electronics

MDPI

Article

A Semi-Fragile, Inner-Outer Block-Based Watermarking Method Using Scrambling and Frequency Domain Algorithms

Ahmet Senol [1], Ersin Elbasi [2,*], Ahmet E. Topcu [2] and Nour Mostafa [2]

[1] Computer Engineering Department, Üsküdar University, Istanbul 34662, Turkey
[2] College of Engineering and Technology, American University of the Middle East, Egaila 54200, Kuwait
* Correspondence: ersin.elbasi@aum.edu.kw

Abstract: Image watermarking is most often used to prove that an image belongs to someone and to make sure that the image is the same as was originally produced. The type of watermarking used for the detection of originality and tampering is known as authentication-type watermarking. In this paper, a blind semi-fragile authentication watermarking method is introduced. Although the main concern in this paper is authenticating the image, watermarking for proving ownership is additionally implemented. The method considers the image as two main parts: an inner part and an outer part. The inner and outer parts are divided into non-overlapping blocks. The block size of the inner and outer part are different. The outer blocks have a greater area than the inner blocks so that their watermark-holding capacity is greater, providing enough robustness for semi-fragility. The method is semi-fragile and the watermarked image is authenticated despite the JPEG being compressed to 75% quality. The embedded watermark also survives innocent types of image operations, such as intensity adjustment, histogram equalization and gamma correction. Semi-fragile and selectively fragile authentication is valuable and in high demand specifically because it survives these innocent image operations while detecting ill-intentioned tampering. In this work, we embed a binary watermark into the inner and outer parts of images using a scrambling algorithm, discrete wavelet transform (DWT) and discrete cosine transform (DCT) in the blocks. The proposed methodology has high image quality after watermarking, with a PSNR value of 40.577 , and high quality is also achieved after JPEG compression. The embedding process provides acceptable image quality after tamper attacks, including JPEG compression, Gaussian noise, average filtering, and scaling attacks with PSNR values greater than 29. Experimental results obtained show that the proposed semi-fragile watermarking algorithm is more robust, secure and resistant than other algorithms in the literature.

Keywords: multimedia security; watermarking; authentication; discrete wavelet transformation; discrete cosine transformation

Citation: Senol, A.; Elbasi, E.; Topcu, A.E.; Mostafa, N. A Semi-Fragile, Inner-Outer Block-Based Watermarking Method Using Scrambling and Frequency Domain Algorithms. *Electronics* **2023**, *12*, 1065. https://doi.org/10.3390/electronics12041065

Academic Editor: Honarvar Shakibaei Asli

Received: 10 January 2023
Revised: 14 February 2023
Accepted: 16 February 2023
Published: 20 February 2023

1. Introduction

Encryption and watermarking are two essential techniques for copyright protection. Copy control, broadcasting, authentication and fingerprinting are some other applications of watermarking. Encryption is a very strong methodology for all kinds of multimedia elements, especially for images and videos. However, encryption provides security during data transfer, but, after decryption, it does not provide any protection. The watermarking method is applied to images or videos to prove ownership. Watermarking is a method to hide secret data from multimedia elements. Secret data might be another image, stamp, logo, or text. The data-hiding scheme is called embedding, while finding out what the embedded message is is called extraction. There are two types of watermarks, which are pseudo random number (PRN) and visible logos. The PRN-based watermarking process only detects whether there is a watermark. Watermarking extraction is based on three methods, including non-blind, semi-blind, and blind watermarking. The non-blind watermarking process uses both the cover image and the watermarked image to extract the

embedded message. Semi-blind watermarking uses a watermark logo and watermarked image, while blind watermarking uses a secret key only to find the embedded watermark.

Image watermarking is mainly used to prove that an image belongs to someone; that the image in question relates to the sender who sent it. There are also other uses of watermarking, such as advertisement tracking, transaction tracking, and metadata storage [1]. Image watermarking involves embedding data into an image in a way that it will not be possible to see or remove the watermark from the image without destroying the overall appearance of the image. Although, generally, it is apparent that the image contains a watermark, it must not be seen or extracted without the key and the relevant method. Watermarking methods aim to prove ownership. The embedded watermark must survive common image operations, such as Lossy compression, format change, filtering, cropping, rotation, or resizing. This property is known as the robustness of the method. The algorithm must also be robust against damaging operations, such as rotation, cropping and re-watermarking [1–3]. It is also desired for the watermarked image to resemble the original image as much as possible. This property is called the fidelity of the method. Fidelity is measured as the peak signal-to-noise ratio (PSNR) value as given in Equation [1]. The rounded mean square error (RMSE) is measured between two images as in Equation [2] where I is the original image and I* is the watermarked image, and i, j are the pixel coordinates. There is always a trade-off between robustness and fidelity. When robustness increases, fidelity decreases.

$$\mathrm{PSNR} = 20\log_{10}(255/\mathrm{RMSE}) \tag{1}$$

$$\mathrm{RMSE} = \mathrm{sqrt}\left(\left(\sum\nolimits_{ij}\left(I^{*}_{ij} - I_{ij}\right)^{2}\right)\right)/(NxN) \tag{2}$$

Another type of watermarking is authentication purpose watermarking. In this type, the aim is to detect changes made to an image and to decide whether the image is the same as the original. Although our work involves proving the watermarking ownership type, it mainly deals with the authentication type of watermarking.

When devising a blind image authentication algorithm it must take into account that the center of the image contains more important data than the edges. Watermark embedding may affect important parts of an image in a negative way. The present study seeks to reduce the effect of watermark embedding on important parts of the image, while making sure that the image does not undergo a malicious change. It is better to determine the genuineness of an image without having to obtain an original copy from a trusted party. In this sense, blind image authentication is a more desirable watermarking method than a non-blind method. A blind authentication and proof of ownership image watermarking algorithm that may resist certain innocent image operations, while detecting malicious alterations to an image, is proposed. The proposed method will make it possible to determine which parts of a received image have been maliciously altered by an attacker.

2. Related Work

Singh et al. [4] proposed an Arnold-transform-based watermarking method for images. Both the cover image and the watermark are shuffled using an Arnold cat map, then a second-level decomposition of DWT and SVD are applied to embed the watermark. The experimental results were compared with the five most frequently used watermarking algorithms. The results showed that the proposed algorithm was very strong against filtering, noise and geometric attacks. Cheng et al. [5] proposed a watermarking method for privacy leakage and response latency in outsourced multimedia elements. In this work, encryption and discrete wavelet transforms were used for information security. Several attacks and methodologies able to find out an embedded watermark, erase or change it were identified. Qi et al. [6] proposed a generic reversible visible watermarking method using graph Fourier transform, which was visible and could resist several attacks. However, the proposed method is a blind watermarking approach, which is more difficult to apply

than other methods, such as non-blind and semi-blind. Singh et al. [6] proposed a hybrid watermarking algorithm for healthcare. Currently, several types of patient data are used in healthcare, with most being images and videos. When using images, it is important to select the region of interest to embed the watermark so as not to distort patient information. In this work, DWT and SVD transformations were used to embed patient information as a watermark. The approach was tested with several geometric and image-processing attacks, and the results obtained were very strong. Application of the measurement metrics PSNR and SSIM indicated that the proposed algorithm was very promising.

DCT is another frequency domain watermarking type; it is a robust and secure method. In the literature, several studies are reported which use PRN embedding using the mid-coefficient of the DCT. Rupa et al. [7] proposed a DCT algorithm to embed a logo image into a cover image. DCT is very successful for image decoding, watermarking and image processing. It is a very fast and secure algorithm for information hiding. Elbasi [8] proposed a third-level decomposition-based wavelet embedding algorithm. The DWT has four bands—the LL band is for low frequencies and other bands are for high frequencies. Embedding a binary watermark in a third-level decomposition of the DWT gives very high PSNR values after geometric and statistical attacks. In addition, the similarity ratio (SR) values are very high after extraction of the watermarks.

Patient data protection is very important for medical imaging, such as ultrasound and magnetic resonance. Hadjer et al. [9] proposed a dual-image watermarking scheme to embed watermarks and electronic patient records (EPRs) into medical images. The watermark image is encrypted using chaotic logistic map methods to increase robustness and security. PSNR, normalized correlation (NC) and bit error-rate measurement metrics were evaluated for the proposed algorithm; the results showed that dual-image watermarking produces higher robustness and imperceptibility values [9]. Zhou et al. [10] proposed a reversible watermarking scheme to protect medical data in colour images. Most of the work in the literature is based on gray-level images which have some limitations in terms of robustness, imperceptibility, and embedded capacity for colour images. In this work, DWT was applied to several medical images, the proposed methodology was found to be more robust and secure than other algorithms described in the literature. Modification of the coefficients in the wavelet was more suitable for information hiding than modification in the spatial domain. The proposed approach was robust against common and geometric attacks, such as rotation and resizing, and demonstrated high data capacity without any distortion black after attacks.

Kushlev et al. [11] worked on medical image watermarking. Medical images might include patient, disease, doctor or hospital information which is private information. In this work, wavelet and DCT frequency-based algorithms were used to hide this information in the region of interest to provide robust and secure hiding. The proposed watermarking algorithm was tested against Gaussian noise, salt and pepper noise, and median filter. The PSNR, mean secure error (MSE) and NC evaluation results were very promising. The medical data watermarking method enables the secure collection, storage and sharing of patient data. Wu et al. [12] proposed a quantum D4 wavelet transform algorithm for images. Combining quantum wavelet transform and a controlled rotating gate produced promising results, especially for attacks. Lena, baboon, boat, man and sailboat images were tested with the proposed algorithm. The PSNR values were higher than 50 dB in all images, indicating greater efficiency than for other frequency and spatial domain algorithms. Simulation results showed that the proposed algorithm was feasible, effective and robust. Mohammmed et al. [13] worked on Canny-edge-detection-based watermarking, the edges being very critical pixels for hiding information. It is very difficult to identify, change and see the watermark, which is hidden in the edge of the image. The embedding process does not distort the image [14,15]. DCT and SVD algorithms were used together in this work. The PSNR values were between 51 dB and 55 dB, which is very strong when compared with embedding with DCT or SVD. The binary image was embedded into the Lena, baboon,

airplane, splash and girl images using the proposed algorithm. The proposed work was resistant against histogram equalization and JPEG compression attacks [16–19].

There are also variations in authentication types of watermarking. Some fields, such as medicine or military, might require exact authentication. In exact authentication, even a bit change in the watermarked image causes the authentication to fail. Usually an image signature or a hash of the image is computed from some part of the image and stored in another part of the image. As is known, even a bit value change in the image will yield a completely different hash value to the embedded hash value. Exact authentication is also known as fragile authentication—there are many studies concerning fragile types of watermarking in the literature. One of the first studies of authentication-type image watermarking was carried out by Yeung et al. [20]. In this study, gray-level values [0...255] were mapped to binary values 0, 1 and this mapping was the key for watermark extraction. The binary watermark was inserted into the host image where the gray-level value was changed with the nearest value having the same mapping to the desired watermark bit value (0 or 1), or remained the same if the current gray-level value mapped to the desired watermark bit. Min et al.'s work [21] used a similar approach in which they mapped DCT domain values to binary values 0,1 instead of to pixel gray-level values. Subsequent to Yeung and Mintzer's work, several articles were published which showed that mapping of gray-level values can be attacked easily [22,23]. Wu and Liu's work [21] also has the same kind of weakness. Rao and Kumari in [24] studied the uses of watermarking in authenticating medical images and ensuring their security.

Generally, the least significant bits are used for authentication-type watermarking. Lin et al. in [25] divided the image into non-overlapping 4×4 blocks and further divided each 4×4 block into 2×2 sub-blocks, firstly setting the least significant two bits of pixels of the block to zero, calculating the parity and authentication bits using the difference between the mean intensity levels of the sub-blocks. Using a mapping algorithm, the authors made pairs of 4×4 blocks, and a 6-bit length mean intensity value of one block was inserted into the least significant bits (LSBs) of the corresponding block. Although their study succeeded in detecting and localizing changes and image restoration to some extent, the method constitutes exact authentication and is sensitive to innocent changes, such as Lossy compression. Chamlawi et al. in [25] proposed a semi-fragile watermarking method in which two watermarks were embedded in a host image, one binary image watermark being embedded in the LL3 band of the third level DWT of the host image, the other watermark calculated as an image digest by taking the DCT of the DWT LL1 band and embedding the image digest into the LH2 and HL2 DWT bands. The first watermark was used for authentication and the second image digest watermark was used for image restoration and tamper localization. The authors claimed that their method ensured authentication, recovery of the image and localization of tampered areas.

Liu et al. in [26] took a colour image into YCbCr colour space, then the DWT LL1 of the Y channel was divided into 8×8 blocks; each block was quantized by a luminance quantization table and the quantized LL1 values replaced the HH1 band of the Y channel. After taking inverse DWT, a robust watermarked image was obtained, which was then taken to the RGB colour space. After that, the red, green and blue channels were watermarked by a fragile watermark. The fragile watermark was inserted into the pixel domain. A sequence of ones and zeros represented the watermark, which was converted to base 10 digits by a 3n-base formula containing a parameter n. Each obtained digit was watermarked as a bit sequence to the LSBs of n pixel values of the corresponding colour channel. In their paper, Pillai and Theagarajan claim to have devised a method that embeds two watermarks into the host image, one for authentication, the other for restoration [27]. The authentication watermark was calculated from the DWT LL1 band of the host image. The LL1 band was divided into blocks, the blocks being grouped into two groups, namely A and B. The blocks were paired as one block from group A, and one block from group B. For each pair of blocks, the DCT of the blocks was taken and compared with the corresponding DCT value of the paired block; a value of 1 or 0 was calculated according to a '<' comparison. The

majority bits of the comparison bit sequences were combined to form the authentication watermark. The authentication watermark was embedded into the HL2 and LH2 bands of the host image's DWT HL1 band. The HL2 and LH2 values were divided by or multiplied by α, depending on the bit value to be embedded. A recovery watermark was obtained by quantizing the LL3 values of the host image, which were then watermarked to the HL1 band's five LSBs. Although a recovery watermark was embedded, the recovery process was not reported in the experiments.

It is easy to insert a similar watermarked block or block pairs from a known authenticated image into another image for forgery purposes [22]. Therefore, in any authentication type of watermarking, if the inserted watermark does not depend on the host image itself, then it is vulnerable to counterfeiting attacks. If the method is block-wise, the watermark must be calculated from one of the block pair and inserted into the other one in the pair. Block-pairing must depend on a key so that it cannot be predicted. Boujerfaoui et al. [28] proposed a convolutional-neural-network-based watermarking algorithm resistant against print-cam attacks, which are very strong attacks and introduce several distortions during picture capture. The proposed approach was compared with Fourier-transformation-based watermarking. The results obtained were robust, secure and of high quality. Cai et al. [29] proposed a Chinese cryptographic algorithm for copyright protection. Nowadays, it is very easy to collect, share, distort, and change images and videos using information technology. It is a concern for everyone because of the security and copyright implications. The Chinese cryptographic algorithm uses SM2 and SM3, which are hash functions for random password operation and generation. Copyright information is embedded into the image using this encryption method. It is low cost and low risk compared with other frequency-based algorithms. Campos et al. [30] proposed a block-based algorithm for tamper detection. Lifting wavelet transformation and check sum hashing algorithms are used together. The embedded pixels are selected from the least significant bits in the cover image. Several evaluation methods were used in experiments undertaken, such as the false positive, false negative and tamper-detection rates. The proposed algorithm was found to be very strong against copy paste, copy move, averaging, adding noise and image manipulations.

The health sector uses electronic data frequently. Patient data can be collected, stored and shared with others using information technology. There are several medical-imaging technologies available in all hospitals. Patient data can be kept secret using watermarking and encryption algorithms for privacy purposes. Singh et al. [31] discussed several spatial domain, frequency domain and cryptographic algorithms to compare their performance in both embedding and extraction. There are some limitations to using watermarking for medical images. For example, if the embedding process is applied to some of the critical parts of the image content, it might affect the doctor's decision. Discrete cosine transformation is one of the frequency-based embedding methods in image watermarking. Especially if the watermark is a pseudo-random number, the scaling factor is an important coefficient to provide balance between invisibility and robustness. Ernawan et al. [32] proposed a flexible scaling-factor-based DCT watermarking algorithm in blocks. In this work, selected coefficients were compared against the average coefficients using flexible scaling. The PSNR and SSIM values were very high compared to the DCT algorithm. The watermarked image was resistant against several filtering, adding noise and compression attacks.

Sahu et al. [33] proposed a reversible fragile watermarking methodology for tamper detection. In this method, two secrets are embedded into the cover image for a dual watermarking scheme. Experiments showed that the proposed method was more robust and had high capacity and transparency. The proposed methodology finds tampered regions and relocates efficiently. Zhang et al. [34] proposed an M-sequence and sliding window-based watermarking method for audio. This method was found to be robust and secure against large-scale cropping attacks. In this methodology, audio is converted into DWT, DCT, graph-based transform (GBT), and SVD. The secret data is applied to cover audio.

3. Proposed Method

In the proposed method, the image is considered as two parts: the center and probably more important part, and the image's exterior part, as seen in Figure 1. In photographs, the important thing, person or the main object is usually centered or around the center. The main idea in this study is to watermark the center of the image with a robust watermark to prove ownership, with a watermark strength that does not degrade the fidelity of the image to a marked extent. After that, the center part and outer part are divided into blocks and the center blocks are paired with the outer blocks of the image, watermarking the image digest of the inner block to the outer block for authentication purpose.

Figure 1. Image consisting of inner part and outer part divided into blocks.

The center part is watermarked with a robust watermark to prevent someone who knows the algorithm from cropping only the center part and using it without permission. The center part is watermarked in the DWT domain with the method proposed in [20]. The DWT of the center part and watermarking are shown in Equations (3) and (4). The watermark is embedded into the low frequencies, which are located in the LL1 band. This watermark does not degrade fidelity very much. The watermarked images after the center part watermarking have a PSNR value of 57, which is a very high fidelity value. In this study, the main concern is the authentication part. Because of this, no experimental results for the robust watermark are provided. For those interested in the method and success of robust ownership watermarking that is used for the inner parts, please see [20].

$$[\text{LL1, LH HL1, HH1} \leftarrow \text{DWT(Center Image)}] \tag{3}$$

$$\text{LL1} \leftarrow \text{LL1} + \alpha * (\text{Binary Image Watermark}) \tag{4}$$

As a next step, the $LL1$ bands of the inner blocks are represented in binary form by making the values 1 that are greater than the threshold value and assigning a value 0 in other cases. The threshold value is decided so as to make the number of ones and zeros almost equal to each other in the whole inner part. This is done to embed the watermark in a more balanced way to decrease the negative effect on fidelity.

In Figure 1, the center part is contoured with thick black lines. The center part is divided into blocks that are of reduced area compared to the outer block sizes. The algorithm depends on a prime number $K1$. The prime number $K1$ will be given to the authenticator program that is used on the other side. After making pairs of blocks, one from the inner part and one from the outer part, a binary image is calculated from the inner block and that binary image block is embedded in the corresponding outer block. The outer blocks are greater in size compared to the inner blocks. This offers greater precision on the inner part to decide which block(s) are changed. This is reasonable because, in most of the images, the important person or thing is generally placed in the center part of the image. Moreover,

the watermark storing capacity of the outer block increases as the block size increases. In Figure 2, the difference in block size is shown more clearly.

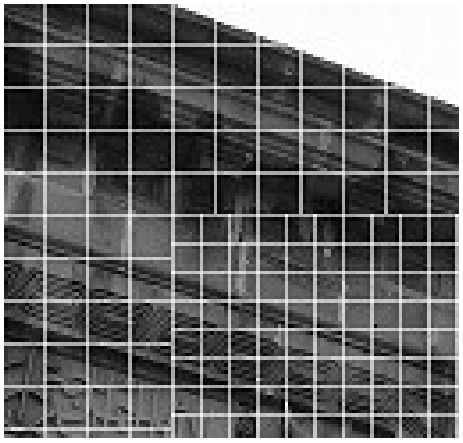


Figure 2. Inner block size is less than outer block size.

3.1. The Embedding Algorithm

The pseudocode for the embedding algorithm is as follows:

In step 1.a.iii, since the number of blocks in the inner part and the outer part may differ, it is considered sufficient to pair at least 90% of the inner blocks with the outer blocks. Since pairing is performed using a secret key, the risk is not high for not pairing at most 10% of the inner blocks. Since the inner blocks are previously watermarked with a robust watermark, this presents no problem for the inner blocks. There might be a risk that, if someone knows the algorithm, they may try to find outer blocks that are not paired with an inner block and try to change the block contents. Firstly, since the pairing depends on a secret key, it is not possible to determine non-paired blocks without the key. Secondly, the non-paired outer blocks are not contiguously located—they are scattered along the exterior part of the image. Changing a 24×24 block may not yield a desired malicious change in the image.

In step 4, $PSNR\_length$ takes into consideration the block size BS_O of the outer blocks. $BS\_O * BS\_O$ is the total number of pixel values of an outer block. In 6.b, while converting the LL1 value to a binary value, a threshold value is calculated to make the number of bits value 1 equal to the number of 0's in the whole of the inner blocks. As shown in step 6.c, the DCT of the outer block is obtained. After that, a zigzag scan of the DCT values is obtained. $V\_exclude$ is the number of values that are not used from the beginning and from the end of the zigzag values. By doing this, we are not changing the DC component and the most precious low-frequency values as well as the high-frequency values. We try to preserve fidelity by not using high-rank, low-frequency components. By doing this, we try to make our watermarking method robust to Lossy compression, which destroys high-frequency components the most. In Figure 3, it is seen how an image is considered as the inner and outer parts and how the inner and outer parts are divided into different block sizes.

3.2. The Authentication Algorithm

The pseudocode for the authentication algorithm is as follows:

1. The image is divided into parts: inner part, outer part with the same principles as in embedding
2. Make pairs (B_Ik, B_Ok), B_Ik from inner part, B_Ok from outer part using the given key S_K
3. Load the given $PSNR$
4. $PSNR\_length \leftarrow (PSNR\_length)$
5. For each block B_Ik from inner part
   (a) Find out DWT (B_Ik)

(b) Obtain binary image $Bin\_LL1\_B\_Ik$ from $LL1$ band of DWT (B_Ik)
(c) $DCT\_B\_Ok\_M \leftarrow DCT(B\_Ok)$, where B_Ok is corresponding block from outer part
(d) $Z\_DCT\_B\_Ok \leftarrow$ zigzagscan$(DCT_B_Ok_M)$
(e) $V\_DCT\_B\_Ok \leftarrow$ take value from$(Z_DCT_B_Ok)$, excluding first $V\_exclude$ and last $V\_exclude$ values
(f) $Processed\_Start = 1$
(g) While $(Processed\_Start <= (Length(V\_DCT\_B\_Ok) - PSNR\_length))$
    i. $Val\_PSNR \leftarrow$ take values of length $PSNR\_length$ from $V\_DCT\_B\_Ok$
    ii. $Correlation\_value1 = correlation\_coefficient(Val\_PSNR, PSNR)$
    iii. $Correlation\_value2 = correlation\_coefficient(Val\_PSNR, PSNR)$
    iv. if $Correlation\_value1 >= Correlation\_value2$
        $bit\_val \leftarrow 1$ else
        $bit\_val \leftarrow 0$
    v. $Extracted\_Bitmap \leftarrow$ Put the bit value in proper place in the order it is embedded
    vi. $Processed\_Start = Processed\_Start + PSNR\_length$
(h) $Bit\_Diff\_Sum \leftarrow Sum(abs(Extracted\_Bitmap - Bin\_LL1\_B\_Ik))$
(i) $BitMapImageNumberOfBits \leftarrow (Row\_Length(Bin\_LL1\_B\_Ik)$ *
(j) If $(Bit\_Diff\_Sum / BitMapImageNumberOfBits) > 0.15 / ^{*}Threshold = 0.15^{*}/$ Mark the inner and outer block as changed

6. Embed robust watermark into center blocks for the purpose of proving ownership as in [20]

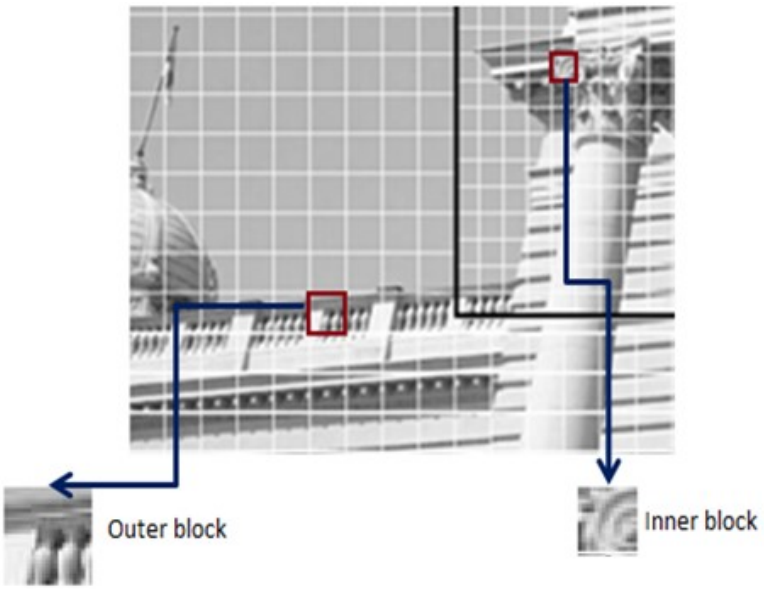


Figure 3. Inner and outer blocks in embedding process.

Both the embedding and extraction algorithms should be robust and secure in the watermarking process. The authentication process is important to find out embedded secret information in the cover images for copyright protection. In the proposed methodology, the cover image is divided into inner and outer blocks. Each block is transformed into the discrete wavelet transformation (DWT). The DWT gives low frequencies (LL band) and high frequencies (HL, LH, and HH bands). The LL bands were transformed into the DCT using zigzag order. If the correlation of the inner block is greater than the correlation of the outer block, then the pixel value is assigned to 1; otherwise 0. In the extraction process, the similarity ratio (SR) is used for quality measurement. For binary watermarking, an SR value of 1 demonstrates the best quality of the extracted watermark.

3.3. The Scrambling Algorithm

In many of the authentication-type watermarking methods, the image is divided into blocks and the blocks are paired as (B1, B2). An image digest, a binary image or image features are calculated from the B1 block and embedded in the B2 block. It is important to make the secret pairing of blocks because, if someone knows or predicts the block sizes and pairs, they could easily replace the block pair with a pair from an already authenticated image. In [25], it is mentioned that torus automorphisms can be used for that purpose. A torus automorphism is a dynamic stately system that has a beginning state and change state at t intervals.

$$S_{t+1} = \int (S_t), t \epsilon \{0, 1, 2.....\} \tag{5}$$

A two-dimensional torus automorphism can be defined by

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, \begin{pmatrix} x_{t+1} \\ y_{t+1} \end{pmatrix} = A \times \begin{pmatrix} x_t \\ y_t \end{pmatrix} \mod N \tag{6}$$

$a_i \epsilon Z, determinant(A) = 1,$
$A\ has\ eigenvalues\ \lambda_{1,2}\ \epsilon\ R - \{-1, 0, 1\},$

The system is chaotic and repeats itself at every time step R, that is $S_R = S_0$. Voyatzis and Pitas [35] proposed a special type of matrix A for Equation (6), where A can be formed from one value k.

$$A = \begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix} \tag{7}$$

In our study, the one-dimensional mapping method mentioned in [25] and given in Equation [8] is used.

$$X^{'} = (k \times X\ mod\ N) \tag{8}$$

where $X, X' \in \{0, 1, \ldots..N-1\}$ are the block numbers at t and t+1, k is a prime number and the secret key, N is the number of blocks. The set of inner blocks is S1 and the number of elements in S1 is N1, whereas the set of outer blocks is S2 and the number of elements is N2. The scrambling algorithm maps the blocks in S1 to blocks in S2 and it is a one-to-one mapping.

Although mapping between inner and outer blocks uses a scrambling algorithm and a secret key, it is not the only security prevention. The block sizes of the inner blocks and the outer blocks are also determined on the run which makes the attacks more difficult. The attacker will not know the blocking structure in the image. The number of excluded values in the DCT transform is also not known by the attacker. A little weakness in the pairing scrambling algorithm may be easily compensated for by the mentioned unknown parts of the algorithm.

4. Experiments and Results

The original image is as shown in Figure 4a. The binary logo watermark image watermarked into the inner part is shown in Figure 4b. In Figure 4c, a watermarked image with a proving ownership and authentication watermark is shown. The PSNR of the image is 40.577. Although the PSNR value may be seen as a lower fidelity value, the sacrifice is with semi-fragility and it pays off. The success of the algorithm for different types of attacks is given in Table 1. The algorithm authenticates an image that is Lossy-JPEG-compressed with a quality factor of 75%; the authenticated image is seen in Figure 5a. It shows only six blocks as changed which are not contiguous and can be considered an innocent type of operation. The algorithm does not authenticate 50% quality and 25% quality JPEG compressed images, as seen in Figure 5b,c. The algorithm also authenticates images with intensity adjustment and histogram equalization, as seen in Figure 6b,c. The most common objective evaluation tool, the mean square error (MSE), is very unreliable, resulting in poor correlation with the human visual system (HVS). The peak signal-to-noise ratio (PSNR) is

one of the image-quality measurement metrics. It represents a ratio between the highest value of a signal and the power of distorted noise.

In Figure 7a, the watermarked image has been tampered with as a non-existent ornament is placed on the mosque on the figure. In Figure 7b, it can be seen that the changed blocks are successfully signed as "changed" by the algorithm without any false negatives. The authenticator program needs the PSNR and the scrambling key for authentication. In Figure 7c, the watermarked image with no attack is attempted to be authenticated with the wrong key and almost all the blocks are signed as tampered with by the algorithm. If the wrong key is given to the authenticator, or the key is not known, the image cannot be authenticated.

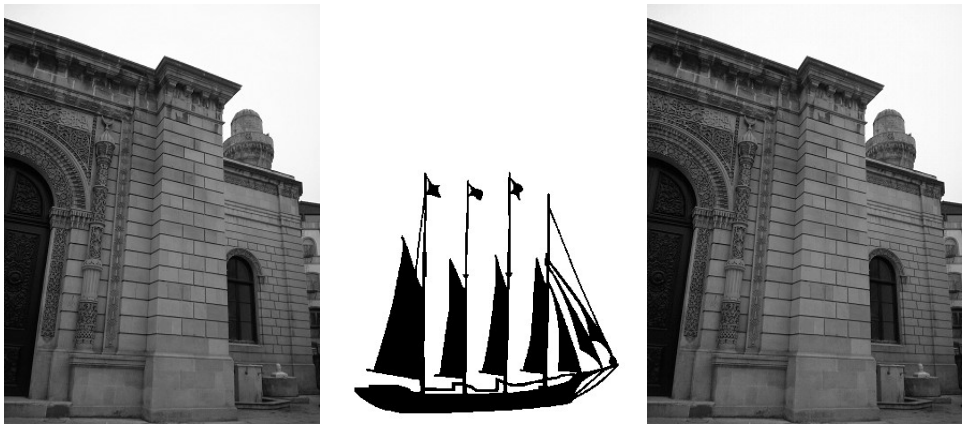
The algorithm does not authenticate watermarked images with scale attacks, which can be seen as an innocent type of operation. Moreover, the number of blocks marked as tampered with is largely as predicted for a watermarked image filtered by a 3×3 averaging filter, as seen in Figure 8a. The Gaussian filtered image is marked tampered with for a very few blocks, as seen in Figure 8b.

Figure 6 demonstrates watermarked images after re-scale authentication, intensity adjustment and histogram equalization attacks. There are several measurement metrics in the watermarking process. In semi-fragile watermarking, we use the similarity ratio, which measures the quality of the extracted secret information. Table 2 shows the SR values for the watermarked image and the extracted watermark.

Table 3 shows a comparison with four of the previous approaches that resemble our study. When previous works are examined, some of the methods divide the host image into blocks and authenticate the blocks rather than the whole image. Most of the block-wise methods use a secret key to pair the blocks and calculate some value from one block and embed it into the corresponding pair. When compared with semi-fragile works [36], a watermarked image compressed with 70% quality is authenticated JPEG, and does not mention another type of image operation that the authentication watermark survives. Our method authenticates an image that is subjected to 75% JPEG compression, histogram equalization and gamma correction. Pillai and Theagarajan's [27] authentication algorithm can resist 90% JPEG compression at most. In these respects, our algorithm performs better. The algorithm may detect some changes in some block pairs in innocent operations of a 3×3 average filter, scale-rescale operation, JPEG 50% compressions, and JPEG 25% compressions. Thus, selective fragility is not successful for this kind of innocent operation.

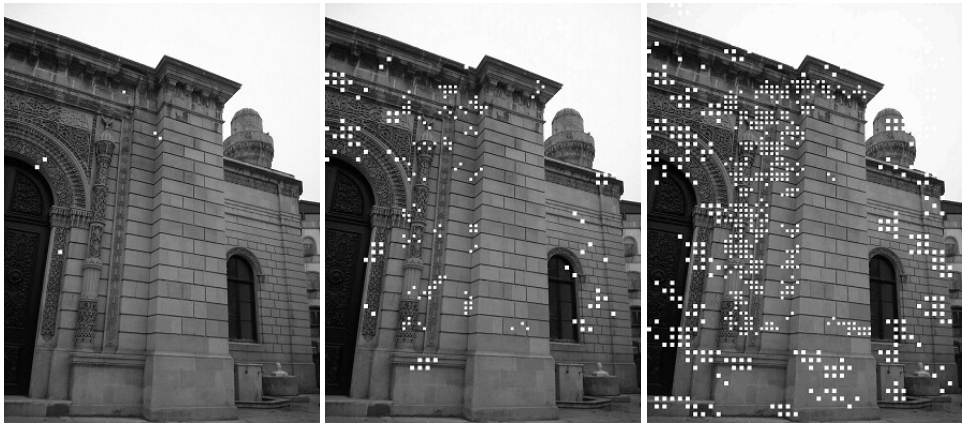
Table 1. Success Rate of Our Method for Different Attack Types.

Type of Attack	PSNR	Marked Tampered/Total # of Blocks	Success %
No attack	40.577	0/2932	100
Tampered	30.902	54/2932	100
JPEG 75% compression	35.107	6	99.8
JPEG 50% compression	33.346	181/2932	-
JPEG 25% compression	31.640	627/2932	-
Gaussian filter	29.981	16/2932	99.5
Histogram equalization	17.458	0/2932	100
Intensity Adjustment	22.114	3/2932	99.9
Scale	29.071	186/2932	-
3×3 Average filter	29.748	129/2932	-
Gamma correction	18.704	11/2932	99.63
Wrong key	-	2111/2932	-



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

Figure 4. (**a**) Original image (**b**) Binary watermark logo inserted into inner part (**c**) Watermarked image with both ownership and authentication watermark.

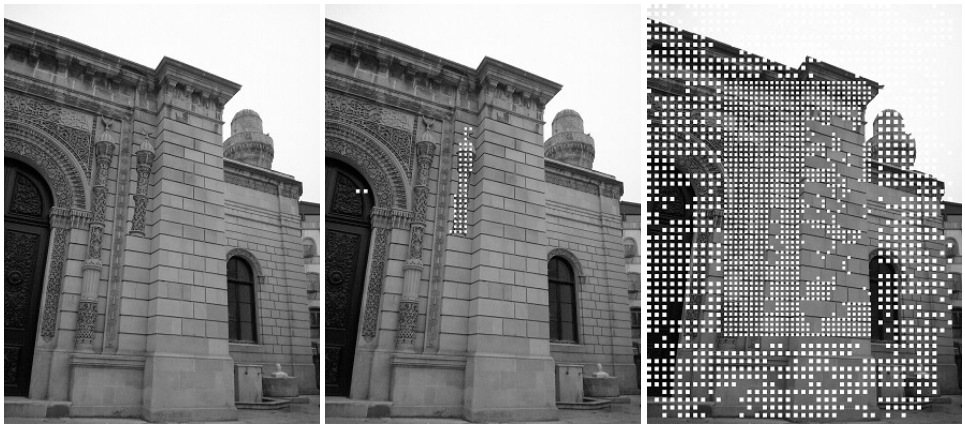


(**a**) (**b**) (**c**)

Figure 5. (**a**) JPEG 75 authentication (**b**) JPEG 50 authentication (**c**) JPEG 25 authentication.

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

Figure 6. (**a**) Re-scale authentication (**b**) Intensity adjustment authentication (**c**) Histogram equalization authentication.



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

Figure 7. (**a**) Tampered watermarked image (**b**) Tampered watermarked image authentication (**c**) Authentication with wrong key.

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

Figure 8. (**a**) 3 × 3 Average filter authentication (**b**) Gaussian filtering authentication.

With respect to tamper localization, our method can localize tamper detection in 4 × 4 block precision, which can be considered as very sensitive. The fidelity metric PSNR is around 40 for watermarked images with our method, which is an acceptable fidelity value and only worse than one of the previous methods. Our method only needs the scrambling key, which is a prime number, and the PSNR, which is not a long sequence. For the security of the watermarking method, these numbers must be passed to the authenticator. When one looks at the previous methods, all the previous methods must pass some secret value to the authenticator.

The proposed algorithm and Chamlavi [36] are semi-fragile embedding methodologies. Both algorithms need a watermark and secret key for the extraction process. The proposed algorithm resists JPEG 75 compression, while the Chamlavi algorithm resists JPEG 70 compression. The proposed algorithm has a better PSNR value than the other algorithms, which shows the high quality of the watermarked image.

Table 2. Similarity ratio for watermarked image and after attacks.

Attack	Similarity Ratio (SR)
Tampered	0.872
JPEG 75%	0.891
JPEG 50%	0.916
JPEG 25%	0.901
Gaussian filter	0.941
Histogram equalization	0.752
Intensity adjustment	0.837
Scale	0.934
Average filtering	0.885
Gamma correction	0.915
No attack	0.992

Table 3. Comparison with Previous Works.

	Lin, Hsieh [37]	**Chamlavi** [36]	**Liu, Lin, Yuan** [26]	**Pillai, Theagarajan** [27]	**Proposed Method**
Block pairing key-based	K (Prime number)	Not block based	No Key	K (Seed Key)	K (Prime number)
Fragile/semi-fragile	Fragile	Semi-fragile 70% JPEG	Fragile	Semi fragile 90% JPEG	Semi-fragile 75% JPEG Histogram eq. Intensity adj. Gamma corr.
Tamper localization	4 × 4 block area	64 × 64 block area	1 × 4 block area	16 × 16 block area	4 × 4 block area
Error Correction, Self-Recovery	Correct	Correct	Incorrect	Recovery digest embedded but recovery not shown	Incorrect
PSNR of **Watermarked Image**	≈44.3	≈38	≈40	≈48	≈40 Center part less affected
Authentication process needs	Scrambling key K	Three Keys, PRN matrix, Watermark	Watermark Parameter n	Scrambling seed K R vector (HHL2/HLH2 ratio)	Scrambling key K, PRNS

5. Conclusions and Future Work

In this study, we devised a new method for authentication-type watermarking that also includes copyright protection. The images are considered as two main parts: an inner part and an outer part. The inner part is first watermarked with a robust watermark for copyright protection. After that, the inner part is divided into blocks, DWT is applied for each block separately and binary image digests of the LL1 bands are formed for embedding into the outer blocks. The outer parts are also divided into larger blocks, and each inner block is paired with one outer block using a scrambling algorithm based on a key value. DCT is applied to the outer blocks and binary image digests of the inner blocks are embedded into the DCT values of the corresponding outer blocks. During this embedding, low-frequency and high-frequency DCT values of the outer blocks, including the DC component, are not changed to preserve the fidelity and to authenticate low-pass image operations. This process authenticates images with JPEG compression of up to a 75% quality level, subjected to histogram equalization, intensity adjustment and gamma correction, which can be considered as innocent types of image operations.

The study makes a contribution to the literature on image watermarking by considering the image as inner and outer parts and dividing the inner part into smaller blocks than the outer parts. By doing so, the watermark-holding capacity of the outer blocks is enlarged, the fidelity of the inner parts is improved, and the authentication watermark's robustness to JPEG compression, intensity adjustment, histogram equalization and gamma correction operations is increased. Tamper localization is also improved for the inner parts by using smaller block sizes. Since the method embeds a watermark obtained from the image itself, and block pairing is performed with a secret key, the method is secure against collage attacks. The proposed algorithm is blind, robust, and secure and has high data capacity, being stronger than other algorithms described in the literature. In the future, we plan to further enhance the algorithms to obtain a more robust, secure, and resistant embedding process for both images and videos. In video watermarking, several additional

issues need to be resolved, such as temporal attacks, including image dropping, swapping, and averaging. In addition, the embedding processes should be resistant to any type of video compression.

Author Contributions: Methodology, A.S. and E.E.; Validation, N.M.; Formal analysis, E.E. and A.E.T.; Investigation, A.S.; Writing—original draft, E.E. and N.M.; Writing—review & editing, A.E.T. and N.M.; Project administration, A.E.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

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

References

1. Cox, I.J.; Miller, M.L.; Bloom, J.A. 1 Introduction. In *Digital Watermarking*; Cox, I.J., Miller, M.L., Bloom, J.A., Eds.; The Morgan Kaufmann Series in Multimedia Information and Systems; Morgan Kaufmann: San Francisco, CA, USA, 2002; pp. 1–10 . [CrossRef]
2. Elbasi, E.; Eskicioglu, A.M. A DWT-based robust semi-blind image watermarking algorithm using two bands. In *Security, Steganography, and Watermarking of Multimedia Contents VIII, Proceedings of the Electronic Imaging, San Jose, CA, USA, 15–19 January 2006*; Delp, E.J., Wong, P.W., Eds.; SPIE: Bellingham, WA, USA, 2006; Volume 6072, pp. 777–787. [CrossRef]
3. Jane, O.; İlk, H.G.; Elbaşı, E. A secure and robust watermarking algorithm based on the combination of DWT, SVD, and LU decomposition with Arnold's Cat Map approach. In Proceedings of the 8th International Conference on Electrical and Electronics Engineering (ELECO), Bursa, Turkey, 28–30 November 2013; pp. 306–310. [CrossRef]
4. Singh, R.; Izhar, L.I.; Elamvazuthi, I.; Ashok, A.; Aole, S.; Sharma, N. Efficient Watermarking Method Based on Maximum Entropy Blocks Selection in Frequency Domain for Color Images. *IEEE Access* **2022**, *10*, 52712–52723. [CrossRef]
5. Cheng, H.; Huang, Q.; Chen, F.; Wang, M.; Yan, W. Privacy-Preserving Image Watermark Embedding Method Based on Edge Computing. *IEEE Access* **2022**, *10*, 18570–18582. [CrossRef]
6. Qi, W.; Guo, S.; Hu, W. Generic Reversible Visible Watermarking via Regularized Graph Fourier Transform Coding. *IEEE Trans. Image Process.* **2022**, *31*, 691–705. [CrossRef]
7. Dharmika, B.; Rupa, C.; Haritha, D.; Vineetha, Y. Privacy Protection of Digital Information using Frequency Domain Watermarking Technique. In Proceedings of the 4th International Conference on Recent Trends in Computer Science and Technology (ICRTCST), Jamshedpur, India, 11–12 February 2022; pp. 202–206. [CrossRef]
8. Elbasi, E. A Robust Information Hiding Scheme Using Third Decomposition Layer of Wavelet Against Universal Attacks. In Proceedings of the 2022 IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, 6–9 June 2022; pp. 611–616. [CrossRef]
9. Hadjer, A.; Ismail, B.H. A Dual Image Watermarking Scheme Based on WPT And Chaotic Encryption for Medical Data Protection. In Proceedings of the 7th International Conference on Image and Signal Processing and their Applications (ISPA), Wuxi, China, 8–10 July 2022; pp. 1–6. [CrossRef]
10. Zhou, X.; Ma, Y.; Zhang, Q.; Mohammed, M.; Damaševičius, R. A Reversible Watermarking System for Medical Color Images: Balancing Capacity, Imperceptibility, and Robustness. *Electronics* **2021**, *10*, 1024. [CrossRef]
11. Kushlev, S.; Mironov, R.P. Analysis for Watermark in Medical Image using Watermarking with Wavelet Transform and DCT. In Proceedings of the 55th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST). IEEE, Nis, Serbia, 10–12 September 2020. [CrossRef]
12. Wu, R.; Xu, Y. Quantum image watermarking technology based on quantum wavelet transform. In Proceedings of the International Symposium on Computer Technology and Information Science (ISCTIS), Guilin, China, 4–6 June 2021. [CrossRef]
13. Mohammmed, A.A.; Elbasi, E.; Alsaydia, O.M. An Adaptive Robust Semi-blind Watermarking in Transform Domain Using Canny Edge Detection Technique. In Proceedings of the 44th International Conference on Telecommunications and Signal Processing (TSP), Virtual Conference, 26–28 July 2021. [CrossRef]
14. Anand, A.; Singh, A.K. A Hybrid Optimization-Based Medical Data Hiding Scheme for Industrial Internet of Things Security. *IEEE Trans. Ind. Inform.* **2023**, *19*, 1051–1058. [CrossRef]
15. Trapiello, C.; Puig, V. A Zonotopic-Based Watermarking Design to Detect Replay Attacks. *IEEE/CAA J. Autom. Sin.* **2022**, *9*, 1924–1938. [CrossRef]
16. Zhang, Q.; Yuan, X.; Liu, T. Blind Dual Watermarking Scheme Using Stucki Kernel and SPIHT for Image Self-Recovery. *IEEE Access* **2022**, *10*, 96100–96111. [CrossRef]
17. Daoui, A.; Yamni, M.; Karmouni, H.; Sayyouri, M.; Qjidaa, H.; Motahhir, S.; Jamil, O.; El-Shafai, W.; Algarni, A.D.; Soliman, N.F.; et al. Efficient Biomedical Signal Security Algorithm for Smart Internet of Medical Things (IoMTs) Applications. *Electronics* **2022**, *11*, 3867. [CrossRef]
18. Fu, L.; Shi, B.; Sun, L.; Zeng, J.; Chen, D.; Zhao, H.; Tian, C. An Improved U-Net for Watermark Removal. *Electronics* **2022**, *11*, 3760. [CrossRef]

19. Xie, X.; Chen, W.; Xu, Z. A Physical-Layer Watermarking Scheme Based on 5G NR. *Electronics* **2022**, *11*, 3184. . electronics11193184. [CrossRef]
20. Yeung, M.; Mintzer, F. Invisible watermarking for image verification. *J. Electron. Imaging* **1998**, *7*, 578–591. . 1.482612. [CrossRef]
21. Wu, M.; Liu, B. Watermarking for image authentication. In Proceedings of the International Conference on Image Processing, ICIP98 (Cat. No.98CB36269), Chicago, IL, USA, 4–7 October 1998; Volume 2, pp. 437–441. [CrossRef]
22. Ellinas, J. A Robust Wavelet-Based Watermarking Algorithm Using Edge Detection. *Int. J. Comput. Sci.* **2007**, *2*, 3.
23. Fridrich, J.; Goljan, M.; Baldoza, A. New fragile authentication watermark for images. In Proceedings of the International Conference on Image Processing (Cat. No.00CH37101), Vancouver, BC, Canada, 10–13 September 2000; Volume 1, pp. 446–449. [CrossRef]
24. Rao, N.; Kumari, V. Watermarking in Medical Imaging for Security and Authentication. *Inf. Secur. J. Glob. Perspect.* **2011**, *20*, 148–155. [CrossRef]
25. Lin, S.; Yang, Z.L. Hierarchical Fragile Watermarking Scheme For Image Authentication. *Intell. Autom. Soft Comput.* **2011**, *17*, 245–255. [CrossRef]
26. Liu, X.L.; Lin, C.C.; Yuan, S.M. Blind Dual Watermarking for Color Images' Authentication and Copyright Protection. *IEEE Trans. Circuits Syst. Video Technol.* **2016**, *28*, 1047–1055. [CrossRef]
27. Nair, J.; Theagarajan, P. Semi fragile watermarking for content based image authentication and recovery in the DWT-DCT domains. *Int. Arab. J. Inf. Technol.* **2018**, *15*, 1076–1081.
28. Boujerfaoui, S.; Douzi, H.; Harba, R.; Gourrame, K. Robust Fourier Watermarking for Print-Cam Process using Convolutional Neural Networks. In Proceedings of the 7th International Conference on Signal and Image Processing (ICSIP), Suzhou, China, 20–22 July 2022. [CrossRef]
29. Cai, Z.; Si, Y.; Zhang, J.; Wang, J. Design and Implementation of Image Copyright Protection System Based on Chinese Cryptographic Algorithms. In Proceedings of the 7th International Conference on Signal and Image Processing (ICSIP), Suzhou, China, 20–22 July 2022. [CrossRef]
30. Campos-Ponce, E.; Cedillo-Hernandez, M. Tamper detection and localization in color images using secure block-based watermarking. In Proceedings of the 2022 IEEE Mexican International Conference on Computer Science (ENC), Veracruz, Mexico, 24–26 August 2022. [CrossRef]
31. Singh, O.P.; Anand, A.; Agrawal, A.K.; Singh, A.K. Electronic Health Data Security in the Internet of Things through Watermarking: An Introduction. *IEEE Internet Things Mag.* **2022**, *5*, 55–58. [CrossRef]
32. Ernawan, F.; Ariatmanto, D.; Musa, Z.; Mustaffa, Z.; Zain, J.M. An Improved Robust Watermarking Scheme using Flexible Scaling Factor. In Proceedings of the International Conference on Computational Intelligence (ICCI), Bandar Seri Iskandar, Malaysia, 8–9 October 2020. [CrossRef]
33. Sahu, A.K.; Sahu, M.; Patro, P.; Sahu, G.; Nayak, S. Dual image-based reversible fragile watermarking scheme for tamper detection and localization. *Pattern Anal. Appl.* **2022**. [CrossRef]
34. Zhang, G.; Zheng, L.; Su, Z.; Zeng, Y.; Wang, G. M-Sequences and Sliding Window Based Audio Watermarking Robust Against Large-Scale Cropping Attacks. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 1182–1195. [CrossRef]
35. Vougiatzis, G.; Pitas, I. Chaotic Mixing of Digital Images and Applications to Watermarking. In Proceedings of the European Conference on Multimedia Applications, Services and Techniques (ECMAST'96), Louvain-la-Neuve, Belgium, 21–23 May 1996.
36. Chamlawi, R.; Khan, A.; Idris, A.; Munir, Z. A Secure Semi-Fragile Watermarking Scheme for Authentication and Recovery of Images based on Wavelet Transform. *Int. J. Comput. Inf. Eng.* **2008**, *2*, 11.
37. Lin, P.L.; Hsieh, C.K.; Huang, P.W. A hierarchical digital watermarking method for image tamper detection and recovery. *Pattern Recognit.* **2005**, *38*, 2519–2529. [CrossRef]