Comparative Evaluations of Image Encryption Algorithms

Zhe Liu

A thesis submitted to the Auckland University of Technology
in partial fulfillment of the requirements for the degree of
Master of Computer and Information Sciences (MCIS)

2018

School of Engineering, Computer and Mathematical Sciences

Abstract

Information security has become a significant issue for protecting the secret information during transmission in practical applications in the era of information. A raft of information security schemes have been used in image encryption. These schemes can be divided into two domains; the first one encrypts the images based on spatial domain, the typical method of spatial image encryption technology is in use of chaotic system, most of the earlier encryption methods are belong to this domain; the other encrypts images on frequency domain, most of the optical image encryption methods are processed in this domain.

In this thesis, a slew of approaches for image encryption have been proposed. The contributions of this thesis are listed as follows. (1) We design the improved encryption method based on traditional Double Random Phase Encoding (DRPE) method and use Discrete Cosine Transform (DCT) to replace Discrete Fourier Transform (DFT) so as to avoid operations on complex numbers; we use a logistic map to generate random matrices instead of random phase masks in the traditional DRPE so as to decrease the size of secret keys. (2) We design the encryption method based on traditional watermarking scheme by using Discrete Wavelet Transform (DWT), DCT and Singular Value Decomposition (SVD) together, the proposed DWT-DCT-SVD method has higher robustness than traditional chaotic scrambling method and DRPE method. (3) We improve the DWT-DCT-SVD method by using denoising techniques and design the denoising method based on Convolutional Neural Networks (CNN); the improved method has higher robustness against noise attacks.

Keywords: image encryption; double random phase encoding; chaotic scrambling; logistic map; image denoising; linear CNN model

Table of Contents

List of Figures

List of Tables

Attestation of Authorship

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person (except where explicitly defined in the acknowledgments), nor material which to a substantial extent has been submitted for the award of any other degree or diploma of a university or other institution of higher learning.

Signature: 刘哲 Date: 25 March 2018

Acknowledgment

This research work was completed as the part of the Master of Computer and Information Sciences (MCIS) courses at the School of Engieering, Computer and Mathematical Sciences (SECMS) in the Faculty of Design and Creative Technologies (DCT) at the Auckland University of Technology (AUT) in New Zealand. I would like to deeply thank my parents for their financial support during my entire time of academic study in Auckland.

My deepest thanks are to my primary supervisor Dr. Wei Qi Yan who has provided me with much appreciated technological guidance and support. I believe that I could not have been able to achieve my Master Degree without his invaluable help and supervision. In addition, I would like appreciate my secondary supervisor Dr. Bobby Yang and school administrators in our school for their support and guidance through the MCIS in the past years.

Zhe Liu

Auckland, New Zealand

March 2018

Chapter 1
Introduction

The first chapter of this thesis consists of five sections. In this chapter, background and motivation of this thesis are introduced, objectives will be discussed in the fourth section. This chapter also covers the details of the research questions after the in-depth comprehensive understanding of the relevant literatures and research background. Finally, we will present an overview of the structure of this thesis in Section 5.

1.1 Background and Motivation

Image encryption techniques can be divided into two groups based on operations on spatial domain or frequency domain. The first group operates in the spatial domain, the encrypted objects are pixel location and intensity, while the other in the frequency domain, the encrypted objects are the frequency coefficients. Earlier encryption methods work in spatial domain. The image encryption methods in the spatial domain require a large amount of computations.

The second group encrypts images in frequency domain. Most recent encryption methods are in this group. By operating in frequency domain, the amount of computation can be reduced and more efficient processes can be used, for example, digitally-filtered processing in the frequency domain using Fourier transform.

Optical cryptographic techniques allow processing images in frequency domain which have been widely used in image security because this kind of techniques can deal with data rapidly using image processing algorithms. In particular, optical image encryption has attracted public attention since the DRPE method has been proposed (Refregier & Javidi, 1995). There are four main problems with traditional DFT-based DRPE. First of all, the secret keys refer to two random phases *M* and *N*, there are only two phase plates as secret keys. The second problem is that the two random phases *M* and *N* are two matrices which have the size as same as its resolution of the original image; therefore, they are too large and the 4F system requires complex conjugate phase plate during the decrypted process; thus, too much storage space is required during the transmission. The third problem is that the encrypted image of DRPE based on Discrete Fourier Transform (DFT) is a complex matrix which requires a large storage. Because of these three problems, the computing costs of DRPE are very high. The fourth problem is the limitation of DRPE itself, the optical encryption method based on DRPE suffers from poor performance if the transmitted image is corrupted with different types of attacks (Mohamed, Samrah & Allah, 2017). In this regard, we also desgined an encryption method based on DRPE by using DCT technique, we tested the proposed algorithm using five types of attacks, the results indicate that this method cannot resist common attacks, so it can easily verify whether an image has suffered attacks or not.

Generally, in the image encryption approachs based on the transform domain, some transform methods such as discrete cosine transform (DCT) and discrete wavelet transform (DWT) are widely used. DCT avoids complex computations compared with traditional DFT (Ahmed, Natarajan & Rao, 1974), DWT can obtain good localization properties of input image in both the spatial and frequency domain (Burrus, Gopinath & Guo, 1998). We know the limitation of DRPE, we are aware that digital watermarking in the frequency domain has high robustness, it can leverage the advantages of transform methods as well. The basic workflow of the digital watermarking is similar to the image encryption and decryption processes in that it hides the original (secret) image into the host image. Therefore, it is meaningful to propose the robust image encryption schemes by using the design idea of digital watermarking techniques. We also notice that image denoising strategies can filter out image noises in image pre-processing; if this kind of techniques can be used in designing image encryption methods, the anti-attack ability of this method against noise attacks will be improved; moreover, the robustness of this method will be greatly improved.

In this thesis, we design DWT-DCT-SVD -based image encryption method based on the idea of digital watermarking techniques; the results show that the designed method has higher robustness than the DRPE based method, it can resist most of attacks preferably; however, for noise attacks, the performance of the designed method is not satisfactory. Thus, we consider further improving the anti-attack ability against noise attacks by using image denoising.

1.2 Research Question

This thesis aims at improving the traditional image encryption method based on DRPE and finally proposing a robust image encryption scheme based on frequency domain. Therefore, the research questions of this thesis are:

Question:

How to overcome the problems of traditional image encryption scheme based on DRPE method ?

What image encryption schemes can be designed which have higher robustness than the traditional encryption scheme based on DRPE method?

We attempt to find answers for the following question which was developed from the main question:

"What algorithms are available for image encryption? which of these algorithm is the best for our research goal which has the highest robustness? How to further improve the robustness of this algorithm?"

The core idea of this thesis is image encryption. Thus, the techniques that we adopted in this research project need to be evaluated and some proper techniques need to be chosen so as to implement the best result of image encryption.

1.3 Contribution

The focus of this thesis is mainly on improving of traditional DRPE-based image encryption method and designing the robust image encryption scheme based on frequency domain. After experiments, our objective is achieved, our contribution can be listed as follows: (1) Design the chaotic scramling encryption method based on logistic map, use logistic map to generated a chaotic sequence. Then, we use this sequence to scramble the image. (2) Design the improved encryption method based on DRPE and use Discrete Cosine Transform (DCT) to replace Discrete Fourier Transform (DFT) so as to avoid operations on complex numbers, we use a logistic map to generate random matrices instead of random phase masks in the traditional DRPE so as to decrease the number of secret key. (3) Design the encryption method based on traditional watermarking scheme. The proposed DWT-DCT-SVD method has higher robustness than traditional chaotic scrambling method and DRPE method. (4) Improve the DWT-DCT-SVD method by using denoising techniques and design the denoising method based on linear CNN network. The improved method has higher robustness against noise attacks.

1.4 Objective of This Thesis

Based on the background of our research, there are two main objectives of this thesis as follows: (1) There are several problems with encryption scheme based on traditional DRPE method, we make efforts on overcoming the problems, designing and implementing the improved encryption scheme based on DRPE method and 4f system; (2) We are aware that digital watermarking in frequency domain has high robustness. The basic workflow of the digital watermarking is similar to the image encryption and decryption processes, so we will try to design the robust image encryption method by using the design idea of digital watermarking. (3) We consider further improving the anti-attack abilty of designed new method against noise attacks, we will try to combine the image denoising techniques with the designed image encryption methods together, so the combined encryption method will have higher robustness.

1.5 Structure of This Thesis

The thesis is structured as follows:

In Chapter 2, literature review will be detailed, such as the previous studies in image encryption from both spatial and frequency domain. Digital watermarking techniques show the relevance to image encryption in frequency domain and the image denoising strategies can further improve the robustness of image encryption methods. Thus, Chapter 2 will introduce widely used methods in both image encryption and digital watermarking area, some image denosing methods which can be applied to image encryption will also be detailed.

In Chapter 3, the explanation of research methodology of this thesis will be addressed. In addition, the potential solutions and answers will also be presented. Moreover, the experimental layout and design as well as datasets and implementations with the evaluation methods will be presented.

In Chapter 4, an introduction of various image encryption methods and related work (image denoising) to further improve the robustness of the methods will be detailed, the methodologies and algorithms we presented will be implemented. Moreover, experimental results and outcomes will be detailed with the support of tables and figures. The limitations of this project will also be addressed as well.

In Chapter 5, a resultant comparison of the proposed image encryption methods is presented, the analysis and discussions are depicted based on experimental results and outcomes we acquired in Chapter 4. Finally, the conclusion and future work will be presented in Chapter 6.

Chapter 2
Literature Review

With in-depth analysis of the research question and rationale reviews of the existing studies, some widely used image encryption methods will be detailed, how the robust watermarking techniques give us new idea which can be applied to design the image encryption method will be summarized, multiple denoising methods will be delineated in this chapter as well.

2.1 Introduction

Image encryption means using scrambling operations to process the image, the original clear image becomes a random-generalized white-noisy image, so as to achieve the purpose of information encryption. Image encryption is an important research direction in the field of information security. The image encryption can be split into spatial and frequency domains. The research of image encryption methods mainly focused on the following five aspects: (1) image encryption on spatial domain, (2) image encryption on frequency domain, (3) image encryption based on chaotic system, (4) image encryption based on neural networks, (5) image encryption based on cellular automata.

In this thesis, we will focus on the first three aspects. In Section 2.1, image encryption on spatial domain processes the pixels of the image directly on the domain, most earlier encryption methods belong to this domain. There are two categories that can be used to achieve the purpose of image encryption. The first one changes the location of image pixels, the other modifies the value of image pixels. These two methods are usually taken and combined with chaotic system, a chaotic system is widely used because it has excellent randomness. Image encryption methods based on spatial domain usually require a large amount of calculations.

Image encryption on frequency domain allows mutual transformation of the images between spatial domain and frequency domain by using specified transform methods. Some broadly-used transforms are DFT, DCT, and DWT. This kind of methods encrypt and decrypt images by scrambling the location of a pixel or the value of the freqeuncy coefficients. Compared with encryption methods on spatial domain, the amount of computations can be reduced and more efficient processes can be used for the image encryption methods on frequency domain.

There are a plethora of image encryption methods proposed on frequency domain by using DRPE. Traditional DRPE-based methods have several problems and limitations, the robustness of this kind of methods is not satisfied. For the same purpose of image hiding, we notice that digital watermarking technique is similar to image encryption which leverages the transform methods on frequency domain and has high roustness. We are also aware that image denoising strategies can filter out noises in image pre-prosessing. If this kind of techniques can be used in image encryption methods, the methods will more effectively resist noise attacks, the robustness can be further improved.

2.2 Image Encryption

Image encryption uses secret key and encryption function, which makes an image into a scrambled image so that the real image information can not be perceived intuitively (Jiasheng & Liu, 2007). The changes between the original image and encrypted image can be presented in the following aspects: (1) Changes of relation between the position of pixels of the image, which is implemented by using image scrambling, that is a very important encryption technique on image encryption. (2) The pixel value of the image has been changed, viewed from the point of information theory, the information entropy of the encrypted image is increased in general. Viewing from the point of statistical theory, the histogram of encrypted image is more smooth than the original image, so it is difficult to obtain the visual information of original image from the histogram. (3) The correlation between adjacent pixels in the image is reduced.

Image encryption belongs to the area of cryptography. The traditional text encryption methods are used widely such us DES, AES and IDEA (Intemational Data Encryption Algorithm), but these methods can't be used in image encryption directly. Image encryption has some particularities, which are mainly embodied in three aspects. (1) Image encryption requires fast computing because an image usually is large. If the image encryption methods will take a long time to encrypt an image, even if these algorithms are highly secure, they may not have practical value. (2) Image encryption requires high fidelity of the decrypted image because they are more sensitive to the fidelity of the image information (Jiasheng & Liu, 2007). If the security of an encryption algorithm is high, but its fidelity is inferior, it also has no pratical value. (3) Image encryption should encrypt the entire image, because the correlation between image data is strong and the redundancy is high, it is not advisable to use the traditional methods to scramble the small area of image data.

Considering these reasons, we usually use symmetric cryptosystem to tackle image encryption. Since the first "information hiding workshop" was held in 1996, the security issues of digital image have attracted the attention of experts from the worldwide. In recent years, image encryption has attracted the interest of experts and researchers as the core problem of image security. Nowdays, the research work on image encryption mainly focused on five aspects which have been mentioned in the introduction of literature review.

2.3 Image Encryption Based on Spatial Domain

Let's consider $f(x, y)$ is the description of an image in spatial domain, which includes the location information (x, y) and the pixel value $f(\cdot)$ of this location. The purpose of encrypting the image can be achieved by changing any one or two of these information. Since this kind of image encryption is encrypted directly on spatial domain, this kind of encryption is called image encryption on spatial domain. Image encryption on spatial domain can achieve the purpose of encryption through two categories: one of them changes the mutual location relationship between image pixels, the methods which belong to this category is called image encryption based on scrambling; another one changes the pixel values by using some encryption rules so that the histogram of encrypted image is smoothed and the information entropy increases to nearly its maxima. The methods, which belong to this category, are called image encryption based on information theory.

2.3.1 Image Encryption using Scrambling

From the functional point of view, image scrambling is equivalent to the substitution method in classical cryptography. In modern cryptosystem, image scrambling is often used in preprocessing and postprocessing of image encryption. In other words, it still plays an important role in cryptography. Recently, experts and researchers have carried out detailed and in-depth research work that has achieved fruitful research results.

Arnold transform, also called cat map, which is proposed by Arnold when he was studying ergodic theory. The Arnold transform has been proposed to the high dimensional transformation (Ding, Yan & Qi, 2001). Then, the research was conducted based on discretization of the Arnold transform, 2D and 3D Arnold transform is suitable for image encryption (Chert & Mao, 2004). Based on this method, the encrypted image is chaotic after several times of Arnold transform which means that the satisfactory result of scrambling can be obtained; it has been widely applied to image encryption, information hiding and digital watermarking. A Russian mathematician proposed Kolmogorov transform (Scharinger, 2000). Wen put forward the image encryption method based on chaotic sequence, scrambled the image by using Kolmogorov transform and obtained the satisfactory scrambled results (Wen & Li, 2005). In 1970, the British mathematician John Conway and others proposed the concept “Game of Life”, this concept refers to a special image marix transformation (Berlekamp & Conway, 1982). Based on this concept, an image scrambling method was designed. Lan first proposed Knight-tour transform (Ding & Yan, 2000), Professor Bai used the Knight-tour transform to design the corresponding image scrambling method which can be used in information hiding (Ian & Parberry, 1997). In addition, researchers proposed other image scrambling methods such as the MagicCube transform, affine transformation which is based on stretching and folding (Zhu & Cao, 2003), Baker’s transformation and MagicCube transform.

Image encryption based on scrambling is mainly applied to preprocessing and post-processing of digital image, which ensures information security. These algorithms can be used as encryption methods for digital images in specific domains. Encryption by using simple image scrambling is vulnerable to statistical attak, which cannot protect image data well.

2.3.2 Image Encryption Based on Information Theory

In 1948, the founder of information theory established the concept of information entropy based on entropy in thermodynamics (Shannon, 1948). The entropy of thermodynamics describes the disorder state of the physical system, and the entropy of thermodynamics is the measurement of degree of disorder. Similarly, we also consider information entropy as a measurement of the degree of disorder of the signals, which is used to characterize the uncertainty of information. When the reciever receives information, the uncertainty is eliminated, the source entropy is reduced so that information is obtained. The purpose of image encryption is to make the encrypted image in a disorganized state. Therefore, image encryption is essentially to increase the security of the original image.

Pixel substitution and pixel diffusion are two effective ways to modify pixel values in image encryption, which can decrease correlation between pixels and increase the information entropy. In pixel substitution process, the value of each pixel will be modified independently, which is not related to others. Considering that image encryption requires fast speed, image substitution usually uses “Exclusive OR” operation (Tomassini & Perrenoud, 2001). In image diffusion process, the pixel value will be modified along with the values of its adjacent pixels by following the certain rules, and there is a correlation between adjacent pixels during this process. At present, there are two main types of image diffusion which are local diffusion and global diffusion (Ma & Qiu, 2003).

2.4 Image Encryption Based on Chaotic System

Chaos theory is a branch of mathematics which is focused on the behavior of dynamical systems that are highly sensitive to initial conditions. Chaos phenomena refers to the random phenomena happened in nonlinear dynamic system; this phenomena is non-periodic, non-convergent, which is extremely sensitive to the initial and external parameters. Chaotic system is a nonlinear dynamic system (Li & Yorke, 1975) which can produce pseudorandom sequence with good randomness and is very suitable for data encryption. The chaotic system was proposed for data encryption in 1997, Fridrich first proposed image encryption scheme based on chaotic system (Fridrich, 1997). In 1998, Fridrich proposed another image encryption method based on 2D chaotic mapping (Fridrich, 1998). In this method, the pixel location of image is changed by using two-dimensional Baker’s mapping; then, the mapping extends into 3D mapping, and the value of each pixel has been modified as well. Since then, chaotic cryptography as a branch of cryptography has been investigated broadly.

The encryption of digital images by using chaotic system is mainly based on the excellent randomness of this system, the chaotic system is usually combined with image encryption methods based on spatial domain. A myriad of encryption methods have been proposed by using chaotic system.

Relying on randomness, which is generated by using the chaotic system, digital images have been encrypted by using chaotic mapping algorithms, such as CKBA encryption method (Guo, 2000), Kolmogorov flows-based encryption (Scharinger, 1998), image replacement and encryption (Guan & Huang, 2005).

In 2006, an image encryption algorithm based on chaotic logistic map has been proposed (Pareek & Patidar, 2006). In combination with the corresponding mathematical methods, the initial values of two logistic sequences are generated by using an external key with the length of eighty bytes and eight types of operations to encrypt the pixels of the image. Each of the 16 pixels of the image is grouped into a small block, each bit of the pixel is operated by using the chaotic logistic sequence. Therefore, the robustness of this algorithm is very high and the capability against attacks of the algorithm is also strong.

In 2012, the standard map (Fu & Chen, 2012) was improved so that it could change the pixel positions. In the chaotic mapping algorithms, the chaotic sequence, which is generated by using secret key stream, is usually used to scramble the pixels. For this improved algorithm, it not only relates to secret key in the scrambling process, but also associates to pixel positions which have been scrambled. This scrambling method improves the security of image encryption and enhances its ability against various attacks.

In 2003, based on Fridrich's method, a fast image encryption scheme has been putforwarded (Mao & Chen, 2003), 3D Baker's mapping has been used in this method. The results show that the encryption speed is 2 to 3 times as fast as the Fridrich's method; the security is also improved.

In 2018, an image encryption algorithm based on the memristive chaotic system, elementary cellular automata (ECA) and compressive sensing (CS) (Chai & Zheng, 2018) was proposed. The original image is transformed by discrete wavelet transform firstly, and the sparse coefficient matrix is obtained. Next, a zigzag scrambling method and the ECA are adopted to scramble the sparse coefficient matrix; then, the measurement matrix produced by the memristive chaotic system is used to compress and perceive the scrambled image; simulation results and performance analyses demonstrate the security and robustness of the proposed method.

2.5 Image Encryption Based on Frequency Domain

Compared with text information, image often contains more amount of data, the redundancy of the image is high and the correlation of the image pixels is strong. In order to transmit and storage the image, orthogonal transform is often applied to the original image. If a method is required, the transformation of this original image from sptail domain to frequency domain before encryption, we call that this kind of methods of image encryption are based on frequency domain. By using the transform algorithms, the mutual transformation can be achieved between spatial domain and frequency domain, some commonly-used transform algorithms are discrete cosine transform (DCT), discrete wavelet transform (DWT) and discrete Fourier transform (DFT). The rationale of this method is to transform the images from spatial domain to frequency domain first, get the frequency coefficients, then change the position or value of the coefficients through those specified rules, and then apply the inverse transform to the transformed data and get an encrypted image.

Image encryption algorithm based on frequency domain encrypts the frequency coefficients based on the characteristics of human visual system, it can encrypt important data which is called selective encryption or partial encryption, so that the amount of encryption data is significantly reduced and the encryption efficiency is improved. At the same time, this kind of methods can work well in combination with the image compression algorithm. The amount of data transmitted over the network can be reduced. However, these methods need to achieve mutual transformation between spatial domain and frequency domain, the amount of computation is increased. Since mainstream image encryption methods focus on the transform domain, widely used image encryption methods and commonly used transforms will be elucidated.

2.5.1 Image Encryption Based on DRPE

Optical image encryption is the most commonly-used methods based on frequency domain. In particular, optical image encryption has attracted public attention since the DRPE has been proposed (Refregier & Javidi, 1995). DRPE uses the techniques such as 4F and Fourier Transform (FT) enabling the spatial and spectral information to be encrypted; the image encryption is implemented by using random-phase encoding for both the input and the Fourier planes. In this way, the whole encryption process converts the input image into white noise. The decryption is conducted by using its inverse process. The decrypted image is correctly obtained only if the secret key and its spatial information are exactly matched. The random phase masks could be treated as secret keys and as the key space is very large. It is extremely difficult to reconstruct the original image without the secret key.

Since the double random phase encoding (DRPE) was proposed in 1995, a large number of image encryption algorithms based on DRPE have been proposed, DRPE technique thus witnessed the development of optical cryptography. With further investigation into this technique, the defects of DRPE have been realized based on the problems of traditional DFT-based DRPE; the corresponding improvement has been developed.

In 2000, an optical image encryption was proposed based on joint transform correlator (JTC) (Nomura & Javidi, 2000). In this work, the original image and one of the phase plates, which was used as the encryption key, are put together on the JCT input plane; then, the Fourier Transform is adopted. After the transform, the joint Fourier power spectrum is obtained as the encrypted image. During the decryption process, the phase plate, which is used as the decryption key, is arranged at the corresponding position on the space plane; the encrypted image is arranged on the Fourier spectrum plane through filtering on frequency domain and inverse Fourier transform. In this way, JTC encryption overcomes the disadvantages of traditional DRPE. As the encrypted image is based on a Fourier power spectrum, it is workable and unnecessary to let the complex conjugate phase plate be as the secret key; the improvement of secret key on the input plane only changes the position of decrypted image; therefore, the quality of decrypted cannot be affected.

In order to obtain more keys and improve performance, Fractional Fourier Transform (FFT) is proposed as a more general DRPE scheme (Unnikrishnan & Joseph, 2000). There are three planes: input plane, encrypted plane and output plane. The FFT has three parameters connecting any two out of three planes; thus, it not only has the scheme used two phase plates as the secret keys, but also the six parameters can also be supplied as the secret key, the key space is greatly enlarged.

In 2013, a multi-image encryption algorithm was proposed based on cascaded fractional Fourier transform (Kong & Shen, 2013). In this method, the input images are successively encrypted using a series of encryption keys until a final encrypted image is obtained. The algorithm not only works for the encryption of multiple images, but also is very secure. Because there are so many secret keys, the algorithm can be applied to multi-user authentication.

In 2000, a generalized image encryption algorithm based on fractional Fourier transform (Zhu & Liu, 2000) was proposed, this method allows us to use a new generalized fractional Fourier transform instead of random phase mask. In this algorithm, the period of fractional Fourier transform is extended to any integer; thus, the period and transformation index are regarded as two secret keys. The generalized fractional Fourier transform is based on realignment of traditional fractional Fourier transform which is called multistage FRT or multichannel FRT.

In 2015, a novel quantum image encryption algorithm based on generalized Arnold transform and double random-phase encoding (Zhou & Hua, 2015) was proposed. The pixels are scrambled by the generalized Arnold transform and the gray-level information of images is encoded by the double random-phase operations. The keys of the encryption algorithm include the independent parameters of coefficients matrix, iterative times and classical binary sequences; thus, the key space is extremely large. The results demonstrate that the proposed algorithm with good feasibility and effectiveness has lower computational complexity than its classical counterpart.

2.5.2 Transform Algorithms Based on DWT

Fourier transforms are able to capture the characteristics of the signals over the whole sample time. However, it cannot be used to carry out multiresolution analysis (MRA). On the other, hand Wavelet Transform (WT) has the ability to represent signal information in both time and frequency domains. Discrete Wavelet Transform (DWT) has been widely used in image processing and we will introduce DWT application in image encryption.

In 2017, three optical encryption schemes based on DRPE by using DWT were proposed (Mohamed & Samrah, 2017). These three schemes were based on DRPE by using DWT and chaotic maps, one of them adopted DWT instead of FFT in traditional DRPE. Another took use of DWT and steganography combined technique; the last one used FRFFT, DWT and steganography together. The results were compared with three traditional techniques for DRPE. From the performance metrics, the proposed three methods based on DWT achieve better performance and robustness versus conventional ones.

In 2013, a new digital image encryption algorithm based on DWT-SVD framework was proposed to resolve the security problem of digital image in communication channel transmission (Wang & Wang, 2013). It had good irreversibility against the geometric attacks on the images singular value as well as DWTs multi-resolution characteristics which can represent local information, the designed SVD-DWT algorithm could well fight against geometric attacks in communication channel, thereby ensure the security, invisibility and robustness of the image transmitted in the channel.

2.5.3 Transform Algorithms Based on DCT

DCT has a strong energy concentration characteristics in the low frequency part after transform. Moreover, when the statistical characteristics of the signal is close to the Markov process, the decorrelated performance of DCT is close to the performance of K-L transform; the latter has the best decorrelated performance (Song, 2013) so that DCT is widely used in image processing such as image compression and image encryption. Compared with DFT, the computations in DCT are in real domain, avoiding complex operations and improving the speed. DCT also has translation, rotation and scaling invariance of Fourier transform which can resist geometric attack effectively. Because of these advantages, DCT has outstanding performance in the field of image encryption and has been used in a lot of recently research projects.

In 2010, an image encryption algorithm was proposed based on Arnold transform and DCT (Liu & Xu, 2010). DCT was chosen because the pixel value of the image is defined in real domain and the matrix still remains in real domain after the transformation. On the other hand, the partition operation was applied before Arnold transform so that the operation can be clearly seen. As a result, the security of these encrypted images was improved.

In 2011, an image encryption algorithm using DCT and Secure Hash Algorithm-1 (SHA-1) were proposed (Yuen & Wong, 2011). In this method, DCT is applied to the original image at the first place, the DCT coefficients of this whole image are separated into two sequences. The low-frequency sequence and secret keys are used to generate message and interact with high frequency sequence. The digital simulation results confirm that the proposed algorithm has high robustness against attacks and high sensitivity to the key.

2.5.4 Transform Algorithms using SVD

Singular value decomposition (SVD) is a matrix transformation method based on eigenvalue. Every image can be presented as a matrix, SVD can decompose the matrix into the sum of many matrices. SVD itself is not related to the transformation between spatial and frequency domain, but the singular value of an image has good stability; it usually combines with transform algorithms in image processing. When the image is subjected to disturbances, the singular value will not be changed too much. Moreover, the singular vector of the matrix also has invariance with regard to translation, rotation, etc. (Yuan & Zhou, 2011). Therefore, the singular value can effectively reflect the characteristics of the matrix. When applied to a matrix of an image, the singular value and its spanned vector space of an image reflect the different components and features of the image. The algebraic characteristics of this image can be represented as well so that the SVD is widely used in image processing. Because of its stability and rotation invariance, most of the current image encryption algorithms are based on SVD which have high robustness.

In 2013, an image encryption algorithm was proposed using singular value decomposition and Arnold transform (Chen & Zhao, 2013). The original image was first transformed in the fractional domain using FRFT and then it was decomposed into three parts using SVD. These three parts were Arnold transform based. In the decryption process, after inverse Arnold transform and inverse FFT, the corrected image can be reconstructed.

In 2014, an image security system based on SVD and Gyrator Transform (GT) was proposed (Abuturab, 2014). The original image is decomposed into three channels during the encryption process. Each channel was modulated by using RPM; then, the Gyrator transform was applied to obtain a ciphertext. After that, the ciphertext is separated using SVD. The numerical simulations were presented and the results have shown the algorithm to have high security level and robustness.

2.6 Digital Watermarking Algorithms

Recently, much progress has been made in digital watermarking as one of the main branches of information hiding. These techniques hide the watermark data into the host data for the purposes such as digital product protection. Based on the different purposes of watermark, these techniques can be divided into robust watermarking techniques and fragile watermarking techniques. Robust watermarking techniques require resistance to various attacks during the transmission such that the watermark information can be extracted after transmissions. The various robust watermarking algorithms can be divided into two domains. The first one embeds and extracts watermark in spatial domain. This kind of algorithms are easy to be achieved, but only little information can be embedded into host data; hence, the robustness of these algorithms is not satisfactory. The other achieves watermark embedment and extraction in frequency domain using algorithms such as DCT, DWT, and DFT. More information can be embedded into the host; they have higher robustness compared to the first one.

It has been noticed that the use of a single algorithm is no longer able to meet the robustness requirements of digital watermarking. Using a single algorithm often introduces that cannot be solved effectively. Hence, current research outcomes focus on designing joint algorithms in frequency domain.

In 2012, a watermarking technique based on DCT-DWT framework was proposed (Deb & Al-Seraj, 2012). In this method, DCT technique was used for compression while the DWT technique provides scalability. Compared with the methods which only use DCT or DWT, the experimental results show that the proposed method has satisfied robustness under various attacks such as JPEG compressiong, cropping, sharping, contrast adjustments and so on.

In 2011, a novel watermarking algorithm for digital images based on DWT-DCT-SVD framework was proposed (Yuan & Zhou, 2011) where a four-layer DWT was applied to the original image. First, the low-frequency subband and three high-frequency subbands of the fourth layers were chosen. Similarly, the same operation was applied to the watermarking image in order to get four subbands. Then, by using DCT and SVD, the four subbands, obtained from the watermarking image, were embedded into those of the original image adaptively. Finally, the watermarked image is obtained after the inverse SVD, DCT and DWT. Compared with the methods by using DCT-SVD and DWT-SVD frameworks, the experiments show that this method has more robustness against noise and geometric attacks.

2.7 Image Denoising Strategies

In the field of digital image processing, the image is often attacked by various noises and the quality of image will be decreased; whether image noise can be effectively filtered out or not will directly affect the subsequent processing such as object segmentation, edge detection, feature extractio, image decryption and so on. Therefore, filtering the image noises is thought as a meaningful work. For the 2D visual signals, we usually have two forms of filterings which are based on spatial domain and frequency domain. Image filtering in spatial domain closely relates to the pixel intensity and its neighbors; meanwhile, image filtering in frequency domain utilizes the coefficients of multiple frequencies after visual signal decomposition.

For these two domains, the corresponding denoising methods can be categorized into spatial domain-based or frequency domain-based methods. The spatial domain-based methods directly tackle the intensity of each pixel of an image. The frequency domain-based methods handle the issue of image denosing by adjusting corresponding coefficients of multiple frequencies after image decomposition in frequency domain. The inverse transformation is usually accomplished to reconstruct the image using those modified coefficients and achieve the purpose of image denoising (Milanfar, 2013). Recently, Artificial Neural Networks (ANN) were employed as a classifier for pattern classification in this field of digital image processing, e.g., optical characters recognition (OCR), face detection and recognition, image restoration and reconstruction, image enhancement, etc. With the further study of neural networks, the merits of neural networks in digital image processing have been fully investigated. Some widely used traditional image denosing methods and the approachs based on nerual networks will be detailed.

2.7.1 Traditional Image Denoising Methods

Average filtering is one of the typical linear filters (He & Pan, 2012) for image denosing. In 2007, combined with wavelet transform and average filtering, an efficient denoising method was proposed (Changlai, 2007). The denoised image was reconstructed by composing together three high-frequency components of the image with average filtering and low-frequency approximation. The method has better denoising result than that of the wavelet thresholding method or average filtering method.

Wiener filtering was a typical image denoising method, especially for motion blur removal. In 2007, considered that the directionalet coefficients of an image with Gaussian noise are subject to a normal distribution, a new algorithm was proposed (Wang, Qv & Cui, 2007). By using Weiner filter with the directionalet coefficients, the image can be denoised effectively; meanwhile, the multidirectional framework has shown its super power in image denoising.

Median filtering can enhance images caused by blurring operations. In 2011, based on traditional median filtering, an improved fast algorithm of median filtering has been designed (Ming & Li-hua, 2011) which could achieve better results of noise removal.

2.7.2 Image Denoising Based on Neural Networks

Artificial neural networks (Xu & Lu, 2003) have been widely used in image denoising because the networks adapt the nonlinear operations for digital image processing; furthermore, a nonlinear model of image denoising can be constructed without prior knowledge. Meanwhile, the parallel processing ability of neural networks makes it possible for image denoising and speeding up image denoising process (Chen & Lien, 2010). The pulse coupled neural network models, convolutional neural network models and fuzzy neural network models are effectively applied to image denoising.

In 2017, a PCNN (pulse coupling neural network)-based image noise reduction has been proposed (Yan & Wu, 2017). In this method, the basic PCNN model has been simplified and the weights have been adjusted adaptively; furthermore, the algorithm accuracy for identifying noises has been improved by posting noise points according to the difference of firing times between a neuron and its surrounding ones. Through using this algorithm, distinct results for image denoising have been achieved.

CNN is a feedforward neural network, whose artificial neurons can respond to a number of surrounding units in a range of coverage that has excellent performance for large image processing (LeCun & Bengio, 1995). It usually includes convolutional layers and pooling layers; a convolutional layer is used to extract features of the image; a pooling layer is usually employed to reduce structure parameters of the network (Liu & Shen, 2015). The weight sharing of CNN reduces computational complexity of the network, especially for the images which have multiple input vectors. These images can be input into the network directly so that the computational complexity problem in the process of feature extraction and pattern classification has been avoided (Zhao & Yu, 1999).

In 2017, a method based on deep CNN was proposed (Yan & Wu, 2017). The method adopted the integrated image as the input and output of the network. The hidden layers are used to build a nonlinear mapping from a noisy image to its denoised image. The network has a symmetric structure consisting of convolution subnet and deconvolution subnet. Convolution subnet learns from image features and the deconvolution subnet recovers the original image based on characteristic graph and obtains more textural details by combining rectified linear units together. This method used VOC2012 as its training dataset and the Google platform TensorFlow as a tool to train the network model in GPU environment.

In 2016, an image denoising method based on convolution neural network has been generated (Wang, 2016). The structure of this CNN model includes only the convolutional layer without pool layer. The denoising process includes image block extraction, nonlinear mapping and image reconstruction. This study expands the applications of convolution neural network in image processing.

In 2016, an extension to traditional deep CNNs and symmetric gated connections, is added to aid faster convergence transfer of high-level information normally lost during downsampling (Zhao, 2016). The proposed model can be applied to solve the classic task of image denoising; after training 50,000 training images, the results showed that the DSC model performed better than traditional downsampling and upsampling structures; gated connections begin to make great improvements in feature learning and image denoising.

In 2012, owning to low-level vision problems that combine sparse coding and deep networks pretrained with denoising autoencoder (DA), an alternative training scheme has been proposed (Xie & Xu, 2012). The proposed scheme adapts DA successfully and it performs well in unsurprised learning. Experimental results demonstrate the effectiveness of the proposed method in the tasks of image denoising and blind inpainting. In image denoising task, the proposed method is compared with traditional KSVD technique, which shows better performance in denoising white Gaussian noise. In blind image inpainting task, the proposed method provides solutions to a plethora of complex problems that have not been tackled before, which in detailed view, a raft of complex patterns like superimposed text from an image can be removed automatically, the problems, e.g., pixel missing, can be avoided effectively.

Chapter 3
Methodology

The main content of this chapter is to articulate research methods, which satisfy the objectives of this thesis. The chapter mainly covers the details of the methodology for all proposed image encryption methods which are the traditional chaotic scrambling-based method, the improved method based on DRPE using DCT, the encryption method based on DCT-DWT-SVD and the improved method based on DCT-DWT-SVD using denoising methods. All of the proposed methods will be clearly introduced.

3.1 Research Designing

In this section, we will provide the research methodlogy and the research project plan, which is designed to execute research methodlogy, the rationale of proposed methods will be also addressed. Based on the objectibve and research questions of this thesis, the aim of this research is to provide the final answers of research questions, so that our research can be defined as conclusive research, which is required formal and definitive methodlogy. In this case, we made the specific research project plan to explain the rationale and execute the methodlogy as the following phases:

(1) Selecting research area, in this project, we will make efforts in image encryption;

(2) Defining the objective and research questions through the relevant literature critiques, in this research, we aim at improving the robustness of traditional DRPE-based method and proposing robust image encryption methods;

(3) Designing the specific experiments to address research questions, then, we propose the conclusive methods to achieve objective of the research from the experimental results. In this research, we proposed four image encryption methods. The first method is the chaotic scrambling method using logistic map; the second is based on traditional DRPE method and 4F system, we design the improved version using DCT to replace DFT; the third one is to use DWT-DCT-SVD framework; the last one we proposed is to combine Method III and the image denoising methods together;

(4) Conducting data collection through results of each method;

(5) Taking account of quantitative data analysis, in this research, we mainly use encrypted and decrypted results, as well as performance metrics of each method to achieve dataanalysis;

(6) Performing comparative analysis via each proposed method, conducting the conclusion, all of the research questions will be answered and our conclusive research will be achieved.

3.1.1 Method I: Chaotic Scrambling Based on Logistic Map

The logistic map is a polynomial mapping, which has been widely used for image encryption. The traditional logistic map generates a chaotic sequence and the number of elements in this sequence is equal to the number of pixels in the original image. We will explain how to use the logistic map for image encryption. Eq. (3.1) is employed as the logistic map to generate the random sequence and furthermore to encrypt a digital image.

$$X_{n+1} = \mu X_n(1 - X_n) \tag{3.1}$$

where $X_n \in [0,1]$, $\mu \in [0,4]$ is a constant. The previous work has shown that when $X_0 \in [0,1]$, the logistic map works in a chaotic state; in this case, the sequence which is generated by using logistic map is aperiodic and non-convergent. If X_0 is beyond the range of $[0,1]$, the sequence converges to a particular value. In our experiment, we selected μ on interval $[3.569,4]$ and used the generated sequence to encrypt an image directly. We sort the double precision sequence which is generated by using the logistic map, we scramble the location of each pixel of the original image.

3.1.2 Method II: Chaotic Map based on DRPE by using DCT

DRPE was implemented using an optical setup, called 4F system, which is illustrated in Figure 3.1.

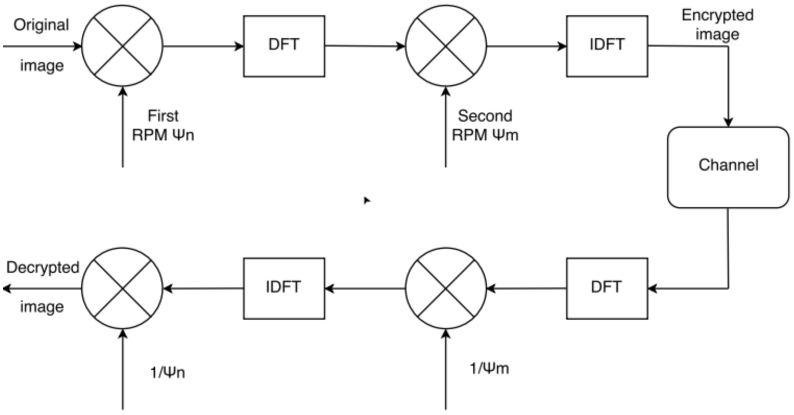


Figure 3.1 The workflow of DRPE by using DFT

Now, let's consider a primary intensity image $\mathrm{OI}(x, y)$, where x and y are the coordinates of a pixel in spatial domain, u and v represent the corresponding coordinates in Fourier domain. Let $\mathrm{EI}(x,y)$ denote the encrypted image, $N(x,y)$ and $M(x,y)$ stand for two uniformly distributions. To encode $\mathrm{OI}(x,y)$ into a white stationary sequence, two random phase masks are used $\Psi_n(x,y) = exp[2i\pi N(x,y)]$ and $\Psi_m(x,y) = exp[2i\pi M(x,y)]$. We thus perform two operations; first, we multiply this image by using the first phase mask $\Psi_n(x,y)$; then, we conduct convolution of this image by using the impulse response $H(x,y)$, which is a phase transfer function and $H(x,y) = M(x,y)$. The impulse response $H(x,y)$ is defined by using Fourier transform.

$$\mathrm{DFT}\{H(x,y)\} = H(u,v) = \Psi_m(u,v) = exp[2i\pi M(u,v)] \tag{3.2}$$

where $N(x,y)$ and $M(x,y)$ are secret keys. The encryption function is

$$\mathrm{EI}(x,y) = \{\mathrm{OI}(x,y)\cdot \Psi_n(x,y)\} * \mathrm{IDFT}\{\Psi_m(u,v)\} \tag{3.3}$$

Since we have used convolution operation in Eq. (3.3), the convolution is represented as Eq. (3.4).

$$f * g = \mathrm{IFT}[\mathrm{FT}(f) \cdot \mathrm{FT}(g)] \tag{3.4}$$

where f and g are two integrable functions, FT refers to Fourier transforms and IFT refers to its Inverse Fourier transforms. Based on Figure 3.1 and the convolution theorem, we use Eq. (3.5) to encrypt a plaintext and the decryption is a reserve process of encryption.

$$\mathrm{EI}(x,y) = \mathrm{IDFT}\{\mathrm{DFT}[\mathrm{OI}(x,y) \cdot \Psi_n(x,y)] \cdot \Psi_m(u,v)\} \tag{3.5}$$

Based on traditional DFT and 4F system, we used DCT to replace DFT and proposed the new method. Meanwhile, DCT is a transform related to the traditional Fourier transform, it is similar to DFT, but it only uses arithmetic operations to process the image. Using DCT to facilitate the process of image encryption and decryption, it avoids complex operations. Therefore, we design the DCT method based on DRPE; in the traditional DRPE system, we use two random phase matrices $N(x,y)$ and $M(x,y)$ as the secret keys which are uniformly distributed in $[0,1]$, the size of these two matrices is equal to the original image $\mathrm{OI}(x,y)$. We see that the amount of secret keys is too large, so it’s inconvenient for transmission. Based on logistic mapping, we use Eq. (1) to generate chaotic maps and the traditional random phase matrices are replaced by using the generated chaotic maps so that the initial value x_0 and parameter μ of the chaotic maps can be utilized as secret keys. As a result, the size of secret keys is reduced effectively.

3.1.3 Method III: Encryption Method Based on DWT-DCT-SVD

In this section, we will apply a similar idea of image watermarking for image encryption so as to hide secret image as the watermark inside the host image. The watermarking algorithm can be treated as the encryption process of secret image. In the process of watermark extraction, the host image is needed and it can be treated as the secret key for encryption. The process of watermark extraction can be treated as the image decryption. The basic workflow for the proposed encryption method based on watermark technique is illustrated in Figure 3.2.

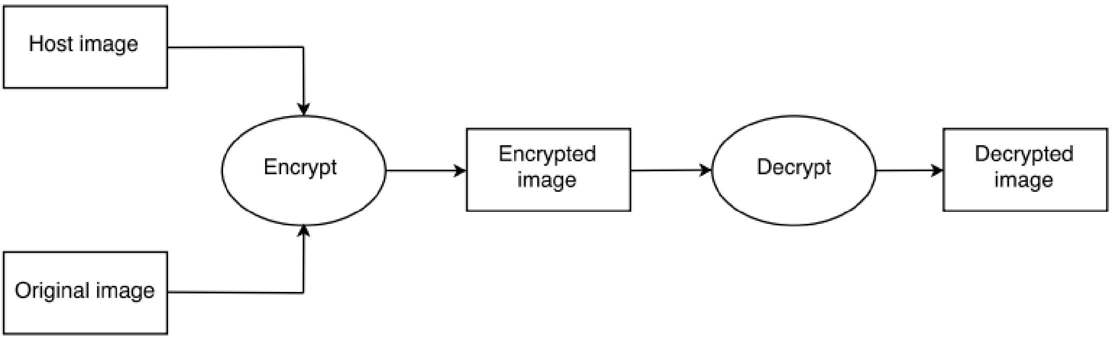


Figure 3.2 The workflow of our method

Since we have mentioned in the literature review, DWT and SVD are two transform algorithms based on transform domain which are widely used in image encryption, image compression and signal-noise separation. We will use these two algorithms in our proposed encryption method, the rationale for these two algorithms will be detailed. Two-dimensional DWT is broadly used in image encryption, the rationale of DWT is illustrated as Figure 3.4.

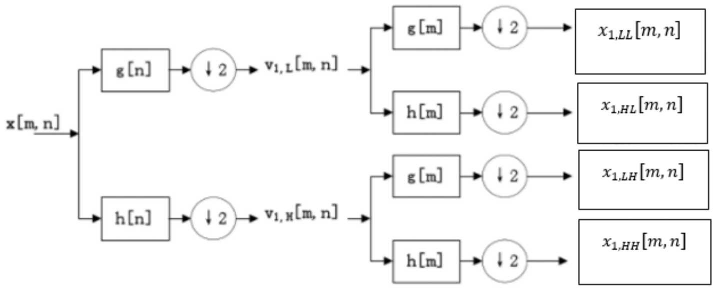


Figure 3.3 One layer 2D DWT

In Figure 3.4, $x_{[m,n]}$ represents the input image, the size of this image is $M \times N$, $\mathrm{g}[n]$ and $\mathrm{g}[m]$ are low-pass filters which can filter the high-frequency part of input signal and output the low frequency part; $\mathrm{h}[n]$ and $\mathrm{h}[m]$ are high-pass filters which can filter out the low-frequency part of input signals and output the high frequency part; $\downarrow 2$ is downsampling filter. If the input signal is $x_{[n]}$, then the output is $y_{[n]} = x[Qn]$, in Figure 3.4 we set $\mathrm{Q} = 2$.

Based on Figure 3.4, the input image $x_{[m,n]}$ will be processed in the vertical direction firstly. Throughout low-pass filter g and high-pass filter h, the output is then downsampled by 2, we will get two components $v_{1,L}[m,n]$ and $v_{1,H}[m,n]$. Through low-pass filter g and high-pass filter h, the outputs are downsampled by 2 in the horizontal direction, respectively. Finally, we get four components which are $x_{1,LL}[m,n]$, $x_{1,HL}[m,n]$, $x_{1,LH}[m,n]$ and $x_{1,HH}[m,n]$, we call the whole process as one-level wavelet transform. After this transform, we get four matrices corresponding to the four components. The total size of output matrices equals to the input matric; but during the process of DWT, the frequency band has been divided into high-frequency part and low-frequency part, so the size of each output matric is $\frac{M}{2} \times \frac{N}{2}$; meanwhile, the original image is divided into four subbands - one low-frequency subband (LL), LL represents the original image through low-pass filter in both of directions. Because a 2D image can be divided into different frequency components, among them, the low-frequency component describes the approximate information of original image, the high-frequency component describes the details of original image. Because the low-pass filter outputs the low frequency part of the image, it describes the approximate information of the original image and used for further decomposition process; among the three high frequency subbands (HL, LH, HH), LH subband represents the original image through the high-pass filter in horizontal direction and low-pass filter in the vertical direction, it describes the horizontal details and approximates vertical information of the original image. In other words, LH extracts the horizontal features of original image; Similarly, HL subband gives the vertical features of original image; for HH subband, the original image, through high-pass filter in the both directions, describes the diagonal features of original image.

Singular value decomposition (SVD) has been widely used in image compression and signal noise separation. Let's consider a matrix $\boldsymbol{A} \in C^{m\times n}$, the size of $\boldsymbol{A}$ is $\mathrm{m}\times\mathrm{n}$, the SVD of $\boldsymbol{A}$ is represented as Eq. (3.6)

$$\boldsymbol{A} = UDV^T = [u_1, u_2, \dots, u_n]\begin{bmatrix}\sigma_1 & & \\ & \dots & \\ & & \sigma_n\end{bmatrix}[v_1, v_2, \dots, v_n]^T = \sum_{i=1}^{n}\sigma_i u_i v_i \quad (3.6)$$

where $\boldsymbol{D}$ is a diagonal matrix, $\boldsymbol{U}$ is an $m \times m$ orthonormal matrix, which is called left singular matrix for $\mathbf{A}$, $\boldsymbol{V}$ is an $n \times n$ orthonormal matrix, which is called right singular matrix for $\mathbf{A}$, $\boldsymbol{U}^T\boldsymbol{U} = E$ and $\boldsymbol{V}^T\boldsymbol{V} = \boldsymbol{E}$; u_i is column vector for $\boldsymbol{U}$, which is defined as orthogonal eigenvectors group for square matrix $\boldsymbol{AA}^T$, v_i is column vector for $\mathbf{V}$, which is defined as orthogonal eigenvectors group for square matrix $\boldsymbol{A^TA}$, we use Eq. (3.7) to represent u_i and v_i.

$$(\boldsymbol{AA}^T)u_i = \lambda_i u_i \quad (3.7)$$

$$(\boldsymbol{A^TA})v_i = \lambda_i v_i \quad (3.8)$$

where λ_i is eigenvalue for matrices $\boldsymbol{AA}^T$ and $\boldsymbol{A^TA}$,

$$\sigma_i = \sqrt{\lambda_i} \quad (3.9)$$

where $i = 1,2,\dots,\sigma$. $\sigma_1, \sigma_2, \dots, \sigma_i$ are called singular values for matrix $\boldsymbol{A}$, and $\sigma_1 \geq \dots \geq \sigma_r \geq \sigma_{r+1} = \sigma_n = 0$.

The idea of the proposed encryption method is based on a watermarking technique which has high stability. We combined DWT, DCT and SVD together and designed the new image encryption sheme which implements the high stability. The entire framework is divided into encryption part and decryption part. The proposed encryption method based on DWT-DCT- SVD framework can be used for both greyscale image and color image; as we know, a color image has R, G and B three comphonents; for the color image encryption, Matlab allows to apply the encryption method to each component.

3.1.4 Method IV: Encryption Method Based on DWT-DCT-SVD by Using Denoising Methods

Based on the DWT-DCT-SVD encryption method, we have designed the method which is suitable for both greyscale image and color image; in this section, we use color image as the input. We will filter out Gaussian and salt-and-pepper noises before image decryption, so that the anti-attack ability of encryption algorithm against these two noise attacks will be improved.

We proposed three traditional denoising methods which are using linear and nonlinear filterings; two of linear filters are average filter and Wiener filter, the nonlinear filter is median filter. We will provide the rationale for each filter.

The average filtering is a typical linear one which uses neighborhood averaging method, the basic rationale for average filtering is to use the average value of all pixels which around target pixel to replace the original target pixel value. For an image, the target pixel will be selected at the first place; then, all the pixels around the target pixel are treated as a filtering operator; meanwhile, the original value of the selected pixel will be replaced by average value of all pixels in the filtering.

We applied the average filtering to digital images; for each pixel of the image, the filtering operation calculates the product of its neighborhood pixel matrix and the corresponding element of the filter operator matrix. Because the filter is centrally symmetric, the filtering operation is equivalent to the convolution between the image and this filter, the filter is also called convolution kernel. Let’s consider the size of image A is $M \times N$, the filter operator can be illustrated as Eq. (3.10)

$$F_{Mean}^{(n)} = \begin{bmatrix} 1/n^2 & \cdots & 1/n^2 \\ \vdots & \ddots & \vdots \\ 1/n^2 & \cdots & 1/n^2 \end{bmatrix} \tag{3.10}$$

The size of this operator is $n \times n$, the value of n should be an odd number, the filter has a center element. In our method, we take $n = 7$ and the filtered image is represented as Eq. (3.11)

$$\bar{A} = A * F_{Mean}^{(n)} \tag{3.11}$$

In our method, image A is a color image, it has R, G and B three color components, each component is formed by a 2D matrix. Let's consider the input image is $A_{in} = (R_{in}, G_{in}, B_{in})$, the output image is $A_{out} = (R_{out}, G_{out}, B_{out})$, the traditional average filtering is to filter each color component separately and only use a convolution kernel (average filter operator), which can be represented as Eq. (3.12)

$$\begin{gathered} R_{out} = R_{in} * F_{Mean}^{(n)} \\ G_{out} = G_{in} * F_{Mean}^{(n)} \\ B_{out} = B_{in} * F_{Mean}^{(n)} \end{gathered} \tag{3.12}$$

Wiener filter is an optimal estimator based on the minimum mean square error criterion for the stationary process. The Wiener filtering minimizes the mean square error between the estimated random process and the desired process; it is an optimal filter and can be used to extract signals contaminated by stationary noise. Wiener filtering leverages the local mean and variance information of an image, the rationale of Weiner filter is represented as Eq. (3.13)

$$\bar{A}(x,y) = \mu + \frac{\sigma^2 - v^2}{\sigma^2}(A(x,y) - \mu) \tag{3.13}$$

where $\bar{A}(x,y)$ is the value of target pixel after filtering, μ represents the mean value around the target pixel $A(x,y)$, σ^2 stands for the variance around the target pixel $A(x,y)$; v^2 is the estimated noise variance for nearby pixels of the target pixel. μ and σ^2 are calculated by using Eq. (3.14)

$$\mu = A * F_{Mean}^{(n)} \tag{3.14}$$

$$\sigma^2 = A^2 * F_{Mean}^{(n)} - \left(A * F_{Mean}^{(n)}\right)^2$$

where $F_{Mean}^{(n)}$ is a convolution kernel for each element in matrix A, we calculate its square value and get the matrix A^2.

Median filtering is a kind of effective noise suppression of nonlinear signal processing technology based on the order statistical theory. The basic rationale for median filtering is for a specific point on the image by calculating the median value of each neighborhood pixel regards to the specific point by using the median value instead of the original pixel value of this point; the isolated noise points can be eliminated. We use Eq. (3.15) to represent the process.

$$g(x,y) = med\{f(x-k, y-l), k, l \in W\} \tag{3.15}$$

where $f(x,y)$ and $g(x,y)$ are original image and the image after denoising, W is median filter. It consists of matries, usually 3×3 or 5×5.

As we know, CNN has made remarkable contribution in many fields related to image processing. In this section, we will use CNN in image denoising. Compared with the traditional image denoising methods, the advantage of CNN is that the parameters of its models can be optimized by learning; but for the traditional algorithms, the parameters are fixed; in other words, the algorithms are not able to optimize the parameters during the filtering process.

We design a linear CNN network and use the convolutional layer in this network to simulate the average filtering. Let the initial size of the convolution kernel be 11×11; during the training process, if a smaller kernel can get better results, then the CNN network will optimize the convolution kernel by letting the external elements of convolution kernel be 0. Afterward, a new convolution kernel can be obtained which is equivalent to the smaller kernel. The structure of this network is illustrated as Figure 3.8. In Figure 3.8, we see that our model has four layers; therefore, we explain the CNN network layer by layer.

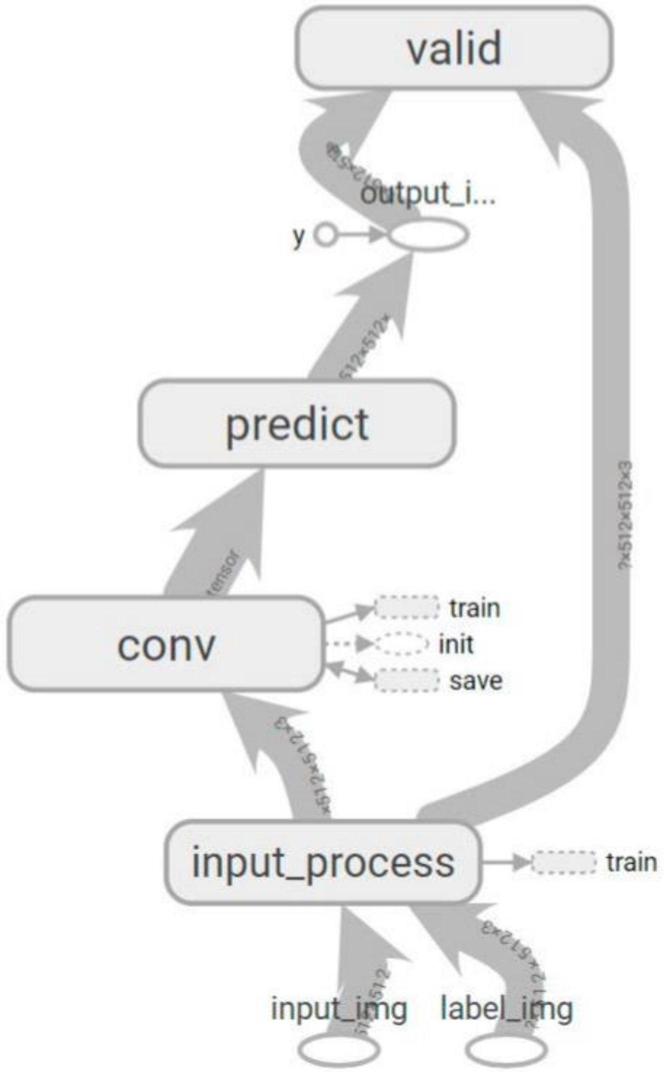


Figure 3.4 The structure of linear CNN network

1) **Input layer**. The input image is represented as a matrix and the intensity of each pixel in the matrices is an integer which belongs to $[0, 255]$. In order to make the computing easier, we normalize the pixel values as a floating number which belongs to $[0, 1]$ in Layer 1.

2) **Convolutional layer**. This layer is the core part of CNN model. The parameter optimization and filtering operations are conducted in this layer. The initial size of this convolution kernel is 11×11 which is self-adaptive for better image denoising based on network training. The filtering operations are represented as Eq. (3.16).

$$I'(i,j) = K \star I(i,j); i,j = 1,2, \dots, N \tag{3.16}$$

where $K = \{W_{ij}\}_{N\times N}$ is the convolution kernel and I refers to the input data of convolutional layer, $'\star'$ is the convolution. As we know, we used a color image as the input in our experiments, the image has three color components: R, G and B, each component is represented by using a 2D matrix. Let's consider that the input pixel color is $A_{in} = (R_{in}, G_{in}, B_{in})$, the output is $A_{out} = (R_{out}, G_{out}, B_{out})$, each color component will be filtered separately as Eq. (3.17)

$$\begin{pmatrix} R_{out} \\ G_{out} \\ B_{out} \end{pmatrix} = \begin{pmatrix} W_{11} & W_{12} & W_{13} \\ W_{21} & W_{22} & W_{23} \\ W_{31} & W_{32} & W_{33} \end{pmatrix} \cdot \begin{pmatrix} R_{in} \\ G_{in} \\ B_{in} \end{pmatrix} \tag{3.17}$$

Compared with the traditional average filtering, the proposed CNN model uses 9 convolution kernels and each output color component is composed with the convolutional outputs of all input color components and multiple convolution kernels. The essence of this filtering process is to use available images as the training dataset to reconstruct the denoised image.

3) **Predict layer**. The pixel values of output image from the convolutional layer are not necessarily in $[0, 1]$; thus, in the predict layer, we will normalize the output image. For the intensities of those pixels $I(x, y)$ which are less than 0, we make them equal to 0; for those pixel values which are greater than 1.0, we take 1.0 shown as Eq. (3.18)

$$I(x,y) = \begin{cases} 1.0 & I(x,y) > 1.0 \\ 0 & I(x,y) < 0 \\ I(x,y) & 0 \le I(x,y) \le 1.0 \end{cases} \tag{3.18}$$

4) **Validation layer**. In this layer, the MSE results between the normalized output images and the normalized labeled images will be calculated. During the training process, the learning rate is represented as Eq. (3.19)

$$\log_{10}\lambda = l_{min} + \frac{k-1}{N-1}(l_{max} - l_{min}) \tag{3.19}$$

In Eq. (3.20), λ is the learning rate, $l_{min} = 10^{-8}$, $l_{max} = 10^{-4}$, N refers to the total number of epochs, $N = 5000$, k is the current epoch number in the training process. The value of learning rate decreases with the increase of the number of epochs.

We calculate the MSE between the output image before normalization and its normalized labeled image. The reason for this operation is to ensure that the optimization can be continued. We will use an optimizer to optimize the parameters of this CNN network so as to decrease the MSE. We use the stochastic gradient descent (SGD) for the optimization, which is represented as Eq. (3.20).

$$W^{(i+1)} = W^{(i)} - \lambda \frac{\partial L}{\partial W}, i = 1,2,\dots \tag{3.20}$$

where $W^{(i)} = \left(w_1^{(i)}, w_2^{(i)}, \dots, w_n^{(i)}\right)$ is the parameter of *i*-th iteration of our linear CNN network, λ is the learning rate and L is the loss function. For the output results from the convolutional layers, if we choose the outputs, then we use an optimizer to optimize the parameter $W^{(i)}$ rather than select $W^{(0)}$ and calculate the MSE directly. With regard to this reason, let's consider x_{ij} is the pixel x on the input image, (i,j) is its location, y_{ij} is the expected output of the pixel x. After the model training, the real output of x_{ij} is $f\left(W_{ij};\ x_{ij}\right)$. The corresponding loss function is represented by using Eq. (3.21).

$$\begin{gathered} L(W;x,y) = h\left(g\left(f\left(W_x;x_{ij}\right)\right);y_{ij}\right) \\ L(W) = h\left(g\left(f\left(W_x\right)\right)\right) \end{gathered} \tag{3.21}$$

where $g(\cdot)$ is a normalized function, $h(\cdot)$ is the function for calculating MSE. We use Eq. (3.22) to represent the normalized function.

$$g(x) = \begin{cases} 1 & x > 1 \\ 0 & x < 0 \\ x & 0 \le x \le 1 \end{cases} \tag{3.22}$$

With regard to pixel x, if the actual output $f\left(W_x;\ x_{ij}\right) < 0$, then we get $g\left(f\left(W_x\right)\right) = 0$. We use Eq. (3.23) to represent $\frac{\partial L}{\partial W}$ in Eq. (3.20).

$$\frac{\partial L}{\partial W_x} = \frac{\partial L}{\partial h} \cdot \frac{\partial h}{\partial g} \cdot \frac{\partial g}{\partial f} \cdot \frac{\partial f}{\partial W_x} \tag{3.23}$$

In Eq. (3.23), we see if $g\big(f(W_x)\big) = 0$, then $\frac{\partial g}{\partial f} = 0$; thus, $\frac{\partial L}{\partial W_x} = 0$, which means stochastic gradient descent algorithm cannot optimize W_x; in this case, we calculate the MSE more times during the training process.

3.2 Evaluations

In this thesis, if the original image is A, the decrypted image is B, the size of the images is $M \times N$, we used five performance metrics to measure the similarity between original image and decrypted image for each encryption method, which are Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Normalized Cross-Correlation (NCC), Number of Pixels Changing Rate (NPCR) and Structure Similarity Index (SSIM). MSE is represented as Eq. (3.24)

$$\mathrm{MSE} = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(A_{ij} - B_{ij}\right)^2 \tag{3.24}$$

MSE can evaluate the degree of change of data; the smaller value of MSE means the better accuracy of prediction model to describe experimental data. In our experiment, MSE refers to the similarity between the encrypted images and the encrypted images after attack. Obviously, the smaller value of MSE means the higher similarity. PSNR is represented as Eq. (3.25)

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{peakval^2}{MSE}\right) \tag{3.25}$$

The unit of PSNR is decibel (dB), the $peakval$ represents the maximum image pixels, for the image represented by the 8bit integer, $peakval = 255$; for the image represented by the real number between 0 and 1, $peakval = 1$. For our experiment, the larger PSNR value means the less image distortion after attack. NCC can be represented as Eq. (3.26)

$$\mathrm{NCC} = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}A_{ij}B_{ij}}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}A_{ij}^2}\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}B_{ij}^2}} \tag{3.26}$$

NCC is used to describe the degree of correlation between two image. We used NCC to measure similarity between encrypted image and the encrypted image after attack; the larger vale of NCC means the similarity is higher. NPCR is represented as Eq. (3.27)

$$NPCR = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}\delta\left(A_{ij}, B_{ij}\right) \tag{3.27}$$

$$\delta(x, y) = \begin{cases} 0 & x = y \\ 1 & x \neq y \end{cases}$$

For images which are represented by floating-point numbers, in order to allow the existence of numerical errors, we convert them into $[0,255]$, then calculate the pixel change rates, which is represented as Eq. (3.28).

$$\delta(x, y) = \begin{cases} 0 & |x - y| \leq 1 / 512 \\ 1 & |x - y| \leq 1 / 512 \end{cases} \tag{3.28}$$

In our experiment, NPCR means the number of pixels changes in the encrypted image after attack; the smaller the *NPCR* is, the higher anti-attack ability of the methods. *SSIM* is represented as Eq. (3.29)

$$SSIM = \frac{(2\mu_A\mu_B + C_1)(2\sigma_{AB} + C_2)}{(\mu_A^2 + \mu_B^2 + C_1)(\sigma_A^2 + \sigma_B^2 + C_2)} \tag{3.29}$$

where μ_A and μ_B are mean values for ***A*** and ***B***, σ_A^2 and σ_B^2 are variance for ***A*** and ***B***, σ_{AB} is covariance for images *A* and *B*. Normally, we take $C_1 = (0.01 \cdot peakval)^2$ and $C_2 = (0.02 \cdot peakval)^2$.

In our experiment, we used *SSIM* to measure the similarity between encrypted image and the encrypted image after attack, *SSIM* is distributed in $[0,1]$; when these two images are the same, the value of *SSIM* is 1; the larger *SSIM* is, the encrypted image is more similar to encrypted image.

3.3 Summary

In this section, we introduced the rationale for our four image encryption methods in detail. The basic workflow for each method was given as well. We also provided the evaluation methods for our experiment which will be used in result discussion and analysis. In the next chapter, we are going to describe the experimental steps for each proposed encryption method, the results will be also summarized.

Chapter 4
Experimental Results

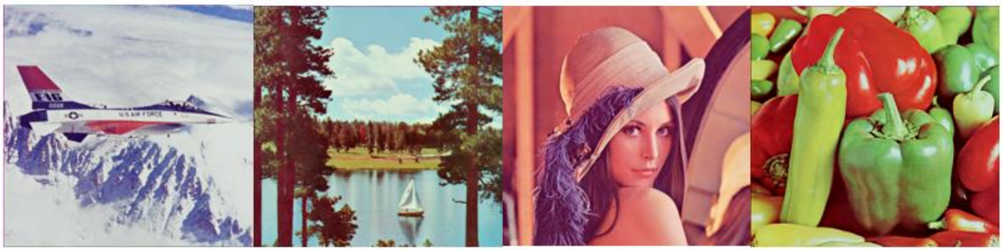
The main content of this chapter is to introduce the schema of all methods and implementation of image encryption. Each step for each method will be detailed; in addition, data collection with experimental environment will be articulated in this chapter as well as the results of each encryption method will be clarified. Furthermore, the results and findings will be evaluated as well as the limitations of this thesis will be pointed out at end of this chapter.

4.1 Data Collection and Experimental Environment

In our experiments, the proposed four encryption methods were tested by using the four sample images as shown in Figure 4.1. For each method, we applied five types of attacks to the encrypted images by using Gaussian noise, salt-and-pepper noise, average filtering, image cropping and image rotating, which is listed as follows:

- **Gaussian Noise** refers to a kind of noise, its probability density function obeys the normal distribution; it has constant mean value and variance. When the mean value is 0, we call it as white Gaussian noise; we usually use it as one of the fixed attack strategies to test the algorithms.
- **Salt-and-pepper noise** refers to a kind of noise caused by the intensity of signal pulse which can randomly put pixels to the minima or maxima; after applying this noise, the black and white pixels can be generated on the image randomly.
- **Average filtering** can calculate the mean value of the pixels around one and use the mean value as the new value of the pixel.
- **Image cropping** usually cuts out a part of the image.
- **Image rotating** is to totate an image at a certain angle.

Thus, we give the original image, the decrypted image and the image size $W \times H$; we use five metrics to evaluate the encrypted images: Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Normalized Cross-Correlation (NCC), Number of Changing Pixel Rate (NPCR), and Structure Similarity Index (SSIM).



(a) Airplane (b) Lake (c) Lena (d) Pepper

Figure 4.1 Four images with the size of 512×512 in the dataset.

In our proposed Method IV, we design the linear CNN network which requires another dataset, we used 10 color images to create the dataset for training the linear CNN network in Figure 4.2. We labeled each original image; for each image, we generated 10 images which include Gaussian noise and 10 images which contain salt-and-pepper noise as the training set. We used each original image as the labeled image; for each image, we also generated 2 images including Gaussian noise and 2 images which include salt-and-pepper noise as the validation sets. During the network training, we have two training sets, each set includes 100 images corresponding to one type of noise; we have two validation sets, each set includes 20 image.

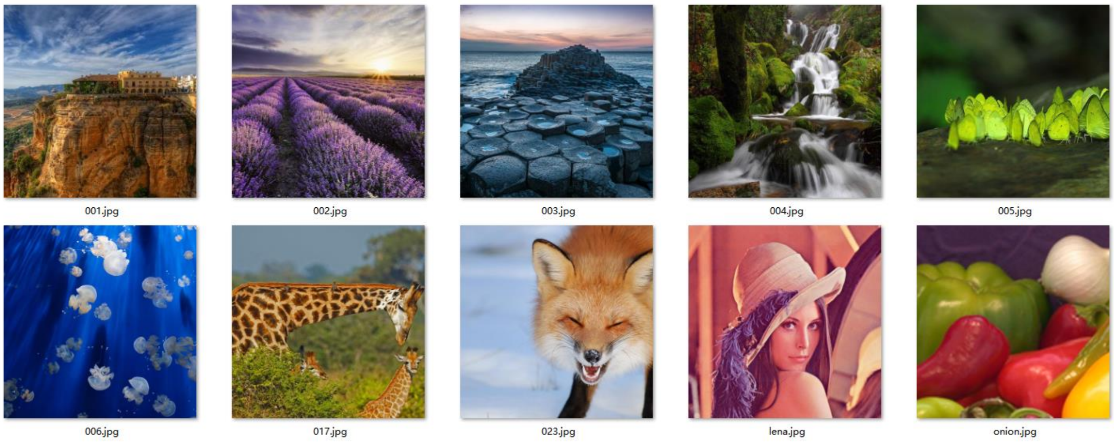


Figure 4.2 10 color images are used in the network training

The experiment is run on a laptop installed Microsoft Windows 10 Operating System using the Intel Core i7 CPU 2.30GHZ. All image encryption methods are developed and implemented in Matlab R2016a; we also use Google TensorFlow to achieve and train the linear CNN network.

4.2 Experimental Results for Each Method

4.2.1 Method I: Chaotic Scrambling Based on Logistic Map

We used Matlab to collect results and the implemented process as follows:

Step 1. Convert the original color image into greyscale one, the size of the greyscale image is $W \times H$;

Step 2. Given the logistic initial values X_0 and the parameter μ as two secret keys, after iterated the computation for $W \times H$ times, a random $W \times H$ matrix is obtained.

Step 3. Convert the image from a two-dimensional matrix into a one-dimensional sequence. We sort the result by following the way in Step 2;

Step 4. Covert the one-dimensional sequence in Step 3 back into two-dimensional image to obtain the encrypted image.

The decryption is the reverse process of its encryption. The encrypted image is transformed into one dimensional vector. Because we know the method in Step 2; if we use the right secret keys (X_0 and μ), then we will get the one-dimensional sequence of original image. Finally, we transpose this one-dimensional sequence into two-dimensional matrix, the decrypted image is obtained.

Let the logistic parameter $\mu = 3.8$ and the initial value $X_0 = 0.5$, we used four original images in the dataset to conduct our experiments. We chose image Lena to illustrate the results, the encrypted and decrypted images are shown in Figure 4.3.

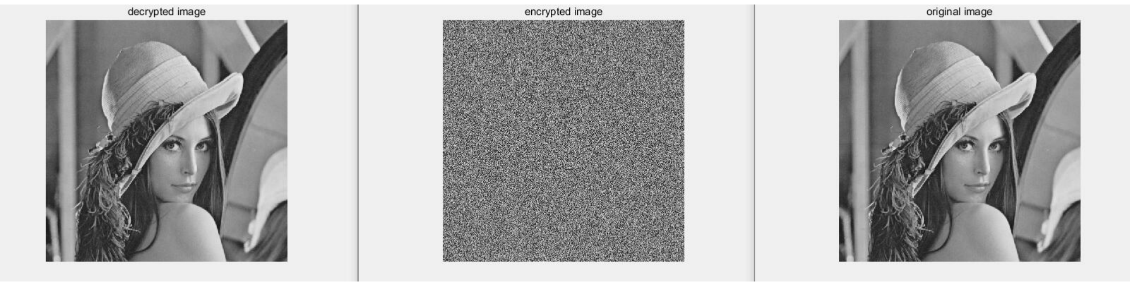


Figure 4.3 The original, encrypted and decrypted images in Method I

Based on these results, we see that the location of each pixel has been changed after logistic mapping. From the decrypted images, we see that the details of original image are perceptual. We find that all of the four results meet the expectations and the encryption method based on logistic map has satisfactory performance.

As we know, the initial value X_0 and parameter μ were used as secret keys in this method. We used original image Lena as the example to conduct the sensitivity test of secret key. Let the logistic parameter $\mu = 3.8$ and the initial value $X_0 = 0.5$, we analyze the sensitivity of secret keys. The results are as shown in Figure 4.4.

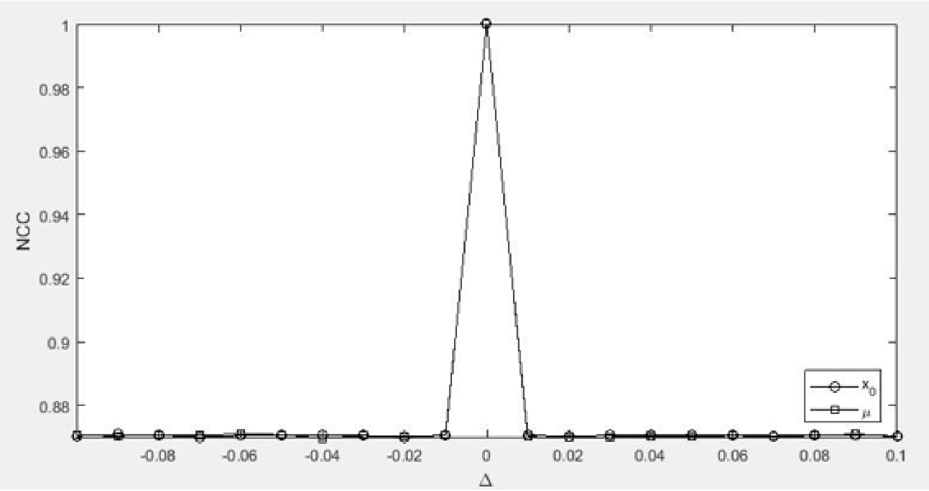


Figure 4.4 The sensitivity test of secret key for Method I

In Figure 4.4, *x*-axis shows the difference between stochastic secret key and real secret key. The Normalized Cross Correlation (NCC) between the decrypted image and the original image. The NCC is distributed in $[-1,1]$, larger the NCC, higher the similarity between two images. During the test, we fixed one secret key and slightly tuned the other. In Figure 4.5, when one of the secret keys is correct, if the other has a small deviation, the decrypted results will be different from the decrypted result. Thus, we cannot get the original one from the incorrect result. This conclusion shows the sensitivity of secret keys for chaotic scrambling algorithm based on logistic map.

We applied five attacks to all the images in the dataset, the decrypted results against each attack for each image was similar. We selected the image Lena as the sample for evaluation which is illustrated as shown in Figure 4.5.

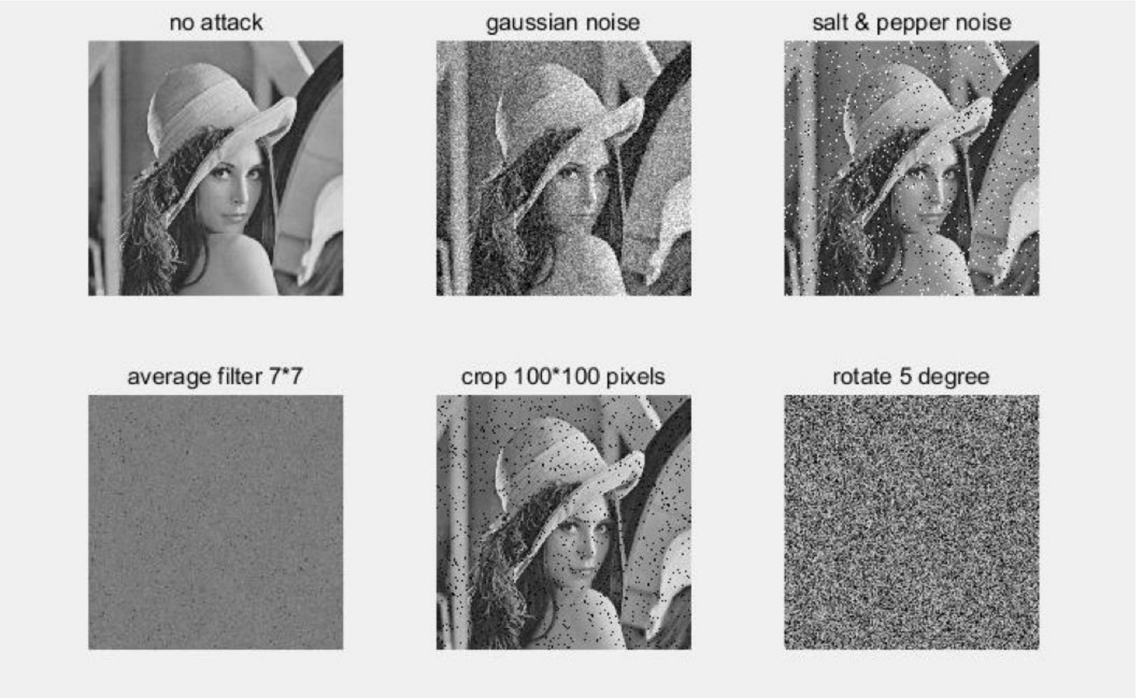


Figure 4.5 The decrypted images after attacks for Method I

4.2.2 Method II: Chaotic Map Based on DRPE by using DCT

We used DCT to replace DFT in traditional DRPE 4F system, we also used generated chaotic map to replace traditional random phase matrices, the worklow of proposed method can be illustrated as Figure 4.6. Based on Figure 4.6, the encryption process can be presented as follows:

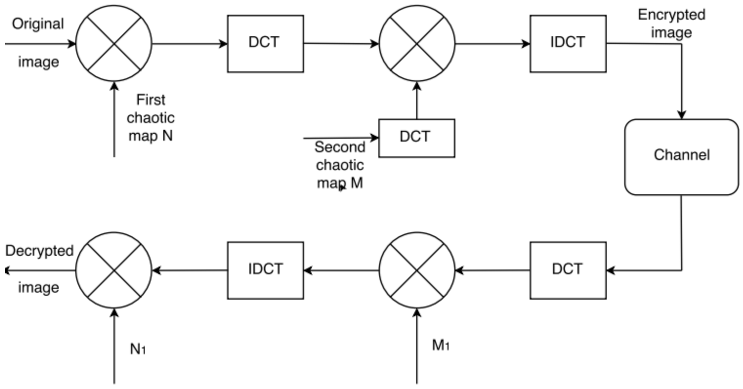


Figure 4.6 The workflow of DRPE by using DCT

Step 1. Select a set of independent random parameters (x_{01}, μ_1), where $X_{01} \in [0,1]$

and $\mu_1 \in (3.569, 4]$ are constants. We use (x_{01}, μ_1) to generate chaotic map N as the first random matrix;

Step 2. Select another set of independent random parameters (x_{02}, μ_2), where $X_{02} \in [0,1]$ and $\mu_2 \in (3.569, 4]$ are constants, we use (x_{02}, μ_2) to generate chaotic map M as the second random matrix;

Step 3. Convert the original color image **I** into greyscale one, then multiply the first chaotic map N to get $\mathbf{I}_1 = N \cdot \mathbf{I}$.

Step 4. Apply the DCT transform to the cyphertext $\mathbf{I}_1$ obtained in Step 3, then apply the DCT transform to the second chaotic map M, we get $\mathrm{DCT(M)}$.

Step 5. Multiply the cyphertext from Step 4 by using $\mathrm{DCT(M)}$ to get $\mathbf{I}_2$= DCT(M)·$\mathbf{I}_1$;

Step 6. Apply Inverse-DCT (IDCT) to $\mathbf{I}_2$ to get the encrypted image E(**I**) =IDCT($\mathbf{I}_2$) and transmit it to receivers along with the keys.

When a receiver received the keys and the encrypted image E(**I**), the image could be decrypted. The decryption is a reverse process of encryption, which is represented as following steps:

Step 1. DCT will be first applied to the encrypted image E(**I**), $\mathbf{I}'_2$=DCT(E(**I**));

Step 2. For the matrix $\mathrm{DCT(M)}$, calculate its inverse matrix and get matrix M_1=[DCT(M)]$^{-1}$, then multiply the cyphertext $\mathbf{I}'_2$ in Step 1 by M_1;

Step 3. Apply Inverse-DCT (IDCT) to the cyphertext $\mathbf{I}'_1$=IDCT($\mathbf{I}'_2 \cdot M_1$) we got from Step 2;

Step 4. For the matrix N, calculate its inverse matrix and get matrix N_1, then multiply by N_1 to get the decrypted image $\mathbf{I}' = \mathbf{I}'_1 \cdot \mathrm{N}^{-1}$

We used four original images in the dataset to verify the encryption algorithm, we chose the image Lena to generate the results in Figure 4.7. From these figures, we see that the original images and the decrypted images are different obviously. Therefore, the proposed algorithm is successful.

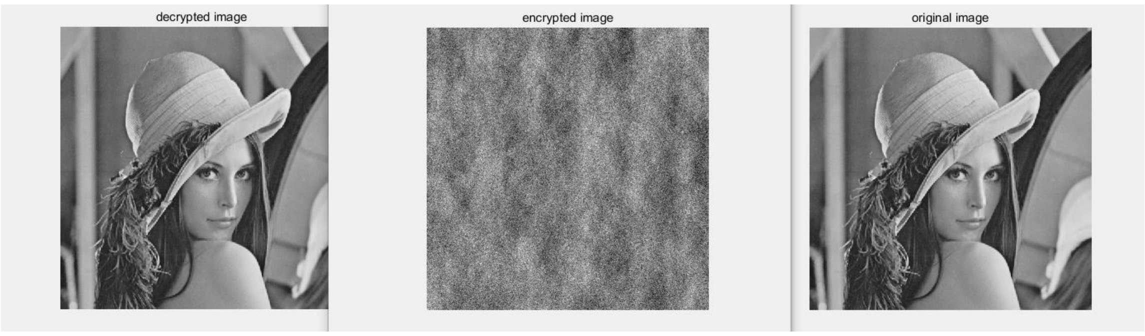
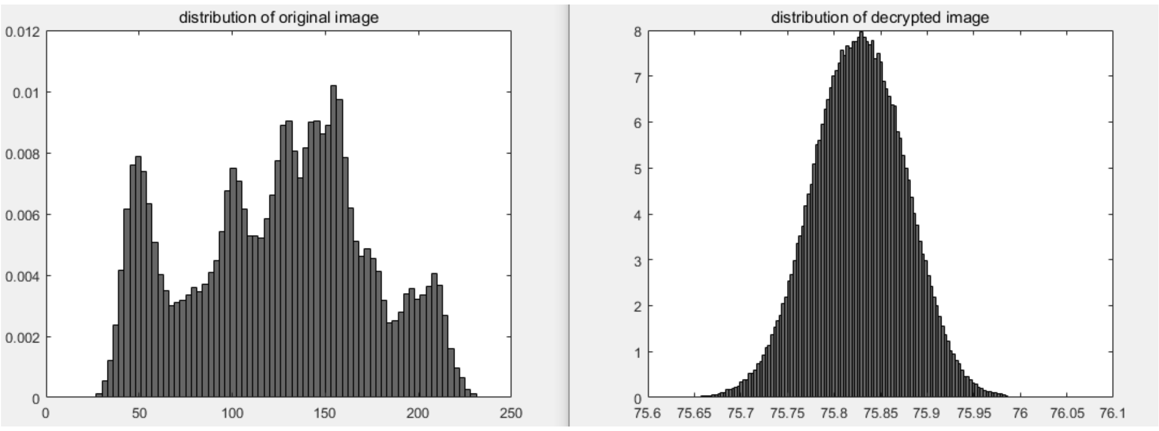


Figure 4.7 The encryption using the method II.

In our proposed algorithm, DCT is applied to encrypt the images; thus, the pixel intensity has been changed. Compared the encrypted images with the original ones, the histogram will be different significantly. We used image Lena as the example to generate the result.



(a) (b)

Figure 4.8 The histograms of the original image and its encrypted image, (a) the histogram of the original image (b) the histogram of the encrypted image.

We used different initial values and parameters to run the test, In Figure 4.8, we used $x_{01} = 0.703, x_{02} = 0.264, \mu_1 = 3.938, \mu_2 = 3.611$. With regard to the greyscale image, the histogram will be increased sharply as shown in Figure 4.8 (a). When the original image is encrypted, because the pixel intensity has been modified, the histogram will be changed correspondingly. In Figure 4.8 (b), we see that the pixels are on a normal distribution. In this case, it is difficult for an attacker to decrypt the image only by using the histogram of the encrypted image; thus, it will reduce the possibility to be decrypted through the histogram only.

As we know, (x_{01}, μ_1) and (x_{02}, μ_2) in logistic map are used as secret keys in proposed method, we let $x_{01} = x_{02} = 0.5, \mu_1 = \mu_2 = 3.8$, we analyze the sensitivity of secret keys, the results are illustrated as Figure 4.8. We also fixed 3 out of 4 secret keys, and changed the other secret keys to run the test. In Figure 4.9, we see that the decrypted result is more sensitive to secret keys x_{02} and μ_2 than secret keys x_{01} and μ_1, the deviations of x_{01} and μ_1 have limited impact on decryption, but the deviation of x_{02} and μ_2 have great impact on decryption.

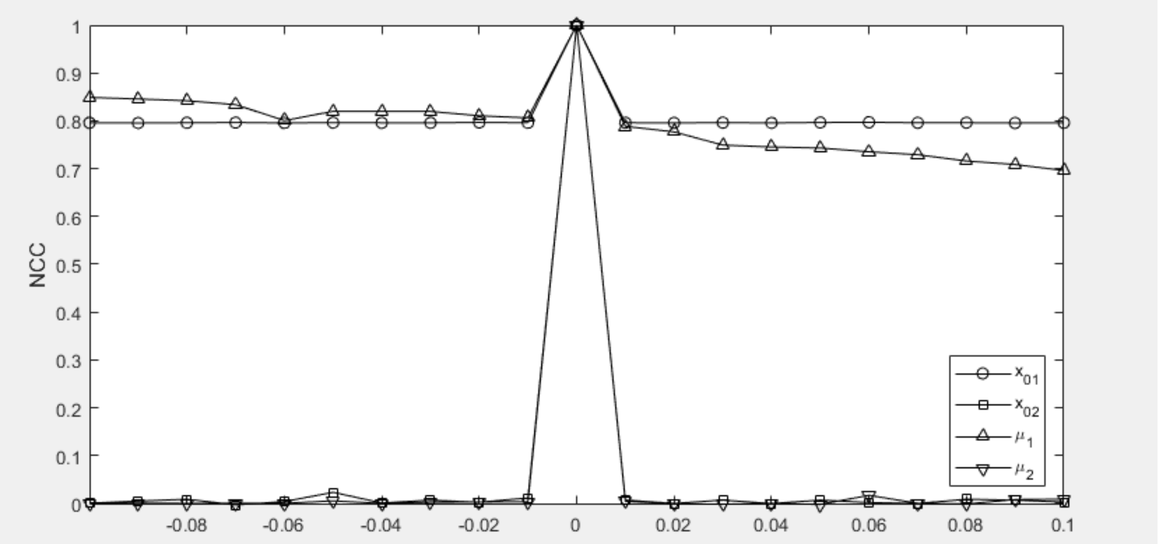


Figure 4.9 The sensitivity test of each key for Method II

We have applied five attacks to all encrypted images, the results show that all images have been decrypted unsuccessfully. We selected the image Lena as the sample for evaluation, the decrypted results after attacks can be illustrated as Figure 4.10.

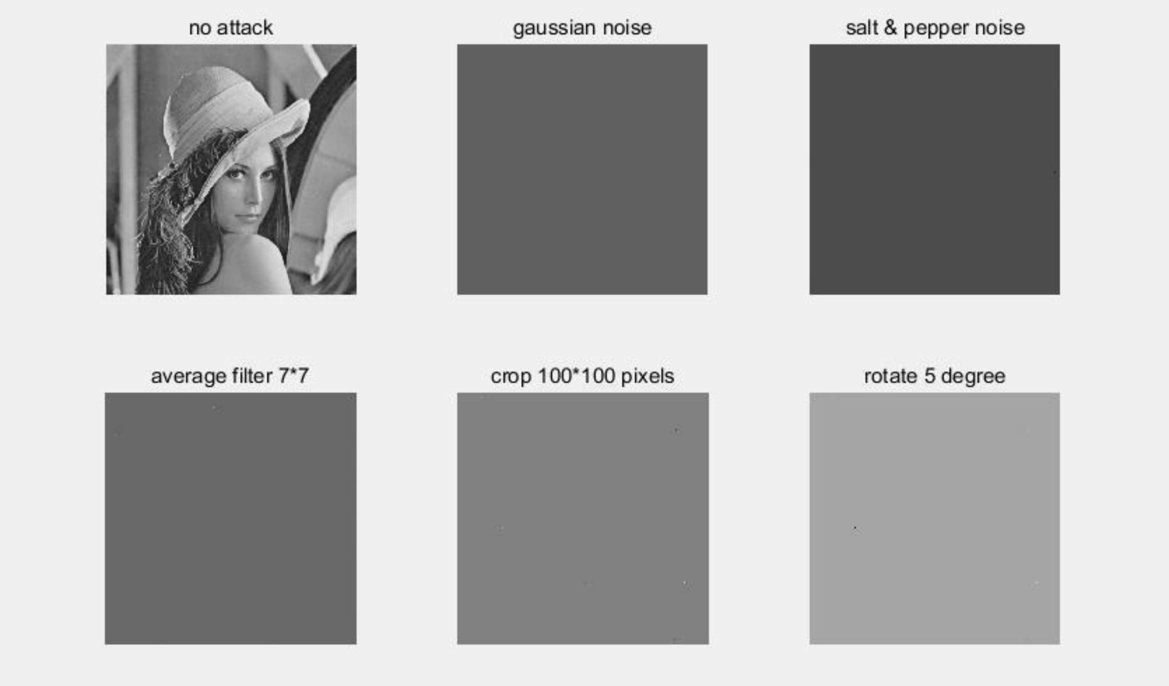


Figure 4.10 Decrypted images after attacks for Method II

4.2.3 Method III: Encryption Method Based on DWT-DCT-SVD

Based on the idea of digital watermarking technique, we design the new encryption method based on DWT-DCT-SVD framework; we have introduced the basic workflow of the designed method in Chapter 3. We will describe the specific encryption and decryption process for greyscale image encryption. The encryption workflow is illustrated in Figure 4.11. In Figure 4.11, the encryption process is presented as the following steps:

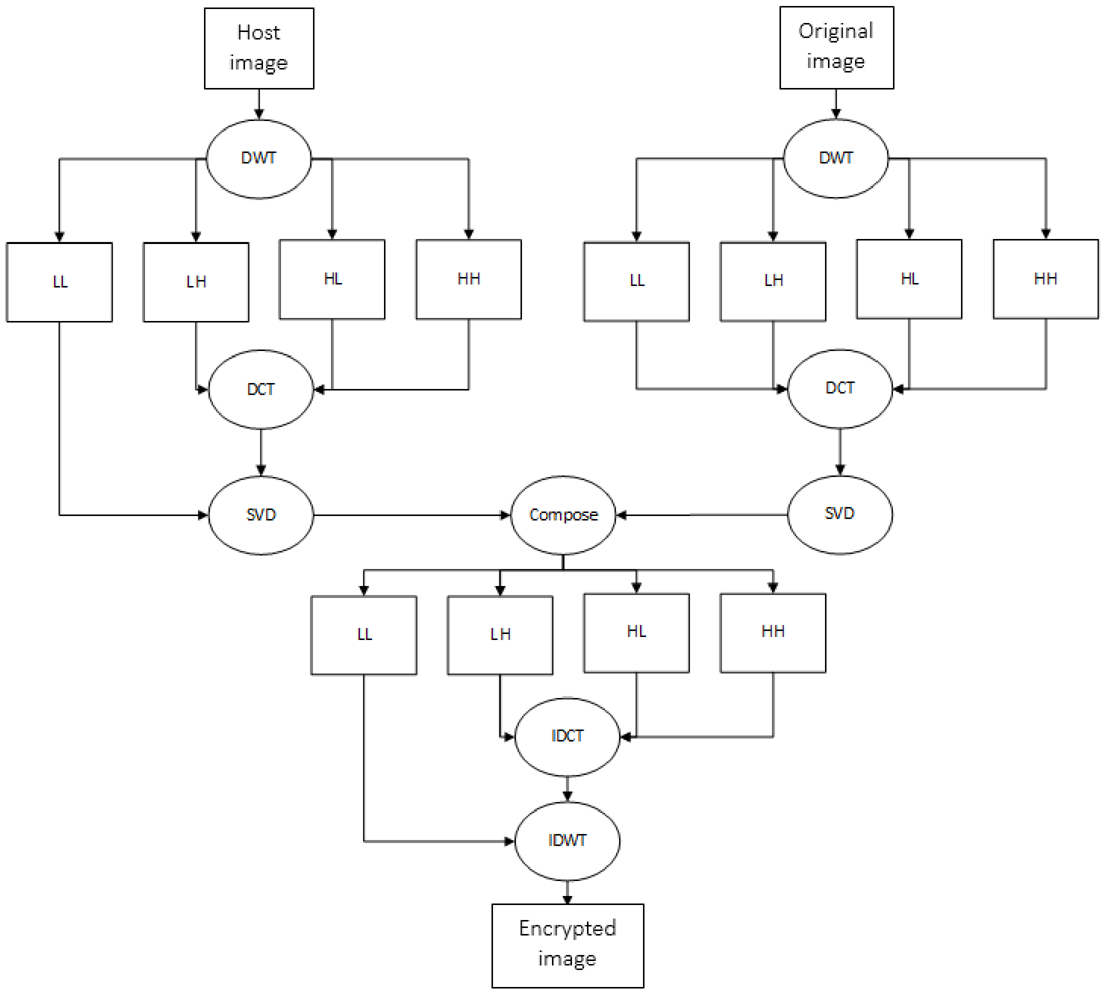


Figure 4.11 The encryption process of the proposed method

Step 1: Select the host image and original image which have the same size, then convert both images into greyscale ones;

Step 2: Apply 2D DWT to the host image, the host image is decomposed into 4 subbands LL_1, HL_1, LH_1 and HH_1;

Step 3: The DCT is applied on HL_1, LH_1 and HH_1 subbands individually, then we get $\mathrm{DCT}(HL_1)$, $\mathrm{DCT}(LH_1)$ and $\mathrm{DCT}(HH_1)$

Step 4: The SVD is applied to LL_1, $\mathrm{DCT}(HL_1)$, $\mathrm{DCT}(LH_1)$ and $\mathrm{DCT}(HH_1)$;

Step 5: Apply 2D DWT to the original image, the original image is decomposed into four subbands LL_2, HL_2, LH_2 and HH_2

Step 6: The DCT is applied to all subbands of the decomposed original image, then we get $\mathrm{DCT}(LL_2)$, $\mathrm{DCT}(HL_2)$, $\mathrm{DCT}(LH_2)$ and $\mathrm{DCT}(HH_2)$;

Step 7: After applying DCT on the four subbands of the decomposed original image, the SVD is applied to each resultant subband from Step 6;

Step 8: After applying SVD on each subband of decomposed host image and original image, we combine four subbands from Step 4 with four subbands from Step 6, the process of composition can be presented as Eq. (4.1)

$$\mathrm{DCT}(HL_1) = U_{HL_1} S_{HL_1} V_{HL_1}^T$$

$$\mathrm{DCT}(HL_2) = U_{HL_2} S_{HL_2} V_{HL_2}^T \tag{4.1}$$

$$\mathrm{DCT}(HL) = U_{HL_1} \left(S_{HL_1} + S_{HL_2}\right) V_{HL_1}^T$$

where $\mathrm{DCT}(HL)$ represents the HL subband of encrypted image, based on Eq. (3.8) we preserve U_{HL_1} and V_{HL_1} as left and right singular matrix for composed HL subband, we take S_{HL_1} from $\mathrm{DCT}(HL_1)$ and S_{HL_2} from $\mathrm{DCT}(HL_2)$, then we calculate $S_{HL_1} + S_{HL_2}$ as the singular value for HL subband of encrypted image. For other three subbands of the decomposed host and original image, we use the same method to get the composed subbands.

Step 9: Apply inverse-DCT on $\mathrm{DCT}(HL)$, $\mathrm{DCT}(LH)$ and $\mathrm{DCT}(HH)$, then apply inverse-DWT to all composed subbands and get the encrypted image.

The decryption work flow is illustrated as Figure 4.10. We use following steps to present the decryption process:

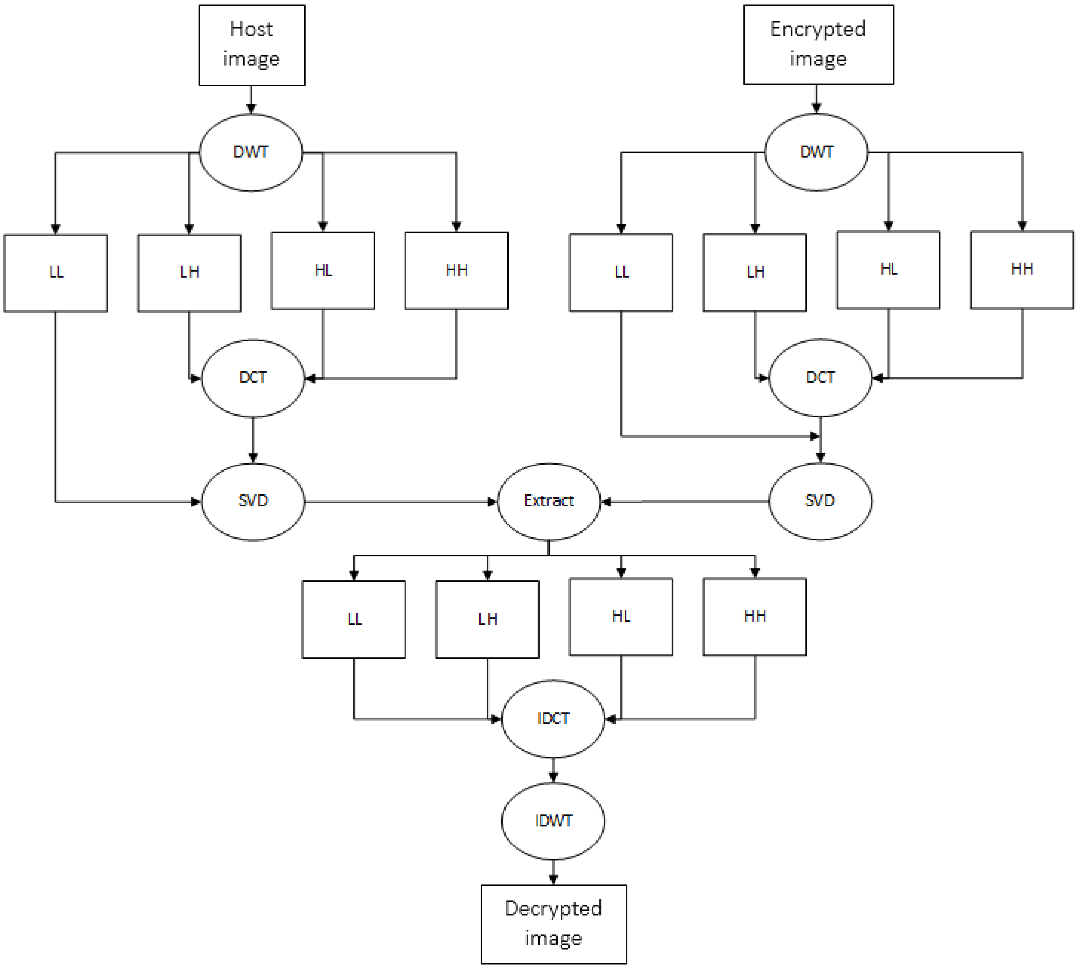


Figure 4.12 The decryption process of the proposed method

Step 1: The host image is decomposed into four subbands LL_1, HL_1, LH_1 and HH_1 by using DWT;

Step 2: The DCT is applied to HL_1, LH_1 and HH_1 subbands individually, then we get $\mathrm{DCT}(HL_1)$, $\mathrm{DCT}(LH_1)$ and $\mathrm{DCT}(HH_1)$

Step 3: The SVD is applied to LL_1, $\mathrm{DCT}(HL_1)$, $\mathrm{DCT}(LH_1)$ and $\mathrm{DCT}(HH_1)$;

Step 4: Apply 2D DWT to the encrypted image, the encrypted image is decomposed into 4 subbands LL, HL, LH and HH.

Step 5: The DCT is applied to HL, LH and HH, then we get $\mathrm{DCT}(HL)$, $\mathrm{DCT}(LH)$ and $\mathrm{DCT}(HH)$.

Step 6: After apply DCT to HL_1, LH_1 and HH_1, the SVD is applied to LL, $\mathrm{DCT}(HL)$, $\mathrm{DCT}(LH)$ and $\mathrm{DCT}(HH)$.

Step 7: We use $\mathrm{DCT}(HL)$ and $\mathrm{DCT}(HL_1)$ in Eq. (4.2) to illustrate the process of extracting subbands of original image, then these subbands are used to get the decrypted image

$$\mathrm{DCT}(HL) = U_{HL}S_{HL}V_{HL}^{T}$$

$$\mathrm{DCT}(HL_1) = U_{HL_1}S_{HL_1}V_{HL_1}^{T} \tag{4.2}$$

$$\mathrm{DCT}(HL_3) = U_{HL_2}\left(S_{HL} - S_{HL_1}\right)V_{HL_2}^{T}$$

where $\mathrm{DCT}(HL_3)$ represents the HL subband of decrypted image, U_{HL_2} and V_{HL_2} are left and right singular matrices of the HL subband of decomposed original image. Based on Eq. (4.2), we take S_{HL} from $\mathrm{DCT}(HL)$ and S_{HL_1} from $\mathrm{DCT}(HL_1)$, then we calculate $S_{HL} - S_{HL_1}$ as singular value of the HL subband of decrypted image. Therefore, we see four singular values which correspond to 4 subbands of decomposed host image are required, the host image is used as a secret key, we get these four singular values in Step 6.We also see that U_{HL_2} and V_{HL_2} are required to extract HL subband of decrypted image, they are two secret keys of the decryption process in order to extract all subbands of decrypted image. We need eight singular matrices as secret keys corresponding to 4 subbands of decomposed original image.

Step 8: Apply inverse DCT on all subbands of decrypted image, then apply inverse DWT on these 4 subbands and get the decrypted image.

We used four secret images in the dataset to test our method and we chose the image Lena to illustrate the results. The encrypted and decrypted images are shown in Figure 4.13. Based on the results, we clearly see that the encrypted image is similar to the host image. In other words, the information of secret image has been hidden successfully in the encrypted image. From the decrypted images, we see that the details of secret image are clearly visible. We find that all of the four results meet the expectations and the encryption method based on DWT-DCT-SVD framework has satisfactory performance.

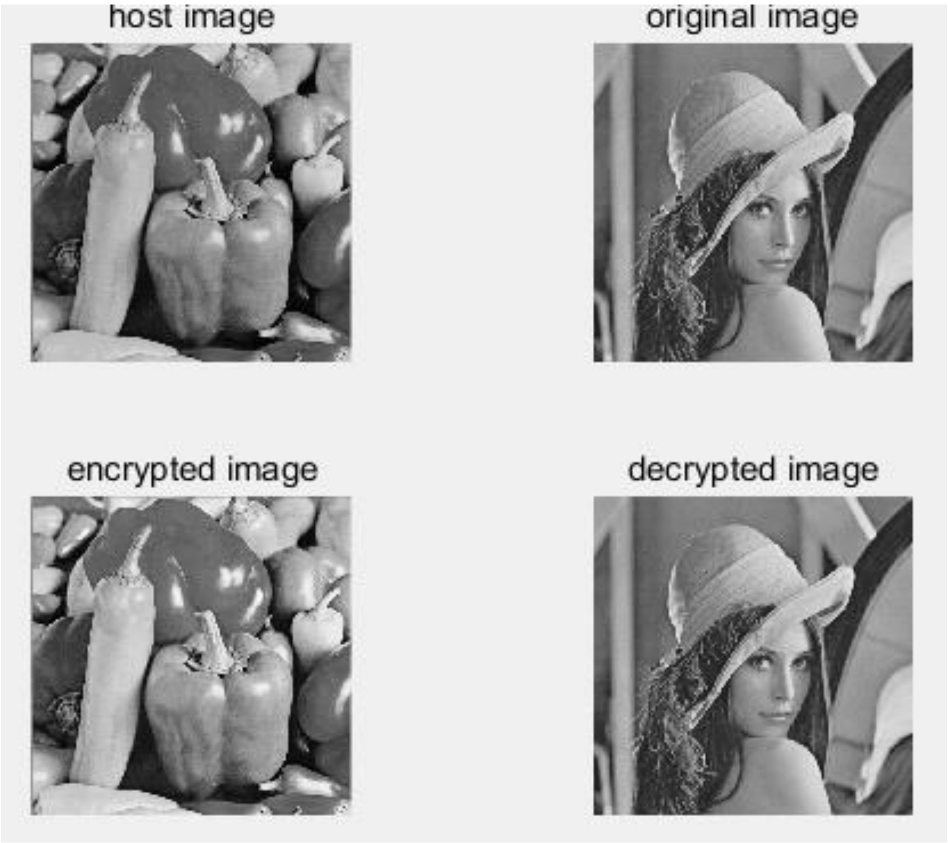
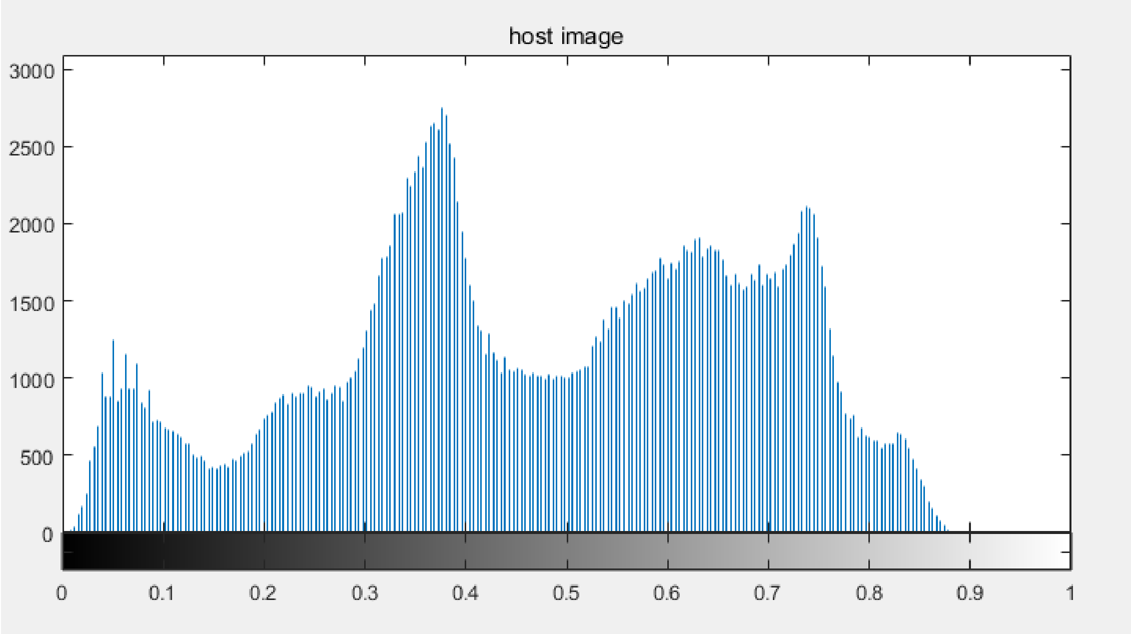
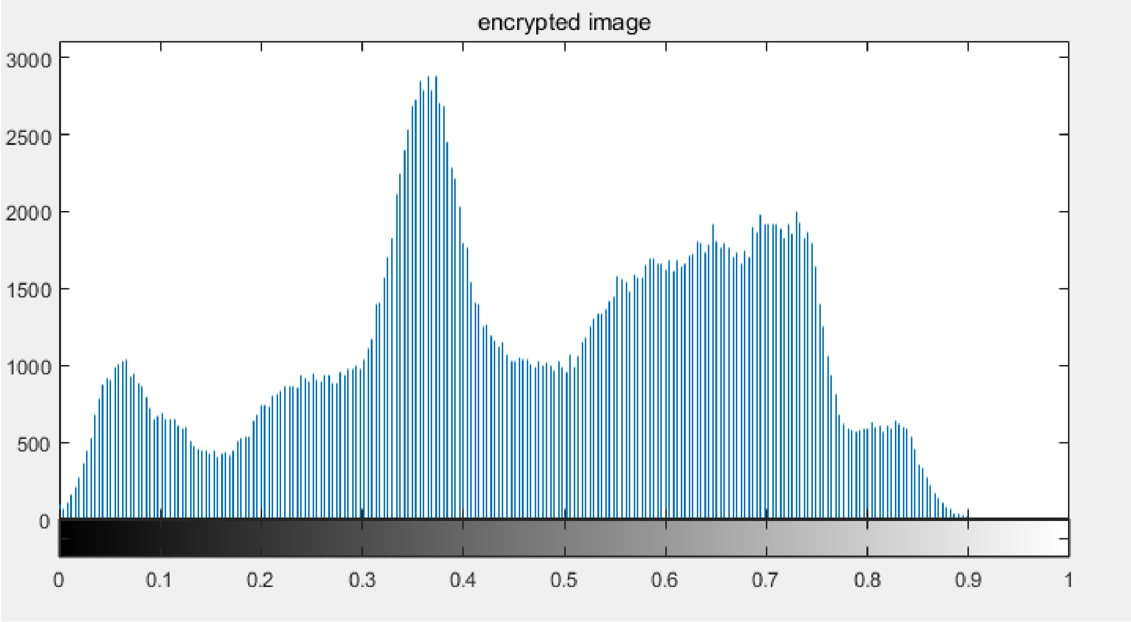


Figure 4.13 The results by using normal image as host image

Figure 4.14 illustrates the histograms between a host image and its encrypted image. From Figure 4.14, we see that the pixel distributions are similar between the host image and its encrypted image. We also calculated the MSE of these two images so as to measure the similarity and the MSE value is only 0.00067. Based on the histograms and MSE value, we summarize that the secret image has been uniformly encrypted into the host image.



(a) Pixels distribution of host image



(b) Pixels distribution of encrypted image

Figure4.14 The pixel distribution of host and encrypted images

Let’s focus on the histogram of the encrypted image. The pixel intensities are usually distributed randomly; but as the encrypted image is very similar to the host image, if attackers use exhaustive method to attack the encrypted image based on the histogram, the results they get will be only about the host image so that the secret image is protected. Therefore, the statistical attack is completely ineffective.

We applied five attacks to all the images in the dataset. The decrypted results against each attack for each image were similar. We selected the results for image Lena as an example, the decrypted results are illustrated in Figure 4.15. For the attack methods image rotation and image cropping, the decrypted image holds not only the overview outline of the original image but also the details, properly showing high similarity between the decrypted image and its original image. For the attack method using average filtering, it shows lower similarity between the decrypted image and secret image. The decrypted image after attack holds the overview outline of secret image, but the details in the decrypted image are blurred compared with the secret image. For the attack methods Gaussian noising and salt-and-pepper noising, the lowest similarity exists between the decrypted image and the secret image. The decrypted images show blurred details related to the secret image.

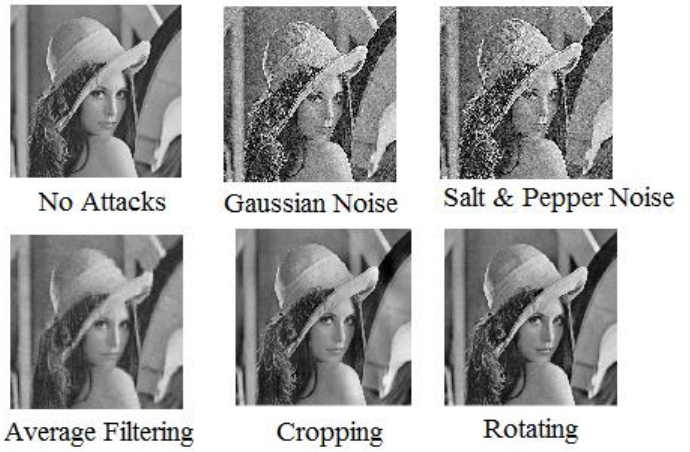
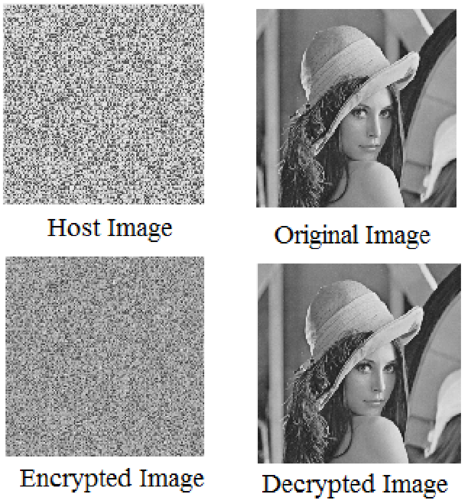


Figure 4.15 The decrypted images after attacks by using normal image as host image

Our proposed method requires the host image should be the secret key which is too large and inconvenient for transmission. As an improvement, we use the logistic map to generate the random image as the host image. The initial value x_0, parameter μ to generate the random image can be utilized as secret keys, reducing the key size. For this method, we need 11 secret keys which are the initial value x_0, parameter μ, 8 singular matrices of the decomposed secret image as well as the selection of the wavelet basis function. We used the same four original images in the dataset to verify the encryption algorithm and we chose the image Lena as shown in Figure 4.16. From these figures, we see that the encrypted image is obviously similar to the host image and the decrypted image resembles the information of original image clearly. Therefore, the improved algorithm is successful.



Host Image

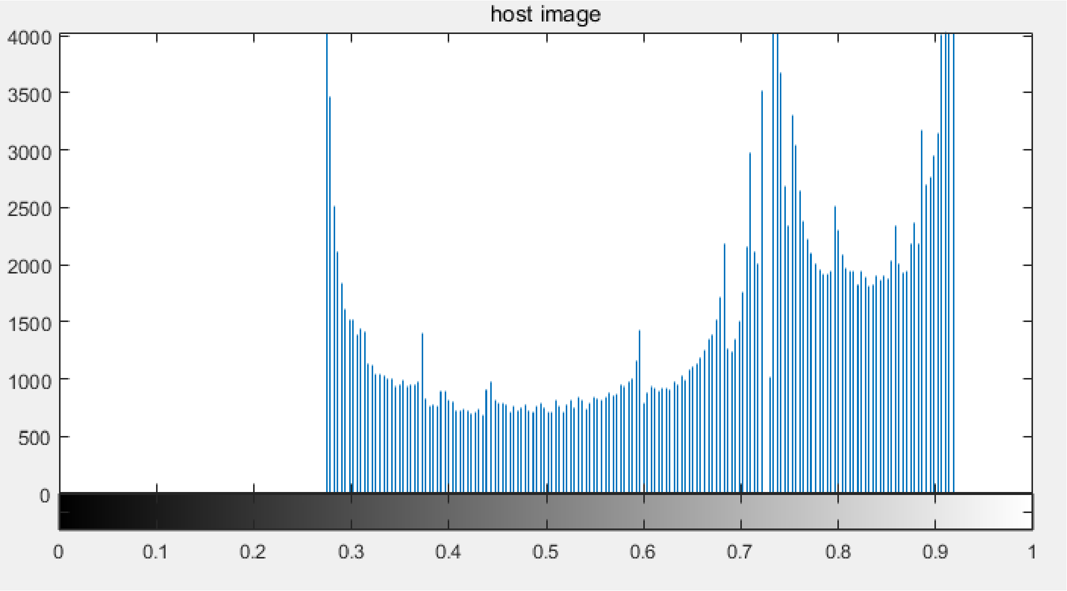
Original Image

Encrypted Image

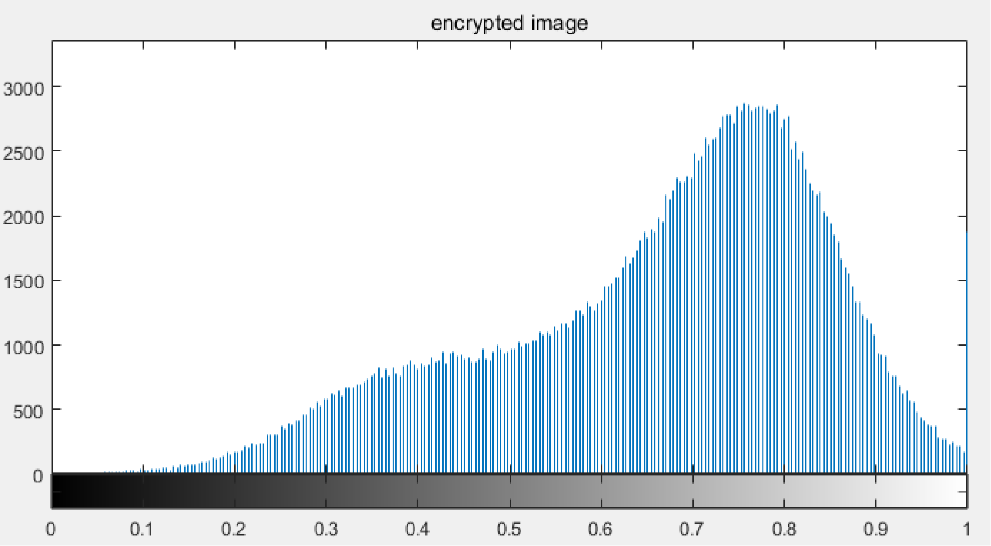
Decrypted Image

Figure 4.16 The results by using random image as host image

Figure 4.17 (a) and Figure 4.17 (b) are the histograms for the original and encrypted images respectively. We see that the pixel distribution in the host image is a random distribution whereas it is a normal distribution in the encrypted image. This means that it is difficult for an attacker to get the encrypted image by using only the histogram of the encrypted image, thus resisting statistical attacks.



(a) Pixel distribution of the host image



(b) Pixels distribution of the encrypted image

Figure4.17 Pixel distribution of the host and encrypted images

We applied five attacks to all the images in the dataset, the decrypted results against five attacks for each image were similar as illustrated using the image Lena. We selected the image Lena as the sample for evaluation which is illustrated as shown in Figure 4.18. For noise attacks, the decrypted images after an attack hold not only the overview outline of the original image but also the details, properly show high similarity between decrypted image and original image. For image cropping and image rotating, the overview outline and details of decrypted images are also statisfied. For the average filtering attack method, it shows the lowest similarity between decrypted image and original image; the decrypted image after attack only holds the blurred outline of original image and it is hard to recognize the original image details in the decrypted image.

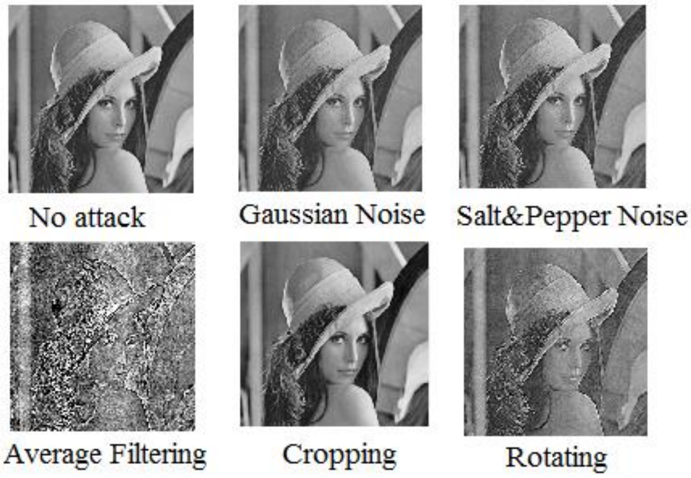


Figure 4.18 The decrypted images after attacks by using random image as the host

4.2.4 Encryption Method Based on DWT-DCT-SVD by Using Denoising Methods

Based on the designed DWT-DCT-SVD encryption method by using normal image as the host image, we use denoising methods before image decryption to further improve the anti-attack ability of this method against the noise attacks. The new workflow is illustrated as Figure 4.19.

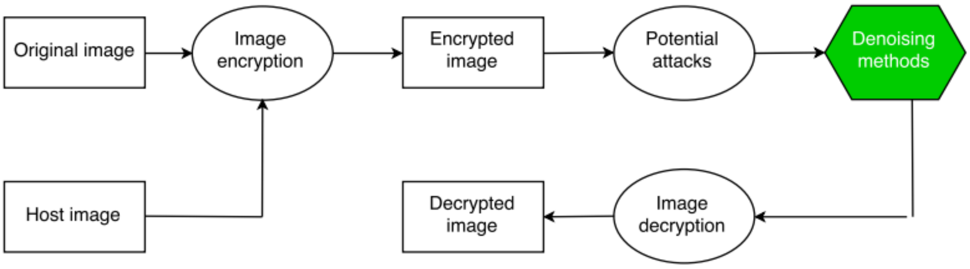


Figure 4.19 The encryption and decryption work flow using denoising methods

Based on Figure 4.19, the encryption and decryption process can be presented as following steps:

Step 1: Select the host image and the original image which have the same size;

Step 2: We applied DWT to the both image firstly and got four subbands for each image; after applying DCT on subbands, we applied SVD to each subband and composed the coincident subbands towards the host image and original image; then, we applied inverse-DWT and inverse-DCT to get the encrypted image, this whole process can be treated as DWT-DCT-SVD encryption process;

Step 3: During the transmission of encrypted image, it may be attacked by noising attacks; we use traditional denoising methods or linear CNN model-based method to filter the attacked encrypted image;

Step 4: The encrypted image will be decrypted and the decrypted process is treated as the inverse process of encryption; then, we got the decrypted image.

In order to get the better denoising results, we need to figure out which traditional method has the best performance for denoising Gaussian noise and salt-and-pepper noise. During the experiments, we added Gaussian noise and salt-and-pepper noise to all sample images in the datasets; for each image, we generated 20 noise images regard to Gaussian noise and 20 noise images regard to salt-and-pepper noise, respectively. Then, three traditional denoising methods were used to remove two kinds of image noises, respectively; eventually, the MSE will be calculated. Ater experiment, we found the results are similar, we chose image Lena as representative to demonstrate the results as shown in Figure 4.20.

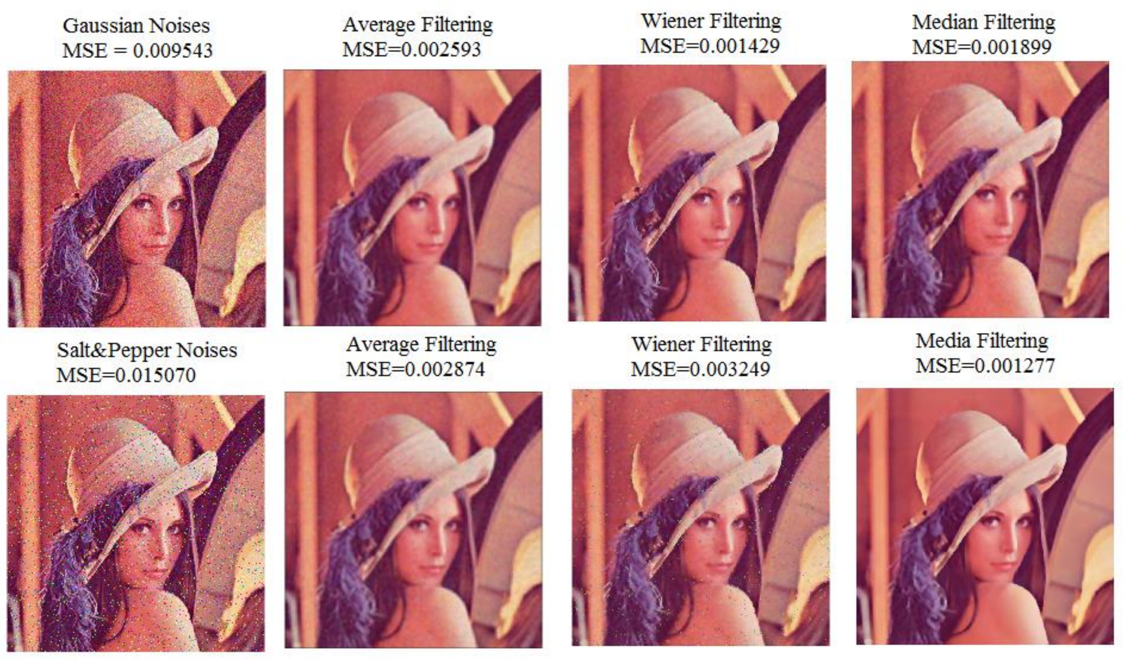


Figure 4.20 Three filtering methods for Gaussian noise and salt-and-pepper noise

In Figure 4.20, we see that Wiener filter for removing Gaussian noise has the lowest MSE. The denoised image is the most similar one to the original image; for salt-and-pepper noise, median filtering has the best performance. These results reflect the general situation of the whole experiment; in image denoising, we apply Wiener filtering to remove Gaussian noise and median filtering to salt-and-pepper noise.

We first use DWT-DCT-SVD method to encrypt and decrypt images without filtering, we apply five attacks to all the images in the dataset, the performance of decrypted results against each attack for each image was similar. We selected the results for image Lena as the example which can be illustrated as Figure 4.21. From Figure 4.21, we see that for attack methods Gaussian noise and salt-and-pepper noise, the decrypted images show blurred overview outline and details with regard to the original image.

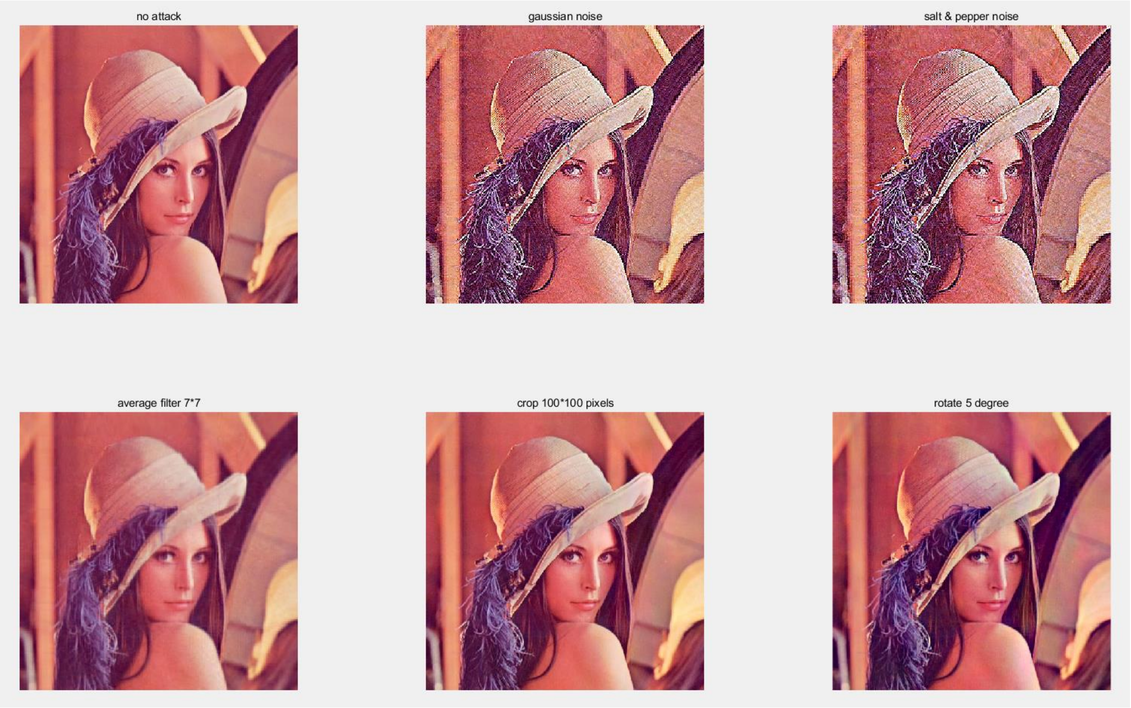


Figure 4.21 Decrypted results based on DWT-DCT-SVD without filtering

We apply filtering operation on the attacked image, the corresponding decrypted results is illustrated as Figure 4.22. From Figure 4.22, we see that for the decrypted image pertaining to two noise attacks, its outline of the original image and details is perceptible clearly.

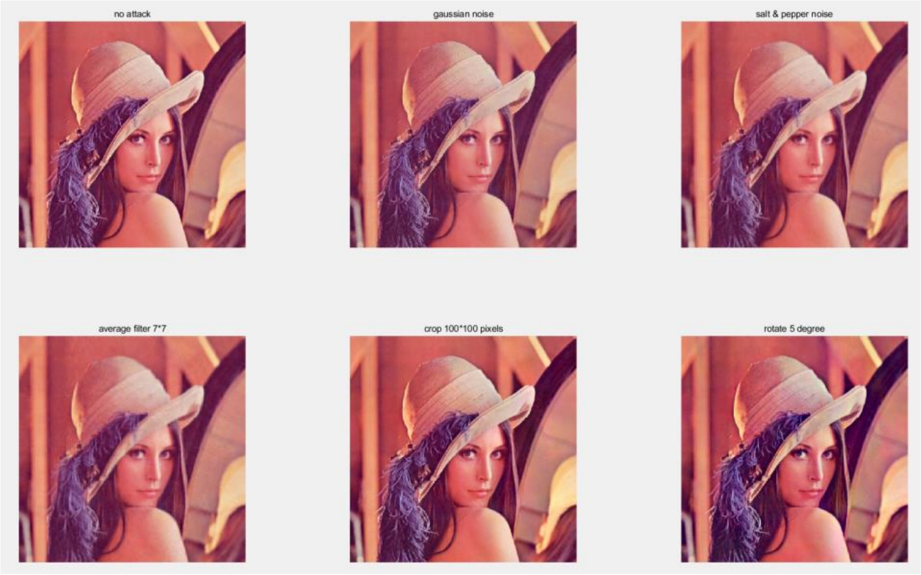


Figure 4.22 Decrypted results by using traditional filtering methods

From the decrypted results, we see that the traditional denoising method is achieved. Now, let’s focus on the image denoising by using designed linear CNN network. For the training set with Gaussian noise, we train it by using the proposed linear CNN network for 5000 epochs of 100 training images and get the linear CNN model I; the number of total training steps is 10000. The result is illustrated in Figure 4.23. The x-axis shows the number of training steps and y-axis indicates MSE. In our experiment, the batch size is 50, which means, we trained 50 images for each step, calculated the MSE values between 50 trained images and their corresponding original images and obtained the mean of 50 MSE values in Figure 4.23. In Figure 4.23, we see that the MSE values have been converged within 1000 training steps and all MSE values are lower than 1.23×10^{-3}, which means the linear CNN model I has satisfactory performance for filtering Gaussian noise. For all training steps, we also calculated the mean of MSE for both training set and validation set, the results show that the MSE of training set is very close to the MSE of the validation set; in other words, the linear CNN model I has high feasibility and reliability.

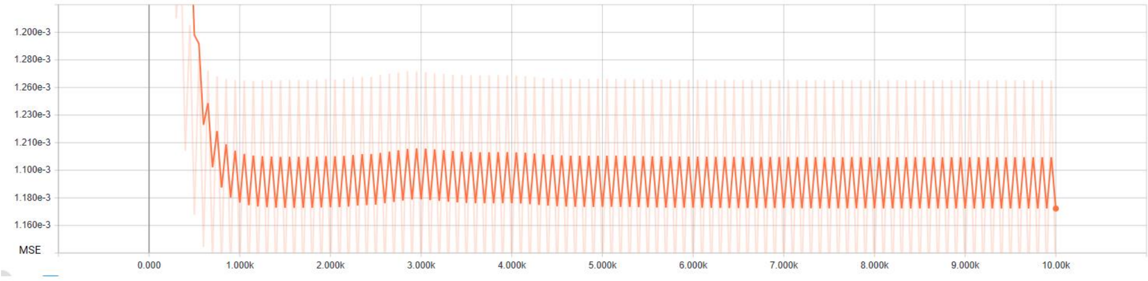


Figure 4.23 Results of network training for removing Gaussian noise

For the training set with salt-and-pepper noise, we also trained it by using the proposed linear CNN network for 5000 epochs of 100 training images and obtained the linear CNN model II, the results are shown in Figure 4.24. We see that the MSE values have been converged within 1000 training steps and all MSE values are lower than 1.71×10^{-3} which reflects that the linear CNN model II has satisfactory performance for filtering salt-and-pepper noise as well.

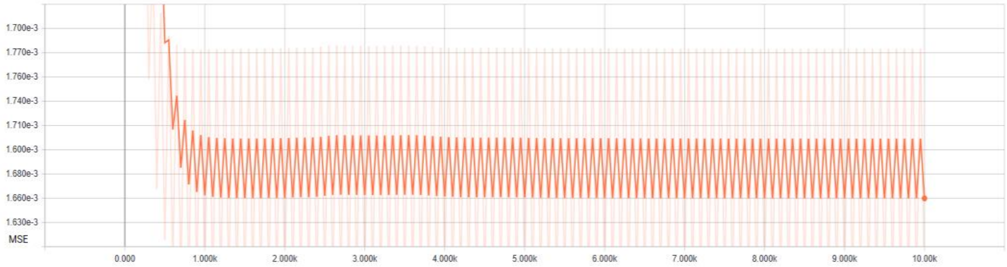


Figure 4.24 Results of network training for removing salt-and-pepper noise

We applied the linear CNN model I to filter Gaussian noise and model II to filter salt-and-pepper noise, the corresponding results are shown in Figure 4.25. From Figure 4.25, we see that with regard to two noise attacks, the outline and details of the original image are much clearly compared to the decrypted image.

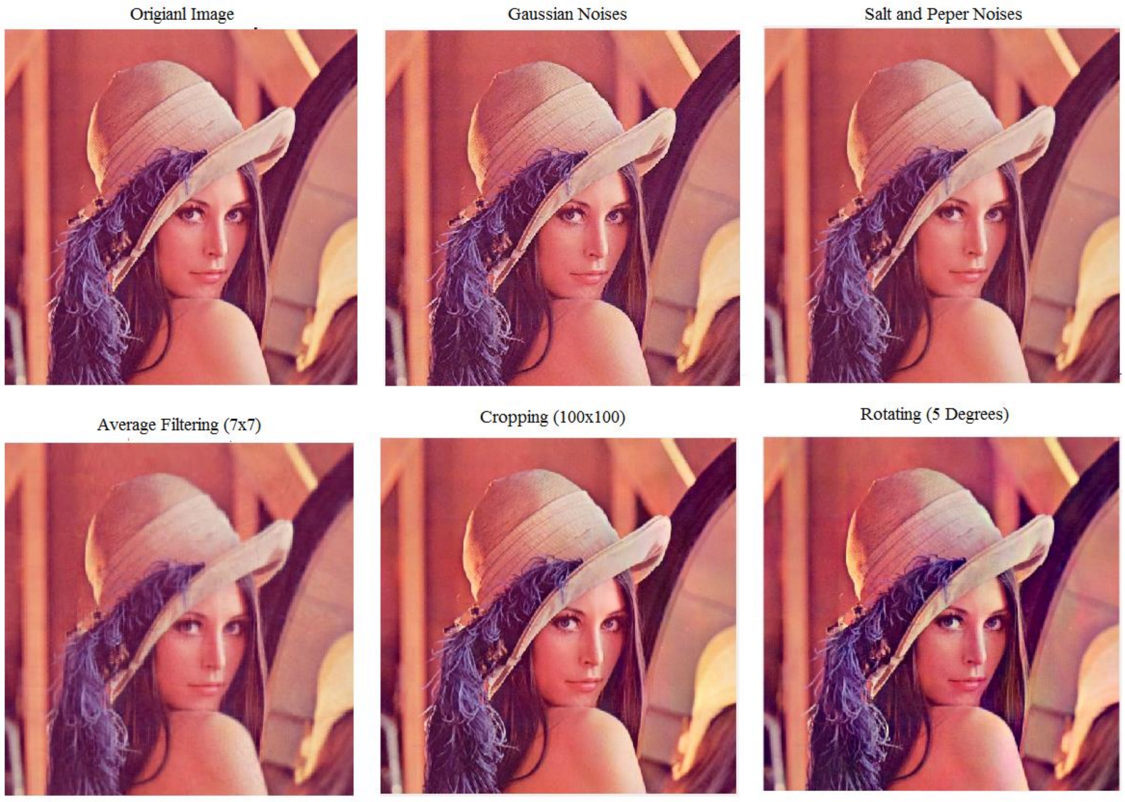


Figure 4.25 Decrypted results by using linear CNN models

4.3 Limitations of the Research

All of the proposed image encryption algorithms have been implemented successfully in this thesis. However, there are still some limitations that should be improved in future. The limitations may include:

(1) Because the secret keys of proposed Method III contain important and sensitive information, left and right singular metrics of original image, etc. We should consider about security issue during transmission secret keys.

(2) In order to test the performance of proposed encryption methods, we only applied five types of attack methods to the encrypted images, more attack methods should be taken into consideration so that the analytics of the robustness of the proposed methods will be more comprehensive.

(3) Four images were used as the dataset for image encryption in this research project, in future we will take more sample images into consideration.

4.4 Summary

In this section, we provided the specific experimental steps and collected the results for each method. In general, all of the proposed methods can encrypt and decrypt images successful, we also applied five types of attacks to all the images in the dataset, and the decrypted results for each method are different. In detail, for the Method I, the decrypted image holds the overview outline for attack methods: Gaussian noising, salt-and-pepper noising and image cropping; for the attack methods: image rotation and average filter, the decyption was failed. For the Method II, all images have been decrypted unsuccessful. For Method III, we have designed two methods based on DWT-DCT-SVD; for the first one which uses a normal image as the host image, the decrypted image not only holds the overview outline but also the details for the attack methods: image cropping, image rotating and average filtering; for the second method which uses a random image as the host image, the decrypted images are clear for the attack methods Gaussian noise, salt-and-pepper noise and image cropping; for the attack methods: average filtering, it shows the lowest similarity between the decrypted image and the original image. For the method IV, we designed two schemes based on DWT-DCT-SVD, one of them uses traditional filters and the other uses linear CNN model. The results for both of sechems are satisfied, the decrypted images not only hold the overall outline but also the details for all attack methods.

Chapter 5

Analysis and Discussions

In this chapter, the discussion and result analysis with respect to the outcomes of these experiments are clearly demonstrated and presented. More specifically, comparisons regarding to performance of all proposed image encryption methods will be reviewed in this chapter. Finally, the significance will be also stated through analyzing the outcomes.

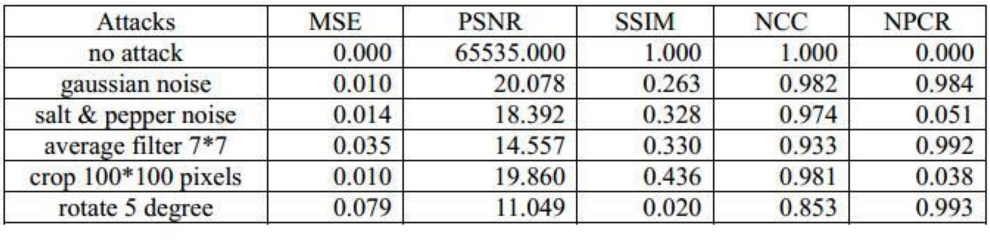
5.1 Analysis for Method I, Method II and Method III

We have introduced the direct results of each encryption method by utilizing MATLAB as stated in the previous chapter. In this chapter, the result analysis will be detailed with the specific performance metrices. In this section, the analysis for the first three encryption methods will be given.

5.1.1 Analysis for Method I

We applied five attacks to all the images in the dataset; the performance of specific metrics against each attack for each image is similar. We selected the results for image Lena as the example for our analysis in Table 5.1. The attack methods using average filtering and image rotating show the lower similarity between the decrypted image and its original image. Compared with the other three attack methods, the results show that the chaotic scrambling method is able to resist Gaussian noise, salt-and-pepper noise and image cropping. The reason is that these three methods only change a part of pixels in the encrypted image. As for the attack methods using average filter and image rotation, they modify all of the pixels in the encrypted pixels; the chaotic scrambling method cannot resist such intensive attacks.

Table 5.1 Image metrics for chaotic scrambling



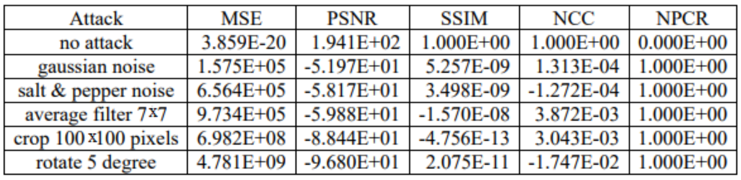
Attacks	MSE	PSNR	SSIM	NCC	NPCR
no attack	0.000	65535.000	1.000	1.000	0.000
gaussian noise	0.010	20.078	0.263	0.982	0.984
salt & pepper noise	0.014	18.392	0.328	0.974	0.051
average filter 7*7	0.035	14.557	0.330	0.933	0.992
crop 100*100 pixels	0.010	19.860	0.436	0.981	0.038
rotate 5 degree	0.079	11.049	0.020	0.853	0.993

Utilizing the scrambling method based on logistic map, we generated a chaotic sequence which contains the same number of pixels as the original image. Then, we used this sequence to scramble the image. This method can resist noise attack and image cropping attack, but it cannot resist intensive attacks (average filtering and image rotating); meanwhile, the sensitivity of the secret keys for this method is high so that the security level is improved. However, this method requires a large amount of calculations, the processing time is longer, the logistic map only changes the location of each pixel, and the encrypted image does not modify the pixel distribution compared with the original image. Therefore, this method cannot resist statistical attack.

5.1.2 Analysis for Method II

As we have introduced in Chapter 4, we have applied five attacks to all the encrypted image and the results show that the attacks led to all images being decrypted unsuccessfully. We selected the image Lena as the sample for evaluation and the results are shown in Table 5.2. The results for other images are similar to the results for image Lena. Compared with the results from the chaotic scrambling method, the DCT-based method cannot resist the tampering from image cropping, average filtering, or image rotating. This means that the proposed method is much more robust to attacks. Even if we change a few pixels in the encrypted image, the decryption still fails. Based on this, we easily verify whether an image has suffered attacks or not.

Table 5.2 Specific metrics for DCT based encryption



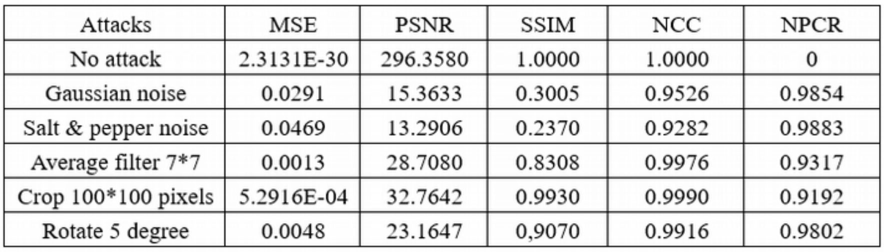
Attack	MSE	PSNR	SSIM	NCC	NPCR
no attack	3.859E-20	1.941E+02	1.000E+00	1.000E+00	0.000E+00
gaussian noise	1.575E+05	-5.197E+01	5.257E-09	1.313E-04	1.000E+00
salt & pepper noise	6.564E+05	-5.817E+01	3.498E-09	-1.272E-04	1.000E+00
average filter 7x7	9.734E+05	-5.988E+01	-1.570E-08	3.872E-03	1.000E+00
crop 100x100 pixels	6.982E+08	-8.844E+01	-4.756E-13	3.043E-03	1.000E+00
rotate 5 degree	4.781E+09	-9.680E+01	2.075E-11	-1.747E-02	1.000E+00

Our encryption method is based on a previous method using traditional double random phase encoding and the 4F method. In order to facilitate the whole process, we replace the traditional DFT with DCT to avoid complex operations; we also substitute the traditional random phase matrices with chaotic maps. Two sets of initial values and parameters were used as secret keys so that the amount of secret keys is decreased. With regard to secret key sensitivity test, the sensitivity for this method is high, the security level has been improved. With regard to anti-attack ability, because this method changed the intensity of each pixel, the pixel distribution became modified correspondingly. Based on the histogram of this encrypted image, we see that it follows the normal distribution and the method can resist statistical attack; thus, the security level is high. On the other hand, we applied five attacks to this method and the decryption resulted in failure.

5.1.3 Analysis for Method III

We applied five attacks to all the images in the dataset. Because the proposed DWT-DCT-SVD method is able to be used for both greyscale image encryption and color image encryption, for the convenience of results comparison in next section, we will talk about the performance for the greyscale image encryption. We found that the performance of specific metrics against five attacks for each image was similar by using the image Lena. We selected the image Lena as the sample for evaluation and the specific metrics are given in Table 5.3.

Table 5.3 Specific metrics for Method III which uses normal image as the host image



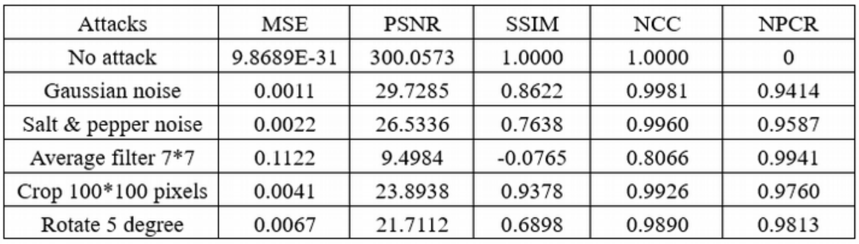
Attacks	MSE	PSNR	SSIM	NCC	NPCR
No attack	2.3131E-30	296.3580	1.0000	1.0000	0
Gaussian noise	0.0291	15.3633	0.3005	0.9526	0.9854
Salt & pepper noise	0.0469	13.2906	0.2370	0.9282	0.9883
Average filter 7*7	0.0013	28.7080	0.8308	0.9976	0.9317
Crop 100*100 pixels	5.2916E-04	32.7642	0.9930	0.9990	0.9192
Rotate 5 degree	0.0048	23.1647	0,9070	0.9916	0.9802

Based on Table 5.3, for attack methods using average filter, image cropping and image rotating, the results are similar; especially for image cropping, the decrypted image shows the highest PSNR, SSIM and NCC and lowest MSE and NPCR; for the attack method image rotating and average filtering, the specific values of MSE and NPCR are little higher than the values for image cropping, the values of PSNR, SSIM and NCC are lower than the values for image cropping, which means the encryption method based on DWT-DCT-SVD is able to resist these three attacks effectively, especially for resisting image cropping. For the attack methods Gaussian noise and salt-and-pepper noise, the decrypted results show the highest MSE and NPCR as well as the lowest SSIM, NCC and PSNR value, especially for SSIM values. After these two noise attacks, the SSIM values are lower than 0.5, which means the proposed DWT-DCT-SVD method cannot resist noise attacks properly.

Based on the workflow, we proposed an encryption method by using DWT-DCT-SVD framework. We selected a host image and a secret image which have the same size; we applied DWT to the both image first and got four subbands for each image. After applying DCT to the subbands, we applied SVD to each subband and composed the coincident subbands towards the host image and secret image; then, we applied inverse DWT(IDWT) and inverse DCT(IDCT) to get the encrypted image, the decrypted process could be treated as the inverse process of encryption. Our method can hide the secret image into the host image so as to obtain the encrypted image. After decryption, the secret image can be obtained. The method resists intensive attacks (average filtering and image rotating) and image cropping, but the performance of this method is not satisfactory against noise attacks. Because the secret image is hidden properly into the host image, the exhaustive method may only obtain information about the host image. Therefore, our encryption method can resist statistical attack and the security level has been improved. However, the method requires the host image as a part of the secret key and we see the secret key is too large making it inconvenient for transmission.

For the improved version of DWT-DCT-SVD method, we use random image to replace the normal image which is generated by using logistic map. We also select the image Lena as the sample for evaluations and the specific metrics are given in Table 5.4.

Table 5.4 Specific metrics for Method II which uses random image as the host image



Attacks	MSE	PSNR	SSIM	NCC	NPCR
No attack	9.8689E-31	300.0573	1.0000	1.0000	0
Gaussian noise	0.0011	29.7285	0.8622	0.9981	0.9414
Salt & pepper noise	0.0022	26.5336	0.7638	0.9960	0.9587
Average filter 7*7	0.1122	9.4984	-0.0765	0.8066	0.9941
Crop 100*100 pixels	0.0041	23.8938	0.9378	0.9926	0.9760
Rotate 5 degree	0.0067	21.7112	0.6898	0.9890	0.9813

Based on Table 5.4, the decrypted results show that the improved version of DWT-DCT-SVD method still has satisfied performance against attack methods image cropping and image rotating. We also see that for attack method based on Gaussian noise and salt-and-pepper noise, the results show the lowest MSE and NPCR as well as the highest NCC and PSNR, which means, the improved method has the ability to resist noise attacks. However, for the attack method average filtering, it shows the highest MSE and NPCR as well as the lowest PSNR, SSIM and NCC; the SSIM value is even lower than 0, which means the improved method cannot resist attack method average filtering.

Based on DWT-DCT-SVD framework, we use logistic mapping to generate the host image to avoid the bandwidth consumption during transmission. This improved method hides the original image into random host image as the encrypted image which can be decrypted successfully. We applied five attack methods in total; the improved method is able to resist four of them effectively, which shows that it has satisfactory robustness. From the histogram of this encrypted image, the pixels are distributed in a normal distribution, which shows the improved method is able to resist statistical attack; thus, the security level is high.

5.2 Comparison and Discussion for the First Three Methods

In this section, the resultant comparison between our proposed encryption Method I, II and III will be discussed. In addition, we have an improved version of our Method III by using chaotic random image as the host image to replace the normal image, the comparison between Method III and its improved version will be also addressed.

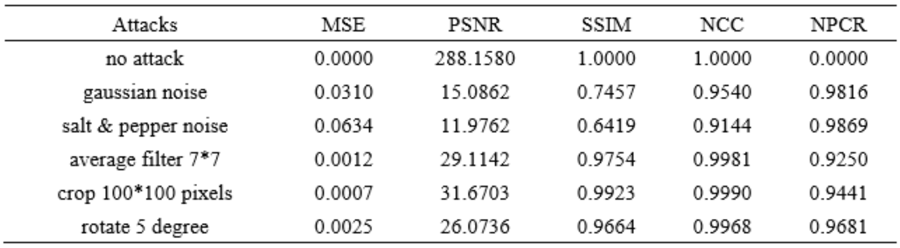
In order to analyze robustness of these three methods, we chose Method III and its improved version, compared them to our proposed Method I and Method II. From Table 5.1, Table 5.2, Table 5.3 and Table 5.4, we find that for all attack methods, the DRPE method using DCT shows the highest MSE and NPCR as well as the lowest SSIM, NCC and PSNR compared to other three methods, which means the DRPE method by using DCT has the lowest robustness; based on this, it is able to be used to verify whether an image has suffered attacks or not. Let’s focus on other three methods; for the noise attacks, the improved version of Method III shows the lowest MSE and PSNR as well as the highest NPCR, SSIM and NCC, which means the improved Method III has the best anti-attack ability against noise attacks; the performance of Method II and Method III is similar. For the attack method average filtering, Method III shows the best performance, the MSE and NPCR are lower than other two methods; SSIM, NCC and NPCR values are higher than other two methods, the performance of Method I against average filtering is trival. The improved method III has the worst performance, the SSIM for this method is even lower than 0. For the attack methods: image cropping and image rotating, Method III and its improved version show satisfied performances which are better than Method I, especially for method III, the decrypted image shows the lowest MSE and PSNR as well as the highest NPCR, SSIM and NCC.

From these comparative measurements, it is clear that the proposed method III and its improved version has better performance compared to traditional chaotic scrambling method except the performance of improved Method III against average filtering. Compared with the DRPE method using DCT, the performance of the proposed methods is much better. By comparing Method III and its improved version, the improved version has better performance against noise attack; but the anti-attack ability against average filtering method is unsatisfied; moreover, for the attack method image cropping and image rotating, performance of the improved version is decreased. From the view of resistence of these attacks, the proposed Method III has achieved higher robustness than that of chaotic scrambling, DRPE method and the DWT-DCT-SVD method by using chaotic random image as the host image against severe composite attacks.

5.3 Analysis for Method IV

We first take advantage of DWT-DCT-SVD method by using a normal image as the host image to encrypt the original color images directly; then, we apply five attacks to all the encrypted images, the performance of decrypted results against each attack for each image was similar. We selected the results for image Lena as the example which is shown in Table 5.5.

Table 5.5 Specific metrics without filtering

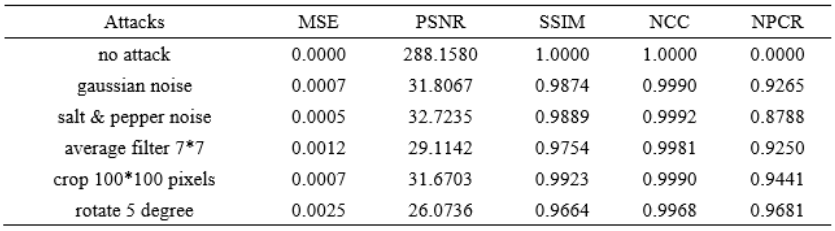


Attacks	MSE	PSNR	SSIM	NCC	NPCR
no attack	0.0000	288.1580	1.0000	1.0000	0.0000
gaussian noise	0.0310	15.0862	0.7457	0.9540	0.9816
salt & pepper noise	0.0634	11.9762	0.6419	0.9144	0.9869
average filter 7*7	0.0012	29.1142	0.9754	0.9981	0.9250
crop 100*100 pixels	0.0007	31.6703	0.9923	0.9990	0.9441
rotate 5 degree	0.0025	26.0736	0.9664	0.9968	0.9681

In Table 5.5, we see that for color image encryption, the Method III still has satisfied performance agaianst attacks: image rotating, image cropping and average filtering; however, just like we used the Method III for greyscale image encryption, for noise attacks, our method has higher MSE and NPCR as well as lower PSNR, SSIM and NCC compared to the performance of other three attack methods; we see that the conclusion is similar to greyscale image encryption, which means that Method III cannot resist noise attack properly for color image encryption. We also test the improved Method III in color image encryption, the conclusion is similar to that of the greyscale image encryption as well. The proposed Method III has the higher robustness against attacks for both of color image and greyscale image encryptions; therefore, we decide to use Method III combining with denoising methods together to conduct our proposed Method IV.

Then, we apply traditional filtering operations to the attacked images, the corresponding performance is shown in Table 5.6. From Table 5.6, we see that for the metrics NPCR and NCC regarding to two types of noises, the optimization effects of image denoising are not obvious; but for the other three metrics, the effects have been improved greatly. SSIM has been raised from less than 0.8 to 0.95, PSNR has been increased more than twice of the original values; the MSE has been dropped obliviously.

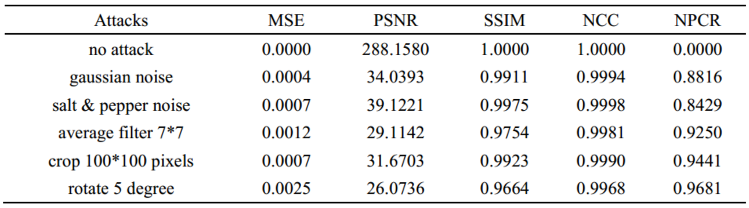
Table 5.6 Specific metrics by using traditional filtering



Attacks	MSE	PSNR	SSIM	NCC	NPCR
no attack	0.0000	288.1580	1.0000	1.0000	0.0000
gaussian noise	0.0007	31.8067	0.9874	0.9990	0.9265
salt & pepper noise	0.0005	32.7235	0.9889	0.9992	0.8788
average filter 7*7	0.0012	29.1142	0.9754	0.9981	0.9250
crop 100*100 pixels	0.0007	31.6703	0.9923	0.9990	0.9441
rotate 5 degree	0.0025	26.0736	0.9664	0.9968	0.9681

For the denosing method based on linear CNN network, we applied the linear CNN model I to filter Gaussian noise and model II to filter salt-and-peper noise, the corresponding performance metrics are shown as Table 5.7.

Table 5.7 Specific metrics by using linear CNN models



Attacks	MSE	PSNR	SSIM	NCC	NPCR
no attack	0.0000	288.1580	1.0000	1.0000	0.0000
gaussian noise	0.0004	34.0393	0.9911	0.9994	0.8816
salt & pepper noise	0.0007	39.1221	0.9975	0.9998	0.8429
average filter 7*7	0.0012	29.1142	0.9754	0.9981	0.9250
crop 100*100 pixels	0.0007	31.6703	0.9923	0.9990	0.9441
rotate 5 degree	0.0025	26.0736	0.9664	0.9968	0.9681

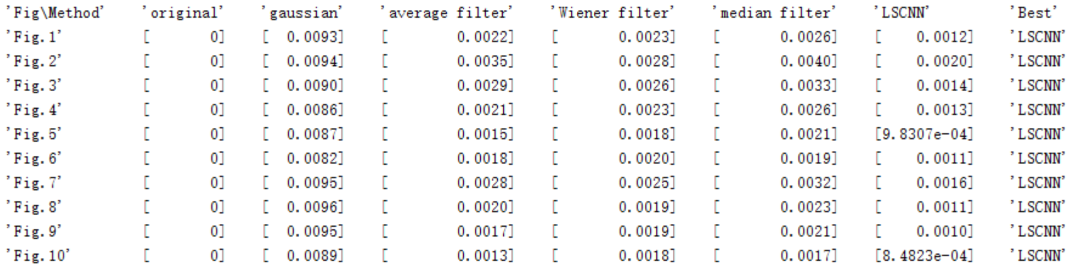
From Table 5.7, we see that for the metrics NPCR and NCC with regard to two types of noises, the optimization effects are obvious; for the other three metrics, the effects have been improved greatly too. SSIM has been raised from less than 0.8 to over 0.99; PSNR has been increased more than twice of the original values; the MSE has been dropped dramatically.

5.4 Comparison and Discussion for the Method IV

In this section, the comparison between traditional denosing methods and the method based on linear CNN models will be dicussed in detail. From Table 5.6 and Table 5.7, we see the results of using linear CNN model are better than the results by using traditional filtering methods for all performance metrics

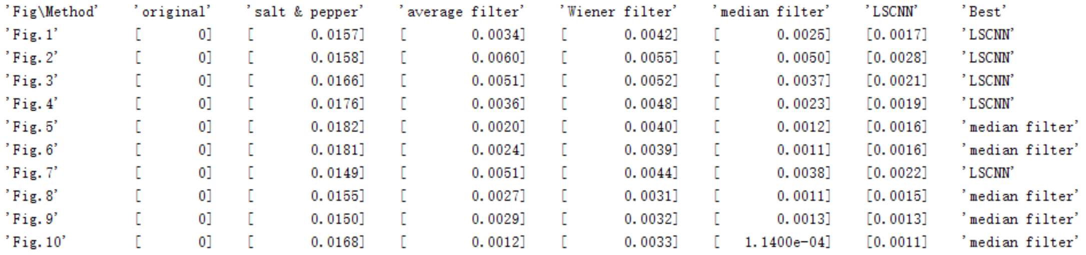
In order to compare the results with traditional filtering methods more specifically, for each original image, we add Gaussian noise first to each image; then, we apply three traditional methods and the linear CNN model I to filter the noise; we use MSE to measure the results as shown in Table 5.8. From Table 5.8, we clearly see that our linear CNN model I shows its lowest MSE for all of the images; in other words, it has better performance for filtering Gaussian noise compared to the three traditional ones.

Table 5.8 Results comparisons for Gaussian noise



```
'Fig\Method’   'original’   'gaussian’   'average filter’   'Wiener filter’   'median filter’   'LSCNN’         'Best’
'Fig.1’        [       0]   [ 0.0093]    [         0.0022]  [         0.0023]  [         0.0026]  [     0.0012]   'LSCNN’
'Fig.2’        [       0]   [ 0.0094]    [         0.0035]  [         0.0028]  [         0.0040]  [     0.0020]   'LSCNN’
'Fig.3’        [       0]   [ 0.0090]    [         0.0029]  [         0.0026]  [         0.0033]  [     0.0014]   'LSCNN’
'Fig.4’        [       0]   [ 0.0086]    [         0.0021]  [         0.0023]  [         0.0026]  [     0.0013]   'LSCNN’
'Fig.5’        [       0]   [ 0.0087]    [         0.0015]  [         0.0018]  [         0.0021]  [9.8307e-04]   'LSCNN’
'Fig.6’        [       0]   [ 0.0082]    [         0.0018]  [         0.0020]  [         0.0019]  [     0.0011]   'LSCNN’
'Fig.7’        [       0]   [ 0.0095]    [         0.0028]  [         0.0025]  [         0.0032]  [     0.0016]   'LSCNN’
'Fig.8’        [       0]   [ 0.0096]    [         0.0020]  [         0.0019]  [         0.0023]  [     0.0011]   'LSCNN’
'Fig.9’        [       0]   [ 0.0095]    [         0.0017]  [         0.0019]  [         0.0021]  [     0.0010]   'LSCNN’
'Fig.10’       [       0]   [ 0.0089]    [         0.0013]  [         0.0018]  [         0.0017]  [8.4823e-04]   'LSCNN’
```

Table 5.9 Results comparisons for salt-and-peper noise



```
'Fig\Method’   'original’   'salt & pepper’   'average filter’   'Wiener filter’   'median filter’   'LSCNN’    'Best’
'Fig.1’        [       0]   [        0.0157]  [         0.0034]  [         0.0042]  [         0.0025]  [0.0017]   'LSCNN’
'Fig.2’        [       0]   [        0.0158]  [         0.0060]  [         0.0055]  [         0.0050]  [0.0028]   'LSCNN’
'Fig.3’        [       0]   [        0.0166]  [         0.0051]  [         0.0052]  [         0.0037]  [0.0021]   'LSCNN’
'Fig.4’        [       0]   [        0.0176]  [         0.0036]  [         0.0048]  [         0.0023]  [0.0019]   'LSCNN’
'Fig.5’        [       0]   [        0.0182]  [         0.0020]  [         0.0040]  [         0.0012]  [0.0016]   'median filter’
'Fig.6’        [       0]   [        0.0181]  [         0.0024]  [         0.0039]  [         0.0011]  [0.0016]   'median filter’
'Fig.7’        [       0]   [        0.0149]  [         0.0051]  [         0.0044]  [         0.0038]  [0.0022]   'LSCNN’
'Fig.8’        [       0]   [        0.0155]  [         0.0027]  [         0.0031]  [         0.0011]  [0.0015]   'median filter’
'Fig.9’        [       0]   [        0.0150]  [         0.0029]  [         0.0032]  [         0.0013]  [0.0013]   'median filter’
'Fig.10’       [       0]   [        0.0168]  [         0.0012]  [         0.0033]  [    1.1400e-04]  [0.0011]   'median filter’
```

Then for each original image, we also generate one image with salt-and-pepper noise; then, we apply three traditional methods and the linear CNN model II to filter out the noises. We use MSE to measure the results shown in Table 5.9. From Table 5.9, we see that the linear CNN model II shows its better performance compared to average filter and

Weiner filter with regard to salt-and-pepper noise. When compared with median filter, the linear CNN model works as same as this traditional method.

5.5 Summary

In this section, we have conucted the comparative analysis for the first three proposed methods based on the specific performance metrics; we found that the proposed Method III has the highest robustness via the first three methods so that we seclect Method III to conduct Method IV. We also have completed the comparison between traditional denoising methods and the method using linear CNN models; we found that the linear CNN models have better performance with regard to both noise attacks compared to traditional methods in general.

Chapter 6
Conclusion and Future Work

In this thesis, in-depth articulation of the techniques was discussed which can be utilized to analyze the performance of image encryption. The corresponding approaches for each encryption method have been implemented as the results of this thesis. In this chapter, we will present this thesis at a scholarly level, also highly organize and integrate the conclusion into the context; meanwhile, the future work will be pointed out by the end of this thesis.

6.1 Conclusion

Since we know the traditional image encryption method based on DRPE has several problems and limitations, this thesis aims at proposing the robust image encryption methods and improve the traditional image methods based on DRPE. We first design an image encryption method based on chaotic scrambling; then we designed the improved DRPE method using chaotic maps and DCT to replace DFT. Then, we are aware that the digital watermarking techniques have high robustness and the idea of watermarking is similar to image encryption; we designed the DWT-DCT-SVD method using the idea of watermarking techniques. After that, we considered further improving the robustness of DWT-DCT-SVD method, so we applied image denoising methods to DWT-DCT-SVD and conducted the improved version. In this thesis, we demonstrated the rationale and workflow for each proposed method in detail. We have verified the proposed image encryption methods could achieve successful encryption and decryption results; we also have tested the performance of each method agaist general attacks. After completed the comparision of performance analytics for each method, the main contributions are summarized as below.

By utilizing the scrambling method based on logistic map, we generated a chaotic sequence which contains the same number of pixels as the original image. Then, we used this sequence to scramble the image. This method can resist image noising and image cropping attack; but it cannot resist intensive attacks (average filtering and image rotating). Meanwhile, the sensitivity of secret keys for this method is high so that the security level is improved.

From the limitation and problems of traditional DRPE method based on DFT, we replace the DFT with DCT to avoid complex operations; we also substitute the traditional random phase matrices with chaotic maps. Two sets of initial values and parameters were used as secret keys so that the amount of secret keys is decreased. With regard to sensitivity test of secret key, the sensitivity for this method is high and the histogram shows that it follows the normal distribution and the method can resist statistical attack;

thus, the security level has been improved. The proposed method cannot resist against five attacks, even if we change a few pixels in the encrypted image, the decryption still fails. Based on this, we can easily verify whether an image has suffered attacks or not.

By summarizing the robust watermarking techniques, we degined a new method based on DWT-DCT-SVD framework and proposed an improved method using the chaotic map to generate random image for use as the host image. We provided the analysis for these two methods and compared the results with traditional chaotic scrambling method and the DRPE method using DCT. The results show the proposed method overcomes the shortcomings of those methods and has a higher robustness; the proposed method has good attack resistence against image cropping, image rotating and average filtering; the improved method has satisfactory anti-attack ability against noise attacks, but for the other methods, the performance is unsatisfactory.

By applying image denoising methods to the proposed DWT-DCT-SVD encryption method using normal image as host image, we proposed the combined method. We designed three traditional denoising methods and a new method based on linear CNN model. After the experiments, we found that the filtering method based on linear CNN model shows the best performance for Gaussian noise; for the salt-and-pepper noise, linear CNN model shows better performance than two of traditional filters and equal performance to median filter. In general, the combined methods have been implemented with the good attack resistence against image cropping, image rotating and average filtering from the DWT-DCT-SVD method, which also has higher robustness against noise attacks; the linear CNN model can improve the performance of filtering.

6.2 Future Work

Our future work includes,

(1) We will work for developing robust image encryption methods by using artificial neural networks and artificial intelligence directly on the image encryption and decryption process, comparing the reults with the methods based on transform domain.

(2) Since we have designed the linear CNN model for image denoising. In future, nonlinear CNN models should be taken into consideration in order to compare with linear CNN model and find the best one.

(3) The number of secret keys for the proposed DWT-DCT-SVD method are too many and the secret keys contain important information. In future, the secret key could be decreased and the security issue of secret keys transmission should be also taken into consideration.

(4) The future work could be more similar to previous work in image encryption based on frequency domain and the comparisons with our proposed methods.

References

Abuturab, M. R. (2014). Color information verification system based on singular value decomposition in gyrator transform domains. Optics and Lasers in Engineering, 57, 13-19.

Ahmed, N., Natarajan, T., & Rao, K. R. (1974). Discrete cosine transform. IEEE Transactions on Computers, 100(1), 90-93.

Aizenberg, N. N., Aizenberg, I. N., & Krivosheev, G. A. (1996, June). CNN based on universal binary neurons: learning algorithm with error-correction and application to impulsive-noise filtering on gray-scale images. In IEEE International Workshop on Cellular Neural Networks and their Applications (pp. 309-314). IEEE.

Al-Haj, A. (2007). Combined DWT-DCT digital image watermarking. Journal of Computer Science, 3(9), 740-746.

Banham, M. R., & Katsaggelos, A. K. (1997). Digital image restoration. IEEE Signal Processing magazine, 14(2), 24-41.

Bracewell, R. N., & Bracewell, R. N. (1986). The Fourier Transform and Its Applications (Vol. 31999). New York: McGraw-Hill.

Burrus, C. S., Gopinath, R. A., & Guo, H. (1997). Introduction to wavelets and wavelet transforms: a primer.

Chai, X., Zheng, X., Gan, Z., Han, D., & Chen, Y. (2018). An image encryption algorithm based on chaotic system and compressive sensing. Signal Processing, 148, 124-144.

Chakraborty, S., Chatterjee, S., Dey, N., Ashour, A. S., & Hassanien, A. E. (2017). Comparative approach between singular value decomposition and randomized singular value decomposition-based watermarking. In Intelligent Techniques in Signal Processing for Multimedia Security (pp. 133-149). Springer International Publishing.

Changlai, G. (2007). Image-denoising method based on wavelet transform and mean filtering. Opto-Electronic Engineering, 1, 19.

Chen, J., Kang, X., Liu, Y., & Wang, Z. J. (2015). Median filtering forensics based on convolutional neural networks. IEEE Signal Processing Letters, 22(11), 1849-1853.

Chen, L., Zhao, D., & Ge, F. (2013). Image encryption based on singular value decomposition and Arnold transform in fractional domain. Optics Communications, 291, 98-103.

Chen, P. Y., Lien, C. Y., & Chuang, H. M. (2010). A low-cost VLSI implementation for efficient removal of impulse noise. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 18(3), 473-481.

Daubechies, I., Meyer, Y., Lemerie-Rieusset, P. G., Techamitchian, P., Beylkin, G., Coifman, R., ... & Donoho, D. (1993). Wavelet transforms and orthonormal wavelet bases. Different Perspectives on Wavelets, 47, 1-33.

Deb, K., Al-Seraj, M. S., Hoque, M. M., & Sarkar, M. I. H. (2012, December). Combined DWT-DCT based digital image watermarking technique for copyright protection. In International Conference on Electrical & Computer Engineering (ICECE) (pp. 458-461). IEEE.

Ding, W., Yan, W., & Qi, D. (2000). Digital image information hiding technology and its application based on scrambling and amalgamation. Journal of Image and Graphics, 5(8), 644-649.

Ding, W., Yan, W., & Qi, D. (2001). Digital image scrambling. Progress in Natural Science, 11(6), 454-460.

Ding, W., Yan, W. Q., & Qi, D. X. (2000). Digital image scrambling and digital watermarking technology based on Conway's Game. Journal of North China University of technology, 12(1), 1-5.

Ding, W., Yan, W. Q., & Qi, D. X. (1999, December). Digital image scrambling technology based on Gray code. In Proc. of International Conference on CAD/CG (pp. 116-119).

Eskicioglu, A. M., & Fisher, P. S. (1995). Image quality measures and their performance. IEEE Transactions on Communications, 43(12), 2959-2965.

Fan, H., & Li, M. (2017). Cryptanalysis and Improvement of Chaos-Based Image Encryption Scheme with Circular Inter-Intra-Pixels Bit-Level Permutation. Mathematical Problems in Engineering.

Feng, C., & Ye, H. (2017). A Digital Image Encryption Algorithm Based on Improved ZigZag Transformation and Chaotic Sequence.

Fu, C., Chen, J. J., Zou, H., Meng, W. H., Zhan, Y. F., & Yu, Y. W. (2012). A chaos-based digital image encryption scheme with an improved diffusion strategy. Optics Express, 20(3), 2363-2378.

Fialka, O., & Cadik, M. (2006). FFT and convolution performance in image filtering on GPU. In International Conference on Information Visualization. (pp. 609-614). IEEE.

Goupillaud, P., Grossmann, A., & Morlet, J. (1984). Cycle-octave and related transforms in seismic signal analysis. Geoexploration, 23(1), 85-102.

Guan, Z. H., Huang, F., & Guan, W. (2005). Chaos-based image encryption algorithm. Physics Letters A, 346(1), 153-157.

Guo, J. I. (2000). A new chaotic key-based design for image encryption and decryption.

In IEEE ISCAS’00 (Vol. 4, pp. 49-52).

Haykin, S. O. (2013). Adaptive filter theory. Pearson Higher Ed.

He, S., Pan, X. L., & Li, Y. M. (2012). Optimization algorithm for average filtering. Information Technology, 3, 041.

Huang, T., Yang, G. J. T. G. Y., & Tang, G. (1979). A fast two-dimensional median filtering algorithm. IEEE Transactions on Acoustics, Speech, and Signal Processing, 27(1), 13-18.

Jin, D., Yan, W., & Kankanhalli, M. S. (2005). Progressive color visual cryptography. Journal of Electronic Imaging, 14(3), 033019.

Kansal, M., Singh, G., & Kranthi, B. V. (2012, September). DWT, DCT and SVD based digital image watermarking. In International Conference on Computing Sciences (ICCS) (pp. 77-81). IEEE.

Kong, D., Shen, X., Xu, Q., Xin, W., & Guo, H. (2013). Multiple-image encryption scheme based on cascaded fractional Fourier transform. Applied Optics, 52(12), 2619-2625.

LeCun, Y., & Bengio, Y. (1995). Convolutional networks for images, speech, and time series. The Handbook of Brain Theory and Neural Networks, 3361(10), 1995.

Li, C. P., Qin, P. Y., & Zhang, J. J. (2017) Research on Image Denoising Based on Deep Convolutional Neural Network. Computer Engineering 2017, 43(3)

Li, T. Y., & Yorke, J. A. (1975). Period three implies chaos. The American Mathematical Monthly, 82(10), 985-992.

Liu, L., Shen, C., & van den Hengel, A. (2015). The treasure beneath convolutional layers: Cross-convolutional-layer pooling for image classification. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 4749-4757).

Liu, Y., Lin, J., Fan, J., & Zhou, N. (2012). Image encryption based on cat map and fractional Fourier transform. Journal of Computational Information Systems, 8(18), 7485-7492.

Liu, Z., Gong, M., Dou, Y., Liu, F., Lin, S., Ahmad, M. A., ... & Liu, S. (2012). Double image encryption by using Arnold transform and discrete fractional angular transform. Optics and Lasers in Engineering, 50(2), 248-255.

Liu, Z., Guo, Q., & Liu, S. (2006). The discrete fractional random cosine and sine transforms. Optics Communications, 265(1), 100-105.

Liu, Z., Li, S., Liu, W., Wang, Y., & Liu, S. (2013). Image encryption algorithm by using fractional Fourier transform and pixel scrambling operation based on double random phase encoding. Optics and Lasers in Engineering, 51(1), 8-14.

Liu, Z., Xu, L., Liu, T., Chen, H., Li, P., Lin, C., & Liu, S. (2011). Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains. Optics Communications, 284(1), 123-128.

Liu, Z., Yan, W., & Yang, M. (2017) Image Encryption Based on Double Random Phase Encodin. IEEE IVCNZ (pp. 3-6).

Liu, Z., Yan, W., & Yang, M. (2018) Image Denoising based on A Linear CNN Model. IEEE ICCAR (pp. 3-6).

Liu, Z., Xu, L., Liu, T., Chen, H., Li, P., Lin, C., & Liu, S. (2011). Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains. Optics Communications, 284(1), 123-128.

Madhesiya, S., & Ahmed, S. (2013). Advanced technique of digital watermarking based on SVD-DWT-DCT and Arnold transform. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 2(5), pp.1918.

Mallat, S. G. (1989). A theory for multiresolution signal decomposition: the wavelet representation. IEEE Transactions on Pattern Analysis and Machine Intelligence, 11(7), 674-693.

Matsumoto, T., Yokohama, T., Suzuki, H., Furukawa, R., Oshimoto, A., Shimmi, T., ... & Chua, L. O. (1990, December). Several image processing examples by CNN. In International Workshop on CNNA-90 Proceedings (pp. 100-111). IEEE.

Matthews, R. (1989). On the derivation of a “chaotic” encryption algorithm. Cryptologia, 13(1), 29-42.

Milanfar, P. (2013). A tour of modern image filtering: New insights and methods, both practical and theoretical. IEEE Signal Processing Magazine, 30(1), 106-128.

Ming, Y., & Li-hua, S. (2011). The application of an improved fast algorithm of median filter on removing image noise. Engineering of Surveying and Mapping, 20(3), 65-69.

Mohamed, M. A., Aboutaleb, M., Abdel-Fattah, M. G., & Samrah, A. S. (2015). Hybrid watermarking scheme for copyright protection using chaotic maps cryptography. International Journal of Computer Applications, 126(4).

Nomura, T., & Javidi, B. (2000). Optical encryption using a joint transform correlator architecture. Optical Engineering, 39(8), 2031-2035.

Oktem, R., Egiazarian, K., Aizenberg, I., & Aizenberg, N. (1998, October). Transform domain denoising using nonlinear filtering and cellular neural networks. In ICIP 98, Vol. 2, pp. 862-866.

Pareek, N. K., Patidar, V., & Sud, K. K. (2006). Image encryption using chaotic logistic map. Image and Vision Computing, 24(9), 926-934.

Pitas, I., & Venetsanopoulos, A. N. (2013). Nonlinear digital filters: principles and applications (Vol. 84). Springer Science & Business Media. (2013)

Rao, K. R., & Yip, P. (2014). Discrete cosine transform: algorithms, advantages, applications. Academic Press.

Refregier, P., & Javidi, B. (1995). Optical image encryption based on input plane and

Fourier plane random encoding. Optics Letters, 20(7), 767-769.

Rekeczky, C., Tahy, Á., Végh, Z., & Roska, T. (1999). CNN-based spatio-temporal nonlinear filtering and endocardial boundary detection in echocardiography. International Journal of Circuit Theory and Applications, 27(1), 171-207.

Scharinger, J. (1998). Fast encryption of image data using chaotic Kolmogorov flows. Journal of Electronic imaging, 7(2), 318-325.

Situ, G., & Zhang, J. (2004). Double random-phase encoding in the Fresnel domain. Optics Letters, 29(14), 1584-1586.

Shi, B. E., Roska, T., & Chua, L. O. (1993). Design of linear cellular neural networks for motion sensitive filtering. IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, 40(5), 320-331.

Song, Z. Z. (2013) Image Encryption Algorithm Based on Chaotic Mapping and Double Phase Encoding Technology (Master's thesis, Harbin Institute of Technology).

Sundararajan, D. (2016). Discrete Wavelet Transform: A Signal Processing Approach. John Wiley & Sons.

Thakeel, S. A., Kadhim, L. M., & Abdlateef, S. A. (2017). A New Color Image Watermarking Technique Using Multiple Decomposition. Journal of Theoretical & Applied Information Technology, 95(10).

Unnikrishnan, G., Joseph, J., & Singh, K. (2000). Optical encryption by double-random phase encoding in the fractional Fourier domain. Optics Letters, 25(12), 887-889.

Wang, B., Ding, J., Wen, Q., Liao, X., & Liu, C. (2009, November). An image watermarking algorithm based on DWT DCT and SVD. In International Conference on Network Infrastructure and Digital Content. (pp. 1034-1038). IEEE.

Wang, J. (2016). Research on Image Denoising Based on Deep Convolutional Neural Network (Doctoral dissertation), Shandong University, China.

Wang, Y.J., &Wang, C. (2013) Implementation of Digital Image Encryption Algorithm Based on DWT-SVD and DSP. Computer Applications and Software, 30 (4), 141-144.

Wang, Z. J., Qv, C. W., & Cui, L. (2007). Images denoising with Wiener filter in directionalet domain. Electronics Optics & Control, 6, 008.

Wang, Z., Simoncelli, E. P., & Bovik, A. C. (2003). Multiscale structural similarity for image quality assessment. In Asilomar Conference on Signals, Systems and Computers (Vol. 2, pp. 1398-1402). IEEE.

Wei, D., Qi, Y. W., & Xu, Q. D. (2001). Digital Image Scrambling Technology based on Arnold Transform. Computer Aided Design and Graphics learned journal April.

Widrow, B., McCool, J. M., Larimore, M. G., & Johnson, C. R. (1976). Stationary and nonstationary learning characteristics of the LMS adaptive filter. Proceedings of the IEEE, 64(8), 1151-1162.

Wu, J., Zhang, L., & Zhou, N. (2010). Image encryption based on the multiple-order discrete fractional cosine transform. Optics Communications, 283(9), 1720-1725.

Xiuping, M. (2008) Application of wavelet transform in image processing. Science and Technology Information: Academic Research 27 (2008): 453-454.

Xu, F., Lu, J. G., & Sun, Y. X. (2003). Application of neural network in image processing. Information and Control, 32(4), 344-351.

Yan, H. P., & Wu, Y. H., (2017).Filtering image impulse noise by using a PCNN image noise reduction technique. CAAI Transaction on Intellihent System, 12(2), 272-278.

Yuen, C. H., & Wong, K. W. (2011). A chaos-based joint image compression and encryption scheme using DCT and SHA-1. Applied Soft Computing, 11(8), 5092-5098.

Yuan, X. G., & Zhou, Z. (2011). A Novel Robust Watermarking Algorithm Based on DWT-DCT-SVD. Computer Engineering & Science, 1, 027.

Zhang, Y., & Xiao, D. (2013). Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform. Optics and Lasers in Engineering, 51(4), 472-480.

Zhao, J., & Yu, D. (1999). A new approach for ME image restoration based on CNN. International Journal of Circuit Theory and Applications, 27(3), 339-346.

Zhou, N. R., Hua, T. X., Gong, L. H., Pei, D. J., & Liao, Q. H. (2015). Quantum image encryption based on generalized Arnold transform and double random-phase encoding. Quantum Information Processing, 14(4), 1193-1213.

Zhu, B., Liu, S., & Ran, Q. (2000). Optical image encryption based on multifractional Fourier transforms. Optics Letters, 25(16), 1159-1161.