Research on Digital Image Watermarking Technology

Xiaomei Zhang
Communication University of China
Beijing,China
2324302742@qq.com

Hu Guan
BJDCRC
Beijing,China
Hu.guan@ia.ac.cn

Ying Huang
Institute of Automation, Chinese Academy of Sciences
Beijing,China
Ying.huang@ia.ac.cn

Shuwu Zhang
Institute of Automation, Chinese Academy of Sciences
Beijing,China
Shuwu.zhang@ia.ac.cn

Abstract—With the continuous development of network technology, people are becoming more and more dependent on digital images. At the same time, some problems have emerged about digital copyright, so the protection of digital images has become a hot issue in research. This paper makes a detailed analysis on the main attributes, classification and system model of digital image watermarking, and systematically introduces several typical image watermarking algorithms and common attack methods. Finally, it proposed the main problems of current digital image watermarking technology, and summarized current situation and looked forward to future research directions.

Keywords-attack method; image watermarking algorithm; digital image watermarking technology

I. INTRODUCTION

In the background of the continuous development of today's network technology, digital works such as articles, pictures, audio, video and other digital works have penetrated into all walks of life.This method of communication is convenient and the cost is relatively low, which brings great convenience to people. However, the security issues that accompany it cannot be ignored. Because the nature of digital works are very easy to transparent, some illegal persons maliciously forged, tampered with, and pirated them for their profit. Once major information is leaked, it will not only bring economic losses, but also be more likely to occur serious social consequences, especially for some special fields, such as military, commercial.Therefore, solving the copyright problem of digital products is a urgent topic that researchers needs a lot of attention.

Researchers initially thought of cryptography,it core is cryptography. The original works and keys must be converted into ciphertexts through encryption algorithms ,then added key into the original work. But the encryption process is cumbersome and complicated,and it needs to be passed again when reading. which is extremely inconvenient for readers, and these encryption algorithms are not unbreakable. Later, the appearance of digital image watermarks just filled this gap, which greatly guaranteed the security of digital works.

At the first International Image Processing Conference in 1993, Tirkel [1] and others proposed the term "water mark" in the article "A digital watermark", which marked the birth of digital watermarking. In this article, the digital watermark technology, the embedding method of digital watermark and the application of digital watermark are introduced in detail . In China, many scholars or research institutes have conducted extensive researches on it. Digital watermarking is to embed the copyright owner's information into digital works by certain technical means, the embedded information is not easy to be detected by human eyes, and only specific personnel with a key can extract the watermarks through special equipment. This kind of thinking has brought the protection technology of digital products to a higher level, and developed the image watermarking technology.

II. WATERMARK BASICS

A. Main classification

1) Fragile watermark and robust watermark

According to the nature of watermark in digital image watermark, watermark can be divided into fragile watermark and robust watermark.Fragile watermark is extremely sensitive to changes,as long as it is damaged a little, this watermark may be meaningless. This kind of watermark is generally used for the integrity protection and authenticity of works.Robust watermark is very resistant to destruction,a litter damage to the watermark does not affect its own meaning. Robust watermarks are generally used to protect the copyright of digital works.

2) Visible watermark and invisible watermark

The digital image watermark is embedded in the picture , whether the watermark itself can be perceived by the human eyes, the watermark can be divided into visible watermark and invisible watermark.Visible watermark can be perceived by the human eyes,this kind of watermark generally existed in a transparent or translucent form, but it does not hinder the reading of the work,this kind of watermark is generally used to preview the public images in the image database to prevent viewers using the work for other purposes.Invisible watermark is not perceivable by human eyes. When a

978-1-7281-8138-7/20/$31.00 ©2020 IEEE
DOI 10.1109/ICCST50977.2020.00070

copyright dispute occurs in a digital work, this watermark is extracted by the copyright owner as evidence of infringement and used to protect their legal rights and interests,so this kind of watermark is being widely used.

3) Blind watermark and non-blind watermark

In digital image watermarking algorithms, watermarks can be divided into blind watermarks and non-blind watermarks according to whether original image is required during the detection process.Blind watermark,original image are needed in the watermark extraction process,contrary to non-blind watermarks needn't original image. In practice, it is not easy or impossible to obtain the original image when watermark is detected in most cases, so blind watermarking has more practical value and application prospects.

B. Attributes

1) Fidelity

Fidelity is invisibility,the invisibility of the watermark means that the difference between the original carrier image and the watermark carrier image are hardly detect for the human eyes. The threshold of invisibility is affected by the illumination,spatial frequency of the signal[2]and texture of the background of the original image.Peak Signal-to-Noise Ratio (PSNR) is used quantitatively as an indicator to measure the invisibility of the watermarked image[3],(1) is PSNR.

$$psnr = 10 \times \log_{10}\left(\frac{\left(2^n - 1\right)^2}{MSE}\right) \tag{1}$$

$$MSE = \left(f1 - f2\right)^2$$

(Among them, the pixel value of the carrier image and the watermark image at pixel n respectively.)

2) Robustness

The robustness of the watermark means that the watermark carrier image can still extract the watermark after various image processing attacks, and the watermark is still valid. Common image processing methods are: cropping, filtering, noise, rotation, compression, printing, etc. Use the Normalization Coefficient(NC) value as a quantitative measure of the robustness of the watermark[4].(2) is the formula of NC:

$$NC = \frac{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} w(i,j) \times w'(i,j)}{\sqrt{\left(\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} w(i,j)\right)^2} \times \sqrt{\left(\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} w'(i,j)\right)^2}} \tag{2}$$

(Where m and n represent the number of rows and columns of the pixel matrix, and w(i,j) and w'(i,j) represent the original watermark image and the extracted watermark image.)

3) Security

The security of the watermark means that every watermark image is matched with a key when it is embedded. Only the specific persons can process the key, and others have no permissions.

4) Embedded Capacity (Capacity)

The watermark embedding capacity refers to the size of a watermark that can be embedded in a digital image,it is usually measured in bits,it is also the maximum amount of watermark information that can be embedded.The amount of embedded information depends on the characteristics of the original carrier image itself, such as the size and format of the carrier image, and has a great relationship with the watermark generation algorithm and embedding algorithm. However, the embedding capacity and the robustness of the watermark are directly related, the larger for embedded watermark capacity, the worse for robustness of the watermark, and the two need to be balanced[5].

C. Common attacks against digital image watermarking

After embedding a watermark in an image, the host image containing the watermark must be able to resist certain attacks. Common attacks include geometric attacks, noise attacks, compression attacks, filtering attacks, and etc.

- Geometric attack

The geometric attack mainly refers to the spatial transformation processing such as cutting, rotating, scaling, and translation. This attack will not completely remove the watermark in the image, but it will cause indirect damage to the detection of the watermark.

- Compression attacks

Compression are JPEG compression and JPEG2000 compression, JPEG compression is also known as lossy compression, mainly using discrete cosine transform (DCT transform), JPEG2000 has better results than JPEG compression, mainly using discrete wavelet transform (DWT transform). This attack may remove visually unimportant information, so the approach for this attack is to place the watermark in some low frequency area.

- Noise attack

Noise attacks mainly include Gaussian noise, white noise, salt and pepper noise, etc. Adding noise is to randomly make some pixel valuesinto 0 or 255 in the watermarked host image, and Gaussian noise makes the probability density of these pixels to be Gaussian distributed. Adding noise will destroy the watermark embedded in the host image, making it impossible to extract or completely unable to distinguish the image.

- Filtering attacks

Image filtering can be performed in the air domain or in the frequency domain, which can change the characteristics of the image.The filtering attacks mainly include mean filtering, median filtering, Gaussian filtering and bilateral filtering[6].

D. Application

1) Copyright protection

The watermark is embedded in the image as some strings and numbers for information of copyright owner. In the

event of a copyright dispute, the copyright owner can extract the watermark in the image through the key to prove his legal rights.

2) Authenticity authentication

Authenticity authentication is also called content authentication. This type of watermark is generally a fragile watermark. It is often used in the verification of electronic bills and electronic seals to verify their authenticity and integrity. When the watermark is changed, you can quickly check and make tampering prompts[7].

3) Piracy tracking

It is used to trace the source of illegal digital works. The information of all users are embedded in the form of digital fingerprints into the collection of legal copies of works, when illegal copies are found, the source of the copies can be quickly determined[8].

E. System model

Image watermarking system generally consists of three parts: watermark generation, watermark embedding, and watermark extraction[9]. Figure 1 is a block diagram of the system model:

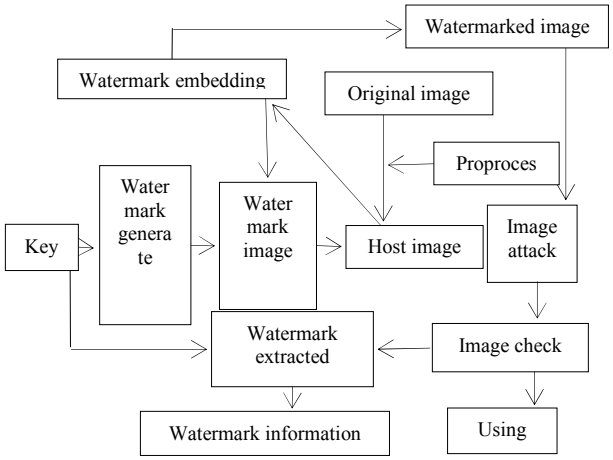

Figure 1. Digital image watermarking system model

F. Embedding method of digital image watermark

The main methods of processing for embedding are: additive rules, multiplicative rules, exponential rules, etc.(3)(4)(5) are follows:

$$X' = X + aw \tag{3}$$

$$X' = X(1 + aw) \tag{4}$$

$$X' = X(1 + aw) \tag{5}$$

Above all equation,X' is the host image matrix of the watermark, X is the original host image matrix, a is the embedded intensity, and w is the watermark image matrix.

G. Digital image watermark preprocessing

1) Scrambling

Scrambling is to scramble the original information of the image, making it difficult to recognize,Common methods of scrambling are: Arnold scrambling (cat face transformation), Fibonacci transformation, Hilbert curve transformation, affine transformation, magic square transformation, etc. Arnold transformation is proposed by Russian mathematician Vladimir I. Arnold. Arnold transformation is periodic, that is, the image transformation will return to the original image after a certain number of transformations. The period of transformation is related to the size of the image.

When the image is square, there is an inverse transform for Arnold transform. (6)(7) are Arnold transformation and inverse transformation:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod(N) \tag{6}$$

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \bmod(N) \tag{7}$$

(Where mod() is the modulus operation, N is the side length of the square image, and (x', y') is the transformed coordinates of the pixels (x, y).)

2) Block

When embedding a watermark in a picture without blocks, there are fewer positions can be embedded , and the embedding capacity is less. But the picture is divided,the watermark can be embedded in a certain position or a few positions in different blocks,so the embedding capacity will be greatly increased. Generally, the host image can be divided into 8x8 or 16x16, etc.

III. COMMON DIGITAL IMAGE WATERMARKING ALGORITHMS

Digital image watermarking,as a research hotpot in recent years, is mainly expressed in the two domains of space domain and transform domain. At the same time, some other methods are also helpful for digital image watermarking technology.

A. Spatial domain algorithm

Spatial domain watermarking directly set the watermark into the digital image works. The relevant algorithms include Least Significant Bit (LSB) algorithm and patchwork algorithm.The digital watermarking algorithm based on the spatial domain is the LSB algorithm proposed by Tirkel etc [1]. The general idea ofthis method is to embed a watermark in the spatial domain of grayscale digital image works, and use watermarks to replace the pixels in the digital image works of the least important position. Later, Abhishek etc. [10] improved its method, that is, compared the absolute difference of adjacent pixels of digital image

works, then constructed a saliency map, the watermark of the largest data is embedded in the most significant area of the digital image, while the smallest data is embedded in the least significant area. This method has better invisibility, and achieves a better balance in watermark embedding capacity and robustness.

The idea of the patchwork algorithm is to randomly select n pairs of pixels (ai, bi). By increasing the brightness value of each ai point by 1 and decreasing the brightness value of each bi point by 1, the average brightness of the entire image remains unchanged. In addition, the Patchwork method has resistance to JPEG compression, FIR filtering, and image cropping, but the amount of information embedded in this method is limited. In order to embedding more watermark information, we can divide the image into blocks, and then embed each image block separately,but the patchwork algorithm in the air domain has poor visibility. The literature [11] proposes a patchwork algorithm based on the transform domain. This algorithm uses DCT transform and combines the characteristics of the human visual system (Human Visual System, HVS) [12],offset the visual impact of watermark embedding.TABLE is the result for this algorithm.

TABLE I. THE ROBUSTNESS OF THE WATERMARK IMAGE UNDER THE PATCHWORK ALGORITH

Attack type	Parameter	NC
No attack	------	0.9508
Enlarge	Resize(2)	0.9478
Shrink	Resize(1/2)	0.8743
Gaussian	Gaussian noise(0.001)	0.5954
JPEG	JPEG90	0.8150
Cropping	Cropping(25%)	0.7419

B. Transform domain algorithm

Transform domain watermarking is an image matrix transformation, make the image data into the transform domain, and achieve the purpose of embedding the watermark by changing the transform domain coefficients. The related image transforms are Discrete Cosine Transform (DCT),Discrete Fourier Transform (Discrete Fourier Transform, DFT), Discrete Wavelet Transform (Discrete Wavelet Transform, DWT), etc. The disadvantage of transform domain algorithms is that the embedding volume is small and of calculation is complex. However, the advantage are more robust than spatial domain algorithms and has great advantages in dealing with compression, filtering and other attacks, so it is more applied widely.

1) Image watermarking algorithm in DCT domain

The earliest proposed DCT domain watermarking algorithm was IJ Cox et al. [13], the main idea is: generate a normally distributed pseudo-random sequence W, and perform a two-dimensional global DCT transformation for the digital image work to get the DC coefficient and then follow a specific Rules such as $X_i'=X_i\ (1+\alpha W_i)$ embed the watermark in the digital image works, and finally do the inverse DCT transform to obtain the digital image works (where X_i is the i-th DC coefficient of the original image, X_i' is the embedding the i-th DC coefficient after the watermark, W_i is the i-th watermark component, and α represents the intensity of the watermark embedding, which is a constant). The DCT domain watermarking algorithm has the advantages of strong robustness, strong invisibility, and compatibility with international compression standards, etc., so it is a hot spot of research.

Embedding watermarks in the DCT domain is prone to block effects. For example, when the low frequency part is embedded in the watermark, many embedding algorithm will cause block effects. Therefore, some people will choose embed a watermark in the mid-low frequency or mid-frequency. In this case, there are many watermarking algorithms that can be designed, such as the adaptive embedding algorithm based on HVS, the algorithm combined with other frequency domain transformations, and the algorithm using the relationship between pixels, etc. In addition, for the embedding capacity, different embedding areas are different. For example, when selecting low-frequency component without block, the capacity will be small.

Document [14] proposed an algorithm: the algorithm divided the host image into 16×16, then divided it into 4 blocks 8×8, and DCT transformed all 8×8, embeding the watermark with a quantization index using the two pixels between adjacent blocks.The pixel position is intermediate frequency value, which effectively overcomes the blockness of the image.TABLE is the result for this algorithm.

TABLE II. WATERMARK ROBUSTNESS UNDER DCT TRANSFORM

Attack type	Parameter	NC
Rotation	10°	0.9531
Filtering	Median filtering(3×3)	0.9258
	Low-pass filtering	0.9152
	Sharpening	0.9579
Noise	Salt and pepper noise(0.01)	0.8545
	Gaussian noise(0.001)	0.9179
JPEG	JPEG80	1
	JPEG50	1
Resize	Resize(0.8)	0.9979
	Resize(1.2)	1
	Resize(1.6)	1
Cropping	top left corner(25%)	0.9000
	top right corner(25%)	0.9027
	bottom left corner(25%)	0.9000
	at bottom left corner(25%)	0.8976

2) DFT domain image watermarking algorithm

DFT has properties such as separability, translation characteristics, rotation characteristics, scaling

characteristics, and conjugate symmetry. Its properties are similar with geometric attacks, so it has certain advantages against geometric attacks, but it is not compatible with international compression standards, and its calculation speed is slow, the design of the algorithm is relatively complicated, so it has always been limited in research.

3) DWT domain image watermarking algorithm

DWT is also called binary wavelet transform. Figure 2 is the result for two-layers of DWT. For most pictures, the low-frequency component contains the characteristics of the picture, and the high-frequency component contains the details of the picture. The low-frequency component is particularly important for describing the content of a picture. The redundancy of the low-frequency part is larger than that of other parts and the number of decomposition layers is determined according to the characteristics of the image and appropriate standards.The decomposition characteristics of the discrete wavelet watermarking algorithm are more consistent with the characteristics of HVS, so it has a good room for development.

In addition, the contourlet transform is similar to DWT. The contourlet transform can decompose the image in any scale and in any direction, it also works better against rotation and scaling.Literature[15] embed the watermark in the low-frequency part of the 2-layer contourlet transform, and embed the watermark by comparing the pixel value of a certain position with the average value of its eight neighborhoods.TABLE is the result for this algorithm.

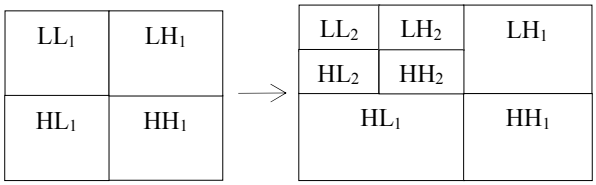

Figure 2. Two-layer wavelet decomposition based on wavelet transform

TABLE III. WATERMARK ROBUSTNESS UNDER CONTOURLET DECOMPOSITION

Attack type	Parameter	NC
Rotation	20°	0.9800
	45°	0.9701
	60°	0.9373
	120°	0.8700

4) QR decomposition image watermarking algorithm

QR decomposition,the embedding area is mainly in the Q matrix and R matrix,Choose the embedding position according to the characteristics of the matrix.Literature [16] divided the RGB of the image into three channels, followed by 4*4 blocks, QR decomposed for all the blocks, modifying the value of the fourth column has little effect on invisibility,so the first row and fourth column of the upper triangular matrix of R is selected as the embedding position. This method completely realizes the blind extraction of watermarks, and the image is more robust.TABLE is the result for this algorithm.

SVD decomposition is similar to QR,the embedding area is mainly in a upper triangular matrix and a lower triangular matrix and a eigenvalue matrix.When embedded in the eigenvalue matrix, the watermark is generally extracted without blind.Literature[18]embed the watermark into the eigenvalue matrix.TABLE is the result for this algorithm.Effective in noise attacks and compression attacks.

TABLE IV. WATERMARK ROBUSTNESS UNDER QR AND SVD DECOMPOSITION

Attack type	Parameter	NC(QR)	NC(SVD)
Filtering	Median filter(3×1)	0.9993	0.9903
	Median filter(5×1)	0.9906	---
	Low-pass filter(100,1)	0.9676	---
	Low-pass filter(100,3)	0.8980	---
	Sharpening(0.2)	0.9999	---
	Sharpening(1.0)	0.9838	---
Filtering	Blurring(0.2)	1	---
	Blurring(1.0)	0.7111	---
Noise	Salt&peppers noise(0.02)	0.9414	0.9307
	Salt&peppers noise(0.10)	0.7504	---
	Gaussian noise(0.1)	0.9817	0.9282
	Gaussian noise(0.3)	0.8598	---
	Addition noise(20%)	---	0.8850
	Addition noise(40%)	---	0.9013
	Addition noise(60%)	---	0.9009
	Addition noise(100%)	---	0.9194
JPEG	JPEG(15)	---	0.9273
	JPEG(50)	---	1.0000
	JPEG(70)	---	1.0000
	JPEG(30)	0.9139	0.9862
	JPEG(90)	0.9999	1
	JPEG 2000(5:1)	0.9950	---
	JPEG 2000(10:1)	0.9930	---
Resize	Resize(4)	0.9999	---
	Resize(1/4)	0.9838	---
Cropping	Cropping(25%)	0.8772	0.8054
	Cropping(50%)	0.6264	---

C. Other algorithms

At present, a single watermark embedding method cannot meet the requirements of copyright certification, multiple watermark technologies can embed two or more watermarks in digital image works to deal with multiple copyrights or other application issues. Reference [17] is aimed at the application of multiple digital watermarks. In the article, a dynamic multiple digital watermarking method is used to solve the problem of the generation of joint watermarks when multiple authors enter digital image works under irregular conditions. The identity information of all authors has played a protective role.

D. Summary

The following is a simple comparison of various digital watermarking algorithms. By comparison, the watermarking algorithms under various transformations can resist common attacks.

TABLE V. COMPARISON OF VARIOUS DIGITAL WATERMARKING ALGORITHMS

Digital image watermarking	Robustness	Imperceptibility	Algorithm complexity
Based on DCT[14]	excellent. It can withstand general attacks such as rotation, scaling, and shearing, as well as resist signal processing such as noise, filtering, and compression.	better	general
Based on Patchwork[11]	better. It can withstand operations such as zooming and shearing, and it can resist signal processing such as noise and compression, but its ability to resist noise is weak and its geometric attack resistance is relatively simple.	better	general
Based on QR[16]	excellent. It can withstand general attacks such as rotation, scaling, and shearing. It can also resist signal processing such as noise, filtering, and compression, especially against JPEG2000 attacks.	better	general
Based on Chaos[17]	excellent. It can withstand general set transformation operations such as rotation, scaling, and shearing, as well as resist signal processing such as noise, filtering, and compression.	better	quite complicated
Based on Contourlet[15]	excellent.the contourlet transform is similar to DWT.it also works better against rotation	better	general
Based on SVD[18]	Effective in noise attacks and compression attacks.But Weak resistance to geometric processing attacks, especially rotation and zoom attacks.	better	general

IV. CONCLUSION

The current watermarking technology has been fully developed, but there are still many directions that require more research.

(1) The contradiction between robustness and invisibility needs to reach a balance, and the process of achieving balance is not easy, which requires in-depth study.

(2) Research on the watermark capacity,although a lot of research has been done in this regard, but still Has a lot of research space.

(3) The size of the host image. The designed algorithm should satisfy all size images, so that the algorithm can be really applied to reality,but many algorithms are difficult to do this.

ACKNOWLEDGMENT

This work was supported by the National Key R&D Program of China (2019YFF0302800) and the Key R&D Program of Shanxi (201903D421007). It was also the research achievement of the Key Laboratory of Digital Rights Services, which is one of the National Science and Standardization Key Labs for Press and Publication Industry.

REFERENCES

[1] A.Z.Tirkel, et al.Electronic watermark [C]. DICTA, 1993: 666-673.

[2] Gao Ting. Research on Invisible and Robust Balanced Watermarking Algorithm [D]. Liaoning University of Engineering and Technology, 2018.

[3] Nie Xuan, Huang Climbing, Guo Dawei, Cao Bei. Overview of digital image watermarking technology [J]. Computer Knowledge and Technology, 2015, 11(03): 189-192.

[4] Chen Hao. Research and implementation of airspace digital image watermarking algorithm [J]. Modern Electronic Technology, 2007, 10(249): 149-150.

[5] Wang Jiaxin, Wen Zhengying. Color digital watermarking algorithm with invisible and robust balance[J]. Computer Simulation, 2014, 31(03): 266-269.

[6] Jiang Ming.Summary of image filtering algorithms [EB]/[OL].https://blog.csdn.net/jiang_ming_/article/details/82594261.2018.

[7] Chen Haipeng. Research on Digital Image Authenticity Authentication Technology [D]. Jilin University, 2011.

[8] Hu Yuping, Zhang Jun. Research on Digital Watermarking Protocol for Piracy Tracking[J]. Computer Science, 2010, 37(01): 91-94.

[9] Wu Yali, Zhang Minrui. Summary of digital image watermarking technology[J]. Modern Electronic Technology, 2007(21):81-84.

[10] Abhishek Basu, Subhrajit Sinha Roy, Avik Chattopadhyay. Implementation of a spatial domain salient region based digital image watermarking scheme[j]. 2016 Second International Conference on Research in Computational Int elligence and Communication Networks (ICRCICN). 2016:269- 270.

[11] Gan Lin, Yang Yu. Improved patchwork watermarking algorithm based on transform domain [J]. Journal of Chengdu University of Information Technology, 2017, 32(06): 623-627.

[12] Sun Dezhi. Research on Spatial Digital Watermarking Algorithm Based on Human Visual System (HVS) [D]. Nanchang University, 2016.

[13] IJCox,etal.Secure Spread Spectrum Watermarking for Multi media[R].Technical Report 9510, NEC Research Institute, Princeton, NJ, 1995.

[14] Loan N A, Hurrah N N, Parah S A, et al. Secure and Robust Digital Image Watermarking using Coefficient Differencing and Chaotic Encryption[J]. IEEE Access, 2018:1-1.

[15] Ji Nuoran, Lu Xiaoqi, Gu Yu, Zhao Ying, Liu Kun. Contourlet domain color image blind watermarking algorithm based on QR code and chaotic encryption[J]. Packaging Engineering, 2017, 38(15): 173-178.

[16] Qingtang Su a b, Yugang Niu b, Gang Wang a, etc. Color image blind watermarking scheme based on QR decomposition[J]. Signal Processing, 2014, 94(1):219-235.

[17] Tang Ming, Wang Lina, Zhang Huanguo. Dynamic multiple digital watermark design scheme. Computer Application Research, 1001-3695 (2006).

[18] Xue Shengnan,Chen Xiuhong.Digital image watermarking algorithm based on chaotic encryption and SVD[J].Computer Engineering,2012,38(19):107-110.