EURASIP Journal on Wireless Communications and Networking

RESEARCH

Open Access

Robust watermarking algorithm for medical images based on log-polar transform

Tianfu Li[1], Jingbing Li[1,3*], Jing Liu[2], Mengxing Huang[1,3], Yen-Wei Chen[4] and Uzair Aslam Bhatti[5]

*Correspondence: jingbingli2008@hotmail.com
[1] School of Information and Communication Engineering, Hainan University, Haikou, China
Full list of author information is available at the end of the article

Abstract

In the information age, network security has gradually become a potentially huge problem, especially in the medical field, it is essential to ensure the accuracy and safety of images, and patient information needs to be included with minimal change. Combined log-polar transform (LPT) and discrete cosine transform (DCT), a novel robust watermarking algorithm for medical images, is proposed. It realized the lossless embedding of patient information into medical images. In the process of feature extraction and watermark embedding, the proposed algorithm reflects the characteristics of LPT, scale invariance and rotation invariance, and retains the advantages of DCT's ability to resist conventional attacks and robustness. As it adopts zero-watermarking embedding technology, it solves the defects caused by the traditional watermark embedding technology to modify the original image data and guaranteed the quality of medical images. The good experimental results show the effectiveness of this algorithm.

Keywords: Log-polar, DCT, Medical images, Watermarking, Robustness

1 Introduction

In the information age, network security has gradually become a potentially huge problem. The main research of network security is the prevention and control of computer viruses and system security. With the increasing expansion and popularization of computer networks today, the requirements for computer security are higher and involve a wider range of areas. It is not only required to prevent viruses, but also to improve the system's ability to resist illegal hackers from outside, and to improve the confidentiality of remote data transmission. Specifically, network security mainly refers to: protecting personal privacy; controlling access to network resources with restricted permissions; ensuring the confidentiality of trade secrets transmitted on the network, the integrity and authenticity of data; controlling unhealthy content or Remarks that endanger social stability; avoid the leakage of state secrets, etc. This shows the importance of network security [1].

With the rapid development of information technology, the demand and use of telemedicine in the medical field are increasing, and increasingly medical images and information are transmitted via Internet. For medical images, it often corresponds to the important information of each patient, which cannot be easily modified, and the leakage of patient private information must also be avoided. Therefore, how to implement information protection for medical images has become an important research topic.

Information hiding is an ancient subject, but its application in digital media still has great potential for development. The concept of information hiding is different from that of information encryption. Information encryption is the use of a certain algorithm to encrypt information and finally form a ciphertext that is difficult to crack. Information hiding technology does not affect people's reading of digital media, but protects hidden data from being discovered. Hence, information hiding technology must have certain immunity, that is, in normal digital signal processing, such as linear transform, Fourier transform, and data compression algorithms, to ensure that the hidden information is not damaged [2]. As an effective copyright protection technology, it has been widely studied and applied in the fields of digital communications and confidentiality. Digital watermarking technology is a new topic in the field of information hiding, which has received extensive attention from researchers in recent years.

Digital watermarking technology is a technology that can embed specific digital signals into digital products to protect the copyright or integrity of digital products. Nowadays, with its robustness, invisibility, and encryption characteristics, digital watermarks have gradually replaced traditional watermarks and are widely used in many fields to ensure the security and confidentiality of multimedia information dissemination. The basic idea of digital watermarking technology is to embed private information or user information in digital media to achieve the purpose of digital copyright information protection, digital product certification, and infringement tracking. Now, digital watermarking technology has become important way to ensure information security and implement copyright protection in the Internet [3]. In the medical field, digital watermarking algorithms applied to medical images can protect the privacy of patients and prevent medical data from being tampered with, and provide a guarantee for the safety and accuracy of medical images.

However, although the existing watermarking algorithms have a better defense against signal processing attacks such as image compression and filtering, they are less effective in dealing with geometric attacks such as rotation, cropping, and scaling [4]. At present, there are few researches on digital watermarking algorithms for medical images, and there are fewer research results on watermarking algorithms for medical data resistant to geometric attacks. Therefore, it is of great significance to research on digital watermarking algorithms that can deal with geometric attacks.

This paper proposes a robust watermarking method for medical images based on LPT-DCT. Its general framework is as follows: first perform LPT on the medical image, then perform DCT on the corresponding matrix of the obtained LPT image, and then extract a resistance from the DCT low-frequency coefficients. The visual feature vector of the texture image of geometric attack, and the organic combination of watermarking technology with chaotic encryption, Hash function and "third-party concept" to realize the resistance to geometric attacks and conventional attacks of digital watermarking. By combining the feature vector of medical image, cryptography, hash function and zero-watermark technology, it makes up for the shortcomings of traditional digital watermarking methods that cannot protect the medical image itself. It has strong robustness and invisibility. At the same time protect the patient's private information and medical image data security.

2 Methods

In this section, we will explain our proposed algorithm. At present, most medical image watermarking algorithms have poor resistance to geometric attacks. The main reason is that people embed digital watermarks in pixels or transform coefficients. The slight geometric transformation of medical images often results in large changes in pixel values or transform coefficient values. This will make the embedded watermark easily attacked. If the visual feature vector that reflects the geometric characteristics of the medical image can be found, then when the image undergoes a small geometric transformation, the visual feature value of the image will not have obvious mutations [5].

To solve this problem, we combined the LPT transform with better rotation invariance and the DCT transform to obtain a feature vector which can resist geometric attacks. From the experimental data, we found that when performing a conventional geometric transformation on a medical image, the magnitude of the DCT lowIF coefficient value may have some changes, but the coefficient sign remains unchanged. According to this rule, we first perform log-polar coordinate transformation (LPT) on medical images, and then perform discrete cosine transform (DCT) on the corresponding matrix of the obtained LPT image. After that, we extract a geometric attack-resistant texture image from the DCT low-frequency coefficient visual feature vector, and organically combine watermarking technology with chaotic encryption, hash function and "third-party concepts" to achieve digital watermarking resistance to geometric and conventional attacks [6]. The proposed algorithm will be explained in detail in the following subsections.

2.1 LPT (log-polar transform) algorithm

The log-polar transform (LPT) is derived from the simulation research on the mapping relationship of the retinal visual cortex. Its principle is to transform the image in the rectangular coordinate system to the logarithmic polar coordinate system through the method of nonuniform sampling, thereby converting the rectangular coordinate system, scale and rotation changes in the middle are transformed into translation changes in the log-polar coordinate system. LPT is similar to the human visual mechanism. The sampling rate at the center of the image is high, which ensures the high resolution of the central area, while the sampling rate of the peripheral area is low, which can ensure that the main area is effectively expressed while reducing the amount of image data, thereby reducing matching calculation amount [7]. Figure 1 shows the sketch map for Log-polar transform.

Given a two-dimensional image, it can be expressed as (x, y) in a rectangular coordinate system, and as (ξ, ψ) in a logarithmic polar coordinate system, then (ξ, ψ) and (x, y) Can be calculated by the following mapping relationship:

$$\rho = \sqrt{x^2 + y^2},\ \theta = \arctan\left(y/x\right) \tag{1}$$

$$\xi = \log\ \rho,\ \psi = \theta \tag{2}$$

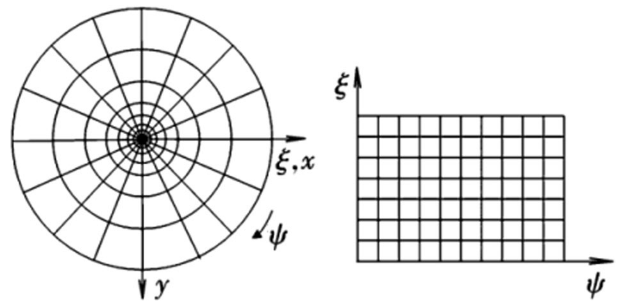

Fig. 1 Sketch map for Log-polar transform

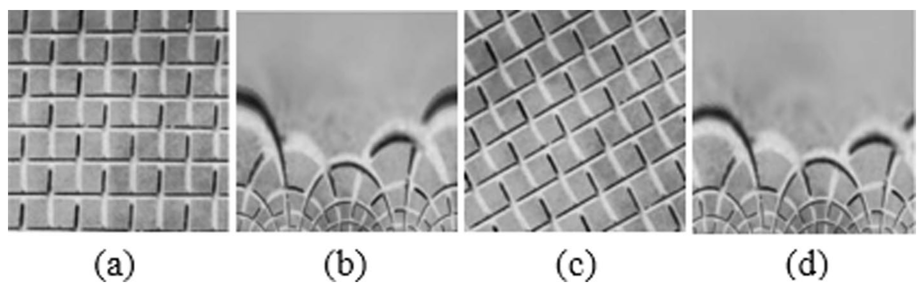

Fig. 2 Results after Log-polar Transform. **a** Original image, **b** image after LPT, **c** image after rotating 30°, **d** image after rotating 30°and LPT

The ξ and ψ calculated by formula (2) are usually not integers, and the range of ξ obtained by images of different resolutions is inconsistent, so formula (2) needs to be corrected:

$$\xi = \left(k_\xi \ \log \rho\right], \ \psi = (k_\theta \theta] \tag{3}$$

where $k_\xi = M/\log$ and $k_\theta = N/360$ are represent correction factors, which extend the range of ξ and ψ to the set image resolution $(M \times N)$ in the log-polar coordinate system. The resolution of the transformed image adopted in this paper is 256 pixels × 256 pixels, and $[x]$ represents the smallest integer not less than x. The results after Log-polar Transform are as Fig. 2 shows.

The gradient value in the horizontal direction of the transformed image is equivalent to the gradient value in the tangent direction of the original image, the gradient value in the vertical direction is equivalent to the radial gradient value of the original image, and the main gradient direction represents the direction in which the radial gradient changes most drastically in the original image [8]. It usually has strong stability, so taking the main gradient direction as the reference direction also has strong stability. Since LPT is an image integration operation, it is not sensitive to image noise. Therefore, using the transformed image gradient value as a feature can significantly improve the robustness of the gradient against image noise; at the same time, LPT is aimed at the averaging the operation of image blocks, and uses gradient values as features to calculate the trend of changes between adjacent image blocks, which can effectively reduce the impact of linear and non-linear illumination changes [9].

2.2 DCT (discrete cosine transform) algorithm

Discrete cosine transform (DCT) is a kind of real number domain transform, which is often applied to the linear transform of digital signal processing, which can make the correlation characteristics of two-dimensional signal be well reflected [10]. After DCT transform, the energy is concentrated, and it has good energy compression and decompression. Related capabilities. The calculation speed is relatively fast, and it is widely used in the fields of digital signal compression and image compression. At the same time, the JPEG compression standard of images is based on the DCT transformation, and the watermarking algorithm's anti-attack JPEG compression ability is greatly enhanced, so the DCT domain transformation is favored in digital watermarking technology [11].

The two-dimensional discrete cosine sine transform (DCT) formula is as follows:

$$F(u,v) = c(u)c(v)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f\left(x,y\right)\cos\frac{\pi(2x+1)u}{2M}\cos\frac{\pi\left(2y+1\right)v}{2N} \tag{4}$$

The two-dimensional inverse discrete cosine transform (IDCT) formula is:

$$f\left(x,y\right) = \sum_{u=0}^{M-1}\sum_{v=0}^{N-1} c(u)c(v)F(u,v)\cos\frac{\pi(2x+1)u}{2M}\cos\frac{\pi\left(2y+1\right)v}{2N} \tag{5}$$

where x, y represent sampling values in the spatial domain; u, v represent sampling values in the frequency domain, and digital images are usually represented by a square pixel matrix, here, $M=N$.

After DCT transform, most of the energy of the image is mainly concentrated in the low frequency part, which will have high compression coding efficiency. The statistical significance of histogram shows that the coefficient values are concentrated near 0, the dynamic range is small, and the DCT coefficients are available. Fewer quantization bits are used to indicate that the watermark information is embedded in the medium and low frequency part of the carrier image, which can better resist JPEG compression. For example, compared with the spatial domain, it can embed more information and has better concealment, and its robustness is also relatively high. The performance of the algorithm combined with the human visual model can be further improved.

2.3 Embedding and encryption scheme

Choose a meaningful binary text image as the watermark embedded in the medical image, denoted as $W=\{w(i,j) \mid w(i,j)=0,\ 1;1\leq i\leq M1,1\leq j\leq M2\}$. Meanwhile, we select a 256 pixels × 256 pixels medical gray-scale image as the original medical image, denoted as $I(i,j)$. $W(i,j)$ and $I(i,j)$ respectively represent the pixel gray value of the watermark and the original medical image [12]. Figure 3 shows the embedding diagram of watermarking.

(1) Perform Log-Polar Transform on the original medical image $I(i,j)$: Transform the image from the Cartesian coordinate system to the polar coordinate system through the polar coordinate transformation, and then take the logarithmic transformation

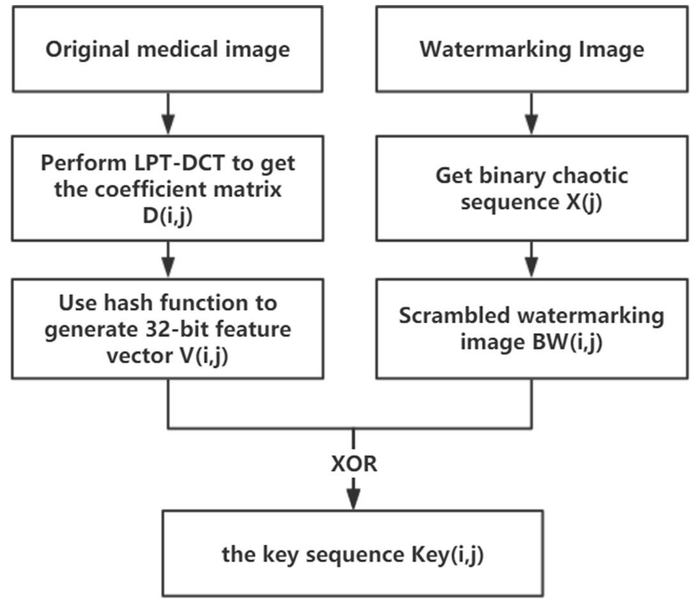

Fig. 3 Embedding diagram of watermarking

to the logarithmic polar coordinate system to obtain the LPT transformed image Matrix $L(i,j)$;

(2) Generate the feature vector of medical images: Perform DCT transformation on the corresponding matrix of LPT to obtain the coefficient matrix $D(i,j)$, and select 4×8 modules in the low-frequency region of $D(i,j)$ to form a new matrix $E(i,j)$; then use the hash function to generate the feature binary sequence $V(i,j)$ of the 32-bit medical image, which is the feature vector of the corresponding medical image.

(3) Obtain a binary chaotic sequence: Generate a chaotic sequence $X(j)$ according to the initial value $\times$ 0. In this experiment, the initial value of the chaotic coefficient is set to 0.2, the growth parameter is 4, and the number of iterations is 32;

(4) Obtain the chaotically encrypted watermark: Sort the median value of the chaotic sequence $X(j)$ from small to large, and then scramble the position space of the watermark pixels according to the position changes before and after each value in $X(j)$ is sorted, and get the scrambled watermark $\mathrm{BW}(i, j)$.

(5) Embed the watermark into the medical image: XOR the feature vector $V(i,j)$ and the encrypted watermark $\mathrm{BW}(i, j)$ bit by bit, and get the logical key $\mathrm{Key}(i,j)$ at the same time, which is after it is used when extracting the watermark. By applying $\mathrm{Key}(i,j)$ as a key to a third party, the ownership and use rights of the original medical image can be obtained, to achieve the purpose of protecting the medical image.

2.4 Extraction and decryption scheme

(1) Extract the feature vector of the medical image $I'(i,j)$: Perform LPT processing on the medical image to be tested, obtain the corresponding matrix of LPT and then perform DCT transform to obtain the coefficient matrix $D'(i,j)$, select 4×8 of the

coefficients The module obtains the visual feature sequence $V'(i,j)$ of the medical image to be tested through the hash function, and then performs the process of the feature vector $V'(i,j)$ of the encrypted image to be tested and the logical key Key(i,j) The exclusive OR operation will extract the encrypted watermark BW$'(i,j)$;

$$\mathrm{BW}'(i,j) = \mathrm{Key}(i,j) \oplus V'(i,j) \tag{6}$$

This algorithm only needs the key Key(i,j) when extracting the watermark, and does not require the participation of the original image [13]. It is a zero-watermark extraction algorithm.

(2) Restore the extracted encrypted watermark: Use the same method as the watermark encryption to obtain the same binary chaotic matrix $X(j)$, and sort the values in $X(j)$ that have been obtained in the order from small to large; then, restore the position space of the pixels in the watermark according to the position changes before and after the various values in it are sorted to obtain the restored watermark $W'(i,j)$;

(3) Confirm the embedded watermark information: By calculating the correlation coefficient NC of $W(i,j)$ and $W'(i,j)$, determine the ownership and related information of the medical image. Figure 4 shows the extraction diagram of watermarking.

3 Results and discussion

To evaluate the effect of watermarking, it is necessary to conduct a simulated attack on the watermarking system to test its performance. Various types of attacks are inevitable in the actual application of a watermarking system. To comprehensively evaluate the performance of watermarking, this paper introduced several common image processing methods as simulation attack methods.

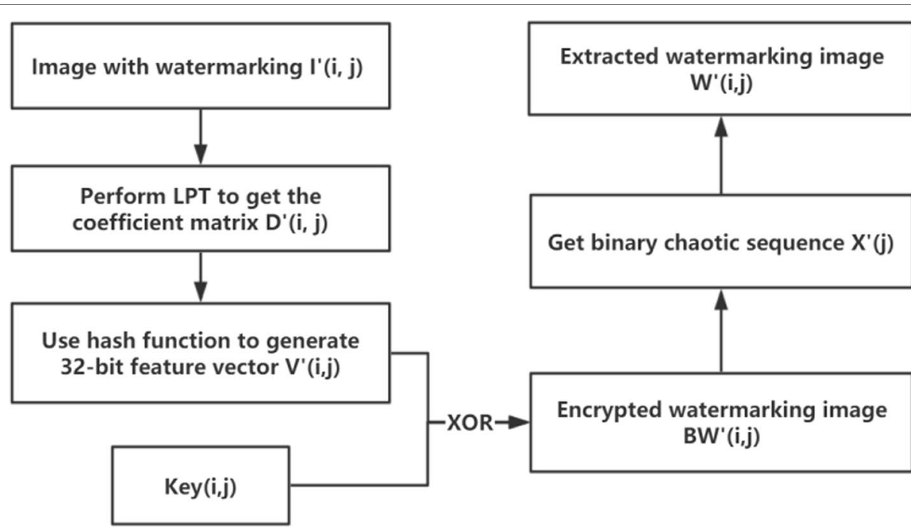

Fig. 4 Extraction diagram of watermarking

Fig. 5 Experimental images. **a** Original image, **b** Original watermark, **c** Scrambled watermark, **d** Extracted watermark

In the simulation experiment, we chose a 256 pixels × 256 pixels brain slice medical image $I(i,j)$ as the experimental test object, as shown in Fig. 5a, and chose a 32 pixels × 32 pixels binary value as the original watermark, as shown in Fig. 5b. The watermark after chaos scrambling through Logistic Map is shown in Fig. 5c. It can be clearly seen that the watermark image has undergone great changes, and the security is improved. Figure 5d is the watermark extracted without interference. We can see when NC = 1.00, and the watermark can be extracted accurately.

We first perform LPT-DCT transform on the original image. Considering the robustness and the capacity of one-time embedding of the watermark, we take 32 coefficients, that is, a 4 × 8 module. Set the initial value of the chaos coefficient to 0.2, the growth parameter to 4, and the number of iterations to 32. The simulation experiment was carried out on the Matlab 2019b platform. Compared with the traditional DCT algorithm, the calculation speed did not drop significantly. After detecting $W'(i,j)$ through the watermark algorithm, we judge whether there is a watermark embedded by calculating NC (Normalized Cross Correlation). When the value is closer to 1, the similarity is higher, to judge the robustness of the algorithm sex. The distortion degree of the picture expressed by PSNR (Peak Signal to Noise Ratio). When the PSNR value is larger, the distortion degree of the picture is smaller. Then, we use specific experiments to judge the anti-conventional attack ability and the anti-geometric attack ability of the digital watermarking method.

Then we chose Gaussian noise, JPEG compression, median filtering, rotation and moving down to test the attack effect of the watermark, and compared with the traditional DCT watermarking algorithm [14]. The extracted watermarking images are shown in Fig. 6 and the experimental results are shown in the table below (Table 1).

From the experimental data, we can see that the watermark based on LPT-DCT has shown good robustness in resisting a variety of attacks. The extracted watermark image is basically undamaged, especially in the face of rotation attacks, the watermark can still be restored relatively well when the image is rotated by 45 degrees. This is due to the good rotation invariance of the LPT algorithm, and it has better stability than the watermark based on the DCT algorithm.

4 Conclusion

This paper proposed a novel robust watermarking algorithm for medical images. The experimental data showed that the proposed algorithm based on LPT-DCT can stably resist attacks of various strengths in the face of traditional attacks, and its overall

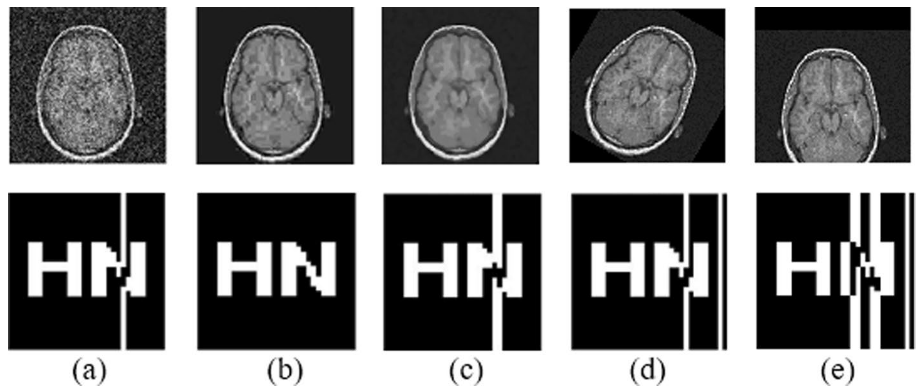

Fig. 6 The attacked images and extracted watermark. **a** Gaussian Noise 10%, **b** JPEG Compression 10%, **c** Median Filtering 5 × 5, **d** Rotation 30°, **e** moving down 10%

Table 1 Results of different algorithms' comparison

Attack methods	Intensity	LPT-DCT(ours)		DCT	
		PSNR(dB)	NC	PSNR(dB)	NC
Gaussian noise	10%	11.90	0.90	12.40	0.60
	20%	9.77	0.89	7.97	0.64
	30%	8.13	0.82	5.97	0.55
Compression	50%	35.46	1.00	26.52	1.00
	10%	29.05	1.00	20.98	0.74
	5%	26.40	1.00	17.61	0.82
Median filtering	3 × 3	28.92	0.94	21.85	0.91
	5 × 5	24.63	0.89	18.28	0.72
	7 × 7	22.25	0.84	16.99	0.63
Rotation	15°	14.61	0.92	12.70	0.78
	30°	14.16	0.90	11.90	0.63
	45°	13.63	0.85	11.58	0.51
Moving down	5%	14.77	0.94	12.33	0.81
	10%	14.43	0.74	11.69	0.76
	15%	13.78	0.61	11.21	0.65

robustness is improved, especially in resisting rotation attacks. Applying it to medical images and encrypting the original medical images can hide the content of the original medical images and effectively protect the privacy and information security of patients.

Digital watermarking is an emerging technology, which involves communication technology, information and coding theory, image and signal processing and other disciplines. Although it has developed rapidly in recent years, it is still in the exploratory stage so far. A mature theoretical system and a unified evaluation standard have not yet been formed. Many problems require further research, and the existing technology also needs to be further improved and improved. At present, the algorithm proposed in this paper still has many shortcomings. The next step will be mainly from the following aspects:

1. Research other transformation methods of the carrier image to find the ideal watermark embedding position. At the same time, the communication model and signal processing technology are combined to realize the embedding of multiple watermarks, and realize the blind detection of watermarks, and improve the invisibility and robustness of the watermarking system.
2. Further study the perception model of the human visual system, qualitatively and quantitatively analyze the texture information and edge information of the image, find a better analysis method of image complexity, and fully apply the visual masking effect of the human visual system to the digital watermarking algorithm.
3. At present, artificial intelligence, big data, and other technologies are developing rapidly. In the future, we can try to consider incorporating algorithms such as neural networks into the watermarking model, and strive to establish a robust system that can be applied to smart medical care, dynamic recognition, etc. Important occasions.

Abbreviations
DCT: Discrete cosine transform; LPT: Log-polar transform; NC: Normalized cross correlation; PSNR: Peak signal to noise ratio.

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

Authors' contributions
MH and Jingbing.L contributed to the conception of the study. TL and Jingbing.L performed the experiment. Jing.L and UAB contributed significantly to analysis and manuscript preparation. TL performed the data analyses and wrote the manuscript. YC helped perform the analysis with constructive discussions. All authors read and approved the final manuscript.

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

Availability of data and materials
All data generated or analysed during this study are included in this published article.

Declarations

Competing interests
The authors declare that they have no competing interests.

Author details
[1]School of Information and Communication Engineering, Hainan University, Haikou, China. [2]Research Center for Healthcare Data Science, Zhejiang Lab, Hangzhou, China. [3]State Key Laboratory of Marine Resource Utilization in the South China Sea, Hainan University, Haikou, China. [4]Graduate School of Information Science and Engineering, Ritsumeikan University, Kusatsu, Japan. [5]School of Geography (Remote Sensing and GIS Lab), Nanjing Normal University, Nanjing, China.

Received: 15 October 2021 Accepted: 10 March 2022
Published online: 25 March 2022

References

1. M. Begum, M.S. Uddin, Digital image watermarking techniques: a review. Information **11**, 110 (2020)
2. N. Agarwal, A.K. Singh, P.K. Singh, Survey of robust and imperceptible watermarking. Multim. Tools Appl. **78**, 8603–8633 (2019)
3. A.K. Singh, B. Kumar, M. Dave, A. Mohan, Robust and imperceptible spread-spectrum watermarking for telemedicine applications, in Proceedings of the National Academy of Sciences, India Section A: Physical Sciences (2015), pp. 1–7

4. V.M. Potdar, S. Han, E. Chang, A survey of digital image watermarking techniques, in Proceedings of IEEE International Conference on Industrial Informatics (2005), pp. 709–716
5. K. Alavi, F. Taher, H. Al-Ahmad, A new multi watermarking algorithm for medical images using DWT and hash functions, in International Conference on Innovations in Information Technology (IIT) (2015), pp. 230–234
6. Sato Y, Bao Y, High speed and high precision facial recognition using log-polar transformation, in 2018 International Conference on Sensor Networks and Signal Processing. Xi'an, China:IEEE (2018), pp. 375–381
7. Qu. Zhiguo, Z. Cheng, M. Luo, W. Liu, A robust quantum watermark algorithm based on quantum log-polar images. Int. J. Theor. Phys. **56**, 3460–3476 (2017)
8. G. Wolberg, S. Zokai, Robust image registration using log-polar transform, in Proceedings 2000 International Conference on Image Processing (Cat. No.00CH37101), vol.1 (2000), pp. 493–496
9. N.C. Sy, H.H. Kha, N.M. Hoang, An efficient robust blind watermarking method based on convolution neural networks in wavelet transform domain. Int. J. Mach. Learn. Comput. **10**, 675–684 (2020)
10. H. Wang, Research on digital image blind watermarking algorithm based on DCT domain. Mod. Vocat. Educ. **14**, 76–77 (2016)
11. S. Roy, Pal AK A blind DCT based color watermarking algorithm for embedding multiple watermarks. AEU Int. J. Electron. Commun. **72**, 149–161 (2017)
12. D. Rajani, P.R. Kumar, An optimized blind watermarking scheme based on principal component analysis in redundant discrete wavelet domain. Signal Process **172**, 107556.1-107556.9 (2020)
13. S. Kumar, B. Panna, R.K. Jha, Medical image encryption using fractional discrete cosine transform with chaotic function. Med. Biol. Eng. Comput **57**, 2517–2533 (2019)
14. Y.-L. Liu, J.-B. Li, DCT and logistic map based multiple robust watermarks for medical image. Appl. Res. Comput. **30**(11), 3430–3433 (2013)

Publisher's Note