Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.036904
Article

Robust Watermarking Algorithm for Medical Images Based on Non-Subsampled Shearlet Transform and Schur Decomposition

Meng Yang[1], Jingbing Li[1,2,*], Uzair Aslam Bhatti[1,2], Chunyan Shao[1] and Yen-Wei Chen[3]

[1]School of Information and Communication Engineering, Hainan University, Haikou, 570228, China
[2]State Key Laboratory of Marine Resource Utilization in the South China Sea, Hainan University, Haikou, 570228, China
[3]Graduate School of Information Science and Engineering, Ritsumeikan University, Kyoto, 5258577, Japan
*Corresponding Author: Jingbing Li. Email: jingbingli2008@hotmail.com
Received: 15 October 2022; Accepted: 10 March 2023

Abstract: With the development of digitalization in healthcare, more and more information is delivered and stored in digital form, facilitating people's lives significantly. In the meanwhile, privacy leakage and security issues come along with it. Zero watermarking can solve this problem well. To protect the security of medical information and improve the algorithm's robustness, this paper proposes a robust watermarking algorithm for medical images based on Non-Subsampled Shearlet Transform (NSST) and Schur decomposition. Firstly, the low-frequency subband image of the original medical image is obtained by NSST and chunked. Secondly, the Schur decomposition of low-frequency blocks to get stable values, extracting the maximum absolute value of the diagonal elements of the upper triangle matrix after the Schur decomposition of each low-frequency block and constructing the transition matrix from it. Then, the mean of the matrix is compared to each element's value, creating a feature matrix by combining perceptual hashing, and selecting 32 bits as the feature sequence. Finally, the feature vector is exclusive OR (XOR) operated with the encrypted watermark information to get the zero watermark and complete registration with a third-party copyright certification center. Experimental data show that the Normalized Correlation (NC) values of watermarks extracted in random carrier medical images are above 0.5, with higher robustness than traditional algorithms, especially against geometric attacks and achieve watermark information invisibility without altering the carrier medical image.

Keywords: Non-Subsampled Shearlet Transform (NSST); Schur decomposition; perceptual hashing; chaotic mapping; zero watermark

1 Introduction

As computer, network, and communication technologies have advanced, social development has entered the digital era, and medical and health care, which is closely related to human beings, has also gradually stepped into informationization and digitalization. Digitalization makes medical care

more convenient and facilitates the storage, transmission and communication of a large amount of medical data. By using computer image processing technology to improve medical imaging technology, it can effectively improve the accuracy of clinical judgment of patient's conditions. Therefore, medical images play an irreplaceable role in pathology presentation, diagnosis and treatment. However, at the same time, tampering, forgery and copying of original information have also developed, and privacy violations and security concerns abound. How to protect patient's personal information [1] is an urgent problem. Digital watermarking [2] is an effective means to solve such problems. By applying digital watermarking to the medical field, the patient's privacy, pathological data or signature can be embedded in the carrier medical image in the form of a watermark, and the watermark is encrypted to improve security [3,4]. In this way, even after the original medical image has been maliciously altered or attacked during transmission, etc., the watermark information can still be effectively extracted. Information exchange is achieved while ensuring the security of digital health care.

There have been lots of researches on digital watermarking in recent years. Digital watermarking algorithms for copyright protection should have good invisibility, high embedding volume and strong robustness [5–8]. Considering the difference of embedding domains, we can divide the digital watermark into two different kinds of watermarks, spatial domain-based and transform domain-based. At the beginning of the technology development stage, the study of digital watermarking was fundamentally based on the spatial domain, that is, adding watermark information to the spatial domain of the carrier data. For example, reference [9] shows that by embedding the processed watermark signal into the gaps of the original image, the spatial domain algorithm is simple, but once the image is attacked so that the spatial domain pixel points change, the watermark information embedded in the carrier medical image can also be corrupted. Thus, the watermark cannot be extracted well and the algorithm is less resistant to geometric attacks. Current research on digital watermarking is mainly focused on the frequency domain. Unlike the spatial domain embedding algorithm, it is implemented by embedding watermark information after transforming the carrier data, and this method does not affect the spatial pixel values of the carrier data. In addition, in the transform domain, the energy distribution is concentrated, which is helpful to ensure the invisibility of the watermark and improve its robustness of the watermark, so this algorithm is widely used. Reference [10] shows that discrete wavelet transform (DWT) has better characteristics of time domain localization and multi-resolution analysis and can better aggregate the image energy, so it is widely used. However, the robustness is not strong and still needs to be improved. Reference [11] shows that DWT first transforms the original image, then singular value decomposition (SVD) is performed on the transformed low-frequency part, and finally, the singular values extracted from the encrypted watermarked image are embedded into the singular values of the original image, the algorithm encrypts the watermark information, which enhances the security and alleviates the false alarm problem brought by SVD, but the extraction process needs to use the original image information, which is a non-blind watermark, and the practical value is not high. Reference [12] shows a fast zero watermarking algorithm based on DWT and Schur decomposition, the low-frequency subband obtained by DWT is chunked, and Schur decomposition is performed to obtain stable values and construct hash binary feature vectors. Schur decomposition avoids the false alarm problem, while the method has strong resistance to geometric attacks and belongs to zero watermarks. However, wavelet transform still has limitations for image texture feature analysis, and the effect is not as good as contourlet, shearlet, and other multiscale decomposition tools. Reference [13] shows feature extraction in the contourlet domain overcomes the limitations of conventional wavelets in scale analysis, but the ability to resist geometric attacks needs to be improved.

The algorithms above meet the requirements of digital watermarking, but their robustness needs to be improved. In this paper, we propose a novel digital watermarking algorithm for medical images with high robustness based on the Non-Subsampled Shearlet Transform (NSST) [14] and Schur decomposition. NSST is a novel multiscale geometric analysis tool, which is an improved algorithm of the shearlet transform. It has the advantages of multi-direction, translation invariance and low computational complexity. Firstly, using NSST to get the low-frequency subband image of the original medical image, which is then separated into blocks. Next, Schur decomposition is performed to obtain stable values, combined with perceptual hash binarization, and extraction of the medical image feature vector. Then the information of watermark is encrypted by logistic chaos system. Finally, the extracted feature sequences and the encrypted watermark information are exclusive OR (XOR) operations to generate the key and realize zero watermarking with third-party authentication. This paper is divided into five parts: introduction, basic theory, proposed algorithm, experiments, and analysis of results and conclusion. Experimental tests show that this algorithm outperforms the traditional wavelet domain-based zero watermarking algorithms and is more robust, especially in the case of resistance to scaling and translation attacks.

2 Basic Theory

2.1 Non-Subsampled Shearlet Transform (NSST)

Shearlet transform is the inner product of the shearlet and signal. Shearlet is a function generated by an elementary function through affine transformation, stretching, shearing and translation, etc., which can better express the characteristics of curves in two dimensions or even multi-dimensional space, solving the problem that the traditional wavelet transform cannot achieve the optimal linear error approximation. The non-Subsampled Shearlet Transform (NSST) is a novel multiscale geometric analysis tool, which is an improved algorithm of shearlet transform, it has the advantages of multi-direction, translation invariance and low computational complexity. The processing of NSST involves two essential parts: multiscale decomposition and direction localization. A non-subsampled pyramid (NSP) achieves multiscale decomposition, which ensures translation invariance and suppresses the pseudo-Gibbs phenomenon. Directional localization decomposition of images by a shear filter (SF). After the original image is decomposed by n-level NSST, one low-frequency subband image is obtained, and n high-frequency subband images with the same size and different scales are obtained. In our experiments, low-frequency image containing a large amount of contour information of the original image is usually selected for further analysis. The low-frequency subband image obtained by NSST decomposition of the medical image in this thesis, see Fig. 1 below.

2.2 Matrix Schur Decomposition

Schur decomposition, a matrix $A \in R^{n \times n}$, is decomposed into a unitary matrix $U \in R^{n \times n}$ and an upper triangular matrix $T \in R^{n \times n}$. See Eq. (1).

$$A = U \times T \times U^T \tag{1}$$

For example:

$$\begin{bmatrix} 1 & 5 & 8 \\ 2 & 6 & 9 \\ 5 & 8 & 7 \end{bmatrix} = U \times \begin{bmatrix} 17.8042 & -2.1943 & -3.6999 \\ 0 & -0.2027 & 0.7044 \\ 0 & 0 & -3.6014 \end{bmatrix} \times U^T$$

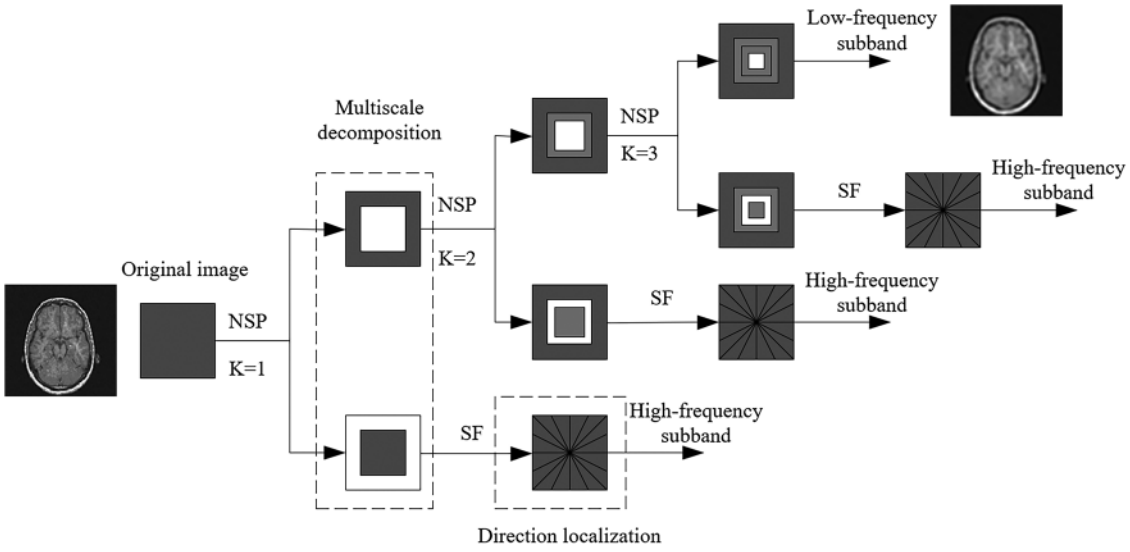

Figure 1: Low-frequency subband image obtained after NSST decomposition

The theory of matrix Schur decomposition has the following three properties, as follows:

(1) The algorithm has low time complexity. Compared to singular value decomposition (SVD) [15], the time complexity of matrix Schur decomposition as the primary, intermediate step of SVD decomposition is $O(8N^3/3)$, Schur decomposition is less than one-third as computationally intensive as SVD, which has a temporal complexity of O(11N3). This means that Schur decomposition will be used more extensively in digital watermarking.
(2) The Schur vector is scaling invariant. When matrix A is expanded by a factor of one, the Schur vector remains unchanged; what changes is that its eigenvalues are boosted by the same factor. Therefore, in the watermarking domain, Schur vectors can effectively resist scaling attacks.
(3) The perturbation is relatively stable. According to the related literature, since the grayscale image can be regarded as a real matrix, and the concern of the diagonal elements of the upper triangular matrix T obtained by the Schur decomposition of the matrix with the image matrix A is also relatively stable. The energy of the matrix after the Schur decomposition is mainly concentrated in the diagonal of the matrix T.

Because of the above properties, the Schur decomposition is a fast, stable, and low false alarm. In addition, previous literature mainly used Schur decomposition to extract the maximum element on the main diagonal of the matrix T to complete the embedding. In this paper, we construct the transition matrix by extracting the maximum of the absolute values of the main diagonal elements of the matrix T, so that the problem of wrongly selecting the largest segment of energy due to positive and negative can be avoided. Therefore, the matrix Schur decomposition theory is applied to digital watermarking, and the algorithm is highly robust and fast in operation.

2.3 Logistic Map

The encryption of images carrying private information is usually done in the form of chaotic systems to protect the information. Chaos refers to the seemingly random results that occur in a specific regular process, whose behavior is uncertain and unpredictable, which is the chaos phenomenon.

Common chaotic systems include a Logistic map [16–18], Tent [19], etc. The most common, well-known, and widely used chaotic system is the Logistic Map. It is a standard one-dimensional chaotic system, which is widely studied and used because of its simple composition structure and convenience in implementation. The composition of the Logistic Map chaotic system is formulated as follows. See Eq. (2).

$$X_{k+1} = \mu \cdot X_k \cdot (1 - X_k) \tag{2}$$

μ is the growth parameter in the above equation, $0 \leq \mu \leq 4$, and the number of iterations is K. In the case of $3.5699456 < \mu \leq 4$, the system is in a completely chaotic state, and the trajectory of the equations exhibits chaotic characteristics in this interval, the Logistic Map system was chaotic. In this paper, $\mu = 4$ and an initial value of 0.2 are taken.

3 Proposed Algorithm

To avoid this situation that when the watermark is applied directly to the spatial domain of the carrier image, the image is easily attacked to change the pixel value during transmission, sharing and saving, thus causing instability and low accuracy. In this paper, we propose a novel digital watermarking algorithm for medical images with high robustness based on NSST and Schur decomposition, which correlates the watermark information with a stable feature vector extracted in the transform domain to achieve a balance of invisibility and robustness. In addition, the algorithm is more resistant to geometric attacks than the traditional wavelet-based algorithm, which is divided into four parts: image preprocessing, image feature extraction, watermark embedding and watermark extraction.

3.1 Image Preprocessing

3.1.1 Watermark Encryption

To ensure the security and accuracy of the embedded watermark information, the watermark image needs to be preprocessed with logistic chaos encryption before embedding the watermark information. The logistic chaotic system's initial value X_0 generates the chaotic sequence X(j), which is one-dimensional, yet the watermark matrix is a two-dimensional matrix, so a dimensional transformation is required. The one-dimensional sequence generated by the chaotic system coefficient values is converted into the desired binary encryption matrix C(i, j) by the dimensional formula. Finally, the binary encryption matrix is an exclusive OR (XOR) operation with the binary watermark W(i, j) to obtain the encrypted watermark CW(i, j). See Eq. (3). In this paper, $\mu = 4$ and an initial value of 0.2 are taken. For the process of watermark encryption, see Fig. 2 below.

$$CW(i,j) = C(i,j) \oplus W(i,j) \tag{3}$$

3.1.2 Medical Image Preprocessing

In order to extract stable regions of the original medical image to improve the resistance of the algorithm to attacks, the actual medical image needs to be preprocessed before embedding the watermark information. So as to overcome the limitations of traditional wavelet transform in direction and scale analysis, this paper adopts a non-downsampling multiscale geometric analysis tool to preprocess medical images. The original image is transformed by NSST to get a low-frequency subband image that better reflects its texture information. It is then processed in chunks, and the matrix Schur decomposition is applied to each chunk to obtain its stability value.

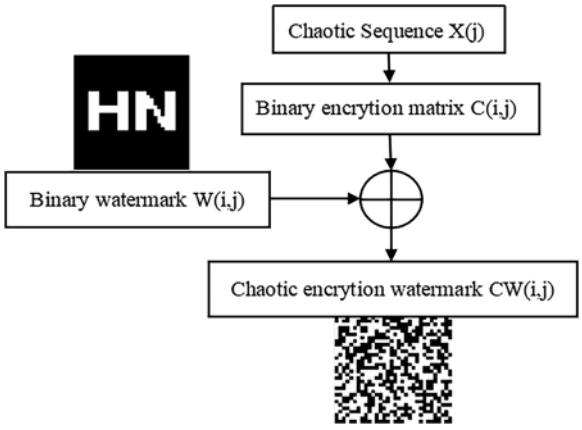

Figure 2: Encryption process of watermark

3.2 Extraction of Visual Feature Vectors of Medical Images

To chunk the preprocessed medical images and perform matrix Schur decomposition on each chunk, extract the maximum value of the absolute value of the diagonal elements of the upper triangular matrix obtained from the Schur decomposition, and construct the transition matrix from it, the mean of the matrix is compared to each element's value, creating a feature matrix by combining perceptual hashing, selecting 32 bits as the feature vector. For further validate the stability of the extracted image feature vectors, various attacks are performed on the images before extracting their feature sequences. From the experimental data, it can be seen that the image feature sequences extracted under different attacks do not change, and the correlation coefficients between them are all 1. See Table 1. Next, we further test whether the image feature sequences extracted using this algorithm can be used to distinguish between different medical images. We selected six different medical images, see Fig. 3 below, and their feature sequences were extracted separately, see Table 2, and conducted similarity tests for each of the two images, see Table 3. The experimental data show that the correlation coefficient values between the images with differences are less than 0.5, which confirms that the image feature vectors extracted by the algorithm can be used to distinguish the features of different images. Therefore, the 32-bit binary sequences extracted by this transformation can be used as visual features of medical images.

Table 1: Feature sequence coefficients under different attacks (32-bit)

Image manipulation	A sequence of coefficient signs	NC
Original image	00111000001111000111110001111100	1.00
Gaussian noise (1%)	00111000001111000111110001111100	1.00
JPEG compression (20%)	00111000001111000111110001111100	1.00
Median filter [3 × 3] (10 times)	00111000001111000111110001111100	1.00
Rotation (clockwise, 10°)	00111000001111000111110001111100	1.00
Scaling (×0.8)	00111000001111000111110001111100	1.00
Translation (7%, left)	00111000001111000111110001111100	1.00
Translation (20%, down)	00111000001111000111110001111100	1.00

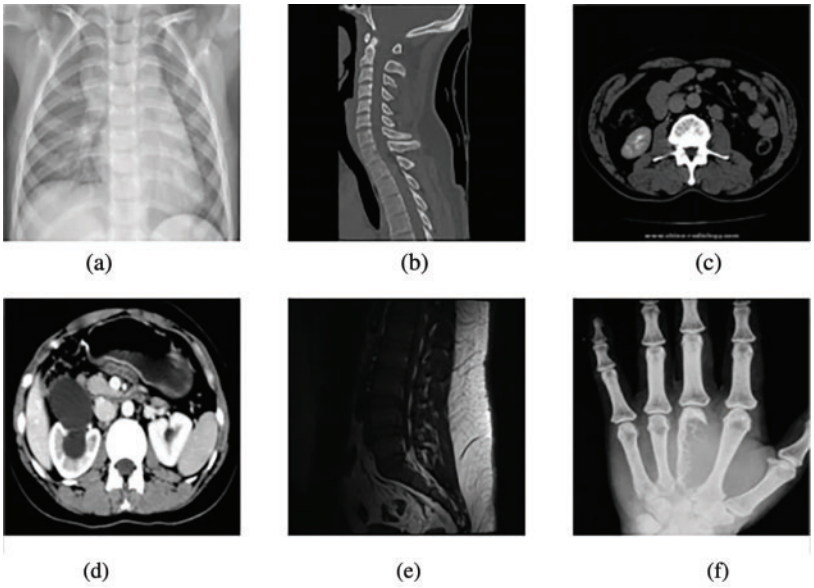

Figure 3: Six different medical images. (a) Pleural. (b) Cervical vertebra. (c) Abdomen. (d) Pancreas. (e) Lumbar spine. (f) Hand

Table 2: Extracted feature sequences of six different medical images (32-bit)

Image	Sequence of coefficient signs
(a)	00011000010110100101101000011100
(b)	00111100001111000011100000111000
(c)	00000000000000000111111001011010
(d)	00000000000000001001000011011100
(e)	00000010000001100000011000000110
(f)	00000000001001000011010001111100

Table 3: Normalized Correlation (NC) values between different images

NC	(a)	(b)	(c)	(d)	(e)	(f)
(a)	**1.0000**	0.2966	0.2660	0.1780	0.0240	−0.0086
(b)	0.2966	**1.0000**	0.0849	−0.0095	−0.3143	0.3568
(c)	0.2660	0.0849	**1.0000**	0.2956	0.1325	0.4182
(d)	0.1780	−0.0095	0.2956	**1.0000**	−0.0971	0.4587
(e)	0.0240	−0.3143	0.1325	−0.0971	**1.0000**	0.1325
(f)	−0.0086	0.3568	0.4182	0.4587	0.1325	**1.0000**

3.3 Embed Watermark

The extracted image feature sequence and the encrypted watermark information are subjected to XOR logic operation to complete the embedding of the watermark, and the key K(i, j) generated in the watermark embedding process is then stored in the third-party copyright authentication center for the extraction process of watermark information. The extraction of feature vectors and the process of implementing the zero watermark, see Fig. 4 below.

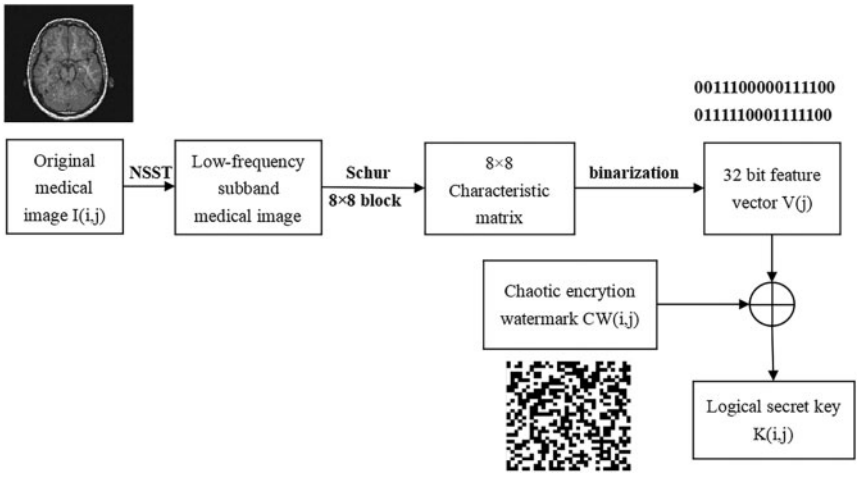

Figure 4: Feature vector extraction and watermark embedding

3.4 Extraction of Watermark

End of attack experiment, the medical image to be tested is obtained. Extracting feature sequences from attacked image and performing XOR logic operation with the key stored in the third-party authentication center at the time of embedding to get a binary logic sequence containing watermark information, see Eq. (4). And then uses logistic system to get a chaotic sequence with the same parameters to decrypt the watermarked image, see Eq. (5), and finally realizes the extraction of the watermark, see Fig. 5 below.

$$CW'(i,j) = V'(j) \oplus K(i,j) \tag{4}$$

$$W'(i,j) = CW'(i,j) \oplus C'(i,j) \tag{5}$$

4 Experiments and Analysis of Results

In this paper, the experiments were conducted in MATLAB R2017b platform, two 512×512 size medical images and a 32×32 size watermarked image were selected for the experiments (we currently use medical images that are publicly available online and medical images that come with MATLAB for research purposes), see Fig. 6 below, and the experimental effect evaluation criteria used Peak Signal to Noise Ratio (PSNR) [20,21], see Eq. (6), and Normalized Correlation (NC) [22], see Eq. (7). PSNR demonstrates the contrast between the original and attacked images. which symbolizes the strength of the attack, the smaller its value indicates the stronger and more destructive the attack. NC can more accurately use the data to objectively evaluate the similarity between images. In this experiment, the NC value represents how similar the original watermark and the watermark created from the attacked

image are to one another, which is used to measure the robustness of the algorithm. The larger its value indicates the better effect of the extracted watermark, that is, the stronger the robustness is. In our experiments, using medical images containing watermarked information, we execute conventional and geometric attacks, respectively.

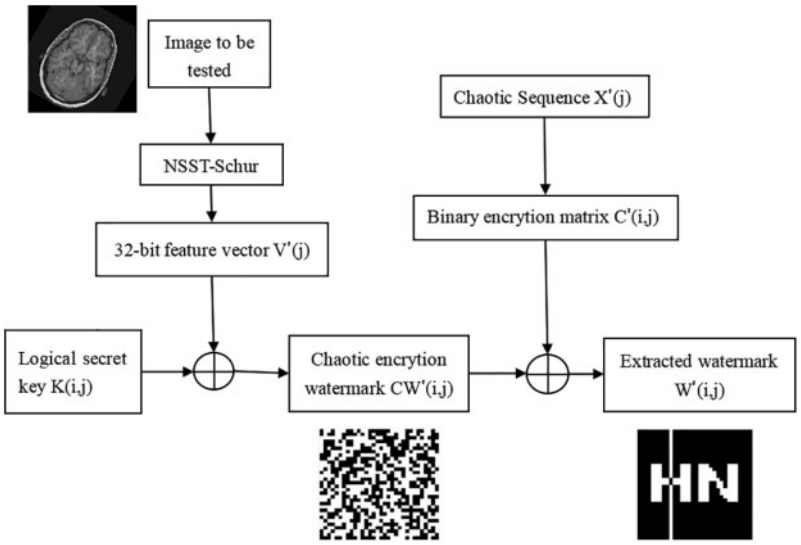

Figure 5: Extraction of watermark

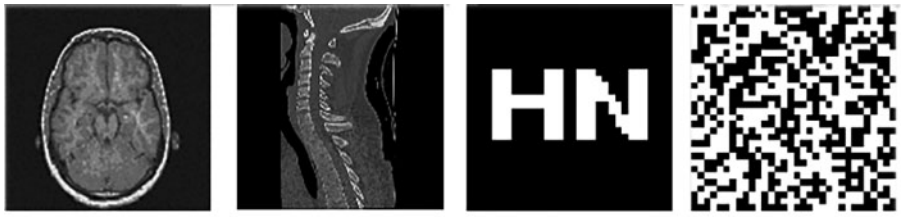

Figure 6: Medical pictures and watermarks. (a) Original medical image 1. (b) Original medical image 2. (c) Original binary watermark. (d) Encrypted watermark

$$PSNR = 10 \lg \left[\frac{MN \max_{i,j}(I(i,j))^2}{\sum_i \sum_j (I(i,j)) - I'(i,j))^2} \right] \tag{6}$$

$$NC = \frac{\sum_i \sum_j W(i,j)\, W'(i,j)}{\sum_i \sum_j W^2(i,j)} \tag{7}$$

The above equation I(i, j) denotes the grayscale value of the original medical image, and I′(i, j) means the grayscale value of the embedded watermarked image, M and N represent the number of matrix rows and columns. W(i, j) is the grayscale value of the binary watermarked image, and W′(i, j) is the gray value of the extracted binary watermarked image, and in general, when NC $\geq$ 0.5 means the two have a good correlation.

4.1 Conventional Attacks

To test the experimental effectiveness of this algorithm, we tested several common conventional attacks on carrier medical images. It can be seen that the PSNR gets smaller as the intensity of different attacks rises, the damage increases with the degree of image distortion, and the NC value eventually drops. The experimental result data showed that when the interference intensity of gaussian noise reaches 25%, the NC value is above 0.88, which is much larger than 0.5; even though the JPEG attack compression quality is only 10%, the NC value is still 1.00; under the attack of 10 repetitions of the median filter with a window size of [7 × 7], it still above 0.79, see Fig. 7 below, indicating that this algorithm is highly robust against conventional attacks. For the experimental data under conventional attacks, see Table 4.

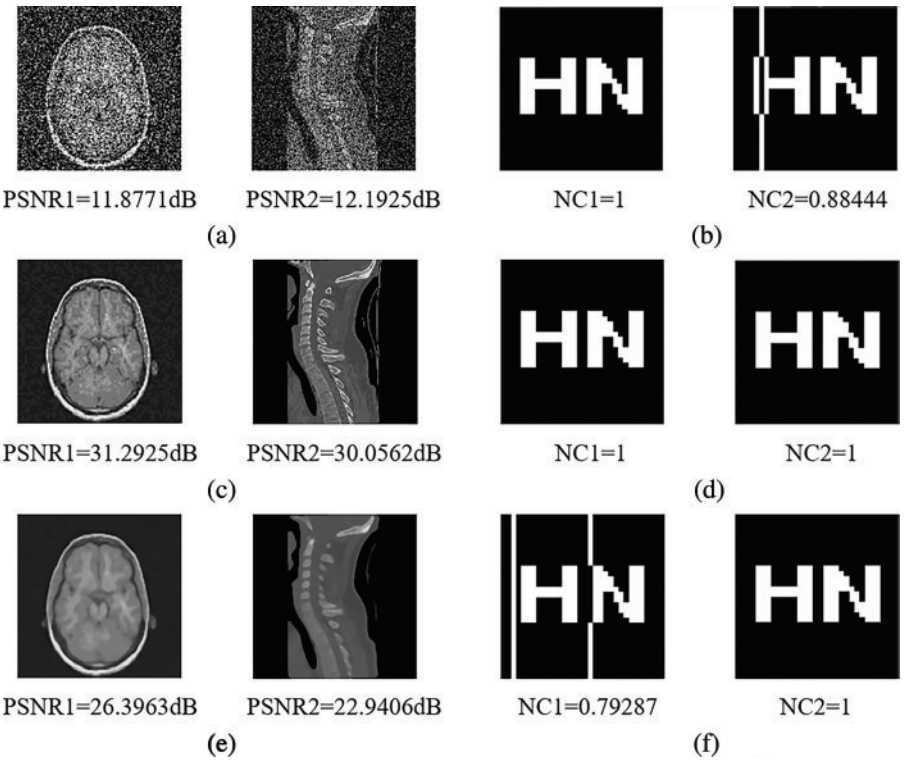

Figure 7: Under conventional attacks. (a) Gaussian noise 10%. (b) Extracted watermarks under attack a. (c) JPEG compression 10%. (d) Extracted watermarks under attack c. (e) Median filter [7 × 7] (10 times). (f) Extracted watermarks under attack e

Table 4: Data under conventional attacks

Conventional attacks	Intensity of attacks	PSNR1/dB	NC1	PSNR2/dB	NC2
Gaussian noise	1%	20.46	1.00	21.40	0.90
	10%	11.88	1.00	12.19	0.88
	25%	9.23	0.90	9.23	0.88

(Continued)

Table 4: Continued

Conventional attacks	Intensity of attacks	PSNR1/dB	NC1	PSNR2/dB	NC2
JPEG compression	10%	31.29	1.00	30.06	1.00
	20%	33.81	1.00	32.42	1.00
	40%	35.46	1.00	34.79	1.00
Median filter (10 times)	[3 × 3]	34.00	1.00	28.79	1.00
	[5 × 5]	28.56	0.88	24.56	1.00
	[7 × 7]	26.40	0.79	22.94	1.00

4.2 Geometric Attacks

The geometric attack resistance of the algorithm is significant, we tested several common geometric attacks on the images containing watermark information, and the NC value can reach above 0.69 when the rotation attack reaches 20 degrees; the NC value can reach 1.00 when the scaling attack is two times; even if the translation (down) is larger degrees, the NC value is above 0.6, see Fig. 8 below, which indicates that the algorithm has strong geometric attack resistance and can be well applied in the zero watermark algorithm. For the data under geometric attacks, see Table 5.

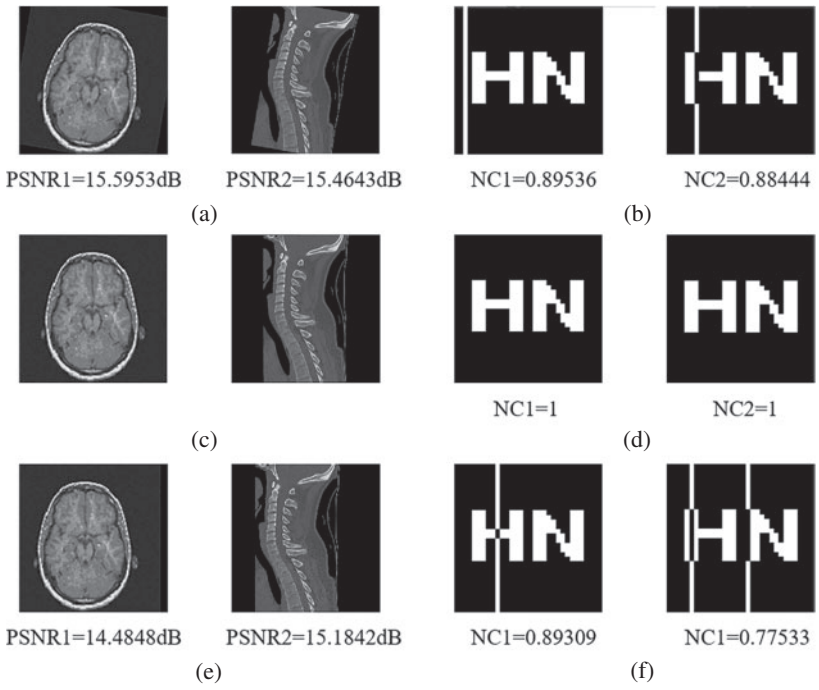

Figure 8: (Continued)

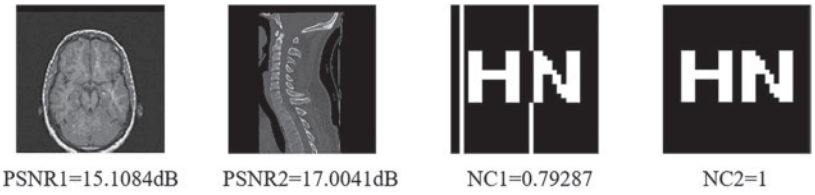

Figure 8: Under geometric attacks. (a) Clockwise rotation 10°. (b) Extracted watermarks under attack a. (c) Scaling 2 times. (d) Extracted watermarks under attack c. (e) Left translation 5%. (f) Extracted watermarks under attack e. (g) Down translation 20%. (h) Extracted watermarks under attack g

Table 5: Data under geometric attacks

Geometrical attacks	Intensity of attacks	PSNR1/dB	NC1	PSNR2/dB	NC2
Rotation (clockwise)	5°	18.00	0.90	16.91	1.00
	10°	15.60	0.90	15.46	0.88
	20°	14.60	0.79	14.24	0.69
Scaling	×0.5	-	0.88	-	1.00
	×0.8	-	1.00	-	1.00
	×2.0	-	1.00	-	1.00
Left translation	3%	15.13	1.00	16.34	0.88
	5%	14.48	0.89	15.18	0.78
	7%	14.31	0.79	14.65	0.56
Down translation	10%	16.19	0.90	18.46	1.00
	20%	15.11	0.79	17.00	1.00
	30%	14.94	0.63	16.14	1.00

To present more clearly the effectiveness of the algorithm against various common attacks. The data under six different attacks are presented on a chart and the average NC value of each attack under two additional medical images is given. See Fig. 9 below. It can be found that the average NC value of the same medical image under different attack types is all above 0.75 and applies to other medical images. It is proved that this algorithm has strong robustness against conventional and geometric attacks.

4.3 Comparison of Algorithms

Comparing this algorithm with two existing zero watermarking algorithms under the same attacks and the same medical image, we can find that although this algorithm has a slight weakness against the median filter and rotation attacks, its robustness against other attacks is significantly higher than that of the two different algorithms. Even when the attack strength is significant, the NC value is still between 0.63 and 1.00, which is stable and has a stronger resistance to attacks, see Table 6.

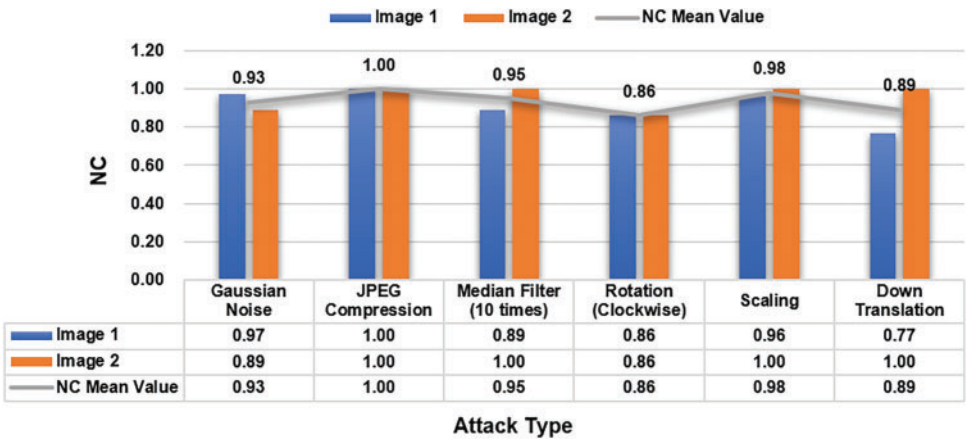

Figure 9: The average NC value of each type of attack under two different medical images

Table 6: Comparison of NC values under common attacks of three algorithms

Watermarking attacks	Intensity	KAZE-DCT [23] NC1	Gabor-DCT [24] NC2	NSST-Schur NC3
Gaussian noise	5%	0.66	0.74	**1.00**
	15%	0.37	0.54	**1.00**
	25%	0.45	0.49	**0.90**
JPEG compression	10%	0.88	0.90	**1.00**
	20%	0.88	1.00	**1.00**
	40%	1.00	1.00	1.00
Median filter (10 times)	[3 × 3]	0.71	1.00	**1.00**
	[5 × 5]	0.37	**1.00**	0.88
	[7 × 7]	0.24	**1.00**	0.79
Rotation (clockwise)	10°	0.88	**1.00**	0.90
	15°	**1.00**	0.89	0.79
	30°	**0.90**	0.64	0.71
Scaling	×0.5	0.52	0.70	**0.88**
	×0.8	0.79	0.90	**1.00**
	×2.0	0.33	0.89	**1.00**
Down translation	10%	0.51	0.71	**0.90**
	20%	0.42	0.49	**0.79**
	40%	0.54	0.20	**0.63**

To express the superiority of this algorithm more clearly, we take the average NC value of each attack and obtain a line graph of the average NC value. It can be found that this algorithm is significantly more robust against geometric attacks, especially against scaling and translation attacks. See Fig. 10 below.

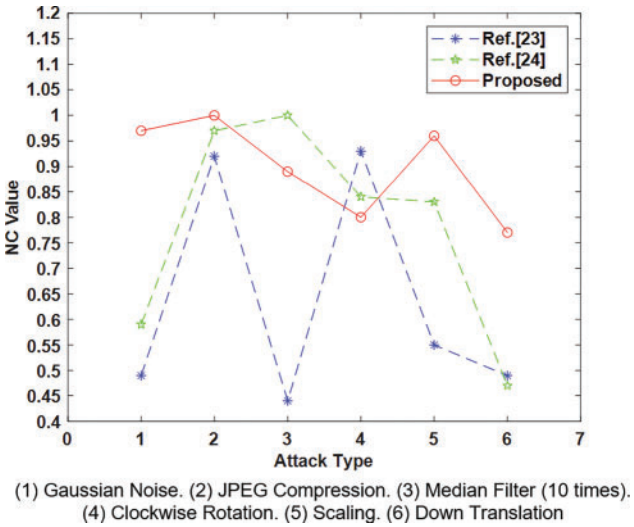

Figure 10: Comparison of the average NC values of these three algorithms under six different attacks

5 Conclusion

This paper proposes a robust watermarking algorithm for medical images based on NSST and Schur decomposition. We combine chaotic encryption and zero-watermarking techniques to improve security and invisibility significantly. Firstly, to reasonably express the texture information of the medical image, the NSST is applied to the medical image to achieve multiscale and multi-directional decomposition of the image. Then, using Schur decomposition, the stable values of the low-frequency subband are obtained, combined with perceptual hash binarization to extract the medical image feature sequences. Finally, the extracted feature sequences and the encrypted watermark information are XOR operations to generate the key and realize zero watermarking with third-party authentication. Combined with a large amount of experimental data research found that this algorithm can effectively resist various types of attacks that often appear on the Internet and in our daily lives, with significant robustness advantages, especially for geometric attacks. To further improve the algorithm, we will combine deep learning methods to extract medical image features for better results.

Acknowledgement: Thanks to the editors and reviewers for suggestions for improving the manuscript.

Funding Statement: This work was supported in part by the Natural Science Foundation of China under Grants 62063004, the Key Research Project of Hainan Province under Grant ZDYF2021SHFZ093, the Hainan Provincial Natural Science Foundation of China under Grants 2019RC018 and 619QN246, and the postdoctoral research from Zhejiang Province under Grant ZJ2021028.

Conflicts of Interest: The authors declare they have no conflicts of interest to report regarding the present study.

References

[1] H. Shi, Y. Wang, Y. N. Li, Y. G. Ren and C. Guo, "Region-based reversible medical image watermarking algorithm for privacy protection and integrity authentication," *Multimedia Tools and Applications*, vol. 80, pp. 24631–24667, 2021.

[2] Y. L. Li and C. K. Chen, *Research on Digital Watermarking Algorithm for Medical Images*. Tianjin: Tianjin University of Technology, 2018.

[3] X. Sun and Y. Yao, *R esearch of Image Encryption and Decryption Algorithm Based on Digital Watermarking*. Wuhan: Central China Normal University, 2020.

[4] Y. P. Cao, F. Yu and Y. M. Tang, "A digital watermarking encryption technique based on FPGA cloud accelerator," *IEEE Access*, vol. 8, pp. 11800–11814, 2020.

[5] D. K. Li, Y. W. Chen, J. B. Li, L. Cao, U. A. Bhatti *et al.,* "Robust watermarking algorithm for medical images based on AKAZE-DCT," *IET Biometrics*, vol. 11, no. 6, pp. 534–546, 2022.

[6] S. Y. Sun and W. J. Liu, *Research on Zero Watermarking Algorithm with Resistance to Geometric Attacks*. Fuxin: Liaoning University of Engineering and Technology, 2018.

[7] W. X. Zhang, J. B. Li, U. A. Bhatti, M. X. Huang, J. X. Ma *et al.,* "Robust zero-watermarking algorithm for medical images based on K-means and DCT," *International Journal of Wireless and Mobile Computing (IJWMC)*, vol. 23, no. 2, pp. 163–172, 2022.

[8] M. S. Sheng, J. B. Li and J. Liu, "Robust zero-watermarking algorithm for medical images based on Hadamard-DWT-DCT," *International Journal of Wireless and Mobile Computing (IJWMC)*, vol. 23, no. 2, pp. 183–192, 2022.

[9] C. H. Yu, "On the application of digital watermarking technology in image encryption," *Journal of Huaiyin Institute of Technology*, vol. 18, no. 5, pp. 57–62, 2009.

[10] D. L. Cui, "Zero watermarking technique for digital images based on DWT," *Journal of Chengdu Information Engineering Institute*, vol. 3, pp. 306–308, 2007.

[11] Z. J. Xiong and L. Wang, "Improved reference watermarking scheme in DWT-SVD domain," *Computer Engineering and Applications*, vol. 50, no. 7, pp. 75–79, 2014.

[12] W. J. Liu, S. Y. Sun and H. C. Qu, "Fast zero watermarking algorithm for Schur decomposition," *Computer Science and Exploration*, vol. 13, no. 3, pp. 494–504, 2019.

[13] X. Q. Wu, J. B. Li, R. Tu, J. R. Cheng, U. A. Bhatti *et al., Research on Digital Watermarking Algorithm of Medical Images Based on Contourlet Transform*. Haikou: Hainan University, 2020.

[14] F. F. Jiang, J. Y. Liu, T. Li, M. J. Luo and D. Li, "An introduction to zero watermarking algorithm based on NSST-DCT," *Heilongjiang Science and Technology Information*, vol. 13, pp. 121, 2017.

[15] C. Liu, J. G. Sun, Y. K. Zhang and W. J. Liu, "Robust zero watermarking algorithm based on SVD," *Journal of Liaoning University of Engineering and Technology (Natural Science Edition)*, vol. 38, no. 4, pp. 372–376, 2019.

[16] A. Kamrani, K. Zenkouar and S. Najah, "A new set of image encryption algorithms based on discrete orthogonal moments and Chaos theory," *Multimedia Tools and Applications*, vol. 79, pp. 20263–20279, 2020.

[17] B. Vijayakumar and S. Khond, "Wavelet based reversible image watermarking with logistic encryption for health informatics systems," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, pp. 3567–3570, 2019.

[18] W. H. Wang and Y. L. Liu, "Research on image encryption algorithm based on two-dimensional logistic chaotic sequence," *Journal of Changchun University of Science and Technology (Natural Science Edition)*, vol. 33, no. 4, pp. 111–113, 2010.

[19] Y. L. Liu, J. B. Li, J. Liu, J. R. Cheng, J. L. Liu *et al.,* "Robust encrypted watermarking for medical images based on DWT-DCT and tent mapping in encrypted domain," *Artificial Intelligence and Security*, vol. 11633, pp. 584–596, 2019.

[20] M. K. Feng, S. M. Zhao and C. Xing, "A PSNR image evaluation method based on visual characteristics," *Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition)*, vol. 35, no. 4, pp. 33–38, 2015.

[21] W. Dong and H. X. Bie, *Research on Image Quality Evaluation Method Based on Shearlet Transform*. Beijing: Beijing University of Posts and Telecommunications, 2021.
[22] Z. Cao, "Exploring the intrinsic relationship of covariance, correlation coefficient, and regression coefficient," *China Collective Economy*, vol. 25, pp. 76–78, 2022.
[23] C. Zeng, J. Liu, J. B. Li, J. R. Cheng, J. J. Zhou *et al.,* "Multi-watermarking algorithm for medical image based on KAZE-DCT," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–9, 2022.
[24] X. L. Xiao, J. B. Li, J. Liu, Y. X. Fang, C. Zeng *et al.,* "A Zero-watermarking algorithm for medical images based on Gabor-DCT," *Cyberspace Safety and Security (CSS)*, vol. 12653, pp. 144–156, 2020.