electronics

MDPI

Article

WMNet: A Lossless Watermarking Technique Using Deep Learning for Medical Image Authentication

Yueh-Peng Chen [1], Tzuo-Yau Fan [1] and Her-Chang Chao [2,*]

[1] Center for Artificial Intelligence in Medicine, Chang Gung Memorial Hospital, Linkou, Taoyuan 33305, Taiwan; yuepengc@gmail.com (Y.-P.C.); yaufan0625@gmail.com (T.-Y.F.)
[2] Department of Computer Science and Information Engineering, Ming Chuan University, Guei-Shan, Taoyuan 33348, Taiwan
* Correspondence: herchang@mail.mcu.edu.tw

Abstract: Traditional watermarking techniques extract the watermark from a suspected image, allowing the copyright information regarding the image owner to be identified by the naked eye or by similarity estimation methods such as bit error rate and normalized correlation. However, this process should be more objective. In this paper, we implemented a model based on deep learning technology that can accurately identify the watermark copyright, known as WMNet. In the past, when establishing deep learning models, a large amount of training data needed to be collected. While constructing WMNet, we implemented a simulated process to generate a large number of distorted watermarks, and then collected them to form a training dataset. However, not all watermarks in the training dataset could properly provide copyright information. Therefore, according to the set restrictions, we divided the watermarks in the training dataset into two categories; consequently, WMNet could learn and identify the copyright information that the watermarks contained, so as to assist in the copyright verification process. Even if the retrieved watermark information was incomplete, the copyright information it contained could still be interpreted objectively and accurately. The results show that the method proposed by this study is relatively effective.

Keywords: convolutional neural network; deep learning; watermarking technique

Citation: Chen, Y.-P.; Fan, T.-Y.; Chao, H.-C. WMNet: A Lossless Watermarking Technique Using Deep Learning for Medical Image Authentication. *Electronics* **2021**, *10*, 932. https://doi.org/10.3390/electronics10080932

Academic Editor: Byung-Gyu Kim

Received: 9 March 2021
Accepted: 12 April 2021
Published: 14 April 2021

1. Introduction

Hospitals and medical research centers are currently moving toward a digitalized diagnosis and treatment environment. These environmental changes have made the security of the usage, management, and transmission of digital medical images extremely important. In response, the standard format Digital Imaging and Communications in Medicine (DICOM) was created as a storage standard for medical images based on the Transmission Control Protocol/Internet Protocol as a foundation for communication to ensure a consistent format for storing, processing, printing, and transmitting medical images and data between facilities. Using the DICOM standard, medical devices from different manufacturers within a network can be used to transmit and use medical images. This enables patients, physicians, and medical research units to share relevant medical images through internet image servers to conduct real-time, convenient disease diagnosis, treatment, and research. However, it cannot be ignored that in such a convenient environment, stored data may be susceptible to attacks, tampering, or misplacement during transmission or storage for diagnosis and treatment. This consideration is especially important in the application of telemedicine [1–3]. Therefore, the problem of ensuring the security and copyright of data when they are disseminated in open channels must be addressed.

Cryptography, steganography, watermarking, and other techniques have been developed to provide different solutions to ensure the security and protection of digital medical image content [4–13]. Rahimi and Rabbani [7] presented a regional watermarking algorithm for DICOM images. Their work illustrates that it is advantageous to apply current

picture archiving and communication systems to digitalize the storage and transmission of medical images. However, it is necessary to address the privacy and security of these medical images. Cedillo-Hernandez et al. [8] proposed a discrete Fourier transform-based watermarking mechanism that allows effective management of medical images. This method encrypts the electronic patient record (EPR) with a secret key and embeds it into the medical image as a watermark. Not only can this method verify the copyright of the protected image, but it can also manage the image based on the embedded EPR data. Parah et al. [9] hid the EPR data of patients in medical images to ensure the security of the data in the electronic healthcare system. Singh et al. [10] proposed a multiple-watermark method for medical images based on discrete wavelet transform (DWT). This method is designed to place the highest priority on the safety of the EPR data.

However, most medical watermarking systems embed watermarks that represent medical image ownership into medical images through algorithms. This causes the quality of the watermark-embedded image and the original image to differ, and as medical images contain many fine features, traditional watermarking methods may tamper with crucial data inside the images. Even small changes may distort fine characteristics and affect the decision-making of medical staff, resulting in unnecessary disputes. For example, a watermark-embedded image produces an inexplicable afterimage because of the embedding of watermark information. Medical staff cannot identify this afterimage as a symptom of the distortion caused by watermark embedding. This leads to confusion among the medical staff and influences their judgments. Therefore, some researchers have focused on developing lossless medical watermarking techniques [14–24]. The key to lossless medical watermarking techniques is the extraction of appropriate features from images. These image features and watermarks are used to generate a verification image that can be used to validate the image. This image is referred to as the ownership share image (OSI). For image verification, image features are extracted in the same way and this feature can be created the master share image (MSI). Finally, the previous OSI and MSI can be used to recover the watermark. Thus, the image is not destroyed.

In addition, a watermarking system generally involves a watermark embedding procedure and a watermark extraction procedure. During watermark embedding, a watermark representing image ownership is embedded by an algorithm into the image to be protected. During watermark extraction, the algorithm is used to extract the watermark from suspected images to authenticate those images. However, conventional measurement systems for watermarks use human vision to identify the information contained within the extracted watermark or use similarity estimation methods, such as bit error rate (BER) or normalized correlation (NC), to confirm that the system can retrieve the watermark. This process is not completely objective. For example, if an extracted watermark has already been distorted and the original content cannot be discerned from the overall appearance, the watermark will still be considered valid if the calculated BER or NC is high.

In this paper, a deep learning model for detecting distortion watermarks, called WMNet, is proposed. WMNet is designed based on the convolutional neural network (CNN) architecture [25]. In recent years, the most popular network architecture for deep learning for images is the CNN and shows very good performance in the application of deep learning [26,27]. When beginning the WMNet construction phase, the watermark that the user intends to use for medical image registration is used in simulated attacks to generate a large number of simulated distorted watermarks, and a detection threshold is set. These watermarks are divided into two categories, namely "Correct" and "Incorrect." Finally, a convolutional neural network is used to generate WMNet for subsequent detection of the watermark ownership. Thus, the image owner can be identified by a more objective method.

The remainder of this paper is organized as follows. Section 2 briefly reviews a lossless watermarking scheme. Section 3 describes the proposed scheme. Section 4 discusses validation of the effectiveness through simulation experiments, and Section 5 concludes the paper.

2. Lossless Watermarking Scheme

Traditionally, when designing a watermarking mechanism to be applied to multimedia, it is expected to meet the characteristics of security, invisibility, robustness, and capacity of an effective watermarking mechanism. However, this is usually a trade-off problem, and several scholars have devoted themselves to identifying the best solution. Shoron et al. [28] proposed a copyright protection mechanism based on DWT and successive mean quantization transform successive mean quantization transform for medical images. Although this scheme achieved satisfactory experiment results, the approaches of malicious attacks that can be resisted do not include most image processing methods. Din et al. [29] explored the security protection of electronic health records adopting different biometrics in the arena of the internet of medical things, which effectively improved the watermark information embedding of algorithms. To develop a better watermarking mechanism, scholars subsequently put forward the lossless watermarking scheme [14–24]. The major key point in the design of a lossless watermarking scheme lies in the extraction of image features. As long as the quality of the protected image is not compromised, this scheme is ideal for protecting sensitive images, such as military and medical images. The flow chart of the generalized lossless watermarking scheme is shown in Figure 1. Image features are extracted from the host image through image capture technology (such as discrete cosine transform and DWT), and then an OSI is generated, which is submitted to a third party for registration. When the ownership of a suspected image needs to be verified, the image is extracted by the same image capture technology, and after the features are extracted, the MSI is generated. Finally, the OSI and MSI are calculated to obtain the watermark and the copyright is confirmed.

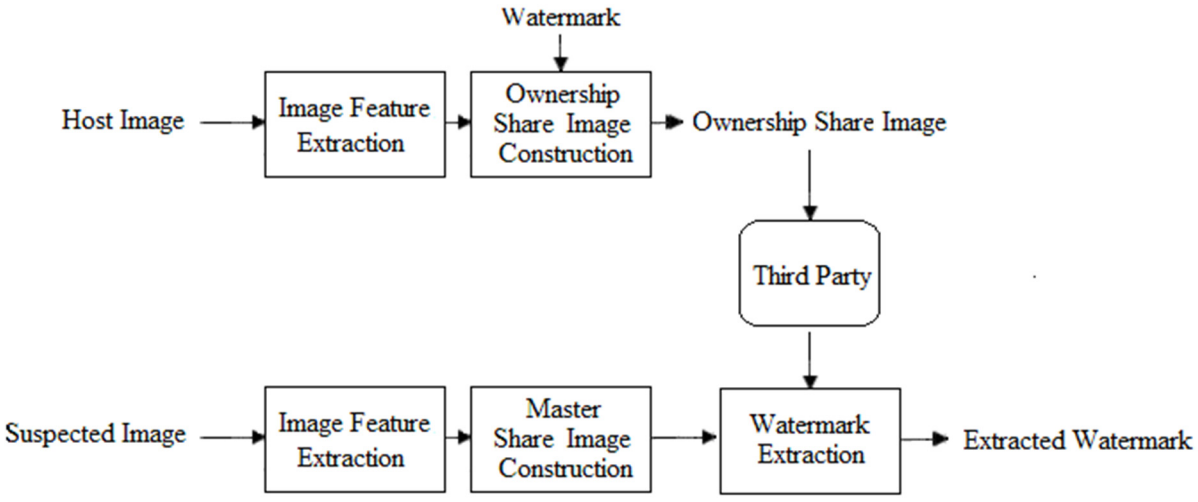


Figure 1. Flow chart of generalized lossless watermarking scheme.

Mechanisms of this type have several notable characteristics. First, the image features extracted from the image are combined with the watermark to generate the OSI and MSI, and the OSI and MSI can be combined with an encryption algorithm to improve the security of the watermarking mechanism. For example, the generated OSI and MSI can be combined with visual cryptography [30] or visual secret sharing [31]. Second, the watermark used by this type of mechanism is not limited by the size of the protected image. In conventional watermarking mechanisms, the size of the watermark used to verify the image is usually clearly defined, which limits the number of watermarks that can be embedded in the image. However, the size of the watermark is independent of the host image in a lossless watermarking scheme. For the mechanism proposed by Wang et al. [14], watermarks of different sizes used in the experiment did not affect the quality of the protected images. Moreover, building on this idea, Fan et al. [15] encoded the watermark

using error correction codes and then generated the OSI and MSI with the image features. Although the damage resistance of the watermark is improved, the size of the resulting OSI is much larger than that of the original watermark. This requires additional processing time to validate the image, which is not suitable for real-time systems.

In addition, lossless watermarking scheme performance depends on the method used to extract the image features, such as using different frequency domains. Lou et al. [16] used DWT to extract low-frequency features of different resolution levels in the image and, thereby, generate the OSI and MSI for image verification. Wang et al. [17] divided an image into non-overlapping blocks and conducted DCT conversion to obtain the low-frequency features of each block as the basis for generating the OSI and MSI. This concept can effectively resist common image compression attacks. Wu et al. [18] adopted a mixed-domain approach, which makes the mechanism resistant to damage from different types of attacks. In addition to using different frequency domain techniques, Thanh et al. [19] and Fan et al. [20] also believed that important features of images should be extracted from scattered locations to better resist clipping or tampering attacks in an area of an image.

The above studies demonstrate that a good watermarking mechanism should satisfy security, invisibility, and robustness requirements. These characteristics can be satisfied using a lossless watermarking scheme. Robust watermarking mechanisms have higher NC and BER values; thus, during validation, the NC or BER is typically calculated after the watermark extraction to determine whether the image belongs to the corresponding copyright. However, although this is reasonable, it is not entirely objective, and it does not allow for the timely interpretation of highly distorted watermarks. Therefore, this paper presents a WMNet detection model with a lossless watermarking scheme. This model does not require a person to interpret image ownership. It can verify and determine directly whether the copyright of the watermark obtained from an image is correct.

3. Proposed Method

In the previous section, we introduced a lossless watermarking system that can be used to extract the watermark from the suspected medical image during authentication, which then allows the information in the watermark to be used to authenticate image ownership. However, if the extracted watermark is severely distorted, the interpretation of information from that watermark becomes extremely subjective. Therefore, WMNet was designed to determine objectively whether the information in the watermark can be used to prove ownership of the image after watermark extraction. In this study, a model for copyright verification based on CNN, known as WMNet, was designed. Generally, to build a CNN model, a large number of training datasets needs to be prepared. The proposed method involved the generation of several distorted watermark images by simulation, but not all distorted watermarks can provide copyright information reasonably. These watermarks were divided into two categories, namely "Correct" and "Incorrect", based on the set restrictions so that they can generate WMNet to distinguish users' copyrights. Finally, WMNet was designed to determine objectively whether the information in the watermark can be used to prove the ownership of the image after watermark extraction. The WMNet flow chart is shown in Figure 2, and the detailed steps are discussed below.

With regard to a binary watermark W of size $m_1 \times m_2$ that is prepared by the user for registration, a simulated W, distorted dataset α needs to be constructed before constructing a WMNet that is specific to W. Therefore, the function $\Psi(W,i)^\tau$ is defined, where $1 \leq i \leq m_1 \times m_2$. The role of $\Psi(W,i)^\tau$ is to generate τ copies of distorted watermarks $\widetilde{W}^\tau$ that are of size W, with the ith pixel values randomly chosen from each $\widetilde{W}^\tau$ using the NOT Boolean operation so that i random pixels in $\widetilde{W}^\tau$ are the opposite of W. Next, to simulate the actual situation, α is $\{\Psi(W,1)^\tau, \Psi(W,2)^\tau, \cdots, \Psi(W,z)^\tau\}$, where $z = 1, 2, \cdots, (m_1 \times m_2) \times 0.7$. After the processing described above, α has $\tau \times (m_1 \times m_2) \times 0.7$ distorted watermarks. For example, if W is a watermark of size 64×64 with τ set to 5, α will have 14,336 distorted watermarks.

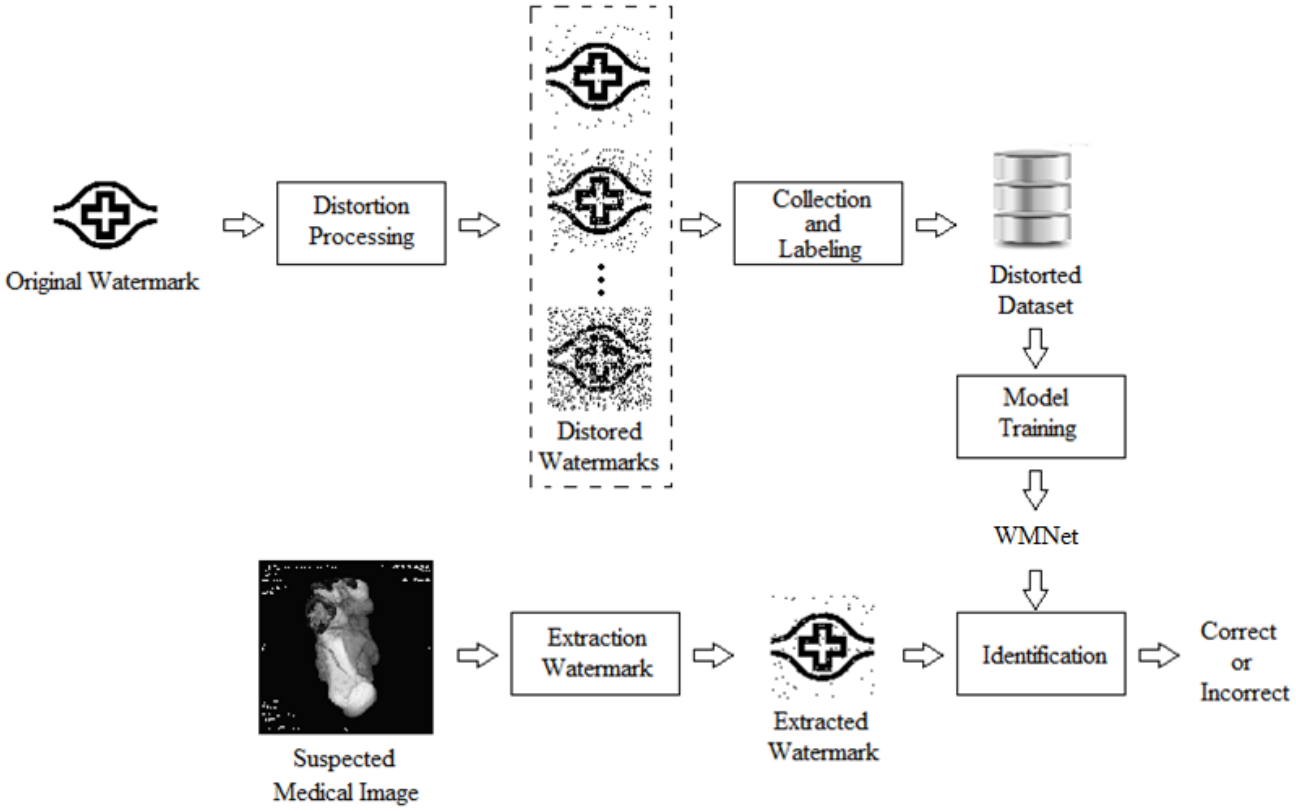
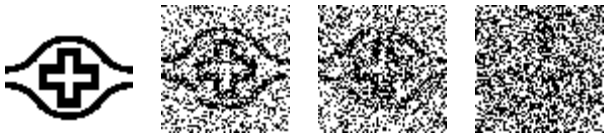


Figure 2. WMNet flow chart.

After generating α, the distorted watermarks are categorized as "Correct" and "Incorrect." NC is used to assess the similarities between these distorted watermarks and the original watermark. For example, Figure 3 presents the results of different NC values. Figure 3a is the original image. Figure 3b–d are distorted watermarks with the corresponding NC values being 0.87, 0.77, and 0.67. It can be seen that different NC values correspond to different degrees of similarity between the distorted and original watermarks. The threshold value T_c is defined to provide training categories to WMNet. If the NC value of the distorted watermark is greater than the threshold value T_c, it is categorized as "Correct". Otherwise, it is categorized as "Incorrect".



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

Figure 3. Distorted watermark images with different normalized correlation (NC) values. (**a**) Original image, (**b**) distorted watermark 1 (NC = 0.87), (**c**) distorted watermark 2 (NC = 0.77), and (**d**) distorted watermark 3 (NC = 0.67).

After the simulated distorted dataset is generated, it can be segmented into the training, validation, and testing datasets. The WMNet framework shown in Table 1 is used for the design. WMNet is based on the design of CNN. Table 1 shows the type, input size, filter size, and output size for each layer. The padding and stride of each layer, which are not listed in the table, were set as "same" and 2, respectively. In addition, the learning rate was set as 0.0005, batch size as 40, and epoch as 50, and the filter numbers of the two convolution layers were set as 16 and 32, respectively. Finally, after the WMNet is complete,

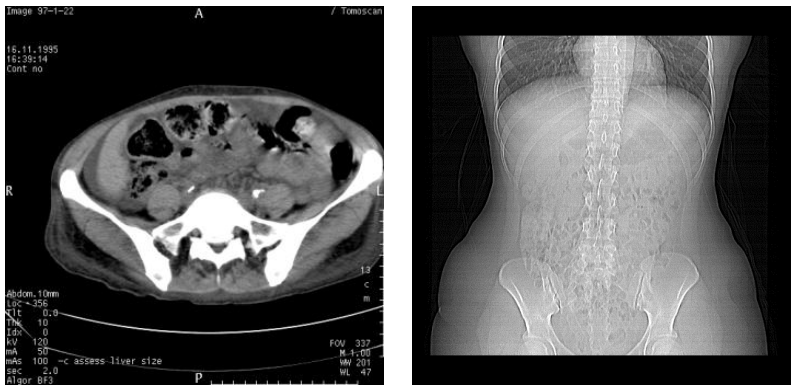
the watermark can be extracted from the suspected medical image for testing to obtain the copyright.

Table 1. WMNet parameters.

Layer	Type	Input	Filter Size	Output
1	Convolution	$64 \times 64 \times 1$	3×3	$32 \times 32 \times 16$
2	Max pooling	$32 \times 32 \times 16$	3×3	$16 \times 16 \times 32$
3	Convolution	$16 \times 16 \times 32$	3×3	$8 \times 8 \times 32$
4	Max pooling	$8 \times 8 \times 32$	3×3	$4 \times 4 \times 32$
5	Fully connected	$4 \times 4 \times 32$	3×3	1×2
6	Softmax	1×2	-	Result

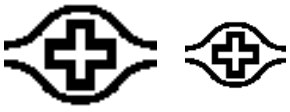
4. Experimental Results

In this section, we show the actual simulation results of WMNet in the ownership authentication verification phase. Figure 4 shows the medical images used in the simulation, which are of size 512×512 pixels. The medical images are computed tomography (CT) and X-ray images. Figure 5 shows the watermarks used in the simulation, which are binary images of sizes 64×64 and 32×32, respectively. Figure 6 shows the simulated result using Fan's lossless watermarking system [15] with no imaging processing damage done to the medical images by the proposed system. Figure 6a,b show the 128×128 OSI and MSI generated from the 128×128 CT image, and Figure 6c shows the extracted watermarks. Figure 6d,e show the 128×128 OSI and MSI generated from the X-ray image, and Figure 6f shows the extracted watermarks. From the simulation results, we can see that the lossless watermarking system can correctly retrieve the watermark if the image has not been attacked by image-processing methods.



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

Figure 4. Medical images used in the experiment. (**a**) Computed tomography (CT) and (**b**) X-ray.



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

Figure 5. Watermark images used in the experiment: (**a**) 64×64 and (**b**) 32×32.

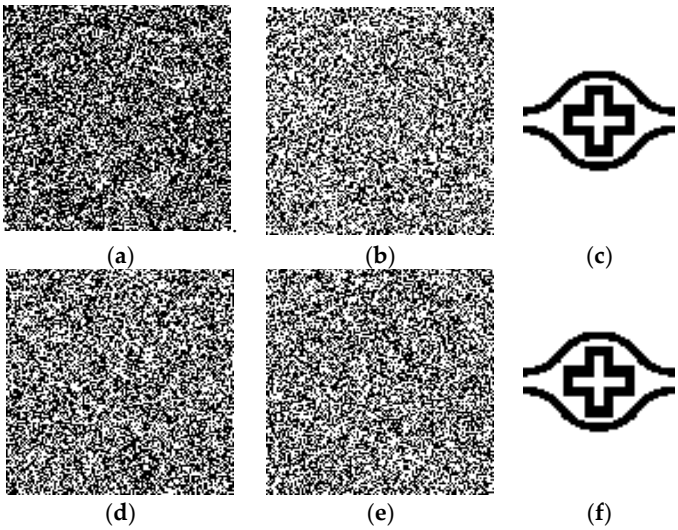


Figure 6. Simulation results when the medical image was not attacked by any image processing. (**a**,**b**) are the ownership share image (OSI) and master share image (MSI) (128 × 128) and (**c**) is retrieved watermarks (64 × 64) after CT image simulation; (**d**,**e**) are the OSI and MSI (128 × 128), and (**f**) is the retrieved watermark (64 × 64) after X-ray image simulation.

For WMNet, we used MATLAB 2020b with an NVIDIA GeForce GTX 1080Ti, τ was set to 5, and α contained 14,336 distorted watermarks. During training, α was divided into the training, validation, and testing datasets in the ratios of 80%, 10%, and 10%, respectively. In addition, T_c was set as 0.65. This meant that when the NC value for the distorted watermark was greater than T_c, it was defined as "Correct" and the number of images was 7165 images. Otherwise, it was defined as "Incorrect" and the number of images was 7170 images. Figure 7 shows the accuracy and loss during the WMNet training processing phase. From Figure 7, we can see that during training, accuracy continuously increased while loss continuously decreased. In addition, the accuracies of the final WMNet training, validation, and testing datasets were 99.8%, 97.9%, and 97.3%, respectively. Furthermore, the confusion matrices of the training, validation and testing datasets, shown in Figure 8, indicate that the rate of incorrect classification is low. Figure 9 shows the corresponding NC values of the incorrectly classified distorted watermarks. It was found that most of the NC values of distorted watermarks that were incorrectly classified by WMNet were located near the set T_c value. In other words, WMNet had good classification results on most distorted watermarks. The T_c value was set at 0.65, which is considered a sufficient threshold in most of the previously published watermarking systems.

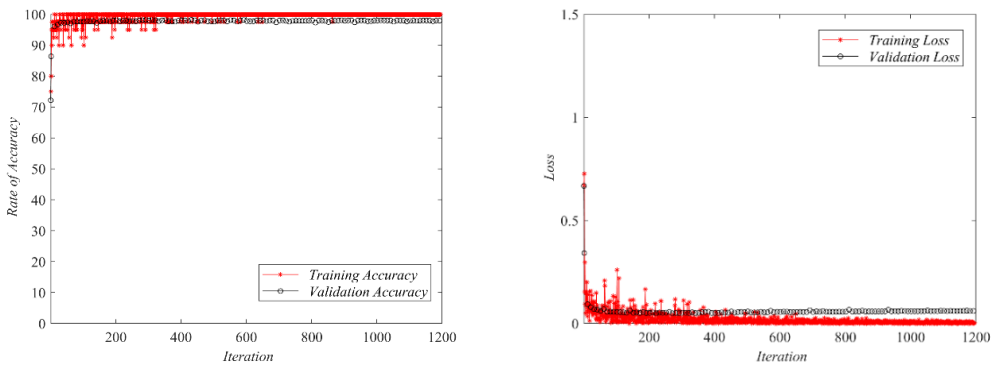


Figure 7. Accuracy and loss results for WMNet training. (**a**) Accuracy and (**b**) loss.

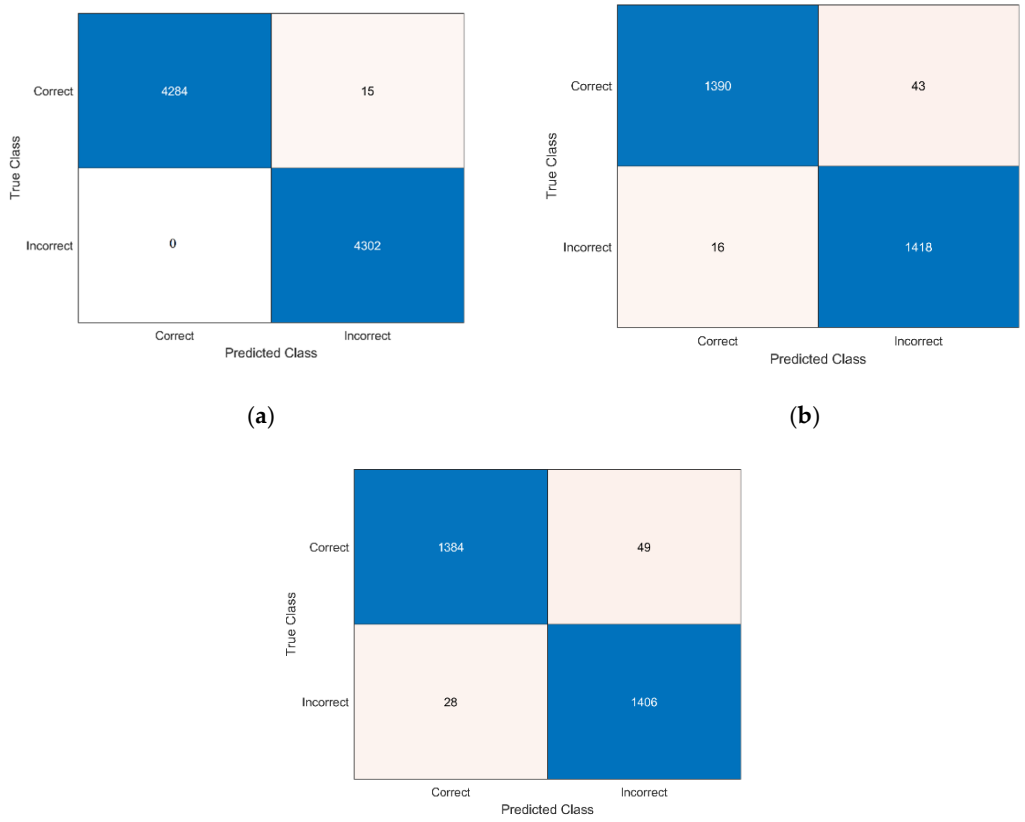


Figure 8. Confusion matrix for WMNet training. (**a**) Training dataset, (**b**) validation dataset, and (**c**) testing dataset.

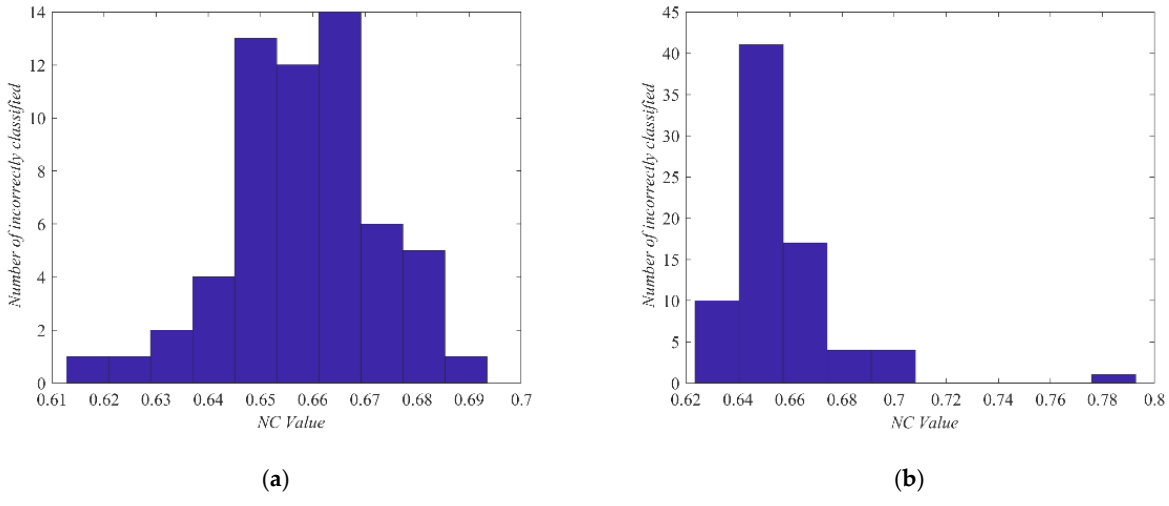


Figure 9. Visualization distribution of incorrectly classified distorted watermarks (T_c is 0.65). (**a**) Validation dataset and (**b**) testing dataset.

In addition, WMNet was evaluated using 5-fold cross validation, with the aim of ensuring that such training materials for simulating distorted watermarks were not specifically composed of sliced data used to train effective WMNets. The simulated 14,336 distorted watermarks were divided into five groups, and the datasets of each group served as the testing dataset once, while the subsets of the other four groups served as the training dataset, so that five WMNets were obtained. The performance results of these five WMNets were evaluated in the testing dataset. In addition, we analyzed the performance using

the following performance measures, where TP is true positive, TN is true negative, FP is false positive, and FN is false negative; the results are compiled in Table 2. It can be seen from the table that the results of each test dataset are very approximate, showing that such datasets generated by the simulation distorted watermark method and WMNet constructed through deep learning techniques have very good efficacy. Thus, WMNet is not only able to generalize the dataset, but overfitting also does not occur. Moreover, it was confirmed that the method of generating several distorted watermarks by simulation and then collecting them into a dataset is free from the problem of data selection bias and can train valid WMNets effectively.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

$$Specificity = \frac{TN}{TN + FP} \tag{2}$$

$$Sensitivity = \frac{TP}{TP + FP} \tag{3}$$

$$Negative\ predictive\ value = \frac{TN}{TN + FN} \tag{4}$$

$$Positive\ predictive\ value = \frac{TP}{TP + FP} \tag{5}$$

$$F - measure = \frac{2TP}{2TP + FP + FN} \tag{6}$$

Table 2. Results of 5-fold cross validation.

Performance Metrics (%)	Testing Dataset					
	1	**2**	**3**	**4**	**5**	**Average**
Accuracy	97.2	97.9	98.1	98	97.9	97.8
Specificity	96.4	98.4	97.8	97.7	97.4	97.5
Sensitivity	97.9	98.4	97.8	97.7	97.4	97.8
Negative predictive value	97.9	97.4	98.4	98.3	98.4	98
Positive predictive value	96.5	98.4	97.8	97.7	97.4	97.6
F-Measure	97.2	97.9	98.1	98	97.9	97.8

The main purpose of the proposed WMNet was to assist in the watermark system verification process. Specifically, if the extracted watermark was distorted because the protected image was attacked by image processing, we intended to determine the effectiveness of confirming the watermark information using WMNet. For simulation experiments using the actual watermarking system, we distorted the medical images using several common image-processing methods: JPEG compression (quality factor = 10%), JPEG 2000 (compression ratio = 8), Gaussian noise addition (mean = 0, variance = 0.5), salt-and-pepper noise addition (noise density = 50%), median filtering (window size = 4×4), rotation (7°), cropping (cropped area of 25%), and scaling (reduction to 1/16). We used peak signal-to-noise ratio (PSNR) [20] and NC to measure the attack intensity of the image. Table 3 summarizes the PSNR results for each medical image that was subjected to each attack. Different image-processing attacks cause different degrees of image distortion.

The copyright protection mechanisms published in recent years have good robustness; hence, we chose those lossless image watermarking systems published in the past that still have room for breakthrough in terms of effectiveness [14,18], applied them to medical images, and used WMNet to assist in the watermark verification stage. Table 4 shows the NC results after a medical image was subjected to attack, the watermark extraction results after the image underwent each image-processing attack, and the WMNet interpretation results. The results in the table show that there is some distortion in most medical images

after an image-processing attack. In addition, the NC of extracted watermarks all showed that lossless image watermarking systems have varying degrees of resilience, primarily because the core methods used by each technology are different, requiring the process to be adapted to resist damage from different types of image-processing attacks. However, even if the extracted watermark is distorted, WMNet can interpret whether the copyright information in the watermark is correct. Note that the watermark size is 64×64 when WMNet is constructed. When watermarks of different sizes are verified, the watermarks need to be resized to 64×64 before being interpreted by WMNet. Here, double linear interpolation is used to adjust the watermark size. Even after resizing, WMNet can clearly determine whether the copyright information in the watermark is correct.

Table 3. Peak signal-to-noise ratio (PSNR) of the medical images after various attacks.

Attacks	PSNR	
	CT	X-ray
JPEG Compression	26.13	29.84
JPEG 2000	41.63	38.18
Gaussian Noise Addition	7.49	7.67
Salt-pepper Noise Addition	6.71	7.37
Median Filtering	18.71	28.48
Rotation	12.79	16.91
Cropping	17.49	13.26
Scaling	16.93	23.21

Table 4. The simulated results of medical images after various attacks with other lossless image watermarking systems.

Attack	Wang's Method [14]								Wu's Method [18]							
	CT				X-ray				CT				X-ray			
	NC	[1] W1	NC	[2] W2	NC	W1	NC	W2	NC	W1	NC	W2	NC	W1	NC	W2
JPEG Compression	0.99	Y	0.99	Y	0.99	Y	0.99	Y	0.99	Y	0.99	Y	0.99	Y	1	Y
JPEG 2000	0.98	Y	0.98	Y	0.99	Y	1	Y	1	Y	1	Y	1	Y	1	Y
Gaussian Noise Addition	0.95	Y	0.95	Y	0.98	Y	0.98	Y	0.92	Y	0.93	Y	0.95	Y	0.95	Y
Salt-pepper Noise Addition	0.93	Y	0.96	Y	0.98	Y	0.99	Y	0.94	Y	0.93	Y	0.95	Y	0.96	Y
Median Filtering	0.97	Y	0.98	Y	1	Y	0.99	Y	0.99	Y	0.99	Y	1	Y	0.99	Y
Rotation	0.94	Y	0.92	Y	0.95	Y	0.93	Y	0.97	Y	0.97	Y	0.93	Y	0.94	Y
Cropping	0.93	Y	0.94	Y	0.92	Y	0.92	Y	0.94	Y	0.94	Y	0.91	Y	0.92	Y
Scaling	0.97	Y	0.96	Y	0.99	Y	0.99	Y	0.99	Y	0.99	Y	0.98	Y	0.99	Y

[1] W1: Results for 64×64 watermark; [2] W2: results for 32×32 watermark; "Y" indicates the extracted watermark is interpreted correctly by WMNet; "N" indicates the extracted watermark is interpreted incorrectly by WMNet.

The above-mentioned experimental results demonstrate that WMNet, as proposed in this study, is effective. Even if the protected image is subjected to different types of image processing attacks, which cause the watermark to produce different distortion conditions, WMNet can be used to interpret watermark information for all watermarks extracted, regardless of the extraction method. This shows that WMNet is relatively flexible and can be used with different watermarking systems. It can improve the verification of the watermarking mechanism of a system for data security without changing the original system. The interpretation of the copyright information in the watermark is more accurate and objective.

5. Conclusions

In recent years, hospitals and medical research centers have been transformed into digitized environments. This evolution has made the security of the usage, management, and transmission of digital medical images an issue of extreme importance. Here, we proposed WMNet, which assists in confirming the ownership of watermarks in a lossless medical image watermarking system. The primary objective of WMNet was to examine the extracted watermark when authenticating suspected medical images. The advantages of WMNet are as follows: (1) WMNet interpretation makes the determination more objective. (2) Even if the extracted watermark is distorted, WMNet interpretation is also relatively successful. (3) WMNet is flexible and can be used to examine distorted watermarks that have been extracted using other schemes. Finally, the experimental results show that the WMNet in this paper has good efficacy, which can be extended to different multimedia applications in the future. The corresponding copyright attribution of the watermark extracted from a protected image can be read directly through WMNet, making the proposed system more objective and suitable for real-time systems.

Author Contributions: Conceptualization, Y.-P.C.; Data curation, T.-Y.F.; Formal analysis, Y.-P.C. and H.-C.C.; Funding acquisition, H.-C.C.; Investigation, T.-Y.F. Methodology, Y.-P.C. and T.-Y.F.; Project administration, Y.-P.C.; Resources, T.-Y.F.; Software, T.-Y.F.; Supervision, H.-C.C.; Validation, Y.-P.C. and H-.C.C.; Visualization, Y.-P.C.; Writing—original draft, T.-Y.F.; Writing—review and editing, H.-C.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Chang Gung Memorial Hospital, Taiwan, R.O.C. (grant number CLRPG3H0012 and CIRPG3H0012); the Ministry of Science and Technology, Taiwan, R.O.C. (grant number MOST 109-2221-E-130-012).

Acknowledgments: The author would like to express his earnest appreciation to the anonymous referees for their constructive suggestions. The authors thank the statistical assistance and wish to acknowledge the support of the Maintenance Project of the Center for Artificial Intelligence in Medicine (Grant CLRPG3H0012, CIRPG3H0012) at Chang Gung Memorial Hospital for study design and monitoring, data analysis, and interpretation. In addition, this research was partly supported by the Ministry of Science and Technology, Taiwan, R.O.C. , under Contract No. MOST 109-2221-E-130-012.

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

References

1. Abo-Zahhad, M.; Ahmed, S.M.; Elnahas, O. A wireless emergency telemedicine system for patients monitoring and diagnosis. *Int. J Telemed. Appl.* **2014**, *2014*, 1–11.
2. Prasad, D.D.; Ray, S.; Majumdar, A.K.; Mukherjee, J.; Majumdar, B.; Paul, S.; Verma, A. Real time medical image consultation system through Internet. *J. Healthc. Eng.* **2010**, *1*, 141–154. [CrossRef]
3. Weng, Y.C.; Hsieh, S.L. Design and implementation of a web-based medical drawing management system. *J. Intell. Inf. Syst.* **2017**, *49*, 391–405. [CrossRef]
4. Nyeem, H.; Boles, W.; Boyd, C. A review of medical image watermarking requirements for teleradiology. *J. Digit. Imaging* **2013**, *26*, 326–343. [PubMed]
5. Shih, F.Y.; Zhong, X. High-capacity multiple regions of interest watermarking for medical images. *Inf. Sci.* **2016**, *367–368*, 648–659. [CrossRef]
6. Lei, B.; Tan, E.L.; Chen, S.; Ni, D.; Wang, T.; Lei, H. Reversible watermarking scheme for medical image based on differential evolution. *Expert Syst. Appl.* **2014**, *41*, 3178–3188. [CrossRef]
7. Rahimi, F.; Rabbani, H. A dual adaptive watermarking scheme in contourlet domain for DICOM images. *Biomed. Eng. Online* **2011**, *10*, 53. [CrossRef]
8. Cedillo-Hernandez, M.; Garcia-Ugalde, F.; Nakano-Miyatake, M.; Perez-Meana, H. Robust watermarking method in DFT domain for effective management of medical imaging. *Signal Image Video Process.* **2015**, *9*, 1163–1178.
9. Parah, S.A.; Ahad, F.; Sheikh, J.A.; Bhat, G.M. Hiding clinical information in medical images: A new high capacity and reversible data hiding technique. *J. Biomed. Inf.* **2017**, *66*, 214–230. [CrossRef]
10. Singh, A.K.; Dave, M.; Mohan, A. Robust and secure multiple watermarking in wavelet domain. *J. Med. Imaging Health Inf.* **2015**, *5*, 406–414.
11. Das, S.; Kundu, M.K. Effective management of medical information through ROI-lossless fragile image watermarking technique. *Comput. Meth. Programs Biomed.* **2013**, *111*, 662–675. [CrossRef]

12. Sharma, A.; Singh, A.K.; Ghrera, S.P. Robust and secure multiple watermarking for medical images. *Wirel. Pers. Commun.* **2017**, *92*, 1611–1624. [CrossRef]
13. Maheshkar, S. Region-based hybrid medical image watermarking for secure telemedicine applications. *Multimed. Tools Appl.* **2017**, *76*, 3617–3647.
14. Wang, M.S.; Chen, W.C. Digital image copyright protection scheme based on visual cryptography and singular value decomposition. *Opt. Eng.* **2007**, *46*, 067006. [CrossRef]
15. Fan, T.Y.; Chieu, B.C.; Chao, H.C. Robust copyright-protection scheme based on visual secret sharing and Bose–Chaudhuri–Hocquenghem code techniques. *J. Electron. Imaging* **2012**, *21*, 043018. [CrossRef]
16. Lou, D.C.; Tso, H.K.; Liu, J.L. A copyright protection scheme for digital images using visual cryptography technique. *Comput. Stand. Interfaces* **2007**, *29*, 125–131. [CrossRef]
17. Wang, M.S.; Chen, W.C. Robust copyright protection scheme based on discrete cosine transform and secret sharing techniques. *J. Electron. Imaging* **2008**, *17*, 023006. [CrossRef]
18. Wu, X.; Sun, W. Robust copyright protection scheme for digital images using overlapping DCT and SVD. *Appl. Soft. Comput.* **2013**, *13*, 1170–1182. [CrossRef]
19. Thanh, T.M.; Tanaka, K. An image zero-watermarking algorithm based on the encryption of visual map feature with watermark information. *Multimed. Tools Appl.* **2017**, *76*, 13455–13471. [CrossRef]
20. Fan, T.Y.; Chieu, B.C.; Chao, H.C. Medical image watermarking based on visual secret sharing and cellular automata transform for copyright protection. *KSII Trans. Internet Inf. Syst.* **2018**, *12*, 6177–6200.
21. Rawat, S.; Raman, B. A blind watermarking algorithm based on fractional Fourier transform and visual cryptography. *Signal Process.* **2012**, *92*, 1480–1491. [CrossRef]
22. Seenivasagam, V.; Velumani, R. A QR code based zero-watermarking scheme for authentication of medical images in teleradiology cloud. *Comput. Math. Methods Med.* **2013**, *2013*. [CrossRef]
23. Shao, Z.; Shang, Y.; Zeng, R.; Shu, H.; Coatrieux, G.; Wu, J. Robust watermarking scheme for color image based on quaternion-type moment invariants and visual cryptography. *Signal Process. Image Commun.* **2016**, *48*, 12–21. [CrossRef]
24. Dong, J.; Li, J. A robust zero-watermarking algorithm for encrypted medical images in the DWT-DFT encrypted domain. In *International Conference on Innovation in Medicine and Healthcare*; Springer: Cham, Switzerland, 2016; pp. 197–208.
25. Sainath, T.N.; Mohamed, A.; Kingsbury, B.; Ramabhadran, B. Deep convolutional neural networks for LVCSR. In Proceedings of the 2013 IEEE international conference on acoustics, speech and signal processing, Vancouver, BC, Canada, 26–31 May 2013; pp. 8614–8618.
26. Suzuki, K. Overview of deep learning in medical imaging. *Radiol. Phys. Technol.* **2017**, *10*, 257–273. [CrossRef]
27. Shrestha, A.; Mahmood, A. Review of deep learning algorithms and architectures. *IEEE Access* **2019**, *7*, 53040–53065. [CrossRef]
28. Shoron, S.H.; Islam, M.; Uddin, J.; Shon, D.; Im, K.; Park, J.-H.; Lim, D.-S.; Jang, B.; Kim, J.-M. A Watermarking Technique for Biomedical Images Using SMQT, Otsu, and Fuzzy C-Means. *Electronics* **2019**, *8*, 975. [CrossRef]
29. Ud Din, S.; Jan, Z.; Sajjad, M.; Hussain, M.; Ali, R.; Ali, A.; Lee, S. Secure Exchange of Medical Data Using a Novel Real-Time Biometric-Based Protection and Recognition Method. *Electronics* **2020**, *9*, 2013. [CrossRef]
30. Naor, M.; Shamir, A. Visual cryptography. In *Workshop on the Theory and Application of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1994; pp. 1–12.
31. Yang, C.N. New visual secret sharing schemes using probabilistic method. *Pattern Recogn. Lett.* **2014**, *25*, 481–494. [CrossRef]