




Article

Secure Exchange of Medical Data Using a Novel Real-Time Biometric-Based Protection and Recognition Method

Shams Ud Din ¹, Zahoor Jan ¹, Muhammad Sajjad ^{1,*}, Maqbool Hussain ^{2,3,*} , Rahman Ali ⁴ , Asmat Ali ⁵  and Sungyoung Lee ^{6,*}

¹ Digital Image Processing Lab, Department of Computer Science, Islamia College University, Khyber Pakhtunkhwa, Peshawar 25000, Pakistan; srehamncs@icp.edu.pk (S.U.D.); zahoor.jan@icp.edu.pk (Z.J.)

² Department of Software, Sejong University, Seoul 05006, Korea

³ Department of Computer Science and Engineering, Oakland University, Rochester, MI 48309, USA

⁴ Quaid-e-Azam College of Commerce, University of Peshawar, Khyber Pakhtunkhwa, Peshawar 25000, Pakistan; rehmanali@uop.edu.pk

⁵ Department of Computer Science, University of Peshawar, Khyber Pakhtunkhwa, Peshawar 25000, Pakistan; aasmat76@gmail.com

⁶ Department of Computer Engineering, Kyung Hee University, Yongin 446-701, Korea

* Correspondence: muhammad.sajjad@icp.edu.pk (M.S.); maqbool.hussain@sejong.ac.kr (M.H.); sylee@oslab.khu.ac.kr (S.L.)

Received: 24 September 2020; Accepted: 13 November 2020; Published: 28 November 2020



Abstract: Security and privacy are essential requirements, and their fulfillment is considered one of the most challenging tasks for healthcare organizations to manage patient data using electronic health records. Electronic health records (clinical notes, images, and documents) become more vulnerable to breaching patients' privacy when shared with an external organization in the current arena of the internet of medical things (IoMT). Various watermarking techniques were introduced in the medical field to secure patients' data. Most of the existing techniques focus on an image or document's imperceptibility without considering the watermark (logo). In this research, a novel technique of watermarking is introduced, which supersedes the shortcomings of existing approaches. It guarantees the imperceptibility of the image/document and takes care of watermark (biometric), which is further passed through a process of recognition for claiming ownership. It extracts suitable frequencies from the transform domain using specialized filters to increase the robustness level. The extracted frequencies are modified by adding the biomedical information while considering the strength factor according to the human visual system. The watermarked frequencies are further decomposed through a singular value decomposition technique to increase payload capacity up to (256×256) . Experimental results over a variety of medical and official images demonstrate the average peak signal-to-noise ratio (PSNR 54.43), and the normal correlation (N.C.) value is 1. PSNR and N.C. of the watermark were calculated after attacks. The proposed technique is working in real-time for embedding, extraction, and recognition of biometrics over the internet, and its uses can be realized in various platforms of IoMT technologies.

Keywords: medical images; biometric watermark; electronic health record privacy; biometric recognition and real-time processing

1. Introduction

The exponential growth of communication over the internet expands the benefits of multimedia (e.g., image, audio, video) in various aspects. It inspires the users to consider it as a preferable choice for communication [1]. The flow of digital content in emerging medical sharing platforms using the internet of medical things (IoMT) technologies requires communication links that are safe and secure from unauthorized and illegal tampering [2]. Digital content sent over insecure and treacherous links can be replicated, tempered, and destroyed due to advancements in multimedia technologies, causing unbearable consequences. In this context, preliminary efforts have been made to enable access controls for IoT systems, facilitating user-controlled access to privileged digital resources [3]. To adequately address issues of security, the concept of digital watermarking emerged to protect the copyright of digital content [4]. There has been a multifold endeavor for the preferment of digital image watermarking techniques. The primary considerations of watermarking are the imperceptibility and recovering of the watermark.

Digital watermarking techniques describe the embedding and extraction of digital content. Protection and authentication are managed collectively in watermarking—the optimization of watermarking concluded by the recognition of the owner of the digital content. In the embedding process, the watermark is embedded into the host image for authentication while the host image and watermark are recovered during the process of extraction [5]. Watermarked videos from global news organizations, hidden communications, broadcast tracking, and copyright protection are well-known examples of digital watermarking.

Watermarking techniques are categorized into two domains: spatial domain and transform domain. The spatial domain entails less processing time and less hardware complexity for both visible and invisible watermarking [5]. These watermarking techniques are mostly simple and directly alter the values of the selected or appropriate pixels of the host image. However, these schemes have very low payload and are not robust enough. Least significant bit watermarking is an example of spatial domain watermarking [6]. On the other hand, transform domain watermarking techniques have improved robustness, payload, and imperceptibility. The transform domain is more robust than the spatial domain as it alters the desired properties to refine and overshadow for evaluation. Intentional and unintentional attacks are the set point for this domain. There are various types of transform domains, such as discrete fourier transform (DFT), discrete cosine transform (DCT), and discrete wavelet transform (DWT) [7]. These methods ensure robustness and high imperceptibility compared to the spatial domain. However, their computational cost is higher than the spatial domain. Every transformation has some uniqueness in properties [8] as well as some weaknesses, which are usually reduced by combining two or more transformations [9].

A large number of watermarking techniques have been introduced in the past. Spatial domain watermarking in the earlier era has been introduced for both visible and invisible watermarking. In recent years, the frequency domain has been introduced for watermarking due to their special properties, which resist attacks. Transform domains have different properties that are valuable against different attacks. For instance, frequency Fourier transforms (FFT, FRFT) are rotation invariant [10] but are not resilient against noise and other attacks. The discrete wavelet domain has better robustness and imperceptibility but possesses less resistance against geometric attacks with specific degrees. To enhance the capability of resiliency against attacks, integer and redistributed wavelet domains have been used with coefficient decomposition methods such as singular value decomposition (SVD) and quantization index modulation (QIM). However, cropping and copying attacks can still destroy the watermark in these methods. Robustness and imperceptibility are equally essential for a technique for which scaling factors are adopted by different evolutionary algorithms such as genetic algorithms and the artificial bee colony (ABC) algorithm [4]. In some methods, a specific ratio for extraction of the watermark is detected by using a support vector machine (SVM) and least-squares support vector machine (LS-SVM) [9]. The watermarked image's imperceptibility can be increased by selecting the

appropriate level of scaling factor, which is usually selected according to the human visual system (HVS). The trade-off gives both robustness and imperceptibility against different attacks [11].

In Reference [5], a system for digital watermarking by combining DWT and DCT is proposed. A DWT domain is used to obtain middle frequencies, and then DCT is applied to extract the final coefficients. The genetic algorithm is used to achieve a predefined image quality after watermark insertion. In Reference [2], the authors presented a technique for tampering detection and self-recovery using SVD. The self-recovery key is used for recovery while a random block-mapping sequence and three unique optimizations are employed to improve efficiency through SVD. In Reference [10], DWT and FRFT are combined by first extracting the middle frequencies and then applying FRFT to the extracted middle frequencies. It resists geometrical attacks to some extent. In Reference [12], a rotation-invariant method is proposed using a 2-D fractional Fourier transform, where detection and extraction are performed with the key. Authors in [13] have proposed a watermarking technique by combining different algorithms such as DWT, SVD, DCT, and QIM. In Reference [14], a technique based on IWT, SVD, and LS-SVM is proposed. First, the image is transformed into the integer wavelet domain. Then the L.L. band is divided into 4×4 blocks, followed by SVD. A least-squares support vector machine (LS-SVM) is used for embedding and extraction.

The techniques presented so far for protection and recognition have some significant problems concerning the low level of imperceptibility after several attacks—such as rotational or cropping attacks. A technique with robustness against geometrical attacks usually fails against filtering attacks, and vice versa. But, the imperceptibility of the recovered watermark is still a challenge for the methods mentioned above. This paper overcomes these problems by proposing a robust digital image watermarking technique using FFT with verified strength factor according to HVS. The FFT is applied to the host image and watermark image (fingerprint, logo) simultaneously in real-time. The embedded frequencies from both host images are selected using a special filter, maintaining the robustness, imperceptibility, and watermark recognition after extraction. The higher scores of normalized correlation and peak signal to noise ratio prove the robustness and imperceptibility of the proposed technique. The host images (official documents, degrees, bank statements, and payrolls) are tested by manipulating intentional and unintentional attacks, showing the resiliency against different attacks.

The main contributions of this work in terms of imperceptibility, robustness, payload, and cost-effectiveness are summarized as follows:

- **Imperceptibility preservation:** The proposed work not only preserves the imperceptibility of the cover image, but it also maintains the imperceptibility of the recovered watermark. The preservation of both the host image and the watermarked image is achieved through a specialized filter to extract the middle range of frequencies and order of SVD, which are used as a decomposer in the proposed framework. For increasing the payload and maintaining the imperceptibility level for both host and watermark images, SVD is used in the proposed framework.
- **Robustness:** Extensive experimental verification from different perspectives proved the robustness of the proposed framework against intentional and unintentional attacks in a real-time environment. The incorporation of the proposed framework into the frequency domain and the decomposition of the middle frequencies extracted via specialized filters nourish the proposed algorithm to resist intentional and unintentional attacks.
- **Payload:** The embedding capacity in the proposed technique increases while maintaining imperceptibility and robustness. The coefficients acquired by decomposing the middle frequencies of the watermarked image and host image guarantee the trade-off between imperceptibility, robustness, and payload. Payload increases due to the embedding in the diagonal matrix in decomposition SVD; the imperceptibility is not affected due to the suitable frequencies using a special filter.
- **Cost-Effectiveness:** Embedding, recovery, and verification of the watermarked can be performed in real-time. After recovery of the watermark, the proposed framework not only retains reasonable

accuracy of watermark recognition but also authenticates the originality of the cover image in real-time.

- The proposed technique can also be used for official correspondence and medical images, and other standard medical documents such as HL7 CDA (clinical document architecture), HL7 CCD (continuity of care documents). The specialized filter and diagonal matrix provide the facility to protect the official or medical documents from unauthorized access. The application has many advantages to secure the ownership with human identification property (fingerprint) such as statements, letters, medical images.

The proposed technique is a candidate solution to exchange secure documents within and across healthcare provider networks. It enables various healthcare applications—electronic medical records (EMR), personal healthcare records (PHR), and picture archiving and communication systems (PACS)—to exchange secure medical data by fulfilling the regulatory patient security and access policies.

The rest of the paper is organized as follows: Section 2 describes the literature review. Section 3 demonstrates the proposed system. Sections 4 and 5 show the experimental results and discussion, followed by the conclusion in Section 6.

2. Related Work

The section is categorized into spatial domain and frequency domain; the literature focuses on frequency domain because the proposed technique is developed in the frequency domain. Furthermore, the frequency domain, classified into fast Fourier transform, DCT, and DWT, combines two or more domains to achieve the property's best level. For opting, the scaling factor automatically machine learning algorithm is used with these transfer domains.

In the spatial domain, Ruizhen Liu and Tieniu Tan [15] proposed a technique for protecting rightful ownership through singular value decomposition (SVD). It provides trustworthy evidence for protecting rightful ownership. Second, it resists distortions due to joint image manipulations. The spatial domain technique is directly applied for the host image to be decomposed in SVD. The watermark is also decomposed for embedding. The method is not robust against various attacks. Chen et al. [16] proposed a technique that only focused on copy attack, where they embedded two watermarks: a periodic watermark and a real watermark by modifying the gray level intensities. There is no usage of host image when watermarks are detected. The technique is robust against print and scanning but failed against several attacks, including rotational, cropping, and scaling. Chang et al. [17] proposed a technique for recovery and temper detection. The LBP operator is used to generate the authentication pattern, which is embedded in the local binary pattern of the 3×3 matrix of the entire, used for recovery and tempering detection. This domain's main flaw is that it cannot resist geometrical, filtering, and cropping attacks. Yunfa Li et al. [18] proposed a user authentication technique using multi-point collaboration on the user image. The method enhances the security system level by capturing and recognizing the image in real-time while all the required system's parameters separate from it. The system protects the information using three-party collaboration for authentication and recognition. The system is reliable to some extent, as it resists some penetrating attacks.

Using fast Fourier transformation, Solanki et al. [19] proposed a technique in DFT, where selective embedding hides information in low-frequency magnitudes and the differential quantization index hides information in the phase of Fourier form to achieve robustness against print and scanning attack. The payload is impressive, but the technique is semi-blind, which does not fully guarantee robustness against different noise attacks. Pramila et al. [20] proposed a technique in multiple domains. In this technique, the templates are embedded into DFT and spatial domain for rotation, scaling, and translation, respectively. The message is embedded into the wavelet domain for robustness. The schema is robust against copy scanning and compression, but the efficiency of the algorithm is not impressive, and it failed against cryptographic attack (cracking the key) and protocol attack (attack on the entire concept). Chun-pung et al. [21] proposed a watermarking algorithm that is robust against geometrical attacks by using radial harmonic Fourier moments (RHFm). The algorithm obtains the

coefficient of the original image in the form of radial harmonic Fourier moments and selected a robust coefficient for modifying or embedding the most suitable watermark; during extraction, the image is reconstructed without concerning the original image. The algorithm is robust against the geometrical attack; it cannot resist some level of compression and specific filtering [22]. It is a technique of digital watermarking to establish the links that exist between the DFT and RGB color channels and the components of quaternion DFT (QDFT) coefficients while considering a general unit pure to embed the watermark. Qingtang Su and Yugangu Niu [23] proposed a technique of blind image watermarking. Firstly, the image is divided into 4×4 blocks, and then the pixels of each block are decomposed by Q.R. (quick response) decomposition, and the first-row fourth column element in the matrix is quantified. This technique is less robust against compression and noise attacks. Furthermore, Jun Lang and Zheng-Guang Zhang [6] proposed a watermarking technique with similar design goals. First, the image divides into non-overlapping blocks. They take 2-D FRFT of each block, each pixel value of the binary watermark is embedded by modifying the back-diagonal FRFT coefficients of each image block at the same location with a random array. This technique is less robust against compression and geometrical attacks. In conclusion, the techniques in this domain cannot resist compression, intentional filtering, and intentional geometrical attacks.

In a discrete cosine transform, Shinfeng et al. [24] proposed a technique in discrete cosine transformation to improve robustness. The watermark is embedded in selected low frequencies; it resists the JPEG compression. Although the result is convincing, the imperceptibility of the watermarked image is very low. Cropping and row-column flipping attacks have also destroyed the watermark. Frank et al. [25] proposed a watermarking technique for medical image watermarking using the frequency domain. In this technique, the host medical image is divided into a region of interest (ROIs) and with a minimum number of blocks belongs to the region of noninterest (RONIs). The watermark is compressed and embedded into the discrete cosine domain of the region of noninterest blocks (RONI) of a medical image. The technique shows robustness against various attacks but failed against geometrical and resizing attacks. X.Wu et al. [26] proposed a watermarking technique using DCT. In this technique, the image is separated into overlapping blocks, and the DCT is applied for the D.C. map. A random series of a map is decomposed (SVD) for ownership share. This technique does not resist rotation and cropping attacks. Musrrat Ali and Chang Wook Ahn [27] proposed a watermarking technique using DCT. The host image is divided into non-overlapping blocks; DCT is applied on each block to obtain a low-level approximation of the direct components (D.C.) of each of the images collected. The SVD is applied to both D.C. of the host and watermark. Differential evolution (D.E.) algorithm is used to obtain the best multiple scaling factors for embedding. The technique is not capable of resisting rotational and cropping attacks. The techniques of this domain suffer from rotational and cropping attacks.

In a discrete wavelet transform, Chun-Shien et al. [28] proposed a watermarking technique in the discrete wavelet domain for copyright protection. The approach uses cocktail watermarking; two watermarks are embedded in DWT after quantizing the wavelet coefficient as making threshold unite of the image. The method is not resistant against geometrical attacks, the imperceptibility of the watermarked image is still very low. C.Yin et al. [29] proposed a color image watermarking schema in DWT. In this technique, the green channel is decomposed into the wavelet coefficient of the singular value decomposition of the L.H., H.L., H.H., added with SVD of the scramble watermark. The technique is robust against various attacks, but it does not show resistance against geometrical attacks and some filtering attacks. Nasrin et al. [30] proposed watermarking using the integer wavelet domain to solve the problem of false-positive. In this algorithm, the problem of false-positive is solved by generating the digital signature. The watermark is embedded into the first level of singular value decomposition of the integer wavelet domain. This technique addresses the shortcomings of conventional techniques; however, it is less robust against translation, sheering, and geometrical attacks. Chetan et al. [31] proposed a watermarking technique for protecting document images using the integer wavelet domain. The document is divide into empty and non-empty non-overlapping blocks; the non-empty blocks

transform into integer wavelet domain up to two-level. The binary logo is compressed by binary block coding and embedded into the integer wavelet domain of the document image. The payload is reduced, but the watermark destroys the compression attack and noise attack. The technique of this domain is not effective against geometrical, embedding capacity, and intentional filter attacks. Liu et al. [32] proposed a video-based technique in a discrete wavelet transform. It analyzes the frames rapidly and selects the frames with distortion. In addition to distortion, it also analyzes the embedded position and hence maximizes the peak signal-noise ratio. The system is resilient against various attacks, but it has limitations in recovering the cropping of rows or columns from attack.

To achieve the benefits of multiple domains and machine learning algorithms at the same time, Santhi et al. [33] proposed an adaptive watermarking visible/invisible technique using Hadamard transform. In this technique, the image transforms into Hadamard, the watermark embedded with the adaptive scaling factor using a sigmoid function. The strength can be adjusted in the custom of visibility and invisibility of the watermark. The technique is less robust against geometrical, filtering, and compression attack. Yahya et al. [9] propose a watermarking technique using a discrete wavelet transform. In this technique, the image transforms into a discrete wavelet transform using the Haar wavelet; the binary watermark is embedded into the selected coefficient. The watermark is extracted using the probabilistic neural network without concerning the original. The technique is robust against most of the attacks, compressing and geometrical attacks still decreases the level of robustness. Wang et al. [34] proposed a watermarking technique using a polar harmonic transform. In this technique, the improved (SURF) is used for a set of feature point detection using probability density function. The affine invariant local elliptical region is constructed using local probability and then constructed the local circle region. Then polar harmonic transform is applied to the local circle region with zero paddings. The technique is robust against geometrical attacks and its various differentiations. The technique still does not resist against the median filter, scaling, cropping with the geometrical attack, and some compression levels. Bouslimi et al. [35] proposed a crypto-watermarking technique for medical images. This technique is based on quantization index modulation and joint watermarking-decryption. The watermark is embedded and encrypted at the receiver side. A watermark is used for decryption for authentication and traceability. The technique is not reliable in the account of various attacks. Wójtowicz et al. [36] proposed a watermarking technique using biometric information. The image is divided into four blocks and independent component analysis (ICA) is applied on those blocks for embedding the two watermarks: fingerprint and iris biometrics. The authentication is very impressive and reliable, but the technique has not shown resistance against specific attacks. M. Ali et al. [4] proposed a watermarking technique using the redistribution invariant wavelet domain. In this technique, the host image transforms into an invariant wavelet domain, the low-level frequency blocks further divide into the non-overlapping block; the most suitable block is selected using the human visual system (HVS). The targeted block is decomposed in singular value decomposition for embedding; the strengthen factor is obtained by the ABC algorithm for imperceptibility and robustness. This technique is robust against various attacks but still shows less robustness against the median filter, rescaling, and noise attacks. Sang et al. [37] proposed a hybrid DWT-DCT video watermarking technique. In this technique, randomly selected frames are transformed (DC components). All the selected frames organize column-wise, followed by a scrambling operation using Arnold Algorithm. Four DC components are reshaped for every column and transform into wavelets for embedding. The proposed technique shows robustness against most of the attacks except geometric attacks.

In conclusion, the existing digital image watermarking algorithms have the following limitations:

- Most of them rely on imperceptibility and robustness, but they failed to recover the full watermark after some attacks being applied.
- The algorithms are failed to facilitate in a real-time environment; they deal in the offline environment.

- Most of the existing algorithms do not embed the biometric as a watermark. If someone does so, then it is not recovered, which may be able to recognize entirely.
- The payload is a fundamental issue for the existing algorithms, as, concerning the watermark capacity, the algorithms are collapsible.

3. Research Methods

The proposed watermarking scheme uses a fast Fourier transform (FFT) to spread the watermark in the host image. The watermark should be added in the middle components for better imperceptibility and robustness. The abstract view of the embedding workflow is depicted in Figure 1. Details of each step are given in the following subsections with detailed pseudo-code in Algorithms 1 and 2. Before digging into the explanation, the readers are encouraged to look into the Abbreviation section for a list of symbols used throughout this section in different formalism and algorithms;

Algorithm 1 Embedding Algorithm

Input: Host image I_H , watermark I_w , secret key K_w , filter for host image F_{I_H} , filter for the watermark image F_{I_w}

Output: Watermarked image W_H^w

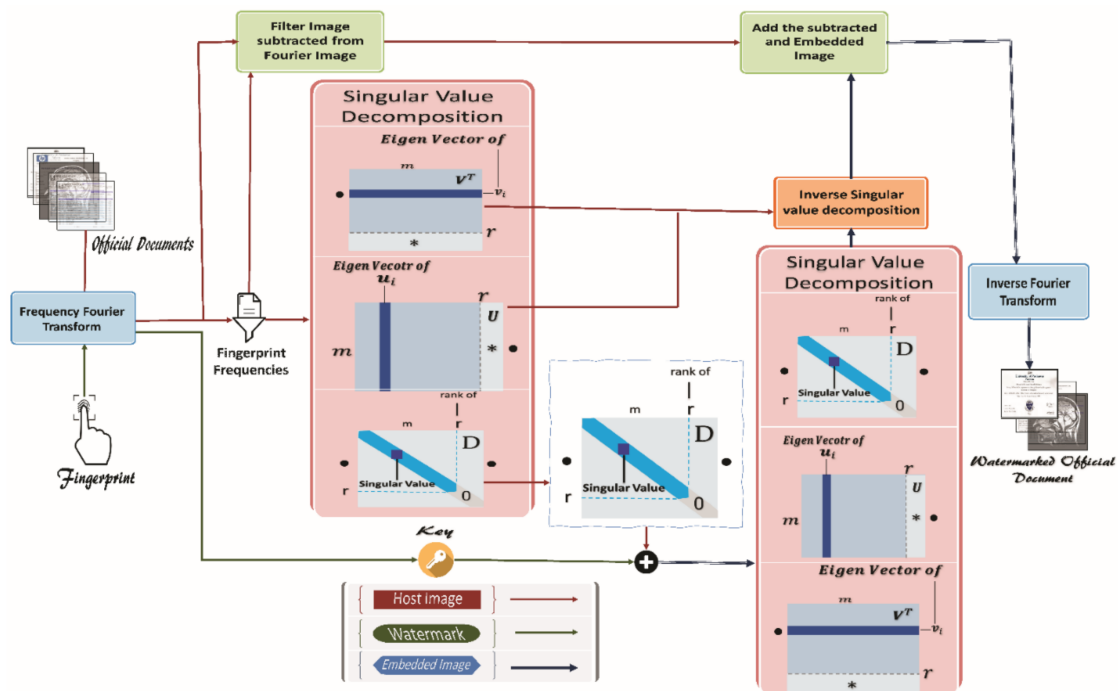
Steps:

1. Select an appropriate host image I_H .
2. Apply frequency Fourier transform on I_H .
3. Select watermark image I_w .
4. Apply frequency Fourier transform on I_w .
5. Apply filter on host image I_H , it becomes F_{I_H} .
6. Apply filter on watermark image I_w , it becomes F_{I_w} .
7. Now subtract F_{I_w} from the I_H to get I_H^F those frequencies which are not suitable for embedding.
 $I_H^F = I_H - F_{I_w}$.
8. Apply singular value decomposition on F_{I_H} , then it will generate two orthogonal matrices O_H^1, O_H^2 and one diagonal matrix D_H .
9. Encrypt the watermark I_w by secret key K_w , multiply resultant encrypted watermark $K_w^{I_w}$ with positive strength factor $\alpha = 10$.
10. The diagonal matrix of the host image D_H added with the encrypted watermark $K_w^{I_w}$, resultant embedded matrix $D_H^{K_w^{I_w}}$.
11. Calculate singular value decomposition of the embedded matrix $D_H^{K_w^{I_w}}$, three matrices will be formed, two orthogonal matrices $O_{D_H^W}^1, O_{D_H^W}^2$ and one diagonal matrix D_H^W .
12. Apply inverse singular value decomposition by multiplying the diagonal matrix of the embedded matrix D_H^W with the first orthogonal matrix O_H^1 and the transpose of the second orthogonal matrix $(O_H^2)^T$ to get I_H^w .
 $I_H^w = O_H^1 \times D_H^W \times (O_H^2)^T$
13. Add the I_H^F and I_H^w to get I_{FF}^W watermark image in the transform domain.

Apply inverse Fourier transform to get the watermarked image W_H^w .

Algorithm 2 Extraction Algorithm**Input:** Watermarked image W_H^w secret key K_w .**Output:** Host image I_H , watermark I_w

1. Select the received watermarked image W_H^w and its suitable parameters for detection and extraction.
2. Apply frequency Fourier transform on watermarked image W_H^w .
3. Apply singular value decomposition on watermarked image W_{fft}^H , then it will generate two orthogonal matrices $O_{W_{ff}}^1, O_{W_{ff}}^2$ and one diagonal matrix $D_{W_{ff}}^M$ of the watermarked image.
4. For restoring the host image, the encrypted watermark $K_w^{I_w}$ is subtracted from the diagonal matrix of the watermarked image $D_{W_H^w}$ and divided by the positive strength factor $\alpha = 10$; the resultant will be D_H^R .
5. Now, apply inverse singular value decomposition by multiplying the diagonal matrix of restoring host image D_H^R with the orthogonal matrix first O_H^1 and transpose the second orthogonal matrix $(O_H^2)^T$ of the host Image; the resultant matrix will be $I_H I_H = O_H^1 \times D_H^R \times (O_H^2)^T$.
6. Apply inverse Fourier transform to get I_H .
7. For restoring watermark, the diagonal matrix of the watermarked image $D_{W_H^w}$ is subtracted for the diagonal matrix of the host image D_H and divide it by the scaling factor $\alpha = 10$ to get the diagonal matrix of the encrypted watermark D_w^K .
8. Now, apply inverse singular value decomposition by multiplying the diagonal matrix of restoring watermark D_w^K with the orthogonal matrix first $O_{D_H}^1$, and transpose the second orthogonal matrix $(O_{D_H}^2)^T$ of the watermarked image, and the resultant matrix will be encrypted watermark $K_w^{I_w}$. $K_w^{I_w} = O_H^1 \times D_H^R \times (O_{D_H}^2)^T$.
9. Now, decrypt the encrypted watermark $K_w^{I_w}$ by secret key K_w , the resultant will be I_w .

**Figure 1.** Framework of the proposed technique for embedding.

3.1. Middle-Frequency Selection in FFT

The host image I_H is transformed into the spectral domain I_{fft} using Equation (1).

$$I_{fft}(r, c) = \sum_{R=1}^N \sum_{C=1}^M I_H(R, C) e^{-2\pi i(Rr/M)(Cc/N)} \quad (1)$$

where $I_{fft}(r, c)$ is the image in the spectral domain with indices $[0-M]$ and $c [0-N]$, $I_H(R, C)$ and size $M \times N$ is the original image with indices R and C and $e^{-2\pi i(Rr/M)(Cc/M)}$ is the Euler's formula

$$e^{-i\theta} = \cos \theta + i \sin \theta \quad (2)$$

In the same manner, the FFT is also applied to the watermark I_w to transform to FFT I_w^{fft} . The inverse FFT is applied to transform back to the spatial domain using Equation (3).

$$I_w(r, c) = \sum_{r=1}^M \sum_{c=1}^M I_{fft}(r, c) e^{-2\pi i(Rr/M)(Cc/M)} \quad (3)$$

The distribution of frequencies, i.e., low frequencies, middle frequencies, and high frequencies, in the shifted image is shown in Figure 2.



Figure 2. (a) Transform domain image (b) After shifting.

Among the different ranges of frequencies, middle frequencies are more suitable to embed the watermark. The shifting of frequencies is performed in a diagonal maneuver, as shown in Figure 2. However, to make the watermark more robust, frequencies from other ranks such as low and high are also mixed with the middle frequencies. The different frequencies bank of Figure 2 can be generated by keeping the mid-range frequencies and removing the other frequencies. To extract the frequencies as depicted in Figure 3c, Equation (6) is applied without attenuating the frequencies of the image within the range of radius R_{LPF} and cuts off the remaining frequencies lie outside the radius.

$$I_{fft}^l(r, c) = \begin{cases} I_{fft}(r, c) & \text{if } D_{LPF} \leq R_{LPF} \\ 0 & \text{otherwise} \end{cases} \quad (4)$$

where R_{LPF} is the radius for low pass filter and D_{LPF} is the distance between $I_{fft}(r, c)$ and $I_{fft}(\frac{M}{2}, \frac{N}{2})$ which can be computed as

$$D_{LPF} = \left[(r - M/2)^2 + (c - N/2)^2 \right]^{1/2} \quad (5)$$

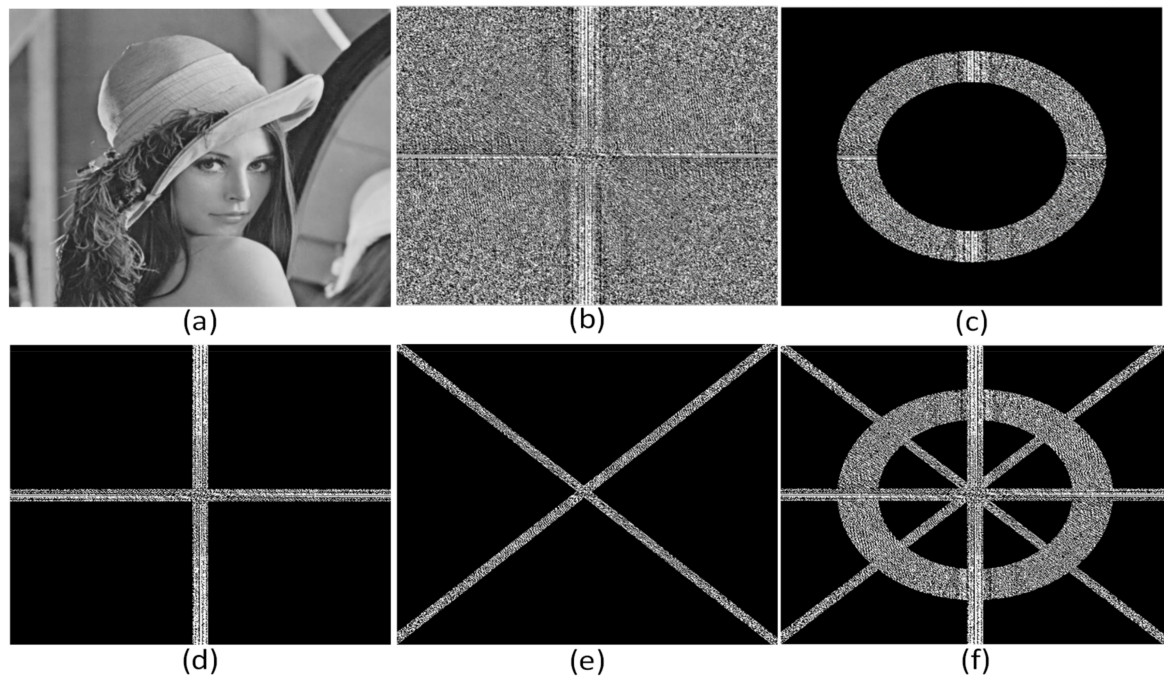


Figure 3. (a) Original Image (b) Fourier Image (c) Representation of difference between low and high pass filter in the frequency domain (d) Representation of low frequencies with minor edges in the frequency domain (e) Representation of selected horizontal, vertical, and diagonal edges in Frequency domain (f) Representation combining all filtered frequencies for embedding.

In the proposed technique, the high pass filter inverts the low pass filter without attenuation. All the frequencies cut off within the circle of radius R_{HPF} pass all the frequencies outside this circle.

$$I_{fft}^H(r, c) = \begin{cases} I_{fft}(r, c) & \text{if } D_{HPF} \leq R_{HPF} \xleftrightarrow{\quad} \text{and } \xleftrightarrow{\quad} D_{HPF} > R_{HPF} \\ 0 & \text{otherwise} \end{cases} \quad (6)$$

As R_{HPF} is the radius for the high pass filter and D_{HPF} the distance between $I_{fft}(r, c)$ and $tI_{fft}(\frac{M}{2}, \frac{N}{2})$ which can be computed as

$$D_{HPF} = \left[(r - M/2)^2 + (c - N/2)^2 \right]^{1/2} \quad (7)$$

In this step, we subtract the low pass filter frequencies I_{fft}^l from the original Fourier image I_{fft} and then high pass filter frequencies form the low pass filter subtracted Fourier image in Equations (8) and (9), respectively.

$$I_{fft}^{LH}(r, c) = \sum_{r=1}^M \sum_{c=1}^N I_{fft}(r, c) - I_{fft}^l(r, c) \quad (8)$$

Then

$$I_{fft}^{LH}(r, c) = \sum_{r=1}^M \sum_{c=1}^N I_{fft}^{LH}(r, c) - I_{fft}^H(r, c) \quad (9)$$

FFT spreads the low frequencies at the edges and corners; therefore, to bring these frequencies to the center, we have used shifting in which the low frequencies are shifted to the center of the Fourier image, the high frequencies are shifted to the corner, and some high frequencies (diagonal edges) are at diagonals of Fourier shifted image. We also need those low frequencies that are mixed with some high frequencies, to get middle frequencies or imperceptibility. Extracting those frequencies, as shown in Figure 3d, can be obtained by applying Equations (10) and (11). Those frequencies are obtained by

taking twenty columns from left to the center and twenty columns to the right for both horizontally I_{fft}^{SH} and vertically I_{fft}^{SV} $\alpha = 20$.

$$I_{fft}^{SV}(r, c) = \sum_{r=1}^M \sum_{c=1}^N I_{fft}(M/2 - \alpha : M/2 + \alpha, c : M) \quad (10)$$

The low frequencies and high information are shifted to the center of the FFT transformed image, to obtain only those frequencies that are suitable for embedding.

$$I_{fft}^{SH}(r, c) = \sum_{r=1}^M \sum_{c=1}^N I_{fft}(c : M, N/2 - \alpha : N/2 + \alpha) \quad (11)$$

The diagonal frequencies are also suitable and valuable frequencies for embedding to increase payload capacity and imperceptibility of the cover media. To extract the diagonal frequencies of the Fourier image, as shown in Figure 3e, Equation (14) has been applied.

Equation (12) is applied for the extraction of the diagonal frequencies from the left top corner to the right bottom corner.

$$I_D^1(r, c) = \sum_{r=1}^M \sum_{c=1}^N I_{fft}(\alpha : 1, c : N) \quad (12)$$

Equation (13) is applied for the extraction of the diagonal frequencies from the left top corner to the right bottom corner.

$$I_D^2(r, c) = \sum_{r=1}^M \sum_{c=1}^N I_{fft}(r : M, \alpha : 1) \quad (13)$$

By combining Equations (12) and (13), we get the diagonal frequencies to form high, middle, and low, which makes the technique consistent according to the said properties.

$$I_{D,D} = I_D^1 + I_D^2 \quad (14)$$

To sum up, all the required frequencies, as shown in Figure 3f by applying the Equation (14). The obtained frequencies guarantee the optimality of the technique in the custom of robustness, imperceptibility, and payload.

$$F_{IH} = I_{fft}^{SH} + I_{fft}^{SV} + I_{D,D} + I_{fft}^{LH} \quad (15)$$

The required frequencies mask subtracted from the Fourier host image to make the difference for recovering the original image more imperceptible.

$$F_{ft}^R(r, c) = I_{fft}^{SH}(r, c) - F_{IH}(r, c) \quad (16)$$

The mask for embedding the watermark, as shown in Figure 3f, will be subtracted by FFT of the host image using Equation (16).

These frequencies are mostly middle or near to middle frequencies, which are more suitable. Some low and high frequencies, which are significant in the custom of watermarking, have been selected.

3.2. Singular Value Decomposition (SVD)

The required frequencies are further decomposed to achieve imperceptibility and recognition of the watermark after extraction. The decomposed frequencies are represented in three matrices of two orthogonal matrices on one diagonal matrix, which contains Eigenvalues and vector. To select which matrix is suitable for embedding the watermark, we analyzed all the matrices. Parent techniques describe the significances of all matrix. The proposed technique guarantees the recovery of watermarking and its recognition, as it takes under consideration, we decompose the selected

frequencies by singular value decomposition. Therefore, we decomposed the $F_{I_H}(r, c)$ into UDV^T in Equation (17).

$$UDV^T = SVD(F_{I_H}) \quad (17)$$

$$SVD \begin{pmatrix} F_{I_H}(1,1) & F_{I_H}(1,2) & \cdots & F_{I_H}(1,N) \\ F_{I_H}(2,1) & F_{I_H}(2,2) & \cdots & F_{I_H}(2,N) \\ \vdots & \vdots & \ddots & \vdots \\ F_{I_H}(M,1) & F_{I_H}(M,2) & \cdots & F_{I_H}(M,N) \end{pmatrix} = \begin{pmatrix} U_{I_H}(1,1) & U_{I_H}(1,2) & \cdots & U_{I_H}(1,N) \\ U_{I_H}(2,1) & U_{I_H}(2,2) & \cdots & U_{I_H}(2,N) \\ \vdots & \vdots & \ddots & \vdots \\ U_{I_H}(M,1) & U_{I_H}(M,2) & \cdots & U_{I_H}(M,N) \end{pmatrix} \times$$

$$\begin{pmatrix} D_{I_H}(1,1) & 0 & 0 & 0 \\ 0 & D_{I_H}(2,2) & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & D_{I_H}(M,N) \end{pmatrix} \times \begin{pmatrix} V_{I_H}(1,1) & V_{I_H}(1,2) & \cdots & V_{I_H}(1,N) \\ V_{I_H}(2,1) & V_{I_H}(2,2) & \cdots & V_{I_H}(2,N) \\ \vdots & \vdots & \ddots & \vdots \\ V_{I_H}(M,1) & V_{I_H}(M,2) & \cdots & V_{I_H}(M,N) \end{pmatrix}^T$$

The decomposition is applied to filtered frequencies to obtain the optimum result in robustness; coefficients are decomposed into two orthogonal and one diagonal matrix. Previously, the embedding was done in the orthogonal matrices, but, in this method, the diagonal matrix is used for embedding. The diagonal matrix of the required frequencies added with encrypted watermarking by multiplying strengthen factor $\beta = 0.10$.

$$D_H^{K_w} = D \setminus + \beta \cdot K_w \quad (18)$$

To obtain the decomposition of the watermark, D_H^W we apply singular value decomposition on the embedded diagonal matrix $D_H^{K_w}$, same as Equation (16) and Equation (20). By decomposition, two orthogonal and one diagonal matrix are formed U_W , V_w^T , and D_H^W respectively.

$$U_W D_H^W V_w^T = SVD(D_H^{K_w}) \quad (19)$$

The embedded coefficient is further decomposed into singular value decomposition. The diagonal matrix D_H^W of the embedded matrix combined with an orthogonal matrix of the filter host image to get the watermarked required frequencies $F_{I_H}^w$ by applying Equation(20), it is also called inverse value decomposition.

$$F_{I_H}^w = U D_H^W V^T \quad (20)$$

To obtain the desired Fourier watermarked image I_{fft}^w , the required watermarked frequencies $F_{I_H}^w$ are added with the unembedded mask of the Fourier image $F_{fft}^R(r, c)$ by applying Equation (21). These frequencies are capable of enhancing the said properties of watermarking.

$$I_{fft}^w = F_{fft}^R + F_{I_H}^w \quad (21)$$

To obtain the resulting watermarked image of the spatial domain, W_H^w the watermarked Fourier image is inversely transformed into the spatial domain by applying Equation (21).

$$W_H^w = \sum_{r=1}^n \sum_{c=1}^m I_{fft}^w(r, c) e^{-2\pi i (Rr/n)(Cc/m)} \quad (22)$$

The extraction procedure is used in the same manner. After the extraction, the fingerprint watermark is recognized through VeriFinger software (see Algorithm 2 and Figure 4).

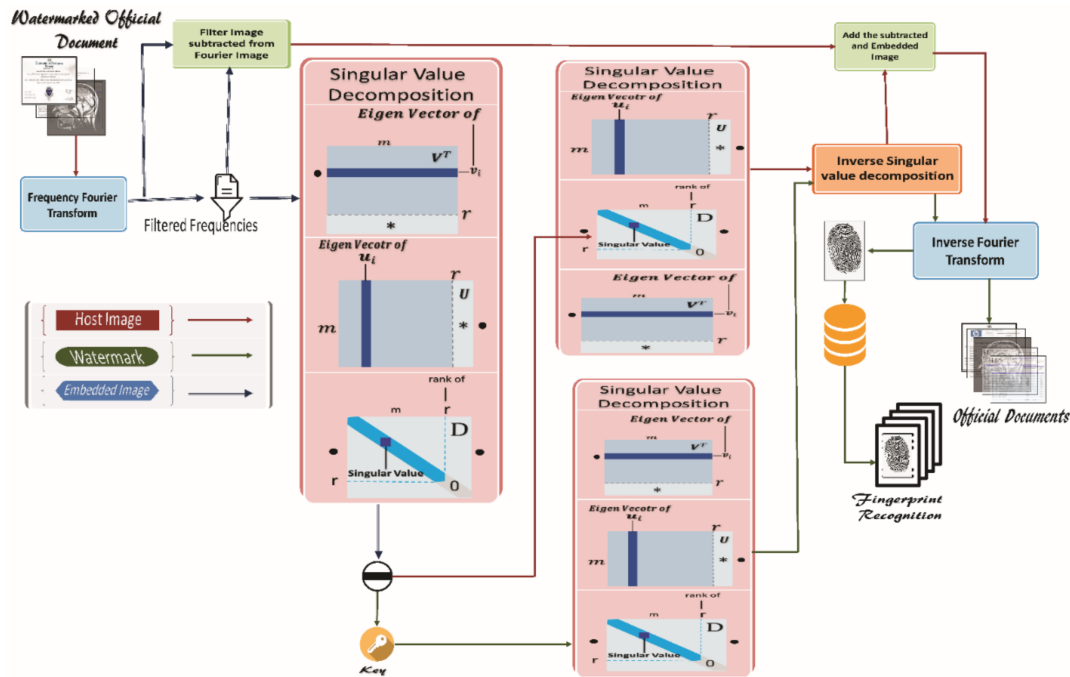


Figure 4. The framework of the proposed technique for extraction.

The extraction process is started from the watermarked image W_H^w . The watermarked image is transformed into frequency Fourier transform W_{fft}^H by applying the same Equation (2) for the detection and extraction of the watermark. The filtered frequencies are obtained in the same manner as embedding frequencies are extracted by applying Equations (3)–(14). To obtain the decomposed form of the frequencies, we apply the same as Equation (15) to get the two orthogonal and one diagonal U_W , V_w^T , and D_H^W respectively.

First, we transform the image/document and watermark. The embedded frequencies are obtained through a specialized filter in the same manner as in embedding; the decomposing isolate the diagonal matrix for extraction; the composition occurs for both the watermark and image/document. Then the image is obtained with a high level of imperceptibility, and the watermark is recognized by Viri-software accurately.

4. Experimental Results

4.1. Dataset

This section describes the dataset link, which is used for the sake of evaluation. The medical images have been taken from different medical institutes. The three hundred medical images contain the MRI images of different parts of the human body. These images are in raster format with a resolution of 201×201 . These images' content includes head, neck, head neck both, hand, wrist, knee, ankle, shoulder, back, backbone, lungs, breast, cardiac, thorax, prostate, pelvis, abdomen, hip, spine, and carotids. The other dataset has been taken from the University of Peshawar and Islamia College Peshawar. Two hundred images of degrees, detail mark certificates, and transcripts have been tested and evaluated by the proposed algorithm. The contents of these images, degrees, and transcripts (detailed marks certificates) of different classes, and sessions were of different formats. The dimensions of all images were adjusted according to the proposed evaluations and testing. It is essential to highlight that the comparative analysis is drawn based on fifteen images. The rationale for selecting these images was based on two factors: (i) all these images were part of existing work experiments with which the proposed method is compared and (ii) these are the most common images used in most of the benchmarks for watermarking and cryptography.

4.2. Experimental Setup

This section is reserved for interpretation of the proposed watermarking technique in the account of performance, collating with other similar methods. The proposed system is assimilating with the parent schemes proposed by Mussarat Ali et al. [4], Fan et al. [38], Lai [11] which have been mentioned and introduced earlier. For brevity purposes, we used the abbreviations DWT-SVD-ABC, SVD, and HVS-SVD, respectively. The rivalry of this technique with other schemas of the proposed system marked emphatically [5,10,37,39], which will call FWT, FrFT, and DWTQ (or DWT), respectively. A recapitulation of the comparison of the schemes is noted in Table 1. In the SVD technique, the watermark embedded works manually in the spatial domain, while other techniques are in the frequencies domain [40]. The SVD has a higher capacity compared to other techniques due to the spatial domain. Capacity for the proposed system is mentioned in Table 1, the N/A representing the capacity of that scheme for which the capacity is not concluded due to dependency on the watermark size. For the experiment, we have taken Fifteen standard images with a dimension of 512×512 and the Islamia college university logo as a watermark. We have downloaded these standard test images from an open-source, which is available on the public internet repository. An Islamia college university logo of size $32 \times 32/64 \times 64/128 \times 128/256 \times 256$ has been taken. The logo is considered as a watermark for the evaluation process. The visual result of the watermark, after extraction, are provided for analysis. The ratification of imperceptibility, robustness, and payload of the proposed system for both host image and watermark image, in diverse image exploiting attacks, is applied to decompose the watermarked image's class. All the schemes are coded and tested in MATLAB2016a on a personal computer (P.C.) and laptop with a Core 2 Duo processor, 4GB of RAM, and Windows 10. For evaluation and comparison with other schemes [13,41,42], we have taken the advocated parameter settings from their appropriate studies. The best results among the comparison in Tables 2–4 are highlighted in **Italic+Bold**, and a tie between results is shown in **Bold**.

4.3. Robustness Against Attacks

This section evaluates the robustness of the proposed system against malicious attack (attacks applied on the watermarked images shown in Figure 5, which are enlisted in Tables 3 and 4. The quality of the extracted watermark is intuiting by standard correlation (normal correlation (N.C.) value using (16). These N.C. values of each watermark of the corresponding schemes are organized in Table 4, and the higher N.C. values reflect more similarity to the original watermark. Lower the N.C. values show less similarity with the original watermark. From Table 3, it is revealed that the proposed technique has leverage on relative schemes. The proposed system's peak signal-to-noise ratio (PSNR) values are much higher and imperceptible from the rest, which concluded that the proposed system has inestimable imperceptibility. Table 2 indicates the value of normal correlation, which is designated for the watermark's similarity, the values with respect to all images have a passable difference. The N.C. concluded the watermark similarity and its payload. The technique can embed the watermark up to 256×256 , which is a countable payload. Table 4 shows the N.C. value for the watermark. It is clear from the N.C. value that the proposed technique is much suitable to resist those malicious attacks. The proposed approach focuses on both the host image and watermark for its imperceptibility and robustness. Table 5 indicates the watermark's visual result after applying different attacks; the proposed system has a clear advantage over the related schemes.

Table 1. Recapitulation illustration of the schemes.

Particulars	SVD	HVS-SVD	FWT	DWTQ	FrFT	DWT-SVD-ABC	Proposed
Host Image	512×512	512×512	512×512	512×512	512×512	512×512	512×512
Watermark	32×32	32×32	20×50	32×16	64×64	32×32	$32 \times 32 / 64 \times 64$
Finger Print	Biometric	Biometric	Biometric	Biometric	Biometric	Biometric	Biometric
Domain	Spatial	Transform	Transform	Transform	Transform	Transform	Transform
S	Manually	Manually	Manually	Automatic	Manually	Automatic	Manually
Capacity (b/p)	0.0625	0.0156	N/A	0.0104	N/A	0.0156	-

Table 2. Peak signal-to-noise ratio (PSNR) watermarked images and original images.

Image Name	SVD [38]	HVS+SVD [11]	FWT [10]	DWTQ [41]	FrFT [6]	RDWT [4]	Proposed
Lena	48.3212	43.2054	22.7807	42.6139	41.2173	44.0207	57.6982
Cameraman	49.3212	44.2054	23.7807	43.6139	41.2173	43.0207	56.6982
House	46.2274	41.3311	22.8192	43.1897	41.2221	45.0148	55.1524
Airplane	45.0615	42.0315	22.6162	43.7749	41.2274	43.0222	53.6556
Sailboat	45.3672	33.9873	22.6162	41.2493	41.2165	40.0038	54.5675
Couple	46.2274	41.3311	22.8192	43.1897	41.2221	42.0148	52.1524
Baboon	42.2943	37.7291	22.8836	44.6238	41.2227	40.0256	54.1256
Pirate	45.4251	43.1866	22.6162	41.2494	41.328	45.0227	51.6896
Bridge	41.8111	35.3789	22.4779	38.9901	41.2623	40.1107	52.5699
Blond	42.9307	40.5057	22.8338	43.0604	41.2284	42.0381	54.5689
Dark hair	47.9664	46.8601	23.8102	42.1843	42.2973	50.0194	54.1256
Einstein	50.2175	44.4398	22.6162	49.2493	41.2186	45.0182	58.6894
Rose	44.8065	41.7695	22.6162	42.8834	41.2171	42.9883	55.4586
Barbara	45.4251	43.1866	22.6162	41.2494	41.3289	45.0227	51.6896
Women	45.0615	42.0315	22.6162	43.7749	41.2274	43.0222	53.6556
Average	45.7643	41.4120	22.8345	42.9931	41.3100	43.3576	54.4334

Table 3. N.C. value of extracted watermark obtained from the watermarked images without any distortion attacks.

Image	SVD	HVS+SVD	FWT	DWTQ	FrFT	RDWT	Proposed
Lena	1	1	0.9082	0.8936	1	1	1
Cameraman	0.9268	0.8066	0.9268	0.7734	1	0.9945	1
House	0.9568	1	0.9219	0.8262	1	1	1
Airplane	0.9568	0.9971	0.9248	0.8965	0.9999	1	1
Sailboat	1	1	0.9111	0.8047	1	1	0.9999
Couple	1	1	0.9326	0.7921	1	1	1
Baboon	1	1	0.9209	0.8594	0.9688	1	1
Pirate	0.9564	0.9521	0.9355	0.8848	1	0.9941	1
Bridge	0.9951	0.9789	0.9336	0.8184	0.9866	1	1
Blond	1	1	0.9258	0.8382	0.9696	1	1
Darkhair	0.9951	0.9981	0.9375	0.8523	0.9988	0.9722	1
Einstein	0.9551	0.9766	0.9474	0.8184	0.9588	0.9889	0.9999
Rose	0.9599	0.9867	0.9245	0.8545	0.9878	0.9678	1
Barbara	0.9854	0.9568	0.9356	0.8105	1	0.9699	1
Women	1	0.9878	0.9436	0.8208	0.9689	0.9632	1
Average	0.9792	0.9760	0.9286	0.8362	0.9893	0.9900	0.9999

Table 4. N.C. value obtained from recovered watermark and original watermark after applying the said attacks.

Image	SVD	HVS+SVD	FWT	DWTQ	FrFT	RDWT	Proposed
lena	0.9915	0.9776	0.9253	0.8376	0.9972	0.9988	0.9999
Cameraman	0.7435	0.9423	0.8167	0.5832	0.6236	0.9076	0.9998
House	0.7312	0.9518	0.6963	0.6978	0.5531	0.9134	1
Airplane	0.9835	0.9727	0.8494	0.6808	0.5247	0.9973	1
Sailboat	0.4983	0.4987	0.4975	0.4656	0.4775	0.9988	0.9999
Couple	0.8690	0.8311	0.8916	0.7893	0.7781	0.8490	0.9999
Baboon	0.9782	0.9731	0.9510	0.7108	0.9456	0.9982	1
Pirate	0.9031	0.9384	0.9279	0.6832	0.9912	0.9830	1
Bridge	0.8389	0.9576	0.9039	0.8065	0.7476	0.9574	1
Blond	0.8398	0.8017	0.8881	0.5365	0.8249	0.8104	0.9998
Darkhair	0.9250	0.8714	0.8936	0.6408	0.8579	0.9347	1
Einstein	0.9466	0.9705	0.9197	0.7699	0.9581	0.9964	0.9999
Rose	0.4807	0.9579	0.9761	0.6813	0.9966	0.9972	1
Barbara	0.8754	0.7303	0.9305	0.7006	0.8631	0.9443	0.9999
Women	0.4807	0.4822	0.5028	0.5286	0.4719	0.9988	1
lena	0.5150	0.5566	0.4982	0.4758	0.4755	0.9988	0.9999
Average	0.8175	0.8384	0.8168	0.6618	0.7548	0.9552	0.9998

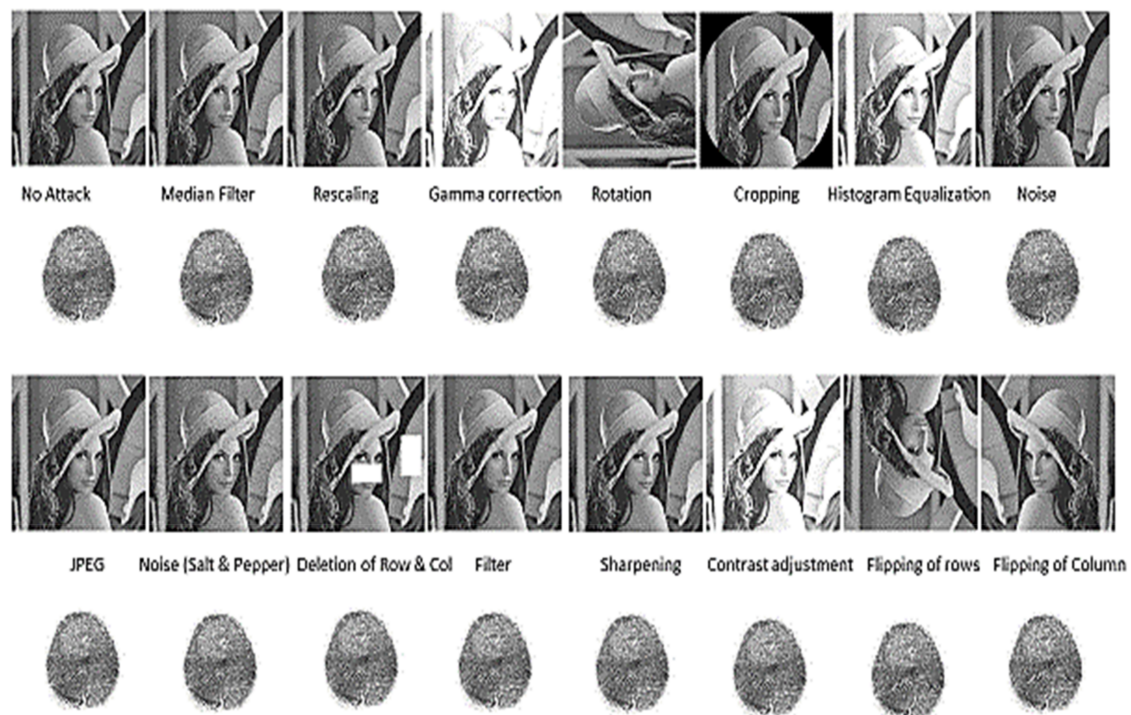
**Figure 5.** Attacks applied to the watermarked image and extracted watermarks (Finger Print).

Table 5. Visual result of extracted watermark image form image 'Lena' by proposed and related schemes.

















































































































Attacks Category	SVD	HVS+SVD	FWT	DWTQ	FrFT	RDWT	Proposed
Attacks/No Attack	 Recognized	 Recognized	 Not Recognized	 Not Recognized	 Recognized	 Recognized	 Recognized
Median filter	 Not Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Recognized
Rescaling	 Not Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Recognized
Gamma Correction with 0.2	 Not Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Recognized	 Recognized	 Recognized
Rotational attacks	 Not Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Recognized	 Recognized
Cropping	 Not Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Recognized
Histogram equalization	 Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Recognized	 Recognized
Noise (Gaussian)	 Recognized	 Not Recognized	 Recognized	 Not Recognized	 Recognized	 Not Recognized	 Recognized
JPEG Compression	 Not Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Recognized

Table 5. Cont.

Attacks Category	SVD	HVS+SVD	FWT	DWTQ	FrFT	RDWT	Proposed
Noise (S&P)	 Not Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Recognized
Deletion of rows and column	 Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Recognized	 Recognized
Filters	 Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Recognized	 Not Recognized	 Recognized
Sharpening	 Not Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Recognized	 Recognized	 Recognized
Contrast adjustment	 Not Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Recognized	 Recognized	 Recognized
Flipping of Rows	 Not Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Recognized
Flipping of Column	 Not Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Not Recognized	 Recognized

The recognition process is carried out through Viri software, which is used to recognize biometric properties worldwide. The results of the extracted watermarks and their recognition status are listed in Table 5. It is clear from the result that the proposed system is robust against every attack, and its watermark is recognized after said attacks. The recognition results are listed in Table 5.

4.4. Non-Parametric Statistical Analysis

Two methods, draconian and consequential, are used to compare the proposed framework's performance, as shown in Table 6. The comparison has been perceived using a non-parametric hypothesis testing named Wilcoxon's sign rank test. It is performed through the statistical software

package SPSS. The null hypothesis assumed as the median of the difference of two samples is zero, the alternative hypothesis t is a significant difference between the two samples, the level of significance for the testing is 5%. In total, there are 112 data samples with sixteen correspondences to each of the systems. Two samples are taken simultaneously for comparison; one reflects the proposed schema, and the others represent existing schemas. Table 6 depicts the overall statistical results derived based on N.C. values. R^+ denotes the number of positive ranks while the number of negative ranks is denoted by R^- , S^+ , S^- , and P -value the sum of ranks of absolute the sum value of the difference between the two test variables greater than zero and less than zero respectively. That is called the sum of positive and negative ranks, respectively. We assign the two signs (\uparrow and \downarrow) based on the result, \uparrow represents that the proposed system is significantly sound compared to the other while \downarrow represents no significant difference between the two systems.

Table 6. Existing methods vs proposed.

Index	SVD-P-value	HVS+S-P-value	FWT-P-value	DWTQ-P-value	FrFT-P-value	RDWT-P-value	Sig
0	0.100	0.100	0.003	0.003	0.028	0.028	\uparrow
1	0.003	0.003	0.003	0.003	0.003	0.003	\uparrow
2	0.003	0.006	0.003	0.003	0.003	0.003	\uparrow
3	0.003	0.003	0.003	0.003	0.003	0.003	\uparrow
4	0.003	0.003	0.003	0.003	0.003	0.003	\uparrow
5	10.006	0.006	0.100	0.003	0.003	0.657	\uparrow
6	0.003	0.003	0.003	0.003	0.003	0.003	\uparrow
7	0.003	0.011	0.003	0.003	0.003	0.006	\uparrow
8	0.003	0.003	0.003	0.003	0.003	0.003	\uparrow
9	0.003	0.003	0.100	0.003	0.028	0.028	\uparrow
10	10.006	0.006	0.006	0.003	0.003	0.003	\uparrow
11	0.003	0.003	0.003	0.003	0.003	0.003	\uparrow
12	0.003	0.006	0.003	0.003	0.028	0.028	\uparrow
13	0.003	0.003	0.003	0.003	0.003	0.003	\uparrow

5. Discussion

In the result section, it has been observed through the quantitative evaluation that the proposed method is superior to the contemporary closely related approaches. Based on N.C. values, the system shows robustness against malicious attacks. It is clearly indicated that the existing approaches did not survive all attacks indicated in Figure 5. Furthermore, using the non-parametric statistical analysis, the proposed method also outperformed with a high significance value compared to existing approaches. In the medical domain, trust in data and knowledge has a significant role. The key to achieving it is to provide a robust workflow of data and knowledge exchange within or across healthcare providers' networks. Within or across the healthcare provider networks, the watermarked image data must be provided with a robust watermark approach—used for authentication or patient data anonymization [43].

In recent trends, the applications are mostly real-time, exchanging a continuous stream of data over the internet. There is a frequent exchange of medical data between hospital networks, their associated laboratories, and other test collection points. Furthermore, cloud-based infrastructures are used to exchange medical data securely in a collaborative fashion among different applications within the same organization's departments [44]. In such cases, data protection enriches the user's gratification level for secure data exchange; therefore, the proposed technique embeds its watermark in real-time. The existing approaches [45–49] concentrate on providing robust protection while lacking in capabilities to handle real-time data exchange.

Furthermore, the proposed methodology's outcome is achieving a high payload by supporting a maximum possible size up to 324×324 of the watermark embedded in the transform domain with special filters and decomposition. On the other end, the extraction processing depends on the high payload for the watermark, especially during watermark recognition (biometric recognition). It is often required to explain the ownership detail from the repository. One of the existing techniques [47] can embed a watermark up to the same size as the host image, which led to a very high payload, but

the method failed to extract the watermark at the recognition level. In the description of extracted watermarks mentioned in [45–49], it is not firmly confirmed that a machine learning algorithm or software recognizes the watermark.

The proposed technique uses the human identification mark (biometric) as a watermark to keep the sender's identity. It only discloses the identity to the appropriate receiver. This approach's utmost outcome is to retain ownership and avoid any intruder attacks during the data exchange. The human identification mark is not used as a watermark to recognize its owner in contemporary techniques [45–49]. The key ownership retention by the proposed approach is straightforward. The sender has the right to embed its biometric information as an image in the host image or document. The sender must be an authorized user to send the data. The image/document on the internet produces a value of ownership, which is secure from all types of tempering and readily available at the receiver end for extraction and verification. The document isolated from the watermark will maintain its imperceptibility and watermark too. The watermark is then ready for the recognition process. The watermark is further processed by open-source Viri software for recognition.

The proposed technique separately calculates the PSNR for watermarks, which recognizes the watermark's imperceptibility. It emphasizes equality between the watermark and host image, which ultimately ensures the robustness and efficiency of the approach against various attacks. This fact is already explained in the result section by including pre and post-attack PSNR calculations for the watermark. The result section also provides a detailed level of imperceptibility and critical validation of robustness and efficiency property. In contrast, the existing techniques [45–49] compromise the imperceptibility because they merely concentrate on watermark embedding and its extraction. Most of these techniques did not process the watermark separately and emphasized the host image, resulting in less balance between manipulating the host image and the intended watermark.

Current work focuses on non-standardized medical images. The key limitation of non-standardized images reduces the level of interoperability for exchanging secure medical data. So we are targeting this issue in our upcoming work, which will deal with standard DICOM [50] based medical images. The future work will emphasize keeping the level of interoperability according to the DICOM standard and provide similar protection against various attacks during exchange among different healthcare provider networks.

6. Conclusions

The proposed work utilizes the most suitable decomposed frequencies in the transform domain by obtaining specialized filters and decomposition. It accommodates the watermark with a high payload across the whole host image, making the technique more robust and imperceptible. A fingerprint is used as a watermark, which claims the recognition of a watermark after extraction. The proposed work guided the watermarking procedure through the human security system, which is novel compared to contemporary techniques used to enhance security. A higher level of imperceptibility and the provision of validating the key robustness and effectiveness against various attacks enables the application of this approach in the medical domain. The main features of this approach give equal importance to the watermark. It not only focuses on the host image imperceptibility, robustness, and payload but also watermark recognition. These key features make it superior to existing approaches.

The results are compared with those recent techniques before and after the attacks. It clearly showed a higher level of imperceptibility and robustness. The performance of the proposed work on color images such as gif, video, and audio will be of keen interest in the research that the authors plan to do in the future. Furthermore, the technique will be extended to handle standard DICOM based medical images.

Author Contributions: S.U.D. is the principal researcher who conceptualized the idea. Z.J. and M.S. are the advisors of the project. They helped in data preparation and finalization of the overall proposal of the idea. M.H. facilitate in preparation and refinement of the conceptualization of the idea and thoroughly revised and reviewed the contents. R.A. and A.A. assisted in technical evaluation of the work and also reviewed the work for

consistencies. S.L. provides financial support for this research work. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2017-0-01629) supervised by the IITP(Institute for Information & communications Technology Promotion)", by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2017-0-00655), by the MSIT(Ministry of Science and ICT), Korea, under the Grand Information Technology Research Center support program(IITP-2020-0-01489) supervised by the IITP(Institute for Information & communications Technology Planning & Evaluation), and by NRF (National Research Foundation of Korea) with grant numbers NRF-2016K1A3A7A03951968 and NRF-2019R1A2C2090504.

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

Abbreviations

The following abbreviations are used in this manuscript:

I_H	Host image
I_w	Watermark image
K_w	Secrete key
I_{fft}	Fourier Transform Image
O_H^1	Orthogonal Matrix
O_H^2	Orthogonal Matrix
D_H	Diagonal Matrix
I_{fft}^L	Low Pass Filter
I_{fft}^H	High Pass Filter
n	Last row of the image
M	Last column of the image
N	Last row of the image
r	Rows of the image
c	A column of the Image
F_{I_H}	Filtered Frequencies of the Host Image
D_{LPP}	Distance computed for the low pass filter
D_{HPF}	Distance computed for the high pass filter
$F_{I_H}^w$	Watermarked required frequencies
$D_H^{K_w}$	Watermarked Diagonal matrix
$F_{fft}^R(r, c)$	Unembedded frequencies of a host image

References

1. Loganathan, A.; Kaliyaperumal, G. An adaptive HVS based video watermarking scheme for multiple watermarks using BAM neural networks and fuzzy inference system. *Expert Syst. Appl.* **2016**, *63*, 412–434. [\[CrossRef\]](#)
2. Dadkhah, S.; Abd Manaf, A.; Hori, Y.; Ella Hassanien, A.; Sadeghi, S. An effective SVD-based image tampering detection and self-recovery using active watermarking. *Signal Process. Image Commun.* **2014**, *29*, 1197–1210. [\[CrossRef\]](#)
3. Hossain, M.; Islam, S.M.R.; Ali, F.; Kwak, K.S.; Hasan, R. An Internet of Things-based health prescription assistant and its security system design. *Future Gener. Comput. Syst.* **2018**, *82*, 422–439. [\[CrossRef\]](#)
4. 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.* **2014**. [\[CrossRef\]](#)
5. Amiri, S.H.; Jamzad, M. Robust watermarking against print and scan attack through efficient modeling algorithm. *Signal Process. Image Commun.* **2014**, *29*, 1181–1196. [\[CrossRef\]](#)
6. Lang, J.; Zhang, Z. Blind digital watermarking method in the fractional Fourier transform domain. *Opt. Lasers Eng.* **2014**, *53*, 112–121. [\[CrossRef\]](#)
7. Ali, M.; Ahn, C.W. An optimized watermarking technique based on self-adaptive de in DWT-SVD transform domain. *Signal Process.* **2014**, *94*, 545–556. [\[CrossRef\]](#)

8. Bhatnagar, G.; Wu, Q.J. A new logo watermarking based on redundant fractional wavelet transform. *Math. Comput. Model.* **2013**, *58*, 204–218. [[CrossRef](#)]
9. Al-nabhani, Y.; Jalab, H.A.; Wahid, A.; Noor, R. Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network. *J. King Saud Univ. Comput. Inf. Sci.* **2015**. [[CrossRef](#)]
10. Elshazly, E.H.; Faragallah, O.S.; Abbas, A.M.; Ashour, M.A.; El-Rabaie, E.-S.M.; Kazemian, H.; Alshebeili, S.A.; El-Samie, F.E.A.; El-sayed, H.S. Robust and secure fractional wavelet image watermarking. *Signal Image Video Process.* **2014**, *9*, 89–98. [[CrossRef](#)]
11. Lai, C.C. An improved SVD-based watermarking scheme using human visual characteristics. *Opt. Commun.* **2011**, *284*, 938–944. [[CrossRef](#)]
12. Gao, L.; Qi, L.; Wang, Y.; Chen, E.; Yang, S.; Guan, L. Rotation Invariance in 2D-FRFT with Application to Digital Image Watermarking. *J. Signal Process. Syst.* **2013**, *72*, 133–148. [[CrossRef](#)]
13. Hu, H.; Hsu, L. Exploring DWT—SVD—DCT feature parameters for robust multiple watermarking against JPEG and JPEG2000. *Comput. Electr. Eng.* **2014**. [[CrossRef](#)]
14. Zheng, P.; Feng, J.; Li, Z.; Zhou, M. A novel SVD and LS-SVM combination algorithm for blind watermarking. *Neurocomputing* **2014**, *142*, 520–528. [[CrossRef](#)]
15. Cox, I.J.; Kilian, J.; Leighton, F.T.; Shamoon, T. Secure spread spectrum watermarking for multimedia. *IEEE Trans. Image Process.* **1997**, *6*, 1673–1687. [[CrossRef](#)]
16. Chen, P.; Zhao, Y.; Pan, J. Image Watermarking Robust to Print and Generation Copy. In Proceedings of the First International Conference on Innovative Computing, Information and Control—Volume I (ICICIC'06), Beijing, China, 30 August–1 September 2006.
17. Chang, J.; Chen, B.; Tsai, C. LBP-based Fragile Watermarking Scheme for Image Tamper Detection and Recovery. In Proceedings of the 2013 International Symposium on Next-Generation Electronics, Kaohsiung, Taiwan, 25–26 February 2013; pp. 173–176.
18. Li, Y.; Tu, Y.; Lu, J. Multi-point collaborative authentication method based on user image intelligent collection in the internet of things. *Electronics* **2019**, *8*, 978. [[CrossRef](#)]
19. Solanki, K.; Madhow, U.; Manjunath, B.S.; Chandrasekaran, S.; El-khalil, I.; Member, S. 'Print and Scan' Resilient Data Hiding in Images. *IEEE Trans. Inf. Forensics Secur.* **2006**, *1*, 464–478. [[CrossRef](#)]
20. Pramila, A.; Keskinarkaus, A.; Sepp, T. Multiple Domain Watermarking for Print-Scan and JPEG Resilient Data Hiding. In Proceedings of the 6th International Workshop on Digital Watermarking, Guangzhou, China, 3–5 December 2007; pp. 279–293. [[CrossRef](#)]
21. Wang, C.-p.; Wang, X.-y.; Xia, Z.-q. Signal Processing: Image Communication Geometrically invariant image watermarking based on fast Radial Harmonic Fourier Moments. *Signal Process. Image Commun.* **2016**, *45*, 10–23. [[CrossRef](#)]
22. Chen, B.; Coatrieux, G.; Chen, G.; Sun, X.; Coatrieux, J.L.; Shu, H. Full 4-D quaternion discrete Fourier transform based watermarking for color images. *Digit. Signal Process. A Rev. J.* **2014**, *28*, 106–119. [[CrossRef](#)]
23. Su, Q.; Niu, Y.; Wang, G.; Jia, S.; Yue, J. Color image blind watermarking scheme based on QR decomposition. *Signal Process.* **2014**, *94*, 219–235. [[CrossRef](#)]
24. Lin, S.D.; Shie, S.; Guo, J.Y. Computer Standards & Interfaces Improving the robustness of DCT-based image watermarking against JPEG compression. *Comput. Stand. Interfaces* **2010**, *32*, 54–60. [[CrossRef](#)]
25. Shih, F.Y.; Zhong, X. High-capacity multiple regions of interest watermarking for medical images. *Inf. Sci.* **2016**, *367–368*, 648–659. [[CrossRef](#)]
26. Wu, X.; Sun, W. Robust copyright protection scheme for digital images using overlapping DCT and SVD. *Appl. Soft Comput. J.* **2013**, *13*, 1170–1182. [[CrossRef](#)]
27. Ali, M.; Ahn, C.W.; Pant, M. A robust image watermarking technique using SVD and differential evolution in DCT domain. *Optik* **2014**, *125*, 428–434. [[CrossRef](#)]
28. Lu, C.; Liao, H.M. Multipurpose Watermarking for Image Authentication and Protection. *IEEE Trans. Image Process.* **2001**, *10*, 1579–1592.
29. Yin, C.; Li, L.; Lv, A.; Qu, L. Color Image Watermarking Algorithm Based on DWT-SVD. In Proceedings of the 2007 IEEE International Conference on Automation and Logistics, Jinan, China, 18–21 August 2007; pp. 2607–2611.
30. Makbol, N.M.; Khoo, B.E. A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition. *Digit. Signal Process.* **2014**, *33*, 134–147. [[CrossRef](#)]

31. Chetan, K.R.; Nirmala, S. An efficient and secure robust watermarking scheme for document images using Integer wavelets and block coding of binary watermarks. *J. Inf. Secur. Appl.* **2015**. [[CrossRef](#)]
32. Liu, Q.; Yang, S.; Liu, J.; Xiong, P.; Zhou, M. A discrete wavelet transform and singular value decomposition-based digital video watermark method. *Appl. Math. Model.* **2020**, *85*, 273–293. [[CrossRef](#)]
33. Santhi, V.; Arulmozhivarman, P. Hadamard transform based adaptive visible / invisible watermarking scheme for digital images. *Inf. Secur. Tech. Rep.* **2013**, 1–13. [[CrossRef](#)]
34. Wang, X.; Liu, Y.; Li, S.; Yang, H.; Niu, P.; Zhang, Y. A new robust digital watermarking using local polar harmonic transform. *Comput. Electr. Eng.* **2015**, 1–16. [[CrossRef](#)]
35. Bouslimi, D.; Coatrieux, G. A Crypto-Watermarking System for Ensuring Reliability Control and Traceability of Medical Images. *Signal Process. Image Commun.* **2016**. [[CrossRef](#)]
36. Wójtowicz, W.; Ogiela, M.R. Digital images authentication scheme based on bimodal biometric watermarking in an independent domain. *J. Vis. Commun. Image Represent.* **2016**. [[CrossRef](#)]
37. Sang, J.; Liu, Q.; Song, C.-L. Robust video watermarking using a hybrid DCT-DWT approach. *J. Electron. Sci. Technol.* **2020**, 100052. [[CrossRef](#)]
38. Fan, M.Q.; Wang, H.X.; Li, S.K. Restudy on SVD-based watermarking scheme. *Appl. Math. Comput.* **2008**, *203*, 926–930. [[CrossRef](#)]
39. Ghofrani, M.J.S.S. A robust blind watermarking method using quantization of distance between wavelet coefficients. *Signal Image Video Process.* **2013**, *7*, 799–807. [[CrossRef](#)]
40. Anuja, D.; Rahul, D. A Review on Digital Image Watermarking Techniques. *Int. J. Image Graph. Signal Process.* **2017**, *4*, 56–66.
41. Hsu, C.-S.; Hou, Y.-C. Copyright protection scheme for digital images using visual cryptography and sampling methods. *Opt. Eng.* **2005**, *44*, 1–10. [[CrossRef](#)]
42. Khan, A.; Siddiq, A.; Munib, S.; Malik, S.A. A recent survey of reversible watermarking techniques. *Inf. Sci.* **2014**, *279*, 251–272. [[CrossRef](#)]
43. 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](#)]
44. Fabian, B.; Ermakova, T.; Junghanns, P. Collaborative and secure sharing of healthcare data in multi-clouds. *Inf. Syst.* **2015**, *48*, 132–150. [[CrossRef](#)]
45. Al-Otum, H.M. Secure and robust host-adapted color image watermarking using inter-layered wavelet-packets. *J. Vis. Commun. Image Represent.* **2020**, *66*, 102726. [[CrossRef](#)]
46. Ma, B.; Chang, L.; Wang, C.; Li, J.; Wang, X.; Shi, Y.Q. Robust image watermarking using invariant accurate polar harmonic Fourier moments and chaotic mapping. *Signal Process.* **2020**, *172*, 107544. [[CrossRef](#)]
47. Sharma, S.; Sharma, H.; Sharma, J.B. An adaptive color image watermarking using RDWT-SVD and artificial bee colony based quality metric strength factor optimization. *Appl. Soft Comput. J.* **2019**, *84*, 105696. [[CrossRef](#)]
48. Anand, A.; Singh, A.K. An improved DWT-SVD domain watermarking for medical information security. *Comput. Commun.* **2020**, *152*, 72–80. [[CrossRef](#)]
49. Liu, Y.; Zhang, S.; Yang, J. Color image watermark decoder by modeling quaternion polar harmonic transform with BKF distribution. *Signal Process. Image Commun.* **2020**, *88*, 115946. [[CrossRef](#)]
50. Das, S.; Kundu, M.K. Effective management of medical information through ROI-lossless fragile image watermarking technique. *Comput. Methods Programs Biomed.* **2013**, *111*, 662–675. [[CrossRef](#)] [[PubMed](#)]

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).