrid robust watermarking system based on discrete cosine transform, discrete wavelet transform, and singular value decomposition. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 5856–5867. [CrossRef]
4. Zhao, X.; Ho, A.T. An introduction to robust transform based image watermarking techniques. *Intell. Multimed. Anal. Secur. Appl.* **2010**, *282*, 337–364.
5. Tao, H.; Chongmin, L.; Zain, J.M.; Abdalla, A.N. Robust image watermarking theories and techniques: A review. *J. Appl. Res. Technol.* **2014**, *12*, 122–138. [CrossRef]
6. Giakoumaki, A.; Pavlopoulos, S.; Koutsouris, D. Multiple image watermarking applied to health information management. *IEEE Trans. Inf. Technol. Biomed.* **2006**, *10*, 722–732. [CrossRef] [PubMed]
7. Lei, B.; Soon, Y.; Zhou, F.; Li, Z.; Lei, H. A robust audio watermarking scheme based on lifting wavelet transform and singular value decomposition. *Signal Process.* **2012**, *92*, 1985–2001. [CrossRef]
8. Lei, B.; Soon, Y.; Tan, E.L. Robust SVD-based audio watermarking scheme with differential evolution optimization. *IEEE Trans. Audio Speech Lang. Process.* **2013**, *21*, 2368–2378. [CrossRef]
9. Lei, B.; Ni, D.; Chen, S.; Wang, T.; Zhou, F. Optimal image watermarking scheme based on chaotic map and quaternion wavelet transform. *Nonlinear Dyn.* **2014**, *78*, 2897–2907. [CrossRef]

10. Megalingam, R.K.; Nair, M.M.; Srikumar, R.; Balasubramanian, V.K.; Sarma, V.S.V. Performance comparison of novel, robust spatial domain digital image watermarking with the conventional frequency domain watermarking techniques. In Proceedings of the 2010 International Conference on Signal Acquisition and Processing, Bangalore, India, 9–10 February 2010; pp. 349–353.
11. Rasti, P.; Anbarjafari, G.; Demirel, H. Colour image watermarking based on wavelet and QR decomposition. In Proceedings of the 2017 25th Signal Processing and Communications Applications Conference (SIU), Antalya, Turkey, 15–18 May 2017; pp. 1–4.
12. Singh, S.; Singh, R.; Singh, A.K.; Siddiqui, T.J. SVD-DCT based medical image watermarking in NSCT domain. *Quantum Comput. Environ. Intell. Large Scale Real Appl.* **2018**, *33*, 467–488.
13. Najafi, E.; Loukhaoukha, K. Hybrid secure and robust image watermarking scheme based on SVD and sharp frequency localized contourlet transform. *J. Inf. Secur. Appl.* **2019**, *44*, 144–156. [CrossRef]
14. Zhou, X.; Zhang, H.; Wang, C. A robust image watermarking technique based on DWT, APDCBT, and SVD. *Symmetry* **2018**, *10*, 77. [CrossRef]
15. Liu, J.; Huang, J.; Luo, Y.; Cao, L.; Yang, S.; Wei, D.; Zhou, R. An optimized image watermarking method based on HD and SVD in DWT domain. *IEEE Access* **2019**, *7*, 80849–80860. [CrossRef]
16. Dhar, P.K.; Hazra, P.; Shimamura, T. Blind color image watermarking using fan Beam transform and QR decomposition. *Symmetry* **2020**, *12*, 486. [CrossRef]
17. Begum, M.; Uddin, M.S. Implementation of secured and robust DFT-based image watermark through hybridization with decomposition algorithm. *SN Comput. Sci.* **2021**, *2*, 221. [CrossRef]
18. Alzahrani, A.; Memon, N.A. Blind and robust watermarking scheme in hybrid domain for copyright protection of medical images. *IEEE Access* **2021**, *9*, 113714–113734. [CrossRef]
19. Srivastava, R.; Tomar, R.; Gupta, M.; Yadav, A.K.; Park, J. Image watermarking approach using a hybrid domain based on performance parameter analysis. *Information* **2021**, *12*, 310. [CrossRef]
20. Nejati, F.; Sajedi, H.; Zohourian, A. Fragile watermarking based on QR decomposition and Fourier transform. *Wirel. Pers. Commun.* **2022**, *122*, 211–227. [CrossRef]
21. Thanki, R.; Kothari, A.; Borra, S. Hybrid, blind and robust image watermarking: RDWT–NSCT based secure approach for telemedicine applications. *Multimed. Tools Appl.* **2021**, *80*, 27593–27613. [CrossRef]
22. Yasmeen, F.; Uddin, M.S. An efficient watermarking approach based on LL and HH edges of DWT–SVD. *SN Comput. Sci.* **2021**, *2*, 82. [CrossRef]
23. Zeng, F.; Bai, H.; Xiao, K. Blind watermarking algorithm combining NSCT, DWT, SVD, and HVS. *Secur. Priv.* **2022**, *5*, e223. [CrossRef]
24. Da Cunha, A.L.; Zhou, J.; Do, M.N. The nonsubsampled contourlet transform: Theory, design, and applications. *IEEE Trans. Image Process.* **2006**, *15*, 3089–3101. [CrossRef] [PubMed]
25. Discrete Wavelet Transform. Wikipedia. Available online: https://en.wikipedia.org/wiki/Discrete_wavelet_transform (accessed on 1 April 2023).
26. Begum, M.; Uddin, M.S. Digital image watermarking techniques: A review. *Information* **2020**, *11*, 110. [CrossRef]
27. Kalman, D. A singularly valuable decomposition: The SVD of a matrix. *Coll. Math. J.* **1996**, *27*, 2–23. [CrossRef]
28. Ford, W. *Numerical Linear Algebra with Applications: Using MATLAB*; Academic Press: Cambridge, MA, USA, 2014.
29. Pratt, W.K. *Introduction to Digital Image Processing*; CRC Press: Boca Raton, FL, USA, 2013.
30. Netravali, A. *Digital Pictures: Representation and Compression*; Springer Science & Business Media: Boston, MA, USA, 2013.
31. Chen, J.M.; Lin, P. A reliable enhanced watermarking based on NSCT and SVD. *Adv. Inf. Sci. Serv. Sci.* **2013**, *5*, 629.
32. Database. Available online: http://sipi.usc.edu/database/ (accessed on 14 May 2023).
33. Image Databases—Imageprocessingplace.com. Available online: https://imageprocessingplace.com/root_files_V3/image_databases.htm (accessed on 17 June 2023).
34. Chest X-ray Images (Pneumonia)—kaggle.com. Available online: https://www.kaggle.com/paultimothymooney/chest-xray-pneumonia (accessed on 17 June 2023).
35. ECG Heartbeat Categorization Dataset—kaggle.com. Available online: https://www.kaggle.com/shayanfazeli/heartbeat/ (accessed on 17 June 2023).
36. Srinivasan, S. Fish Species Image Data. Kaggle, Year of Dataset Publication. Available online: https://www.kaggle.com/sripaadsrinivasan/fish-species-image-data/ (accessed on 14 May 2023).
37. Aalborg University Brackish Dataset. Kaggle, 2023. Available online: https://www.kaggle.com/aalborguniversity/brackish-dataset/ (accessed on 14 May 2023).
38. Qiu, J.; Tian, Z.; Du, C.; Zuo, Q.; Su, S.; Fang, B. A Survey on Access Control in the Age of Internet of Things. *IEEE Internet Things J.* **2020**, *7*, 4682–4696. [CrossRef]
39. Hao, K.; Feng, G.; Zhang, X. Robust image watermarking based on generative adversarial network. *China Commun.* **2020**, *17*, 131–140. [CrossRef]
40. Lin, X.; Li, C.T. Refining PRNU-based detection of image forgeries. In Proceedings of the 2016 Digital Media Industry & Academic Forum (DMIAF), Santorini, Greece, 4–6 July 2016; pp. 222–226. [CrossRef]
41. Bertini, F.; Sharma, R.; Montesi, D. Are Social Networks Watermarking Us or Are We (Unawarely) Watermarking Ourself? *J. Imaging* **2022**, *8*, 132. [CrossRef]

42. Li, M.; Liu, C.; Shan, C.; Song, H.; Lv, Z. A Dual-Embedded Tamper Detection Framework Based on Block Truncation Coding for Intelligent Multimedia Systems. *Inf. Sci.* **2023**, *649*, 119362. [CrossRef]
43. Li, M.; Shan, C.; Tian, Z.; Du, X.; Mohsen, G. Adaptive Information Hiding Method Based on Feature Extraction for Visible Light Communication. *IEEE Commun. Mag.* **2023**, *61*, 102–106. [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.