



**NANYANG  
TECHNOLOGICAL  
UNIVERSITY**

## **Design of Information Hiding in Image**

**CAO YUN**

**SCHOOL OF ELECTRICAL AND ELECTRONIC ENGINEERING**

**2019**

<b>ABSTRACT</b>	I
<b>LIST OF FIGURES</b>	II
<b>LIST OF TABLES</b>	III
<b>CHAPTER 1 INTRODUCTION</b>	1
1.1 Digital Watermarking Background	1
1.2 Motivation	3
1.3 Major Contribution	4
1.4 Organization	5
<b>CHAPTER 2 LITERATURE REVIEW</b>	6
2.1 Basic Principle of Digital Watermark	6
2.1.1 Spatial Domain Algorithm	6
2.1.2 Frequency Domain Algorithm	7
2.1.3 Properties of Digital Watermark	9
2.1.4 Attacks on Digital Image Watermarking	9
2.1.5 Performance Measurements	10
2.2 Literature Survey	13
2.2.1 DWT-DCT-SVD Approach	13
2.2.2 Attacks on Digital Watermark	14
2.2.3 Different Algorithms Application	15
<b>CHAPTER 3 AN OPTIMIZED ALGORITHM</b>	17
3.1 System Model	17
3.2 Mathematic Basis	17
3.2.1 Singular Value Decomposition	17
3.2.2 DWT-SVD Scheme	18
3.2.3 DCT-SVD Scheme	20
3.2.4 Two-Dimensional Arnold Transform	22

3.2.5	Magic Square Transform	24
<b>3.3</b>	<b>Double-scrambling Algorithm Based on 2D-Arnold and Pseudo Magic Square Transform</b>	<b>25</b>
3.3.1	Double-scrambling Based on 2D-Arnold Transform	25
3.3.2	Pseudo Magic Square Transform	27
<b>3.4</b>	<b>DWT-DCT-SVD Digital Watermarking Algorithm Using New Scrambling Technique</b>	<b>28</b>
3.4.1	Watermark Embedding	30
3.4.2	Watermark Extraction	31
	<b>CHAPTER 4 EXPERIMENTAL RESULTS</b>	<b>34</b>
4.1	Experimental Results of Proposed Scrambling Method	34
4.2	Experimental Results of Imperceptibility Test	36
4.3	Experimental Results of Robustness Test	40
4.4	Analysis and summary	43
	<b>CHAPTER 5 CONCLUSION</b>	<b>45</b>
	<b>REFERENCES</b>	<b>47</b>

# 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. The development of cryptography and information security technologies has provided support for content security and copyright protection for multimedia works. As an important information security scheme, digital watermarking technology provides a powerful solution to the protection of multimedia works.

Based on the previous work, this paper completed the following work in response to the current development of digital watermarking.

1) Understand the characteristics, classification and application of digital watermarking technology, review the research background of digital watermarking technology, study several common transformations of image domain watermarking in transform domain and image scrambling technology, based on existing algorithms. An image digital watermarking algorithm combining discrete wavelet transform, discrete cosine transform and matrix singular value decomposition and new scrambling technique is proposed. According to the shortcomings of related algorithms, grayscale scrambling and pseudo magic square transform is used to improve the robustness of the algorithm.

2) Experiments based on Python 3.7 are made to test the proposed watermarking algorithm. All the experimental results show that the image watermarking algorithm based on DCT-DWT-SVD and scrambling proposed in this paper has strong imperceptibility and robustness. When the watermark is added, the image undergoes common signal processing such as chopping, rotation, filtering, etc. After that, the presence of the watermark can still be detected and the calculation speed is faster.

**Key words:** Digital Watermarking, DWT-DCT-SVD, Double-scrambling, Arnold Transform, Pseudo Magic Square Transform, Robustness

# List of Figures

Figure 2.1 2-level Discrete Wavelets transform Decomposition.....	12
Figure 3.1 Optimized digital watermarking procedure.....	17
Figure 3.2 DWT-SVD watermark embedding procedure.....	19
Figure 3.3 DWT-SVD watermark extraction procedure.....	20
Figure 3.2 DCT-SVD watermark embedding procedure.....	21
Figure 3.2 DCT-SVD watermark extraction procedure.....	22
Figure 3.6 Arnold Transform.....	23
Figure 3.7 Double-scrambling procedure.....	26
Figure 3.8 Pseudo magic matrix.....	27
Figure 3.9 Watermark embedding procedure.....	31
Figure 3.10 Watermark extraction procedure.....	32
Figure 4.1 Arnorld transform double-scrambling effect.....	34
Figure 4.2 Image gray histogram comparison before and after double scrambling.....	35
Figure 4.3 Image recover effect with wrong keys.....	35
Figure 4.4 Comparison of the original image and image after transform.....	35
Figure 4.5 (a)-(e). (a) Cover image, (b) Watermark image, (c) Watermarked image using DWT-SVD, (d)Watermarked image using DCT-SVD, (e) Watermarked image using DWT-DCT-SVD method.....	36

# List of Tables

Table I. Typical watermarking techniques comparisons.....	8
Table II. PSNR and NC using different $k$ values.....	37
Table III DWT-DCT-SVD vs. proposed method.....	37
Table IV. Effect of embedding different watermark to same image.....	38
Table V. Effect of embedding same watermark to different image.....	39
Table VI. Robustness test results.....	40

# Chapter 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. The definition of watermarking is that any processing that may be harmful for watermark detection.[1-2] There are various representative classes of common attacks that can threaten the watermarked image, including scaling, cropping, rotation, adding noise etc.

## 1.1 Digital Watermarking Background

Cryptography is one of the most common and important means of data protection. It can ensure that data is not illegally obtained during transmission, but it cannot solve the problem of illegal copying and tampering of data. Because once the data is decrypted, the cryptography technology is no longer protective, and the user can continue to copy, tamper with, and propagate the decrypted copy of the content. In addition, if the attacker tampers with the encrypted data information, the recipient cannot correctly obtain the decrypted data file even if it is authorized to allow decryption. These problems make cryptography a little inadequate in terms of data protection.

Digital watermarks has solved the above weaknesses of cryptography, and more effectively protects the security of digital works. People naturally remind of watermarks

in paper currency, which can prevent counterfeiting. The earliest watermarks occur back to about 700 years ago, when about 40 paper factories in a town in Italy produced paper of different styles, qualities and prices. The competition between them was fierce. In order to track the source of the paper and to identify the paper style and quality, a watermarking technique was invented and used. By the end of the century, the Englishman William Congreve invented a technique for making colored watermarks that inserted dyed material into paper currency during the manufacture of it. The paper's watermark can indicate the manufacturer and trademark of the paper. It can also be used to indicate the style, quality and strength of the paper, the manufacture date and the basis for identification of the paper. In modern times, watermarks are widely used in currency, securities, bills, and various papers that require identification to serve as a marker and anti-counterfeiting.

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. 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. Digital watermarking technique does not prevent the occurrence of piracy activities, but it can be determined whether the object is protected. Protecting, monitoring the spread of protected data, identifying authenticity and illegal copying of data, resolving copyright disputes and providing evidence is one of the most important and effective methods in the field of multimedia data protection.



## 1.2 Motivation

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 wild application in many fields, the actual performance of it is very important. After making literature survey, I found that in the previous research, attacks using statistical characteristics are not paid enough attention. To solve that problem, an algorithm using double-scrambling technique and pseudo magic transform is proposed.

### 1.3 Major Contribution

In my preliminary preparation, I conclude the major technique in information hiding field, including watermarking, cryptography etc. Also, digital watermarking algorithm research is done and simulated based on Python.

The research goal is to propose a digital watermarking algorithm based on image signal singular value decomposition and image scrambling technique. The algorithm can maintain high invisibility and has strong resistance to common signal processing and attack, can effectively achieve image information integrity and copyright protection.

The proposed technique combining double-scrambling and pseudo magic square transform enhances the performance facing some specific attacks using statistical characteristics. With the new scrambling technique, DWT-DCT-SVD digital watermarking shows better performance than the previous algorithms.

## 1.4 Organization

The dissertation is divided into five chapters:

The first chapter mainly describes the development background and main application of digital watermarking technology and explains the main research work content and the structure of the article.

The second chapter introduces the basic principles of digital watermarking technology in detail, including the basic concept and system framework of watermark, the characteristics of digital watermarking, the classification of digital watermark, the attack and the performance evaluation of watermark. Then some classic and newly proposed digital watermarking algorithms are briefly described

The third chapter introduces the mathematical theoretical basis involved with the proposed algorithm, including discrete wavelet transform, discrete cosine transform, singular value decomposition and image scrambling transform technology. Combing with a new double-scrambling technique based on two-dimensional Arnold transform and pseudo magic square transform, a watermark algorithm based on DWT-DCT-SVD method is proposed.

The fourth chapter shows the experimental results of scrambling, imperceptibility and robustness test of proposed watermarking algorithm. Comparison is made with proposed and previous methods.

The fifth chapter summarizes the work of the full paper and puts forward the prospects for future work.

# Chapter 2 Literature Review

## 2.1 Basic Principle of Digital Watermark

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.

For signal processing, digital watermark embedded into cover image can be regarded as adding a weak signal compared to the strong background of the carrier. In general, As long as signal strength of the embedded components is lower than the human visual system contrast threshold, the existence of the signal cannot be perceived.

### 2.1.1 Spatial Domain Algorithm

Digital watermarking can be classified as:

*Spatial domain(SD)*- The transform is completed on the image pixel values.

*Frequency domain(FD)*- Transform is completed on frequency components.

The SD watermarking techniques are:

***Least significant bit (LSB)***: In LSB method, the least significant bit pixels of the original image are used to embed watermark. LSB supports large information capacity and has little influence on original image. This algorithm is also simple in coding complexity but bit robust against attacks.

***Patchwork Algorithm***: This method uses pseudorandom statistical model by inserting a patchwork imperceptible with Gaussian distribution.

***Correlation based Techniques***: This method adds pseudorandom noise to the watermarked images. The mission of decoder is finding the correlation between watermarked images and random noise. Detection can be completed only if the value does not exceed a threshold limitation.

In summary, although the spatial domain algorithm is simple to implement, it has

less embedded information and poor robustness. Generally, previous watermarks use this algorithm, and algorithms using this technique alone have rarely been seen now.

### 2.1.2 Frequency Domain Algorithm

The watermarking techniques used in frequency domain, compared with that in spatial domain, the capacity of data hiding is much more robust against various attacks. The techniques used in FD watermarking are:

***Discrete Fourier Transform (DFT):*** The advantages of DFT include rotation resistance, translation immutability and strongly robust against geometric attacks.

***Discrete Cosine Transform (DCT):*** Comparing with using complex computation in DFT, in DCT, the images are transformed and divided into cosine frequencies with diverse amplitudes. For some special applications, like pattern recognition, DCT is an efficient method. However, the disadvantage is not as robust as DWT against geometric attacks.

DCT's procedures are:

- Split the original image into various blocks without overlapping.
- Calculate each block's DCT coefficients.
- Use Human Visual System (HVS) Blocks selection criteria.
- After the first three steps, highest coefficients are selected in the output.
- Watermark is embedded among the calculated coefficients.
- Inverse Discrete Cosine transform (IDFT) is applied to each block.

***Discrete Wavelets Transform (DWT):*** Images are divided into various sub bands with different resolution and decomposed to disparate levels. The images are divided into four levels:

- *LL*: Low frequency components of the original images.
- *LH*: Vertical components of the original images.
- *HL*: Horizontal components of the original images.
- *HH*: High frequency components of the original images.

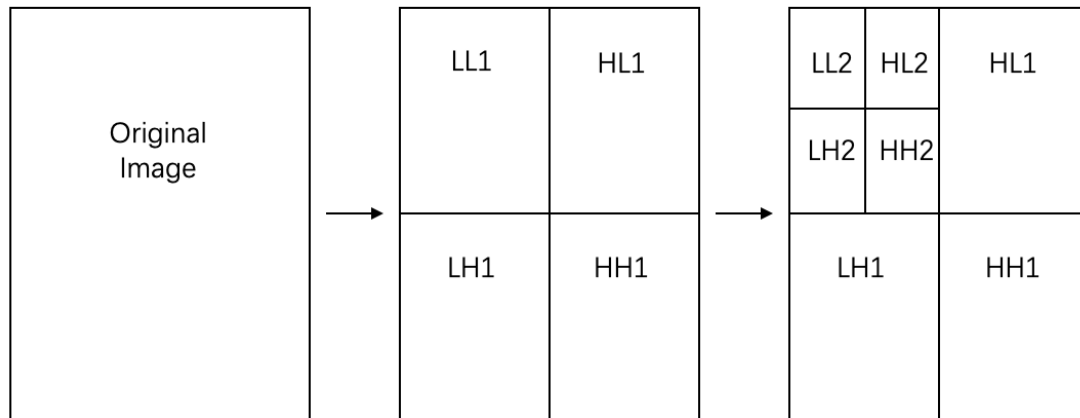


Figure 2.1 2-level Discrete Wavelets transform Decomposition

For the algorithm DWT combined with **SVD** (Singular Value Decomposition), the stable features in the image are mainly used as a guide for extraction, and the feature values of the image matrix are generally used. Compared with DWT, the anti-interference ability is poor, and the amount of watermark information that can be attached is smaller.

Techniques	Advantages	Disadvantages
LSB	<ol style="list-style-type: none"> <li>1. Low implementation complexity.</li> <li>2. Low perception for human eyes.</li> </ol>	<ol style="list-style-type: none"> <li>1. Poor Robustness against scaling, cropping etc.</li> <li>2. High sensitivity to noise.</li> </ol>
DCT	Watermark is inserted into the mid frequency range, which provides acceptable perceptual loss and robustness against attacks as well.	In quantization process, frequency components in a n image that higher than middle range frequency are suppressed.
DWT	<ol style="list-style-type: none"> <li>1. Better localized performance in both SD and FD.</li> <li>2. Much higher compression ratio.</li> </ol>	<ol style="list-style-type: none"> <li>1. Higher computation complexity.</li> <li>2. Larger Compression time cost.</li> </ol>

DFT	Better recovering performance in geometric distortion, because it is invariant to rotation, scaling and translation.	Hard to implement due to high computation cost.
-----	--	---

Table I. Typical watermarking techniques comparisons

### 2.1.3 Properties of Digital Watermark

To judge the quality of a digital watermarking technique, first we explain the important properties based on the watermarking systems:

- a) **Effectiveness:** The probability of detected message in the watermarked image, it should be as high as close to 1.
- b) **Robustness:** In transmission there are various kinds of attacks including scaling, rotating, adding noise etc. which can significantly reduce digital watermark quality. Robustness indicates that the embedded digital watermark must be able to resist both unintentional and intentional attacks that may be encountered during transmission, so that the watermark information can still be extracted.
- c) **Imperceptibility:** The primary feature of digital watermark is imperceptibility, also known as transparency. Imperceptibility is the level of the host signal changes due to watermark embedding. After embedding the digital watermark in the protected information, it should not cause a significant drop in the quality of the original host and a significant change in vision, and does not affect the normal use.

In general, while satisfying the high robustness requirements of digital watermark, it is desirable that the embedded watermark has good imperceptibility. Therefore, designing a watermarking algorithm always requires the balance between imperceptibility and robustness. The watermarking algorithm should be an optimal solution of both of them.

### 2.1.4 Attacks on Digital Image Watermarking

Watermark attack is any processing that may reduce the watermark extraction

accuracy rate. It can be divided into four main types:

i) Geometry, ii) Removal, iii) Protocol, iv) Cryptographic.

Each of them can be further divided into various specific subclasses.

Geometric attacks are basic geometric transformations, which do not remove the digital watermark from the images but disturb the synchronization of watermark detection.

Geometric attacks include 4 subclasses:

- Rotation
- Scaling
- Cropping
- Translation

Removal attacks attempt to completely take the watermark out from the images without destroying watermark algorithm security. Removal attacks can be divided into 4 sub-classes:

- Blur
- Adding Noise
- Median Filter
- Sharpen

Protocol attacks are attacks that other watermark is added to the cover images. Protocol attacks are divided to 2 sub-classes:

- Copy attack
- Invertible

Cryptographic attacks are attacks that tend to destroy the security method of watermark scenario.

## **2.1.5 Performance Measurements**

The most critical properties of evaluating digital watermarking are invisibility, robustness and watermarking capacity. The performance evaluation of digital watermark mainly focuses on the performance of these three aspects.

The basis of digital watermarking is to use the human eye's insensitivity to image



signals. The human eye has a great redundancy in the image. Image information hiding requires embedding information into the image without visual abnormality. Digital watermark embedding can be regarded as a special case of hiding information. In general, for the same algorithm, the larger the amount of information embedded in the image, the greater the modification to the host data and the worse the visual effect of the image. In other words, for the same embedding algorithm, the degree of change of the carrier image data is directly proportional to the information capacity of data embedded. However, for different embedding algorithms, the amount of embedded data is not necessarily directly related to the visual effect of the carrier image. For different embedding algorithms, the amount of data embedded can be more or less, and the degree of change to the image of the carrier is different, but the visual effects obtained by both can be similar. Therefore, a good watermarking algorithm should be able to insert more information capacity and cause less visual perception.

The robustness of the watermark depends on the amount of information embedded and the strength of the watermark embedding. The greater the amount of information embedded, the lower the robustness of the watermark. Greater the strength of watermark embedded, higher the robustness. There is a trade-off between the embedding intensity of the watermark and the perceptibility of the watermark. The watermark is highly robust and requires more reliable embedding scheme, which in turn improves the perceptibility of the watermark.

To evaluate the performance and quality of watermarked images and watermark extraction, the common measurements are Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) etc.

MSE can directly reflect the changes of the assessment object, and the behavioral characteristics of the assessment object can be observed by the MSE value. In watermarking technique, the purpose of using MAE or MSE is to make comparison between the host and recovered image pixel-by-pixel. The mathematic expressions of MSE are:

$$MSE(W, C) = \frac{1}{M} \sum_{m=1}^M \sum_{n=1}^N [C(m, n) - W(m, n)]^2$$

Where W and C are watermarked image and cover image respectively.

PSNR is another important and widely applied performance measures used for distortion calculation. The peak signal to noise ratio PSNR is a value that shows the ratio of the maximum power of the signal to the noise power. Usually, image compression can cause the output somewhat different from the host image. To measure the quality of the processed image, we usually refer to the PSNR value to determine that a process is not satisfactory enough. For two-dimensional images of size M\*N, PSNR is simply defined by mean square error

$$PSNR = 10 \log_{10} \frac{255 \times 255}{MSE}$$

Higher PSNR values and lower MSE values, better the watermarking performance. Both of the two parameters measure the watermarking quality degradation.

After the digital watermark is extracted from the image to be detected, its fidelity depends on the subjective view of the observer. The experience of the observer, the sensitivity of the image, etc. are related to many factors, and have great randomness. The robustness strength of watermarked image can be calculated by the similarity values of original host image and watermarked image. To objectively evaluate the degree of the similarity between the extracted watermark and the original one, a normalized cross-correlation number NC is usually used for a 2D-image of size M\*N. NC is described as follows:

$$NC = \frac{\sum_{x,y} p_{x,y} \tilde{p}_{x,y}}{\sum_{x,y} p_{x,y}^2}$$

So far, there is a lack of good objective evaluation methods to reasonably evaluate digital watermarking algorithms. We need objective evaluation methods to evaluate the invisibility of a digital watermarking algorithm, the robustness and security of the attack, and whether this algorithm is practical. The results of the study indicate that these metrics are not well correlated with the human visual system. Depending on the type of noise, or some human interface have different effects on the image, some images with high PSNR leave the impression with poor quality, while some images with low

PSNR give the acceptable impression. If the above metric is used to calculate the distortion of the image without being associated with subjective testing, it may cause misleading of the distortion metric. Therefore, we need both subjective and objective aspects simultaneously evaluate whether a digital watermarking algorithm is satisfactory.

## **2.2 Literature Survey**

### **2.2.1 DWT-DCT-SVD Approach**

Digital watermarking based on DWT is an important algorithm. Anurag Mishra et al. [3] proposed a digital watermarking scheme based on DWT-SVD. First Three-level DWT is applied to the original image and then using multiple scaling factors (MSFs) to embed watermark image in the LL3 sub-band coefficients' singular values. Experimental results show prominent imperceptibility and good robustness for this algorithm.

Further, Musrrat Ali et al. [4] present another approach applying self-adaptive differential evolution (SDE) based on optimized DWT–SVD, which can be divided into four steps:

- 1) For the cover image, first apply Two-Level DWT and SVD.
- 2) To make the watermark imperceptible, apply One-Level DWT to it.
- 3) Apply SVD to each sub-band of the previous result in order to scale it down by multiplying various scaling factors.
- 4) Embed the scaled components to corresponding blocks positions in the singular value matrix of the cover image.

The experimental results show good imperceptibility but not satisfied enough robustness.

There are also many other papers [5,6,7,8] 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 [5] 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. [9] 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, achieved by three following steps:

- 1) Divide the cover image into blocks and apply DCT.
- 2) Each DC coefficient is collected to rebuild a low-resolution approximation image then apply SVD to it.
- 3) Embed singular values of watermark into the coefficients.

This scheme has satisfied robustness performance to different common attacks but has clear disadvantages in watermark extraction. J Prasad et al. [10] 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. [11,12]. But the imperceptibility, the peak signal to noise ratio, PSNR value, is low.

### **2.2.2 Attacks on Digital Watermark**

During the past decades, a number of studies are presented on the effects of various types of digital watermarking attacks. In this part, a subset of such studies is illustrated.

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. In the analysis, the advantages of their proposed attacks analysis are

concluded:

- 1) Results proved the effective applicability for digital watermarking.
- 2) Algorithm is robust to different noise attacks.
- 3) The algorithm has good embedding capacity and does not degrade the quality of the watermark image.

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.

### **2.2.3 Different Algorithms Application**

Tao Wang [16] 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, followed by three steps:

- 1) Perform a scrambling encryption on the watermark and carrier images.
- 2) Partition the scrambled image and decompose each partition using SVD.
- 3) Define quantization parameters to modify the singular values of each partition and insert the watermark into the feature domain.

The experimental results show that the algorithm has a high effect in protecting the invisibility of the inserted watermark. The algorithm is also very robust to image processing methods (such as JPEG compression and filtering) as well as cropping, rotation and scaling.

Prachi Pradeep Nerurkar et. [17] introduced a new technology for advanced image watermarking using the Firefly Algorithm (FA). The main focus of this paper is to insert an imperceptible watermark (logo) image into the main image, the ultimate goal is that the intensity of the image will be expanded. In the proposed system, two strategies are used to implant the watermark. The first is a discrete wavelet transform (DWT) with singular value decomposition (SVD) and the other is a discrete cosine transform (DCT) with SVD. The FA is stimulated by the flashing behavior of fireflies. The idea behind FA is that fireflies have low brightness and pull in the direction of fireflies with higher brightness. A structural similarity index measure (SSIM) is proposed to illustrate the robustness and invisibility of the watermarking scheme.

# Chapter 3 An Optimized Algorithm

## 3.1 System Model

In my research, a new scrambling technique combining 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 Fig 3.1.

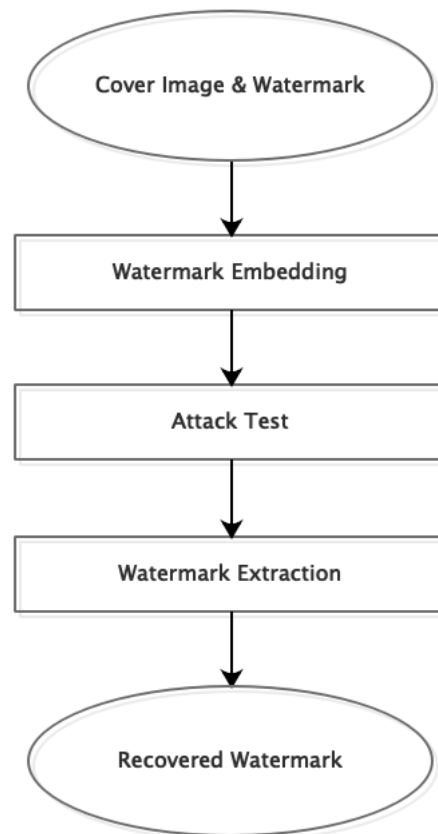


Fig 3.1 Optimized digital watermarking procedure

## 3.2 Mathematic Basis

### 3.2.1 Singular Value Decomposition

Singular Value Decomposition (SVD) is now widely applied in signal processing

fields. In programming platform, an image can be converted to a grayscale matrix. As a linear algebra tool, when SVD is applied to an image, the digital image matrix can be regarded as a matrix formed by many non-negative scalars. Therefore, various matrix processing techniques can be applied to image processing to realize rapid image large-scale data.

In SVD, the image matrix is factorized into three different parts: unitary matrix part ( $U$ ), diagonal matrix part ( $S$ ) and transpose of unitary matrix part ( $V$ ). Suppose we have an image  $I$ , convert it to matrix  $A$ ,  $A$  can be divided into 3 parts  $U, S, V$ :

$$A = U \cdot S \cdot V^T$$

Where  $A$  has size of  $m \times n$ ,  $U$  has size of  $m \times m$ , diagonal matrix  $S$  has size of  $m \times n$ , and  $V$  has size of  $n \times n$ . Columns of vector  $U$  and  $V$  are left singular vectors and right singular vectors respectively. Image brightness is decided by geometric characteristics: singular vectors. SVD has an important property that if any changes are made to the single qualities at that point, the framework stays unchanged. This property is extremely Important in the proposed algorithm for embedding transformed components to singular value matrix of the cover image after SVD transform.

### 3.2.2 DWT-SVD Scheme

A. C. Phadke et al.[18] concluded the procedure of DWT-SVD and DCT-SVD algorithm used in digital watermarking. DWT operates target in both spatial domain and frequency domain. Figure 3.2 and 3.3 are the flow chart of DWT-SVD watermarking embedding and extraction. As the result of reference [18] shows, applying DWT-SVD only, it has a good performance on hiding watermark information. However, the watermarked image is not robust enough against attacks, which is also the common disadvantages of spatial domain algorithm.

#### Scheme-I: DWT-SVD application in digital watermarking procedure

##### A. Watermark Embedding:



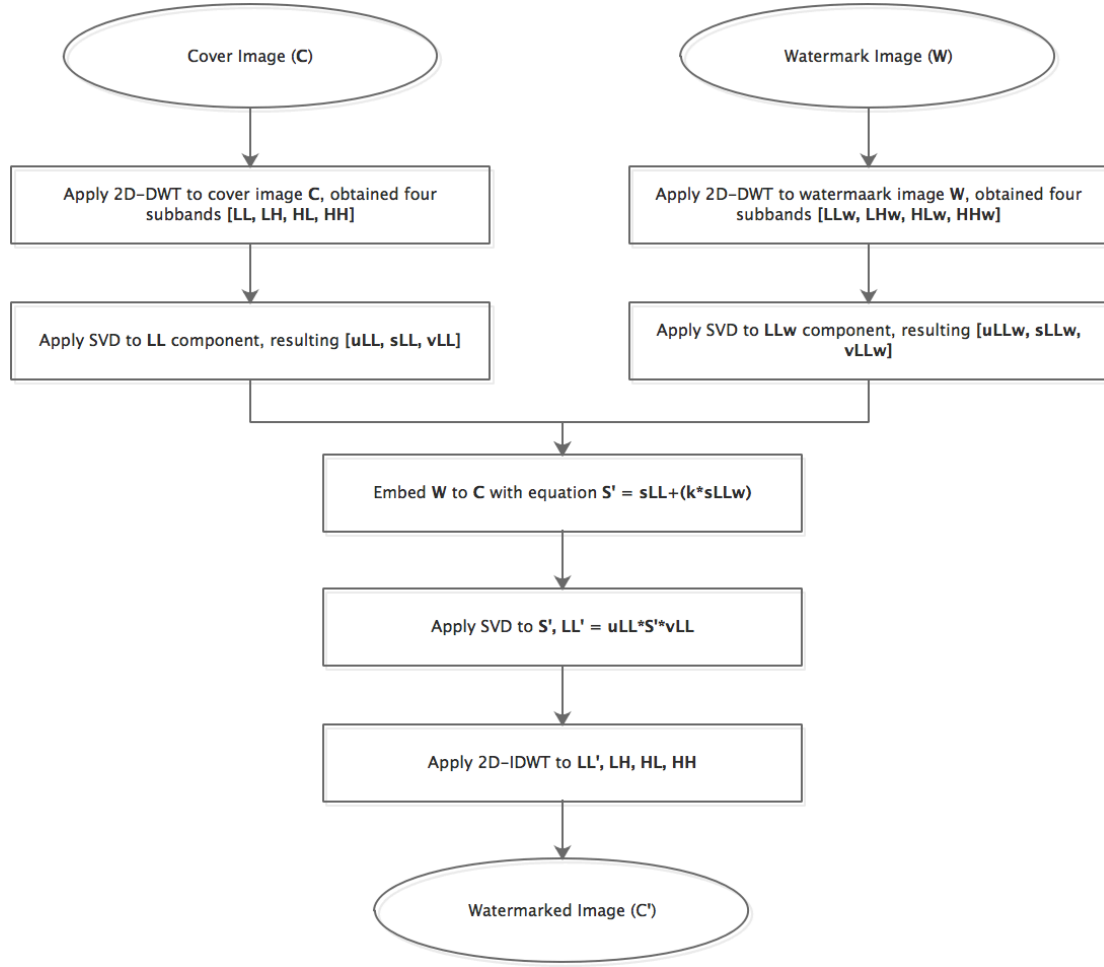


Figure 3.2 DWT-SVD watermark embedding procedure

## B. Watermark Extraction:

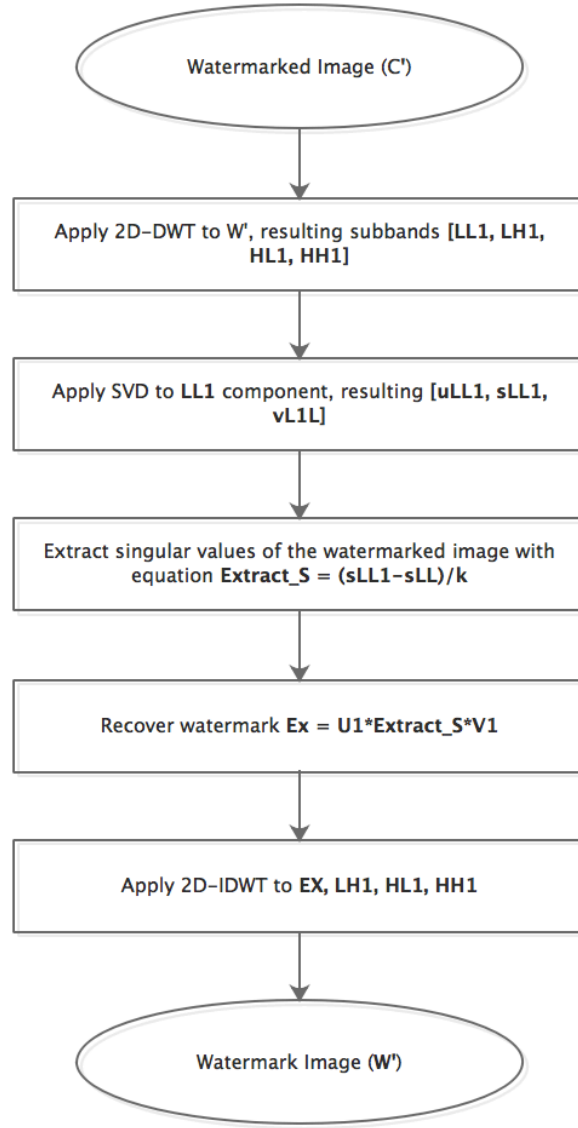


Figure 3.3 DWT-SVD watermark extraction procedure

### 3.2.3 DCT-SVD Scheme

A. C. Phadke et al.[18] also described the procedure of applying DCT-SVD method, the flow charts of DCT-SVD watermark embedding and extraction procedure are presented in Figure3.4 and Figure 3.5 From the result in reference [18], we can see that the robustness is satisfactory while the imperceptibility has poor performance.

#### Scheme-II: DCT-SVD application in digital watermarking procedure

##### c. Watermark Embedding:

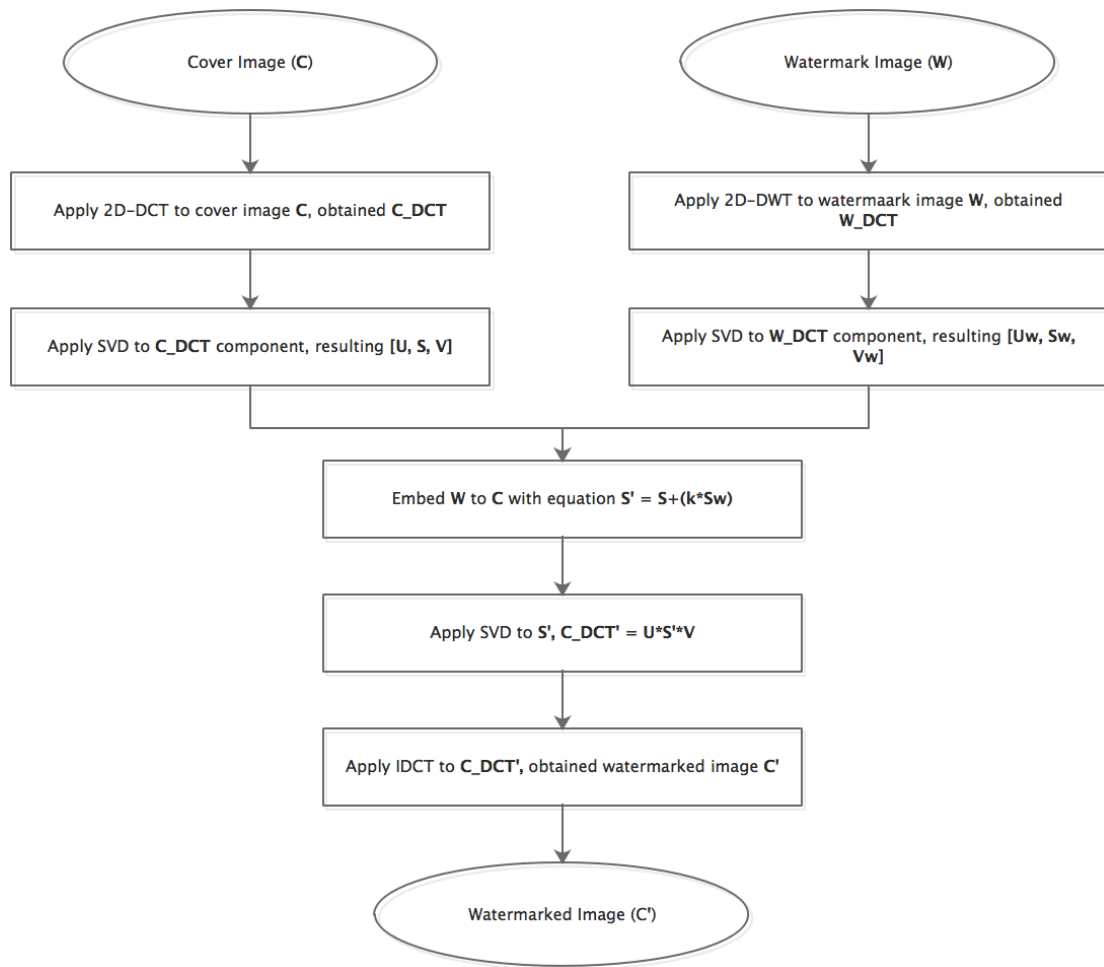


Figure 3.4 DCT-SVD watermark embedding procedure

**d) Watermark Extraction:**

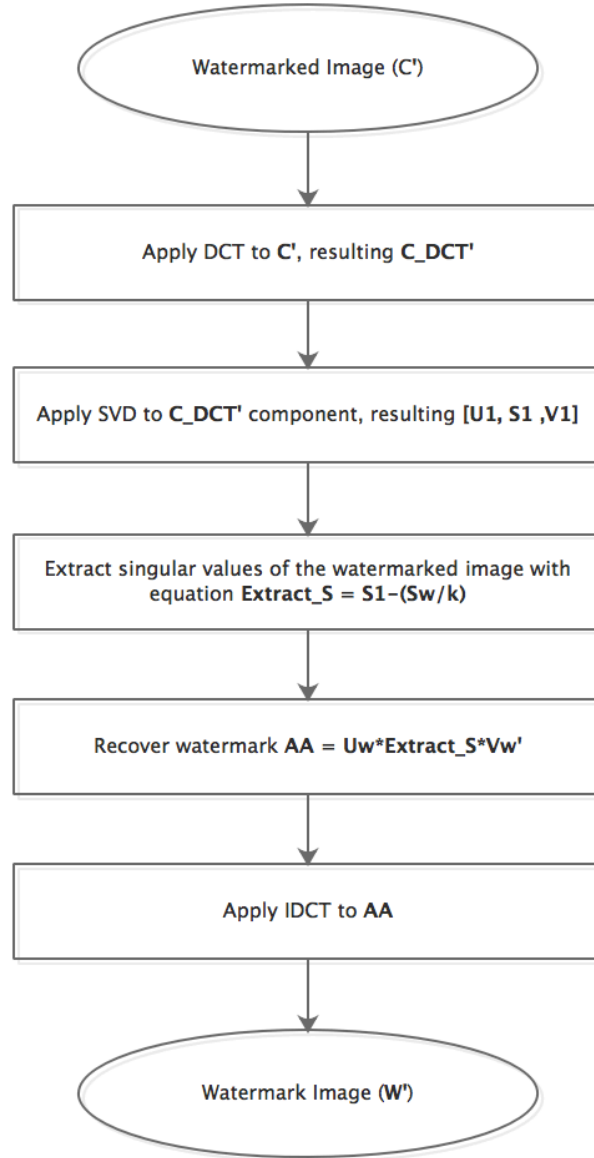


Figure 3.5 DCT-SVD watermark extraction procedure

### 3.2.4 Two-Dimensional Arnold Transform

According to the selected phase space, it can be divided into two-dimensional, three-dimensional, four-dimensional to n-dimensional Arnold transformation.

For digital images, a 2D-Arnold transform is used. A 2D-Arnold transformation can be expressed as:

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

Where (x, y) represents the coordinates of a point in the original matrix, and (x, 'y')

represents the coordinates of the point after the transformation. Arnold transformation can be seen as a procedure of cropping and splicing, by which the points in the discretized digital image matrix are rearranged. Since the discrete digital image is a finite point set, the result of this iterative successive transformation, although the change of the pixel position in the matrix at the beginning stage is quite confusing, the iteration proceeds to a certain number of steps, and it is inevitably restored to the original position. Therefore, Arnold transformation has periodicity. Since Arnold transform has different periods for different matrix orders  $n$ , in order to minimize the cost of the transform, we hope that the period of the Arnold transform is as short as possible.

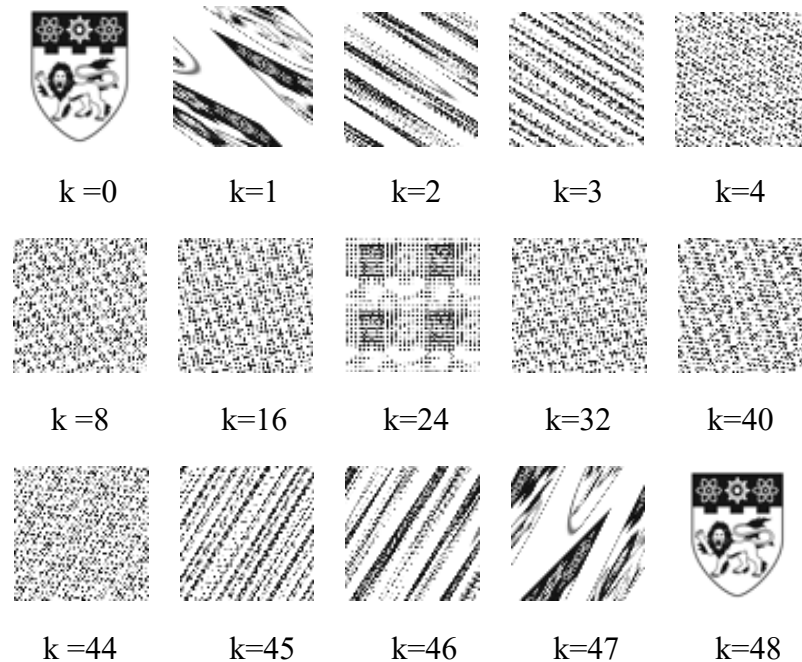


Figure 3.6 Arnold Transform

Figure 3.6 shows the effect of a 64\*64 grayscale image "NTU badge" after Arnold transform.

For a watermark image, when the carrier image is attacked, a certain part of the image is usually damaged or lost, so that the embedded watermark image will be damaged or lost as well. If the watermark image is preprocessed by the Arnold transform, it is scrambled before embedding, and the extracted scrambled image continues to use the Arnold transform to recover the watermark image. Because in the process of recovery, the Arnold transform will spread the previously damaged bits,

reducing its impact on human vision and improving the robustness of digital watermarking.

### 3.2.5 Magic Square Transform

If the matrix  $A = (a_{i,j})_{n \times n}$  is satisfied:

$$\sum_{i=1}^n a_{i,j} = \sum_{j=1}^n a_{i,j} = \sum_{i=1}^n a_{i,i} = \sum_{i=1}^n a_{i,n-i} = \frac{n(n^2 + 1)}{2}$$

Then matrix  $A$  is a standard magic square matrix.

The magic square transformation moves the element in  $A$  to the position of the next element and moves the last element to the position of the first element. After such replacement, matrix  $A$  is converted to matrix  $A'$ , and  $A' = EA$ . For the digital image matrix  $I$ , pay attention to the correspondence between  $I$  and  $A$  elements, and correspondingly shift the corresponding pixel values in  $I$  with  $A$  to  $A'$ , and generate a new digital image matrix  $I'$ , denoted as  $I' = EI$ . For example:

$$A = \begin{pmatrix} 16 & 2 & 3 & 12 \\ 5 & 11 & 10 & 8 \\ 9 & 7 & 6 & 12 \\ 4 & 14 & 15 & 1 \end{pmatrix} \rightarrow A' = \begin{pmatrix} 15 & 16 & 2 & 12 \\ 13 & 7 & 9 & 10 \\ 8 & 11 & 5 & 6 \\ 3 & 4 & 14 & 11 \end{pmatrix}$$

Under the scrambling effect of the fourth-order magic square matrix  $A$ , Matrix  $I'$  is obtained:

$$I = \begin{pmatrix} i_{11} & i_{12} & i_{13} & i_{14} \\ i_{21} & i_{22} & i_{23} & i_{24} \\ i_{31} & i_{32} & i_{33} & i_{34} \\ i_{41} & i_{42} & i_{43} & i_{44} \end{pmatrix} \rightarrow I' = \begin{pmatrix} i_{43} & i_{44} & i_{12} & i_{34} \\ i_{41} & i_{23} & i_{31} & i_{32} \\ i_{24} & i_{33} & i_{21} & i_{22} \\ i_{13} & i_{14} & i_{42} & i_{11} \end{pmatrix}$$

Magic square transform achieves the purpose of encryption by interfacing the pixels of the image and scrambling the position of the pixels in the image. Magic square transformation is essentially the elementary transformation of the matrix, with periodicity, the transformation period is  $n^2$ , and the period of the transformation is also regular. Matrix  $I'$  is transformed into matrix  $I$  after multiple replacements. The difficulty in using Magic Square for scrambling transform is to find the magic square that matches the image size. When  $n$  is relatively large, the transformation steps required for image restoration will also increase. Since the magic square matrix is a finite dimensional

matrix, the adjacent pixels in the original image are mostly spatially adjacent after scrambling, so the scrambling effect of this method is poor, in order to better scrambling effect, which requires multiple transforms, thus greatly increases the amount of calculation.

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

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

In previous work, Arnold transform is applied to preprocess watermark image. 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:

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

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  $h$ :

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

Where:  $h_i, h_i' \in \{1, \dots, F\}; i = 1, 2$ .

So  $h' = (h_1', h_2')_H$  is the corresponding pixel value after  $h$  scrambling.

Figure 3.7 shows the entire double-scrambling procedure.

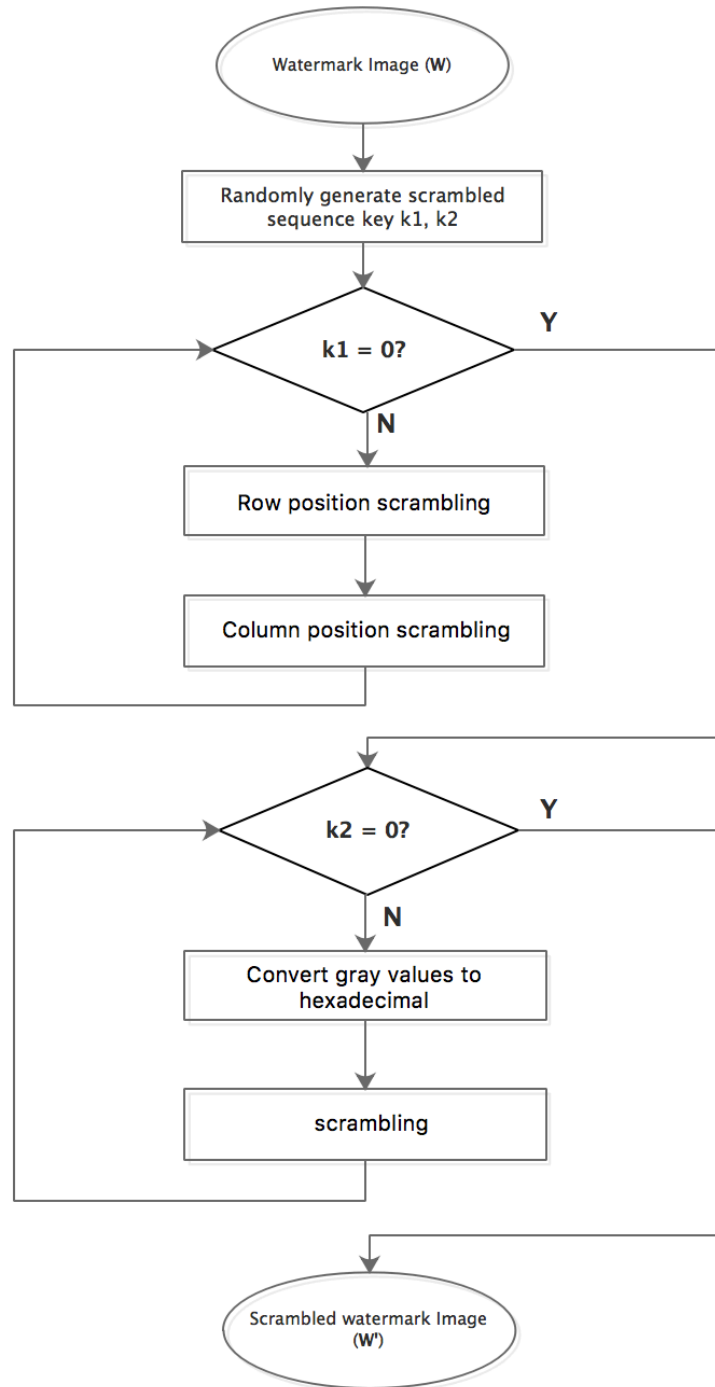


Fig 3.7 Double-scrambling procedure



### 3.3.2 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 of Figure 5.2. 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 fig. 3.8. 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.

$$x' = x + x_d$$

$$y' = y + y_d$$

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

Fig 3.8 Pseudo magic matrix

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

### **3.4 DWT-DCT-SVD Digital Watermarking Algorithm 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 [17]. 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 lossy 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.

### 3.4.1 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:

- Load cover image  $C$  and watermark image  $W$  as input.
- Convert  $C$  to YCbCr color space, obtained  $[Y, Cb, Cr]$
- 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.
- Split  $LL$  into small blocks, each of them has  $4*4$  size. Apply DCT to each block, resulting  $B$ .
- Apply Singular Value Decomposition (SVD) to  $B$ , resulting with  $[uLL, sLL, vLL]$ .

$$[uLL, sLL, vLL] = \text{svd}(B)$$

- Apply DCT to each block of  $W$ , resulting  $B_w$ .
- Apply SVD to  $B_w$ , resulting with  $[uLLw, sLLw, vLLw]$ .

$$[uLLw, sLLw, vLLw] = \text{svd}(B_w)$$

- Embed  $sLLw$  into cover image using equation:  $S' = S * (1+k*sLLw)$ . Where  $k$  is the scaling factor.
- Apply IDCT to  $S'$  to get  $LL'$ :

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

- Apply 2D-IDWT to  $LL'$  and other previous sub-bands to build watermarked image.
- Obtain watermarked image  $C'$ .

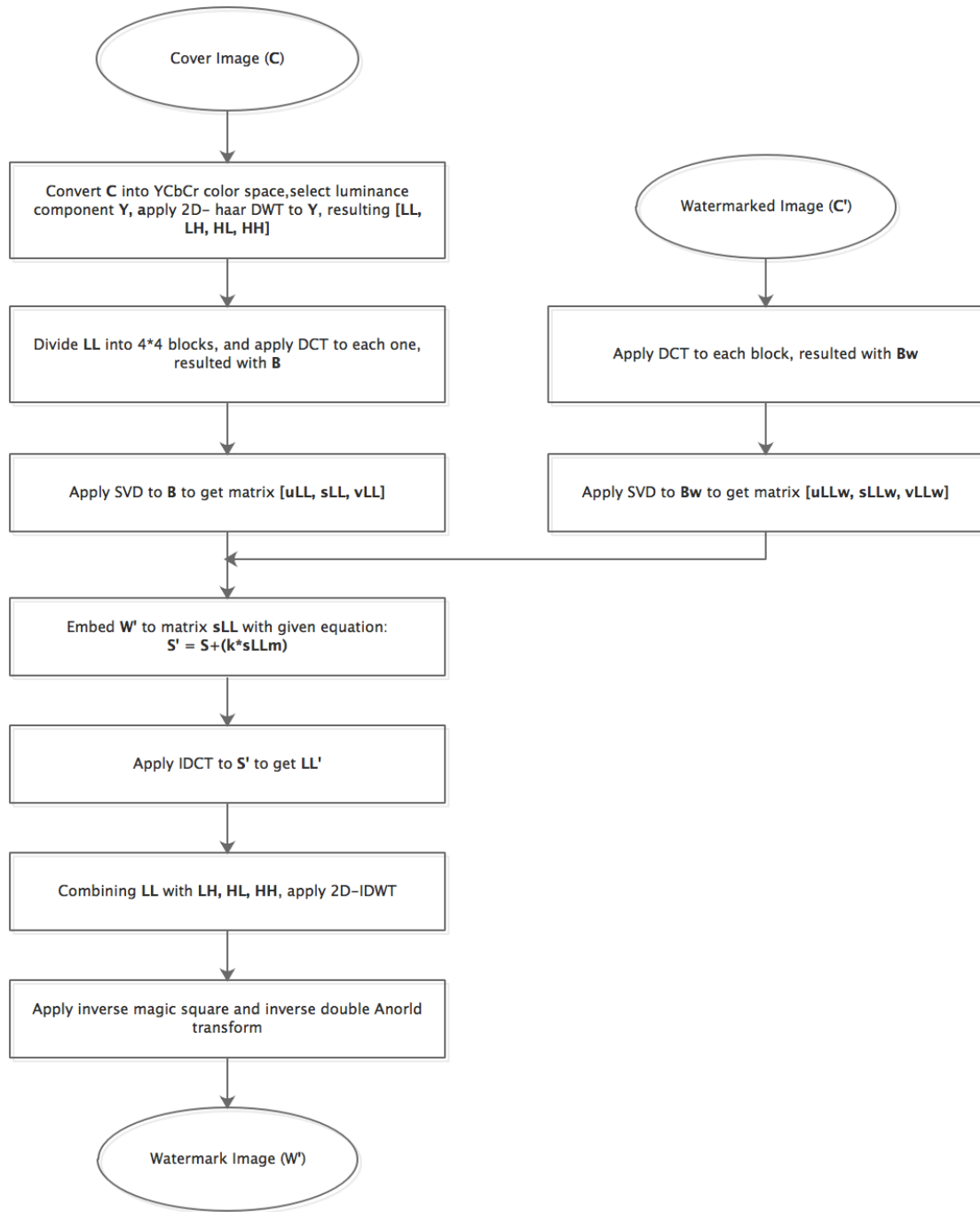


Figure 3.9 Watermark Embedding Procedure

### 3.4.2 Watermark Extraction

Watermark Embedding procedure:

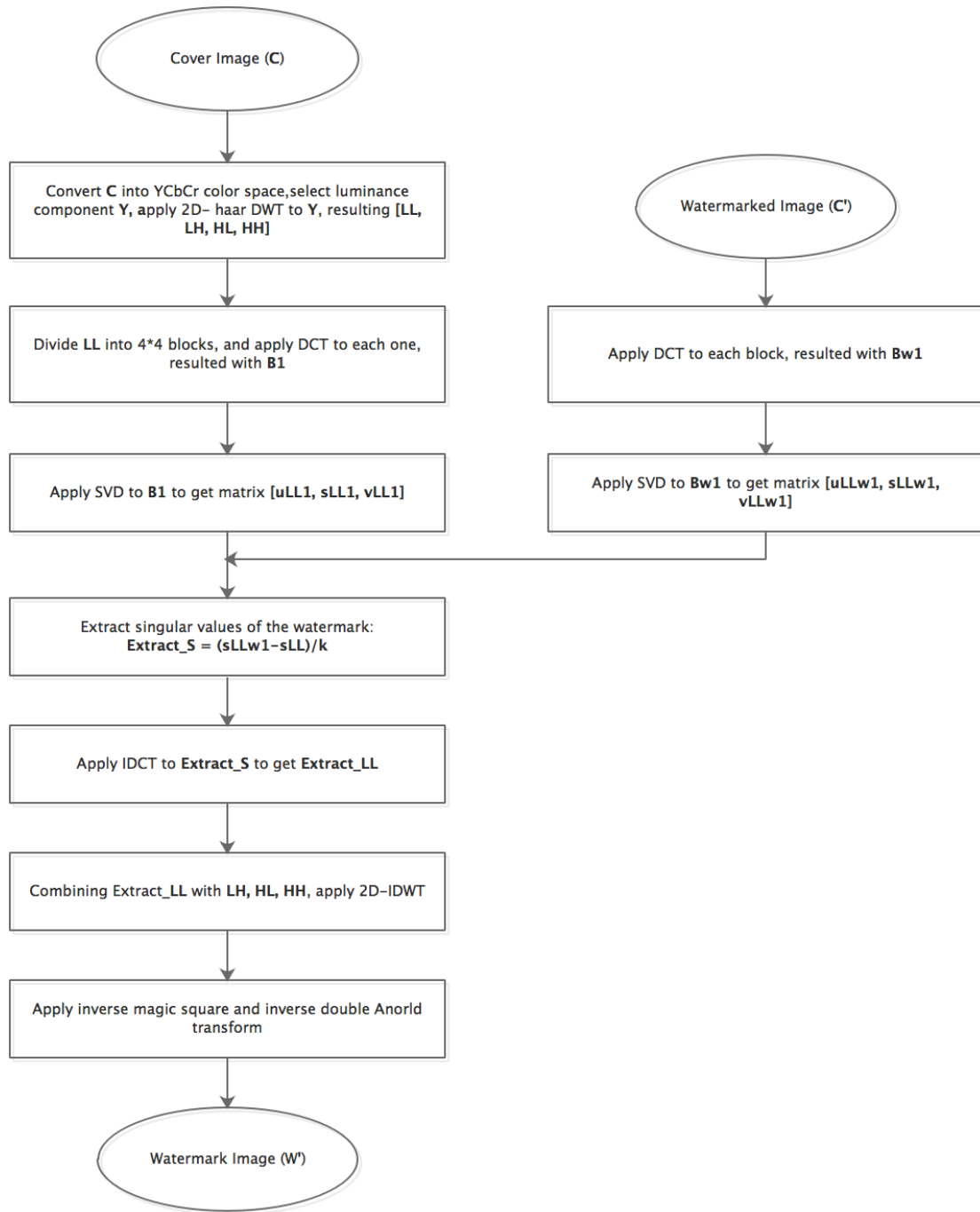


Figure 3.10 Watermark Extraction Procedure

- Load cover image  $C$  and watermarked image  $C'$  as input.
- Convert  $C$  to YCbCr color space, obtained  $[Y, Cb, Cr]$
- 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.
- Split  $LL$  into small blocks, each of them has  $4 \times 4$  size. Apply DCT to each block,

resulting  $BI$ .

- Apply SVD to  $BI$ , resulting with  $[u_{LL1}, s_{LL1}, v_{LL1}]$ :

$$[u_{LL1}, s_{LL1}, v_{LL1}] = \text{svd}(B1)$$

- Split  $BI$  into small blocks, each of them has  $4*4$  size. Apply DCT to each block, resulting  $BwI$ .

- Apply SVD to  $BwI$ , resulting with  $[u_{LLw1}, s_{LLw1}, v_{LLw1}]$ .

$$[u_{LLw1}, s_{LLw1}, v_{LLw1}] = \text{svd}(Bw1)$$

- Extract the singular values of the watermark with the following equation:

$$\text{Extrac\_S} = (s_{LLw} - s_{LL})/k$$

- Apply IDCT to  $\text{Extrac\_S}$  to get  $\text{Extract\_LL}$ :

$$\text{Extract\_LL} = u_{LL} * \text{Extrac\_S} * v_{LL}$$

- Apply 2D-IDWT to  $\text{Extract\_LL}$  and other previous sub-bands to build watermarked image.
- Obtain watermark image  $W'$ .

# Chapter 4 Experimental Results

## 4.1 Experimental Results of Proposed Scrambling Method

Select different  $k$  combinations, apply the proposed scrambling method in 3.3 to the Lena image. Here we select Lena image because its color information is much richer than the watermark image, it is more vivid. From Figure 4.1, we can see that simple position scrambling, after a small number of iterations, still can be observed obvious texture, can't really hide the image information.

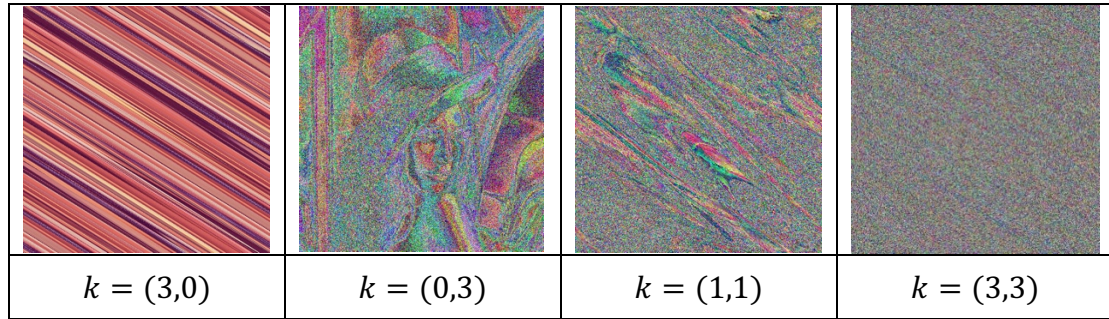


Figure 4.1 Arnold transform double-scrambling effect

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 4.2 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.

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 4.3 shows the results using wrong keys to recover the original image.



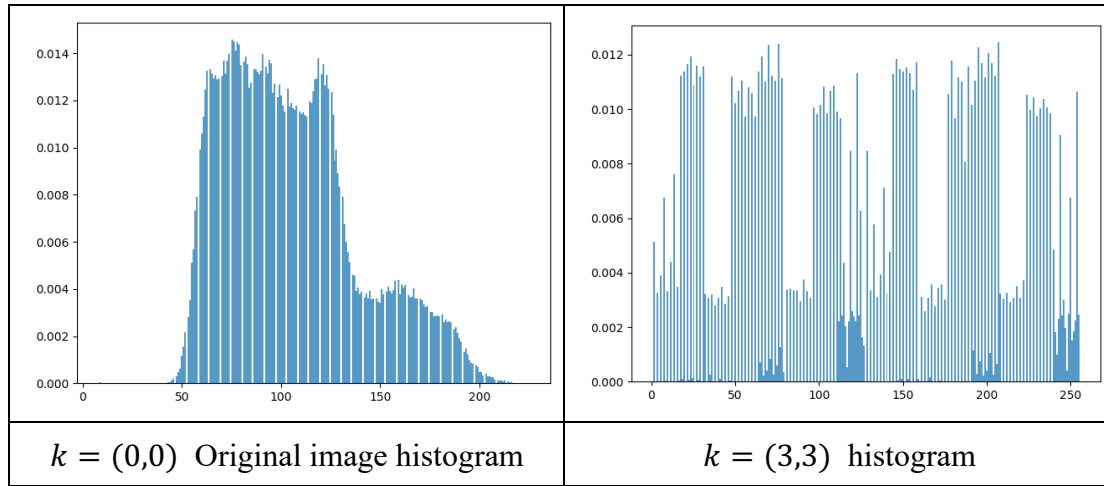


Figure 4.2 Image gray histogram comparison before and after double scrambling

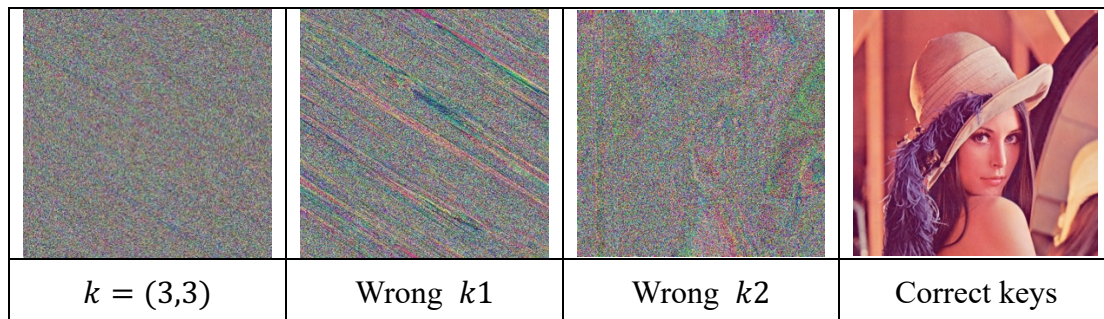


Figure 4.3 Image recover effect with wrong keys

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

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

Let  $N = 4, A = 2, B = 3$ . Figure 6.4 shows the comparison of the original image and image after transform.

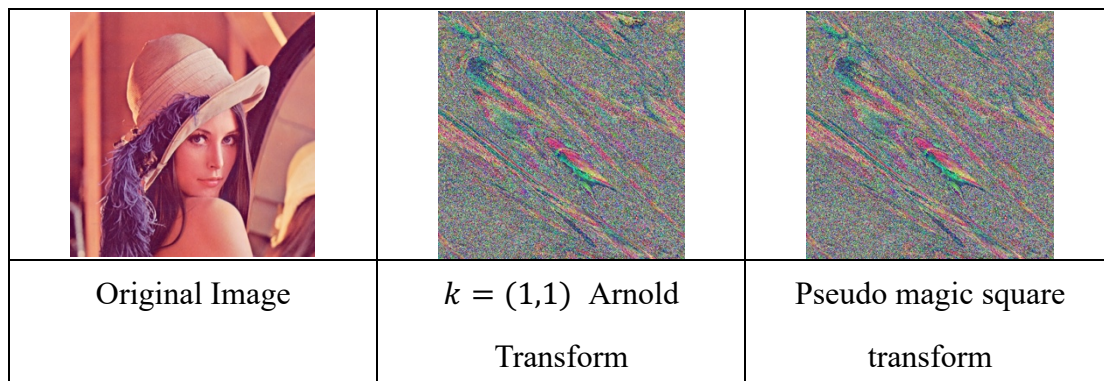


Figure 4.4 Comparison of the original image and image after transform.

## 4.2 Experimental 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 Fig 4.5 (a). The watermark image has size of  $256 \times 256$ , as shown in Fig 4.5 (b). It is inserted to the cover image with three different algorithms, the watermarked images appear in Fig 4.5 (c)-(e), using DWT-SVD, DCT-SVD and DWT-DCT-SVD method respectively.

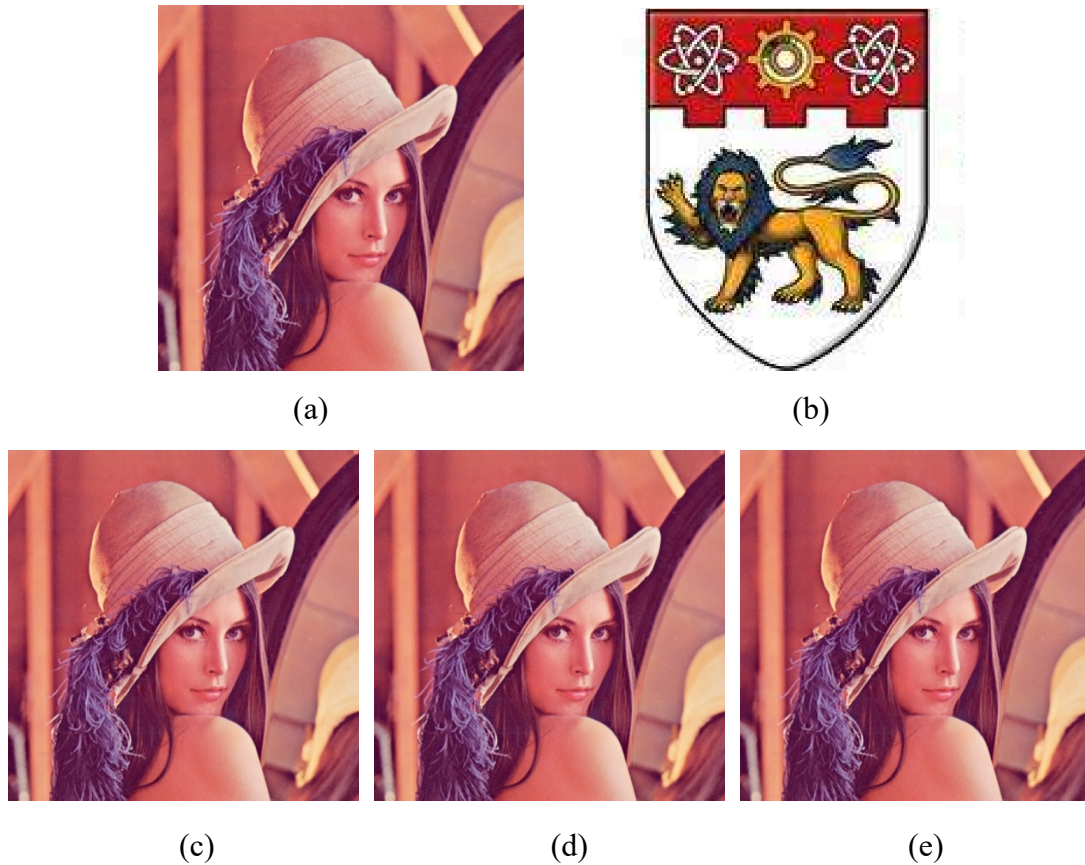


Fig 4.5 (a)-(e). (a) Cover image, (b) Watermark image, (c) Watermarked image using DWT-SVD, (d) Watermarked image using DCT-SVD, (e) Watermarked image using DWT-DCT-SVD method

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 shows the experimental results of applying different  $k$ .

$k$ 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 II. PSNR and NC using different  $k$  values

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 III shows the comparison.



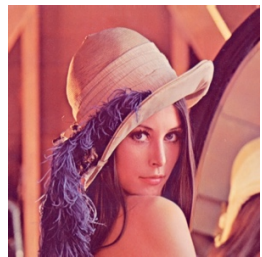

Technique	Watermarked Image	Extracted watermark	PSNR	NC
DWT-DCT-SVD			56.1048	0.9309
Proposed Method			43.2552	0.9789

Table III DWT-DCT-SVD vs. proposed method

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.













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 IV. Effect of embedding different watermark to same image

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.






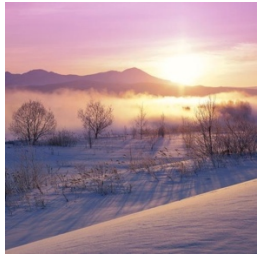











Watermarked Image	Embedded Watermark	Extracted watermark	PSNR	NC
			43.2552	0.9789
			43.2251	0.9624
			42.9842	0.9713
			41.5362	0.9532

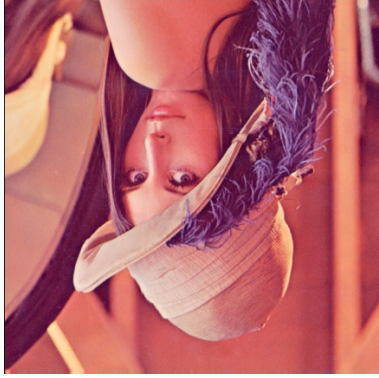
Table V. Effect of embedding same watermark to different image

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.

### 4.3 Experimental 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.

	Attacked watermark image	NC	NC in [13]
Chop 5% $486 \times 512$		0.9692	0.9532
Chop 30% $358 \times 512$		0.9142	0.9006
90° Rotation		0.9021	0.8534

180° Rotation		0.8845	0.8243
10% Brighter		0.9842	0.9697
Insert random lines		0.9703	0.9523
Randomly Cover		0.9531	0.9328




Add salt and pepper noise		0.9625	0.9475
Gaussian Low-pass Filter		0.9734	0.9024
Median Filter		0.9842	0.9582
Average Filter		0.9852	0.9511



Image blur		0.9696	0.9702
Grayscale process		0.9732	0.9877

Table VI. Robustness test results

#### 4.4 Analysis and summary

Table VI 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 [18] and the DCT-SVD algorithm in the reference [18], objectively illustrate the proposed improved algorithm has better robustness and visual effects. It can be seen from the data in Table V that except Grayscale process, the robustness of other attacking algorithms has been improved to varying degrees.

In this paper, an image digital watermarking algorithm based on DWT-DCT-SVD and improved scrambling technology is proposed. Experimental results show that the algorithm is effective and has good applicability. Combining the data of Table V with the results of the previous tests, facing conventional image attacks such as Gaussian noise, salt and pepper noise, low-pass filtering, rotation and other geometric attacks, both subjectively and objectively, the attacks are very resistant and have better robustness than the SVD algorithm in the literature [18] and the DCT-SVD algorithm

in the literature [18].

In general, although the proposed scrambling method introduces computational complexity, it increases the watermark capacity. Double-scrambling reduces the computational complexity while grayscale scrambling enhances the ability against attacks using statistical characteristics.

# Chapter 5 Conclusion

The proposed scrambling technique combining double scrambling and pseudo magic square transform has advantages against attacks using statistical characteristics. Compared with traditional digital watermarking algorithm based on DWT-DCT-SVD, results in chapter 4 shows strong robustness in geometric attacks and much better robustness performance in statistical attacks.

This paper first discusses the basic concepts and theories of digital watermarking, analyzes the research background of digital watermarking, the application status and development prospects based on digital watermarking, and has achieved a comprehensive understanding of digital watermarking. The application model and classification of existing digital watermarks are analyzed, and the basic theory of digital watermarking and embedding technology are reviewed. Then several common transform domain image digital watermarking techniques are introduced in detail. Based on in-depth research, 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. By observing the similarity between the extracted watermark and the original watermark Degree, calculate the correlation coefficient of the two, and judge the presence or absence of the watermark. 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.

This paper has done some work in the digital watermarking algorithm, but there are still many deficiencies that need to be improved, and the level and depth of research need to be further improved.

The proposed methods now are pretty mature, the research can be explored in some other areas:

- 1) Expand from grayscale images to color images. And combined with mobile phones, digital cameras and other applications, on the one hand to protect the copyright ownership of digital works, on the other hand to ensure the non-repudiation of the origin of digital works.
- 2) Extend watermark information from image to barcode, and combined with encryption algorithm to make watermark information further protected in terms of uniqueness and security.
- 3) The productization and commercialization of digital watermarking technology. Currently, e-commerce industry is developing very rapidly. How to apply digital watermarking technology to e-commerce and solve the problems of copyright protection, anti-counterfeiting and non-repudiation in the middle of e-commerce will be of great significance and value.

# 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] Asna Furqan, Munish Kumar “Study and Analysis of Robust DWT-SVD Domain Based Digital Image Watermarking Technique Using MATLAB”, 2015 IEEE International Conference on Computational Intelligence & Communication Technology
- [4] Shankar Parimi, A. Sai Krishna, 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]
- [5] S. Abolfazl Hosseini, Arash Saboori “A New Method for Color Image Watermarking Based on Combination of DCT and PCA”
- [6] 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
- [7] Olcay Duman and Olcay Akay “A New Method of wavelet Domain WaterMark Embedding and Extraction using Fractional Fourier Transform” (page no 187-191)
- [8] Shiji Johny, Anil Antony “Secure Image Transmission Using Visual Cryptography Scheme without Changing the Color of the Image”, ICETECH’15 © 2015 IEEE
- [9] Mishra A, Agarwal C, Sharma A, et al. “Optimized gray-scale image watermarking using DWT-SVD and Firefly Algorithm[J].” Expert Systems with Applications, 2014, 41(17):7858-7867.
- [10] Ali M, Chang W A. “An optimized watermarking technique based on self-adaptive DE in DWT-SVD transform domain[J].” Signal Processing, 2014, 94(1):545-556.

- [11] Ali M, Chang W A, Pant M. "A robust image watermarking technique using SVD and differential evolution in DCT domain[J]." *Optik - International Journal for Light and Electron Optics*, 2014, 125(1):428- 434.
- [12] Maheshwari J P, Kumar M, Mathur G, et al. "Robust Digital Image Watermarking using DCT based pyramid transform via image compression[C]// International Conference on Communications and Signal Processing." IEEE, 2015:1059-1063.
- [13] Yuqi He, Yan Hu, "A proposed Digital Image Watermarking Based on DWT-DCT-SVD[C]", 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[C]" First International Conference on Next Generation Computing Technologies
- [15] S. K. Prajapati, A. Naik and A. Yadav, "Robust Digital Watermarking using DWT-DCT-SVD[J]", *International Journal of Engineering Research and Applications* vol. 2, no. 3, pp.991-997, May-Jun 2012.
- [16] Chunping Fu, "Research on a Digital Watermarking Algorithm Based on Sum[D]", Suzhou University, 2008
- [17] 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
- [18] Prachi Pradeep Nerurkar , Dr. A. C. Phadke , "Digital Image Watermarking Using Firefly Algorithm[J]", 978-1-5386-5257-2/18/\$31.00 ©2018 IEEE