

---

# Design of a Hybrid Digital Watermarking Algorithm with High Robustness

---

Yi Xie<sup>1,\*</sup>, Yulin Wang<sup>1</sup> and Maode Ma<sup>2</sup>

<sup>1</sup>*School of Computer Science, Wuhan University, Wuhan, China*

<sup>2</sup>*School of Electrical & Electronic Engineering, Nanyang Technological University, Singapore*

*E-mail: yix@whu.edu.cn; yulinwang@whu.edu.cn; emdma@ntu.edu.sg*

*\*Corresponding Author*

Received 12 August 2020; Accepted 20 August 2020;  
Publication 06 November 2020

## Abstract

With the development of the Internet, storage and transmission technologies such as printers and scanners, digital multimedia products are rapidly transmitted through the Internet broadcasting, multimedia works becoming easy to obtain and illegally tampering and copying. The copyright of media works urgently needs to be protected. As an important information security scheme, digital watermarking technology provides a powerful solution to the protection of multimedia works. In this paper, we propose an image digital watermarking algorithm combining discrete wavelet transform, discrete cosine transform and matrix singular value decomposition and new scrambling technique. Furthermore, to improve the robustness of the algorithm, grayscale scrambling and pseudo magic square transform are used. To evaluate our proposed algorithm, we realize the simulation based on Python 3.7. All the simulation results show that our proposed algorithm has strong imperceptibility and robustness.

**Keywords:** Digital watermarking, digital multimedia security, hybrid algorithm, information security, high robustness.

*Journal of Web Engineering, Vol. 19.5–6, 725–746.*

doi: 10.13052/jwe1540-9589.19567

© 2020 River Publishers

## 1 Introduction

Intellectual Property (IP) protection has become increasingly important with the development of digital information distribution. The digital information, including audio, images, video, or conventional text are all stored and transmitted in a digital format. The advantages of digital format are high fidelity and efficiently distribution. However, it can also be disadvantage because digital binary information may be easily copied by anyone with acceptable loss. The digital watermark technique then is developed to solve this problem.

The ideally effective digital watermark technique should be imperceptible, and robust enough to the attacks. Digital watermarks have obvious similarities with paper watermarks. In order to use a technology that can play an anti-counterfeiting and labeling role in digital products, the concept of digital watermarking is proposed. The definition of watermarking is that any processing that may be harmful for watermark detection [1,2]. It is a new and advanced technique that integrates signal processing, digital communication, computer network, cryptography and other multidisciplinary technologies. Digital watermarking technique is a new and advanced technique that integrates signal processing, digital communication, computer network, cryptography and other multidisciplinary technologies. It can use some algorithms to mark some kinds of landmark information as serial numbers, barcodes, and special meanings. Text, etc., can be used to identify the source, version, author, owner, issuer, and legal user's ownership of the data, directly embedded in the multimedia data, but does not have affect on application and the original data. Also, it will not be perceived by human perception system, as hearing and vision. Watermark information can only be detected or extracted through a dedicated detector or reader. Unlike cryptography, digital watermarking technique aims to provide effective content protection for digital multimedia and to make up for some of the deficiencies of cryptography. As one of the most important and effective methods in the field of multimedia data protection, digital watermarking technique does not prevent the occurrence of piracy activities, but it can determine whether the object is protected.

Although the driving force behind the generation and development of digital watermarks is copyright protection and prevention of tampering, digital watermarking is currently used in many occasions. Including broadcast monitoring, operation tracking, content authentication, copy control, covert communication, etc.

(1) Copyright protection

The owner of the digital work can use the key to generate a watermark, embed it in the original data, and then publicly publish the work with the watermark information. When the work is pirated or a copyright dispute arises, the owner can obtain the watermark signal from the pirated works or the watermark works as a basis to protect the owner's rights. When digital watermarking is applied to copyright protection, potential application markets have e-commerce to distribute multimedia content online and offline as well as large-scale broadcast services.

(2) Authentication and integrity check

In many applications, it is necessary to verify that digital content has not been modified or impersonated. Although the authentication of digital products can be accomplished by conventional cryptographic techniques, the advantage of using digital watermarks for authentication and integrity verification is that authentication is inseparable from content, thus simplifying the process. When verifying the digital content in which the watermark is inserted, the watermark must be extracted with a unique key associated with the data content, and then the integrity of the digital content verified by verifying the integrity of the extracted watermark. The application of digital watermarking in authentication mainly focuses on the fields of e-commerce and multimedia product distribution to end users.

(3) Covert communication

With the emergence and development of digital watermarking technology, watermarking technology has achieved certain results in covert communication. The digital watermark hides the message as a watermark in a general digital media file, thereby enabling covert communication. The traditional encryption method makes the encrypted content messy and easier to attract attention. The content embedded in the hidden information by using the watermark technology still appears as an ordinary multimedia file in the transmission process, which reduces the possibility of being attacked.

(4) Copy control

Copy control is used to prevent people from illegally copying and using copyrighted content. Digital watermarking technique can provide a good way to implement copy control. The watermark detection module is pre-installed by the recording equipment manufacturer. When a watermark that is prohibited from being copied is detected, the device prohibits recording, thereby implementing copy control.

As digital watermarking technique has wide application in many fields, the actual performance of it is very important. Unfortunately, none of the existing related research paid enough attention on the attacks with statistical characteristics. To solve the problem mentioned above, we propose a hybrid watermarking algorithm. Specifically, image signal singular value decomposition and image scrambling technique are used, which can ensure high invisibility and let the algorithm have strong resistance to common signal processing and attack. Furthermore, double-scrambling and pseudo magic square transform are combined in our proposed algorithm to enhance the performance facing some specific attacks using statistical characteristics.

The rest of the paper is organized as follows. Some recent related works are introduced in Section 2. Next, a double-scrambling algorithm based on 2D-Arnold and Pseudo Magic Square transform is proposed to resolve the security problem during digital media transmission in Section 3. Furthermore, a method using new scrambling technique is illustrated to improve the robustness of the algorithm in Section 4. Simulation is realized and analyzed in Section 5. At last, we conclude the paper in Section 6.

## **2 Related Works**

Digital watermarking is an information hiding technique that embeds secret and private information into digital carriers such as digital audio, images and video, in order to protect copyright of digital innovation, detect the authorized work, locate piracy or provide other options for copyright protection. Many researchers have made useful research on both algorithms and some many attacks.

### **2.1 DWT-DCT-SVD Algorithm and the Related Applications**

Musrrat Ali et al. [3] present another approach applying self-adaptive differential evolution (SDE) based on optimized DWT-SVD. The experimental results show good imperceptibility but not satisfied enough robustness. There are also many other papers [4-7] that use DWT-SVD approach. As it showed from the results of these literatures, in general, DWT-SVD algorithm has good performance in the concealment of watermark, but the watermarked image is not robust enough against various attacks. Besides DWT-SVD, another mainstream algorithm of digital watermarking is based on DCT-SVD. Shankar Parimi [4] et al. proposed a method using novel DCT. In the scheme, digital watermark is inserted to improve security. The algorithm makes it



sure that the visual sense of the original image is guaranteed. Musrrat Ali et al. [8] propose a watermarking approach using DCT-SVD. Not only using scaling factors in image watermarking, they also import another parameter, differential evolution (DE), to find a balance point of imperceptibility and robustness. This scheme has satisfied robustness performance to different common attacks but has clear disadvantages in watermark extraction. J Prasad et al. [9] propose a robust digital image watermarking using DCT based on pyramid transform. Experimental results show that this approach is robust against JPEG attack or other compression attacks. In addition to this, the algorithms based on DCT is clearly satisfied in nice robustness. [10,11]. But the imperceptibility, the peak signal to noise ratio, PSNR value, is low. Tao Wang [12] proposed an algorithm for obtaining robust digital watermarking by image scrambling and SVD, which aims to enhance the robustness and perceived invisibility of embedded watermarks.

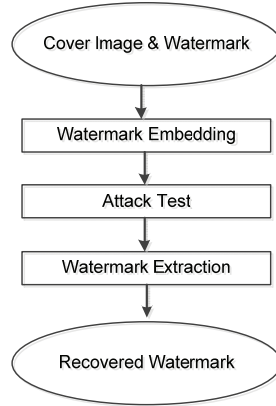
## **2.2 Some Attacks on Digital Watermark**

M. Sharma and S. Shiwani [13] showed the analysis of applying various watermarking algorithm against different noises (Gaussian, Speckle etc). Their work commented on various attacks on the watermarked image aiming at altering the watermark. M.Alirezanejad et al. [14] presented an approach t for recovering watermarks more accurately in spatial domain watermarking. High boost filtering is used prior to performing the watermark extraction process. The experimental results show that the extraction performance of the correlation-based watermarking technique is improved by executing the filter. C. Song et al. Al [15] analyzed many digital watermark attacks and divided them into several categories. They also presented a set of experimental results to show the impact of these attacks on watermarks in various watermarking schemes. In this work, they show that the LSB and DWT technologies do not have full mutual advantage in terms of the robustness of the attacks.

## **3 Double-scrambling Algorithm Based on 2D-Arnold and Pseudo Magic Square Transform**

### **3.1 System Model**

In this paper, a new scrambling technique combing double scrambling and pseudo magic square transform is proposed. After that, I use the proposed scrambling method to optimize the DWT-DCT-SVD digital watermarking algorithm. The whole procedure of applying proposed optimized digital watermarking algorithm is shown as Figure 1.



**Figure 1** Optimized digital watermarking procedure.

### 3.2 Double-scrambling Based on 2D-Arnold Transform

In image processing, traditional 2D-Arnold transform is usually applied in spatial domain. Three or higher dimensional Arnold transform operates in grayscale domain, changing grayscale correlation. However, higher dimensional Arnold transform still has some problems:

- a) Scrambling applied in grayscale domain requires higher order matrix transform with high computational complexity.
- b) Scrambling in spatial domain requires multiple iterations to achieve a satisfactory scrambling effect. At the same time, this scrambling method only disturbs the order of the original image, but does not change the statistical characteristics of the image (such as histogram). It is possible for attackers to judge or destroy confidential information through statistical characteristics.

I proposed an image double-scrambling algorithm for two-dimensional Arnold transform, which uses a two-dimensional Arnold transformation matrix to scramble the position and color information of the image, and the number of scrambling is determined by the randomly generated key.

For image scrambling in spatial domain, apply row-column scrambling transform:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod{n} \quad (1)$$

Where:  $x, y, x', y' \in \{0, 1, \dots, N - 1\}$ ,  $(x, y)$  is the original image pixel position,  $(x', y')$  is image pixel position after scrambling;  $n$  is the order of the digital image matrix.

For image scrambling in grayscale domain, we apply the following equation to each pixel  $h$ :

$$\begin{pmatrix} h'_1 \\ h'_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} h_1 \\ h_2 \end{pmatrix} \pmod{16} \tag{2}$$

Where:  $h_i, h_i' \in \{1, \dots, F\}; i = 1, 2$ . So  $h' = (h_1', h_2')$  is the corresponding pixel value after  $h$  scrambling. Figure 2. shows the entire double-scrambling procedure.

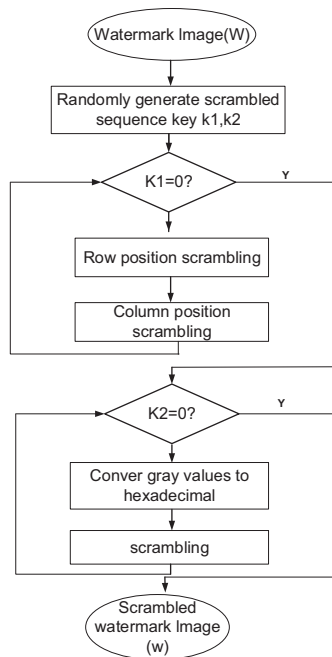


Figure 2 Double-scrambling procedure.

### 3.3 Pseudo Magic Square Transform

Although Arnold transform is simple and easy to operate, the periodic characteristics are too obvious, it can't resist exhaustive attack very well. Pseudo magic square transform offers unique code every time, and the matrix content changes frequently, which can ensure the security very well. Therefore, watermark information is first applied Arnold transform, and then use pseudo

magic square transform, is a good way to destroy the correlation among watermark pixels.

The specific watermark scrambling procedure is as follows:

Step 1: Read scrambled watermark image  $W'$ .

Step 2: Divide  $W'$  into  $4 \times 4$  blocks.

Step 3: Scan watermark image from top to bottom and from left to right, convert the pixel pair  $(x, y)$  one by one. Take the pseudo magic square matrix as an example, substituting pixel pairs  $(x, y)$  into the formula  $f(x, y) = N((y - Ax) \bmod N) + ((y - Bx) \bmod N)$ . The obtained value is matched with the data in Table 1. If the same value matches, the corresponding row number and column number are recorded, are respectively subtracted from the line number and column number of  $(0, 0)$ . The difference pair  $(x_d, y_d)$  is obtained, and the modified pixel pair  $(x', y')$  is obtained by the following two formulas; if there is no identical value match, the pixel value does not change.

$$\begin{aligned} x' &= x + x_d \\ y' &= y + y_d \end{aligned} \quad (3)$$

1	8	13	12
14	11	2	7
4	5	16	9
15	10	3	6

Step 4: Repeat step 3 to the remaining sub-blocks of the watermark image to obtain a scrambled watermark image.

#### 4 Robust Improvement Using New Scrambling Technique

The DCT transform converts the image into frequency domain data: DC coefficient and AC coefficient. DC component indicates the average brightness of the image, and AC can be divided into low and high frequency coefficients respectively. AC represents the energy distribution of the image, and the low frequency part concentrates the highest percentage of the image energy. As a contrast, high frequency coefficient energy is weak. In the DCT domain, different DCT coefficients have distinct effects on the robustness as a watermark carrier. In order to make the watermark have better robustness, the DCT coefficients used to embed the watermark should satisfy the following conditions:

- a) The coefficients can be well preserved after common signal transform and noise interference, that indicates these coefficients may not be excessively processed for signals.
- b) The change in noise interference has a large sensory capacity so that the watermark does not cause a significant change in the visual quality.

Cox et al. believe that the watermark should be placed on the most critical component of the visual system, corresponding to the LF parts of the FD [16]. The reason is that the important components of the image are the main components of the image signal, carrying more signal energy, and retaining the main component even when the image has a certain distortion. The AC low frequency coefficient carries more signal energy, which makes the watermark embedding intensity relatively large, and has very strong robustness to low-pass filtering and loss compression. However, embedding watermark into the AC low-frequency coefficient is more likely to cause image quality reduced, so it is not guaranteed to be invisible.

The DCT coefficient represents the characteristics of image energy distribution from high to low, while DWT has multi-resolution characteristics and has layering characteristics, which enables the embedding and detection of watermarks in a certain sub-band or some sub-bands. Secondly, wavelet transform and Human Visual System (HVS) is consistent with each other. In addition, since wavelet transform has the ability to characterize local features of signals in both time and frequency domains, its characterization and location attack ability is stronger, and the computational complexity is smaller than DCT. However, the coefficients do not have geometric invariance, so the resistance to geometric attacks is not robust, and the watermark information must be synchronized during the extraction process.

The stability characteristics of SVD makes it suitable for application in the field of digital watermarking. First, the stability of the image singular value is high, and the singular value of the image does not change much when the image suffers from small attacks. Thus, if we embed watermark into the singular value of the cover image, as long as the watermarked image suffers from a small external attack, we can extract the watermark information from the decomposed singular value due to the stability of the singular value. Moreover, since the singular value has rotation invariance, it is unique in the application of the watermark. When the watermarked image suffers from a rotation attack, since the singular value is not affected by the image rotation, the watermark can still be well extracted. The advantage of the primary anti-rotation attack is unmatched by other transform domain watermarking algorithms. Second, the singular value, the singular vector

pairs, corresponding to the brightness characteristics of the image, the geometric characteristics of the image. The singular values represent the intrinsic characteristics of the image rather than the visual characteristics, reflecting the relationship between the elements of the image matrix. Therefore, we embed the watermark onto the singular value without damaging the geometrical characteristics of the image, and since the singular value is based on a representation of the relationship between the matrix elements rather than the visual characteristics, the embedding of the watermark on the singular value can be very It is good to ensure the visual invisibility of the watermark, which provides guarantee for the concealment and security of the watermark algorithm.

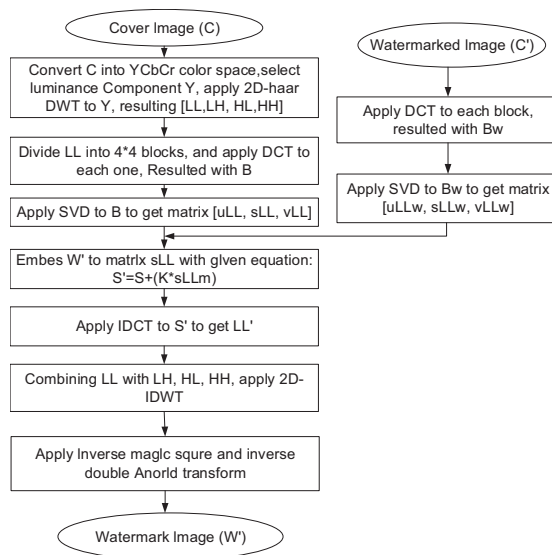
#### 4.1 Watermark Embedding

In previous work, two advanced image watermarking algorithm is proposed: DWT-SVD and DCT-SVD. In my algorithm, the two methods are combined together to enhance imperceptibility and robustness performance.

Watermark Embedding procedure is shown as Figure 3.

Step 1: Load cover image  $C$  and watermark image  $W$  as input.

Step 2: Convert  $C$  to  $YCbCr$  color space, obtained  $[Y, C_b, C_r]$



**Figure 3** Watermark Embedding Procedure.

Step 3: Apply two-level “haar” DWT to  $Y$  to get sub-band components  $[LL, LH, HL, HH]$ , where  $LL$  is the low frequency components and  $[LH, HL, HH]$  constitute high frequency components.

Step 4: Split  $LL$  into small blocks, each of them has  $4 * 4$  size. Apply DCT to each block, resulting  $B$ .

Step 5: Apply Singular Value Decomposition (SVD) to  $B$ , resulting with  $[uLL, sLL, vLL]$ .

$$[uLL, sLL, vLL] = svd(B)$$

Step 6: Apply DCT to each block of  $W$ , resulting  $Bw$ .

Step 7: Apply SVD to  $Bw$ , resulting with  $[uLLw, sLLw, vLLw]$ .

$$[uLLw, sLLw, vLLw] = svd(Bw)$$

Step 8: Embed  $sLLw$  into cover image using equation:  $S' = S * (1 + k * sLLw)$ . Where  $k$  is the scaling factor.

Step 9: Apply IDCT to  $S'$  to get  $LL'$ :

$$LL' = uLL * S'vLL$$

Step 10: Apply 2D-IDWT to  $LL'$  and other previous sub-bands to build watermarked image.

Step 11: Obtain watermarked image  $C'$

## 4.2 Watermark Extraction

The watermark extraction procedure is shown as Figure 4.

Step 1: Load cover image  $C$  and watermarked image  $C'$  as input.

Step 2: Convert  $C$  to  $YC_bC_r$  color space, obtained  $[Y, C_b, C_r]$

Step 3: Apply two-level “haar” DWT to  $C$  to get sub-band components  $[LL, LH, HL, HH]$ , where  $LL$  is the low frequency components and  $[LH, HL, HH]$  constitute high frequency components.

Step 4: Split  $LL$  into small blocks, each of them has  $4 * 4$  size. Apply DCT to each block, resulting  $B1$ .

Step 5: Apply SVD to  $B1$ , resulting with  $[uLL1, sLL1, vLL1]$ :

$$[uLL1, sLL1, vLL1] = svd(B1)$$

Step 6: Split  $B1$  into small blocks, each of them has  $4 * 4$  size. Apply DCT to each block, resulting  $Bw1$ .

Step 7: Apply SVD to  $Bw1$ , resulting with  $[uLLw1, sLLw1, vLLw1]$ .

$$[uLLw1, sLLw1, vLLw1] = svd(Bw1)$$

Step 8: Extract the singular values of the watermark with the following equation:

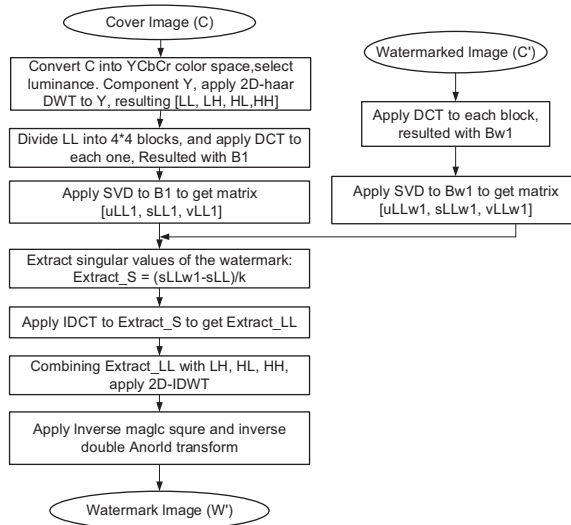
$$Extract\_S = (sLLw - SLL)/k$$

Step 9: Apply IDCT to  $Extract\_S$  to get  $Extract\_LL$ :

$$Extract\_LL = uLL * Extract\_S * vLL$$

Step 10: Apply 2D-IDWT to  $Extract\_LL$  and other previous sub-bands to build watermarked image.

Step 11: Obtain watermark image  $W'$



**Figure 4** Watermark Extraction Procedure.



## 5 Simulation Analysis

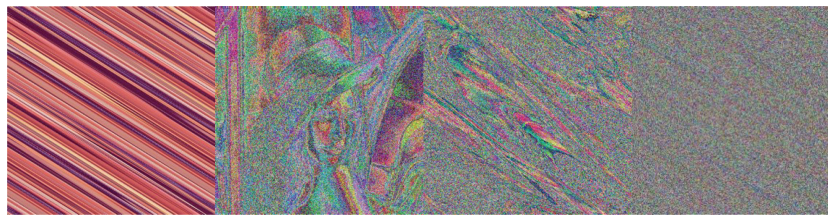
As the color information of the Lena image is much richer than many image and it is more vivid, we select Lena image as the original image in the simulation. Next, we will evaluate our proposed algorithm by three aspects: (1) Results of proposed scrambling method; (2) Results of imperceptibility test; (3) Results of robustness test. Two metrics, peak signal to noise ratio (PNSR) and normalized cross-correlation number (NC), are used as two measurements to evaluate the performance and quality of the watermarked images and watermark extraction.

### 5.1 Simulation Results of Proposed Scrambling Method

We select different  $k$  combinations, and apply the proposed scrambling method the Lena image. The result is shown as Figure 5. We can see that after a small number of iterations, simple position scrambling still can be observed obvious texture, which cannot really hide the image information.

Scrambling the grayscale of an image using a two-dimensional Arnold transform can achieve better results with fewer iterations. However, some areas still have not reached chaotic state. At the same time, scrambling on the position and the pixel at same time can achieve better scrambling effect after a small number of scrambling times, and the image is visually closer to the chaotic state.

Figure 6 shows grayscale histograms of images before and after double scrambling. The grayscale histogram change of the image before and after scrambling is obvious, and the statistical information of the image before and after scrambling is completely different, that is, the information of the original image cannot be obtained from the grayscale information of the image after scrambling.



(a)  $k = (3,0)$       (b)  $k = (0,3)$       (c)  $k = (1,1)$       (d)  $k = (3,3)$

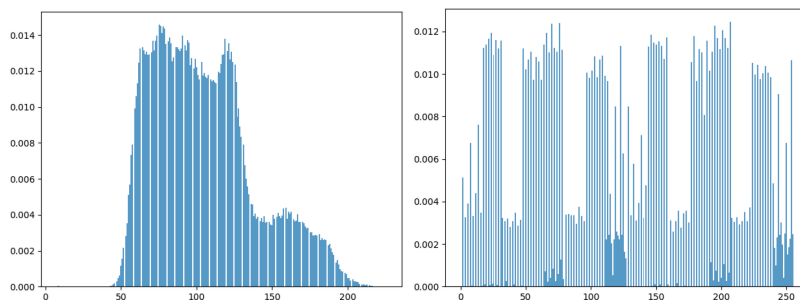
**Figure 5** Arnold transform double-scrambling effect.

For the security performance of the algorithm, we select different  $k$  combinations by random. Different keys lead to different image scrambling procedure. Only the true key owners can recover the original image correctly. Figure 7 shows the results using wrong keys to recover the original image.

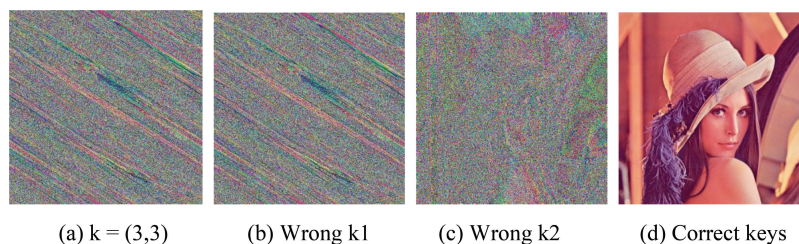
After applying the improved Arnold transform method to the image, we obtain image  $I$ . Apply pseudo magic square transform to  $I$  with formula:

$$f(x, y) = Ni(y - Ax) \bmod N + ((y - Bx) \bmod N)$$

Let  $N = 4, A = 2, B = 3$ . Figure 8 shows the comparison of the original image and image after transform.

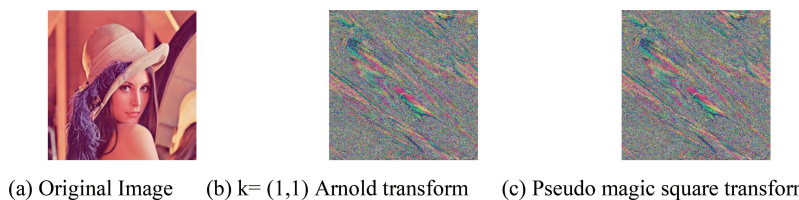


**Figure 6** Image gray histogram comparison before and after double scrambling.



(a)  $k = (3,3)$  (b) Wrong  $k_1$  (c) Wrong  $k_2$  (d) Correct keys

**Figure 7** Image recover effect with wrong keys.



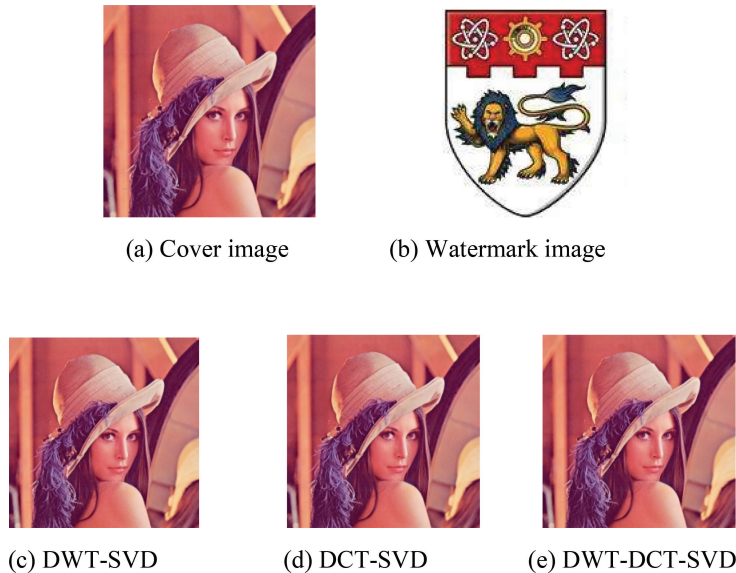
(a) Original Image (b)  $k = (1,1)$  Arnold transform (c) Pseudo magic square transform

**Figure 8** Comparison of the original image and image after transform.

## 5.2 Simulation Results of Imperceptibility Test

To evaluate the imperceptibility and robustness performance of the proposed watermarking algorithm, and make comparison with the previous algorithm, programming experiments are carried out based on Python 3.7 platform. The experiments are performed on the typical Lena cover image with size of  $512 \times 512$ . The original cover image is shown in Figure 9(a). The watermark image has size of  $256 \times 256$ , as shown in Figure 9(b). It is inserted to the cover image with three different algorithms, the watermarked images appear in Figure 10(c)–(e), using DWT-SVD, DCT-SVD and DWT-DCT-SVD method respectively.

From the perspective of imperceptibility, all the above algorithms applied in frequency domain, thus for human vision, it is hard to distinguish the difference among them. In the proposed watermarking algorithm, there is a scale factor  $k$  is used. Different  $k$  values can affect the imperceptibility and extracted results. The following Table 2 shows the experimental results of applying different  $k$ .







**Figure 9** Simulation Results of Imperceptibility Test

**Table 2** psnr and NC using different k values

k Value	PSNR	NC
0.05	55.1049	0.8010
0.1	52.9942	0.9241
0.2	50.4224	0.9523
0.3	47.1314	0.9669
0.5	43.2552	0.9789

**Table 3** DWT-DCT-SVD vs. proposed method

Technique	Watermarked Image	Extracted watermark	PSNR	NC
DWT-DCT- SVD			56.1048	0.9309
Proposed Method			43.2552	0.9789

The above table shows the best k value should be 0.5. Then we choose  $k = 0.5$  as the scale factor and apply it in the following procedure.

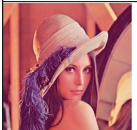





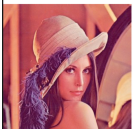


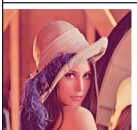


If we don't apply proposed scrambling method to preprocess the watermark image, just apply DWT-DCT-SVD method to Lena image, the extracted watermark image shows a clear diagonal line. After using proposed scrambling method, diagonal distortion is scrambled by the proposed Arnold transform to the leftmost column. The visual effect has been significantly improved, and the NC value has also been partly improved. Table 3 shows the comparison.

To further test invisibility and effectiveness of the proposed algorithm, we embed different watermark image to the same host image and embed same watermark to different cover image respectively.













The above test shows that for the same image, after embedding different watermark images by the watermark algorithm proposed in this paper, the watermark can be detected and extracted. Next, we use different cover images, embedding the same watermark image.

Embedding the same watermark to different images has a good performance in terms of imperceptibility and validity, and the preprocessing before transforming the watermark image can improve the subjective and objective performance of the algorithm. The test results of the above parts show that the proposed algorithm is effective and has good applicability.

**Table 4** Effect of embedding different watermark to same image

Watermarked Image	Embedded Watermark	Extracted Watermark	PSNR	NC
			43.2552	0.9789
			42.5625	0.9865
			48.1594	0.9521
			58.0248	0.9140

**Table 5** Effect of embedding same watermark to different image

Watermarked Image	Embedded Watermark	Extracted Watermark	PSNR	NC
			43.2552	0.9789
			43.2251	0.9624
			42.9842	0.9713
			41.5362	0.9532

### 5.3 Simulation Results of Robustness Test

The following part is a test of whether the robustness of the digital watermarking algorithm proposed in this paper is satisfactory for different attacks. The test process also includes the use of transform preprocessing watermarks and non-preprocessing watermarks. We use Lena image as the cover image and NTU badge image as the watermark image.

**Table 6** Robustness test results

	Attacked watermark image	NC	NC in [13]
Chop 30% 358 × 512		0.9142	0.9006
180° Rotation		0.8845	0.8243
10% Brighter		0.9842	0.9697
Randomly Cover		0.9531	0.9328
Add salt and pepper noise		0.9625	0.9475
Gaussian Low-pass Filter		0.9734	0.9024
Image blur		0.9696	0.9702
Grayscale process		0.9732	0.9877

Table 6 lists the value of the watermarked image and the watermark NC value extracted by attacks, and compares it with the SVD algorithm in the reference [17] and the DCT-SVD algorithm in the reference [17], objectively illustrate the proposed improved algorithm has better robustness and visual effects. It can be seen from the data in Table 5 that except Grayscale process, the robustness of other attacking algorithms has been improved to varying degrees.

## **6 Conclusions**

In this paper, an image digital watermarking algorithm based on DWT- DCT-SVD is proposed with reference to some effective algorithms. In order to further improve the performance of the watermark, the preprocessing of the watermark image using double-scrambling and pseudo magic cube transform is introduced. The algorithm uses 8-bit gray image as the watermark signal, uses the transform domain coefficient as the watermark carrier, embeds the watermark in the transform domain, and achieves the purpose of embedding the watermark without reducing the image quality. The watermark performance is tested by a number of experiments on the validity and invisibility of the watermarking algorithm and the robustness against conventional image processing methods on the Python platform. The experimental results show that the proposed algorithm can satisfactorily meet the basic characteristics of digital watermark, and can resist the common signal processing and image processing attacks, and the speed of operation is fast.

## **References**

- [1] Sanjay Kumar and Ambar Dutta, "A Study on Robustness of Block Entropy Based Digital Image Watermarking Techniques with respect to Various Attacks", IEEE International Conference On Recent Trends In Electronics Information Communication Technology, May 20-21, 2016, India.
- [2] R. Gayathri, Dr. V. Nagarajan "Secure data hiding using Steganographic technique with Visual Cryptography and Watermarking Scheme", IEEE ICCSP 2015 conference 978-1-4799-8081-9/15 © 2015 IEEE.
- [3] Shankar Parimi, A. SaiKrishna, N. Rajesh Kumar, N.R. Raajan "An imperceptible Watermarking Technique for Copyright content using Discrete Cosine Transformation", 2015 International Conference on Circuit, Power and Computing Technologies [ICCPCT].

- [4] S. Abolfazl Hosseini, Arash Saboori “A New Method for Color Image Watermarking Based on Combination of DCT and PCA”.
- [5] R. Gayathri, Dr. V. Nagarajan “Secure data hiding using Steganographic technique with Visual Cryptography and Watermarking Scheme”, IEEE ICCSP 2015 conference 978-1-4799-8081-9/15 © 2015 IEEE.
- [6] Olcay Duman and olcay Akay “A New Method of wavelet Domain WaterMark Embedding and Extrection using Fractional Fourier Transform” (page no 187–191).
- [7] Shiji Johny, Anil Antony “Secure Image Transmission Using Visual Crptography Scheme without Changing the Color of the Image”, ICETECH’15© 2015 IEEE.
- [8] Mishra A, Agarwal C, Sharma A, et al. “Optimized gray-scale image watermarking using DWT-SVD and Firefly Algorithm.” *Expert Systems with Applications*, 2014, 41(17): 7858–7867.
- [9] Ali M, Chang W A. “An optimized watermarking technique based on self- adaptive DE in DWT-SVD transform domain.” *Signal Processing*, 2014, 94(1): 545–556.
- [10] Ali M, Chang W A, Pant M. “A robust image watermarking technique using SVD and differential evolution in DCT domain.” *Optik - International Journal for Light and Electron Optics*, 2014, 125(1): 428–434.
- [11] Maheshwari J P, Kumar M, Mathur G, et al. “Robust Digital Image Watermarking using DCT based pyramid transform via image compression// International Conference on Communications and Signal Processing.” IEEE, 2015:1059-1063.
- [12] Chunping Fu, “Research on a Digital Watermarking Algorithm Based on Sum”, Suzhou University, 2008.
- [13] Yuqi He, Yan Hu, “A proposed Digital Image Watermarking Based on DWT- DCT-SVD”, 2018 2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC 2018).
- [14] S. Kaur, R. Gill, R. Kaur, “Comparative Analyses of YCbCr Color Space and CIELab Color Space Based On DWT and SVD” First International Conference on Next Generation Computing Technologies.
- [15] S. K. Prajapati, A. Naik and A. Yadav, “Robust Digital Watermarking using DWT-DCT-SVD”, *International Journal of Engineering Research and Applications* vol. 2, no. 3, pp. 991–997, May–Jun 2012.



- [16] D. Kirovski and F. A. P. Petitcolas, "Blind pattern matching attack on watermarking systems", IEEE Transactions on Signal Processing, Volume 51, Issue 4, pp. 1045 –1053, 2003.
- [17] Prachi Pradeep Nerurkar, Dr. A. C. Phadke, "Digital Image Watermarking Using Firefly Algorithm", 978-1-5386-5257-2/18/\$31.00 © 2018 IEEE.

## Biographies



**Yi Xie** is a Ph.D. Candidate at the Wuhan University, China since 2012. He obtained his master and bachelor degree in 2008 and 2006 from Nanyang Technological University of Singapore and University of Electronics Science and Technology of China respectively. His research interests include digital watermarking, network security, blockchain and IOT.



**Yulin Wang** is a full professor and PhD supervisor in International School of Software, Wuhan University, China. He got PhD degree in 2005 in Queen Mary, University of London, UK. Before that, he has worked in high-tech industry for more than ten years. He has involved many key projects, and hold 8 patents. He got his master and bachelor degree in 1990 and 1987 respectively from Xi-Dian University, and Huazhong University of Science and Technology (HUST), both in China. His research interests include digital rights management, digital watermarking, multimedia and network security,

and signal processing. In recently 10 years, Prof. Wang has published as first author 3 books, 40 conference papers and 45 journal papers, including in IEEE Transactions and IEE proceedings and Elsevier Journals. Prof. Wang served as editor-in-chief for International Journal of Advances in Multimedia in 2010.



**Maode Ma** received his Ph.D. degree in computer science from Hong Kong University of Science and Technology in 1999. Now, he is an Associate Professor in the School of Electrical and Electronic Engineering at Nanyang Technological University in Singapore. He has extensive research interests including network security and wireless networking. He has led and/or participated more than 20 research projects funded by government, industry, military and universities in various countries. He has been a general chair, technical symposium chair, tutorial chair, publication chair, publicity chair and session chair for about 100 international conferences. He has been a member of the technical program committees for about 200 international conferences. Dr. Ma has more than 400 international academic publications including about 220 journal papers and over 210 conference papers. He currently serves as the Editor-in-Chief of International Journal of Computer and Communication Engineering and Journal of Communications. He also serves as a Senior Editor for IEEE Communications Surveys and Tutorials, and an Associate Editor for International Journal of Security and Communication Networks, International Journal of Wireless Communications and Mobile Computing and International Journal of Communication Systems. He had been an Associate Editor for IEEE Communications Letters from 2003 to 2011 and an Associate Editor for International Journal of Network and Computer Applications from 2007 to 2015. Dr. Ma is a Fellow of IET, a senior member of IEEE, and a member of ACM. He is the Secretary of the IEEE Singapore Section. He is also the Chair of the ACM, Singapore Chapter. He is serving as an IEEE Communication Society Distinguished Lecturer from 2013 to 2016.