August 2012

Master’s Degree Thesis

Improved Secret Fragment Visible Mosaic Image for Information Hiding

Graduate School of Chosun University

Department of Information and Communications Engineering

Zhu Lin

Improved Secret Fragment Visible Mosaic Image for Information Hiding

가시적 비밀 조각 모자이크 이미지 방식의
개선된 정보 은닉 기법

August 25, 2012

Graduate School of Chosun University

Department of Information and Communications Engineering

Zhu Lin

Improved Secret Fragment Visible Mosaic Image for Information Hiding

Advisor: Prof. Seung Jo Han

This thesis is submitted to Chosun University in partial fulfillment of the requirements for a Master's degree

April 2012

Graduate School of Chosun University

Department of Information and Communications Engineering

Zhu Lin

주 림의 석사학위 논문을 인준함

위원장 조선대학교 교수 변 재 영 印 邊宰榮印

위 원 조선대학교 교수 김 영 식 印 金榮植印

위 원 조선대학교 교수 한 승 조 印 韓承朝印

2012년 5월

조선대학교 대학원

Graduate School of Chosun University

Gwangju, South Korea

CERTIFICATE OF APPROVAL

MASTER' S THESIS

This is to certify that the Master' s Thesis of

Zhu Lin

has been approved by the examining Committee for the thesis requirement for the Master' s Degree in Information and Communication Engineering

Thesis Examining Committee

Committee Chairperson ____________________

Prof. Jae-Young Pyun

Committee Member ____________________

Prof. Young-Sik Kim

Committee Member ____________________

Prof. Seung Jo Han

Table of Contents

Table of Contents ········· i

List of Figures ········· iii

List of Tables ········· iv

Abstract ········· v

Ⅰ. Introduction ········· 1

A. Thesis Motivation and Overview ········· 2

B. Thesis Contribution ········· 2

C. Thesis Organization ········· 3

Ⅱ. Background ········· 4

A. Basis of The Information Hiding Technology ········· 4

B. Principle of Information Hiding and Cryptography ········· 5

C. The Terminology, Mode and Branch of Information Hiding ·6

D. Characteristics of Information Hiding ········· 8

E. Information Hiding Algorithms ········· 10

F. Assessment of Image Quality ········· 11

G. Related Works ········· 13

Ⅲ. Chaotic System ··15

A. Logistic Map and Chebyshev Map ···15

B. Combination of Logistic Map and Chebyshev Map ··························17

Ⅳ. Color Transfer ··21

A. Color Space ···21

B. Color Transfer Algorithm ···25

Ⅴ. New Mosaic Image for Information Hiding based on Mixed Chaotic Sequences ··33

A. Basic Idea of The Proposed Method ··34

B. Encrypt The Blocks of Secret Image ···34

C. Color Transformations of Blocks ···35

D. Mosaic Image Generation ···36

E. Embedding the Recovery Information ···37

F. The Secret Image Recovery Algorithm ···38

Ⅵ. Experimental Results ···42

Ⅶ. Conclusion ···51

References ···52

List of Figures

Figure. 2.1 Block diagram of information encryption ······5
Figure. 2.2 Block diagram of information hiding ······5
Figure. 2.3 Block diagram of information hiding ······6
Figure. 2.4 Typical block diagram of information hiding ······7
Figure. 2.5 The classification of information hiding ······8
Figure. 3.1 The Chaotic system ······16
Figure. 3.2 Combination of Logistic Map and Chebyshev Map ······19
Figure. 3.3 The result image using combination map ······20
Figure. 4.1 RGB color space ······22
Figure. 4.2 lαβ color space ······23
Figure. 4.3 Color transfer based Reinhard method ······27
Figure. 4.4 Geometrical representation of SVD ······30
Figure. 4.5 Color transfer based Xiao method ······32
Figure. 5.1 Mosaic image creation ······41
Figure. 6.1 Experimental results of the proposed method ······42
Figure. 6.2 Comparison of Li method and the proposed method ······43
Figure. 6.3 Comparison of Li method and the proposed method ······44
Figure. 6.4 Comparison of Li method and the proposed method ······45
Figure. 6.5 Comparison of Li method and the proposed method ······46
Figure. 6.6 The mosaic image created by different block size ······47
Figure. 6.7 Comparison of Li method and the proposed method ······48
Figure. 6.8 Graphical of RMSE and PSNR ······50

List of Tables

Table 6.1 Competitive Results ··49

초 록

가시적 비밀 조각 모자이크 이미지 방식의 개선된 정보 은닉 기법

주 림
지도교수: 한승조, 교수, Ph.D
정보통신공학과, 대학원, 조선 대학교

이 논문에서는 가시적 비밀 조각 모자이크 이미지를 기반으로 새로운 정보 은닉 방법을 제안한다. 이 알고리즘은 정보를 숨겨 있는 모자이크 이미지를 생성하는 컬러 전송의 응용 프로그램에 대한 개발되었다. RGB 색 공간은 세 컬러 채널 간의 강한 상관관계를 가지고 있기 때문에, 탠덤의 모든 색상 채널을 수정해야한다. 따라서 어떤 색상 수정 과정이 복잡해지는 문제가 있다. 이 색상 공간에서 또 다른 문제는 비밀 이미지 블록 시퀀스의 복구 정보의 비트 스트립의 크기이다. 따라서 모자이크 이미지에 큰 비트 스트립을 포함하는 것은 결과 이미지의 품질을 악화시킨다. 본 논문에서는 서로 관련적인 색상 공간에서 색상 전송 기술을 사용하여 이러한 문제를 해결하는 새로운 방법을 제안한다. 픽셀 값은 입체 확률 변수와 이미지 샘플의 집합으로 간주된다. 색상 전송 프로세스는 번역, 스케일링 및 회전으로 구성된 기하학적인 변환에 의해 이루어진다. 색상 공간중의 상관관계는 공분산을 연구하여 측정 및 색상 전송 프로세스에 사용된다. 강력한 암호화 및 낮은 비트 레이트 요건을 얻기 위해서 logistic map 하고 chebyshev map의 조합이 사용되어 비밀 이미지 암호화 시퀀스를 생성하게 된다.

I. Introduction

With the rapid development of the network and multimedia technology, application and dissemination of information have become an essential part of daily life. On the one hand, information technology has brought convenience for people while on the other hand, the insecurity and destruction of information can cause huge loss to community. Thus the assurance of security and the distribution system of information have become an important research topic. In traditional information security system the secret information is encrypted to protect important information through different encryption algorithm [1]. However, breaking of encryption algorithm is possible only under the case of the good strength of computing and processing capacities of computers. Consequently, it is urgently imminent to look for a new information security technology. Information hiding is a new technology that integrates the theories and technologies of many academic and technical subjects. For information hiding, digital media are used as the carrier of the information to be hidden. The carrier conceals secret messages by covering the form of their existence. It has changed the view of the past security technology. In simple terms, it is based on human vision system and auditory sense of multimedia information systems. Redundancy algorithm will be embedded by hiding the embedded message in the multimedia. The human beings are unable to distinguish between the original multimedia and embedded message. As a result it is difficult for the attacker to find the secret information in the communication process, because he cannot feel the existence of secret information.

There are two major disciplines of information hiding: steganography and digital watermarking [2]-[3]. Cryptography deals on protection of the content of messages, while the steganography is about concealing their very existence and it is mainly interpreted to hide information in other information. The digital watermarking on the one hand is closely related to steganography, while on the other hand, it has an additional notion of resilience against attempts to remove the hidden data. Thus, watermarking rather than steganography principles are used whenever the cover-data is available to parties who know the existence of the hidden data and may have an interest on removing it. A popular application of watermarking is to give proof of ownership of digital data by embedding copyright statements [4]-[5]. While information hiding is the recent rise, its application range is very extensive.

A. Thesis Motivation and Overview

Information security and privacy have been ensured with data encryption techniques traditionally. Information hiding is also one part of communications security like encryption. It is about protecting the content of message. An important sub-discipline of information hiding is Steganography. This technique is about concealing their very existence. Nowadays, researchers have started to utilize information hiding techniques to enhance the security level of data encryption systems. Thus the information hiding techniques have become important in these areas. Information hiding conceals not only the content of the secret message, but also it is very existence.

B. Thesis Contribution

In this thesis, a new algorithm for information hiding is presented based on secret fragment visible mosaic image. This algorithm is called secret fragment visible mosaic image based algorithm. It was designed for the safety of information while transmitted over the unsecured communication channels. This thesis surveys algorithms that have already been proposed. Important algorithms that are proposed in the literature and designed for information hiding are identified and explained in this thesis. The main contributions of this thesis are as follows:

New Algorithm: A new algorithm is designed for the information hiding with two main features: bit rate reduction and better visual quality.

Design Procedure: A design procedure is given in order to find the important parameters of this algorithm. For a given application with its specifications and requirements, an engineer can follow the steps in this procedure to find the important parameters and also the appropriate number of phases in this algorithm.

Simulation: A simulation code was written in Matlab R2010a to test the performance of this algorithm and compare with other algorithms.

C. Thesis Organization

The remainder of this thesis is organized in modular chapters. Chapter II presents overview of the information hiding and the related works that have already been carried out. Chapter III describes the basic features of Chaotic system. Chapter IV describes the basic features of color transfer. Chapter V shows the main features and algorithms for the proposed algorithm of this research work. Chapter VI demonstrates the information hiding achieved by proposed algorithm through experimental results. Thesis is concluded in the last chapter with wrapping text for the summary of this research.

II. Background

This chapter is devoted to the background necessary for discussing the work in this thesis. This chapter first points out the basis of the information hiding technology by comparing encryption to introduce the basic principles and characteristics of information hiding technology. Then the terminology and model of information hiding technology, the basic properties and classification method are described later.

A. Basis of the Information Hiding Technology

Information hiding techniques commonly use images (text, sound, and video) as a carrier. The multimedia information has redundancy in time or space and people has the masking effect on the information changes. Thus the information can be hidden in the multimedia data.

- Multimedia information consist lot of redundancy. From the perspective of information theory, coding efficiency of uncompressed multimedia information is very low. Therefore, it is entirely feasible that some of the information can be embedded in the multimedia information for secret transmission without effecting the multimedia information transmission and use.

- Visual or auditory sensory system has some masking effect of certain information. In the edge component of image where the brightness is changing, the adjacent pixel of the edge is masked. The people become insensitive, inaccurate, which is called as the visual masking effect. The resolution of the human eye usually have only a few dozen gray-scales thus it is insensitive to the information near the edge. These features can be very useful for hiding the information without being noticed.

B. Principle of Information Hiding and Cryptography

Information hiding and cryptography protect the key rather than the information. Information hiding technique follows the basic ideas and concepts of traditional encryption techniques. However both use different means of information protection. The Cryptography encrypts the meaningful information to become random gibberish. As shown in Figure 2.1, the eavesdropper knows that the message contains important information in intercepted cipher-text, but they cannot decipher.

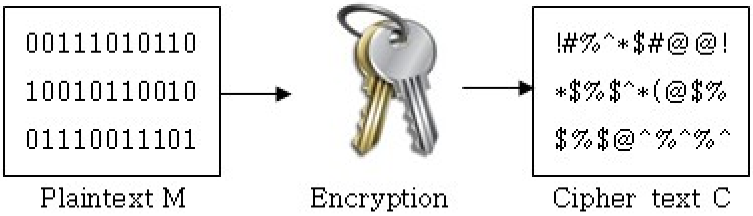


Figure. 2.1: Block diagram of information encryption

Information hiding method hides meaningful message in another ordinary message called carrier, and then sends secret information as normal information shown in Figure 2.2. The attacker does not know whether the message is hidden or the general information. Even if the attacher knows about information, it is also difficult to extract the hidden information.

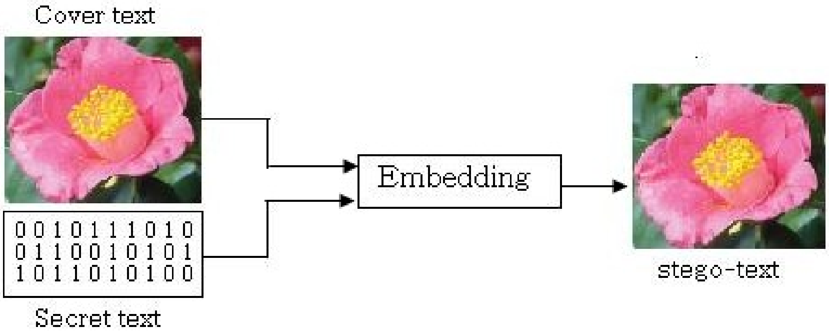


Figure. 2.2: Block diagram of information hiding

In order to increase the difficulty of deciphering further to improve the security of confidential information, we can use the combination of cryptography and information hiding techniques together. The message M is encrypted to become cipher-text C, and then C is hidden in the vectors in S. Figure 2.3 shows if an attacker wants to obtain the secret information, he should detect the existence of the information and should know how to extract the secret information M from vector S' and how to decrypt M from C.

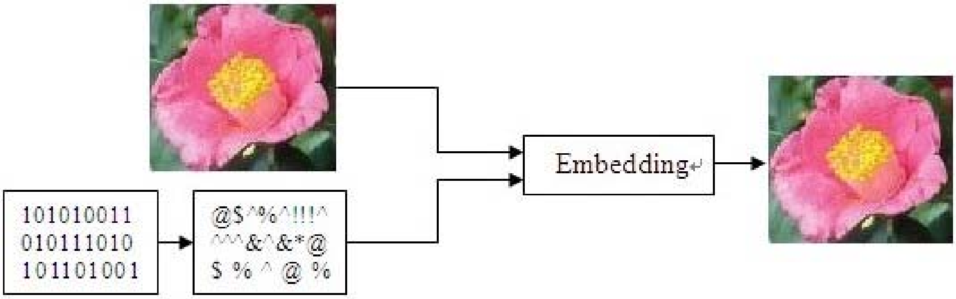


Figure. 2.3: Block diagram of information hiding

C. The Terminology, Mode and Branch of Information Hiding

In the 1996, the first information hiding technology international conference was held, the terms of information hiding was unified, and proposed the framework and branch of information hiding [1]. In Information hiding system, generalized model can be used as in Figure 2.4. In generalized model the secret message is the information that one wishes to send secretly. It is usually hidden in an innocuous message referred to as a cover message, cover image or cover media information as appropriate, the stego-text or other stego-object. A stego-key is used to control the hiding process so as to restrict detection and recovery of the embedded data to parties who know it. As the purpose of steganography is having a covert communication between two parties whose existence is unknown to a possible attacker, a successful attack consists in detecting the existence of this communication.

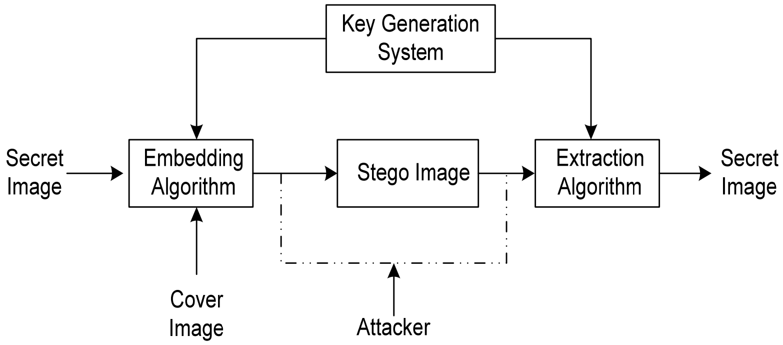


Figure. 2.4: Typical block diagram of information hiding

The system includes an embedded process and an extraction process. The embedded process uses embedding algorithm of information hiding algorithm to add the secret information in the cover object to generate the hidden object. Hidden objects called Stego-object may be intercepted in the transmission process by analysis. The extraction process uses the extraction algorithm to recover the secret information from the received hidden object. The hidden object may be modified. The extraction process may require the participation of the cover object. Usually the former is called non-blind extraction and the latter is called the blind extraction. The information hiding techniques can be classified as in Figure 2.5.

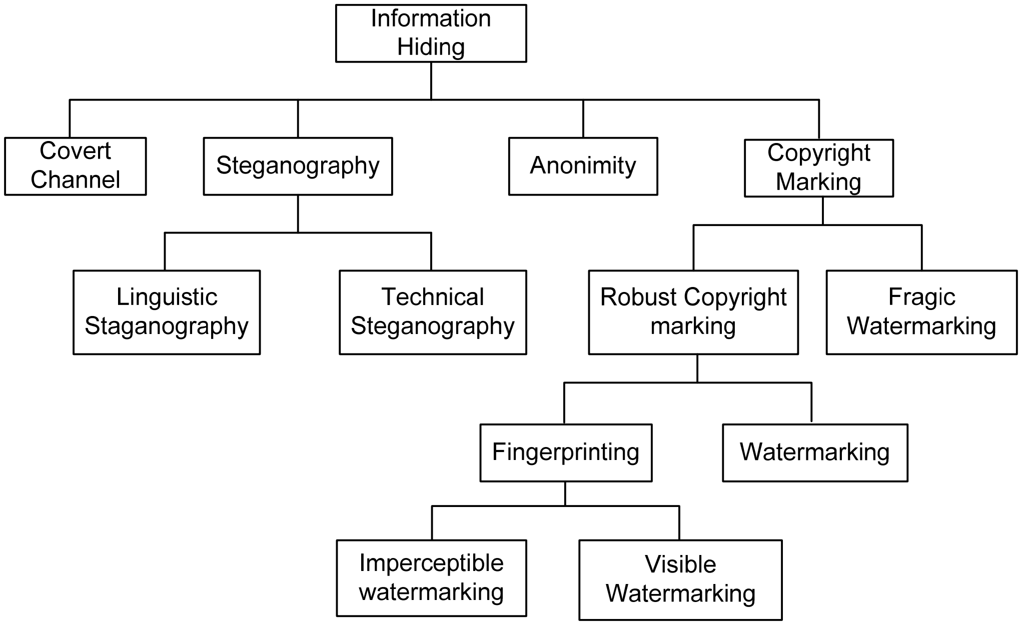


Figure 2.5: Classification of information hiding

D. Characteristics of Information Hiding

Information hiding is different from traditional encryption algorithm. Since its purpose does not limit the normal data access, but rather to ensure that the hidden data will not be violated. Therefore, the information hiding technology must consider the threat on the information posed by the normal data manipulation in order to make the confidential information having immune to the normal data manipulation. The key to this immunity is to make complex to damage the part of hidden information by the operation of the normal data. According to the purpose of information hiding and requirements of the techniques the newly developed technology has to meet the following requirements.

1. Robustness

Robustness refers to the ability to detect the watermark after common signal processing operations. In the watermarking, the watermarked contents may undergo various attacks before the watermark is retrieved, where the attack is defined as any alteration of contents that can damage the watermark. Resistance against attacks is the key issue when designing a watermarking system. The watermarking system should be resistant against any intentional or unintentional processing of the watermarked contents that can be an image, audio, video, or text. This attribute of a watermarking system is called robustness. If the watermark can survive in the object even if it was tampered, it is then called a robust watermark. Robustness also means that it must be nearly impossible to defeat a watermark without degrading the marked contents to a large extent to the extent that the contents remain no longer useful and valuable. While designing a watermarking technique, it is necessary to bear in mind the intended application and the corresponding set of conceivable attacks. Secondly, we must strive to achieve robustness, making it resistant against attacks.

2. Imperceptibility

Stego-objects and cover objects should have consistent characteristics. It is the fundamental requirement of watermarking meaning that the watermark must be embedded in the object imperceptibly. To preserve the quality of watermarked contents, the watermark should not noticeably distort the original content. The original and the watermarked objects should look similar and ideally, the original content and watermarked content should be perceptually identical. The watermark should not be perceived by the viewer, or the watermark should not degrade the quality of content.

3. Capacity

Capacity means the number of bits the technique can encode in a unit amount of time. It indicates the upper limit of watermark length. Generally, capacity of any watermark scheme should be high. However, different applications have different capacity requirements for example, in case of broadcast monitoring very high capacity is required.

4. Security

Embedding algorithm has a strong capability of anti-attack. It must be able to withstand some kinds of attack so that the confidential information will not be destroyed. The security of a watermark refers to its ability to resist hostile attacks.

E. Information Hiding Algorithms

1. **Spatial Domain:** Hiding in the space domain of digital images in spatial domain, simple information hiding method namely least significant bit (LSB) replacement method was proposed in 1989. The LSB method is to replace the least significant bits in the selected cover pixels to imply the binary secret message.

2. **Transform Domain algorithm:** For the sake of advance the robustness of hidden information, many scholars suggest lots of algorithms based on transform domain, such as DCT, DWT and DFT domain algorithm. At present DCT domain algorithm is most extensively used for information hiding because of compaction of energy in few transformed coefficients.

3. Spread Spectrum: The spread spectrum is a very well known method used in communication. It uses a larger frequency band and a lower power density to transmit signal. The most important interest of this method is to transform a non- Gaussian ambient noise into white Gaussian noise.

4. Mosaic Image: It is a new type of computer art called secret-fragment-visible mosaic image. This effect of information hiding is useful for covert communication or secure keeping of secret images. This method was proposed in 2011 by Lai et al [9]. The mosaic image is generated by dividing the secret image into fragments. Recently, another paper is proposed using color transfer to transform the color characteristics to be those of the blocks of the target image.

F. Assessment of Image Quality

Image quality evaluation is one of the basic technologies of the image information engineering. The image communication should go through the process of collection, transmission, processing and record. All of the processing and communicating of these technologies will affect the image quality. The digital image information hiding system must give the quality evaluation between stego-image and recovered image. There are some methods to measure them. The most common methods are Mean Square Error (MSE), Normalized Mean Square Error (RMSE) and Peak Signal to Noise Ratio (PSNR), MSE can reflect to the proximity of pixels. However it is poor for correlation with subjective evaluation. Thus the result is often inconsistent with the subjective feeling. PSNR is one of the most commonly used image quality assessments.

1. RMSE(Root Mean Squared Error)

RMSE is a frequently used measure of the difference between values predicted by a model or an estimator and the values actually observed. RMSE is a good measure of accuracy. It is defined as:

$$RMSE = \sqrt{\frac{\sum_{x=1}^{M}\sum_{y=1}^{N}[g(x,y) - f(x,y)]^2}{M \times N}} \quad (2.1)$$

where $f(x,y)$ and $g(x,y)$ denote original image and Stego-image and M, N denote the width and height of image. If the value is small, the difference of two images is small. The two images are more similar.

2. PSNR (Peak Signal-to-Noise Ratio)

PSNR is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Since many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale. It is defined as:

$$PSNR = 10\log\frac{M \times N \times 256 \times 256}{\sum_{x=1}^{M}\sum_{y=1}^{N}[g(x,y) - f(x,y)]^2} \quad (2.2)$$

The big value of PSNR indicates that two images are more similar.

G. Related Works

Numerous information hiding methods have been proposed. Fundamentally they are classified into two categories. First is spatial domain and next is transform domain.

The spatial domain techniques embed messages in the intensity of the pixels directly. Least significant bit (LSB) substitution based method proposed by Lee et al. [4] is one of the example of spatial domain technique. In this method the least significant bit LSB of each pixel in the cover image is modified to embed a secret message .The bit plane of each block truncation coding (BTC) block is exploited to embed a secret message. Similarly, wang et al. [6] exploited the optimal solution of LSB. This method is based on the substitution of LSB of secret data. This method generates higher quality stego image. However the generated stego image is highly sensitive to modification.

In transform domain techniques the image in spatial domain is transformed to frequency domain. DCT based image coding is one of widely used transform domain coding system [7]. In this technique, DCT coefficients are obtained for the given carrier image in first step. The secret data is embedded in the carrier image for DCT coefficients lower than the threshold value. In order to avoid visual distortion, embedding of secret information is avoided for zero valued DCT coefficients. Alturki [8] proposed a simple bit-replacement of quantized DCT coefficients based method. In this method the coefficients are calculated from a randomly permuted image. In the method, the distortion distribution is approximately a generalized Gaussian distribution.

Recently, a new computer art based information hiding technique has been proposed by Lai et al [9]. This method creates a target image automatically by composing small fragments of a given image in mosaic image form. However large database is created to search target image with highest similarity with secret image. In order to reduce large database an improvement was proposed in [10]. The basis of this method was the conversion of color characteristics from target image to secret image. The data requirement in previous method was solved however they got this result with the sacrifice in image quality.

III. Chaotic System

The basic idea of the chaos theory was originated in the early 20th century and formed in 1960s. In recent years, digital image encryption based on chaos theory has become a hot research topic in information security. The classic one-dimensional chaotic maps are the Logistic map and Chebyshev map. The main advantages of the two chaotic characteristics are the initial value sensitivity of chaotic maps and long-term unpredictability of chaotic behavior. Since the output sequence has good pseudo-randomness and statistical properties, it has been widely used in the digital image encryption.

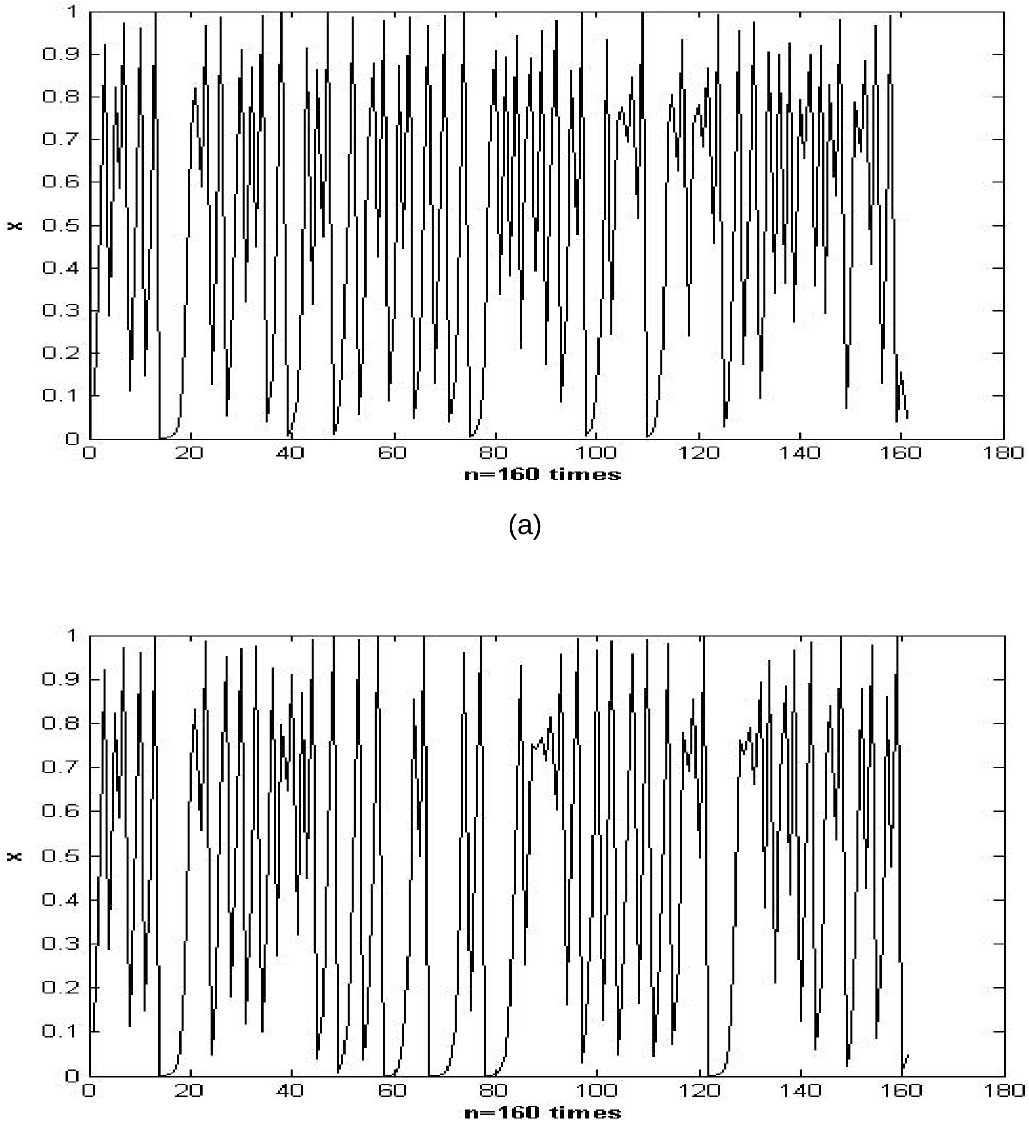
A. Logistic Map and Chebyshev Map

1. Logistic Map

Chaotic systems have been studied for more than 35 years. In 1963, Edward Lorenz discovered the first chaotic system almost by accident, while searching for equations explaining the behavior of weather patterns. Since then many methods for the analysis and synthesis of chaotic systems have been proposed. The Logistic Map is expressed as

$$x_{n+1} = \mu x_n \bullet (1 - x_n) \tag{3.1}$$

where x_n is a number such that $x_i \in (0,1)$and represents the ratio of existing population to the maximum possible population at year n. x_0 represents the initial ratio of population to maximum population (at year 0), μ is a positive number and represents a combined rate for reproduction and starvation. When $3.5699456 < \mu \leq 4,$ Logistic map into the chaotic state.



(a)

(b)

Figure 3.1: Chaotic system (a) Logistic map1 (b) Logistic map2

Two result are shown when $x_0 = 0.10000000$ and $x_0{}' = 0.10000001, \mu = 4$, n is 160. When $k = 27$, that is $x_{27} = 0.053742$ and $x_{27}{}' = 0.95307$. The map generated at the above given parameters is shown in Figure 3.1 (a) and (b). From the figure, it is clear that the generated map has good initial value sensitivity and the long-term unpredictability.

2. Chebyshev Map

The Chebyshev map is another useful method of one-dimensional chaotic map, the Chebyshev map is written as:

$$x_{n+1} = \cos(k \bullet \arccos(x_n)) \qquad (3.2)$$

where $n = N$, the defined interval of $x_i \in (-1,1)$. Here, we set $x_i \in (0,1)$, the value of k should larger than 5, when $k > 5$, Chebyshev map is in the chaotic state.

B. Combination of Logistic Map and Chebyshev Map

The Logistic map and Chebyshev map separately have good initial value sensitivity and the long-term unpredictability, however the invalid-key and the quasi invalid-keys also exists in the Logistic map. If we use the invalid-keys or the quasi invalid-keys as the initial value of the Logistic map, we can't get the chaotic sequence to scramble the digital images. Furthermore, there are infinite invalid-keys and quasi invalid-keys in the Logistic map.

1. The Invalid-Keys

If set $x_0 = 1 - \frac{1}{\mu}$ and input it into the system of Logistic map. We get $x_i = 1 - \frac{1}{\mu}, i = 0,1,2,.....$ Here x_i is called invalid-key with 1 cycle. Now, $x_k = x_0$

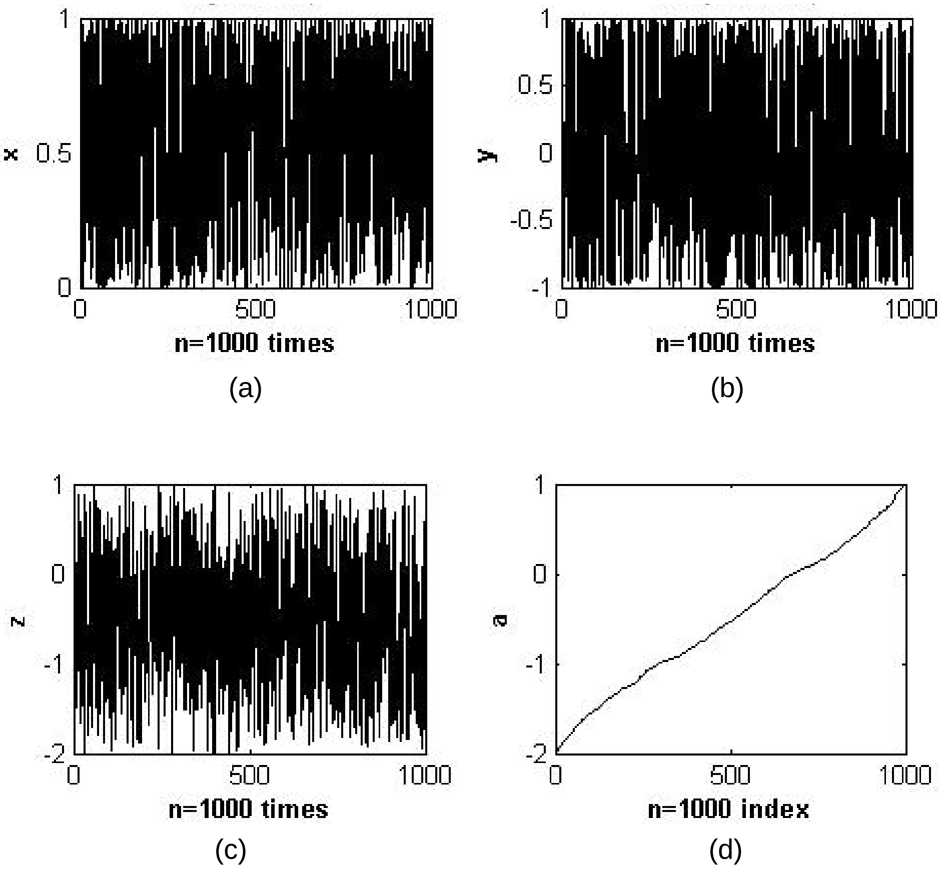
and $x_{n+k} = x_{n,(n=0,1,2,......)}$ is called invalid-key with cycle is k. The Logistic map has key as many as k. Thus it cannot be used in scrambling.

2. The Quasi Invalid-Keys

Let set $x^{\langle k \rangle}$ as invalid-key with k cycles and get the equation: $x^{(k)} = f(x)$. If x satisfies the equation then it is the invalid-key. For example, if $x^{(k)} = 0.25$, $x = 1 - x^{(k)} = 0.75$, the value 0.25 is invalid-key and 0.75 is quasi invalid-key with cycle of 1. The sequence of Logistic map will be 0.75, 0.25. Thus we can say that this key cannot be used to scramble the secret image [14].

3. Combination of Logistic Map and Chebyshev Map

Logistic map comes with the advantages of high-level efficiency and simplicity. However some weakness also exists in this method. when we only using the Logistic map to encrypt the secret image, the receiver use same key to decrypt the secret image, but in the recovered image has some noises, because in the sequence of Logistic map has same values, so the position of some blocks can not change back their original position. In this paper, this propose the method based on the combination of Logistic map and Chebyshev map to scramble and encrypt the secret image blocks. Since the difference between Chebyshev map and the Logistic map in the expressions structure is big, the probability of their invalid-key and the quasi invalid-keys is minimal. It is shown in Figure 3.2, (a) is the Logistic map, (b) is Chebyshev map, (c) is combination of Logistic map and Chebyshev map. The running times n=1000.



(a)

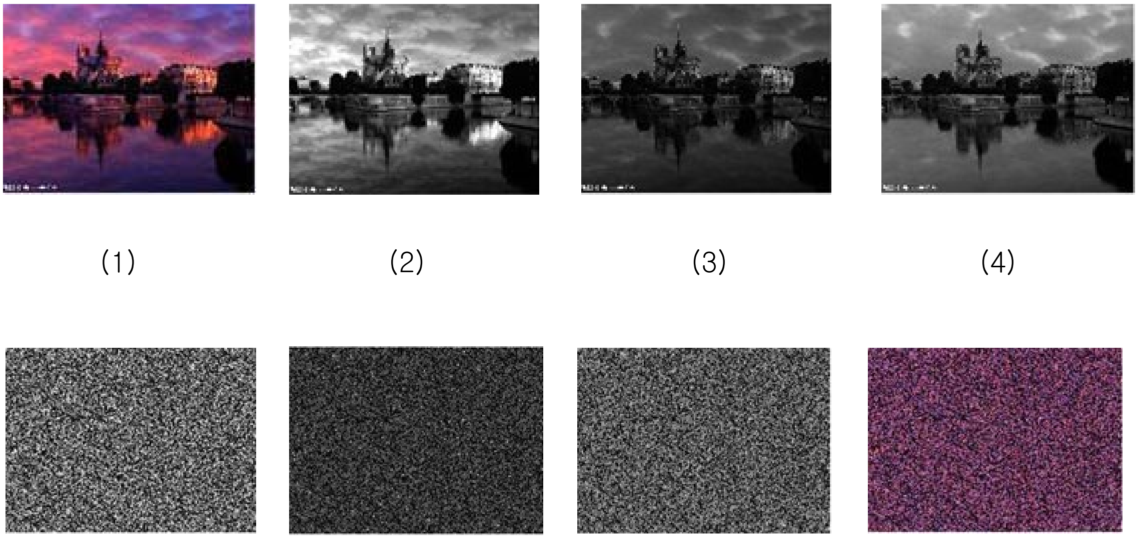
(b)

(c)

(d)

Figure 3.2: Combination of Logistic map and Chebyshev map, (a) Logistic map, (b) is Chebyshev map, (c) is combination of Logistic map and Chebyshev map, (d) sorted map in ascending order.

Since x_n is a number between zero and one in Logistic map and Chebyshev map the probability of reoccurrence of the difference between Logistic map and Chebyshev map in the new sequence is very small. Thus in this paper a method to find difference between Logistic map and Chebyshev map is proposed. In the proposed method first, the scrambling sequence of Logistic map $q_1, q_2, q_3, ...$ and sequence of Chebyshev map $Q_1, Q_2, Q_3, ...$ are created. Next the difference between these sequences is calculated. Now, the new sequence is $q_1 - Q_1, q_2 - Q_2, q_3 - Q_3, ...$ that is combination of Logistic map and Chebyshev map. The method of combination of Logistic map and Chebyshev map is not only to find difference between two sequences but also to insert with each other: $q_1, Q_1, q_2, Q_2, q_3, Q_3, ...$[13] and so on. In the proposed method, using difference between Logistic map and Chebyshev map. Figure 3.3 is the secret image using combination of Logistic map and Chebyshev map,



(1) (2) (3) (4)

(5) (6) (7) (8)

Figure 3.3: The result Image using combination map (1)-(4) are the secret images with RGB three color channels, (5)-(8) are the image encrypted by combination map using different key in three color channels.

Ⅳ. Color Transfer Technology

In this chapter, we will describe the concept of color transfer and introduce different types of color transfer algorithms and summarize the advantages and disadvantages of these algorithms. Color transfer is a process of color alteration that changes image color to accord with another image color characteristics making the image having similar color with original image. In fact, the color transfer can be expressed as a transformation such that $C(x,y) = T(f(x,y))$, where $f(x,y)$ is the source image and $C(x,y)$ is the transformed image. Reinhard et al. [15] proposed a simple but very successful technique that transfers color characteristics from a source to a target image. This technique works on orthogonal color space without correlations between the axes. The strong correlation exists in RGB color space between the three channels values. Most pixels have large values for the red and green channel, if the blue channel is large. This implies that if we want to change the appearance of a pixel's color in a coherent way, we must modify all color channels in tandem. This complicates any color modification process. However most of the existing display devices visualize three dimensional color space based on Red, Green and Blue channels generally called the RGB color pace. Thus, the color in other color spaces should be converted to RGB color space to visualize the real object.

A. Color Space

1. RGB Color Space

This is an additive color system based on tri-chromatic theory, often found in systems that use a CRT to display images. RGB is easy to implement but non-linear with visual perception. It is device dependent and specification of colors is semi-intuitive. RGB is very common. This is shown in Figure 4.1.

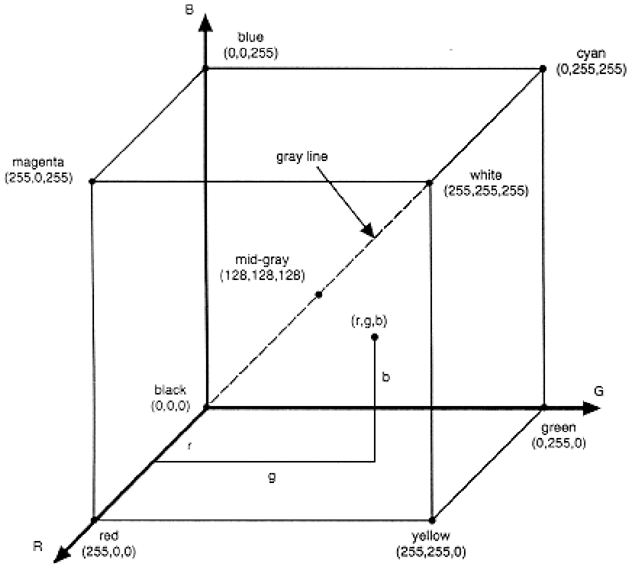


Figure 4.1: RGB Color Space

2. $l\alpha\beta$ Space

In 1998, Ruderman et al. [17] introduced a crucial color space called $l\alpha\beta$ color space. This space minimizes correlation between channels for many natural scenes based on data-driven human perception research that assumes the human visual system is ideally suited for processing natural scenes. In this space, l denotes changes in radiance and the other two are reminiscent of the blue-yellow and red-green chromatic. There is little correlation between the axes in $l\alpha\beta$ space. We can apply different operations in different channels with some confidence that undesirable cross-channel artifacts will not occur. Correlation diagrams in the logarithmic space for $l-\alpha, l-\beta$, and $\alpha-\beta$ as shown in Figure 4.2.

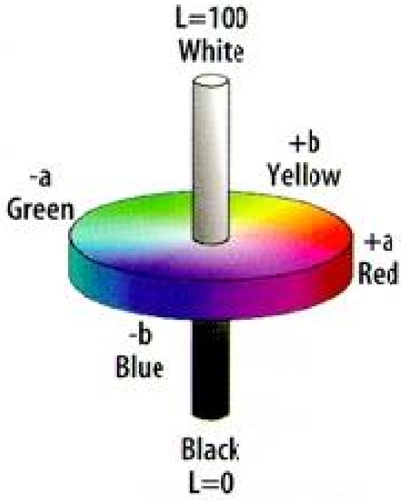


Figure 4.2: $l\alpha\beta$ Space

3. Color Space Conversion

The process of transformation from RGB to $l\alpha\beta$:

- Conversion of the image from RGB to LMS space can be achieved in two steps. First, conversion from RGB to XYZ tristimulus values is performed. Then in second step these values are converted to LMS space. This is shown in Eq. (4.1), and Eq. (4.2).

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = \begin{bmatrix} 0.5141 & 0.3239 & 0.1604 \\ 0.2651 & 0.6702 & 0.0641 \\ 0.0241 & 0.1228 & 0.8444 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{4.1}$$

$$\begin{bmatrix} L \\ M \\ S \end{bmatrix} = \begin{bmatrix} 0.3897 & 0.6890 & -0.0787 \\ -0.2298 & 1.1834 & 0.0464 \\ 0.0000 & 0.0000 & 1.0000 \end{bmatrix} \begin{bmatrix} X \\ Y \\ Z \end{bmatrix} \tag{4.2}$$

- Combination of these two matrices gives the transformation of RGB to LMS cone space [18].

$$\begin{bmatrix} L \\ M \\ S \end{bmatrix} = \begin{bmatrix} 0.3811 & 0.5783 & 0.0402 \\ 0.1967 & 0.7244 & 0.0782 \\ 0.0241 & 0.1288 & 0.8444 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{4.3}$$

- The data in this color space shows a great deal of skew, which can be largely eliminated by converting the data into logarithmic space [17].

$$\begin{aligned} L' &= \log L \\ M' &= \log M \\ S' &= \log S \end{aligned} \tag{4.4}$$

- After converting the data to logarithmic space, the following matrix multiplications can be used to convert LMS color space to color space.

$$\begin{bmatrix} l \\ \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{3}} & 0 & 0 \\ 0 & \frac{1}{\sqrt{6}} & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & -2 \\ 1 & -1 & 0 \end{bmatrix} \begin{bmatrix} L' \\ M' \\ S' \end{bmatrix} \tag{4.5}$$

- After color processing, we must transfer the result back to RGB to display it. We convert from to using this matrix multiplication:

$$\begin{bmatrix} L' \\ M' \\ S' \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & -1 \\ 1 & -2 & 0 \end{bmatrix} \begin{bmatrix} \frac{\sqrt{3}}{3} & 0 & 0 \\ 0 & \frac{\sqrt{6}}{6} & 0 \\ 0 & 0 & \frac{\sqrt{2}}{2} \end{bmatrix} \begin{bmatrix} l \\ \alpha \\ \beta \end{bmatrix} \tag{4.6}$$

- After raising pixel values to the power ten, conversion from to color space can be obtained by

$$\begin{aligned} L &= 10^{L'} \\ M &= 10^{M'} \\ S &= 10^{S'} \end{aligned} \tag{4.7}$$

- Converting the data from logarithmic space to Linear space LMS

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 4.4679 & -3.5873 & 0.1193 \\ -1.2186 & 2.3809 & -0.1624 \\ 0.0497 & -0.2439 & 1.2045 \end{bmatrix} \begin{bmatrix} L \\ M \\ S \end{bmatrix} \tag{4.8}$$

B. Color Transfer Algorithm

Recently, there was an important work in color transfer proposed by Xue Zhong Xial et al. [19] This method focuses on manipulating directly images color in RGB space. All documents of color transfer algorithms is based on the $l\alpha\beta$ color space, because of the correlations between the three channels values in RGB color space, they transform pixels' values from RGB to $l\alpha\beta$ color space. they transform pixels' values from RGB to $l\alpha\beta$ color space, and then manipulate them separately, and finally return to RGB color space. So the following we will describe the Reinhard etal algorithm and Xue Zhon et al algorithm.

1. Color Transfer In De-correlated Color Space

The color transfer algorithm is based on statistical analysis. One images color characteristics can be imposed on another by transferring the mean and standard deviation values. This straightforward operation can produce surprisingly good output images for suitable source images. Thus the algorithm is suitable for natural image.

The algorithm includes 3 stages of operations:

- Transformation from RGB color space to color space of target image and secret image.
- Respectively compute the means and standard deviations of each of the channels of target image and secret image by the following formulas:

$$\mu_c = \frac{1}{n}\sum_{i=1}^{n} c_i \ , \ \mu'_c = \frac{1}{n}\sum_{i=1}^{n} c'_i \tag{4.9}$$

$$\sigma_c = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(c_i - \mu_c)^2} \ , \sigma'_c = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(c'_i - \mu'_i)^2} \tag{4.10}$$

where $\mu_l,\mu_\alpha,\mu_\beta$, $\sigma_l,\sigma_\alpha,\sigma_\beta$, $\mu'_l,\mu'_\alpha,\mu_\beta'$ and $\sigma'_l,\sigma'_\alpha,\sigma'_\beta$ denote the mean and standard deviation of the source and target image.

$$
\begin{aligned}
l^{*}_{target} &= \frac{\sigma^{l}_{target}}{\sigma^{l}_{source}}\left(l_{source} - \bar{l}_{\ source}\right) + \bar{l}_{\ target} \\
\alpha^{*}_{target} &= \frac{\sigma^{\alpha}_{target}}{\sigma^{\alpha}_{source}}\left(\alpha_{source} - \bar{\alpha}_{\ source}\right) + \bar{\alpha}_{\ target} \\
\beta^{*}_{target} &= \frac{\sigma^{\beta}_{target}}{\sigma^{\beta}_{source}}\left(\beta_{source} - \bar{\beta}_{\ source}\right) + \bar{\beta}_{\ target}
\end{aligned}
\tag{4.11}
$$

After the color transformation, we must transfer the result back to RGB to display it, the equations is shown in Eq. (4.6) ~ (4.8). This is one example of Rein hard color transfer algorithm:

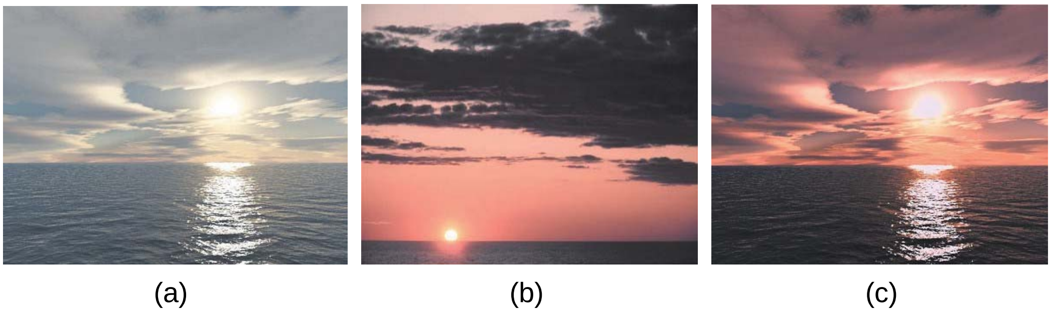


Figure 4.3: color transfer based on Reinhard model (a) target image (b) source image (c) color processed result image

This algorithm is suitable for nature image but not for images with big gap between different chromaticity.

2. Color Transfer In Correlated Color Space

Xue zhong Xiao et al.[19] proposed a method that can transform color from source image to target image directly in RGB color space or any 3D space. Their method based on the geometrical transformations, SVD and covariance. We first introduce the geometrical transformations and SVD decomposition.

A. Geometrical transformations

The translation, scaling, and rotation transformations are essential to many graphics application Since the RGB space is 3D space, the translation in 3D is a simple extension from that in 2D:

$$T(d_x, d_y, d_z) = \begin{bmatrix} 1 & 0 & 0 & d_x \\ 0 & 1 & 0 & d_y \\ 0 & 0 & 1 & d_z \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{4.12}$$

where d is unit parallel to the x axis or y,z axis. Similarly the scaling is also extended as

$$S(s_x, s_y, s_z) = \begin{bmatrix} s_x & 0 & 0 & 0 \\ 0 & s_y & 0 & 0 \\ 0 & 0 & s_z & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{4.13}$$

where s_x, s_y, s_z are units parallel along the x axis and y,z axis. The 3D rotation about the z,$x\,\mathrm{or}\,y$ axis is:

$$R_z(\theta)=\begin{bmatrix}\cos\theta & -\sin\theta & 0 & 0\\ \sin\theta & \cos\theta & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}$$

$$R_x(\theta)=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & \cos\theta & -\sin\theta & 0\\ 0 & \sin\theta & \cos\theta & 0\\ 0 & 0 & 0 & 1\end{bmatrix} \tag{4.14}$$

$$R_y(\theta)=\begin{bmatrix}\cos\theta & 0 & \sin\theta & 0\\ 0 & 1 & 0 & 0\\ -\sin\theta & 0 & \cos\theta & 0\\ 0 & 0 & 0 & 1\end{bmatrix}$$

If we want to move the point $P_1(x,y,z)$ to point $P_2(x_1,y_1,z_1)$ by translation rotation and scaling we can use the following equation as shown

$$(x',y',z',1)^T = T(x_1,y_1,z_1,1)\times R(\theta)\times S(s_x,s_y,s_z,1)\times T(-x,-y,-z,1) \tag{4.15}$$

B. SVD decomposition

The singular value decomposition (SVD) is one of the widely useful decompositions. The factorization of a matrix A into the product $U\Sigma V^T$ of a unitary matrix U, a diagonal matrix Σ and another unitary matrix V^T. One of the most important features of the SVD is its use of orthogonal matrices. The columns of U are perpendicular to each other and have unit length. The matrix U is orthogonal matrix having multiple rows as A. The matrix V is orthogonal and has as multiple columns same as A. Σ is of the same size as A, however its nonzero elements are on the main diagonal. The diagonal elements of Σ are the singular values and the columns of U and V are the left and right singular vectors. We should note that the image of the unit sphere under any $m \times n$ matrix multiplication is an ellipse. Figure. 4.4 shows the geometrical meaning of SVD.

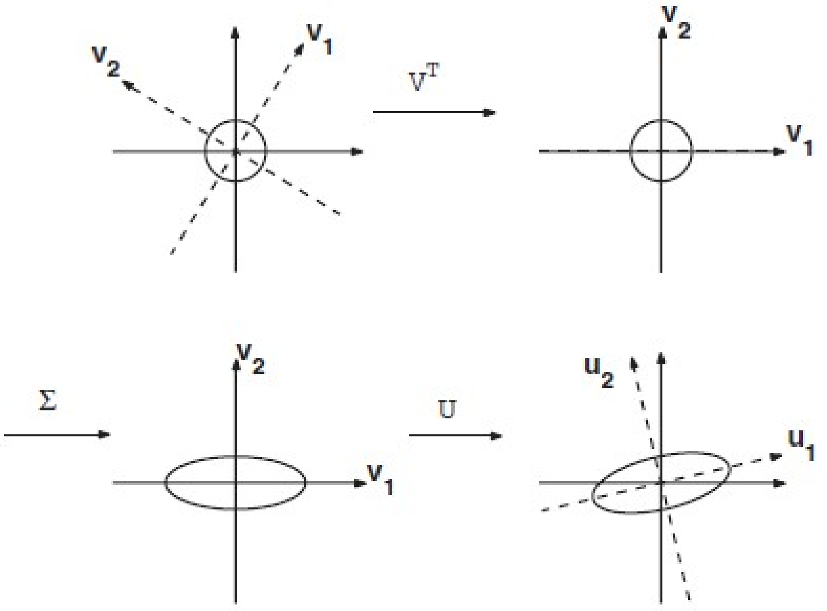


Figure 4.4: Geometrical Representation of SVD

where the V^T is a pure rotation of the circle and the circle is stretched by Σ in the directions of the coordinate axes to form an ellipse. U is a pure rotation of the ellipse into its final position. Thus U and V^T can rotate and scale the ellipse of color space of one image as similar as other ellipse of color space to make the image has similar look and feel. For decomposing the matrix of covariance, the orthonormal columns of and V^T is same.

The algorithm includes 3 stages of operations:

- Obtain the covariance between three components of pixel values and calculate the mean along each of the three axes.

$$\overline{X_i} = \frac{1}{N}\sum_{n=1}^{N} X_{in} \tag{4.16}$$

$$\sigma^2\{X_i\} = \frac{1}{N}\sum_{n=1}^{N}\left(X_{in} - \overline{X_i}\right)^2 \qquad i \in \{r,\, g,\, b\} \tag{4.17}$$

$$\sigma\{X_i, X_j\} = \frac{1}{N}\sum_{n=1}^{N}\left(X_{in} - \overline{X_i}\right)\left(X_{jn} - \overline{X_j}\right) \qquad i,j \in \{r,\, g,\, b\},\, i \neq j \tag{4.18}$$

$$Cov = \begin{bmatrix} \sigma^2\{X_r\} & \sigma\{X_r, X_g\} & \sigma\{X_r, X_b\} \\ \sigma\{X_g, X_r\} & \sigma^2\{X_g\} & \sigma\{X_g, X_b\} \\ \sigma\{X_{b,} X_r\} & \sigma\{X_b, X_g\} & \sigma^2\{X_b\} \end{bmatrix} \tag{4.19}$$

where $\overline{X_i}$ is the mean of target image and source image in three color channels, $i \in \{r, g, b\}$, N is the number of pixels in one block.

- Decompose the covariance matrix using SVD algorithm [22] and get a rotation matrix.

$$Cov = U \bullet \Sigma \bullet V^T \tag{4.20}$$

- Scale, rotate and shift pixel data of target image to fit data points cluster of source image in the current color space and get the resultant image which takes on source image's look and feel.

$$I = T_{src} \bullet R_{src} \bullet S_{src} \bullet S_{tgt} \bullet R_{tgt} \bullet T_{tgt} \bullet I_{tgt} \tag{4.21}$$

where $t^r_{src} = \overline{R}_{src},\ t^g_{src} = \overline{G}_{src}, t^b_{src} = \overline{B}_{src},\ t^r_{tgt} =- \overline{R}_{tgt}, t^g_{tgt} =- \overline{G}_{tgt}, t^b_{tgt} =- \overline{B}_{tgt}$

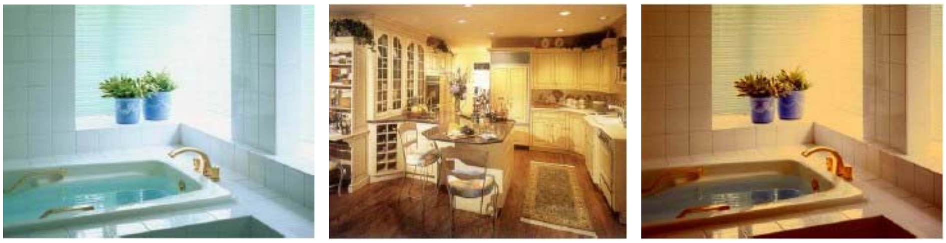
$$T_{src} = \begin{bmatrix} 1 & 0 & 0 & t_{src}^{r} \\ 0 & 1 & 0 & t_{src}^{g} \\ 0 & 0 & 1 & t_{src}^{b} \\ 0 & 0 & 0 & 1 \end{bmatrix}, T_{tgt} = \begin{bmatrix} 1 & 0 & 0 & t_{tgt}^{r} \\ 0 & 1 & 0 & t_{tgt}^{g} \\ 0 & 0 & 1 & t_{tgt}^{b} \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$R_{src} = U_{src}, R_{tgt} = U_{tgt}^{-1} \tag{4.22}$$

$$S_{src} = \begin{bmatrix} s_{src}^{r} & 0 & 0 & 0 \\ 0 & s_{src}^{g} & 0 & 0 \\ 0 & 0 & s_{src}^{b} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, S_{tgt} = \begin{bmatrix} s_{tgt}^{r} & 0 & 0 & 0 \\ 0 & s_{tgt}^{g} & 0 & 0 \\ 0 & 0 & s_{tgt}^{b} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$s_{src}^{r} = \lambda_{src}^{R},\ s_{src}^{g} = \lambda_{src}^{G},\ s_{src}^{b} = \lambda_{src}^{B},\ s_{tgt}^{r} = \frac{1}{\sqrt{\lambda_{tgt}^{R}}},\ s_{tgt}^{g} = \frac{1}{\sqrt{\lambda_{tgt}^{G}}},\ s_{tgt}^{b} = \frac{1}{\sqrt{\lambda_{tgt}^{B}}}$$

Here is an example of Xiao [19] color transfer algorithm



(a) (b) (c)

Figure 4.5: Color transfer based Xiao [19] Method (a) target image (b) source image (c) color processed result image

The method for borrowing one image's color characteristics from another directly in RGB color space, and has good result similar with Reinhard et al.

V. New Mosaic Image for Information

Hiding Based on Mixed Chaotic Sequences

In this chapter, we will introduce the proposed method on new computer art-information hiding via the Secret-Fragment-Visible mosaic image by color transfer in correlated color space and combination of logistic map and Chebyshev map.

In order to reduce the volume of the generated information, Li et al. [10] method performed the conversion in RGB space instead of color space. This method can produce better results. Inspired by the work of this method, we have also explored the mosaic image for information hiding. However, the proposed method is based on the color transfer in correlated color space that considers pixels value as a three dimension stochastic variable and an image block as a set of samples and chaotic systems rather than in de correlated space. The superiority of our approach is that we consider the correlation between three color channels using a series of transformations created by decomposing the covariance matrix using the SVD algorithm [21-23]. Thus the correlation of mosaic image pixel's value in three color channels has similar feel as target image. Another work in this paper is the combination of logistic map and Chebyshev map to encrypt the original secret image. The logistic map and Chebyshev map are based on sensitive dependence on their initial condition. If we just input three key to create a chaos sequence and use that chaos sequence to encrypt the secret image, these same keys can be used to create the same sequence and decrypt the secret image in the receiver end. Thus, Instead of using large number of keys for embedding the sequence of secret image blocks in mosaic image only two keys are sufficient in the proposed method.

A. Basic Idea of the Proposed Method

The proposed method consists of the following five major functional steps.

1: encrypt the blocks of secret image using proposed combination of logistic map and Chebyshev map.

2: transform the color characteristics from target image block to secret image block.

3: generate the mosaic image using secret image blocks color transformed in phase 2.

4: embed the recovery information in mosaic image for recovering secret image

5: recover the secret image by using the information embedded before.

B. Encrypt the blocks of Secret Image

The given secret image is divided into non overlapping blocks. Each block is assigned a serial number from the top-leftmost to the bottom-rightmost corner of image. In order to encrypt blocks of secret image, three keys are used as chaotic system parameter. Here and are initial condition for the combination of logistic map and Chebyshev map described in chapter 3. The Number of cycles is same set as equal number of secret image blocks. First, we compute the sequence $K_1, K_2, ...K_n$ generated by the combination of logistic map and Chebyshev map. The index of the generated sequence are well-ordered and sorted in ascending order. The old index of $K_1^{'}, K_2^{'}, ...K_n^{'}$ are recorded as the index in original sequence. Finally, the old index are used to rearrange the position of the blocks in secret image to decrypt the secret image.

Primarily, there are two advantages of this encryption system. First, the secret image is encrypted by chaotic technology which makes the secret image more secured. Next, we don't need to embed long sequence of secret image blocks in mosaic image to recover the secret image which reduces the number of bits required to generate the encrypted image. The method of combination of logistic map and Chebyshev map also can be used in the method proposed by Ya-Lin Li and Wen-Hsiang Tsai to reduce the recovery information bit.

C. Color Transformations of blocks

Color transformation of blocks is performed in following steps

- Calculate the mean and covariance matrix between the three components in blocks of secret image and target image. The given secret image and target image is divided into a set of blocks and. Each block S and T are described as set of pixels $\{s_1, s_2, ...s_n\}$ and $\{t_1, t_2, ...t_n\}$. The color of pixel in the color space is denoted by $\{r_i, g_i, b_i\}$ and by $\{r'_i, g'_i, b'_i\}$ for secret image block and target image block. The mean and covariance of S and T in each of the three color channels are described by equation (4.16 - 4.19)

- Next decompose the covariance matrices using SVD algorithm by equation (4.20) where U as a rotation matrix to manipulate pixels of the secret image, Σ as a scaling matrix and the mean matrix is as translation matrix.

D. Mosaic Image Generation

The new color values of secret image block is calculated by

$$I = T_{tgt} \bullet R_{tgt} \bullet S \bullet R_{\sec} \bullet T_{\sec} \bullet I_{\sec} \qquad (5.1)$$

It is based on the covariance decomposition and Geometrical transformation, where $I=(R,G,B,1)^T$ denote the homogeneous coordinates of pixel in RGB color space for resulting image, and $I_{\sec}=(R,G,B,1)^T$ denote for secret image. $T_{tgt}, T_{\sec}, R_{tgt}, R_{\sec}, S_{tgt}, S_{\sec}$ denote the matrices of translation, rotation and scaling derived from the target image to secret image. These are generated by decomposing the covariance matrix. The result in a new secret image block with a new color characteristic will be most similar to that of target image block. We also can use same form of that equation to recover secret image, just doing Inverse. Note that the number of λ^R is big. However λ^G and λ^B are almost close to 0. If the denominator is 0, in the MATLAB the computation will generate errors. To solve this problem, and add a decimal in the denominator.

$$T_{tgt} = \begin{bmatrix} 1 & 0 & 0 & \overline{R}_{tgt} \\ 0 & 1 & 0 & \overline{G}_{tgt} \\ 0 & 0 & 1 & \overline{B}_{tgt} \\ 0 & 0 & 0 & 1 \end{bmatrix}, T_{\sec} = \begin{bmatrix} 1 & 0 & 0 & -\overline{R}_{\sec} \\ 0 & 1 & 0 & -\overline{G}_{\sec} \\ 0 & 0 & 1 & -\overline{B}_{\sec} \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$R_{tgt} = U_{tgt}, R_{\sec} = U_{\sec}^{-1} \qquad (5.2)$$

$$S = \begin{bmatrix} S^R & 0 & 0 & 0 \\ 0 & S^G & 0 & 0 \\ 0 & 0 & S^B & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\textit{where} \quad S^i = \sqrt{\lambda_{tgt}^i} \Big/ \lambda_{\sec}^i, \quad i \in \{R,G,B\} \tag{5.3}$$

E. Embedding the Recovery Information

In order to recover the secret image from mosaic image, we should embed some information about secret image in mosaic image. The information required to recover secret image block mapped to target block includes the rotation and scaling is performed on the 3×3 matrix which is created by decomposing the covariance matrices and the overflow/underflow residual values. In the matrices of rotation and scaling, every elements are different. Hence for one block we should use more than 200 bit for embedding the elements of rotation and scaling matrices of secret image and target image. It is not good for directly embedding them in mosaic image. We know that value of the element in covariance matrix is not small. It is not a good idea for reduce the embedding information. For this, we set and compute the equation described above

$$a = T_{tgt} \bullet R_{tgt} \bullet S \bullet R_{\sec} \bullet T_{\sec} \tag{5.4}$$

$$a_{ij} = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{5.5}$$

where a is 4×4 matrix described in Eq. (5.5). Since a_{ij} is closed to 0 while $i,j \in 1,2,3$, only a_{14}, a_{24}, a_{34} are within the range of {0, 255}. In order to recover the secret image is most similar to original secret image, we use 8 bits to represent a_{ij} $i,j \in 1,2,3$, and use 10 bits to represent the values of

a_{14}, a_{24}, a_{34} because we don't need to embed the sequence for secret image in mosaic image, so we can embed more information about a matrix for secret image recovery. Thus we embed the elements of a in mosaic image to recover the original secret image. For one block, the bit segments M_i are encoded in data items of matrix as described before. We concatenate the bit stream as the recovery information for secret image in a raster-scan order to form a total bit stream M for all the each pair secret image block and target image block. In order to protect form being attacked, we encrypt it with a secret key to obtain an encrypted bit stream M'. Here, we use a technique of reversible contrast mapping proposed by Coltuc and Chassery [24-25]. Now we setup the key of Chaotic map, which decompose the user password into encryption keys, x_0, μ, k.

Thus we don’t need to embed key of chaotic map in mosaic image. even thoght the attacker intercept the mosaic image, and they also can extract a part of the information for secret image recovery, but without same three keys, the secret image can not be read.

F. The secret Image Recovery algorithm

1. Extraction of the Information

When the receiver receives the mosaic image created using the secret image, the receiver recovers the secret image from the mosaic image using the relevant recovery information of secret image.

In the proposed method, the receiver extracts the recovery information M' first from mosaic image for secret image recovery process using a reverse version of the method [24-25] and decrypts M' using secret key into non-encrypted version M the bit stream M is the original bit stream of matrix a.

Next, M is decomposed into n bit streams M_i. Here n is the number of bits represented for a matrix and i is the i_{th} bit stream for $i=1,2,....n$. Bit stream M_i includes the elements of matrix a. The bit steam M_i of each block image is decoded to obtain the following data: (a) the value of a_{ij} $i,j \in 1,2,3$ (b) the value of a_{14}, a_{24}, a_{34}.

2. Secret Image Recovery

The recovery information a_{ij} is obtained first. We know that the mosaic image pixels is obtained by the matrix multiplication of translation matrix, rotation matrix scaling matrix of target image with the translation, rotation and scaling matrix of secret image. Thus the inverse matrix multiplication is applied to recover the pixels of secret image as in Eq. (5.6) and (5.7). which can be simply represented by

$$Y = A \cdot X \qquad \Rightarrow X = A^{-1} \cdot Y$$

$$a = A \cdot B \quad , a^{-1} = (AB)^{-1} \quad , b = B^{-1} \cdot A^{-1} \quad \Leftrightarrow a = b$$

$$I_{mosaic} = T_{tgt} \cdot R_{tgt} \cdot S_{tgt} \cdot S_{\sec} \cdot R_{\sec} \cdot T_{\sec} \cdot I_{\sec}$$

$$I_{\sec} = T_{\sec}^{-1} \cdot R_{\sec}^{-1} \cdot S_{\sec}^{-1} \cdot S_{tgt}^{-1} \cdot R_{tgt}^{-1} \cdot T_{tgt}^{-1} \cdot I_{mosaic} \tag{5.6}$$

$$set \quad a = T_{tgt} \cdot R_{tgt} \cdot S_{tgt} \cdot S_{\sec} \cdot R_{\sec} \cdot T_{\sec}$$

$$I_{mosaic} = a \cdot I_{\sec} \qquad \Leftrightarrow I_{\sec} = a^{-1} \cdot I_{mosaic}$$

$$I_{\sec} = a^{-1} \bullet I_{mosaic} \tag{5.7}$$

Then, decompose the password to obtain the key of chaotic map. Figure.5.1 shows an example of the result of applying this scheme to the secret image and target image, respectively. The mosaic image and recovered secret image are created by the method describe above. The image size are 1024*768 and we use the block size of 8*8. Figures 5.1(a)-(d) show the secret image and three color channels. Figures 5.1(e)-(h) show the secret image and three color channels encrypted by combination of Logistic map and Chebyshev map. Similarly, Figures 5.1(i)-(j) are secret image encrypted and target image. Figures 5.1(k)-(l) show the mosaic image and recovered secret image. The mosaic image has high similarities to target image. Figures 5.1(m)-(o) show the three color channel of recovered image that have same feel with original secret image.

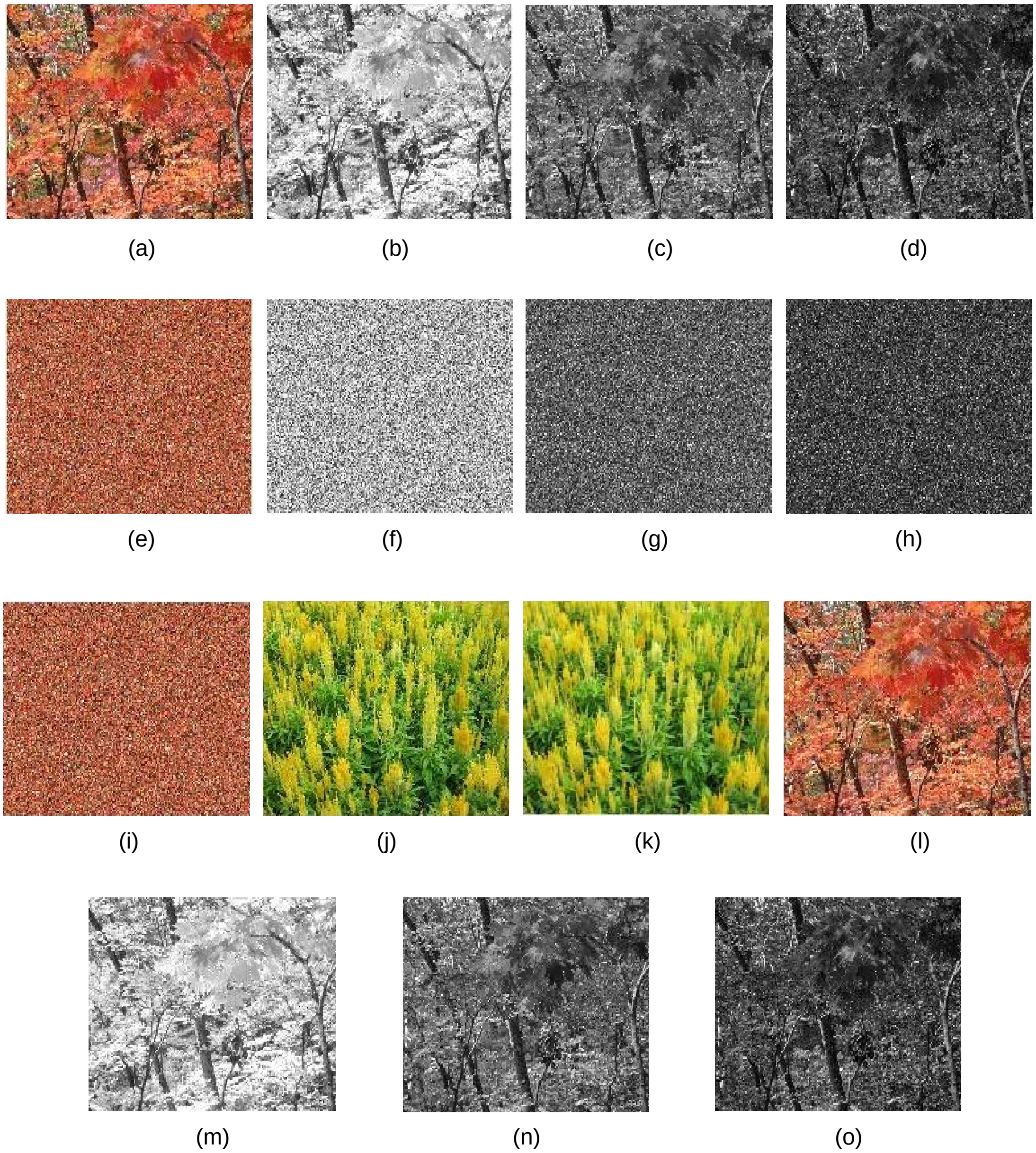
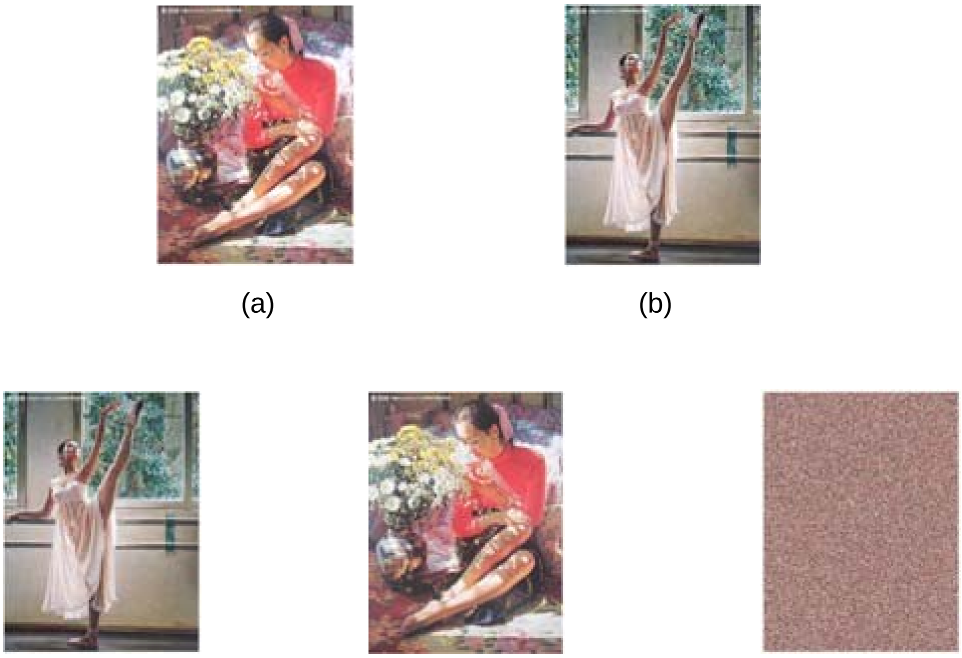


Figure. 5.1: Result yielded by proposed method (a) Original secret image (b) R color channel (c) G color channel (d) B color channel (e) Encrypted secret image (f) Encrypted R (g) Encrypted G (h) Encrypted B (i) Encrypted secret image (j) target image (k) mosaic image (l) recovered image (m) Recovered R channel (n) G channel (o) B channel.

VI. Experimental Results

Some experimental results are presented in this section. Experiments were preformed on 1024×768 image of different classes. The size of block N was set to 8. The performance of proposed algorithm is evaluated in both objective and subjective qualities. Peak Signal to noise ratio and RMSE is used to measure the objective quality. Two different experiments are performed separately. First, the mosaic image created and tested with the correct and wrong keys. Figures 6.1(a - e) show the experimental results.



(a) (b)

(c) (d) (e)

Figure 6.1: Experimental results of the proposed method (a) Secret Image (b) Target Image (c) Mosaic Image (d) Recovered Image with correct key (e) Recovered Image with wrong key

Second, the mosaic image are generated, embedded with recovery information and finally recovered. The quality of mosaic image and recovered image is tested in terms of both subjective and objective quality. We compared the result of the proposed method with Li [10] method. Figures 6.2-6.6 show the comparison of mosaic image and recovered image generated by the proposed method and the L method. Table 6.1 show the RMSE and PSNR values of recovered secret images and RMSE of mosaic image before and after embedding the recovery information of Figures 6.2-6.6.

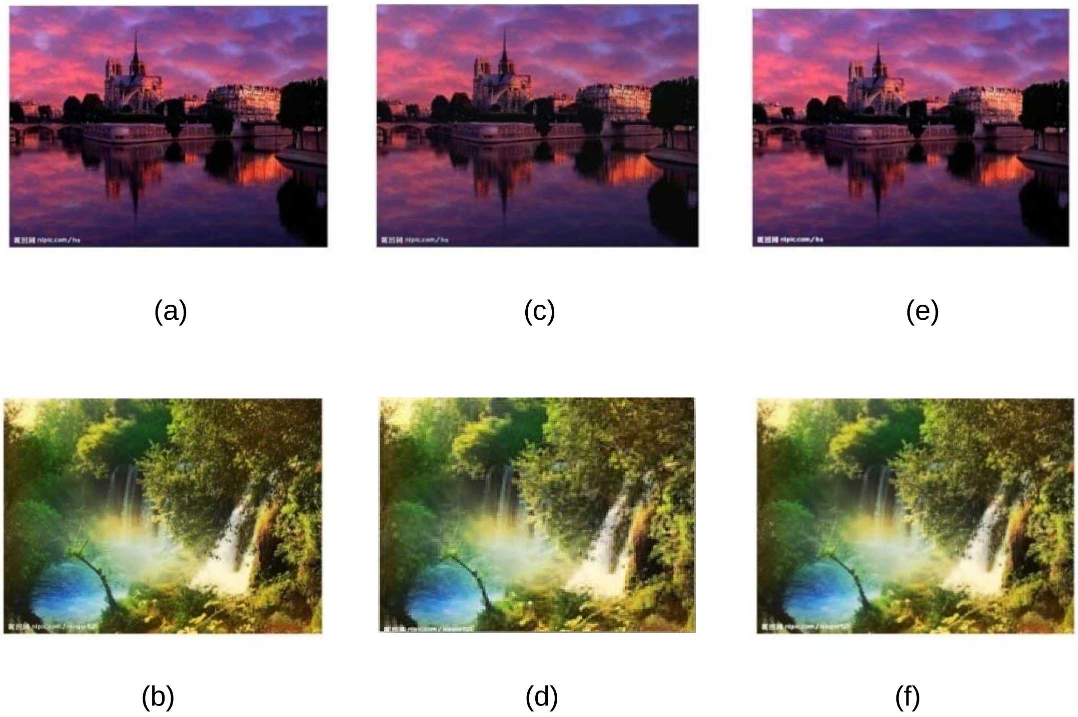


Figure 6.2: Comparison of results of Li Method and the proposed method. (a) Secret Image (b) Target Image (c) and (d) are recovered secret image by proposed (e) and (f) are recovered secret image and mosaic image by Li method

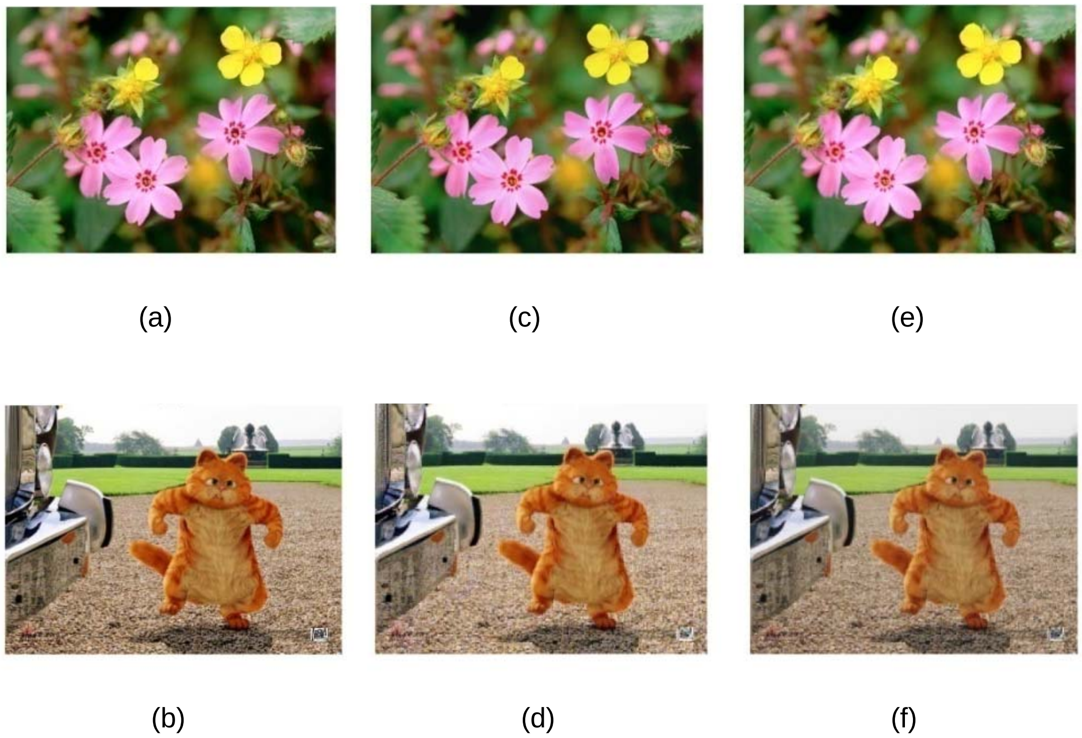


Figure 6.3: Comparison of results of Li Method and the proposed method. (a) Secret Image (b) Target Image (c) and (d) are recovered secret image by proposed (e) and (f) are recovered secret image and mosaic image by Li method

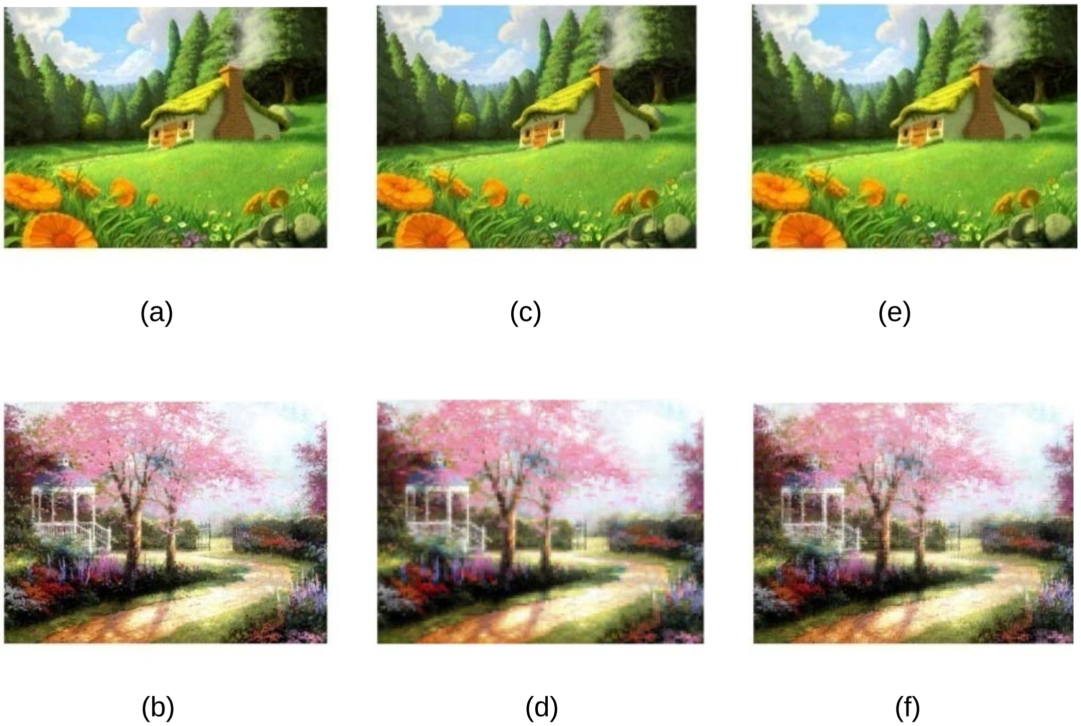


Figure 6.4: Comparison of results of Li Method and the proposed method (a) Secret Image (b) Target Image (c) and (d) are recovered secret image by proposed (e) and (f) are recovered secret image and mosaic image by Li method

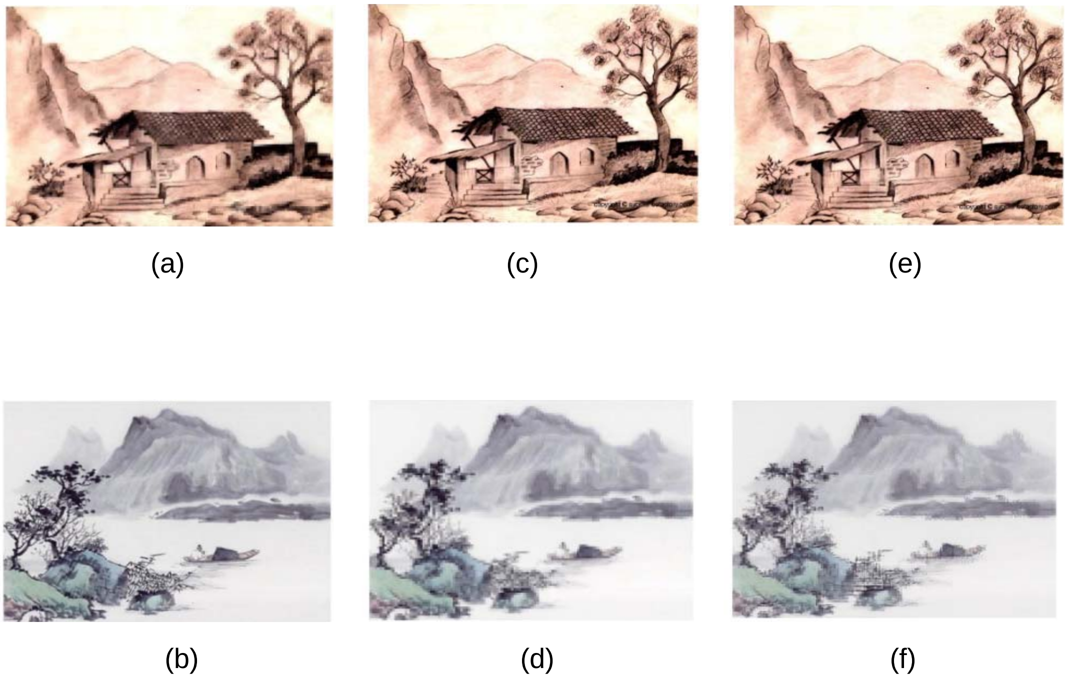


Figure 6.5: Comparison of results of Li et al. and the proposed method.(a) Secret Image (b) Target Image (c) and (d) are recovered secret image by proposed (e) and (f) are recovered secret image and mosaic image by Li method

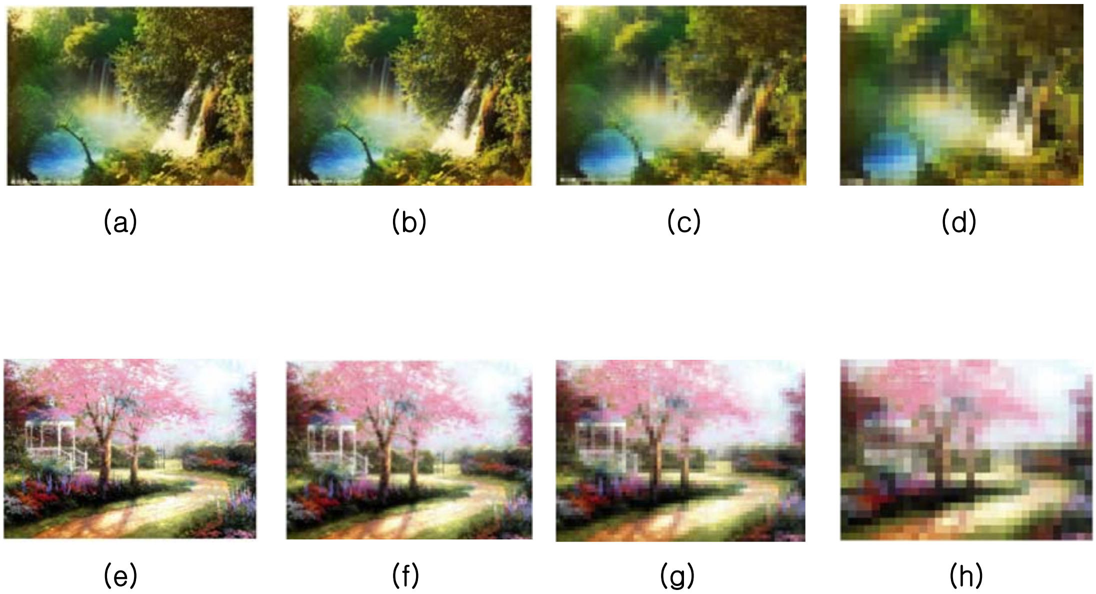
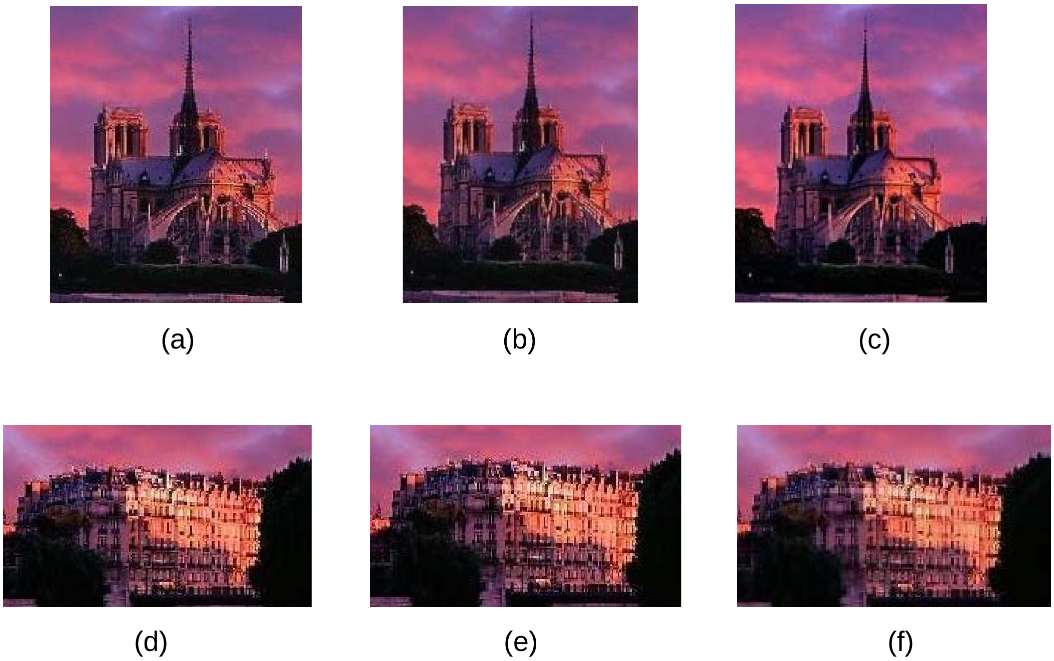


Figure 6.6: The Mosaic image by different block size, 4x4, 8x8, 16x16, 32x32, the mosaic image (a) and (e) are created by 4x4 secret image block, (b) and (f) are created by 8x8, (c) and (g) are created by 16x16, (d) and (h) are created by 32x32.

The Figure 6.6 show the created mosaic image for different block size. It can be seen from the figures that the created mosaic image retains more details of the similar ay-mosaic images created with smaller blocks image sizes have smaller RMSE values with respect to the target image. However, when the block size is large (32x32), the created mosaic image still looks quite similar to the target image. The number of bits required to embed for recovering the secret image is increased when the blocks size is smaller.



(a) (b) (c)

(d) (e) (f)

Figure 6.7: Comparison of Image detail of Ya-Lin Li et al. and the proposed method. (b), (e) and (h) are image detail information of proposed method. (c), (f) and (i) are the image detail information of method proposed by Ya-Lin Li et al.

Table 6.1: Competitive Results.

RMSE – Recovered Secret Image						
Method	Fig. 5.1	Fig. 6.1	Fig. 6.2	Fig.6.3	Fig. 6.4	Fig. 6.5
Proposed	0.6559	0.7183	0.7411	0.5477	0.6070	0.5361
Li [10]	0.8270	0.9482	0.9591	1.1051	1.0537	0.8507

(a)

PSNR – Recovered Secret Image						
Method	Fig. 5.1	Fig. 6.1	Fig. 6.2	Fig.6.3	Fig. 6.4	Fig. 6.5
Proposed	51.9255	51.3068	50.7387	53.5928	53.0193	53.5956
Li [10]	49.7806	48.5946	48.4632	46.6241	47.8889	49.2563

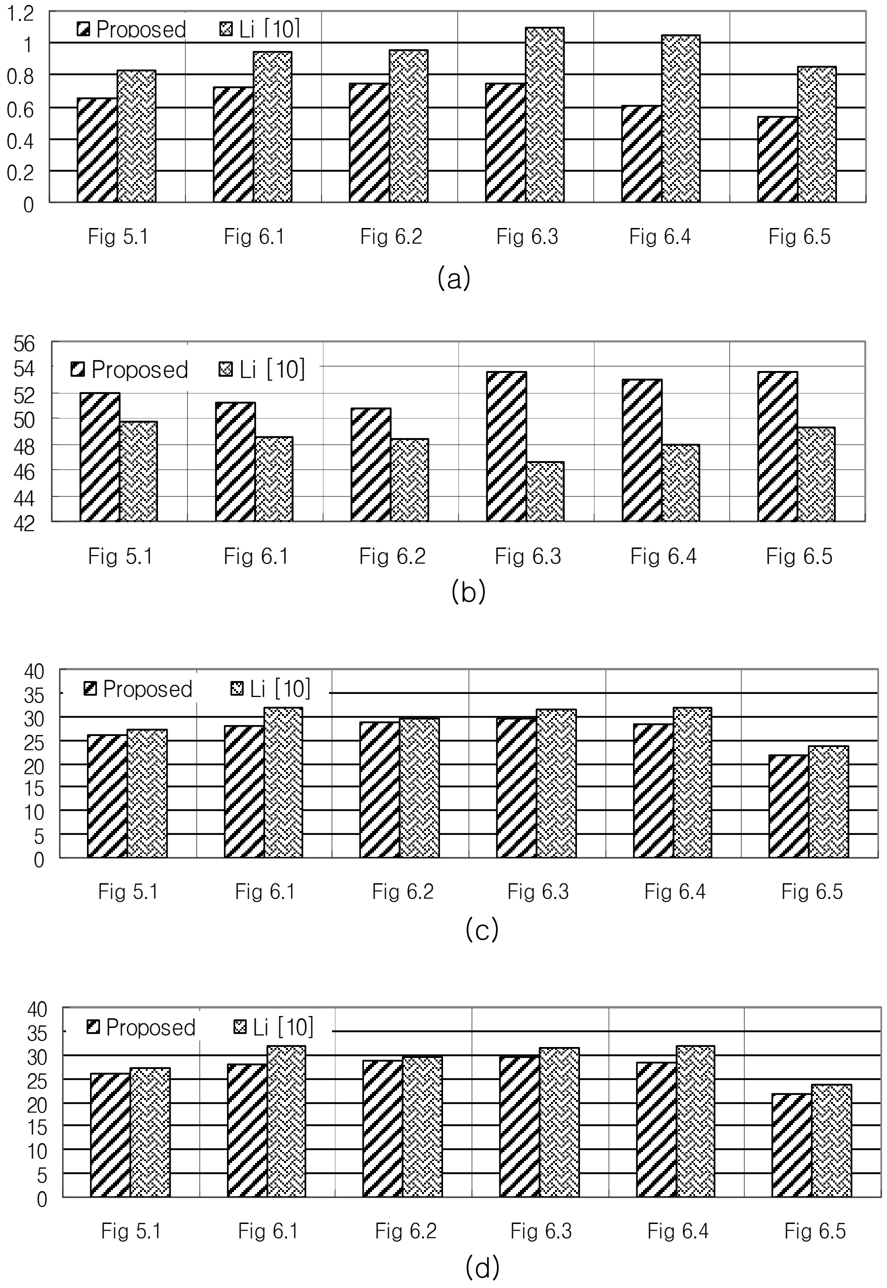
(b)

RMSE – Mosaic Image before embedding with target image						
Method	Fig. 5.1	Fig. 6.1	Fig. 6.2	Fig.6.3	Fig. 6.4	Fig. 6.5
Proposed	25.8560	27.7974	28.6410	29.6162	28.5033	21.7697
Li [10]	27.0415	31.8927	29.6362	31.5381	31.7624	23.5073

(c)

RMSE – Mosaic Image after embedding with target image						
Method	Fig. 5.1	Fig. 6.1	Fig. 6.2	Fig.6.3	Fig. 6.4	Fig. 6.5
Proposed	25.8578	27.8054	28.6472	29.6219	28.5091	21.7953
Li [10]	27.0469	31.8975	29.6418	31.5441	31.7675	23.5137

(d)



(a)

(b)

(c)

(d)

Figure 6.8: Graphical Comparison in terms of RMSE and PSNR obtained from (a) RMSE of recovered secret image (b) the PSNR of recovered image (c) the RMSE of mosaic image

VII. Conclusion

The Contribution we made in information hiding in this carried research were presented in chapter three. We developed a new sequence of encryption using a combination of logistic map and chebysev map. Then we proposed color transform from target image block to secret image. We analysed and efficiency of the proposed algorithm and presented the analytical and experimental results to revel the better performance they owned in comparison to legacy one.

In the first proposition, we discussed and proposed the new Choatic system with one dimensional Logistic map and Chaotic map. Because of intial value sensitivity and chaotic map long term predictability of chaotic behaviour the difference between these two maps were used for encryption sequence generation.

In the second proposition, a new color transfer technique for the mosaic image generation was proposed. We verified the efficiency of covariance SVD based color transfer technique for mosaic image generation through test in wide range of images. The key idea is to measure the correlation between color spaces and use it for the color transfer which we achieved by studying the covariance through SVD algorithm.

References

[1] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn, “Information Hiding - A Survey,” in Proceedings of the IEEE special issue on protection of multimedia content, vol. 87, no. 7, pp.1062-1078, Jul. 1999.

[2] Ingemar J. Cox, Matthew L.Miller, Jeffrey A. Bloom, Jessica Fridrich and Ton Kalker, “Digital Watermarking and Steganography”, Second Edition.

[3] Jen-Bang Feng, Iuon-Chang Lin, Chwei-Shyong Tsai, and Yen-Ping Chu, “Reversible Watermarking: Current Status and Key Issues,” International Journal of Network Security, vol.2, no.3, pp.161-171, May. 2006.

[4] Lee, G. J., Yoon, E. J. and Yoo, K. Y., “A new LSB based Digital Watermarking Scheme with Random Mapping Function,” in proceeding of International Symposium on Ubiquitous Multimedia Computing, 2008.

[5] Stefan Katzenbeisser, Fabien A. P. Petitcolas, “Information hiding techniques for steganography and digital watermarking”, Artech House.

[6] WANG, R. A., LIN, C. F., LIN, J. C. Image hiding by optimal LSB substitution and genetic algorithm. Patterm recog., vol. 34, no.3, pp.671-683, 2001

[7] Andrew B. Watson, “Image Compression Using the Discrete Cosine Transform”, NASA Ames Research Center, Mathematica Jourmal, vol.4, no.1, pp.81-88, 1994

[8] Faisal Alturki, and Russell Mersereau, “A Novel Approach for Increasing Security and Data Embedding Capacity in Images for Data Hiding Applications”, International Conference on Information Technology: Coding and Computing, pp.228-233, 2001.

[9] I-Jen Lai and Wen-Hsiang Tsai, “Secret-Fragment-Visible Mosaic Image-A New Computer Art and Its Application to Information Hiding”, IEEE Transactions on information forensics and security, vol. 6, no.3, September. 2011.

[10] Ya-Lin Li, Wen-Hsiang Tsai, “New Image Steganography via Secret-Fragment-Visible Mosaic Images by Nearly-reversible Color Transformation”.

[11] L. Douglas Kiel and Euel Elliott, “Chaos Theory in the Social Sciences: Foundations and Applications,” First paperback edition, Michigan University of Michigan Press, 1997

[12] Fan yan-jun, “Chaos and Image-scrambling Algorithm Based on Chaotic Sequences," 2004

[13] LIU Xiang-dong, Zhang Jun-xing, Zhang Jin-hai, He Xi-qin, “Image Scrambling Algorithm Based on Chaos Theory and Sorting Transformation”, IJCSNS International Journal of Computer Science and Network Security, vol.8 no.1, January 2008

[14] FAN Yan-jun, SUN Xiao-hu, and YAN Xiao-dong, ZHENG Lin-tao, “An Image-scrambling Algorithm Based on Mixed Chaotic Sequences”, Journal of Image and Graphics, 2006, vol.11, no.3, pp.387-393

[15] Erik Reinhard, Michael Ashikhmin, Bruce Gooch, and Peter Shirley, “Color Transfer between Images,” Computer Graphics and Applications, vol.21, no.5, September/October 2001.

[16] Chung-Ming Wang and Yao-Hsien Huang, “A Novel Color Transfer Algorithm for Image Sequences,” Journal of Information Science and Engineering 20, pp.1039-1056 ,2004

[17] Daniel L. Ruderman, Thomas W. Cronin, and Chuan-Chin Chiao, “Statistics of cone Responses to Natural Image: Implications for Visual Coding,” J. Qpt. Soc. Am. A/ vol.15, no.8, PP.2036-2045.

[18] G. Wyzecki and W. S. Stiles, Color Science: Concepts and Methods, Quantitative Data and Formulae, 2nd ed., John Wiley &Sons, New York, 1982.

[19] Xue-zhong Xiao and Li-zhuang Ma, “Color transfer in correlated color space”, Proceedings of the 2006 ACM international conference on Virtual reality continuum and its applications 06, pp.305-309, 2006.

[20] Foley, J.D., Dam, A.V., Feiner, S.K., and Hughes, J.F., “Computer graphics: principles and practice,” Second edition, Addison-Wesley publishing company, pp.201-217, 1990

[21] Konstantinides, K., and Yao, K., “Statistical analysis of effective singular values in matrix rank determination”, IEEE Trans. Acoustics, Speech and Signal Processing ASSP-36, 5, pp.757-763, 1988.

[22] “Professor SVD”, Reprinted from The Math Works News & Notes, October 2006.

[23] Neil Muller, Lourenc¸o Magaia, B. M. Herbst. “Singular Value Decomposition”, Eigenfaces and 3D Reconstructions, SIAM REVIEW c 2004 Society for Industrial and Applied Mathematics, vol. 46, no. 3, pp.518–545

[24] Coltuc, D. Chassery, J.-M: “Very Fast Watermarking by Reversible Contrast Mapping”, IEEE Signal Processing Letters, vol.14, no.4, pp.255-258, 2007

[25] Yeh-Shun Chen, Ran-Zan Wang, Yeuan-Kuen Lee, Shih-Yu Huang, “Steganalysis of Reversible Contrast Mapping Watermarking,” Proceedings of the World Congress on Engineering 2008 vol. I, WCE 2008, July 2 - 4, London, U.K., 2008

ABSTRACT

Improved Secret Fragment Visible Mosaic Image for Information Hiding

Zhu Lin
Advisor: Seung Jo Han, Ph.D
Department of Information Communication Engineering
Graduate School of Chosun University

We propose a new method for information hiding based on secret fragment visible mosaic image. This algorithm has the been developed for the application of color transfer to generate the mosaic image hiding the information. Since the RGB color space has strong correlation between three color channels, we must modify all color channels in tandem. Thus it complicates any color modification process. Another problem in this color space is the size of bit stream of recovery information of secret image block sequence. Hence embedding this large bit stream in the mosaic image reduces the quality of the resulting image. In this paper, a new way to solve these problems using the color transfer technique in correlated color space was proposed. The pixel value is considered as a three dimensional stochastic variable and an image a set of samples. Color transfer process is achieved by the geometrical transformations, such as translation, scaling and rotation. The correlation between the color spaces is measured and further used for the color transfer process by studying the covariance between the color space. In order to get more robust encryption and lower bit rate requirement, the combination of logistic map and Chebyshev map is used to generate the encryption sequence of the secret image.

Acknowledgement

I would like to express my deep and sincere gratitude to my supervisor, Prof. Seung Jo Han. His valuable support, encouragement, supervision, personal guidance, and useful suggestions throughout the course of my research have provided a good basis for the completion of this thesis.

I wish to express my warm and sincere thanks committee members, Prof. Jae-Young Pyun and Prof. Young Sik Kim for their detailed and constructive comments, and for their important support throughout this work.

I also like to express thanks to all my lab mates of Computer Network and information security and all friends in Korea for their support and cooperation.

I owe my loving thanks to my parents. They have lost a lot due to my research abroad. Without their encouragement and understanding it would have been impossible for me to finish this work.

The financial support of the Chosun University is greatly acknowledged.