

Retraction

Retracted: Robust Zero Watermarking Algorithm for Medical Images Based on Zernike-DCT

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

Copyright © 2024 Security and Communication Networks. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

- (1) Discrepancies in scope
- (2) Discrepancies in the description of the research reported
- (3) Discrepancies between the availability of data and the research described
- (4) Inappropriate citations
- (5) Incoherent, meaningless and/or irrelevant content included in the article
- (6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.



The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

- [1] C. Yang, J. Li, U. A. Bhatti, J. Liu, J. Ma, and M. Huang, "Robust Zero Watermarking Algorithm for Medical Images Based on Zernike-DCT," *Security and Communication Networks*, vol. 2021, Article ID 4944797, 8 pages, 2021.

Research Article

Robust Zero Watermarking Algorithm for Medical Images Based on Zernike-DCT

Chengshan Yang ¹, Jingbing Li ^{1,2}, Uzair Aslam Bhatti,³ Jing Liu,⁴ Jixin Ma,⁵ and Mengxing Huang^{1,2}

¹School of Information and Communication Engineering, Hainan University, Haikou, China

²State Key Laboratory of Marine Resource Utilization in the South China Sea, Hainan University, Haikou, China

³School of Geography (Remote Sensing & GIS Lab), Nanjing Normal University, Nanjing, China

⁴Research Center for Healthcare Data Science, Zhejiang Lab, Hangzhou, China

⁵School of Computing & Mathematical Sciences, University of Greenwich, London, UK

Correspondence should be addressed to Jingbing Li; jingbingli2008@hotmail.com

Received 19 August 2021; Revised 8 September 2021; Accepted 4 October 2021; Published 10 November 2021

Academic Editor: Xingsi Xue

Copyright © 2021 Chengshan Yang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Digital medical system not only facilitates the storage and transmission of medical information but also brings information security problems. Aiming at the security of medical images, a robust zero watermarking algorithm for medical images based on Zernike-DCT is proposed. The algorithm first uses a chaotic logic sequence to preprocess and encrypt the watermark, then performs edge detection and Zernike moment processing on the original medical image to get the accurate edge points, and then performs discrete cosine transform (DCT) on them to get the feature vector. Finally, it combines perceptual Hash and zero watermark technology to generate the key to complete the watermark embedding and extraction. The algorithm has good robustness to conventional and geometric attacks, strong antinoise ability, high positioning accuracy, and processing efficiency and is superior to the classical edge detection algorithm in extraction effect. It is a stable and reliable image edge detection algorithm.

1. Introduction

In the past two decades, the advent of the era of big data has allowed the explosive development of computer science technology and multimedia communication technology, which has accelerated the digital development process of the healthcare system [1]. When the data containing our personal private information are uploaded to the cloud storage server, we lose direct control over the data, which makes us worry about the security of our private information [2]. With the continuous development of modern medical imaging technology, medical institutions produce a large number of different types of medical images every day, such as CT, MRI, color Doppler ultrasound, OCT, and X-ray [3]. However, when these medical images are stored and transmitted on the Internet, they are susceptible to

unintentional or a variety of malicious attacks, resulting in poor security [4, 5]. Medical images are the main basis for doctors to judge the condition, so it is very important to ensure the safety of medical images during network transmission [6]. The emergence of digital watermarking technology [7–9] is an effective improvement to traditional encryption technology. It embeds the patient's personal information and the cause of disease as a digital watermark into medical images. It has strong security and robustness. It can ensure that after network transmission and data processing, the digital watermark can still be extracted completely and reliably, and the patient's personal information can be protected.

So far, many experts have done a lot of research on the design of digital watermarking and put forward many feasible digital watermarking algorithms [10, 11]. Cui et al.

[12] proposed a color image wavelet domain digital watermarking optimization algorithm based on differential evolution. Firstly, Arnold scrambling transform was used to encrypt the watermark image, and then the color image was transformed from RGB space to YIO space suitable for the human visual system, and then three-level DWT transform and SVD decomposition were performed on it. The algorithm adaptively selected scale factor for embedding watermark information. However, it is a little complex, time-consuming, and generally robust. Kamble et al. [13] proposed an innovative data recovery method based on robust reversible watermarking. The algorithm uses a pseudo-random number generator to generate a random key. The key and the data are binary XOR encrypted, and then the encrypted data are embedded into the cover image using the least significant bit (LSB) algorithm to form a watermark image. This algorithm only embeds three bytes of encrypted data, so the capacity of the payload needs to be improved. Fang et al. [14] proposed a blind watermarking technology based on DCT domain. First, Arnold chaotic scrambling was performed on the watermark before embedding to obtain a one-dimensional sequence. Then, the original image was transformed by $8 * 8$ block DCT, and intermediate frequency coefficients were selected. Then, a one-dimensional sequence was embedded in it, and each block was transformed by IDCT to obtain the image-embedded watermark. The algorithm is simple to embed and extract and does not need the participation of the original image, so it realizes the blind extraction. However, it is less robust to strong noise attack and geometric attack. Ghosal and Mehrotra [15] proposed for the first time to use Zernike orthogonal moments to calculate parameters to realize subpixel edge detection, but this algorithm did not consider the amplification effect of the template, resulting in large errors in the calculation results. Dong and Liu [16] proposed the application of Zernike moment in medical image processing, which proved that Zernike moment is an effective image description method, and has its unique advantages, which meets the technical requirements of high accuracy, good robustness, insensitive to noise and artifacts, and easy to combine with a variety of algorithms in the field of medical image processing. Xue et al. conducted in-depth ontology matching research in order to solve the heterogeneous problem of biomedical ontology [17–19]. An extended compact genetic algorithm-based ontology entity matching technique (ECGA-OEM) is proposed, which uses both the compact encoding mechanism and linkage learning approach to match the ontologies efficiently. A central concepts-based ontology partitioning algorithm is first used to divide the ontology into several disjoint segments, which borrows the idea from the social network and firefly Algorithm (FA). The comparison with the most advanced ontology matching technology shows the robustness and effectiveness of these methods. At present, there are many research studies based on deep learning, which can carry out image feature extraction [20, 21] and natural language processing [22–24], but deep learning requires a large number of samples and corresponding tags. There are few

samples of medical images and corresponding privacy labels, so only professionals can calibrate medical image labels.

The disadvantage of these algorithms is that they are not very robust to geometric attacks [25], especially rotation attacks. In the field of medical image digital watermarking research, geometric attacks are still a relatively difficult problem to solve so far. In practical applications, medical digital watermarking images are often subject to both conventional attacks and geometric attacks [26]. Therefore, to improve the security of medical information, this paper proposes a zero watermarking algorithm of medical images based on Zernike-DCT. In this scheme, edge detection and Zernike moment processing are performed on the medical image, then discrete cosine transform is performed, and the 32-bit coefficient matrix is selected as the feature vector of the medical image to embed and extract the watermark. The watermark is encrypted by chaos, and zero watermark [27] and blind extraction are realized by using Perceptual Hashing technology [28] and cryptography principle. The algorithm solves the contradiction between invisibility and robustness, and can well resist conventional attacks and geometric attacks, especially rotation attacks. The robustness of the algorithm is very good, and the security of the watermark is improved.

This paper consists of five sections: Introduction, Fundamental Theory, Watermarking Algorithm, Results and Discussion, and Conclusion. The first section mainly introduces the development background of medical images in the era of big data, the importance of security and privacy, and the in-depth research on digital watermarking algorithms by experts in recent years. The second section mainly introduces the fundamental theory of the algorithm proposed in this paper, including Canny edge detection, Zernike moment, and Logistic mapping. The third section mainly introduces the specific implementation process of the algorithm proposed in this paper, including watermark encryption, watermark embedding, watermark extraction and decryption, and watermark evaluation methods. The fourth section mainly introduces the results and discussion, including the experimental platform and materials, display of the data and images, and analysis of the experimental results. The fifth section mainly summarizes the main ideas and advantages of this algorithm, which has good robustness, imperceptibility, stability, and reliability.

2. The Fundamental Theory

2.1. Canny Edge Detection. The edge of a gray image is generally the place where the gray level of the image changes dramatically. There are many methods of gray image edge detection [29]. The Canny edge detection method is considered to be one of the most successful gray edge detection methods, and it is also the most widely used edge detection method. Canny edge detection process is as follows.

Firstly, a Gaussian filter is used to filter the input image to reduce the influence of noise on gradient calculation. The Gaussian filter formula is as follows:

$$G(x, y, \sigma) = \frac{1}{2\pi\sigma^2} \exp\left(-\frac{x^2 + y^2}{2\sigma^2}\right). \quad (1)$$

First-order difference operator is used to calculate the gradient amplitude components in the horizontal and vertical directions so as to obtain the gradient amplitude and gradient direction of the image.

$$M = \sqrt{Gx^2 + Gy^2}, \quad (2)$$

$$\theta = \arctan\left(\frac{Gy}{Gx}\right). \quad (3)$$

The gradient amplitude is not maximally suppressed. The gradient intensity of the current pixel is compared with the two pixels along the positive and negative gradient direction. If the gradient intensity of the current pixel is the largest compared with the other two pixels, the pixel is retained as an edge point; otherwise, the pixel will be suppressed.

Through the method of double threshold to extract the edge of the image, TH is the high threshold and TL is the low threshold; it is recommended that the ratio of high threshold and low threshold should be 2 : 1 or 3 : 1. If the gradient value of the edge pixel is higher than the high threshold, it is marked as a strong edge pixel. If the gradient value of the edge pixel is less than the high threshold and greater than the low threshold, it is marked as a weak edge pixel. If the gradient value of the edge pixel is less than the low threshold, it will be suppressed. The selection of threshold depends on the content of the given input image.

2.2. Zernike Moment. The n -th-order m -order Zernike moment of two-dimensional continuous image $f(x, y)$ is defined as follows:

$$Z_{nm} = \frac{n+1}{\pi} \iint_{x^2+y^2 \leq 1} f(x, y) V_{nm}^*(\rho, \theta) dx dy, \quad (4)$$

where $V_{nm}^*(\rho, 0)$ is the conjugate complex number of $V_{nm}(\rho, 0)$.

From the ideal subpixel edge detection model of an image, the mode of an image before and after rotation remains unchanged, and only the phase angle changes. The relationship between Zernike moment Z_{nm}' after rotation and Zernike moment Z_{nm} before rotation and the formula of edge parameters are as follows:

$$Z_{nm}' = Z_{nm} e^{-im\varphi}, \quad (5)$$

$$\varphi = \arctan\left(\frac{\text{Im}[Z_{11}]}{\text{Re}[Z_{11}]}\right). \quad (6)$$

The other three edge parameters h , K , and l can be calculated by using the Zernike moment formula of image rotation where h is the background gray, K represents gray scale difference, and l is the vertical distance from the center of the unit circle to the edge:

$$k = \frac{3Z_{11}}{2(1-l^2)^{3/2}} e^{j\varphi}, \quad (7)$$

$$h = \frac{Z_{00}(k\pi/2) + k \arcsin l + kl\sqrt{1-l^2}}{\pi}, \quad (8)$$

$$l = \frac{Z_{20}}{Z_{11}} e^{-j\varphi}. \quad (9)$$

In the discrete case, the template and pixel gray value convolution are used to calculate the moment [30]. Due to the template effect, when the unit circle is used for sampling in the $N \times N$ pixel area, the template moves on the image for convolution. The template contains N^2 pixels around the center of the template. At this time, the unit radius becomes $N/2$, so it needs the vertical distance l calculated on the unit circle which is enlarged by $N/2$ times, so the calculation formula of the subpixel coordinates of the pixel point is as follows:

$$\begin{bmatrix} x_s \\ y_s \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix} + \frac{N}{2} l \begin{bmatrix} \cos \varphi \\ \sin \varphi \end{bmatrix}. \quad (10)$$

Among them, x_s and y_s are the subpixel coordinates of the edge and x and y are the origin coordinates.

2.3. Logistic Mapping. The encryption of the watermark adopts a logistic map. One-dimensional logistic map is one of the most famous chaotic maps, and it is a simple dynamic nonlinear regression with chaotic behavior. Its mathematical definition is as follows:

$$x_{k+1} = \mu \cdot x_k (1 - x_k), \quad (11)$$

where $x(k) \in (0, 1)$, $0 < \mu \leq 4$, and μ is called logistic parameter. Logistic map is not necessarily in a chaotic state, which is related to the value of μ . Experiments show that when $3.5699456 < \mu \leq 4$, the value generated by iteration is in a state of pseudo-random distribution. At this time, a logistic map works in a chaotic state [31], and a logistic chaotic sequence can be used as an ideal key sequence.

3. Watermarking Algorithm

3.1. Watermark Encryption. The process of digital watermark encryption is shown in Figure 1.

The chaotic sequence is generated by the initial value x_0 of the logistic mapping. The chaotic sequence generated by different initial values is different, and it is a one-dimensional sequence. It also needs to be upgraded to a binary sequence $B(i, j)$ and then XOR with the original watermark $W(i, j)$ to get the encrypted digital watermark $BW(i, j)$. Even if the algorithm is public, the original watermark cannot be restored without the private key x_0 .

3.2. Watermark Embedding. The digital watermarking system mainly includes watermark embedding and extraction. At the same time, this paper also combines the zero watermark technology and perceptual hash to

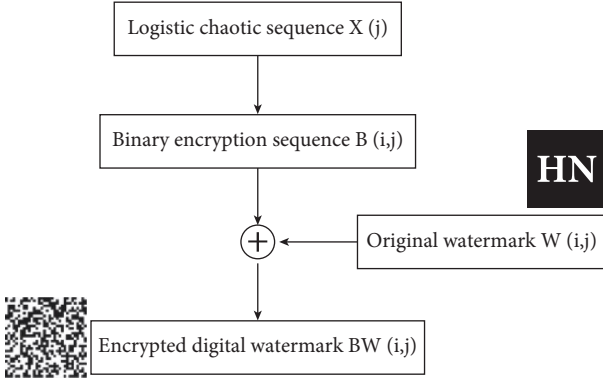


FIGURE 1: Digital watermark encryption process.

achieve zero watermark embedding without changing the original medical image. The specific steps are shown in Figure 2.

It can be seen from Figure 2 that the Canny operator is used to perform edge detection on the original medical image $F(i, j)$. The coordinates and gradient direction of the edge point are determined at the pixel level to obtain the coarse positioning of the edge point and the edge point coordinate matrix $C(i, j)$.

According to the constructed edge point vector and reference threshold, the edge points are repositioned by the Zernike moment algorithm to realize the subpixel edge detection of the image, and the subpixel coordinate matrix $Z(i, j)$ is obtained, and finally DCT transformation is performed on it and a hash function is used to obtain $4 * 8$ visual feature vector $V(j)$.

The visual feature vector $V(j)$ and the encrypted digital watermark $BW(i, j)$ obtain the $Key(i, j)$ through the hash function commonly used in cryptography and save it to a third party to obtain the ownership of the original image so that it can be used to extract the watermark later.

$$Key(i, j) = BW(i, j) \oplus V(j). \quad (12)$$

3.3. The Extraction and Decryption of Watermark. Watermark extraction is the reverse process of watermark embedding. The process of extracting and decrypting the original watermark is shown in Figure 3.

According to the method of extracting the feature vector of the original medical image, the feature vector of the medical image to be tested is extracted, and the encrypted watermark $BW'(i, j)$ in the image to be tested is obtained by hash function with the $Key(i, j)$ mentioned above. The binary encryption sequence $B'(i, j)$ is obtained by upgrading the dimension of the one-dimensional sequence generated by the initial value x_0 of logistic mapping. It can restore watermark $W'(i, j)$ by Hash function properties with $BW'(i, j)$. The method proposed in this paper does not need the original medical image when extracting the watermark, which can protect the medical image from any interference and improve the security of the watermark.

$$BW'(i, j) = Key(i, j) \oplus V'(j), \quad (13)$$

$$W'(i, j) = B'(i, j) \oplus BW'(i, j). \quad (14)$$

3.4. Evaluation of Watermark. The normalized correlation coefficient is used to evaluate the similarity between the original watermark and the extracted watermark, and the peak signal-to-noise ratio is used to measure the distortion of the medical image with the watermark.

$$NC = \frac{\sum_i \sum_j W(i, j) W'(i, j)}{\sum_i \sum_j [W(i, j)]^2}, \quad (15)$$

$$PSNR = 10 \lg \left[\frac{MN \max(I(i, j))^2}{\sum_i \sum_j (I(i, j) - I'(i, j))^2} \right]. \quad (16)$$

4. Simulation and Results

This experiment is simulated on matlab2018a. The $32 * 32$ -pixel meaningful letter “HN” image is selected as the digital watermark, and the $512 * 512$ -pixel brain medical image is selected as the original medical image. In the watermark encryption process, the initial value of the logistic chaotic system is 0.2, the growth parameter is 4, and the number of iterations is 32. To verify the particularity and feasibility of this algorithm, the similarity between six different medical images is tested. Figure 4 shows six different medical images, and Table 1 shows the tested NC values. The data show that the NC values of different images are less than 0.5, and the NC values of the same image are all 1, which shows that the algorithm is special and feasible.

4.1. The Results of the Attack on Encrypted Watermark.

To verify the robustness of the digital watermark under this algorithm, the encrypted watermark is subjected to different degrees of conventional attacks and geometric attacks, as shown in Table 2 and Figure 5. From the data in Table 2, with the increase in attack intensity, the PSNR and NC values of the encrypted watermark decrease gradually, but the NC value is still far greater than 0.5, indicating that the watermark can be extracted clearly. When the intensity of Gaussian noise reaches 30%, the NC value is 0.68, greater than 0.5, which can effectively resist the Gaussian noise attack. When the JPEG compression strength is 20%~80%, the NC value is 1, which shows that the algorithm has strong robustness against JPEG compression attack. When the median filter window is $7 * 7$, the NC value is 0.73, which can effectively resist the median filter attack. Geometric attack is a difficult problem for all encryption algorithms, but this algorithm still has an excellent performance in resisting geometric attack, especially in resisting rotation attack; when the medical image rotates clockwise to 38° , the NC value of the encrypted watermark is still as high as 0.6. When the scaling degree is 2, the NC value is 0.95. When the strength of left movement attack and cropping attack is 10%, the NC values are 0.63 and 0.74, respectively, and the NC

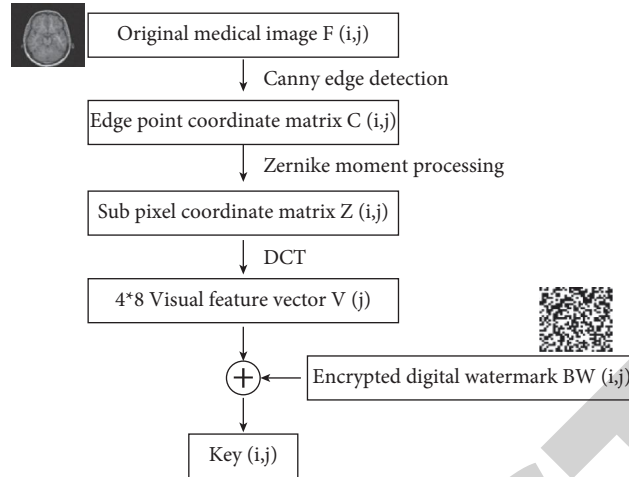


FIGURE 2: Medical image feature vector extraction and watermark embedding process.

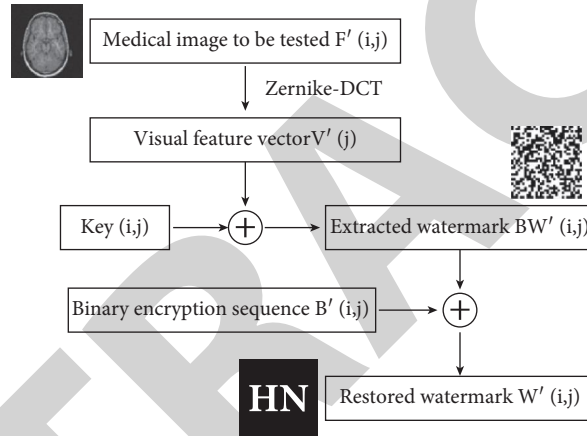


FIGURE 3: Watermark extraction and decryption process.

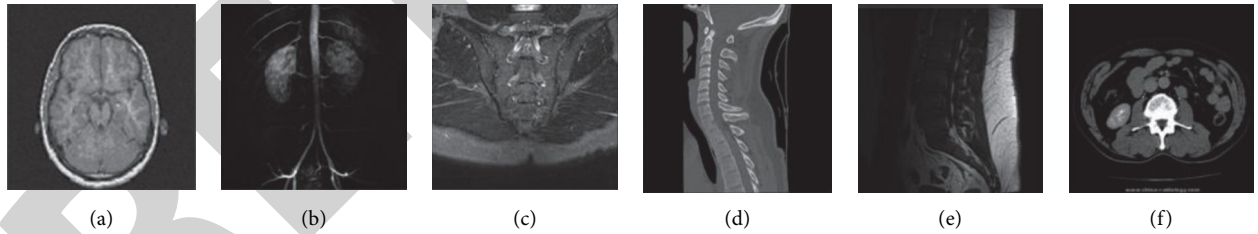


FIGURE 4: Different medical images: (a) brain; (b) lung; (c) sacroiliac; (d) spine; (e) knee; (f) kidney.

TABLE 1: Correlation coefficient value between different images (32 bit).

Image	Brain	Lung	Sacroiliac	Spine	Knee	Kidney
Brain	1	0.313	0.208	-0.125	-0.063	0.125
Lung	0.313	1	0.448	0.062	0.011	-0.062
Sacroiliac	0.208	0.448	1	-0.07	0.048	0.069
Spine	-0.125	0.062	-0.069	1	-0.063	-0.12
Knee	-0.063	0.011	0.048	-0.064	1	0.063
Kidney	0.125	-0.063	0.069	-0.125	0.063	1

value after geometric attack is greater than 0.5, which proves that the algorithm has strong robustness, and can better resist conventional attacks and geometric attacks.

4.2. Algorithms Comparison. To further verify the superiority of the algorithm proposed in this paper, we compare it with the NC value of the Canny-DCT algorithm, as shown in Table 3.

TABLE 2: PSNR and NC values under different attacks.

Type of attacks	Parameter	PSNR	NC
Gaussian noise (%)	5	14.31	0.92
	10	11.86	0.92
	20	9.76	0.87
	30	8.77	0.68
JPEG compression (%)	20	33.81	1
	40	35.46	1
	60	36.42	1
	80	37.82	1
Median filter (5 times)	3 * 3	34.49	0.95
	5 * 5	29.95	0.91
	7 * 7	27.54	0.73
Rotation (°) (clockwise)	5	18.00	0.82
	10	15.60	0.82
	20	14.60	0.79
	30	14.40	0.70
	38	14.13	0.60
Scaling factor	0.4	—	0.68
	0.8	—	0.87
	1.2	—	1
	2	—	0.95
Movement (%) (left)	1	17.99	1
	5	14.48	0.91
	8	14.21	0.72
	10	13.82	0.63
Cropping (%) (Y direction)	3	—	0.91
	5	—	0.78
	10	—	0.74
	20	—	0.64

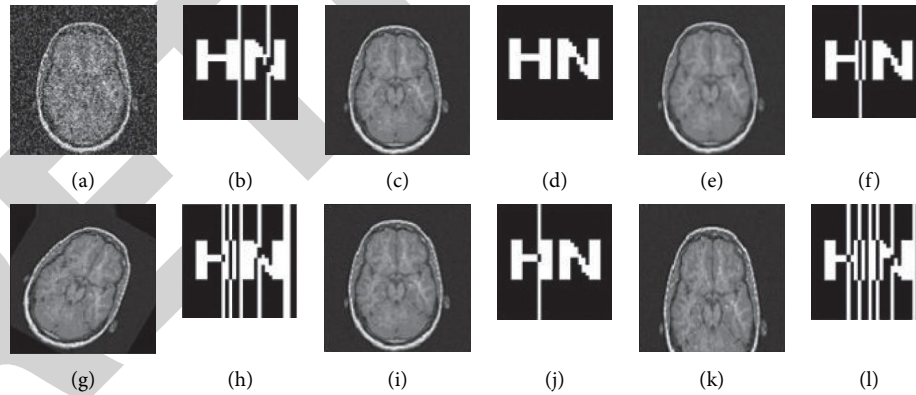


FIGURE 5: Part of the medical image and the extracted watermarking after the attacks: (a) Gaussian noise 5%; (c) JPEG compression 80%; (e) median filter [5 * 5], 5 times; (g) rotation 30%; (i) scale 2 times; (k) cropping (Y direction) 20%; (b), (d), (f), (h), (j), and (l) extracted watermarking.

From the data, we can see that the NC value of the algorithm proposed in this paper is much larger than the NC value of the Canny-DCT algorithm; for scaling and clipping attacks in geometric attacks, the NC value of this algorithm is similar to that of the Canny-DCT algorithm. In terms of rotation and left shift attacks, the NC value of the algorithm is larger than that of the Canny-DCT algorithm. In general, it is proved that the

proposed algorithm is more robust than the comparison algorithm, and it is a zero watermark algorithm with higher security.

4.3. Runtime Performance. Runtime performance is the key evaluation criterion. Table 4 shows the running time of each key step of the algorithm.

TABLE 3: Comparison between different algorithms.

Type of attacks	Parameter	Canny-DCT	Zernike-DCT
Gaussian noise (%)	5	0.35	0.92
	10	0.40	0.92
JPEG compression (%)	20	0.78	1
	40	0.96	1
Median filter (5 times)	3 * 3	0.81	0.95
	5 * 5	0.59	0.91
	7 * 7	0.42	0.73
Rotation (°) (clockwise)	10	0.67	0.82
	20	0.71	0.79
	35	0.67	0.70
Scaling factor	1.2	0.96	1
	2	0.83	0.95
Movement (%) (left)	1	0.78	1
	5	0.70	0.91
	10	0.48	0.63
Cropping (%) (Y direction)	10	0.69	0.74
	20	0.60	0.64

TABLE 4: The running time of each part in the proposed algorithm.

Time	Description	Running time (ms)
T1	The time it takes to encrypt the watermark image	6.5
T2	The time it takes to extract the features of Figure 4(a)	61.8
T3	The time it takes to embed an encrypted watermark in Figure 4(a)	1.8
T4	The time it takes to extract the encrypted watermark from the attacked Figure 4(a)	1.3
T5	The time it takes to decrypt the extracted encrypted watermark	5.2

5. Conclusions

A robust zero watermarking algorithm for medical images based on the Zernike-DCT transform is proposed. Firstly, the traditional Canny operator is used for edge detection to get coarse edge points. Then, the Zernike moment is used for processing to get subpixel accurate edge points. Finally, the DCT transform is used to get a 32-bit visual feature vector; a logistic chaotic map is used to encrypt the digital watermark, which further improves the security of the algorithm. The algorithm combines Perceptual Hashing, zero watermark technology, and the concept of a third party, which can complete the embedding and extraction of the watermark without changing the original medical image data. Experimental results show that the algorithm has good robustness to conventional and geometric attacks and has good imperceptibility. It effectively solves the contradiction between imperceptibility and robustness and has a strong antinoise ability. It is a stable and reliable robust digital watermarking algorithm for medical images.

5.1. Limitations. The low-order moment eigenvector describes the overall shape of an image target, and the high-order moment eigenvector describes the details of the image target. The Zernike moment template used in this algorithm is $7 * 7$. The larger the Zernike moment template, the higher the accuracy, but the longer the operation time.

Data Availability

The data supporting the reported results can be found in the article.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by the Natural Science Foundation of China under Grants 62063004 and 61762033, by the Hainan Provincial Natural Science Foundation of China under Grants 2019RC018 and 619QN246, and by the Major Scientific Project of Zhejiang Lab under Grant 2020ND8AD01.

References

- [1] Z. Li and P. Han, "Current situation and problems of smart city development in China based on big data analysis," *IOP Conference Series: Materials Science and Engineering*, vol. 750, Article ID 012116, 2020.
- [2] K.-K. R. Choo, "A cloud security risk-management strategy," *IEEE Cloud Computing*, vol. 1, no. 2, pp. 52–56, 2014.
- [3] A. F. Qasim, F. Meziane, and R. Aspin, "Digital watermarking: applicability for developing trust in medical imaging

- workflows state of the art review,” *Computer Science Review*, vol. 27, pp. 45–60, 2017.
- [4] Y. Liu and M. Cui, “Analysis of influencing factors and countermeasures of computer network security,” in *Proceedings of the International Conference on Application of Intelligent Systems in Multi-Modal Information Analytics*, Springer, Changzhou, China, 2020.
 - [5] Rostrom, *Framework to Secure Cloud-Based Medical Image Storage and Management System Communications*, Brigham Young University (BYU) Scholars Archive, Provo, UT, USA, 2017.
 - [6] M. Elhoseny, K. Shankar, S. K. Lakshmanaprabu, A. Maseleno, and N. Arunkumar, “Hybrid optimization with cryptography encryption for medical image security in Internet of Things,” *Neural Computing & Applications*, pre-published, vol. 32, no. 15, pp. 10979–10993, 2018.
 - [7] R. O. Preda and D. N. Vizireanu, “A robust digital watermarking scheme for video copyright protection in the wavelet domain,” *Measurement*, vol. 43, no. 10, pp. 1720–1726, 2010.
 - [8] J. Blake and S. Latifi, “Digital watermarking security,” *Defence Science Journal*, vol. 61, no. 5, pp. 408–414, 2011.
 - [9] L. I. Min, “Digital watermark algorithm integrated with space domain and time-frequency domain,” *Computer Engineering*, vol. 37, p. 120, 2011.
 - [10] F.-P. An and J.-e. Liu, “Image encryption algorithm based on adaptive wavelet chaos,” *Journal of Sensors*, vol. 2019, Article ID 2768121, 12 pages, 2019.
 - [11] Y. Xie, Y. Wang, and M. Ma, “Design of a hybrid digital watermarking algorithm with high robustness,” *Journal of Web Engineering*, vol. 19, p. 5, 2020.
 - [12] X. Cui, Y. Niu, X. Zheng, Y. Han, and X. Li, “An optimized digital watermarking algorithm in wavelet domain based on differential evolution for color image,” *Plos One*, vol. 13, p. 5, Article ID e0196306, 2018.
 - [13] P. Kamble, N. Raut, and A. Raut, “An innovative approach for data recovery using robust reversible watermarking,” in *Proceedings of the 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, Tirunelveli, India, April 2019.
 - [14] M. Fang, J. P. Zhang, and W. Zhang, “A blind watermarking technology based on DCT domain,” in *Proceedings of the 2012 International Conference on Computer Science and Service System*, pp. 397–400, IEEE, Nanjing, China, 2012.
 - [15] S. Ghosal and R. Mehrotra, “Orthogonal moment operators for subpixel edge detection,” *Pattern Recognition*, vol. 26, no. 2, pp. 295–306, 1993.
 - [16] S. Dong and Y. Liu, *Application of Zernike Moments in Medical Image Processing*, China Medical Equipment, Beijing, China, 2012.
 - [17] X. S. Xue and J. Zhang, “Matching large-scale biomedical ontologies with central concept based partitioning algorithm and adaptive compact evolutionary algorithm,” *Applied Soft Computing*, vol. 106, pp. 1–11, 2021.
 - [18] X. S. Xue, C. F. Yang, C. Jiang, P. W. Tsai, G. J. Mao, and H. Zhu, “Optimizing ontology alignment through linkage learning on entity correspondences,” *Complexity*, vol. 2021, Article ID 5574732, 12 pages, 2021.
 - [19] X. S. Xue, X. J. Wu, C. Jiang, G. J. Mao, and H. Zhu, “Integrating sensor ontologies with global and local alignment extractions,” *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 6625184, 10 pages, 2021.
 - [20] T. H. Kim, H. Oh, K. Kim, and Y. Lee, “Investigating single image super-resolution algorithm with deep learning using convolutional neural network for chest digital tomosynthesis,” *Optik-International Journal for Light and Electron Optics*, vol. 203, Article ID 164070, 2020.
 - [21] J. E. Lee, J. W. Kang, W. S. Kim, J. K. Kim, and D. K. Kim, “Digital image watermarking processor based on deep learning,” *Electronics*, vol. 10, p. 1183, Article ID 164070, 2021.
 - [22] H. Hu, H. Zhou, Z. Tian, Y. W. Zhang, and Y. Patterson: Investigating transfer learning in multilingual pre-trained language models through Chinese natural language inference, Findings of ACL-IJCNLP, 2021.
 - [23] H. Hu, Y. T. Li, Y. Patterson, Z. Y. Tian, and Y. W. Zhang, “Building a literary treebank for translation studies in Chinese,” in *Proceedings of the 19th International Workshop on Treebanks and Linguistic Theories (TLT)*, pp. 18–31, Dusseldorf, Germany, 2020.
 - [24] H. Hu, W. Li, H. Zhou, Z. Y. Tian, and Y. W. Zhang, “Ensemble methods to distinguish mainland and Taiwan Chinese,” in *Proceedings of the Sixth Workshop on NLP for Similar Languages, Varieties and Dialects at NAACL*, Minneapolis, MN, USA, 2019.
 - [25] A. Abbasi, C. S. Woo, and S. Shamshirband, “Robust image watermarking based on Riesz transformation and IT2FLS,” *Measurement*, vol. 74, pp. 116–129, 2015.
 - [26] A. Mahmood, T. Hamed, C. Obimbo, and R. Dony, “Improving the security of the medical images,” *International Journal of Advanced Computer Science and Applications*, vol. 4, no. 9, 2013.
 - [27] Q. Wen, X. F. Sun, and S. X. Wang, “The concept and application of zero watermark,” *Acta Electronica Sinica*, vol. 31, pp. 214–216, 2003.
 - [28] Q. Shen and Y. Zhao, “Perceptual hashing for color image based on color opponent component and quadtree structure,” *Signal Processing*, vol. 166, Article ID 107244, 2020.
 - [29] X. Leng, K. Ji, X. Xing, H. Zou, and S. Zhou, “Hybrid bilateral filtering algorithm based on edge detection,” *IET Image Processing*, vol. 10, pp. 809–816, 2017.
 - [30] T. Le-Tien, T. K. Huynh, P. V. Hoan, A. Tran-Hong, N. Dey, and M. Luong, “Combined Zernike moment and multiscale Analysis for tamper detection in digital images,” *Informatica: An International Journal of Computing and Informatics*, vol. 41, pp. 59–70, 2017.
 - [31] A. Kanso and N. Smaoui, “Logistic chaotic maps for binary numbers generations,” *Chaos, Solitons & Fractals*, vol. 40, no. 5, pp. 2557–2568, 2009.