electronics

Article

A Novel Fragile Zero-Watermarking Algorithm for Digital Medical Images

Zulfiqar Ali [1,*], Fazal-e-Amin [2,*] and Muhammad Hussain [3]

[1] School of Computer Science and Electronic Engineering, University of Essex, Colchester CO4 3SQ, UK
[2] Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia
[3] Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh 11541, Saudi Arabia; mhussain@ksu.edu.sa
* Correspondence: z.ali@essex.ac.uk (Z.A.); famin@ksu.edu.sa (F.-e.-A.)

Abstract: The wireless transmission of patients' particulars and medical data to a specialised centre after an initial screening at a remote health facility may cause potential threats to patients' data privacy and integrity. Although watermarking can be used to rectify such risks, it should not degrade the medical data, because any change in the data characteristics may lead to a false diagnosis. Hence, zero watermarking can be helpful in these circumstances. At the same time, the transmitted data must create a warning in case of tampering or a malicious attack. Thus, watermarking should be fragile in nature. Consequently, a novel hybrid approach using fragile zero watermarking is proposed in this study. Visual cryptography and chaotic randomness are major components of the proposed algorithm to avoid any breach of information through an illegitimate attempt. The proposed algorithm is evaluated using two datasets: the Digital Database for Screening Mammography and the Mini Mammographic Image Analysis Society database. In addition, a breast cancer detection system using a convolutional neural network is implemented to analyse the diagnosis in case of a malicious attack and after watermark insertion. The experimental results indicate that the proposed algorithm is reliable for privacy protection and data authentication.

Keywords: breast cancer; computer-aided diagnostic system; deep learning; chaotic randomness; privacy protection; content authentication

Citation: Ali, Z.; Fazal-e-Amin; Hussain, M. A Novel Fragile Zero-Watermarking Algorithm for Digital Medical Images. *Electronics* **2022**, *11*, 710. https://doi.org/10.3390/electronics11050710

Academic Editor: Qingqi Pei

Received: 16 January 2022
Accepted: 22 February 2022
Published: 25 February 2022

1. Introduction

Rapid development in image processing techniques has significantly increased the importance of digital images because of their enhanced usage in various applications, ranging from computer-aided diagnostic (CAD) systems to biometric recognition systems [1–4]. At the same time, due to the availability of sophisticated tools, images can be tampered with easily and are facing the problems of content authentication and copyright protection.

Unlike authentication systems, tampering with medical images may prove to be life-threatening [5,6]. If a medical image is tampered with, then the CAD system may lead to a false diagnosis. Ultimately, a healthy person may face mental disturbance and spend money and time to follow up on the misdiagnosed condition. If a patient is suffering from a disease, then the delay due to a false diagnosis will make his or her condition severe to the point that it cannot be cured. Therefore, authenticating medical images before diagnosis using CAD systems is crucial.

In addition to data tampering, the privacy of patients becomes highly vulnerable when the data are stored offline in their original form or transmitted through wireless communication for centralised processing or expert opinions using cloud-based environments and edge or fog computing [7,8]. The protection of patients' particulars, such as names and social security and medical numbers, should be the top priority of health care providers [9–11]; otherwise, they may face consequences in the form of regulatory fines, legal fees and a bad reputation in the market. To avoid such situations, digital watermarking is one of the potential solutions for privacy protection and data integrity.

Digital watermarking embeds patients' information (watermark) into medical signals to ensure privacy, and only authorised health care staff with a relevant secret key can disclose patients' identities. One of the common approaches in watermarking is the insertion of patients' information in the region of noninterest (RONI). This region is unaffected by the lesion, and the insertion of the watermark will not have any negative impact on the decision of CAD systems. However, the detection of RONI becomes challenging when an image contains more than one region of interest (ROI) [2], and an erroneously detected RONI may lead to a false diagnosis [12,13]. Another difficult situation is if ROI annotations are unavailable in images. Therefore, approaches based on RONI and ROI are unsuitable for privacy protection and data integrity.

Similarly, conventional digital watermarking distorts the characteristics of the host image after inserting the watermark and may lead to a false diagnosis [14–17]. Nevertheless, in the reversible watermark, the watermark is extracted before the diagnosis; hence, it does not affect the diagnosis. However, the major drawback of this approach is that medical images become vulnerable after identity extraction [18–21].

To avoid the limitations of such types of watermarking, various algorithms for zero watermarking have been proposed in the literature [22–24]. Zero watermarking does not degrade the host image after inserting the watermark. Therefore, the diagnosis results are unaffected.

Image encryption is also a prime concern for protecting data from illegal usage. In a recent study [25], mammograms are encrypted through visual cryptography. Multiple secret shares are generated from the original mammograms to protect them from unauthorised access. Mammograms can be decrypted only when all secret shares are available simultaneously.

Finally, image authentication is extremely critical for the accurate detection of lesions. In the case of a malicious attack, an image of a normal person may exhibit irregular patterns and look like a patient's image due to the complex and transient behaviour introduced by the attack. In [26], the effect of a noise attack is discussed by adding the noise of different signal-to-noise (SNR) ratios to the medical signals. Different performance measures are computed to compare the original and extracted watermarks (retrieved from attacked host signals). The results indicate that the recovered identity becomes more distorted as the SNR increases. As a result, the diagnosis system fails to detect the disease correctly. This suggests that patients' identities and mammograms should be authenticated before diagnosis.

Therefore, watermarking should not only provide privacy protection but also authenticate the medical image content. This scenario leads to fragile watermarking, as any change in an image distorts the watermark [27], and the health care staff will be alarmed over its authenticity.

Normally, watermarking and authenticity fall under two different categories of image forensics [28]. Fragile watermarking is one of the examples of active forensics [29], and authenticity detection is categorised as passive forensics [30]. In this study, we propose a hybrid solution to protect privacy and content authentication. A watermark can be public or secret. As patients' identities should not be revealed, watermarking will not be visible in the proposed solution. Most importantly, the proposed solution inserts the watermark in a secret key instead of the host medical image to avoid any distortion. Therefore, zero watermarking is considered. The main contribution of this study is to provide a hybrid solution containing new embedding and extraction processes with the following capabilities:

- Content authentication using fragile watermarking;
- Privacy protection using zero watermarking;
- Dual protection for privacy through visual cryptography;
- Intractable chaotic randomness.

Although various components of the proposed solution such as Shamir's secret sharing scheme, logistic maps and local binary patterns (LBPs) have been explored in the domain of watermarking and other scientific areas, these components are used in an entirely different way in embedding and extraction processes, which makes the proposed fragile zero-watermarking algorithm a novel approach. A patient's identity is encrypted using one of the visual cryptography schemes (i.e., Shamir's secret sharing scheme). Then, the embedding and extraction processes of the proposed algorithm are used to insert and recover the watermark, respectively. To enhance the reliability of protection, a logistic map is implemented. The proposed algorithm is evaluated using two datasets of digitised mammograms. The baseline results for the detection of breast cancer in these datasets are obtained by developing a system using a convolutional neural network (CNN). These results help in determining any negative impact of the proposed algorithm on the detection of breast cancer.

The rest of the paper is organised in the following manner. Section 2 describes the main components of the proposed algorithm. Section 3 illustrates the core processes of the newly proposed algorithm: watermark embedding and extraction. Section 4 evaluates the algorithm and provides its analysis using experimental results and discussion. This section also highlights the comparisons with existing works. Finally, Section 5 draws some conclusions.

2. Components of the Proposed Algorithm

In this study, the digitised mammograms were taken from the Digital Database for Screening Mammography (DDSM) [31] and the Mini Mammographic Image Analysis Society (Mini-MIAS) database [32]. The necessary components of the proposed fragile zero-watermarking algorithm are briefly described in this section.

As zero watermarking does not embed the watermark in a host image, the image characteristics or features are still crucial to observe. Without these characteristics, the secret key carrying the watermark cannot be generated. Figure 1 shows that mammograms have a consistent black background, which is an unwanted area for feature extraction. Therefore, it is removed by applying an automatic method.

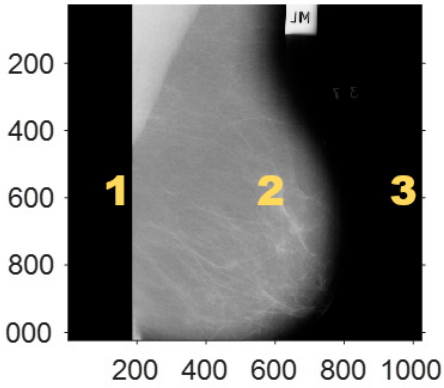


Figure 1. An original mammogram with unwanted areas (consistent black background) indicated by labels 1 and 3.

Moreover, the process to generate the secret shares of the watermark and the use of chaotic randomness are illustrated in the following subsections.

2.1. Removal of Background from Mammograms

Region 2 represents the breast in the mammogram, and an appropriate edge detection algorithm is required to determine its outer edges (i.e., the borders between the three regions). In Figure 1, the breast contains various types of vessels, and the algorithm must avoid them when detecting the outer edges. To perform this task, the Sobel operator was implemented, which has been a widely used edge detection algorithm. Its overall performance is better than other contemporaneous operators, such as the Prewitt operator [33].

The Sobel operator comprises two convolutional kernels, O_x and O_y, as given by Equation (1). They are applied on the mammogram for the gradient approximation of each pixel in the horizontal and vertical directions [34]. This operator enhances the edges, where the gradients are usually larger than the homogeneous regions in the mammogram:

$$O_x = \begin{bmatrix} 1 & 0 & -1 \\ 2 & 0 & -2 \\ 1 & 0 & -1 \end{bmatrix} \text{ and } O_y = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix}. \tag{1}$$

For each pixel, the gradient approximations are combined using the following relation to obtain the gradient magnitude:

$$O = \sqrt{{O_x}^2 + {O_y}^2}. \tag{2}$$

The operator was first applied on the original grey scale image (illustrated in Figure 1). The resultant image is depicted in Figure 2a, showing that the vessels (edges) inside the breast were also detected but were undesired. To solve this issue, the original image was first converted to a black and white image, and then the operator was applied. The obtained image is displayed in Figure 2b, clearly highlighting the borders between the three regions. Then, the features of this region are computed and analysed.

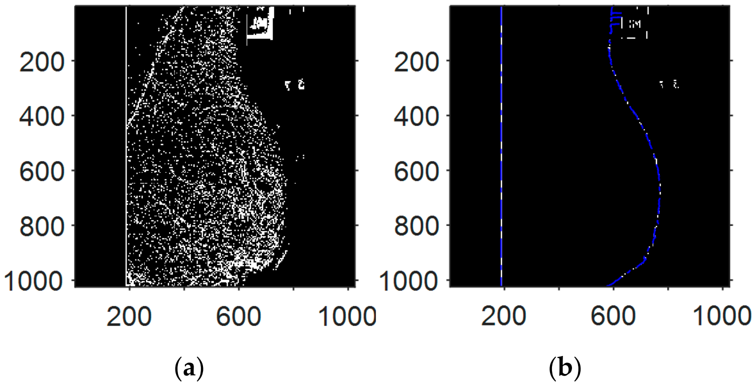


Figure 2. Detection of the outer edges of the breast (region 2) (**a**) after applying the operator on the original grey scale mammogram and (**b**) after applying the operator on the black and white mammogram.

2.2. Feature Extraction for the Insertion Process

In this study, the features were extracted using the local binary pattern (LBP) from the extracted region of the mammograms (only the breast without the background). The LBP is a simple yet efficient texture operator [35]. To compute the LBP, the extracted area is divided into 3 × 3 blocks. Then, the centre element is compared with its eight neighbours. If the centre element is equal to or greater than a neighbour, the neighbour is replaced by 1; otherwise, it is 0. Similarly, the centre element is compared with all eight neighbours, and an eight-bit binary number is generated. The range of these binary numbers in equivalent decimal numbers is from 0 to 255. This process is repeated for each 3 × 3 block of region 2. Hence, every pixel in the selected regions is represented by equivalent decimal numbers, which are also referred to as LBP codes.

The generated LBP codes were grouped as uniform and nonuniform patterns based on the number of 1-to-0 and 0-to-1 transitions in a binary number. The codes with two or fewer transitions were designated to be uniform, and all other codes with three or more transitions were referred to as nonuniform. For instance, 10101011 with 6 1-to-0 and 0-to-1 transitions represents a nonuniform code, whereas 00001100 is a uniform code with two transitions. In the range from 0 to 255, 58 uniform and 198 nonuniform codes were recorded. Each uniform code was represented by a unique bin in a histogram. However, all nonuniform codes were grouped in the last bin (i.e., the 59th bin). This part explains why nonuniform codes were chosen for the watermark insertion process, as they would be good in the context of randomness.

The distribution of LBP codes for region 2 of a mammogram is illustrated in Figure 3. The total number of nonuniform codes was around 55,000, and they were sufficient to accommodate the watermark. The same number of nonuniform codes was observed in all mammograms of both datasets.

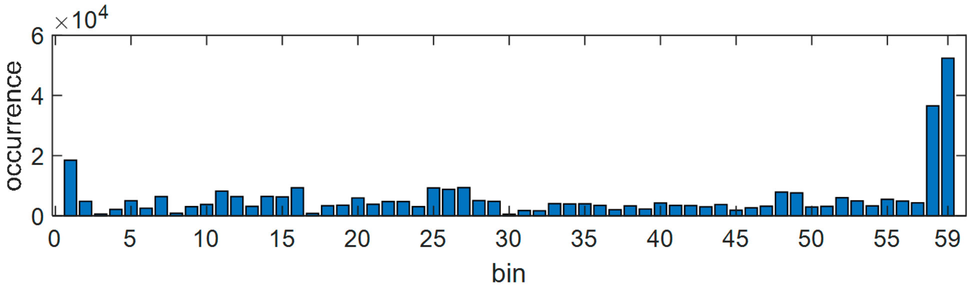
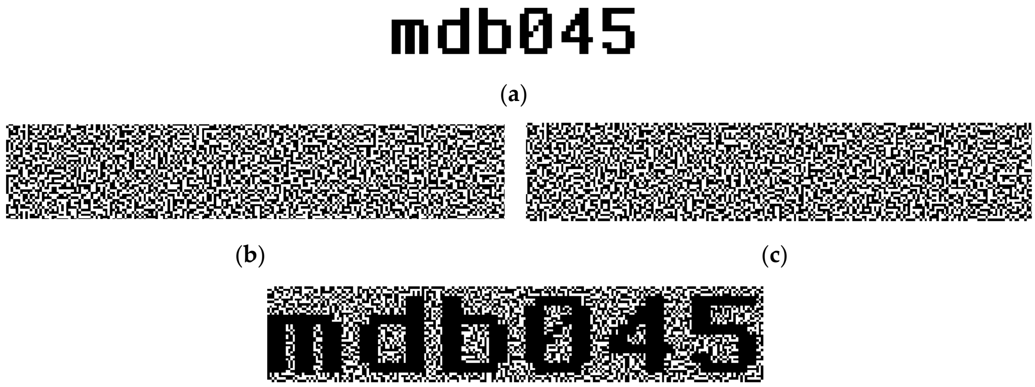


Figure 3. Distribution of uniform and nonuniform LBP codes in a mammogram.

After removing the unwanted background from the mammograms and the computation process of the LBP, the next important component was the generation of secret shares of the watermark and the creation of random numbers for the insertion and extraction processes.

2.3. Generation of Secrete Shares of Patients' Identities

The watermarks in this study are patients' identities, which are six-character-long alphanumeric strings and represented by I. They are converted into black and white images that are 20 × 108. The image of one of the patient's identities is depicted in Figure 4a.



(**a**)

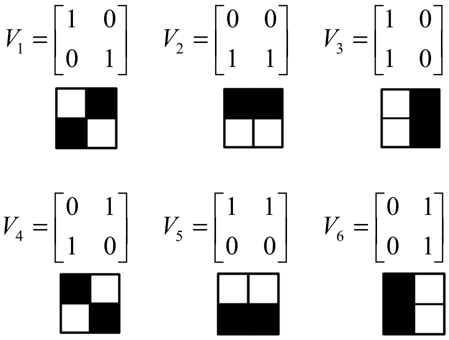
(**b**) (**c**)

(**d**)

Figure 4. The original patient's identity (watermark) and its generated secret shares using Shamir's scheme: (**a**) original identity I, (**b**) first secret share S_1, (**c**) second secret share S_2, (**d**) retrieved identity by overlapping (bitwise AND operation) of S_1 and S_2.

One of the objectives of the proposed algorithm is to protect patients' particulars, which should not be transmitted to the recipients or stored in their original form to avoid a breach of privacy. To provide double the security, two secret shares of I (say S_1 and S_2) were created using Shamir's secret sharing scheme as shown in Figure 4b,c, respectively. These generated shares were used in the embedding process of the proposed algorithm and embedded into the watermark key.

The method to generate secret shares is as follows. Every pixel of I is replaced by one of the 2 × 2 matrices given in Figure 5. If the pixel is white, then it is replaced by the same matrix (say V_2) in both shares S_1 and S_2. In the case of a black pixel, if it is replaced by V_3 in S_1, and then its complement (V_6) replaces the corresponding pixel in S_2. The matrices V_1–V_6, are selected randomly for each pixel using the random numbers in the range [1–6].



$$V_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad V_2 = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \quad V_3 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$$

$$V_4 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad V_5 = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \quad V_6 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$$

Figure 5. Each pixel of *I* is replaced by one of these blocks to generate two secret shares.

As each pixel of I is replaced by a 2 × 2 matrix, the dimensions of each generated share are doubled (i.e., 40 × 216). Thus, the total number of bits required to insert these shares was 17,280 (8640 + 8640). Every pixel of S_1 and S_2 was embedded randomly in the secret key using the computed features of the selected region.

The simplicity in retrieving the identity (I) using the generated shares (S_1 and S_2) was a prime reason to use Shamir's scheme. The overlapping of shares printed on the transparencies or bitwise AND operation between them would reveal I as shown in Figure 4d. This step is described in the extraction process of the proposed algorithm.

Before explaining the proposed algorithm, the process of creating deterministic randomness is discussed in the following section.

2.4. Deterministic Randomness

Random numbers can be generated in different ways. Normally, the length of a sequence of random numbers is equivalent to the watermark. Sometimes, it also needs to be transmitted to the recipient with the host image for the watermark extraction. Depending on the watermark, the length of the sequence can be very long. However, this can be avoided by using chaotic systems due to their deterministic nature of randomness. The same sequence of random numbers can be regenerated using the initial conditions received from the sender, and the recipient does not need the sequence.

One of the simplest chaotic systems, known as the logistic map, was implemented to generate random sequences in the proposed algorithm. It was introduced by P. F. Verhulst and belongs to the family of first-order difference equations, which can be represented mathematically using Equation (3):

$$L_{x+1} = \mu L_x(1 - L_x), \tag{3}$$

where $\mu \in$ [0,4] is a system parameter and $L_0 \in (0, 1)$ is the initial condition. The behaviour of the logistic map is chaotic when $\mu \in$ (3.5699456,4), except for a narrow window near 3.8284 [36]. For every value of the system parameters in this range, the generated chaotic sequences (L_x; x = 1, 2, 3, . . .) are unique. The logistic map is highly sensitive to μ. A small variation in the value of μ generates an entirely different sequence, and it is uncorrelated statistically. The values of $\mu \in$ (3.8284, 3.8510) will not be used in this study due to oscillation among the specific values in this range.

The random numbers were generated for the creation of a watermark key during the embedding process of the proposed algorithm, which is discussed in the following section.

3. Proposed Fragile Zero-Watermarking Algorithm

Two major processes of the newly proposed fragile zero-watermarking algorithm are illustrated step by step for embedding and extracting patients' identities I in the following sections and in Figures 6 and 7, respectively.

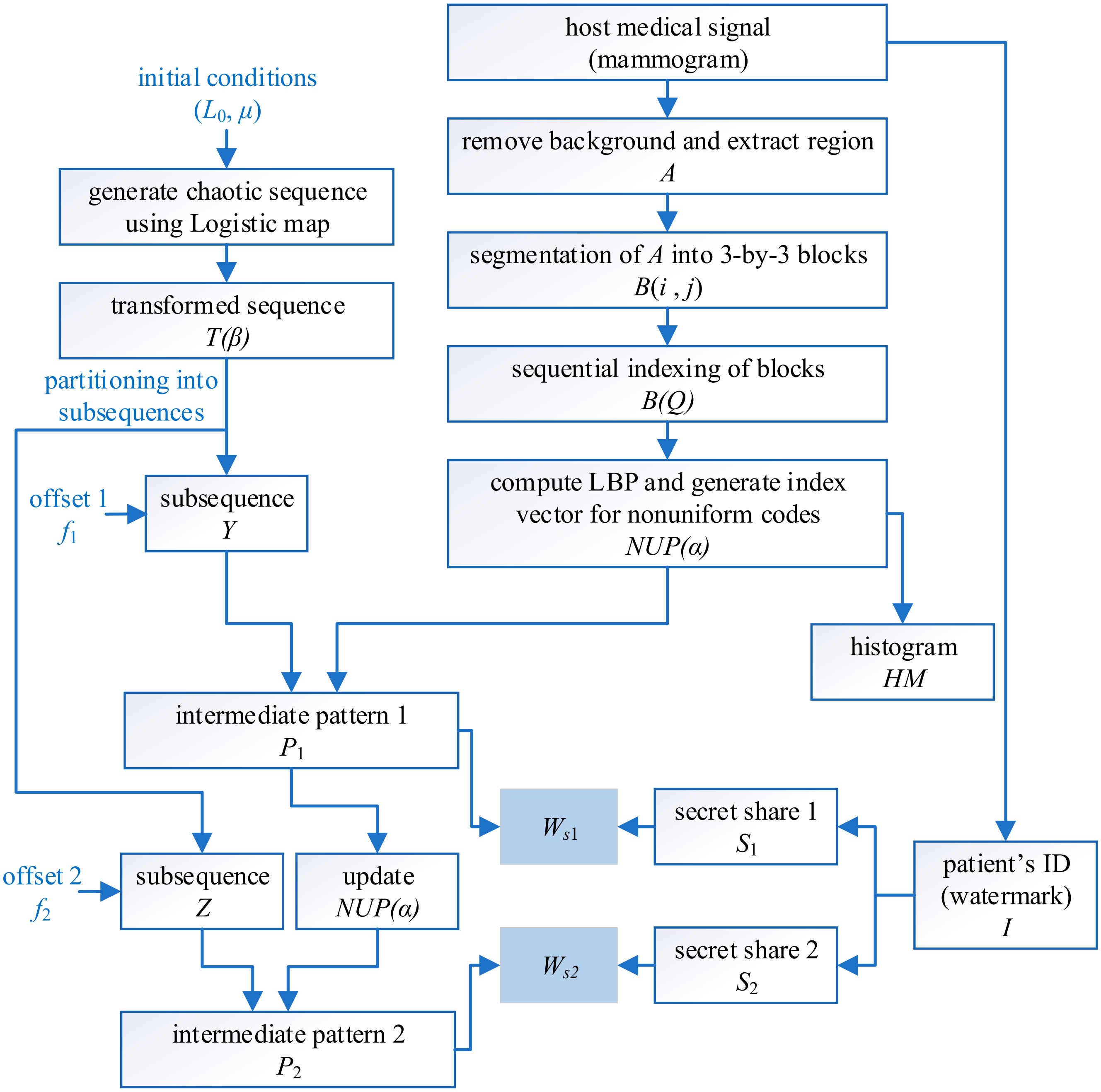

host medical signal (mammogram)
remove background and extract region A
segmentation of A into 3-by-3 blocks $B(i, j)$
sequential indexing of blocks $B(Q)$
compute LBP and generate index vector for nonuniform codes $NUP(\alpha)$
histogram HM
initial conditions (L_0, μ)
generate chaotic sequence using Logistic map
transformed sequence $T(\beta)$
partitioning into subsequences
offset 1 f_1
subsequence Y
intermediate pattern 1 P_1
offset 2 f_2
subsequence Z
update $NUP(\alpha)$
intermediate pattern 2 P_2
W_{s1}
W_{s2}
secret share 1 S_1
secret share 2 S_2
patient's ID (watermark) I

Figure 6. Block diagram of the embedding process of the proposed algorithm.

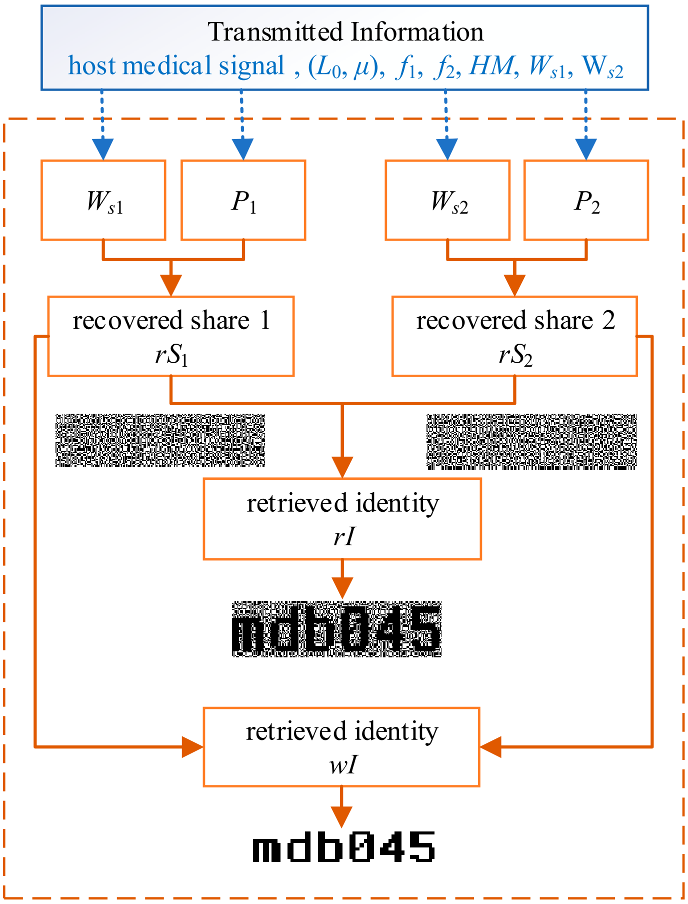


Figure 7. Block diagram of the extraction process of the proposed algorithm.

3.1. Embedding Process

The patients' identities were disguised using the following steps of the embedding process:

1. Create two secret shares, S_1 and S_2, for I using Shamir's secret sharing scheme. The dimensions of each share are $s \times t$.
2. Read a host image and detect region 2 (as shown in Figure 2) by removing the background with the Sobel operator. The indices A of the desired region are given in Equation (4):

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1N_1} \\ a_{21} & a_{22} & \cdots & a_{2N_2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{M1} & a_{M2} & \cdots & a_{MN_n} \end{bmatrix} \tag{4}$$

   where M indicates the number of rows. For each row, the columns are varying and represented by $N = N_1, N_2, N_3, \ldots, N_n$.
3. Using these indices, segment the region into overlapping 3 × 3 blocks (without zero padding) such that each element is the centre of a block. Moreover, during segmentation, if the rows have varying numbers of columns, consider a small index. To keep the remaining process simple, ascending sequential indices are assigned to the blocks after concatenating them horizontally. An index Q is assigned to a 3 × 3

block $B(i, j)$ starting from the ith row and jth column according to the relationship in Equation (5):

$$\begin{array}{l} Q = j + \sum\limits_{l=1}^{i-1} \psi_l \\ \text{where} \\ i = 1, 2, 3, \ldots, M-2 \\ j = 1, 2, 3, \ldots, \psi_i \\ \text{and } \psi_i = \min(N_i, N_{i+1}, N_{i+2}) - 2 \end{array} \tag{5}$$

4. Compute the LBP code of each block $B(Q)$, and if it is nonuniform, then store index Q as given by Equation (6):

$$NUP(\alpha) = [Q|\text{LBP}(B(Q)) \text{ is non-uniform}] \tag{6}$$

In addition, to detect the malicious attack, a histogram *HM* using all LBP codes is generated, where the frequency of each LBP code from 0 to 255 is represented by a single bin.
5. Randomly determine two integers, say f_1 and f_2, in the range [1–1000] to set an offset for choosing nonuniform blocks randomly.
6. Using the initial conditions (μ, L_0) in the logistic map (form the range discussed in Section 2.4), produce a sequence of length greater than α to introduce the randomness in the secret key. The generated numbers are up to four decimal places and are normally between 0 and 1. As the index of a block is always an integer, the number is transformed into an integer using Equation (7):

$$T(i) = \left(R_{iD_1} + R_{iD_2}\right)\text{mod}5 \tag{7}$$

where D_1 and D_2 are the digits at the first and second decimal places, respectively, in the ith random number R. The transformed number in the sequence *T(i)* is ignored if it is zero, as the intention is not to repeat the same nonuniform block. Each element of *T(i)* guides toward skipping the number of nonuniform blocks in selecting the next block from *NUP*. Ultimately, a sequence $T(\beta)$ is obtained, where $\beta = 1, 2, 3, \ldots, \alpha > [2 \times (s \times t)/8]$.
7. Partition *T(β)* into two subsequences, Y and Z, where each of them provides the random locations of blocks with nonuniform LBP codes. These subsequences are mathematically defined in Equation (8):

$$\begin{array}{c} Y_\gamma = f_1 + cumsum\left(T(1) \text{ to } T\left(\frac{s\times t}{8}\right)\right) \\ Z_\gamma = f_2 + cumsum\left(T\left(\frac{s\times t}{8}+1\right) \text{ to } T\left(2\times\frac{s\times t}{8}\right)\right) \end{array} \tag{8}$$

8. Generate two intermediate patterns P_1 and P_2. For P_1, take the first index from Y. Assume that this index is 205, which means select the 205th block with a nonuniform LBP code. Then, convert the code to an eight-bit binary number and store it in P_1. Mathematically, this step is expressed in Equation (9):

$$P_1 = convertTObinary(LBP(B(NUP(Y_\gamma)))) \tag{9}$$

Now, determine the binary digit for the next block according to Y and append it at the end of P_1. Repeat this process for all values of Y. Later, delete all these indices from *NUP* and repeat the process to determine pattern P_2 by using Z.
9. Finally, create secret watermark keys by performing bitwise exclusive OR operator between intermediate keys (P_1 and P_2) and the secret shares (S_1 and S_2), as given by Equation (10):

$$\begin{array}{l} W_{S1} = S_1 \oplus P_1 \\ W_{S2} = S_2 \oplus P_2 \end{array} \tag{10}$$

Now, the host image, histogram *HM*, secret key W_{S1}, offset f_1 and initial conditions (μ, L_0) are sent to health care staff 1. Likewise, the image, secret key W_{S2}, both offsets and the initial conditions (μ, L_0) are sent to health care staff 2. Both secret keys are depicted in Figure 8a,b, respectively.

(*MSE* = 0.42, *PSNR* = 3.11, *SSIM* = 0.03)
(**a**)
(*MSE* = 0.55, *PSNR* = 2.54, *SSIM* = −0.11)
(**b**)

Figure 8. Embedded secret shares (W_{S1} and W_{S2}) and their comparison with the corresponding original shares (S_1 and S_2, illustrated in Figure 4b,c) using the *MSE, PSNR* and *SSIM*. (**a**) First embedded secret share W_{S1} (*MSE* = 0.42, *PSNR* = 3.11 and *SSIM* = 0.03 when compared with S_1). (**b**) Second embedded secret share W_{S2} (*MSE* = 0.55, *PSNR* = 2.54 and *SSIM* = -0.11 when compared with S_2).

3.2. Extraction Process

The identity of a patient will not be revealed unless staff members do not have relevant secret keys. After extracting the secret shares with relevant keys, they must combine them to obtain the identity.

To reveal I using the transmitted information, the health care staff repeats steps 1–7 of the embedding process to reconstruct random sequences Y and Z. Then, the following steps of the extraction process are followed:

1. Staff 1: Reconstruct intermediate pattern P_1 by using random sequence Y and perform bitwise exclusive OR operator with the transmitted secret key W_{S1} to recover the first share rS_1 of I as given in Equation (11):

$$rS_1 = W_{S1} \oplus P_1 \tag{11}$$

2. Staff 2: Delete the block pointed out by Y and reconstruct P_2 by using Z. Then, perform bitwise exclusive OR operator with the transmitted secret key W_{S2} to recover the second share rS_2 of I as given in Equation (12):

$$rS_2 = W_{S2} \oplus P_2 \tag{12}$$

3. Finally, combine both recovered shares to reveal identity using the bitwise AND operator expressed in Equation (13). Figure 9a shows the retrieved identity, say *rI,* which is obtained using the following equation:

$$rI = rS_1 \text{ AND } rS_2 \tag{13}$$

If the recovered identity should be with the white background as shown in Figure 4a, then proceed to step 4.

4. When the corresponding 2 × 2 blocks are the same in S_1 and S_2, then the recovered pixel will be 1. Similarly, if the corresponding blocks complement one another, then the recovered pixel will be 0. Ultimately, the identity (e.g., *wI*) will be retrieved with a white background.

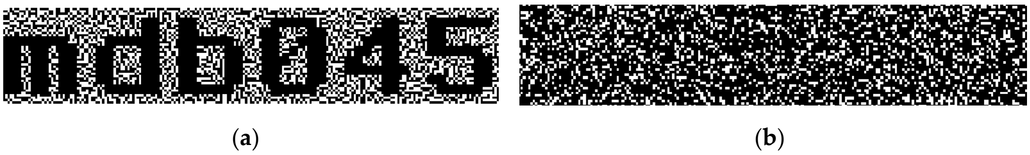


Figure 9. Revealed identities after the overlapping of (**a**) original shares S_1 and S_2 and (**b**) embedded shares W_{S1} and W_{S2}.

Now, various aspects of the proposed algorithm will be evaluated, such as the achieved imperceptibility after inserting the watermark, the detection reliability of a watermark with a nonrelevant secret key, and data integrity in the case of a malicious attack.

4. Experimental Results of the Proposed Algorithm and Discussion

Two datasets were used to investigate the key aspects of the proposed algorithm. Obtaining their baseline results was important. These results helped in analysing any negative impact on the detection of breast cancer caused by the proposed algorithm.

The first dataset was the Curated Breast Imaging Subset of DDSM (CBIS-DDSM) [37], which is the latest version of DDSM [31]. CBIS-DDMIS was converted into the standard DICOM format, whereas the format of digitised film mammograms in DDMIS is a lossless JPEG, which is obsolete. CBIS-DDMIS contains 2478 mammography images of 1249 women, and most of the cases include both views (i.e., mediolateral and craniocaudal). The baseline results of this dataset for the classification of malignant and benign images were obtained using the same set-up that was used in [2]. Two structures, a deep neural network 16 layers deep (VGG16) and a residual neural network 50 layers deep (ResNET50), were implemented. The CNN was trained in two steps. First, a patch classifier was trained. Second, the whole image classifier converted from the patch classifier was trained. An average accuracy of 91% with a sensitivity and specificity of 86.1% and 81%, respectively, was achieved.

The second dataset was mini-MIAS, which comprises 322 digitised mammograms collected from 161 women. The baseline results for mini-MIAS were also obtained with VGG16 and ResNet50 for the classification of malignant and benign images. The obtained accuracies were 73.47% and 68.76%, the sensitivity was 76.42% and 74.46%, and the specificity was 68.78% and 61.29%, respectively. In both datasets, the dimensions of all the mammograms were 1024 × 1024.

Different metrics were used to evaluate the performance of the proposed algorithm for privacy protection and data integrity: the mean square error (*MSE*), peak signal-to-noise ratio (*PSNR*) and structural similarity index (*SSIM*). The formulae for the *MSE*, *PSNR* and *SSIM* are given by Equations (14)–(16), respectively. Using these measures, the quality of the identities when retrieved using a relevant secret key, a nonrelevant secret key and in the case of an attacked mammogram was determined by comparing them with the original identities:

$$MSE(im_1, im_2) = \frac{\sum_{g=1}^{d_1} \sum_{h=1}^{d_2} [im_1(g,h) - im_2(g,h)]^2}{d_1 \times d_2} \tag{14}$$

$$PNSR(im_1, im_2) = 20 \log_{10}\left(\frac{2^{NBP} - 1}{\sqrt{MSE}}\right) \tag{15}$$

$$SSIM(im_1, im_2) = \frac{(2\mu_{im_1}\mu_{im_2} + c_1)(2\sigma_{im_1 im_2} + c_2)}{(\mu_{im_1}^2 + \mu_{im_2}^2 + c_1)(\sigma_{im_1}^2 + \sigma_{im_2}^2 + c_2)} \tag{16}$$

where $d_1 \times d_2$ represents the image's dimensions, NBP stands for the number of bits per pixel and μ_{im1}, μ_{im2}, σ_{im1}, σ_{im2} and σ_{im1im2} indicate the local means, standard deviations and cross-covariances for images im_1 and im_2. In addition, c_1 and c_2 are regularisation constants given by $c_1 = (0.01 \times u)^2$ and $c_2 = (0.03 \times u)^2$, where $u = 2^{NBP} - 1$.

All experiments for the embedding and insertion processes were performed with MATLAB (version R2021b), whereas Python (version 3.8.10) was used for the CNN-based CAD system and installed on a computer with an Intel Core i7-45000U CPU @ 1.80 GHz processor, 16 GB of memory, a 1-TB hard disk, and a Windows 10 Pro operating system. With these specifications, the average time taken by the embedding and extraction processes to secure and retrieve an identity was 1.81 s and 2.42 s, respectively.

4.1. Insertion and Extraction Reliability of the Proposed Algorithm

The first step in the evaluation of the proposed algorithm was to observe the performance of its embedding and extraction processes. By following the steps of the embedding process, the secret shares S_1 and S_2 with dimensions of 40 × 216 each (Figure 4a,b) were generated, and the indices A were determined after removing the background of the mammogram of dimensions 1024 × 1024. Two offsets (f_1 = 100 and f_2 = 200) were randomly generated. Then, a chaotic sequence with initial conditions μ = 3.6 and L_0 = 0.1 was produced to yield subsequences Y and Z for the random selection of blocks with nonuniform LBP codes. Only 1080 (out of 55,000) LBP codes were used in this process. Finally, the intermediate patterns P_1 and P_2 were computed, and the secret shares S_1 and S_2 were embedded into them to obtain the secret keys W_{S1} and W_{S2}. The secret keys were in fact embedded secret shares, and they are shown in Figure 8. To measure the difference between the original shares (S_1 and S_2) and the embedded shares (W_{S1} and W_{S2}) the *MSE*, *PSNR* and *SSIM* were computed, and they are given in Figure 8.

The computed *MSE* of 0.42 for share 1 indicates that the original and embedded shares were significantly different from each other. The low values for the *PSNR* and *SSIM* also suggest the same. A similar trend was exhibited in the case of share 2; patients' identities remained unknown even after combining these embedded secret shares. This factor could be verified by performing the bitwise AND operation between the embedded shares (W_{S1} and W_{S2}), and the retrieved identity is displayed in Figure 9b.

Another example is provided in Figure 10 for explaining the functionality and reliability of the embedding and extraction processes of the proposed algorithm.

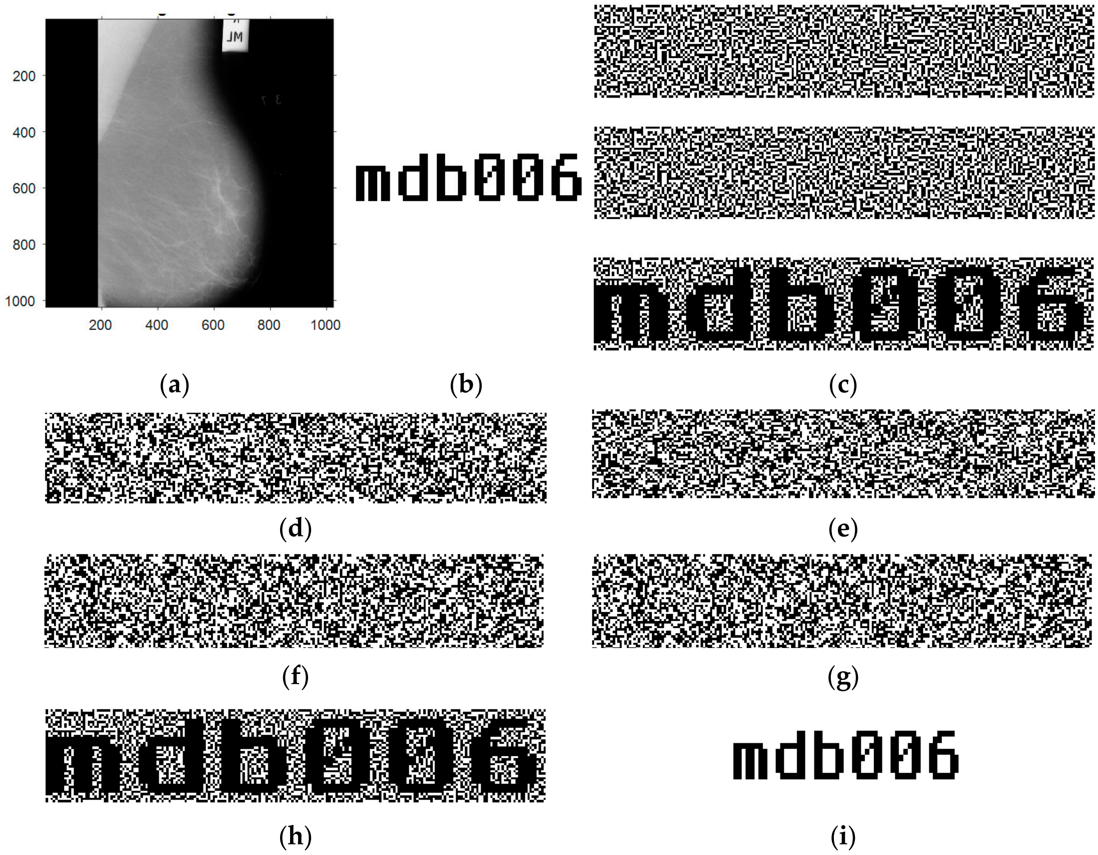


Figure 10. Identity insertion and retrieval for patient mdb006. (**a**) Original mammogram. (**b**) Patient's ID (I). (**c**) Secret shares S_1 and S_2 of I and revealing I after overlapping. (**d**) Embedded secret shares 1 (W_{S1}). (**e**) Embedded secret shares 2 (W_{S2}). (**f**) Retrieved secret share 1 (rS_1). (**g**) Retrieved secret share 2 (rS_2). (**h**) Retrieved identity rI after overlapping of rS_1 and rS_2. (**i**) Retrieved identity wI using step 4 of extraction process.

Figures 9 and 10 strengthen the fact that the identity could not be revealed once inserted using the proposed algorithm. In Figure 10, the embedded shares W_{S1} and W_{S2} could not reveal the identity without retrieving the shares rS_1 and rS_2, and then their overlapping would disclose the identity rI.

The identities of all patients in the mini-MIAS dataset were embedded using the same setting (offsets and initial conditions), and the computed performance measures are shown in Figure 11.

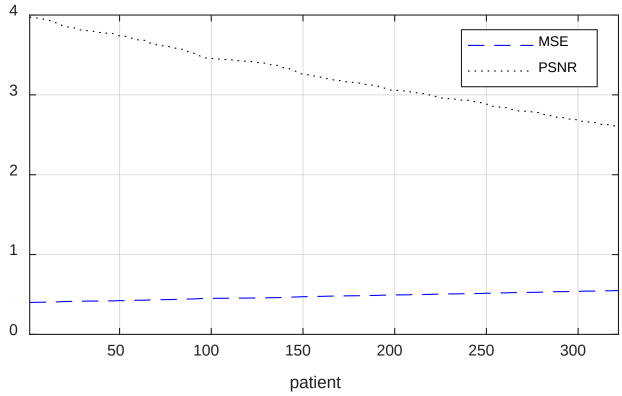


Figure 11. Performance measures *MSE* and *PSNR* when embedded shares are compared with the original shares for all mammograms of mini-MIAS.

Evidently, Figure 11 displays that the embedded shares were significantly different from the original shares for all patients. The *MSE* and *PSNR* exhibited the same behaviour for the CBIS-DDMIS dataset, with very high values for the *MSE* and low values for the *PSNR*.

The only method for disclosing I is to follow the extraction process of the proposed algorithm. Each health care staff member receives one of the secret keys, host mammogram, initial conditions and offsets. Using this transmitted information, each member can extract one of the secret shares rS_1 and rS_2. They will be absolutely the same as the original secret shares S_1 and S_2. Therefore, the *MSE* will be zero for the corresponding original and retrieved secret shares. Consequently, the identity of the patient will be revealed successfuly. Now, whether the proposed algorithm will affect the mammogram during the embedding and extraction processes will be observed.

4.2. Imperceptibility

One of the positive aspects of the proposed algorithm is keeping the host image in its original state. The algorithm does not introduce any change due to the insertion of a watermark because the patient's identity I is embedded into a secret key instead of the mammogram. Therefore, imperceptibility is naturally achieved, as no clue exists for the presence of a watermark in the host image.

Imperceptibility is one of the important phenomena in the evaluation of a watermark algorithm. In medical applications, this phenomenon becomes critical, as the degradation of a medical image may lead to false diagnosis. The privacy of patients is a prime concern but not at the cost of an accurate diagnosis.

Due to the use of the zero-watermarking approach in the proposed algorithm, the *MSE* values of the host mammograms before and after inserting I were zero. Ultimately, the achieved *PSNR* was large (i.e., infinity). All these measures—*MSE, PSNR* and *SSIM*—were optimal and concluded that the proposed algorithm did not affect the accuracy of the breast detection system. Hence, the proposed algorithm achieved the goal of protecting the patients' privacy without leading to a false diagnosis.

In the following section, we show the reliability of the proposed algorithm to make sure that identities cannot be disclosed using nonrelevant secret keys.

4.3. Detection Reliability of the Watermark

An authorised health care staff must possess the relevant transmitted secret keys to retrieve patient identities. However, what will happen if an unauthorised individual tries to reveal one identity with a nonrelevant secret key? The proposed algorithm was investigated to determine whether the identity of a patient could be retrieved using any nonrelevant secret key.

For this purpose, we first determined what would be a reasonable change in an initial condition such that the proposed algorithm should not disclose any identity using the condition of other. An attempt was made to retrieve an identity by altering the initial value from μ = 3.6 to 3.6005. The obtained the values of the *MSE, PSNR* and *SSIM* were 0.38, 4.24 and 0.06, respectively. The retrieved identity is depicted in Figure 12.

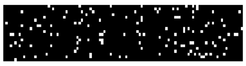


Figure 12. Retrieved identity when attempting to disclose with a nonrelevant secret key (false initial condition).

The computed measures indicate that the retrieved identity with the false initial condition was significantly different from the original identity. It concluded that the identity had no chance to be disclosed even with such a small variation in the initial condition. The difference between the corresponding values of sequences using μ = 3.6 and μ = 3.6005 was more than 75%. Moreover, the sequence generated with μ = 3.6 was compared with 200 other sequences (produced using different values of μ). The difference was always greater than 75%, as illustrated in Figure 13. That is tosay, the randomness using the logistic map was intractable when the initial conditions were unknown.

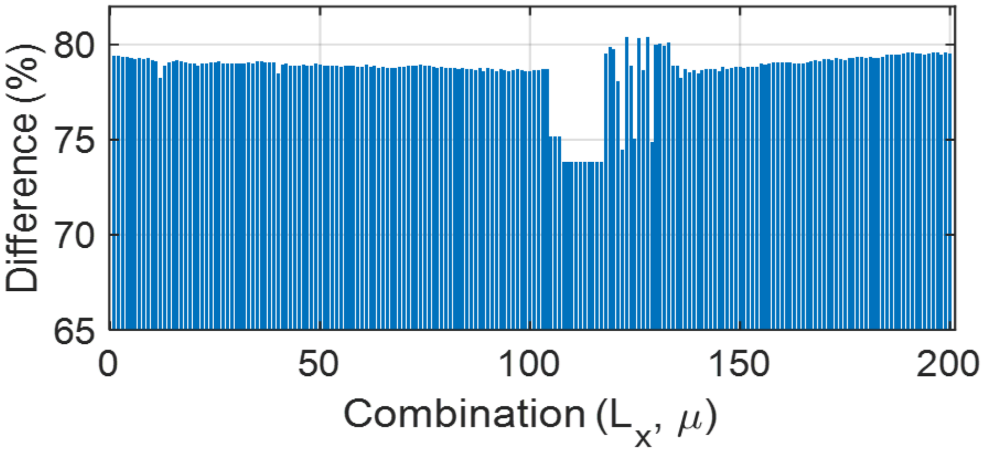
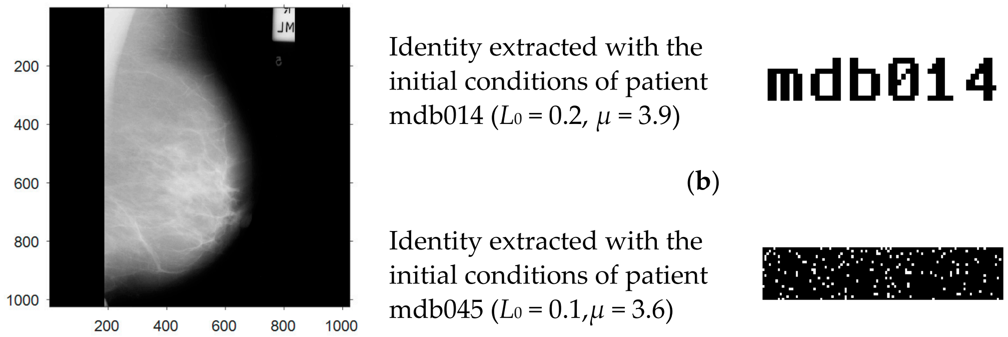


Figure 13. Comparison of 200 sequences generated using different values of μ with the sequence generated with μ = 3.6. For all sequences, L_0 was the same; that is, it was 0.1.

In addition, another illicit attempt was made to reveal the identity of patient mdb014 using the initial conditions (L_0, μ) of patient mdb045, as depicted in Figure 14. Two things were concluded. First, the identity of patient mdb014 was not disclosed, because the relevant information of the patient was not used. Secondly, the identity of any other patient was also not revealed as each patient had unique initial conditions, and it was impossible to retrieve the identity without them.



Identity extracted with the initial conditions of patient mdb014 (L_0 = 0.2, μ = 3.9)

(**b**)

Identity extracted with the initial conditions of patient mdb045 (L_0 = 0.1, μ = 3.6)

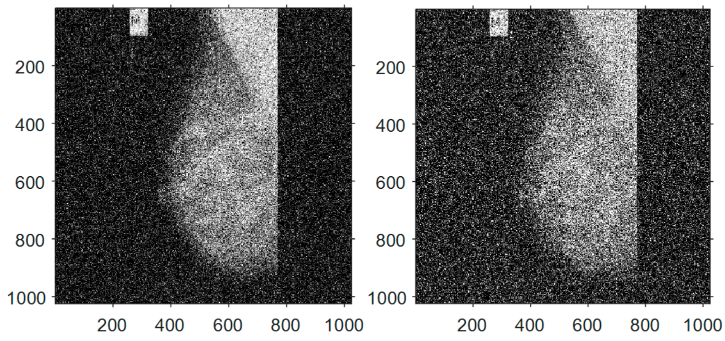
(**a**) (**c**)

Figure 14. Extraction of identity with relevant and nonrelevant information. (**a**) Original mammogram of patient mdb014. (**b**) Identity retrieved by using information of mdb014. (**c**) Identity retrieved by using information of patient mdb045.

The next point was if an unauthorised person attempted different combinations of μ and L_0 to guess the relevant secret keys and how many combinations of μ and L_0 were possible in the range from [3.6, 4] to [3.8284, 3.8510] and (0, 1), respectively. With the increment of 0.0005, the possible combinations of μ were 755, and those of L_0 were 1999. Hence, the total number of options would be more than 1.5×10^6. Furthermore, the offsets were random integers between 0 and 1000. As both offsets could be distinct, the overall number of significantly different random sequences would exceed 1.5×10^{12}. In addition, the number of nonuniform LBP codes was 198. That is to say, an unauthorised person attempted $198 \times 1.5 \times 10^{12}$ options to determine the relevant secret key. The experimental results show that the proposed algorithm was reliable for inserting and recovering patients' identities. Its robustness to authenticate data originality will be explored in the following section.

4.4. Data Authentication

For reliable detection of breast cancer using a CAD system, transmitted or stored mammograms must be authenticated. In the case of a malicious attack, a normal mammogram exhibits an irregular pattern and may behave similar to a malignant mammogram, as shown in Figure 15. The mammogram was attacked with Gaussian white noise. When such a mammogram was tested for breast cancer using the CNN-based detection system, the diagnosis was false. Therefore, the system accuracy decreased to 52% for both datasets.



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

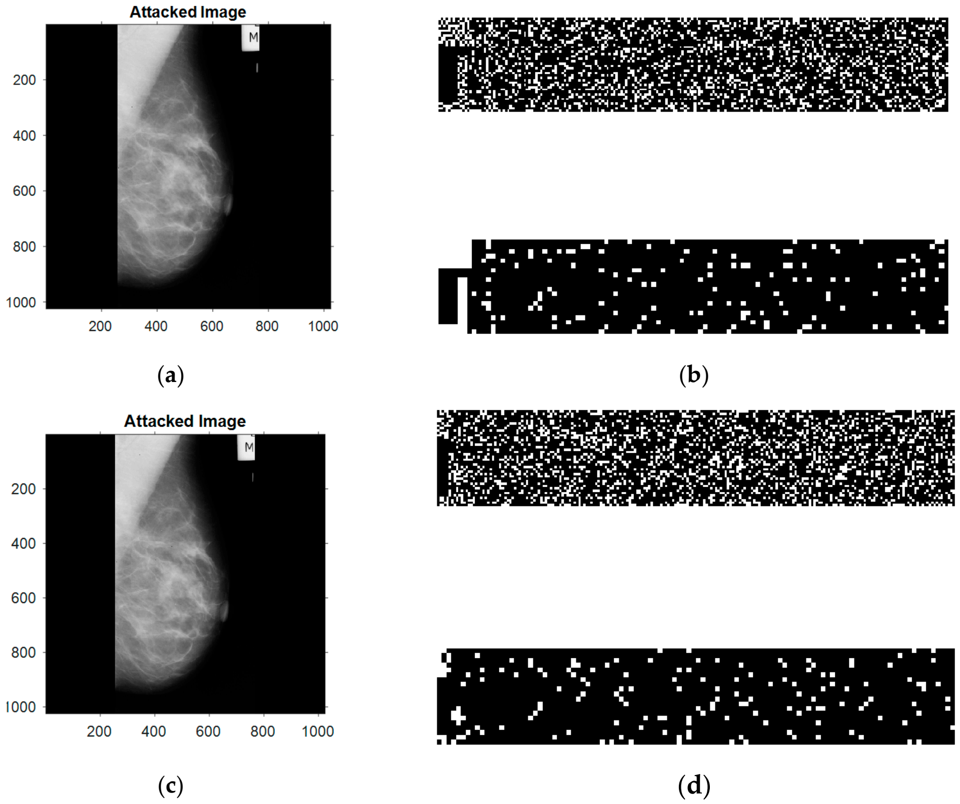
Figure 15. Mammogram attacked with Gaussian white noise of zero mean and variance of (**a**) 0.10 and (**b**) 0.02.

Due to the fragile nature of the proposed zero-watermarking algorithm, it had the ability to authenticate the contents of a mammogram. In the case of Gaussian white noise, the retrieved identity was distorted even when using relevant information. The malicious attack changed the characteristics of the mammogram, and as a result, the locations of the nonuniform LBP codes would be affected. Therefore, chaotic sequences Y and Z could not locate the required blocks of the nonuniform LBP codes. Hence, the retrieved identity was distorted, indicating that the mammogram was not genuine and was tampered with or attacked.

Although the proposed algorithm could detect the attack in the case of Gaussian noise, tampering in the mammogram was visible with the naked eye. Therefore, the question is if the attack is not visible, how will the proposed algorithm detect it? To answer such a question, the mammogram was attacked by altering some pixels in region 2. This region was approximately one fourth of the whole mammogram.

To avoid visibility, the pixels were altered in such a way that they should be replaced by a number having the same number of 1-to-0 and 0-to-1 transitions with a one-bit difference. For example, 148 was replaced by 150. Then, when the recipient would determine nonuniform codes after the attack, some uniform codes would become nonuniform, and vice versa. Therefore, the indices of the nonuniform LBP codes in NUP would be changed. In addition, if the type of the code was not changed, it might have been replaced by another code of the same type. Then, the intermediate patterns P_1 and P_2 would be distorted during the extraction process. Consequently, the disturbance in NUP, P_1 and P_2 would lead to retrieving the distorted identity, indicating that the mammogram is not in the original form and may lead to a false diagnosis.

It can be observed from Figure 16 that when a mammogram was attacked by altering 0.01% and 0.02% of its pixels, the tampering was not visible. However, the retrieved identities (rI and wI) in both cases were significantly distorted, which was also highlighted by the performance measures (high MSE and very low $PSNR$ and $SSIM$). Moreover, the increase in the values of the MSE and decrease in the $PSNR$ and $SSIM$ for the increasing number of attacked pixels shows that the retrieved identity became more distorted.



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

(**c**) (**d**)

Figure 16. *Cont.*

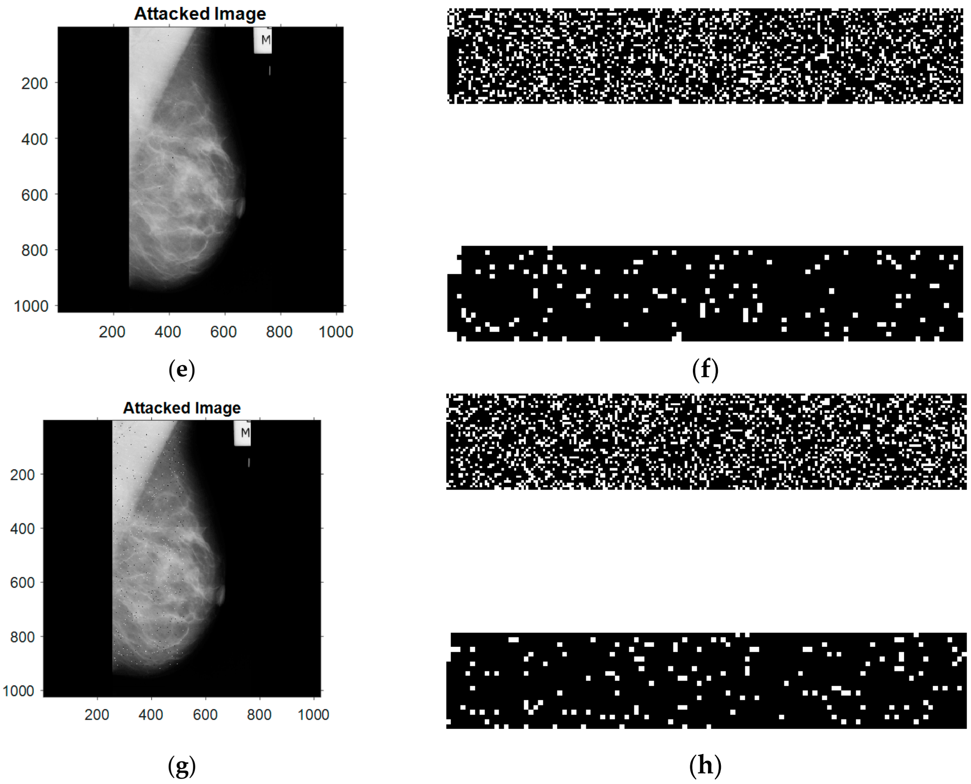


Figure 16. Malicious attack and retrieved identities. (**a**) Attack by altering 25 pixels (0.01%) of the mammogram. (**b**) Corresonging retrieved identity *rI* and *wI* (*MSE* = 0.33, *PSNR* = 4.81 and *SSIM* = 0.17). (**c**) Attack by altering 50 pixels (0.02%) of the mammogram. (**d**) Corresponding retrieved identity *rI* and *wI* (*MSE* = 0.34, *PSNR* = 4.75 and *SSIM* = 0.16). (**e**) Attack by altering 250 pixels (0.1%) of the mammogram. (**f**) Corresponding retrieved identity *rI* and *wI* (*MSE* = 0.36, *PSNR* = 4.40 and *SSIM* = 0.09). (**g**) Attack by altering 2524 pixels (1%) of the mammogram. (**h**) Corresponding retrieved identity *rI* and *wI* (*MSE* = 0.37, *PSNR* = 4.26 and *SSIM* = 0.07).

The accuracy of the CAD system should also be observed with the increasing number of attacked pixels. The baseline results of the CAD system did not change when 0.01% and 0.02% of the pixels of the mammograms were attacked. For 0.1% and 1% attacked pixels, the mammograms should not be used for diagnosis by the healthcare staff as tampering becomes visible. However, to observe the effect of tampering on the diagnosis, the experimental result for the mini-MIAS dataset is listed in Table 1.

Table 1. Classification of benign and malignant mammograms after malicious attack for mini-MIAS.

	Attacked Pixels	Sensitivity	Specificity	Accuracy
VGG16	0.01%, 0.02%	76.5%	68.2%	73.6%
	0.1%	58.8%	68.2%	62.0%
	1%	47.1%	68.2%	54.3%
ResNet50	0.01%, 0.02%	74.1%	61.4%	69.8%
	0.1%	56.5%	61.4%	58.1%
	1%	45.9%	61.4%	51.2%

The sensitivity decreased when the number of attacked pixels increased because the benign mammograms exhibited unusual changes which made them similar to malignant mammograms. Ultimately, the accuracy significantly dropped and was equal to 54.3% for 1% tampered pixels. A similar trend was found for the CBIS-DDMIS dataset, and the accuracy decreased to 52.5%.

Furthermore, another criterion was implemented to authenticate the mammogram, which is given by Equation (17). According to this criterion, a mammogram was in its original form if there was no difference in the frequency of the LBP codes in the histograms computed during the insertion and extraction processes:

$$\begin{aligned} &\text{original} = \begin{cases} \text{yes} & \text{if} \quad \mathit{check} = 0 \\ \text{no} & \text{if} \quad \mathit{check} > 0 \end{cases} \\ &\text{where} \\ &\mathit{check} = \sum_{i=0}^{255} |HM(i) - HX(i)| \end{aligned} \tag{17}$$

In Equation (17), *HM* and *HX* represent the histograms of the embedding and extracting processes, respectively, and *i* indicates the bin number. In case of a malicious attack, the change in pixels with respect to its neighbours will produce a new LBP code of the same type or a different type. In either case, the frequency of LBP codes will be changed in the histogram. The values of *check* for 0.01%, 0.02%, 0.1% and 1% attacked pixels were nonzero and equal to 112, 228, 520 and 5276, respectively.

This criterion, along with the retrieved identities, makes the proposed algorithm robust in the authentication of mammograms so that they can be used reliably for the detection of breast cancer. To highlight the performance and positive aspects of the proposed algorithm, it is compared with existing works.

4.5. Comparisons

The proposed algorithm was compared with existing fragile zero-watermarking methods. To the best of our knowledge, only the following four kinds of fragile zero-watermarking schemes are available in the literature. In [38], fragile zero watermarking for images was proposed with all the important steps, including image encryption, watermark embedding, watermark extraction and image decryption. However, the algorithm neither discusses the randomness nor investigates the chances to extract the watermark with non-relevant secret keys. In another study [39], a fragile zero-watermarking scheme is presented to detect malicious modifications in database relationships, but this scheme cannot be used for images. Moreover, watermark encryption and decryption are not performed in this scheme. Similarly, in [40], lightweight elliptic curve cryptography using fragile zero watermarking is implemented to authenticate the users of the Internet of Things. This approach is also not viable for images. Likewise, a semi-fragile zero-watermarking approach is proposed in [41] for audio. In comparison with these schemes, the proposed algorithm encrypts patients' identities and embeds their encrypted shares by using fragile zero watermarking reliably, because chaotic randomness prevents unauthorised access to patients' identities. Furthermore, identity extraction and decryption only need the initial conditions of the chaotic system to regenerate the random sequence. Transmitting the complete random sequence to the staff is no longer necessary, which is another positive aspect of the proposed algorithm.

5. Conclusions

The proposed fragile zero-watermarking algorithm offers a reliable solution for the protection of patients' data privacy and integrity. The algorithm provides dual protection, as it uses visual cryptography (for identity encryption and decryption) and watermarking (for the insertion and extraction of encrypted identities). Due to the implementation of the chaotic system in the algorithm, the deterministic randomness in the generation of watermark keys eliminated any chance of revealing identities by an unauthorised person. Using this algorithm, patients' information can be transmitted reliably from a remote health facility to a specialised health centre via wireless communication. The fragile watermarking will alert the recipient health care staff in case of tampering or a malicious attack, as the integrity of medical images is of immense importance for accurate diagnoses of diseases. The CNN-based breast cancer detection system confirms that an image affected by Gaussian noise attack leads to a false diagnosis. The proposed algorithm avoids such situations. In addition, the results of the detection system are unchanged before and after watermark insertion, as the proposed algorithm does not change the characteristics of the host medical image. Furthermore, the proposed algorithm resolved the problem of capacity. It uses only 2% of the space (LBP codes) for watermark insertion, which means that the size of the watermark is not an issue, and patients' other particulars can also be protected when needed. In future works, the proposed solution will be extended to localise the tampered regions of medical images in case of an attack.

Author Contributions: Conceptualisation, Z.A., F.-e.-A. and M.H.; methodology, Z.A.; formal analysis, Z.A., F.-e.-A. and M.H.; writing—original draft preparation, Z.A.; project administration, F.-e.-A. and M.H. All authors have read and agreed to the published version of the manuscript.

Funding: This project was funded by the National Plan for Science, Technology and Innovation (MAARIFAH) of King Abdulaziz City for Science and Technology in the Kingdom of Saudi Arabia, Grant No. 5-18-03-001-0007.

Data Availability Statement: Two publicly available datasets were used in this study. CBIS-DDSM is available at https://wiki.cancerimagingarchive.net/display/Public/CBIS-DDSM (accessed on 15 September 2021), and mini-MIAS can be downloaded from https://www.repository.cam.ac.uk/handle/1810/250394 (accessed on 25 September 2021). To obtain the baseline results in this study for the classification of mammograms, the implementation of a CNN in [2] was used and obtained from https://github.com/lishen/end2end-all-conv (accessed on 10 October 2021).

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

References

1. Liaqat, S.; Raja, G. Computer-Aided Detection of COVID-19 Using Chest Imaging. In Proceedings of the 11th International Conference of Pattern Recognition Systems (ICPRS 2021), Online, 17–19 March 2021.
2. Shen, L.; Margolies, L.R.; Rothstein, J.H.; Fluder, E.; McBride, R.; Sieh, W. Deep Learning to Improve Breast Cancer Detection on Screening Mammography. *Sci. Rep.* **2019**, *9*, 1–12. [CrossRef] [PubMed]
3. Luo, Z.; Li, J.; Zhu, Y. A Deep Feature Fusion Network Based on Multiple Attention Mechanisms for Joint Iris-Periocular Biometric Recognition. *IEEE Signal Process. Lett.* **2021**, *28*, 1060–1064. [CrossRef]
4. Moolla, Y.; De Kock, A.; Mabuza-Hocquet, G.; Ntshangase, C.S.; Nelufule, N.; Khanyile, P. Biometric Recognition of Infants using Fingerprint, Iris, and Ear Biometrics. *IEEE Access* **2021**, *9*, 38269–38286. [CrossRef]
5. Ali, Z.; Imran, M.; Alsulaiman, M.; Shoaib, M.; Ullah, S. Chaos-based robust method of zero-watermarking for medical signals. *Futur. Gener. Comput. Syst.* **2018**, *88*, 400–412. [CrossRef]
6. Ali, Z.; Imran, M.; McClean, S.; Khan, N.; Shoaib, M. Protection of records and data authentication based on secret shares and watermarking. *Futur. Gener. Comput. Syst.* **2019**, *98*, 331–341. [CrossRef]
7. Ali, Z.; Hossain, M.S.; Muhammad, G.; Aslam, M. New Zero-Watermarking Algorithm Using Hurst Exponent for Protection of Privacy in Telemedicine. *IEEE Access* **2018**, *6*, 7930–7940. [CrossRef]
8. Mukherjee, M.; Matam, R.; Shu, L.; Maglaras, L.; Ferrag, M.A.; Choudhury, N.; Kumar, V. Security and Privacy in Fog Computing: Challenges. *IEEE Access* **2017**, *5*, 19293–19304. [CrossRef]
9. Hsu, C.-L.; Lee, M.-R.; Su, C.-H. The Role of Privacy Protection in Healthcare Information Systems Adoption. *J. Med. Syst.* **2013**, *37*, 1–12. [CrossRef]
10. Gong, T.; Huang, H.; Li, P.; Zhang, K.; Jiang, H. A Medical Healthcare System for Privacy Protection Based on IoT. In Proceedings of the 2015 Seventh International Symposium on Parallel Architectures, Algorithms and Programming (PAAP), Nanjing, China, 12–14 December 2015.
11. Hayajneh, T.; Mohd, B.J.; Imran, M.; Almashaqbeh, G.; Vasilakos, A.V. Secure Authentication for Remote Patient Monitoring with Wireless Medical Sensor Networks. *Sensors* **2016**, *16*, 424. [CrossRef]
12. Eswaraiah, R.; Reddy, E.S. Robust medical image watermarking technique for accurate detection of tampers inside region of interest and recovering original region of interest. *IET Image Process.* **2015**, *9*, 615–625. [CrossRef]
13. Singh, A.; Dutta, M.K.; Prinosil, J.; Riha, K. Wavelet based robust watermarking scheme for copyright enforcement and integrity control in tele-ophthalmology. In Proceedings of the 2016 8th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Lisbon, Portugal, 18–20 October 2016.
14. Walia, E.; Suneja, A. Fragile and blind watermarking technique based on Weber's law for medical image authentication. *IET Comput. Vis.* **2013**, *7*, 9–19. [CrossRef]
15. Viswanathan, P.; Krishna, P.V. A Joint FED Watermarking System Using Spatial Fusion for Verifying the Security Issues of Teleradiology. *IEEE J. Biomed. Health Inform.* **2014**, *18*, 753–764. [CrossRef] [PubMed]

16. Dutta, M.K.; Singh, A.; Singh, A.; Burget, R.; Prinosil, J. Digital identification tags for medical fundus images for tele-ophthalmology applications. In Proceedings of the 2015 38th International Conference on Telecommunications and Signal Processing (TSP), Prague, Czech Republic, 9–11 July 2015; pp. 781–784. [CrossRef]
17. Hadar, O.; Gonen, E.; Kaminsky, E. Rate distortion optimization for efficient watermarking in the DCT domain. In Proceedings of the 2008 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting, Las Vegas, NV, USA, 31 March–2 April 2008.
18. Siau-Chuin, L.; Zain, J.M. Reversible medical image watermarking for tamper detection and recovery. In Proceedings of the 2010 3rd International Conference on Computer Science and Information Technology, Chengdu, China, 9–11 July 2010.
19. Dragoi, I.-C.; Coltuc, D. Adaptive Pairing Reversible Watermarking. *IEEE Trans. Image Process.* **2016**, *25*, 2420–2422. [CrossRef] [PubMed]
20. Abhilasha, S.; Malay Kishore, D. A Reversible Data Hiding Scheme for Efficient Management of Tele-Ophthalmological Data. *Int. J. E-Health Med. Commun. IJEHMC* **2017**, *8*, 38–54.
21. Pakdaman, Z.; Saryazdi, S.; Nezamabadi-Pour, H. A prediction based reversible image watermarking in Hadamard domain. *Multimed. Tools Appl.* **2016**, *76*, 8517–8545. [CrossRef]
22. Zhang, L.; Cai, P.; Tian, X.; Xia, S. A novel zero-watermarking algorithm based on DWT and edge detection. In Proceedings of the 2011 4th International Congress on Image and Signal Processing, Shanghai, China, 15–17 October 2011. [CrossRef]
23. Bilal, M.; Imtiaz, S.; Abdul, W.; Ghouzali, S.; Asif, S. Chaos based Zero-steganography algorithm. *Multimed. Tools Appl.* **2013**, *72*, 1073–1092. [CrossRef]
24. Rani, A.; Bhullar, A.K.; Dangwal, D.; Kumar, S. A Zero-Watermarking Scheme using Discrete Wavelet Transform. *Procedia Comput. Sci.* **2015**, *70*, 603–609. [CrossRef]
25. Abdul, W.; Ali, Z.; Ghouzali, S.; Alsulaiman, M. Security and Privacy for Medical Images Using Chaotic Visual Cryptography. *J. Med. Imaging Health Inform.* **2017**, *7*, 1296–1301. [CrossRef]
26. Ali, Z.; Imran, M.; Alsulaiman, M.; Zia, T.; Shoaib, M. A zero-watermarking algorithm for privacy protection in biomedical signals. *Future Gener. Comput. Syst.* **2018**, *82*, 290–303. [CrossRef]
27. Arnold, M.; Schmucker, M.; Wolthusen, S.D. *Techniques and Applications of Digital Watermarking and Content Protection*; Artech House: Houston, TX, USA, 2003; p. 21.
28. Yang, B.; Guo, H.; Cao, E. Chapter Two—Design of cyber-physical-social systems with forensic-awareness based on deep learning. In *Advances in Computers*; Hurson, A.R., Wu, S., Eds.; Elsevier: Amsterdam, The Netherlands, 2021; pp. 39–79.
29. Fragoso-Navarro, E.; Cedillo-Hernandez, M.; Nakano-Miyatake, M.; Cedillo-Hernandez, A.; Perez-Meana, H.M. Visible Watermarking Assessment Metrics Based on Just Noticeable Distortion. *IEEE Access* **2018**, *6*, 75767–75788. [CrossRef]
30. Ulutas, G.; Ustubioglu, A.; Ustubioglu, B.; Nabiyev, V.V.; Ulutas, M. Medical Image Tamper Detection Based on Passive Image Authentication. *J. Digit. Imaging* **2017**, *30*, 695–709. [CrossRef] [PubMed]
31. Heath, M.; Bowyer, K.; Kopans, D.; Moore, R. The Digital Database for Screening Mammography. In *Proceedings of the Fifth International Workshop on Digital Mammography, Toronto, ON, Canada, 11–14 June 2000*; Medical Physics Publishing: Madison, WI, USA, 2001.
32. Suckling, J.; Dance, D.; Astley, S.; Hutt, I.; Boggis, C.; Ricketts, I.; Stamatakis, E.; Cerneaz, N.; Kok, S.; Taylor, P.; et al. *Mammographic Image Analysis Society (MIAS) Database v1.21*; University of Cambridge: Cambridge, UK, 2015.
33. Nixon, M.S.; Aguado, A.S. Chapter 4—Low-level feature extraction (including edge detection). In *Feature Extraction & Image Processing for Computer Vision*, 3rd ed.; Nixon, M.S., Aguado, A.S., Eds.; Academic Press: Oxford, UK, 2012; pp. 137–216.
34. Misra, S.; Wu, Y. Chapter 10—Machine learning assisted segmentation of scanning electron microscopy images of organic-rich shales with feature extraction and feature ranking. In *Machine Learning for Subsurface Characterization*; Misra, S., Li, H., He, J., Eds.; Gulf Professional Publishing: Houston, TX, USA, 2020; pp. 289–314.
35. Ojala, T.; Pietikainen, M.; Maenpaa, T. Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. *IEEE Trans. Pattern Anal. Mach. Intell.* **2002**, *24*, 971–987. [CrossRef]
36. Mayoral, E.; Robledo, A. A Recent Appreciation of the Singular Dynamics at the Edge of Chaos. In *The Logistic Map and the Route to Chaos*; Springer: Berlin/Heidelberg, Germany, 2006; pp. 339–354. [CrossRef]
37. Lee, R.S.; Gimenez, F.; Hoogi, A.; Miyake, K.K.; Gorovoy, M.; Rubin, D. A curated mammography data set for use in computer-aided detection and diagnosis research. *Sci. Data* **2017**, *4*, 170177. [CrossRef] [PubMed]
38. Li, M.; Xiao, D.; Zhu, Y.; Zhang, Y.; Sun, L. Commutative fragile zero-watermarking and encryption for image integrity protection. *Multimed. Tools Appl.* **2019**, *78*, 22727–22742. [CrossRef]
39. Khan, A.; Husain, S.A. A Fragile Zero Watermarking Scheme to Detect and Characterize Malicious Modifications in Database Relations. *Sci. World J.* **2013**, *2013*, 1–16. [CrossRef]
40. Sarwar, K.; Yongchareon, S.; Yu, J. Lightweight ECC with Fragile Zero-Watermarking for Internet of Things Security. In Proceedings of the 2018 17th IEEE International Conference On Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018.
41. Tang, X.; Ma, Z.; Niu, X.; Yang, Y. Compressive Sensing-Based Audio Semi-fragile Zero-Watermarking Algorithm. *Chin. J. Electron.* **2015**, *24*, 492–497. [CrossRef]