



Research Article

ISSN : 0975-7384  
CODEN(USA) : JCPRC5

## A blind digital watermarking algorithm based on DWT

Lianjie Dong\*<sup>1</sup> and Ruihong Wang<sup>2</sup>

<sup>1</sup>College of Science, Agriculture University of Hebei, Baoding, China

<sup>2</sup>College of Information Science & Technology, Agriculture University of Hebei, Baoding, China

---

### ABSTRACT

*With the rapid development of network communication and broad application of multimedia technology, copyright protection of digital media work is becoming more and more important. Digital watermarking is viewed as an effective tool for copyright protection of multimedia data. At first the principle, research background and status of digital watermark is described. Then, a blind watermarking algorithm based on DWT is proposed. The watermark image is scrambled by a generalized Arnold transform so as to improve the security of the watermark; the watermark is embedded into the middle-frequency subband which guarantees the robustness of the algorithm; In order to implement the blind extraction, this paper improves an embedding algorithm based on HVS, which enhances the applicability of the algorithm. This paper tests the algorithm by VC++6.0, and quantity of experiment data shows that algorithm has good robustness, and the imperceptibility of watermark can be guaranteed at the same time.*

**Key words:** copyright protection, digital watermark, DWT, image scrambling, HVS

---

### INTRODUCTION

#### I. RESEARCH BACKGROUND

With the development of digital technology and Internet, various types of digital multimedia works, including image, video and audio, have been transmitted or published via Internet.[1,2] Digital works have convenience with low cost and high speed in copying and transmitting, whereas these features may be exploited by pirates, for which anti-pirate is urgent. In addition to lawful and regulatory measures such as copyright protection, special technological protection should be provided. Under this kind of application requirement, Digital watermark technology developed rapidly [3,4,5].

As an important branch of information hiding technology, Digital watermark is an effective combination of digital copyright protection and data security maintenance technology, closely related with data encryption [6,7,8]. It is able to conceal in the digital works, such as image, audio, documents and video, the meaningless signal or markers of particular significance including serial number, copyright mark, as proof of the author's ownership of their work and evidence of illegal infringement prosecution and identification. Also it is able to ensure that the completeness and reliability of digital information through the watermark detection and analysis. Thus, Digital watermark becomes an effective measure of copyright protection and digital multimedia protection.

#### II. ALGORITHM DESIGN IDEAS

Although digital watermark technology has seen rapid development and emergence, there are a lot of problems to solve in research in this field, for an instance, the enhancement of robustness to compression may lead to a weakened robustness to geometric attack, and the enhancement of robustness to geometric attack may lead to a weakened robustness to imperceptibility. Therefore, the main goal of this paper is to design a digital watermark algorithm with great robustness to geometric attack, filtering and compression and great imperceptibility of

watermark.

As two basic requirements of invisible watermark, robustness and imperceptibility are paradoxical, for which it can be known that one of the basic problems of the algorithm is to seek compromise between robustness and imperceptibility. The best compromise point is to select proper transform domain, loading position, and then with the premise of watermark invisibility, to load watermark with greatest strength to get the greatest robustness. With the different type, transform domain, load position or the image feature, the strength of watermark loading and performance varies [9,10]. Thus, the first to consider is watermark type, and then is preprocessing the watermark signal, because that loading position can only be selected after watermark type is determined. With copyright protection as the goal of this paper, the robustness of watermark must be ensured primarily. The embedded algorithm should consider the robustness to geometric attack in addition to the selection of watermark type and embedding position.

### III. ALGORITHM FEASIBILITY ANALYSIS

It's human being who appreciate image and judge the quality of image, therefore, Almost all of the digital image processing techniques are tightly around the human visual system (HVS), Such as JPEG image compression technology is according to the characteristics of human visual system to determine the quantization step length. When embedding watermark in an image, the imperceptibility and robustness of watermark to solve must consider the characteristics of human visual system, that is, under the requirements of the invisibility, making full use of the characteristics of human visual system, distributing reasonably the energy of watermark signal, improving as far as possible the local intensity of watermark weight in some areas, to not affect the visual perception effect of the original image, at the same time improve the robustness of the watermark.[10,11,12]

After embedding watermark into an image, no matter what method to use, the image pixel values must be changed by some or all, but as long as the change of the amplitude is lower than the scope human eye can perceive and the whole image contrast remains the same or changes very small. Therefore, with pixel value changes within the acceptable range, the human eye will see no change.

### IV. WATERMARK GENERATION AND PRETREATMENT TECHNOLOGY

#### 4.1 Image scrambling.

Image scrambling is to use an algorithm to make the location of the pixels in the image or the color of pixel messed up, with the total pixel number unchanged and the histogram constant. Changing the original image into a new chaotic image, if you don't know the scrambling transform used, it is difficult to restore the original image. Digital image scrambling transform is reversible, which is through transforming position or the gray scale, to disrupt the image, so as to confuse the third party to a certain extent. Due to removing the watermark pixel space correlation, scrambling watermark can improve the robustness of watermark against image clipping operations.

In this paper Arnold transform is mainly used, which is intuitive, simple, cyclical, and very convenient for application.

Arnold transformation is a kind of transform put forward by Arnold in Ergodic Theory, also known as Arnold's Cat Map. Suppose drawing a cat face image within the unit square, Arnold's Cat Map formula is:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \text{ mod } 1 \quad (1)$$

Through the transform, the clear cat face image becomes blur, which is actually a location movement of the point, and the transform is one to one. For a digital image P with size  $N \times N$ , discretization of Arnold transform can be performed:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \text{ mod } N \quad (2)$$

$(x, y) \in (1, 2, \dots, N)$ , said a pixel point of the image matrix before transform,  $(x', y')$ , said the new location after transform, N is the order number of image matrix. When transforming every pixel in the image, an Arnold transform of the image is completed.

For digital images, the location movement here is actually the movement of the corresponding points of the grey value or an RGB color value, which is to move the corresponding grey value or RGB color value of the original

point  $(x, y)$  to  $(x', y')$ . Through transform, a clear image becomes blurring. Through the replacement of discrete point set, and transfer of the image information to come over, when traversing all points of the original image, a new image has been created.

Using Arnold transforms features, Digital watermarking technique firstly scrambles the watermark image to be embedded into a digital product, and then using various kinds of algorithms embed the scrambled image into a digital product [13,14,15]. When the digital product is under user's modification or malicious attack, a portion of the digital products often is damaged or lost (e.g., cutting), so that a part of the embedded digital watermark will be damaged or lost. After the damaged digital watermark is extracted, continuing to use Arnold transform can restore digital watermarking image. Because in the process of restoration, Arnold transform will have the original damaged bits scattered to the full, reducing the impact of the damage to human visual, and correspondingly improving the robustness of digital watermarking.

#### 4.2 Watermark embedding domain analysis.

By embedding positions, digital watermarking can be divided into the airspace and transform (frequency) domain digital watermarking.

Airspace digital watermark can be embedded by modifying the image intensity values or grey value, which doesn't transform the original image, with simple calculation and high efficiency, however as a result of watermarking to balance imperceptibility and robustness, the range of properties to select is small and the generated watermark is localized and difficult to resist common image processing attacks and the influence of noise interference with poor robustness.

Transform domain digital watermark is a watermark added to the original image of a transform coefficient, which needs to transform the original image, with complicated calculation and good robustness. According to human visual properties, embedding watermark information into the high frequency part of the image, not only can make the concealment of the embedded watermark better, but also can embed in larger amount of information, with strong ability against the attack of the method, so it's very suitable for the digital works copyright protection.

#### 4.3 Comparative analysis of typical transform domain watermarking algorithm.

Transform domain technology can embed watermark information and does not cause sensual feelings, generally based on the common transform, such as Discrete Fourier Transform(DFT)、Discrete Cosine Transform(DCT)、Discrete Wavelet Transform(DWT), Discrete Hadamard Transform (DHT). Transform domain method usually has very good robustness, with certain resistance to data compression, common filtering processing, noise, and so on.

Fourier transform has long been in the field of signal processing one of the most widely used analysis method, however it's just a kind of pure frequency domain analysis method and can't provide any frequency information on local time. To this end, the method of short time Fourier transform (STFT) adds before signal Fourier transform with a translation of the time window [16]. However, due to the practical problems often require resolution on the time domain to frequency domain transformation, the resolution of the method in time domain resolution of short time Fourier transform (STFT) with selected and fixed window functions, so it still can't solve many practical problems. Wavelet transform method is in order to adapt to the requirements, it based on the frequency and time, in accordance with the special method for sampling, can effectively solve the problem of mutual transformation between time domain and frequency domain. Therefore, wavelet transform method is a very effective time and frequency domain analysis method; it is a milestone in the history of the development of harmonic analysis.[17,18]

Discrete wavelet transform has good time-frequency features. The wavelet transform of watermarking method basically has the following three advantages: One is that you can guarantee in a new generation of compression standard JPEG - 2000 the watermark information will not be removed; Two is that the research result on visual characteristics in image coding research can be used in watermark technology; Three is that it is possible to provide methods to embedded watermark directly in the compressed domain.

By the above analysis, considering one of the design goal of the algorithm is effective resistance to compression attack, therefore, this paper chose embedding watermarking in the transform domain, and chose the discrete wavelet transform in the transform domain.

#### 4.4 Discrete Wavelet Transform

If  $x(t)$  satisfy

$$\int_R |x(t)|^2 dt < \infty \quad (3)$$

Then  $x(t)$  is a quadratically integrable function, denoted by  $x(t) \in L^2(R)$

Suppose  $x(t)$  is a square integrable function,  $\phi(t)$  is a wavelet function or mother wavelet function, then

$$WT_x(a, \tau) = \frac{1}{\sqrt{a}} \int x(t) \phi^* \left( \frac{t-\tau}{a} \right) dt = \langle x(t), \phi_{a,\tau}(t) \rangle \quad (4)$$

Referred to as the wavelet transform of  $x(t)$ , in which  $a > 0$  is scale factor,  $\tau$  is shift factor,  $\langle x, y \rangle$  is inner product, the implication of which is (superscript \* is Taking the conjugate)

$$\langle x(t), y(t) \rangle = \int x(t) y^*(t) dt \quad (5)$$

$\phi_{a,\tau}(t) = \frac{1}{\sqrt{a}} \phi\left(\frac{t-\tau}{a}\right)$  is the shift and scale expansion and shrinkage of basic wavelet.

Continuous wavelet is a kind of linear transform, additive, shift invariant, scale conversion can be carried out and in line with the inner product theorem, and the inverse transformation expression is:

$$x(t) = \frac{1}{C_\phi} \int_0^{+\infty} \frac{da}{a^2} \int_{-\infty}^{+\infty} WT_x(a, \tau) \phi_{a,\tau}(t) d\tau \quad (6)$$

But in practice, continuous wavelet transform is hard to get effective application, because the scale factor and displacement factor is continuously transformed, which implies the information redundancy is high, large amount of calculation, and its reconstruction algorithm it is difficult to implement by computer, and is applied in theory derivation, prove, discuss with nature. In order to meet the needs of practical application, mostly the discrete wavelet transform is used, discretizing  $a$  and  $\tau$  to calculate the wavelet transform. Conventionally, suppose  $a = a_0^j$ ,  $\tau = a_0^j k \tau_0$ ,  $j, k \in Z$ . Hence

$$DWT_x(a_0^j, k\tau_0) = \int x(t) \phi_{a_0^j, k\tau_0}^*(t) dt \quad (7)$$

$\phi_{a_0^j, k\tau_0}(t) = a_0^{-\frac{j}{2}} \phi\left[\frac{t}{a_0^j}, k\tau_0\right]$  usually referred to as discrete wavelet transform (DWT).

If discrete wavelet sequence consists of A frame, set the upper and lower bounds the A and B, respectively, thus when A = B (at this time frame for tight frame), the inverse transformation of discrete wavelet transform (IDWT) formula is:

$$x(t) = \frac{1}{A} \sum_{j,k} DWT_x(j, k) \phi_{j,k}(t) \quad (8)$$

## V. OVERALL IMPLEMENTATION OF ALGORITHM

### 5.1 Implementation of embedding algorithm

#### 5.1.1 Image Scrambling

After scrambling, watermark image can make more uniform distribution of image information, avoid watermark image contour in the image that the human eye can distinguish after embedding the watermark, decrease of embedded watermark image's relying on the carrier image airspace to resist attacks such as cutting, prevent watermark damage is concentrated in a block which causes obviously drop quality of the extracted watermark in order to improve the robustness of the watermark.

Scrambling matrix is adopted in this paper is  $A = \begin{pmatrix} 3 & 7 \\ 8 & 11 \end{pmatrix}$ . Figure 1 shows the k times scrambling watermark image and its effect:

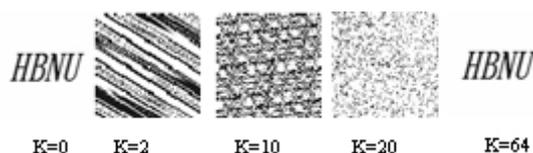


Fig 1. Watermark scrambling

### 5.1.2 Blocks of the Image

Divide the image with size of  $M \times N$  into blocks of  $16 \times 16$ , thus get  $(M/16) \times (N/16)$  blocks, each piece is represented by a matrix, and the small pieces of coordinates is corresponding to the image coordinates [19]. The input of the module is a complete image and the output is a three-dimensional matrix, for which one dimensional images show the code no. of every little piece of a block, and the other two dimensional images is the abscissa and ordinate of a block of image. The algorithm process is as follows:

Setp1: Get the size of image, and get the position of each small piece in the original image's row  $r$  and column  $c$ .

Setp2: Compare mark  $i$  and  $r*c$ , if  $i$  is smaller, go to Setp3, otherwise, Step 5;

Setp3: Judge whether this small piece is at the rightmost of the image, if rightmost, then assign value to parameters of  $X_1, X_2, Y_1$  and  $Y_2$ :  $X_1 = 16(i/r - 1) + 1$ ,  $X_2 = 16(i/r)$ ,  $Y_1 = 16*(c - 1) + 1$ ,  $Y_2 = 16*c$ ; otherwise, assign value to parameters of  $X_1, X_2, Y_1$  and  $Y_2$ :  $X_1 = 16(i/c) + 1$ ,  $X_2 = 16(i/c)$ ,  $Y_1 = 16*(i \bmod r) + 1$ ,  $Y_2 = 16*(i \bmod r)$ ;

Setp4: Get a small piece of the image, and increase  $i$  by 1, go to Step 2;

Setp5: Program ends and gets each small piece of the image.

### 5.1.3 Wavelet decomposition

Decomposing the image can well realize the human eye visual description of the image multi-resolution, and can realize the separation of image smooth composition and non-stationary composition, has the characteristics of being combined with human visual characteristics. After discrete wavelet decomposition of the original image, the effect is as right in figure 2.



Fig 2. The discrete wavelet decomposition of Elaine image

In this paper, discrete wavelet transform is an important step of the algorithm of watermark embedding and detection.

The decomposing process is as follows:

Step1: Get the blocks of image  $n$ ;  
 Step2: Judge whether iteration factor is smaller than number of image blocks  $n$ ;  
 Step3: If smaller than  $n$ , make the level 3 discrete wavelet transform, and go to Step2.  
 Step4: Otherwise, break and the program ends.

The output of this module is a data array of 4 elements, respectively low-frequency wavelet coefficient LL, Middle-frequency wavelet coefficient LH, HL and high-frequency wavelet coefficient HH.

#### 5.1.4 Ordering groups

Sort the coefficients of the decomposition of the original image by groups. According to the characteristics of the human eye, sorting wavelet coefficient by groups is repeatedly embedding wavelet coefficient into the watermark image, and according to different luminance mask features adopt different modulation factor, by which great robustness and imperceptibility can be met [20].

#### 5.1.5 Wavelet reconstruction

Wavelet reconstruction and wavelet decomposition is the process of function to buck, but when wavelet decomposition is DWT, discrete wavelet decomposition and wavelet reconstruction is discrete wavelet reconstruction IDWT. The main steps are as follows:

Step1: Judge whether iteration factor is smaller than the number of blocks of image  $x$ , denoted by  $n$ ;

Step2: If smaller than  $n$ , then make discrete wavelet reconstruction of this small piece, and go to Step 2;

Otherwise, break and the program ends.

This module is to reconstruct the image after dividing blocks and wavelet decomposition, whose input is each wavelet coefficient and number of blocks, and output is reconstructed small pieces.

#### 5.1.6 Image Synthesis

Because in the algorithm using the image block, so in the last to synthesize image, making it a complete image. This process is the inverse process of image block, in which make the coordinates of each piece and the image coordinates corresponding, and in the image synthesis is to make the entire image coordinates and the coordinates of each piece corresponding.

#### 5.2 Embedding Process

Set the original image is gray image  $I$  with size  $M \times N$ , watermark image to gray image  $W$  with size  $M \times N$ , embedded process flow diagram shown in figure 3, the embedded steps are as follows:

Step1: Make Arnold transform to watermark image  $W$ , and the number of transformation as a key. After scrambling watermark image for using line scan form one-dimensional vector, one dimensional digital watermark sequence is obtained  $W = \{w(i), 1 \leq i \leq m \times n\}$ .

Step2: After scrambling watermark image of level 2 discrete wavelet decomposition to get 7 sub-images, respectively for  $HH'_1, HL'_1, LH'_1, HH'_2, HL'_2, LH'_2, LL'_2$ , with length of  $L_m (m = 1, 2, \dots, 7)$ .

Step3: Divide the original image into image block of fixed size (e.g.  $16 \times 16$ ), so the original image is divided into  $\frac{M}{16} \times \frac{N}{16}$  small blocks.

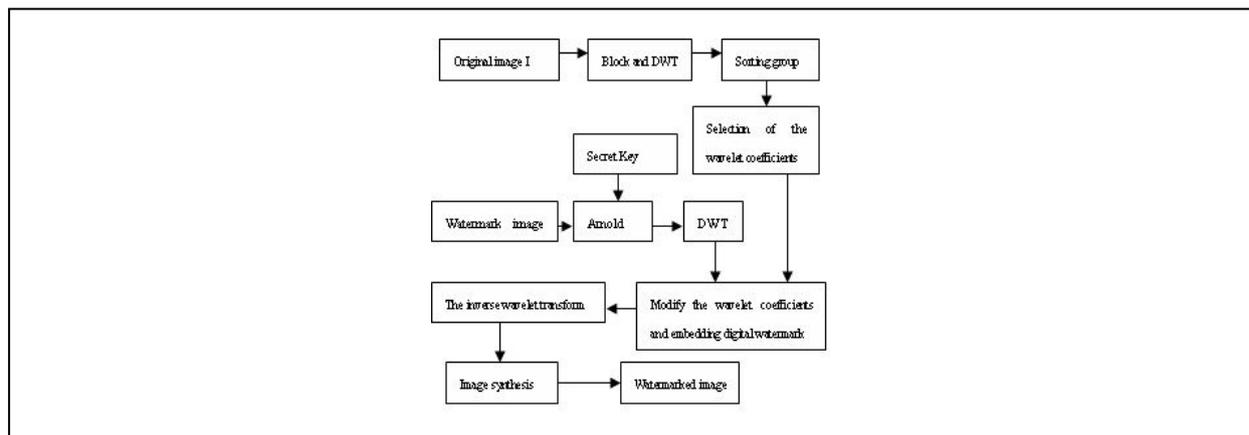
Step4: Make level 3 wavelet decomposition to each image block and get 10 sub-images, denoted by  $HH_1, HL_1, LH_1, HH_2, HL_2, LH_2, HH_3, HL_3, LH_3, LL_3$ , sort the middle-frequency coefficient ( $HH_2, HL_2, LH_2, HH_3, HL_3, LH_3$ ) in descending order, and record the index of sort  $B(t)$ .

Step5: Take the first  $m \times n$  corresponding middle-frequency coefficients, using the formula  $x_w(i) = x(i) + aw(i)$ , repeatedly embed each sub-image after level 2 wavelet decomposition into the corresponding sub-images after making level 3 wavelet decomposition of the original image  $W$ . In the formula,  $x(i)$  is the selected wavelet coefficient,  $w(i)$  is the  $i$ th component of a one-dimensional digital watermark series,  $x_w(i)$  is the new wavelet coefficient after embedding watermark. Parameter  $a$  is the intensity of embedding the watermark, the selection of

which has no strict theoretical standard, and in general needs multiple experiments to determine. Both the perceptual and robustness of the watermark's request, after repeated experiments, the values are between 0.06 and 0.08.

Step6: The modified medium frequency sub-image in combination with other unmodified sub-image for inverse wavelet transform, the insets to synthesis, get image I' which is embedded into effective digital watermarking .

Step7: It's important to note that you must write down the sort index, when extracting the watermark, the index can be used to sort the embedded watermark image wavelet decomposition coefficients .If location deviation in the process of extracting watermark, scrambling technology can greatly reduce the visual effect of digital watermark instead.



### 5.3 Implementation of Extraction and detection algorithm

Watermark extraction and detection process is generally the inverse process of watermark embedding process, therefore, some function modules and functions in the embedded algorithm can be used in the detection and extraction. The function modules and functions in the extraction and detection algorithm is less than those in the embedded algorithm. The algorithm mainly includes: the image block, image wavelet decomposition, the wavelet reconstruction and so on, these module functions and implementation are the same as the watermark embedded in, so no longer repeated here.

#### 5.3.1 Extraction and detection process

When extracting the watermark, don't need original image. Corresponding to the above digital watermarking embedding algorithm, watermark extraction process are shown in figure 4, the extraction steps are as follows

Step1: Divide the watermark image I' into blocks of fixed size (the same method as the watermark embedding), thus the image containing the watermark information is divided into  $\frac{M}{16} \times \frac{N}{16}$  blocks.

Step2: Each image block is to level 3 discrete wavelet decomposition, and according to the sorting index B (t) in the embedded process ,order each of the intermediate frequency coefficients ( $HH_2, HL_2, LH_2, HH_3, HL_3, HL_3$ ).

Step3: Taking the first  $m \times n$  intermediate frequency coefficients, and according to formula(9) to extract watermark information. In the formula,  $x(i)$  is the selected original image wavelet coefficient,  $w(i)$  is a one-dimensional digital watermark series,  $x_w(i)$  is the new wavelet coefficient after embedding watermark. Parameter  $a$  is embedding strength of the digital watermark.

$$w(i) = \frac{x_w(i) - x(i)}{a} \quad (9)$$

Step4: Ordering  $w(i)$  in ascending order gets the matrix of  $m \times n$ . Then according to the key making the Arnold inverse transform, then image synthesis for extraction of watermark image  $W'$  .

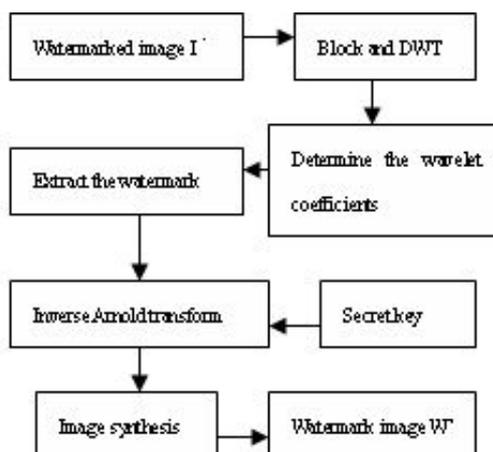


Fig 4. The Diagram of watermark extracted

## VI EXPERIMENTAL RESULTS AND ANALYSIS

### 6.1 Simulation results

This paper uses the Peak signal-to-noise Ratio (PSNR) to estimate the image distortions containing the watermark after the watermark is embedded into the original image, and reflects a digital watermarking algorithm's imperceptibility indicator. While the index is not very accurate, it can be used as a good empirical rule to measure watermark's imperceptibility. The formula of PSNR is:

$$PSNR = 10 \lg \frac{M^2 \cdot \max_{u,v} Y^2(u,v)}{\sum_{u,v} (X(u,v) - Y(u,v))^2} \quad (10)$$

Among them,  $X(u,v)$  and  $Y(u,v)$  respectively represents the original image  $X$  and image  $Y$  with embedded watermark in the value of the position  $(u,v)$ ,  $M$  is the size of  $X$  pixel, the unit of PSNR is decibels (dB).

In order to quantitatively describe the known watermarking system's robustness for specific attacks, attacks can be continuously increased until the watermarking can no longer be reliably extracted. The similarity between the initial watermark and extracted watermark reflects the robustness of watermarking system, this paper mainly adopts the normalized correlation coefficient (NC) to measure robustness:

$$NC = \frac{\sum_{u,v} W'(u,v)W(u,v)}{\sum_{u,v} W^2(u,v)} \quad (11)$$

$W(u,v)$  and  $W'(u,v)$  respectively represents the original watermark  $W$  and the extractive watermark  $W'$  in the value of the position  $(u,v)$ .

Figure 5 shows that author give the original image and original watermark image, and using the approach which has been introduced above to prove that digital watermark is an effective tool in the copyright protection.



Fig 5.Original image、 Watermark image

### 6.2 Results of attacks experiment and analysis

In this paper the application background of Watermark is copyright protection, therefore, requires higher robustness of the watermark, the watermark should for a variety of watermark has strong ability of resist attack. The attack on watermarking refers to using various means try to disable watermark, mainly includes: destroy the watermarks so that can it can't be extracted, or can be extracted but has been damaged to the point of visual unrecognizing, disavowal of the authority and legitimacy of the embedded watermark, trying to replace the embedded watermark with other watermark or cover the original watermark, etc.

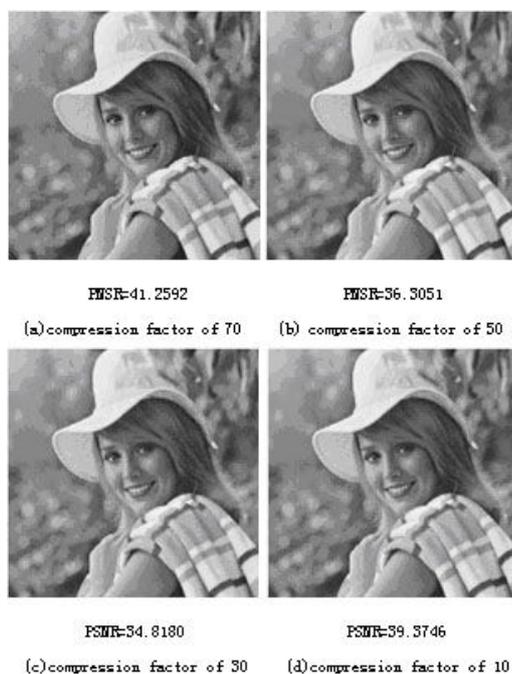


Fig 6.compression factor of 70\50\30\10

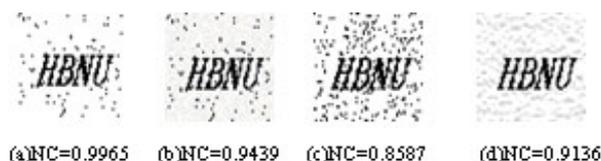


Fig 7. Watermark image extracted from fig 6

### 1) JPEG compression attack

Compression attack is to compress the image to be detected, in order to make the watermark information lost and can't correctly extract watermark. In the process of all kinds of image processing, JPEG compression's blow to the existence of digital watermark is bigger, in this paper; the performance of algorithm to resist JPEG compression is inspected. Figure 6 respectively with quality factor of 70, 50, 30, 10 JPEG compressed images, figure 7 (a) (b) (c) (d), respectively from the figure 6 (a) (b) (c) (d) to extract the watermark image.

As can be seen from the figure, after compressing the image to be detected, image in visual basically did not change, as can be seen from the figure 8 and 9, the image to be detected after compression can still extract complete watermark. It's visible that this algorithm can effectively resist compression attacks of watermark.

### 2) Noise attack

In general, image transmission in the network, is vulnerable to noise pollution. In this paper, the embedded watermark image is to add a more common noise: salt and pepper noise. Figure 8 (a) and figure 8 (b) respectively show the image after adding the salt and pepper noise with intensity of 0.01 and 0.02, figure 9 (a) and figure 9 (b) respectively for the two cases, extract the watermark.

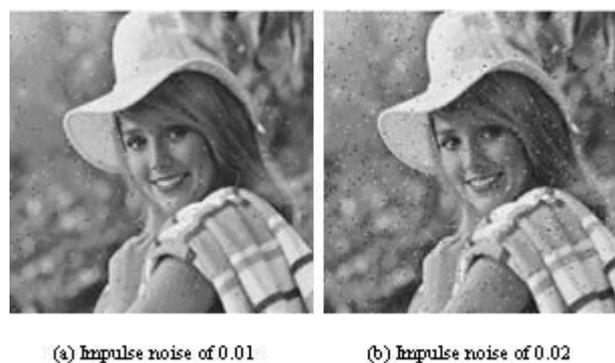


Fig 8. Image of noise-adding

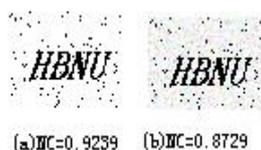


Fig 9. Watermark image extracted from fig 8

As can be seen from the figure, after under different intensity of salt & pepper noise attack, the image to be detected still can extract the relatively complete watermark image; therefore, algorithm in this paper has strong ability of resistance to noise attack.

### 3) Filtering attack

Filtering attack is to filter the image to be detected by using the low-pass or high-pass filter, in order to make the watermark information lost and can't perfectly extract watermark. In image processing, filtering attack is a common approach. The attacker usually uses different filtering attack for different application purposes. In this paper, author use three kinds of filtering attack, which is median filtering attack and two kinds of Gaussian filter, to inspect the performance of algorithm to resist filtering attack.



Fig 10. image of median filter and the extracted watermark image



Fig 11. image of 3×3 Gaussian filter and the extracted watermark image



Fig 12. image of 5×5 Gaussian filter and the extracted watermark image

As can be seen from the experimental results in the figure 10,11,12, the algorithm's effect, which resisting the attack of median filter and Gaussian filter, is better.

## CONCLUSION

Results can be found through the experiment, the blind watermarking algorithm put forward in this paper has good robustness and ability against the attack, but if the image is at the same time under a variety of attacks, the robustness of the watermarking algorithm can appear sharp decline. Secondly, the algorithm cannot reach the optimal though for some attack has good robustness, but the embedding and detection speed not quick, meanwhile there is contradiction between the robustness of the watermark and embed watermark capacity, it is also the problem to face and solve in the future.

## REFERENCES

- [1] Bender W, Cruhl D, *IBM System*, 1996, 35:313-336.
- [2] I.J.K Ouanaith et al, "Phase watermarking of digital images," *Proc. of ICIP'96*, 1996, Vol'3, pp.239-242.
- [3] I.J.K Ouanaith and T.Pun, "Rotation, Scale and Translation invariant digital images," *Proc. Of ICIP'97*, 1997, Vol.1, pp.536-539.
- [4] Cox IJ, Killia J, Leighton et al. *IEEE Transactions on Image Processing*. December 1997, Vol.8, No.12, pp.1673-1687,.

- [5] E.Koch and J. Zhao. Towards, "Robust and Hidden Image Copyright Labeling Processing Workshop," 1995, *Thessaloniki, Greece*.
- [6] Teskeridon S, Pitas I, *IEEE Int.Conf.on Acoustics, Systems and Signal Processing*, 2000:1967-1970.
- [7] Niu Xiamu, Lu Zheming, Sun Shenghe, *IEEE Trans On Consumer Electronics*, 2000,46(1):838-843.
- [8] Min-Jen Tsai and Hsiao-Ying Hung, "Wavelet transform Based Digital Watermarking for Image Authentication," [J] 2005.
- [9] A.H.Paquet and P.K.Ward, *Int.Conf.Electrical and computer Engineering*, 2002, Vol.2, pp.879-884.
- [10] G.J.Yu, C.S.Lu, and Y.M.Liao, *IEEE Trans.Multimedia*, 2003, Vol.5, pp.161-173.
- [11] Zhang Chongxiong, Song Chenzhi, "Design and realization of detecting instrument for digital watermark trademark based on ARM," *Proceedings - IEEE 2011 10th International Conference on Electronic Measurement and Instruments, ICEMI 2011*, v 3, p 158-162, 2011.
- [12] Zhang Bin, Wang Jiazhen, Wen Jiafu, Tong Zhongling, "A novel digital watermark against RST distortion based on SURF," *Proceedings 2010 IEEE International Conference on Information Theory and Information Security, ICITIS 2010*, p 130-133.
- [13] Shi Hongqin, Lv Fangliang, "A blind digital watermark technique for color image based on integer wavelet transform," *2010 International Conference on Biomedical Engineering and Computer Science, ICBECS 2010*, 2010.
- [14] Zhong Yunfei, Fu Lujing, Zou Jie, Deng Ronghua, *Applied Mechanics and Materials*, 2013, v 262, p 181-185, *Advances in Printing and Packaging Technologies*.
- [15] Ge Jing, Zhang Guoping, Yu Zetai, "A web-based image transmission system using digital watermark," *2011 International Conference on Electric Information and Control Engineering, ICEICE 2011 - Proceedings*, 2011, p 1130-1133, 2011.
- [16] Xu Jian, Ma Bin, "Digital watermark for document electronic seal system based on DCT technology," *Proceedings of the International Conference on Uncertainty Reasoning and Knowledge Engineering, URKE 2011*, 2011, v 2, p 5-8.
- [17] Zhu Changqing, Ren Na, "An algorithm for digital watermark based on pseudo-random sequence and DCT for remote sensing image," *Wuhan Daxue Xuebao (Xinxi Kexue Ban)/Geomatics and Information Science of Wuhan University, December 2011*, v 36, n 12, p 1427-1429+1499.
- [18] Ma Bin, "Experimental research of image digital watermark based on DWT technology," *Proceedings of the International Conference on Uncertainty Reasoning and Knowledge Engineering, URKE 2011*, 2011, v 2, p 9-12.
- [19] Jia Xiaolin, Qi Yanli, Shao Liping, Jia Xiaobo, "An anti-geometric digital watermark algorithm based on histogram grouping and fault-tolerance channel," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2012, v 7202 LNCS, p 753-760.
- [20] Song Jianhua, Song Jianwei, Bao Yuhua, "A blind digital watermark method based on SVD and Chaos," *Procedia Engineering, 2012 International Workshop on Information and Electronics Engineering*. 2012, v 29, p 285-289.