A Study on Visually Encrypted Images for Rights Protection and Authentication

March, 2014

Shenchuan LIU

TOKYO METROPOLITAN UNIVERSITY

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

In this thesis, visually encrypted images for rights protection and authentication is studied. Right protection and authentication are discussed in the following sections.

1.1.1 Right Protection

Human rights include right to life, freedom from torture, freedom from slavery, freedom of speech, and freedom of thought, etc. In this thesis, right protection contains two parts, copyright protection and privacy protection. Copyright protection has a long history. Privacy protection has been paid more attention in recently years.

The British Statute of Anne 1710, entitled with ”An Act for the Encouragement of Learning, by vesting the Copies of Printed Books in the Authors or purchasers of such Copies, during the Times therein mentioned”, was the first copyright law. Initially copyright law only applied to the copying of books. Because by that time, digital cameras or computers were not invented. In late 1970s, computer software was still distributed in audio cassettes, copying was time-consuming and unreliable, the benefit from making copies were low [1, 2]. Usually, official software in audio cassette cost 15 US dollars, audio cassette itself cost 5 US dollars,

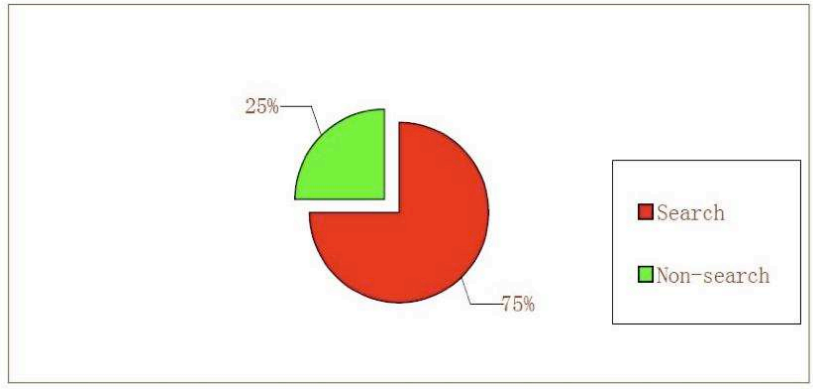


Figure 1.1: Microsoft's report in 2007 [3]. It shows percents of companies who do online research about candidates and who do not.

moreover, the quality of illegal copy was lower, so copy brought little benifits.

From 1980s to 1990s, floppy disks and CDs were used for media carriers. These carriers also suffered copyright infringement. For example, copiers could be reproduced by copying an entire track in floppy disks at a time, ignoring how the sectors were marked. Recently, it has become very common for software to requre activation, such as name & serial, a phone activation code, or device ID(like the IMEI of a smartphone). Technologies for content protection are well developed and can realize a sufficiently strong protection system, but they are casuing inconvenience to users.

In the United States, an article with the title 'The Right To Privacy', is the first implicit declaration of a U.S. right to privacy on December 15, 1890. New technologies are considered to alter the balance between privacy and disclosure. In earlier ages when digital cameras were not invented, it was hard to imagine exposing one's image on the Internet. Actually with the development of the Internet, nearly everything can be saved on the Internet. Fig. 1.1 shows the percentages of companies who search employee's information. According to Microsoft's Report in 2007, 25% of companies don't search employees' information, 75% of companies search employees' information before they are hired through web, twitter, etc. 70% of US recruiters report that they rejected candidates because of information found on the Internet [3].

Figure 1.2: Log on to a computer.

1.1.2 Authentication

Authentication is the process of identifying an individual, usually based on a username and password. Generally, authentication is used for access control. While using a computer, a username and a password are required. Fig. 1.2 shows an example of logging on to a computer. Fig. 1.3 shows the concept of fingerprint and iris recognition. A computer system is supported to be used only by authorized users. The system should detect and exclude the unauthorized users. Common access control involving authentication include:

- Entering a secure facility by using iris recognition
- Withdrawing money from an ATM
- Opening a door with a key
- Using one time password to log on to a server
- Unlocking an IPHONE 5s by using fingerprint

Figure 1.3: Concept of using fingerprint and iris recognition.

1.1.3 Problems

With the development of digital communication, it is easy and popular to generate digital images. It is also convenient for anyone to copy or compile digital images. This situation makes it difficult to protect the copyright of digital images. Moreover, digital images provide us a lot of information. From the point of individual privacy protection and secret protection, it is significant to control the accessibility of changing images content or editing the image freely.

Unauthorized copying and distribution accounted for $2.4 billion in United States in 1990s [1]. Publishers of music and films in digital form use encryption to make copying more difficult. Encryption has long been used by militaries and governments to facilitate secret communication. It is now commonly used in protecting information within many kinds of civilian systems. For example, the Computer Security Institute reported that in 2007, 71% of companies surveyed utilized encryption for some of their data in transit, and 53% utilized encryption for some of their data in storage [4]. Encryption can be divided into symmetric key encryption and public key encryption. Symmetric key encryption is also known as symmetric key algorithm, and is a class of algorithms for cryptography that uses the same cryptographic key for both encryption of plaintext and decryption of ci-

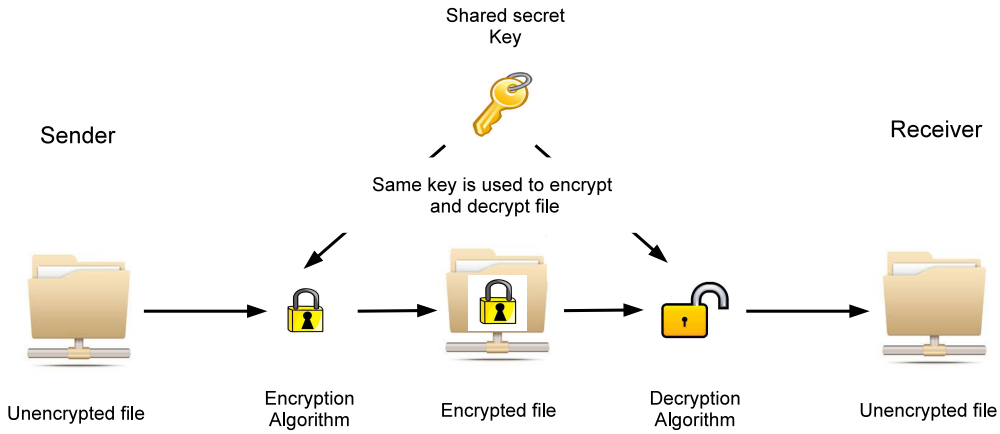


Figure 1.4: Figure of symmetric-key algorithm.

phertext. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link [5–10]. Fig. 1.4 shows the conception of symmetric-key algorithm.

Public-key cryptography, also known as asymmetric cryptography, refers to a cryptographic algorithm which requires two separate keys one is secret (or private) and the other is public. The public key is used to encrypt plaintext; whereas the private key is used to decrypt ciphertext. It is computationally easy for a user to generate his or her public and private key-pair and to use them for encryption and decryption. The strength lies in the fact that it is "impossible" (computationally infeasible) for a properly generated private key to be determined from its corresponding public key. Thus the public key may be published without compromising security, whereas the private key should not be known to anyone else. This relationship ties the keys in the pair exclusively to one another: a public key and its corresponding private key are paired together and are related to no other keys. Public key algorithms [11–15], unlike symmetric key algorithms, do not require a secure initial exchange of secret key between the parties. Fig. 1.5 shows the conception of asymmetric-key cryptography.

Signal processing techniques in encrypted domain have been widely researched as its application in biometric matching [16–20] and privacy-preserving data min-

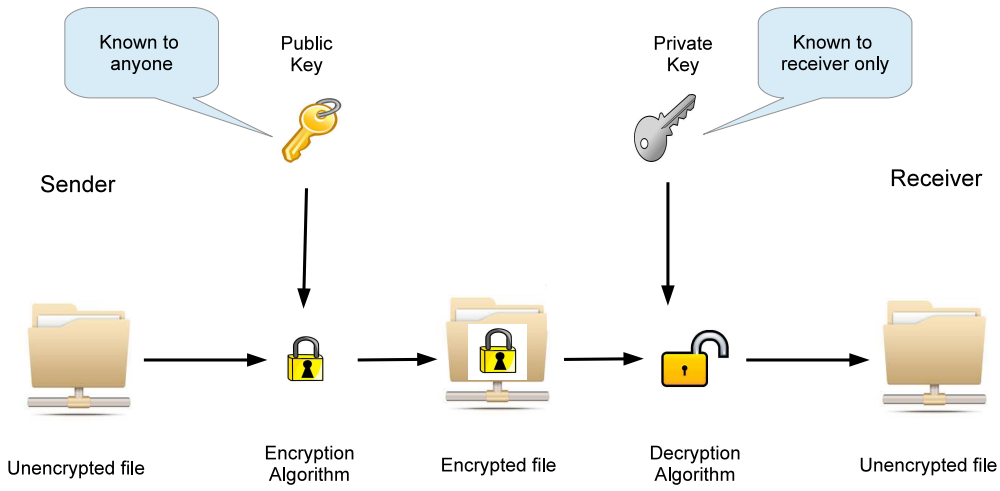


Figure 1.5: Figure of public-key algorithm.

ing [21–26]. Some schemes [27–35] use visual encryption in transmission multimedia data through the Internet while the data need to be encrypted. Some schemes [36–40] are also used for image matching while protecting the content of the image. Visual encryption is also used for detection [41–44] of moving objects of motion JPEG videos. In this thesis, visual encryption is used in the image trading system and visual cryptography to share secrets.

In traditional ways, digital fingerprinting or transaction tracking [45] which hides consumers' information to the content by a data hiding technique is one of the effective ways to protect the content from illegal copy and distribution in trading systems [46]. This model is useful only if the content providers (CPs) are perfectly trustworthy. Practically, CPs are not always trustful, trusted third parties (TTPs) or arbitrators [47] are introduced to trading systems to enhance the security. A consumer asks a TTP to send an ID to him/her, and the consumer is identified by this ID instead of his/her personal information in trading with CPs. So, CPs are now free from consumers' privacy. A CP sends the content which the consumer purchases to the TTP, and the TTP embeds consumer ID to the content before transmitting the content to the consumer. Now, the TTP plays the most important role in the trading system and has potential risk of accidental leakage of consumers' privacy, because the TTP knows and stores all the transactions among

consumers and CP and consumer information themselves. To reduce the above potential leaking risk at TTPs, a new framework has been proposed for TTP-based content trading systems [48–52]; a content is divided into two pieces by a CP. One piece is sent to a consumer, and the other is fingerprinted by the TTP before the consumer receives it. This time TTP knows only a part of the content. In the literature [48–52], an image is equally divided into two pieces in the spatial domain, and another literature [53] uses saliency map [54] to effectively divide images in the spatial domain.

These conventional schemes [48–53] still face unsolvable problems: while dividing images into two pieces in the spatial domain, 1) the piece to be watermarked is smaller than the original image, this leads to relative weakness of digital fingerprinting or distortion of watermarked images, and 2) an adversary has a possibility to estimate the original image from the piece which is leaked from a TTP. So, in order to protect consumer's privacy, it is quite necessary to keep the piece sent to TTP unrecognizable.

This theis proposes a use of *amplitude-only images* for the trading systems with TTPs [55]. It is well known that amplitude-only images are unrecognizable in comparisons with *phase-only images* which are inversely transformed phase spectra of original images [56, 57]. Any arbitrary fingerprinting mechanism such as spread spectrum watermarking [58]-based implementation [59] can be used in this conventional scheme. An image quality guaranteeing block discrete cosine transformation (DCT)-based data hiding technique [60] is used as an example of the digital fingerprinting technique here. Several attacks provided by StirMark [62, 63] and compression by JPEG 2000 [64] are used to evaluate the proposed scheme.

A secret sharing (SS) scheme [65] divides a secret into n pieces referred to as shares. n shares are held by n different parties and the secret is recovered if and only if k or more shares are gathered. This scheme is called as a (k, n)-threshold SS scheme. Visual SS (VSS) in which decryption can be done by human eyes has been proposed for binary images [66]. Later, VSS has been extended to non-

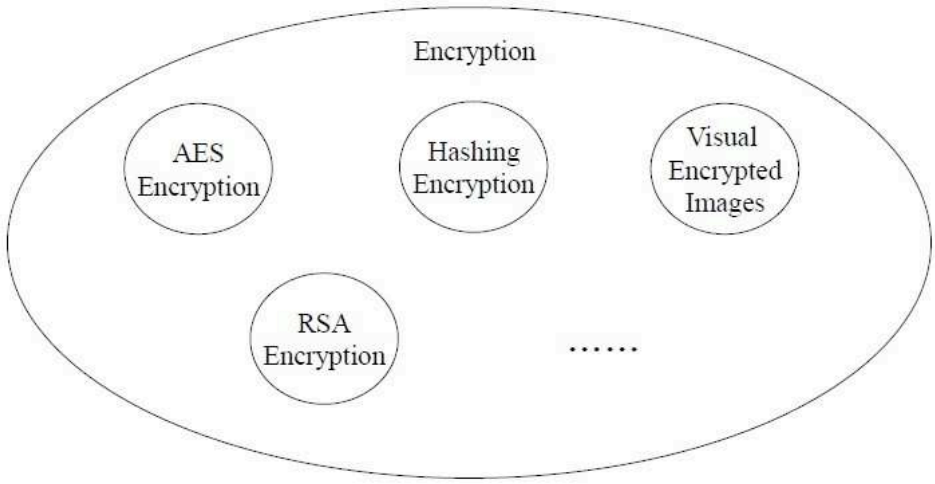


Figure 1.6: Different kinds of encryptions.

binary images [67, 68]. Color VSS have also been proposed [69–71]. Instead of random share images [66], meaningful shares are employed in a scheme [72]. Some schemes [73, 74] allow to embed multi-secret within one image. A weaken security scheme [75, 76] is also proposed to improve the visuality of recovered image. Other direction reduces the pixel expansion size and improves the contrast of the recovered image [77, 78].

On the other hand, it is assumed in a scenario that malicious parties deceive an honest party, and cheat-prevention VSS schemes have been proposed to fight it [53, 79, 80, 82]. A literature [81] found that the original cheat-prevention VSS scheme [80] is not well function in some circumstances. The literature [81] also proposes a new scheme, but pixel expansion is sacrificed significantly. Later, the same authors proposed another scheme [82] with less pixel expansion, but its application is limited to $(2, n)$-threshold VSS and it introduces a further restriction.

These conventional schemes [48–53] of image trading system and conventional schemes [79–82] of visual cryptography still face unsolvable problems:

1. The piece to be watermarked is smaller than the original image, this leads to relatively weakness of digital fingerprinting or distorted of watermarked images

2. An adversary has a possibility to estimate the original image from the piece which is leaked from a TTP

3. Although compression is requested in reality, non of these conventional schemes take compression into consideration.

4. Cheating Prevention is not well functional or limitation is too much.

5. The contrast of revealed secret image is low, it is hard to recognize by human eyes.

Fig. 1.6 shows differents kinds of encryption. It is proved that encryption is good way for rights protection and anthentication. From the aspects of security, encryption can be divided into information theoretic encryption and computationl security encryption. In information theoretic encryption, the encrypted files are theoretically secure. In computational security encryption, the encrypted files are secure because of limited computational power. Visually encrypted images belong to both. This property makes visually encrypted images applicable in different areas. For visually encrypted images, the plaintext is an image and the encrypted file is an image, that is to say, the format is preversed.

1.2 Aim of this thesis

Through consideration of new expression and perspective of visually encryption image, this thesis is aimed at development of new theoretical visually encryption method. The main aims are as follows:

1. Copyright protection in the image trading system and authentication of images' accessibility in visual cryptography

2. Reduction of the affection caused by lossy compression of visual encryption in the image trading system

3. Improvement the contrast of revealed secret image and the robustness against malicious attack

1.3 Organization

This thesis is organized around the three purposes. The reminder of this thesis is organized as follows.

Chapter 2: Visually Encrypted Images

Visually encrypted images are described in this chapter. The definition of visually encrypted images is given. There are different techniques to produce visually encrypted images, two of which are discussed in details. In the image trading system, amplitude-only image is used for visually encryption. In visual cryptography, random pixel expansion is used for visually encryption.

Chapter 3: Image Trading System for Copyright- and Privacy-Protection

An image trading system should protect the images' copyright and consumers' privacy as well. However, in conventional schemes, consumers' privacy is not well protected, that is, potential information leakage will reflect consumers' privacy. This chapter proposes a novel image trading system in which images' copyright and consumers' privacy are both protected.

Chapter 4: Compression-Friendly Image Trading System for Copyright- and Privacy-Protection

In the previous chapter, compression is not considered. Actually, compression is always requested when images are either transmitted on the Internet or being stored in servers. In this chapter, an image trading system with efficient compression is proposed. JPEG 2000 lossy compression is applied in this chapter. Its affection between conventional image systems and the proposed system are evaluated.

Chapter 5: Cheating Prevention Visual Cryptography

Visual cryptography is also called visual secret sharing. Contrast of revealed secret image is very important. Usually, in order to gain the highest contrast, pixel expansion is minimized. As the pixel expansion is minimized, cheating between share holders may happen. Conventional schemes have been proposed to prevent cheating. However, either larger pixel expansion is used or cheating prevention is not well functional. In this chapter, a new cheating prevention visual cryptography is proposed. The proposed scheme gain larger contrast of revealed secret image with relatively less pixel expansion. At the same time, cheating prevention is functional.

Chapter 6: Conclusion

Chapter 6 concludes this thesis and mention several possible extensions that may be of interest for application and future research.

Chapter 2

Visually Encrypted Images

2.1 Introduction

In this chapter, Visually encrypted images are introduced. For visually encrypted images, the format of input files is image and the format of output files is also image. It is difficult to estimate visual information of original image from the visually encrypted image. Fig. 2.1 shows different applications of visually encrypted images. This chapter introduces visually encrypted images in image trading system and access control in details. The rest of the applications are roughly reviewed.

Visual encryption is one kind of signal processing techniques in encrypted domain. Visual encryption techniques have drawn much attention in recent years due to its application in biometric matching [16–20] and privacy-preserving data mining [21–26]. Usually, visual encryption is used to protect the content of images and videos in different applications. Visual encryption can be widely used in transmission of multimedia data through the Internet while the data need to be encrypted [27–35]. Fig. 2.2 shows an example of a scheme [30] for a commutative perceptual encryption and image compression for JPEG 2000.

Visual encryption is also used for image matching while protecting the content of the image [36–40]. In these schemes, scrambling methods for image matching using phase-only correlation (POC) or discrete cosine transform sign phase corre-

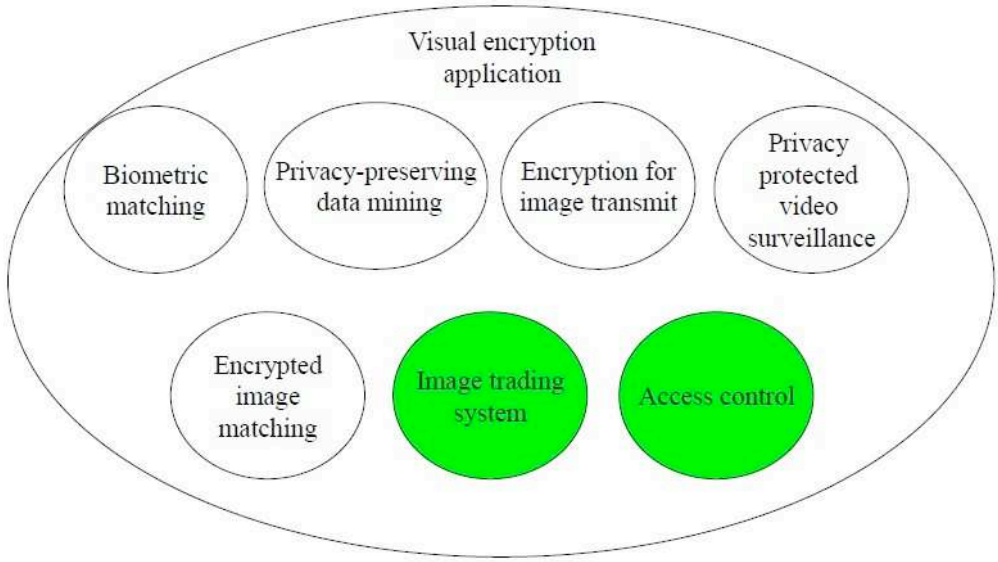
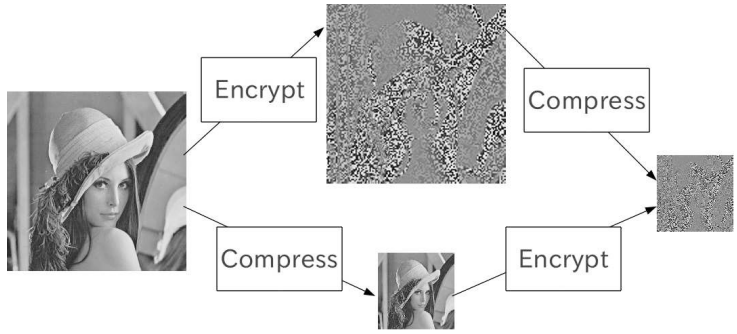


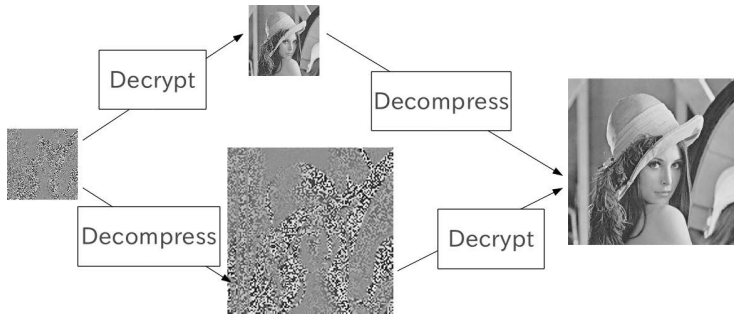
Figure 2.1: Different applications of visually encrypted images.

lation (DCT-SPC) are proposed. These methods distort only the phase, which has significant information of images. The information in each image is protected by the distorted phase information. Fig. 2.3 shows the original and phase scrambled images. Visual encryption is also used for detection [41–44] of moving objects of motion JPEG videos. In this scheme, a scrambling method for motion JPEG (MJ) videos and moving objects (MOs) detection from scrambled videos is proposed. Both scrambling and MOs detection utilize the property of the positive and negative sign of discrete cosine transform (DCT) coefficients. Fig. 2.4 shows the original and visually encrypted frames.

Many kinds of techniques can be used for generation of visually encrypted images, such as amplitude-only image, block scrambling in spatial domain, random pixel expansion, etc. This thesis uses amplitude-only image and random pixel expansion for image trading system and access control, respectively. Visually encrypted images are used in the image trading system for the protection of consumer privacy and image copyright and they are also used in visual cryptography to share secrets. In the following sections, amplitude-only image and visual cryptography are discussed in details.



(a) Encryption and compression.



(b) Decryption and decompression.

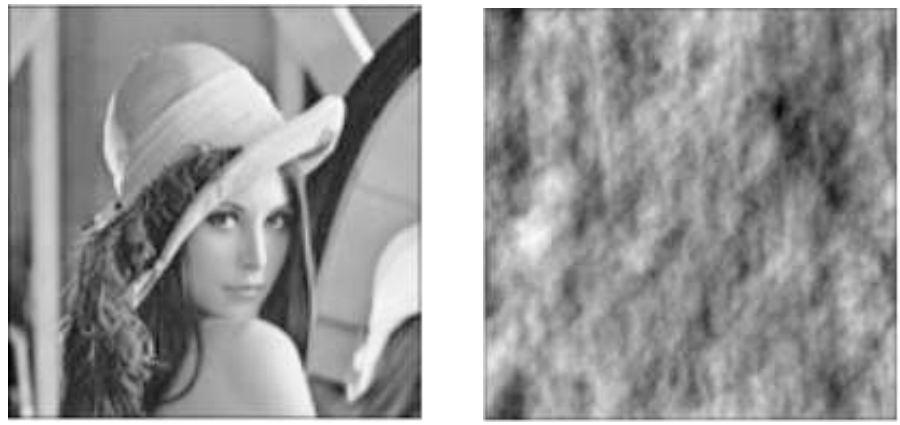
Figure 2.2: This scheme [30] is a commutative perceptual encryption and image compression for JPEG 2000.

2.2 Amplitude-Only Image

According to the domain where an amplitude-only image is generated, amplitude-only image can be divided into two types, namely, discrete Fourier transformation based amplitude-only image (DFT-based amplitude-only image) and discrete cosine transformation based amplitude-only image (DCT-based amplitude-only image).

2.2.1 DFT-based Amplitude-Only Image

$N_1 \times N_2$-sized original image $\mathbf{f} = \{f(n_1, n_2)\}$ where $n_1 = 0, 1, \ldots, N_1 - 1$ and $n_2 = 0, 1, \ldots, N_2 - 1$ is firstly transformed to two-dimensional (2D) discrete Fourier spectra $\mathbf{F} = \{F(k_1, k_2)\}$ where $k_1 = 0, 1, \ldots, N_1 - 1$ and $k_2 = 0, 1, \ldots, N_2 - 1$ by applying the 2D discrete Fourier transformation (DFT) to $\mathbf{f}$. That is, image signal



(a) Original image 'Lena'. (b) Phase scrambled image.

Figure 2.3: Original and phase scrambled images of schemes [36, 37].

f and spectra **F** are given as,

$$f(n_1, n_2) = \frac{1}{N_1 N_2} \sum_{k_1=0}^{N_1-1} \sum_{k_2=0}^{N_2-1} F(k_1, k_2) W_{N_1}^{-k_1 n_1} W_{N_2}^{-k_2 n_2}, \tag{2.1}$$

$$F(k_1, k_2) = \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} f(n_1, n_2) W_{N_1}^{k_1 n_1} W_{N_2}^{k_2 n_2}, \tag{2.2}$$

where, $W_{N_1} = \exp\left(-j\frac{2\pi}{N_1}\right)$, $W_{N_2} = \exp\left(-j\frac{2\pi}{N_2}\right)$, and $j = \sqrt{-1}$.

Spectra **F** can be divided to amplitude and phase spectra as

$$\mathbf{F}_a = \{F_a(k_1, k_2)\} = \{|F(k_1, k_2)|\}, \tag{2.3}$$

$$\mathbf{F}_p = \left\{F_p(k_1, k_2)\right\} = \left\{\frac{F(k_1, k_2)}{|F(k_1, k_2)|}\right\}, \tag{2.4}$$

where $\mathbf{F}_a$ and $\mathbf{F}_p$ are amplitude and phase spectra, respectively. Applying the inverse 2D DFT to $\mathbf{F}_a$ and $\mathbf{F}_p$, $N_1 \times N_2$-sized amplitude-only image $\mathbf{f}_a$ and $N_1 \times N_2$-sized phase-only image $\mathbf{f}_p$ are generated, respectively.

2.2.2 DCT-based Amplitude-Only Image

$N_1 \times N_2$-sized original image $\mathbf{f} = \{f(n_1, n_2)\}$ where $n_1 = 0, 1, \ldots, N_1 - 1$ and $n_2 = 0, 1, \ldots, N_2 - 1$ is firstly transformed to 2D discrete cosine spectra $\mathbf{F} = \{F(k_1, k_2)\}$

(a) Original frames.

(b) Visually encrypted frames.

Figure 2.4: Original and visually scrambled frames of scheme [44].

where $k_1 = 0, 1, \ldots, N_1 - 1$ and $k_2 = 0, 1, \ldots, N_2 - 1$ by applying the 2D discrete cosine transformation (DCT) to $\mathbf{f}$. That is, image signal $\mathbf{f}$ and spectra $\mathbf{F}$ are given as,

$$f(n_1, n_2) = \sum_{k_1=0}^{N_1-1} \sum_{k_2=0}^{N_2-1} \alpha(k_1)\alpha(k_2)F(k_1, k_2)C(n_1, k_1, N_1)C(n_2, k_2, N_2), \tag{2.5}$$

$$F(k_1, k_2) = \alpha(k_1)\alpha(k_2) \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} f(n_1, n_2)C(n_1, k_1, N_1)C(n_2, k_2, N_2), \tag{2.6}$$

where,

$$\alpha(k_1) = \begin{cases} \sqrt{1/N_1}, & k_1 = 0 \\ \sqrt{2/N_1}, & \text{otherwise} \end{cases}, \tag{2.7}$$

$$\alpha(k_2) = \begin{cases} \sqrt{1/N_2}, & k_2 = 0 \\ \sqrt{2/N_2}, & \text{otherwise} \end{cases}, \tag{2.8}$$

$$C(n_1, k_1, N_1) = \cos \frac{(2n_1 + 1)k_1\pi}{2N_1}, \tag{2.9}$$

$$C(n_2, k_2, N_2) = \cos \frac{(2n_2 + 1)k_2\pi}{2N_2}. \tag{2.10}$$

Spectra $\mathbf{F}$ can be divided to amplitude and phase spectra as

$$F_a(k_1, k_2) = |F(k_1, k_2)|, \tag{2.11}$$

$$F_p(k_1, k_2) = \text{sgn}\left(F(k_1, k_2)\right), \tag{2.12}$$

where $\mathbf{F}_a$ and $\mathbf{F}_p$ are amplitude and sign spectra, respectively. Applying the inverse 2D DCT to $\mathbf{F}_a$ and $\mathbf{F}_p$, $N_1 \times N_2$-sized amplitude-only image $\mathbf{f}_a$ and $N_1 \times N_2$-sized phase-only image $\mathbf{f}_p$ are generated, respectively.

2.2.3 Amplitude-Only Image with Random sign

Firstly, a CP divides $N_1 \times N_2$-sized original image $\mathbf{f} = \{f(n_1, n_2)\}$ to $N_1 \times N_2$-sized Amplitude-Only Image (AOI) $\mathbf{f}'_a = \{f'_a(n_1, n_2)\}$ and $N_1 \times N_2$-sized phase components $\mathbf{F}_p = \left\{F_p(k_1, k_2)\right\}$ where $n_1 = 0, 1, \ldots, N_1 - 1$, $n_2 = 0, 1, \ldots, N_2 - 1$, $k_1 = 0, 1, \ldots, N_1 - 1$, and $k_2 = 0, 1, \ldots, N_2 - 1$.

1. The CP applies 2D DCT to $\mathbf{f}$ to get $N_1 \times N_2$-sized 2D-DCT coefficients $\mathbf{F} = \{F(k_1, k_2)\}$;

2. Separate real numbered DCT coefficients $\mathbf{F}$ into amplitude components $\mathbf{F}_a = \{F_a(k_1, k_2)\}$ and phase components $\mathbf{F}_p$.

   where $F_a(k_1, k_2)$ and $F_p(k_1, k_2)$ are amplitude and phase component of $F(k_1, k_2)$, respectively, and sgn$(\cdot)$ returns the positive and negative sign of the input.

It is noted that

$$F(k_1, k_2) = F_a(k_1, k_2)F_p(k_1, k_2). \tag{2.13}$$

3. $N_1 \times N_2$-sized random matrix $\mathbf{R} = \{R(k_1, k_2)\}$ which consists of ± 1 is multiplied to $\mathbf{F}_a$ as

$$\mathbf{F}'_a = \mathbf{F}_a \circ \mathbf{R}, \tag{2.14}$$

where $\circ$ represents Hadamard product.

4. Applying the inverse 2D DCT (2D-IDCT) to $\mathbf{F}'_a$ generates AOI $\mathbf{f}'_a$.

2.3 Visual Cryptography

Secret sharing (also called secret splitting) is referred as distributing a secret among a group of parties, each of whom holds a share (or shares) of the secret. The secret can be recovered only when enough share holders combine their shares together. Individual shares are completely of no use on their own. Generally, there is one dealer and n parties. The dealer distributes a secret into n shares and gives these shares to the parties, but only when specific conditions are fulfilled will the parties be able to recover the secret from their shares. The dealer accomplishes this by giving each player a share in such a way that any group of k (for threshold) or more players can together recover the secret but no group of less than k parties can. Such a scheme is called a (k, n)-threshold scheme. Secret sharing was invented independently by Adi Shamir and George Blakley in 1979 [65].

Secret sharing is an ideal scheme to store sensitive and important information. Examples include: encryption keys, missile launch codes, and numbered bank accounts. Each of these pieces of information must be kept confidential, as their exposure could be disastrous, however, it is also critical that they should not be lost.

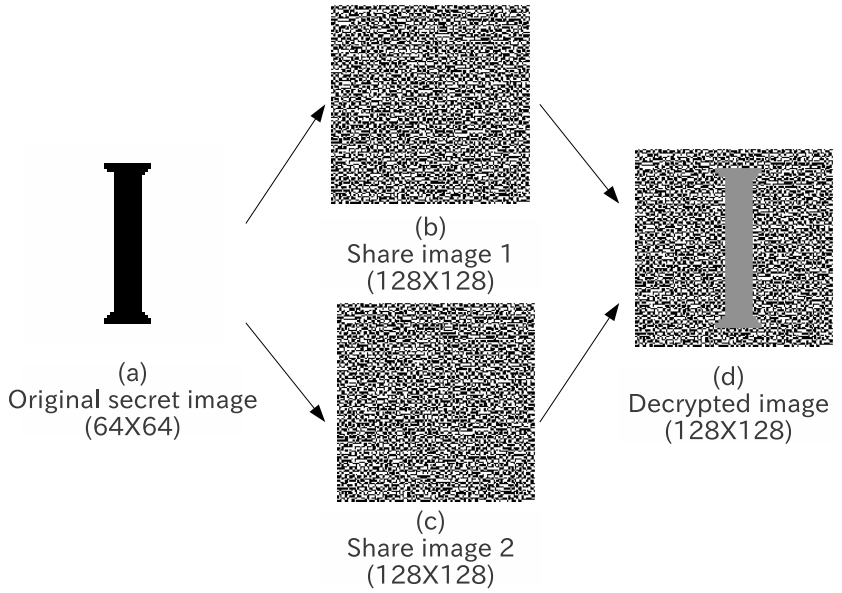
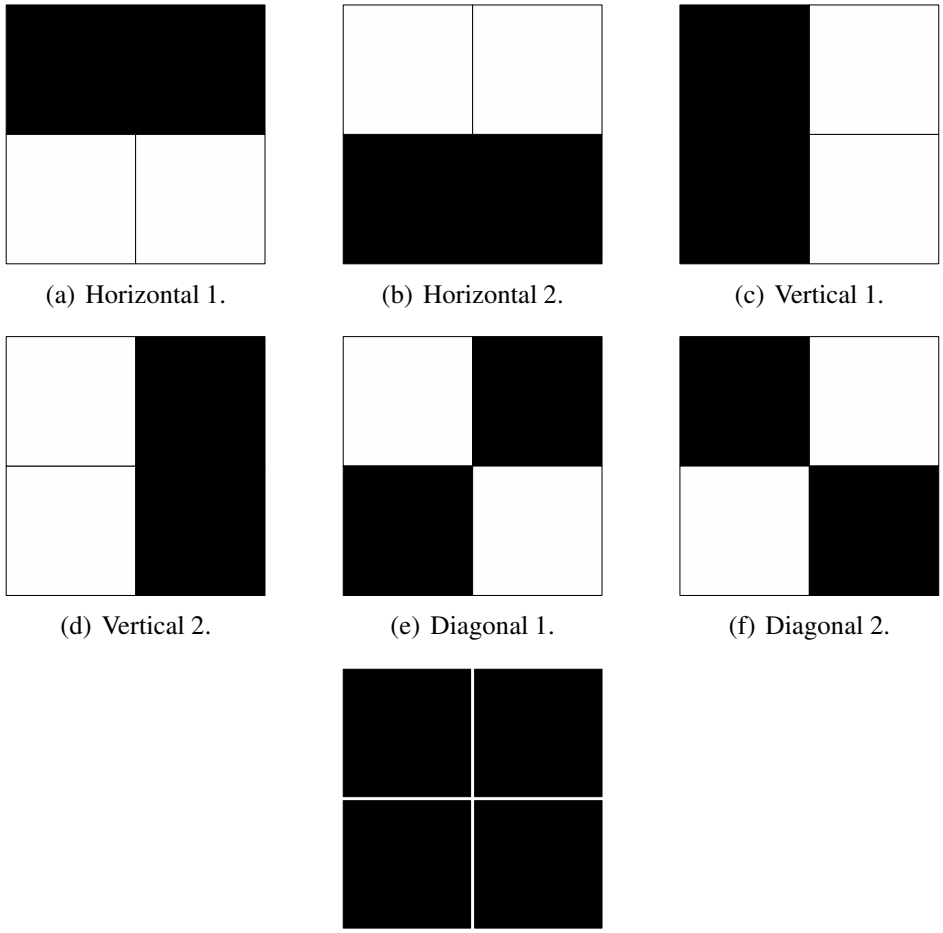


Figure 2.5: An example of the first and fundamental visual secret sharing scheme [66]. All two shares are required to recover the secret image in this example; $(2, 2)$-threshold implementation.

Traditional methods for encryption are not suitable for simultaneously achieving high levels of confidentiality and reliability. Because while storing the encryption key, one must choose between keeping a single copy of the key in one location for maximum secrecy, or keeping multiple copies of the key in different locations for greater reliability. Increasing reliability of the key by storing multiple copies lowers confidentiality by creating additional attack vectors; there are more opportunities for a copy to fall into the wrong hands. Secret sharing schemes address this problem, and allow arbitrarily high levels of confidentiality and reliability to be achieved.

When a dealer distributes a secret into many images (share images), a secret sharing scheme becomes a visual cryptography. Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. Fig. 2.5 shows the simplest example of the VSS scheme [66]. In the VSS scheme [66], a secret binary image consisting of black and white pixels is split up to n shares in which all shares are random binary



(a) Horizontal 1. (b) Horizontal 2. (c) Vertical 1.

(d) Vertical 2. (e) Diagonal 1. (f) Diagonal 2.

(g) Four black pixels.

Figure 2.6: Random pads for $(2, 2)$-threshold visual secret sharing scheme [66]. (a)-(f) six pads for expanding a pixel in a secret image to a 2×2-sized pixel block in a share. (g) a black pixel in the secret image is represented by a black pixel block in stacked shares, i.e., in the decrypted image.

images. When k or more shares printed on transparencies are stacked together, the human eyes can do the decryption for recovering the secret image, whereas the decryption is totally unsuccessful except the size of the secret image if less than k shares are collected and superimposed. This condition is referred to as (k, n)-threshold VSS as well as the ordinary SS [65]. In this scheme, each pixel is handled individually and it should be noted that the white pixel represents the transparent color.

In the $(2, 2)$-threshold implementation, i.e., $k = 2$ and $n = 2$, of the conven-

tional VSS scheme [66], each pixel of a secret binary image is expanded to a 2×2-sized pixel block in share images. To expand a pixel of the secret image, this implementation uses six of 2×2-sized matrices referred to as *random pad*s as shown in Figs. 2.6; they are horizontal pads (Figs. 2.6 (a) and (b)), vertical pads (Figs. 2.6 (c) and (d)), and diagonal pads (Figs. 2.6 (e) and (f)), i.e., three pad pairs exist.

Two pads are used to generate two shares. When a pixel in the secret binary image is black, one pad pair among three pairs is chosen and a pad and the other are assigned to one share and the other, respectively. On the other hand, if the pixel is white, one pad among six pads is used twice to generate two shares. When the shares are superimposed, the black pixel in the secret image will be represented of a black pixel block as shown in Fig. 2.6 (g), and the white pixel in the original binary image will be represented of two white and two black pixels as shown in Fig. 2.6 (a)-(f).

Recall Fig. 2.5 here. Figure 2.5 is an example of $(2, 2)$-threshold implementation of the conventional VSS scheme [66]. In this example, a 64×64-sized original binary image is expanded to 128×128-sized shares by using six pads shown in Fig. 2.6, and thus, the recovered image becomes 128×128-sized.

2.4 Advantages of Visually Encrypted Images

In image trading system, amplitude-only images can be used to prevent estimate the original image. So, even if the images sent to TTP are released accidently, there is no clue what kind of images the users are buying.

In visual cryptography, random pixel expansion can be used to produce secret shares. Visual cryptography belongs to information theoretic encryption, so the secret information cannot be recovered if not enough shares are stacked or analyzed.

Chapter 3

Image Trading System for Copyright- and Privacy-Protection

3.1 Introduction

With the development of digital equipment, billions of multimedia can be found in the Internet with copyright or without copyright, and more and more multimedia contents will be put on the Internet for sale. With popularity of personal computers, the existing adversary will be more powerful and this also brings any individual convenience to be an adversary. In addition, any transactions between providers and consumers are stored in the Internet, the information leakage becomes more serious. So, the simultaneous protection of the copyright of multimedia and the privacy of consumers becomes a critical problem.

In traditional ways, digital fingerprinting or transaction tracking [45] which hides consumers' information to the content by a data hiding technique is one of the effective way to protect the content from illegal copy and distribution in trading systems [46]. This model is useful only if the content providers (CPs) are perfectly trustworthy. From a practical viewpoint, since any individual can be a CP to distribute multimedia over the Internet, CPs are not always trustful; it has the potential to be cracked. So, the conventional fingerprinting is not well enough to protect the privacy of consumer.

In order to overcome this situation, trusted third parties (TTPs) or arbitrators [47] are introduced to trading systems. A consumer asks a TTP to send an ID to him/her, and the consumer is identified by this ID instead of his/her personal information in trading with CPs. So, CPs are now free from consumers' privacy. A CP sends the content which the consumer purchases to the TTP, and the TTP embeds consumer ID to the content before transmitting the content to the consumer. Now, the TTP plays the most important role in the trading system and cannot afford to accidental leakage of consumers' privacy, because the TTP knows and stores all the transactions among consumers and CPs and consumer information themselves.

To reduce the above potential leaking risk at TTPs, a new framework has been proposed for TTP-based content trading systems [48–52]; a content is divided into two pieces by a CP. One piece is directly sent to a consumer by the CP, and the other is watermarked by the TTP before the consumer receives it. The consumer obtains the watermarked content by combining two received pieces. By doing so, the TTP knows only a part of the content. In the literature [48–52], an image is equally divided into two pieces in the spatial domain, and another literature [53] uses saliency map [54] to effectively divide images in the spatial domain.

These conventional schemes [48–53] still face unsolvable problems: while dividing images into two pieces in the spatial domain, 1) the piece to be watermarked is smaller than the original image, this leads to relatively weakness of digital fingerprinting or distorted of watermarked images, and 2) an adversary has a possibility to estimate the original image from the piece which is leaked from a TTP. So, in order to protect consumer's privacy, it is quite necessary to keep the piece sent to TTP unrecognizable.

This chapter proposes a use of *amplitude-only images* for the trading systems with TTPs [55]. An amplitude-only image is inversely transformed amplitude spectra of an image. It is well known that amplitude-only images are unrecognizable in comparisons with *phase-only images* which are inversely transformed phase spectra of original images [56, 57]. In the proposed system, the image to be

transmitted to a consumer is divided into the amplitude- and phase-only images. The former will be watermarked by a TTP and the latter is directly sent to the consumer. Since the most of digital fingerprinting techniques modify the amplitude components of images, almost any arbitrary technique can be used in the proposed system and the robustness of watermarks only depends on the used fingerprinting technique. Since the proposed system uses amplitude-only images whose size is the same as the original image instead of spatially divided images, it is found that the proposed scheme is more robust than the conventional schemes.

The rest of the chapter is arranged as follows. In Section 3.2, the framework of image trading systems and the conventional schemes for the system with TTPs in which an image is divided into two pieces [48–53] will be reviewed. The new scheme is proposed in Section 4.3. Experimental results are showed in Section 4.4, and conclusions and future work are given in Section 4.5.

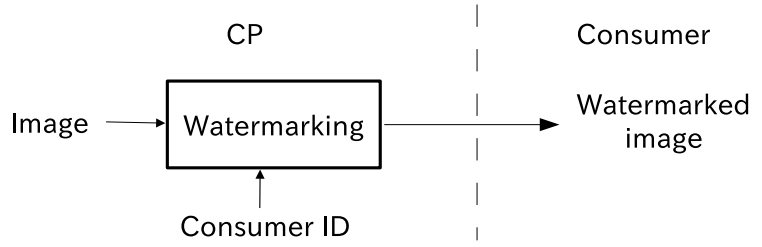
3.2 Preliminaries

This section reviews the framework for image trading systems and the conventional schemes based on the framework with TTPs in which images are divided into two pieces [48–53].

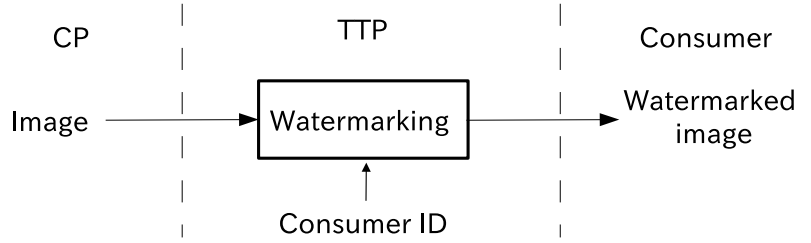
3.2.1 Frameworks

Figure 3.1 shows the framework for image trading systems; (a) the classical digital fingerprinting-based system [46], (b) the system with TTPs [47], and (c) the system with TTPs in which an image is divided into two pieces [48–53]. In the classical system [46], the image sold from a CP to a consumer conveys the consumer's digital fingerprinting, so the copyright of the image is protected. The consumer's privacy, however, is not guaranteed to be protected from malicious or vulnerable CPs.

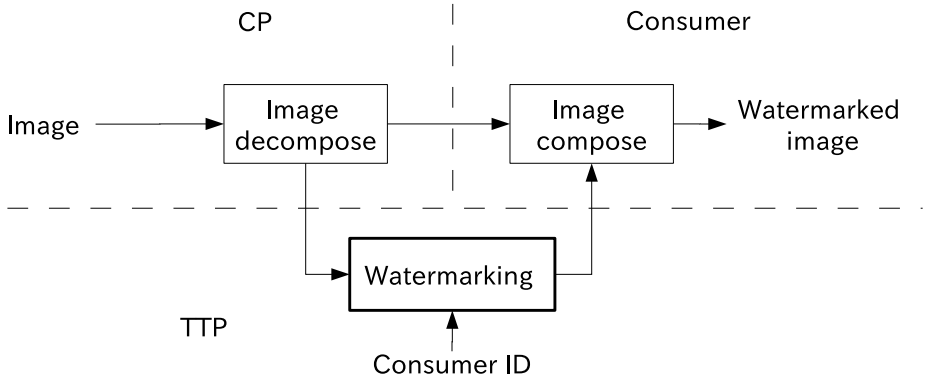
The second framework introduces TTPs to the framework itself in which a TTP stands between a CP and a consumer [47]. The TTP issues a consumer ID



(a) Classical digital fingerprinting-based [46].



(b) With trusted third parties [47].



(c) With trusted third parties and images are divided into two pieces [48–52].

Figure 3.1: Image trading systems.

to the consumer and all transactions between the CP and the TTP are based on the ID instead of the consumer's information themselves. That is, the consumer's private information is protected from CPs. The TTP also embeds the consumer ID to the image which is from the CP to the consumer to protect the copyright of the image. This framework protects consumer's privacy from malicious or vulnerable CPs but not from accidental leakage of consumer information at TTPs.

To overcome this situation, a CP divides an image into two pieces in the latest framework [48–52]. One piece which is relatively less important part is directly

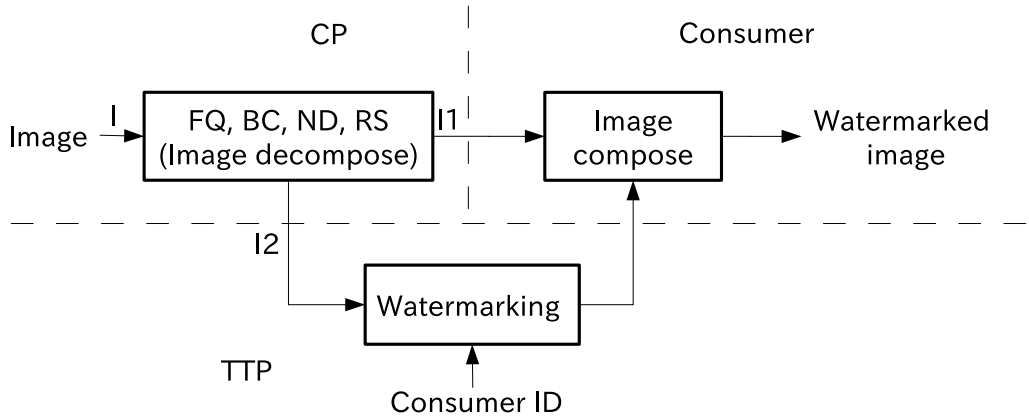


Figure 3.2: Conventional scheme 1 [48–52]. Original image 'I' is divided into two pieces 'I1' and 'I2' through frequency decomposition (FQ), block-based checker board pattern decomposition (BC), block-based noise-like bitplane decomposition (ND), and block shuffling (RS).

sent to a consumer, whereas the other important piece is sent to a TTP. The TTP hides the consumer ID to the received piece, and it sends the watermarked piece to the consumer. The consumer composes the watermarked image from two received pieces. The TTP now knows a part of the image from which the whole image cannot be estimated, so the privacy of the consumer is now expected to be protected.

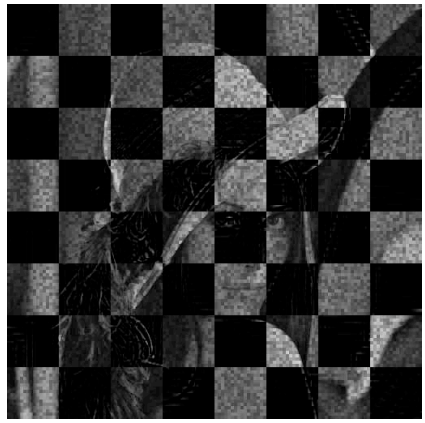
3.2.2 Conventional Schemes

This section reviews the two conventional schemes [48–53] for the last framework mentioned above, from the viewpoint of image decomposition.

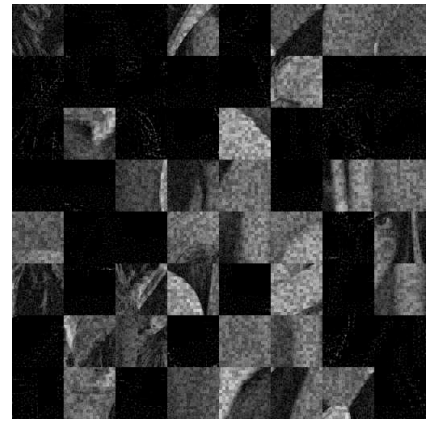
Conventional Scheme 1

Figure 3.2 is the block diagram of the conventional scheme 1 [50], where an image is divided into two pieces by a combination of frequency decomposition ('FQ' in Fig. 3.2), block-based checker board pattern decomposition (BC), block-based noise-like bitplane decomposition (ND), and block shuffling (RS). Figure 3.3 shows (a) original image 'I,' (b) piece 'I1,' and (c) piece 'I2' in this conventional scheme. Piece 'I2' in which blocks are shuffled to be invisible is watermarked by

(a) Original image 'I.'



(b) Piece 'I1.'



(c) Piece 'I2.'

Figure 3.3: Images in the conventional scheme 1 [48–52]. Piece 'I1' is directly sent to a consumer, whereas 'I2' is watermarked by a trusted third party.

a TTP. Here, it is found that important information of original image 'I' are left in piece 'I2' and 'I' can be estimated from 'I2.'

In addition, the TTP in this conventional scheme [50] uses two proprietary watermarking mechanisms, namely, coefficients comparison embedding and patchwork watermarking, because 'I2' contains two different characteristic blocks; high frequency component blocks and noise-like blocks, and two watermarking mechanisms are suitable to each of them.

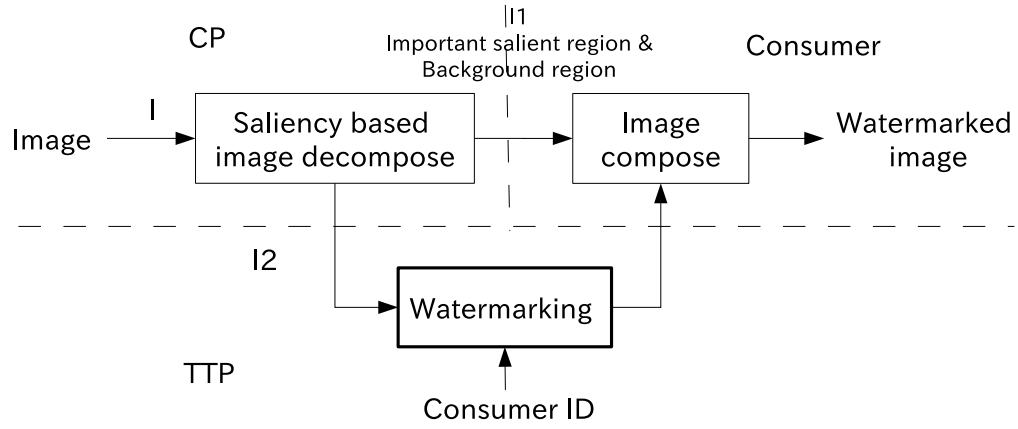


Figure 3.4: Conventional scheme 2 [53]. An original image is divided into two pieces based on the saliency map of the image.

Conventional Scheme 2

Figure 5.5 shows the block diagram of conventional scheme 2 [53]. First, the saliency [54] of original image 'I' is calculated to extract the important content of 'I.' Image 'I' is, then, decomposed into two pieces based on the saliency map. Figure 3.5 (a) is original image 'I,' and Fig. 3.5 (b) shows the saliency map of 'I' obtained by a saliency detection technique [54]. The map is then binarized (Fig. 3.5 (c)) and divided into blocks (Fig. 3.5 (d)), and two pieces shown in Figs. 3.5 (f) and (e) are generated from the original image based on this block divided map. It is found that from the image shown in Fig. 3.5 (g) which the TTP receives, the original image can be estimated.

Even the reshaped 'I2' is a small and long image, it is a normal image. So, any arbitrary fingerprinting mechanism such as spread spectrum watermarking [58]-based implementation [59] can be used in this conventional scheme.

The above mentioned two conventional schemes [48–53] do divide original image 'I' into two pieces 'I1' and 'I2,' but 'I2' which is watermarked by a TTP can be still visible in both schemes as shown as Figs. 3.3 (c) and 3.5 (f). That is, the privacy information of consumers are not perfectly protected.

The next section proposes a completely new image decomposition scheme for image trading systems. Images passed to TTPs are completely invisible, whereas

images sent to consumers are visible but drastically degraded.

3.3 Proposed Scheme

This section proposes a new trading system by using amplitude-only images. Figure 4.1 shows the block diagram of the proposed scheme. In the proposed scheme, an original image is divided into an amplitude-only image which is watermarked by a TTP and a phase-only image which is directly sent to a consumer. The image decomposition and digital fingerprinting in the proposed scheme are described in the subsequent sections and the feature of the proposed scheme is then summarized.

3.3.1 Image Decomposition

In the proposed scheme, $N_1 \times N_2$-sized original image $\mathbf{f} = \{f(n_1, n_2)\}$ where $n_1 = 0, 1, \ldots, N_1 - 1$ and $n_2 = 0, 1, \ldots, N_2 - 1$ is firstly transformed to two-dimensional (2D) discrete Fourier spectra $\mathbf{F} = \{F(k_1, k_2)\}$ where $k_1 = 0, 1, \ldots, N_1 - 1$ and $k_2 = 0, 1, \ldots, N_2 - 1$ by applying 2D discrete Fourier transformation (DFT) to $\mathbf{f}$. That is, image signal $\mathbf{f}$ and spectra $\mathbf{F}$ are given as,

$$f(n_1, n_2) = \frac{1}{N_1 N_2} \sum_{k_1=0}^{N_1-1} \sum_{k_2=0}^{N_2-1} F(k_1, k_2)\, W_{N_1}^{-k_1 n_1} W_{N_2}^{-k_2 n_2}, \tag{3.1}$$

$$F(k_1, k_2) = \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} f(n_1, n_2)\, W_{N_1}^{k_1 n_1} W_{N_2}^{k_2 n_2}, \tag{3.2}$$

where, $W_{N_1} = \exp\left(-j\frac{2\pi}{N_1}\right)$, $W_{N_2} = \exp\left(-j\frac{2\pi}{N_2}\right)$, and $j = \sqrt{-1}$.

Spectra $\mathbf{F}$ can be divided to amplitude and phase spectra as

$$\mathbf{F}_a = \{F_a(k_1, k_2)\} = \{|F(k_1, k_2)|\}, \tag{3.3}$$

$$\mathbf{F}_p = \left\{F_p(k_1, k_2)\right\} = \left\{\frac{F(k_1, k_2)}{|F(k_1, k_2)|}\right\}, \tag{3.4}$$

where $\mathbf{F}_a$ and $\mathbf{F}_p$ are amplitude and phase spectra, respectively. Applying the

inverse DFT to $\mathbf{F}_a$ and $\mathbf{F}_p$, $N_1 \times N_2$-sized amplitude-only image $\mathbf{f}_a$ and $N_1 \times N_2$-sized phase-only image $\mathbf{f}_p$ are generated, respectively.

A TPP receives $\mathbf{f}_a$ and it generates watermarked amplitude-only image $\hat{\mathbf{f}}_a$. A consumer receives watermarked amplitude-only image $\hat{\mathbf{f}}_a$ from the TPP and phase-only image $\mathbf{f}_p$ from a CP. By applying 2D-DFT to $\hat{\mathbf{f}}_a$ and $\mathbf{f}_p$, watermarked amplitude spectra $\hat{\mathbf{F}}_a$ and phase spectra $\mathbf{F}_p$ are obtained, respectively. Watermarked spectra $\hat{\mathbf{F}}$ is obtained by composite $\hat{\mathbf{F}}_a$ and $\mathbf{F}_p$, and watermarked image $\hat{\mathbf{f}}$ is finally obtained by applying the inverse DFT to $\hat{\mathbf{F}}$.

3.3.2 Digital Fingerprinting

In the proposed scheme, amplitude-only image $\mathbf{f}_a$ is used for digital fingerprinting. As most fingerprinting techniques modify the amplitude components of images, almost any arbitrary fingerprinting techniques are applicable to the proposed scheme.

It is noted that the size of amplitude-only image $\mathbf{f}_a$ is the same as original image $\mathbf{f}$ as mentioned in the previous section whereas the size of the image sent to TTP to be watermarked is smaller than the original image in the conventional schemes [48–53]. This brings more payload capacity, more robustness, or better image quality in the proposed scheme while using most fingerprinting techniques.

3.3.3 Features

This section summarizes the features of the proposed scheme, namely, an amplitude-only image is unrecognizable and it has the same image size as the original image.

The proposed scheme divides an original image in the frequency domain, whereas the conventional schemes [48–53] do in the spatial domain. It has two advantages. The first one is that the amplitude-only image is unrecognizable [56, 57] and it gives no valuable information about the original image to a TTP, i.e., the TTP will has no knowledge about what kind of image the consumer is purchasing. The second advantage is that phase-only image is recognizable [56, 57] and

the consumer can confirm whether the piece is for the image which he/she purchased. The phase-only image is degraded and has no commercial value by itself, so the copyright of the image is protected. It is concluded that the usage of amplitude- and phase-only images makes copyright- and privacy-protected image trading systems practical.

The proposed scheme embeds fingerprints to amplitude-only images. Most digital fingerprinting techniques modify the amplitude of images, so almost any arbitrary fingerprinting techniques can be used in the proposed image trading system. In addition, an amplitude-only image has the same size as the original image, whereas the image to be passed to a TTP is smaller than the original image in the conventional schemes [48–53]. The proposed scheme, thus, has an advantage that watermarked images are less degraded, more robust, or have larger capacity in comparison with the conventional schemes [48–53].

3.4 Experimental Results

This section confirms that piece 'I1' which is directly sent to a consumer and piece 'I2' which is sent to a TTP to be watermarked have the following properties in the proposed scheme:

1. Image 'I' can be recognized from 'I1.'
2. Piece 'I1' has no commercial value.
3. No one can estimate the original image 'I' from 'I2.'
4. TTP can robustly embed a watermark into piece 'I2.'

1), 2), and 3) are discussed in Section 4.4.1, and 5) is discussed in Section 4.4.3.

3.4.1 Unrecognizability and Recognizability of Pieces

Figures 4.3 (a) and (b) show amplitude-only image $\mathbf{f}_a$ (piece 'I2') and phase-only image $\mathbf{f}_p$ (piece 'I1') of original image $\mathbf{f}$ (image 'I') shown in Fig. 4.3 (a), respec-

tively.

1) As shown in Fig. 4.3 (b), the edge of the original image is left, so original image 'I' can be recognized. In this way, the consumer can confirm the image he/she bought.

2) Piece 'I1' only reveals the edges of the original image as shown in Fig. 4.3 (b), it obviously has no commercial value.

3) Since piece 'I2' shown in Fig. 3.3 (c) is obtained by interleaving blocks, there is a chance that piece 'I2' can be reconstructed similar to 'I1' which is shown in Fig. 3.3 (b). As image 'I' can be estimated from 'I1,' it is quite possible to estimate 'I' from deinterleaved 'I2.' Even the whole original image can't be estimated, several blocks may leak sensitive information about 'I.' For example, conventional schemes [48–53] are applied to the image shown as Fig. 3.5 (a), the flight number on the tail of the airplane might be left. In contrast, piece 'I2' shown in Fig. 4.3 (a) is completely unrecognizable [56, 57] in the proposed scheme, i.e., no valuable information can be obtained.

It is, thus, concluded that the proposed scheme protects consumer's privacy against accidental information leakage from the TTP, whereas the conventional schemes [48–53] cannot completely protect the privacy as shown as Figs. 3.3 (c) and 3.5 (f).

3.4.2 Fingerprinting Performance

The robustness of the digital fingerprinting in the proposed scheme is compared with the conventional scheme 2 [53] by using the data hiding technique described in the next section.

Fingerprinting Technique

Almost any arbitrary data hiding technique can be used in the proposed and conventional schemes [53], an image quality guaranteeing block discrete cosine transformation (DCT)-based data hiding technique [60] is used as an example of the

digital fingerprinting technique here.

Figure 3.8 shows the block diagram of the embedding technique. $N_1 \times N_2$-sized amplitude-only image $\mathbf{f}_a$ is divided into $B_x \times B_y$-sized blocks, and 2D DCT is applied in each block. The embedding technique modifies T of DCT coefficients in each $B_x \times B_y$-sized block to embed watermark to $\mathbf{f}_a$, where $0 < T \leq B_x B_y$ and T coefficients are selected from low frequency coefficients. After modification of T DCT coefficients, applying inverse 2D DCT and block composition give watermarked amplitude-only image $\hat{\mathbf{f}}_a$.

It is assumed that the digital fingerprint for consumer i is $\mathbf{w}_i$ with length L;

$$\mathbf{w}_i = \{w_{i,l}\}, \tag{3.5}$$

where $l = 0, 1, \ldots, L-1$. It is also assumed that $\left|w_{i,l} - \bar{w}_i\right|$ is finite, where $\bar{w}_i$ is the average of $\mathbf{w}_i$ and σ_w is the standard deviation of $\mathbf{w}_i$. For binary sequence $\mathbf{w}_i = \{w_{i,l} \in \{0, 1\}\}$, $\bar{w}_i = 0.5$ and $\sigma_w = 0.5$. Fingerprint $\mathbf{w}_i$ is adjusted to $\mathbf{w}'_i = \left\{w'_{i,l}\right\}$ as

$$w'_{i,l} = a\left(w_{i,l} - \bar{w}_i\right) \tag{3.6}$$

before data hiding, where a is the scaling constant given by

$$a = \frac{M_\sigma Q}{2N_\sigma \sigma_w}. \tag{3.7}$$

Finally, T of DCT coefficients in each $B_x \times B_y$-sized block are modified to watermark as

$$\hat{c}_t = Q\,\mathrm{round}\left(\frac{c_t}{Q}\right) + w'_{i,l}, \tag{3.8}$$

where c_t is the t-th chosen coefficient and $t = 0, 1, ..., T-1$. Function round$(\cdot)$ returns the nearest integer of the input. Hidden fingerprint $\hat{w}_{i,l}$ is easily extracted

by

$$\hat{w}'_{i,l} = \hat{c}_t - Q\,\mathrm{round}\left(\frac{\hat{c}_t}{Q}\right), \tag{3.9}$$

$$\hat{w}_{i,l} = \left(\frac{\hat{w}'_{i,l}}{a} + \bar{w}_i\right). \tag{3.10}$$

M_σ is used for energy adjustment and $0 < M_\sigma < 1$. Q is the quantization step for data hiding and it is given by

$$Q = 10^{-0.05R}\sqrt{\frac{\sum_{n_1=0}^{N_1-1}\sum_{n_2=0}^{N_2-1} f_a^2(n_1,n_2)}{\frac{N_1N_2}{B_xB_y}\frac{T}{D}}}, \tag{3.11}$$

where $f_a(x,y)$ is the pixel value at position (x,y) of image $\mathbf{f}_a$. R is the desired signal-to-watermark ratio (SWR) which this fingerprinting technique guarantees the SWR of a watermarked image becomes R [dB]. The SWR is defined as,

$$\mathrm{SWR} = 10\log_{10}\frac{\sum_{n_1=0}^{N_1-1}\sum_{n_2=0}^{N_2-1} f_a^2(n_1,n_2)}{\sum_{n_1=0}^{N_1-1}\sum_{n_2=0}^{N_2-1}\left\{f_a(n_1,n_2) - \hat{f}_a(n_1,n_2)\right\}^2}[\mathrm{dB}]. \tag{3.12}$$

Here, D is given as

$$D = \frac{12N_\sigma^2}{N_\sigma^2 + 3M_\sigma^2}, \tag{3.13}$$

where $T\dfrac{Q^2}{D}$ is the distortion in each block by watermarking. D is set to make sure that watermarking can be extracted without original image, then distortion in each $B_x \times B_y$-sized block can be derived as TQ^2/D. Details can be found in the chapter [60]. Positive number N_σ is chosen to satisfy

$$\left|w_{i,l} - \bar{w}_i\right| \le N_\sigma\sigma_w. \tag{3.14}$$

Table 3.1: Piece size and watermark length in conventional scheme 2 [53] ($B_x = B_y = 8$ and $T = 1$).

Image	Reshaped I2 [pixels]	Embeddable watermark L [bits]
Airplane	64×1920	1920
Baboon	64×1880	1880
Lena	64×1892	1892
Peppers	64×1768	1768
Sailboat	64×1970	1970

R, B_x, B_y, N_σ, M_σ, and $\bar{w}_i$ are common in the trading system. For binary sequence $\mathbf{w}_i$, consumer i is identified by decoding $\hat{\mathbf{w}}_i = \{\hat{w}_{i,l}\}$. For other sequences such as Gaussian sequence, consumer i is identified by a correlation-based detector in which cross correlations between $\hat{\mathbf{w}}_i$ and all possible sequences are calculated, as well as mechanism [58, 59] used in the conventional scheme [53].

Performance

In order to confirm the effectiveness of proposed scheme, the above mentioned data hiding technique [60] is used in the conventional scheme 2 [53] and the proposed scheme under the condition that one coefficient from a 8×8-sized DCT block is used for watermarking ($B_x = B_y = 8$ and $T = 1$). That is, the same embedding technique is used in two different image decomposition schemes. It is noted that the literature [53] says the conventional 2 is better than the conventional 1 [48–52], so the conventional scheme 1 is not evaluated here.

Five 512×512-sized 8-bits grayscale images are used for evaluation, namely, 'Airplane,' 'Baboon,' 'Lena,' 'Peppers,' and 'Sailboat.' Saliency varies from image to image, so the embedding capacity for salience regions also fluctuates as shown in Table 3.1. Based on Table 3.1 and making $\mathbf{w}_i$ a L-bits binary sequence consisting of equiprobable zeros and ones, σ_w, M_σ and N_σ are set to 0.5, 0.5, and 1, respectively.

Table 3.2 shows the averaged correct extracting rate of embedded fingerprint against several attacks provided by StirMark [62, 63] and compression by JPEG

Table 3.2: Averaged correct extracting rate of hidden fingerprints against several attacks provided by StirMark [62, 63] and JPEG 2000 compression [64][1].

(a) Desired signal-to-watermark ratio R is 25 dB.

Attack	Conventional scheme 2 [53]	Proposed scheme
CONV	74.80%	83.15%
JPEG	94.34%	95.86%
MEDIAN	85.11%	94.31%
ROTSCALE	51.01%	66.40%
FMLR	80.87%	88.75%
JPEG 2000	89.78%	94.11%

(b) Desired signal-to-watermark ratio R is 30 dB.

Attack	Conventional scheme 2 [53]	Proposed scheme
CONV	69.62%	80.44%
JPEG	86.53%	91.03%
MEDIAN	74.88%	83.57%
ROTSCALE	50.32%	58.24%
FMLR	66.35%	74.59%
JPEG 2000	82.36%	85.41%

Table 3.3: Quantization steps Q for the same desired SWR (R = 25 [dB]).

Image	Conventional scheme 2 [53]	Proposed scheme
Airplane	90	160
Baboon	132	144
Lena	85	149
Peppers	84	146
Sailboat	83	150

2000 [64]. The same L-bits watermark is hidden to the piece per image in both schemes and the desired SWR for two schemes are the same. From Table 3.2, it was found that the proposed scheme is superior to the conventional scheme 2 [53] in terms of the averaged correct extracting rate of hidden fingerprint.

Because the image sent to TTP is relatively larger in the proposed scheme than that in the conventional scheme 2 [53], the actual embedding strength which is given by quantization step Q in the proposed scheme is relatively larger for the same SWR as shown in Table 3.3. This explains why the proposed scheme is more robust than the conventional scheme 2 [53] as shown in Table 3.2. As mentioned

Table 3.4: SWR improvement in the proposed scheme when quantization steps of conventional scheme 2 [53] shown in Table 3.3 are used.

Image	Quantization step Q	SWR [dB]
Airplane	90	42
Baboon	132	37
Lena	85	38
Peppers	84	37
Sailboat	83	36

above, the literature [53] says the conventional scheme 2 [53] is more robust than the conventional scheme 1 [48–52]. So, it is concluded that the proposed scheme is the best among three schemes in terms of copyright protection.

It is noted the proposed scheme can improve the quality of watermarked images instead of robustness improvement. With quantization steps Q shown in Table 3.3 which are for conventional scheme 2 [53], the averaged SWR in the proposed scheme becomes 38 dB as shown in Table 3.4 whereas $R = 25$ [dB] in conventional scheme 2.

3.5 Conclusions

This chapter has proposed a use of amplitude-only images for privacy- and copyright-protected image trading systems. Amplitude-only images which are passed to the trusted third parties (TTPs) are unrecognizable in the proposed scheme, whereas the images in which valuable content are left are passed to the TPP in the conventional scheme [48–53]. So consumer's privacy is protected from accidental leakage of them from the TTPs in the proposed system. Phase-only images are recognizable, and a consumer can confirm the content which he/she bought. Since most of data hiding techniques modify the amplitude component of images, almost any arbitrary techniques can be used in the proposed scheme where robustness de-

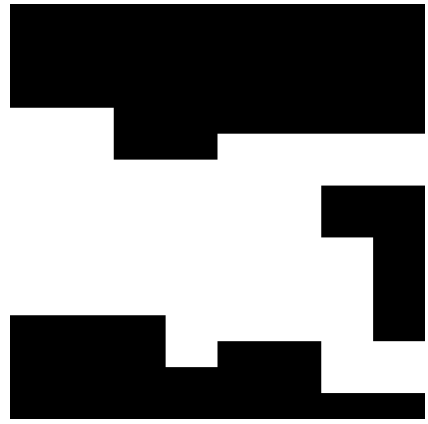
[1]CONV: average of attacks with 3×3 Gaussian filter and those with 3×3 sharpening filter. JPEG: average of compression with parameter 10, 20 ,30, 40, 50, 60, 70, 80 and 90. MEDIAN: average of attacks with 2×2, 3×3, and 4×4 median filters. ROTSCALE: average of rotation with 0.25, 0.5, 0.75, and 1.00 degrees with cropping and scaling. FMLR: Frequency mode Laplacian removal. JPEG2000: average of compression ratio 0.5, 0.1, and 0.05.

pends on the fingerprinting technique itself. With a block DCT-based data hiding technique [60], it was found that the proposed scheme is superior to the conventional schemes [48–53] in terms of the robustness against attacks to watermarked images provided by StirMark [62, 63] and compression by JPEG 2000, because the size of the image to be watermarked is larger than that in the conventional schemes.

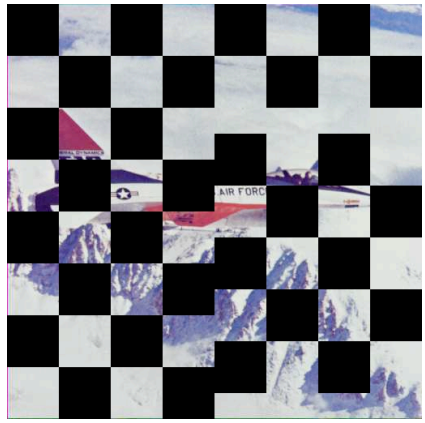
(a) Original image 'I.'

(b) Saliency map [54] of 'I.'

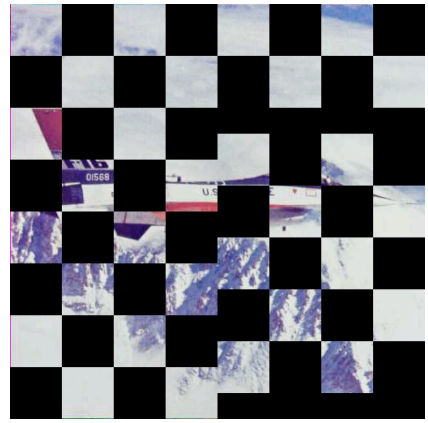
(c) Binarized saliency map.



(d) Block-based saliency map.



(e) Piece 'I1.'



(f) Piece 'I2.'

(g) Reshaped 'I2'.

Figure 3.5: Images in the conventional scheme 2 [53].

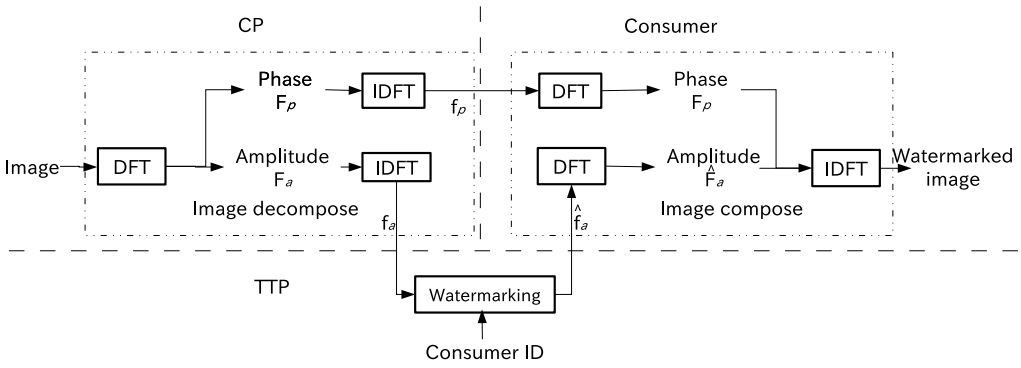
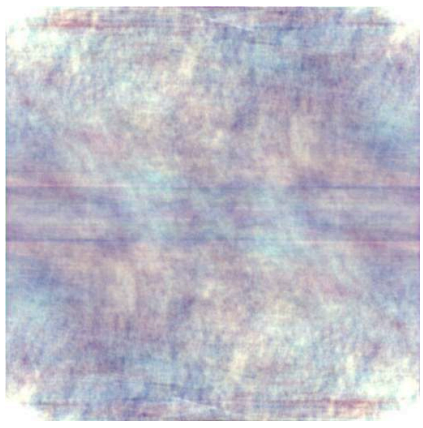
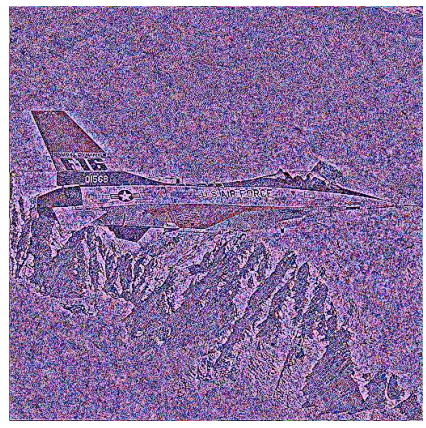


Figure 3.6: Block diagram of the proposed scheme.

(a) Original image **f**.



(b) Amplitude-only image $\mathbf{f}_a$.



(c) Phase-only image $\mathbf{f}_p$.

Figure 3.7: Amplitude-only and phase-only images.

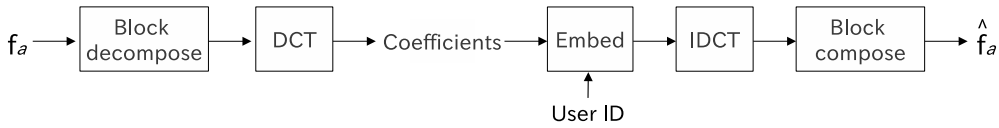


Figure 3.8: Block diagram of watermark technique [60].

Chapter 4

Compression-friendly Image Trading System for Copyright- and Privacy-Protection

4.1 Introduction

In order to protect the copyright held by content providers (CPs) and the privacy of consumers in trading images, a new framework has been proposed [52]; an image is divided into two pieces by a CP where one is directly sent to a consumer from the CP and the other is fingerprinted by a trusted third party (TTP) before the consumer receives it. The consumer obtains the fingerprinted image by combining two received pieces. By doing so, the TTP knows only a part of the content. However, in conventional systems dividing images in the spatial domain [52, 53], an adversary has a possibility to estimate the original image from the piece which is leaked from a TTP, and a fingerprint for copyright protection can only cover a half of the image. The latest system separates an image into an unintelligible amplitude-only image (AOI) and a visible phase-only image (POI) to solve these problems [55], where the AOI and POI are inversely transformed amplitude and phase components of discrete Fourier transformed (DFTed) coefficients of the image, respectively. However, this system does not take compression into account, and it is quite difficult to efficiently compress AOIs.

4.2 Conventional Schemes and Those Problems

In conventional scheme [55], an image purchased by a consumer is divided into an AOI and a POI by using the DFT. The AOI is fingerprinted by a TTP and the POI is directly sent to a consumer; This system reduces the potential information leakage at TTPs by introducing AOIs which are unintelligible. The POI is too distorted to be of commercial value, but the POI reveals the original image and it is useful for consumers to confirm the received image.

Images may be compressed for transmission between a CP and a TTP and between the TTP and a consumer in practical scenarios, conventional system [55] has never taken compression into account.

4.3 Proposed Scheme

This section proposes an efficient compression scheme of AOIs for the copyright- and privacy-protected image trading system. As shown in Fig. 4.1, the proposed scheme applies the DCT instead of DFT to an original image for generating the AOI, where the phase component of DCT coefficients are the positive and negative signs, i.e., ± 1, which can be transmitted with one bit per coefficient without compression. By multiplying random signs to the amplitude component of DCT coefficients, the scheme compresses AOIs efficiently.

The image decomposition, quantization and compression, digital fingerprinting, image composition, and fingerprint extraction in the proposed scheme are described in the subsequent sections and the feature of the proposed scheme is then summarized.

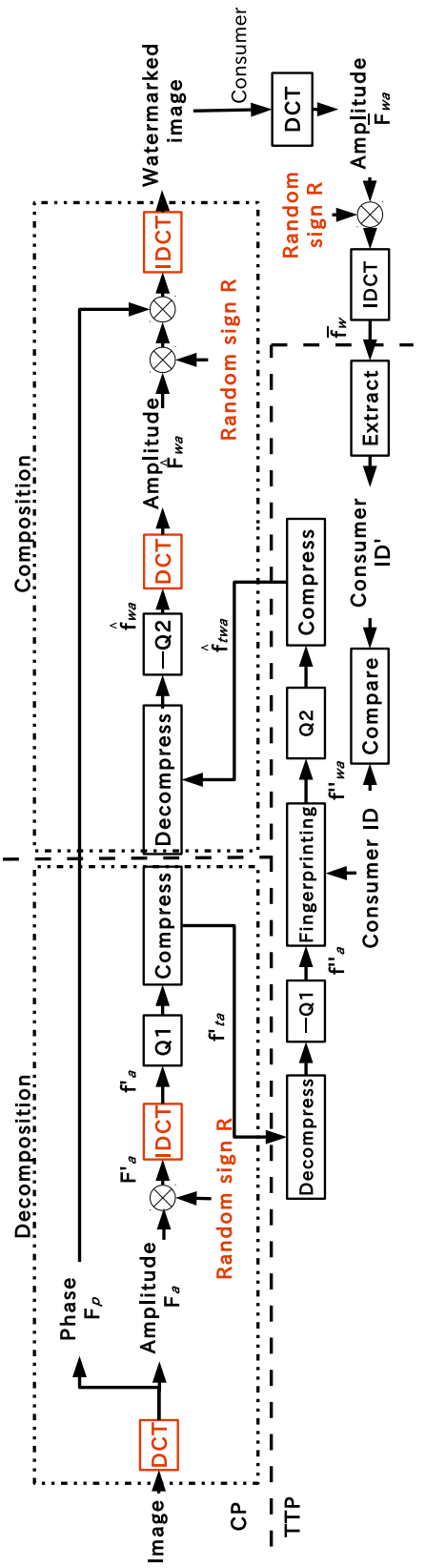


Figure 4.1: Block diagram of the proposed scheme. Q1: quantization between a CP and a TTP, −Q1: inverse quantization for Q1, Q2: quantization between the TTP and a consumer, −Q2: inverse quantization for Q2.

4.3.1 Compression-Friendly Image Decomposition

Firstly, a CP divides $N_1 \times N_2$-sized original image $\mathbf{f} = \{f(n_1, n_2)\}$ to $N_1 \times N_2$-sized AOI $\mathbf{f}'_a = \{f'_a(n_1, n_2)\}$ and $N_1 \times N_2$-sized phase components $\mathbf{F}_p = \left\{F_p(k_1, k_2)\right\}$ where $n_1 = 0, 1, \ldots, N_1 - 1$, $n_2 = 0, 1, \ldots, N_2 - 1$, $k_1 = 0, 1, \ldots, N_1 - 1$, and $k_2 = 0, 1, \ldots, N_2 - 1$.

1. The CP applies two-dimensional (2D) DCT to $\mathbf{f}$ to get $N_1 \times N_2$-sized 2D-DCT coefficients $\mathbf{F} = \{F(k_1, k_2)\}$;

$$F(k_1, k_2) = \alpha(k_1)\alpha(k_2)\sum_{n_1=0}^{N_1-1}\sum_{n_2=0}^{N_2-1} f(n_1, n_2)C(n_1, k_1, N_1)C(n_2, k_2, N_2), \quad (4.1)$$

where

$$\alpha(k_1) = \begin{cases} \sqrt{1/N_1}, & k_1 = 0 \\ \sqrt{2/N_1}, & \text{otherwise} \end{cases}, \quad (4.2)$$

$$\alpha(k_2) = \begin{cases} \sqrt{1/N_2}, & k_2 = 0 \\ \sqrt{2/N_2}, & \text{otherwise} \end{cases}, \quad (4.3)$$

$$C(n_1, k_1, N_1) = \cos\frac{(2n_1 + 1)k_1\pi}{2N_1}, \quad (4.4)$$

$$C(n_2, k_2, N_2) = \cos\frac{(2n_2 + 1)k_2\pi}{2N_2}. \quad (4.5)$$

2. Separate real numbered DCT coefficients $\mathbf{F}$ into amplitude components $\mathbf{F}_a = \{F_a(k_1, k_2)\}$ and phase components $\mathbf{F}_p$ as

$$F_a(k_1, k_2) = |F(k_1, k_2)|, \quad (4.6)$$

$$F_p(k_1, k_2) = \text{sgn}\left(F(k_1, k_2)\right), \quad (4.7)$$

where $F_a(k_1, k_2)$ and $F_p(k_1, k_2)$ are amplitude and phase component of $F(k_1, k_2)$, respectively, and sgn$(\cdot)$ returns the positive and negative sign of the input.

It is noted that

$$F(k_1, k_2) = F_a(k_1, k_2)F_p(k_1, k_2). \tag{4.8}$$

3. $N_1 \times N_2$-sized random matrix $\mathbf{R} = \{R(k_1, k_2)\}$ which consists of ± 1 is multiplied to $\mathbf{F}_a$ as

$$\mathbf{F}'_a = \mathbf{F}_a \circ \mathbf{R}, \tag{4.9}$$

where $\circ$ represents Hadamard product.

4. Applying the inverse 2D DCT (2D-IDCT) to $\mathbf{F}'_a$ generates AOI $\mathbf{f}'_a$, where 2D-IDCT of $\mathbf{F}$ is defined as

$$f(n_1, n_2) = \sum_{k_1=0}^{N_1-1} \sum_{k_2=0}^{N_2-1} \alpha(k_1)\alpha(k_2)F(k_1, k_2)C(n_1, k_1, N_1)C(n_2, k_2, N_2). \tag{4.10}$$

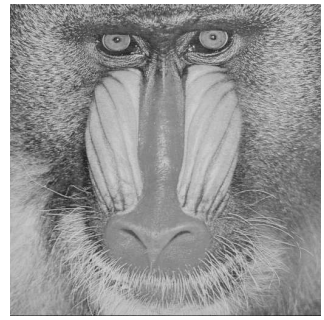
4.3.2 Quantization and Compression

AOI $\mathbf{f}'_a$ consisting of real numbers is processed to be transferred to a TTP from the CP; quantization as Q1 shown in Fig. 4.1 and compression.

1. Quantize AOI $\mathbf{f}'_a$ to an image with K-bit integers.
2. Compress quantized AOI.
3. The CP sends quantized and compressed AOI to the TTP, whereas the CP sends phase components $\mathbf{F}_p$ to a consumer.

It is noted that any arbitrary quantization and image compression techniques can be employed here in the proposed scheme. In addition, phase component $\mathbf{F}_p$ are just positive and negative signs in the proposed scheme, i.e., one bit per coefficient, the CP sends $\mathbf{F}_p$ to a consumer efficiently even without compression.

(a) Airplane.



(b) Baboon.

(c) Lena.

(d) Peppers.

(e) Sailboat.

Figure 4.2: Five 512×512-sized 8-bit grayscale images for evaluation.

4.3.3 Digital Fingerprinting

The TTP hides the consumer's fingerprint $\mathbf{w}$ to received AOI.

1. The TTP decompress and inversely quantizes the received image to obtain $\mathbf{f}''_a = \{f''_a(n_1, n_2)\}$.

2. Hide $\mathbf{w}$ into $\mathbf{f}''_a$ and watermarked AOI $\mathbf{f}''_{wa} = \{f''_{wa}(n_1, n_2)\}$ is generated.

3. Quantize as Q2 shown in Fig. 4.1 and compress $\mathbf{f}''_{wa}$ for sending it to the consumer.

It is noted that any arbitrary digital fingerprinting technique which hides data to the amplitude components of the image can be used in the proposed scheme, as an implementation [59] of a well-known spread spectrum-based technique [58] is used in conventional system 1 [53] and as an image quality guaranteed technique [60, 61] is used in conventional system 2 [55].

Table 4.1: Range of amplitude-only image $\mathbf{f}_a$ and random-sign image $\mathbf{f}'_a$.

Image	Airplane	Baboon	Lena	Peppers	Sailboat
$\mathbf{f}_a$	7192	9851	7134	6490	8490
$\mathbf{f}'_a$	403	331	383	378	477

4.3.4 Image Composition

The consumer gets $N_1 \times N_2$-sized watermarked image $\hat{\mathbf{f}}_w = \left\{\hat{f}_w(n_1, n_2)\right\}$ from received two pieces.

1. Decompress and inversely quantized the received watermarked-quantized-compressed AOI to obtain watermarked AOI $\hat{\mathbf{f}}_{wa} = \left\{\hat{f}_{wa}(n_1, n_2)\right\}$.
2. Apply 2D-DCT to $\hat{\mathbf{f}}_{wa}$ to generate amplitude components $\hat{\mathbf{F}}_{wa} = \left\{\hat{F}_{wa}(k_1, k_2)\right\}$.
3. Multiply $\mathbf{R}$ to $\hat{\mathbf{F}}_{wa}$ as $\hat{\mathbf{F}}_{wa} \circ \mathbf{R}$.
4. Combine the above processed amplitude components and received $\mathbf{F}_p$ to form watermarked DCT coefficients.
5. Apply 2D-IDCT to the watermarked DCT coefficients to get watermarked image $\hat{\mathbf{f}}_w$.

4.3.5 Fingerprint Extraction

From a suspected image which is identical or similar to $\hat{\mathbf{f}}_w$, the TTP extracts the fingerprinting as follows,

1. Apply 2D-DCT to the suspected image to get amplitude component $\bar{\mathbf{F}}_{wa}$.
2. Apply 2D-IDCT to $\bar{\mathbf{F}}_{wa} \circ \mathbf{R}$ to get image $\bar{\mathbf{f}}_w$.
3. Extract fingerprinting $\mathbf{w}$ from $\bar{\mathbf{f}}_w$.

By comparing the extracted fingerprinting with the fingerprinting stored at the TTP, the malicious consumer can be identified.

4.3.6 Features

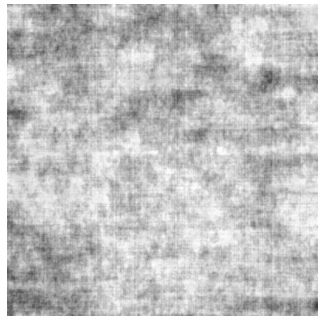
Besides the same features as conventional system 2 [55] that an AOI is unintelligible and has the same size as the original image, the main feature of the proposed scheme is efficient compression of two separated pieces. This feature is achieved by introducing the DCT and random signs.

The 2D-DCT is used in the proposed scheme whereas conventional system 2 [55] employes the 2D-DFT, even the proposed scheme separates an original image in a transformed domain as well as conventional system 2. The POI in conventional system 2 consists of real numbers, so it should be quantized and compressed to be transmitted from a CP to a consumer. In contrast, the phase components in the proposed scheme consist of just positive and negative signs, i.e., ± 1, so it can be transmitted with one bit per coefficient without quantization and compression.

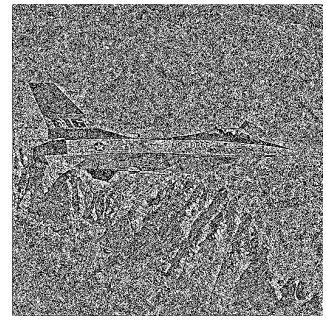
As shown in Table 4.1, the ranges of random-sign images are about $\frac{1}{30} \sim \frac{1}{20}$ ranges of amplitude-only images. Random sign dramatically reduces the range of AOI, because initial phases are randomized so that the sum peak of initial phases is reduced. The proposed scheme efficiently compress unintelligible AOIs, whereas it is generally hard to compress perceptually encrypted images efficiently. The scheme applies random signs to amplitude component of 2D-DCT coefficients of the original image before applying 2D-IDCT to the amplitude component to generate an AOI. Random signs reduce quantization and compression errors of AOIs. That is, an efficient compression of AOIs is achieved. It is noted that AOIs in the proposed scheme are still unintelligible, so the consumers' privacy are well protected as conventional system 2 does [55].

4.4 Experimental Results

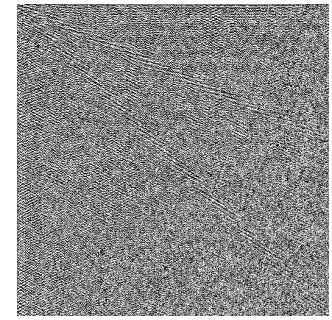
By using five grayscale images shown in Fig. 4.2, this section confirms that piece $\mathbf{F}_p$ which is directly sent to a consumer and piece $\mathbf{f}_a$ which is sent to a TTP to be watermarked have the following properties in the proposed scheme:



(a) AOI $\mathbf{f}_a$ of Fig. 3.5 (a).



(b) POI $\mathbf{f}_p$ of Fig. 3.5 (a).



(c) Phase components $\mathbf{F}_p$ of Fig. 3.5 (a).

Figure 4.3: Images in the proposed scheme. Images are based on 2D-DCT.

1. Original image $\mathbf{f}$ can be recognized from $\mathbf{f}_p$.
2. Piece $\mathbf{f}_p$ has no commercial value.
3. No one can estimate original image $\mathbf{f}$ from $\mathbf{f}_a$.
4. Two pieces are efficiently compressed.
5. A TTP can embed a fingerprint into piece $\mathbf{f}_a$ robustly to quantization and compression.

1), 2), and 3) are discussed in Section 4.4.1, 4) and 5) are discussed in Sections 4.4.2 and 4.4.3, respectively.

4.4.1 Unrecognizability and Recognizability of Pieces

Figures 4.3 (a) and (b) show AOI $\mathbf{f}_a$ and POI $\mathbf{f}_p$ of the proposed scheme for original image $\mathbf{f}$ shown in Fig. 3.5 (a), respectively. It is noted that $\mathbf{f}_p$ is easily obtained by applying 2D-IDCT to phase component $\mathbf{F}_p$ shown in Fig. 4.3 (c).

1) As shown in Fig. 4.3 (b), the edge of the original image is left, so original image $\mathbf{f}$ can be recognized. In this way, the consumer can confirm the image he/she bought as well as in conventional system 2 [55].

2) Piece $\mathbf{f}_p$ only reveals the edges of the original image as shown in Fig. 4.3 (b), it obviously has no commercial value as well as in conventional system 2.

3) As shown in Fig. 4.3 (a), it is quite hard to estimate original image $\mathbf{f}$ from AOI $\mathbf{f}_a$ as well as conventional system 2. In contrast, there is a chance that estimation of $\mathbf{f}$ from piece 'I2' is successful in spatial domain-based conventional systems [52, 53].

It is concluded that the proposed scheme protects consumer's privacy against accidental information leakage from the TTP as well as conventional system 2 [55].

4.4.2 Compression Performance

Here, a simple linear quantizer given as

$$q(n_1, n_2) = \text{round}\left(\frac{f(n_1, n_2) - \min_{n_1,n_2} f(n_1, n_2)}{s}\right), \tag{4.11}$$

$$s = \frac{\max_{n_1,n_2} f(n_1, n_2) - \min_{n_1,n_2} f(n_1, n_2)}{2^K - 1}, \tag{4.12}$$

$$Q(n_1, n_2) = sq(n_1, n_2) + \min_{n_1,n_2} f(n_1, n_2), \tag{4.13}$$

is employed for quantizing AOIs and POIs, where $q(n_1, n_2) \in [0, 2^K - 1]$ and $Q(n_1, n_2)$ are quantized and inversely quantized images of $f(n_1, n_2)$, respectively. A set of rounding real numbers to integers and clipping integers into $[0, 2^K - 1]$ is compared with the quantizer.

Kakadu [64], a JPEG 2000 codec, is used for compression/decompression of quantized AOIs and POIs here. Compression rate c is given as $c = c_a + c_p$ where c_a and c_p are the compression rate for an AOI and a POI, respectively. It is noted that c_p is always one in the proposed scheme as mentioned in Section 4.3.2.

Figure 4.4 shows the peak signal-to-noise ratio (PSNR) between reconstructed and original 'Lena'. Note that fingerprints are not hidden into AOIs here. From Fig. 4.4, the simple linear quantization is obviously superior to rounding and clipping. In addition, regardless of quantization technique, random signs drastically improve the quality of reconstructed images. Moreover, a perceptual encryption by random permutation of the original image degrades compression performance because of the loss of the correlation between neighboring pixels, whereas the

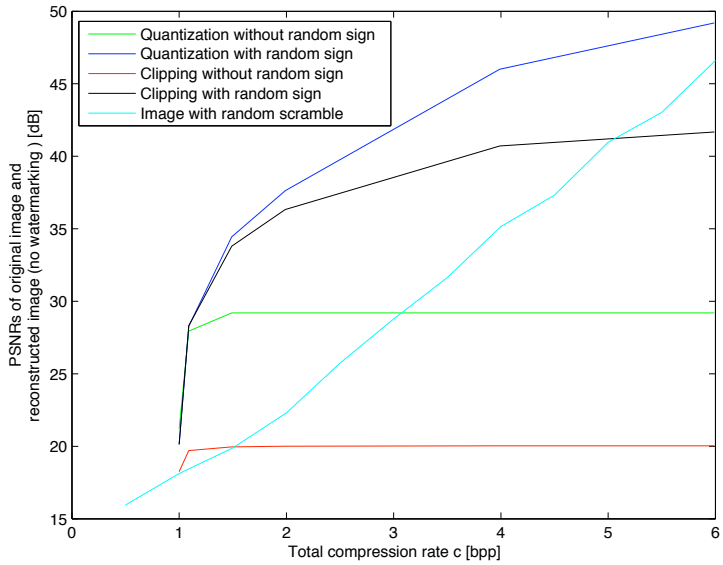


Figure 4.4: PSNR's of reconstructed 'Lena'. The proposed scheme using the quantization and the random signs is the best.

correlation partially remains in an AOI.

The PSNR's averaged over five test images are evaluated in the proposed scheme and conventional system 2 [55], where $c_a = c_p = c/2$ for conventional system 2. It is confirmed from Fig. 4.5 that the proposed scheme (DCT with random signs) is superior to conventional system 2 (DFT without random signs). From the figure, it is also confirmed that introducing random signs much improves the compression efficiency.

It is concluded that the proposed scheme compresses $\mathbf{f}_a$ and $\mathbf{F}_p$ efficiently, i.e., property 4) is satisfied.

4.4.3 Fingerprinting Performance

The robustness of fingerprinting is compared between the proposed scheme and conventional system 1 [53], because the previous section shows that the quality of reconstructed images in conventional system 2 [55] is too degraded. Even any arbitrary fingerprinting technique can be used in the proposed scheme and con-

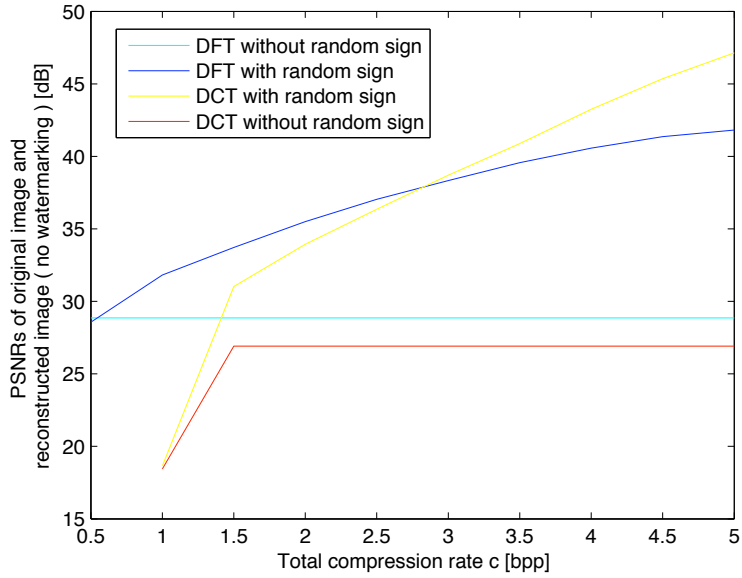


Figure 4.5: PSNR's comparison between the proposed scheme (DCT with random signs) and conventional system 2 [55] (DFT without random signs). The quantizer is used.

ventional system 1 as mentioned in Section 4.3.3, the image quality-guaranteed data hiding technique [60, 61] employed for performance evaluation in the literature [55] is used here. This technique can control the energy of a watermark sequence, and this section utilizes this feature of the technique to set the PSNR of watermarked images the same regardless of scheme or system. It is noteworthy that the fingerprinting performance depends on the used fingerprinting technique.

Tables 4.2 and 4.3 show the fingerprinting performance of the proposed scheme and conventional system 1 [53] where the embedding strength for each image are the same between tables. Total compression ratio c is set to 5 bits per pixel (bpp) for keeping watermarked images with high quality in Table 4.2 where two pieces are equally compressed with 2.5 bpp in conventional system 1 and an AOI is compressed with 4 bpp and the phase component is sent with 1 bpp in the proposed scheme. The payload size which is the length of a binary fingerprint fluctuates according to images, but those of the proposed scheme and conventional system 1 are set to be the same.

Table 4.2: Fingerprinting performance comparisons. Compression rate $c = 5$ [bpp]. BER: bit error rate.

Image	Payload size [bits]	Proposed scheme		Conventional system 1 [53]	
		PSNR [dB]	BER [%]	PSNR [dB]	BER [%]
Airplane	1920	44.34	0.0	44.05	0.0
Baboon	1880	40.24	0.0	40.14	0.0
Lena	1892	44.44	0.0	44.12	0.0
Peppers	1768	45.08	0.0	44.41	0.0
Sailboat	1970	42.90	0.0	42.88	0.0

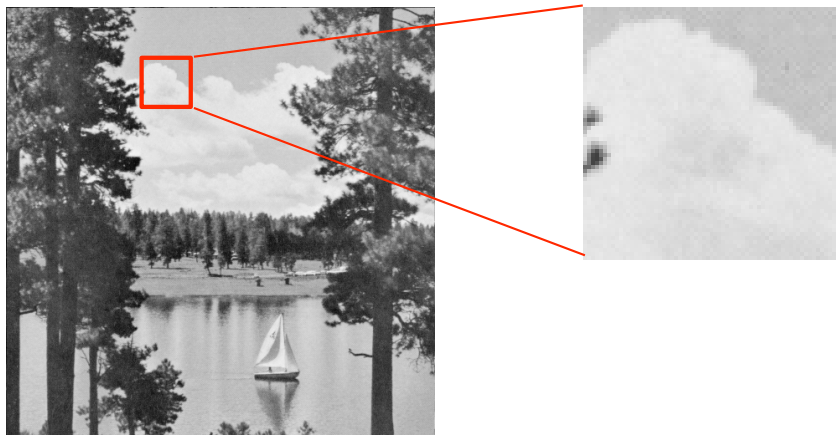
Table 4.3: Fingerprinting performance of the proposed scheme. The payload size and embedding strength are the same as those in Table 4.2.

Image		Total compression rate c [bpp]					
		2.5	3.0	3.5	4.0	4.5	5.0
Airplane	PSNR [dB]	38.42	40.33	42.23	42.98	43.74	44.34
	BER [%]	41.3	19.6	12.1	0.0	0.0	0.0
Baboon	PSNR [dB]	30.00	32.14	34.30	36.64	38.57	40.24
	BER [%]	46.9	46.4	30.4	25.9	5.8	0.0
Lena	PSNR [dB]	39.17	40.76	42.37	43.18	44.32	44.44
	BER [%]	32.9	12.7	11.9	1.8	0.0	0.0
Peppers	PSNR [dB]	37.37	39.17	40.64	42.36	44.13	45.08
	BER [%]	43.7	21.7	14.3	4.7	0.0	0.0
Sailboat	PSNR [dB]	35.08	37.18	38.87	40.39	41.66	42.90
	BER [%]	47.2	33.4	20.8	20.3	2.3	0.0

It is found from Table 4.2 that the proposed scheme is comparable to conventional system 1 [53] in terms of the PSNR of watermarked image and the robustness to image compression. Watermarked images in conventional system 1, however, have a severe security problem; the watermarked areas which belong to piece 'I2' are revealed as shown in Fig. 4.6 (a). Conventional system 1 divides an original image into two pieces in the spatial domain which only piece 'I2' is watermarked and piece 'I1' is left as is [53], and it makes watermarked areas recognizable. So, there is a chance for a malicious consumer to remove or corrupt the hidden fingerprint.

Table 4.3 shows an example of fingerprinting performance in the proposed scheme in which the performance gets worse as the compression rate becomes

(a) Conventional scheme [53].



(b) Proposed scheme.

Figure 4.6: Watermarked images of 'sailboat' in conventional system 1 [53] and the proposed scheme. The PSNR is 42.9 [dB] for both images.

lower. This scheme suppresses the error to 20 % for images with the PSNR over 40 dB even it embeds about 2000 bits data. It should be mentioned again that the performance depends on the used fingerprinting technique.

It is concluded that the proposed scheme is robust to image compression. That is, the proposed scheme has property 5). In addition, the proposed scheme takes compression into account, the proposed scheme makes the image trading system practical.

4.5 Conclusions

This chapter has proposed an efficient compression scheme of AOIs for the copyright- and privacy-protected image trading system. The proposed scheme introduces the DCT to the piece splitting process so that a CP sends a piece to a consumer without compression, whereas conventional system 2 uses the DFT [55] and the CP sends a piece to the consumer with quantization and compression. The scheme further introduces random signs for generation of AOIs so that it reduces quantization and compression error to AOIs. These strategies improve compression efficiency in comparison to conventional system 2. In addition, it was found that fingerprinting performance of the proposed scheme is superior to conventional system 1 [53]. The proposed scheme makes the image trading system practical.

Chapter 5

Cheating Prevention Visual Cryptography

5.1 Introduction

In recent years, powerful computers offer even ordinary users the encryption of secret information. To encrypt and decrypt secret information, a key (or a key pair) is used and should be securely and safely guarded. This straightforward key protection, however, still has the risk of key loss and leakage. On the other hand, with the development of fast network technologies, many people collaborate on secret projects over the public Internet. Information should be secret even a few member collude to leak the secret information. To overcome such situations, secret sharing (SS) has been proposed [65].

A SS scheme [65] divides a secret into n pieces referred to as shares. n shares are held by n different parties and the secret is recovered if and only if k or more shares are gathered. This scheme is called as a (k, n)-threshold SS scheme. Even computer technology is highly developed, it is not always possible to use computer. In order to overcome these situations, visual SS (VSS) in which decryption can be done by human eyes has been proposed for binary images [66].

Later, VSS has been extended to non-binary images [67, 68]. Color VSS have also been proposed [69–71]. Instead of random share images [66], meaningful

shares are employed in a scheme [72]. Some schemes [73, 74] allow to embed multi-secret within one image. A weaken security scheme [75,76] is also proposed to improve the visuality of recovered image. Other direction reduces the pixel expansion size and improves the contrast of the recovered image [77, 78].

On the other hand, it is assumed in a scenario that malicious parties deceive an honest party, and cheat-prevention VSS schemes have been proposed to fight it [53, 79, 80, 82]. This chapter focuses on cheat-prevention VSS. A literature [81] found that the original cheat-prevention VSS scheme [80] is not well function in some circumstances. The literature [81] also proposes a new scheme, but pixel expansion is sacrificed significantly. Later, the same authors proposed another scheme [82] with less pixel expansion, but its application is limited to $(2, n)$-threshold VSS and it introduces a further restriction.

This chapter proposes a new cheat-prevention VSS scheme which solves the problem in the original cheat-prevention VSS scheme [80] without sacrificing pixel expansion. By introducing randomness into share generation, it simultaneously overcomes the above mentioned two problems in the conventional schemes [53, 80]. In addition, the proposed scheme can be applied to (k, n)-threshold VSS, whereas a latest scheme [82] which is only applicable to $(2, n)$-threshold VSS.

The rest of this chapter is arranged as follows. In Section 5.2, SS [65], VSS [66], and the concept of cheat-prevention VSS will be reviewed. Conventional cheat-prevention VSS schemes [53, 80, 82] are introduced in Section 5.3. The improved scheme is proposed in Section 5.4. Experimental results are shown in Section 5.5 and conclusions and future works are given in Section 5.6.

5.2 Preliminaries

This section briefly describes secret sharing (SS), visual SS (VSS), and cheat-prevention VSS.

5.2.1 Secret Sharing

Here, a (k, n)-threshold SS method [65] in which k of n shares should be gathered to recover the secret information is described with introducing terms and notations.

Let $\mathbf{P} = \{P_1, P_2, \ldots, P_n\}$ be the set of n parties, and each party P_i holds share S_i where $i = 1, 2, \ldots, n$. Let $2^{\mathbf{P}}$ be the set of all subsets of $\mathbf{P}$.

Let Γ_Q and Γ_F be the qualified sets and forbidden sets, respectively. Assume Γ_Q is monotone increasing and Γ_F is monotone decreasing. Denote Γ_Q^* and Γ_F^* as the minimum qualified sets and the maximum forbidden sets.

Here, $(\mathbf{P}, \Gamma_Q, \Gamma_F)$ is an access structure if $\Gamma_Q \cap \Gamma_F = \emptyset$ and $\Gamma_Q \cup \Gamma_F = 2^{\mathbf{P}}$. Access structure $(\mathbf{P}, \Gamma_Q, \Gamma_F)$ for a (k, n)-threshold SS method is that $X \in \Gamma_Q$ if and only if $|X| \geq k$, where $|X|$ is the number of parties in X.

5.2.2 Visual Secret Sharing

VSS is a kind of secret sharing [66], so the access structure of VSS is the same as SS. There are two differences between VSS and SS; 1) images are used as shares in VSS and 2) decryption needs no computations, it is done by human eyes of watching stacked share images.

Let $\mathbf{S}^0$ and $\mathbf{S}^1$ be the $n \times m$-sized basic matrices for the share image generation in a black-and-white VSS method where $\mathbf{S}^0$ and $\mathbf{S}^1$ are for white and black pixels, respectively. For example, in the original (k, n)-threshold VSS method [66] in which a pixel in a secret image is expanded to m subpixels in share image S_i, $\mathbf{S}^0$ and $\mathbf{S}^1$ are given as

$$\mathbf{S}^0 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \quad \text{and} \quad \mathbf{S}^1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{5.1}$$

under the condition that $n = m = 3$ and $k = 2$. Each party P_i holds share image S_i where $i = 1, 2, \ldots, n$. This $(2, 3)$-threshold VSS method generates share image S_i as

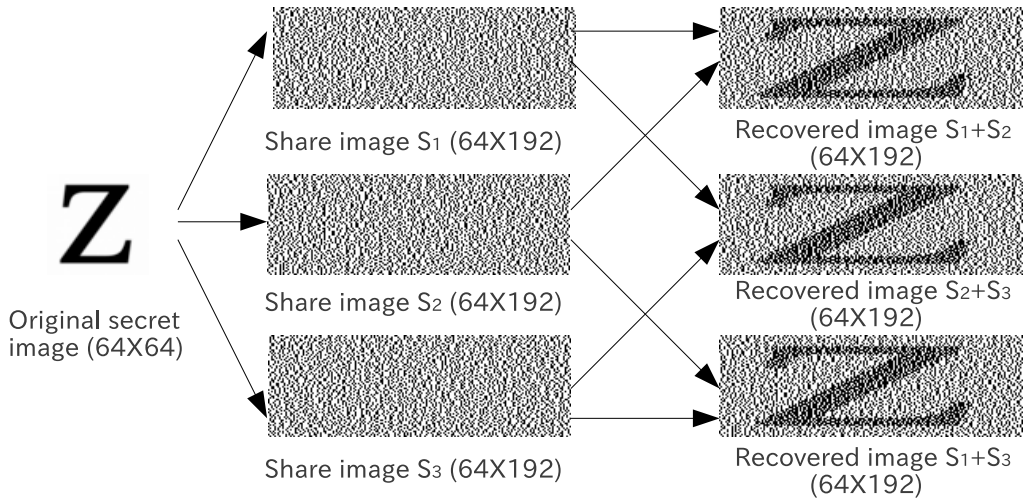


Figure 5.1: An example of the $(2, 3)$-threshold visual secret sharing method for binary images [66]. A pixel in the secret image is expanded to three subpixels in a share image, i.e., $m = 3$.

1. For each white pixel in the secret image, put the i-th row of $\mathbf{S}^0$ to S_i as m-length subpixels.

2. For each black pixel in the secret image, put the i-th row of $\mathbf{S}^1$ to S_i as m-length subpixels.

Figure 5.1 shows an example for this $(2, 3)$-threshold VSS method [66].

In general, a VSS method is expected to meet the following requirements.

1. The increase in pixel expansion should be as small as possible.

2. The contrast of the secret image in the stacking of shares is not significantly reduced.

3. It does not rely on the help of an on-line trusted authority.

5.2.3 Cheat-Prevention Visual Secret Sharing

In normal VSS methods, two or more parties can collude to generate fake shares. For example, as shown in Eq. (5.1), subpixels corresponding to a white pixel are [1 0 0] regardless of party P_i in the $(2, 3)$-threshold VSS scheme with $m = 3$. In

addition, when two parties collude, $\mathbf{S}^1$ can be easily estimated from subpixels in their shares which subpixels correspond to black pixels. Now, colluded two parties know $\mathbf{S}^0$ and $\mathbf{S}^1$, they can generate a fake share to deceive the other party. In this scenario, the fake secret image is revealed by stacking the fake shares and share (shares) from honest party (parties) as shown in Fig. 5.2. In order to overcome this situation, cheat-prevention VSS have been proposed [53, 80].

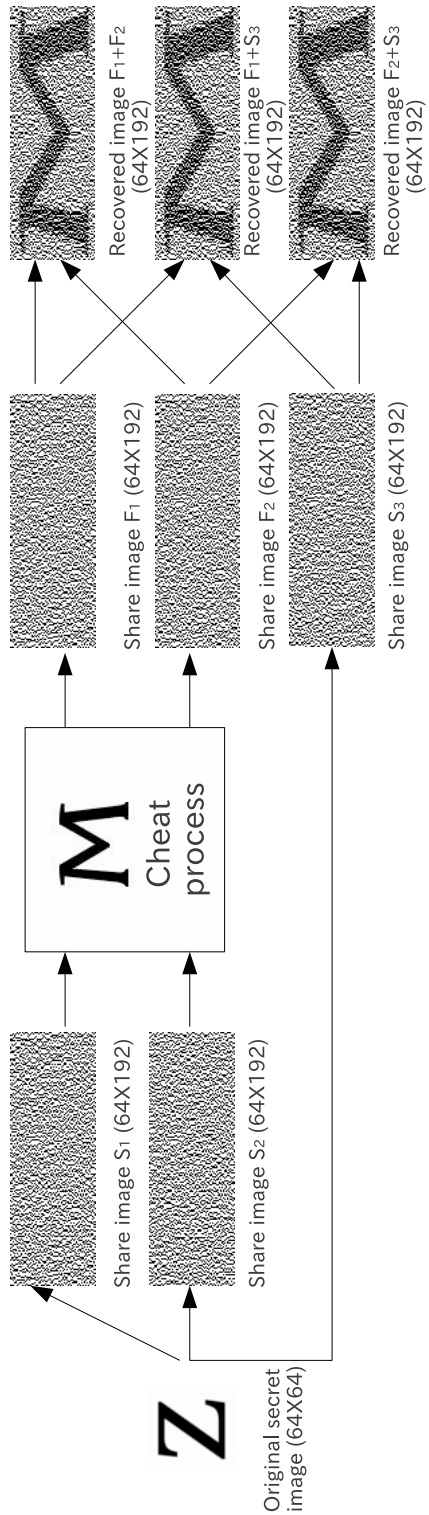


Figure 5.2: Two malicious parties collude to deceive the other honest party in the $(2, 3)$-threshold VSS scheme with $m = 3$.

It is noted that the above cheat is successful when Req. 1 is satisfied. The more the pixel is expanded in the VSS method, the harder the cheat becomes. For example, in the $(2, 3)$-threshold VSS scheme with $m = 4$, $\mathbf{S}^0$ and $\mathbf{S}^1$ are given as

$$\mathbf{S}^0 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad \text{and} \quad \mathbf{S}^1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{5.2}$$

When two parties are collusive to cheat, $\mathbf{S}^0$ can be estimated, but $\mathbf{S}^1$ can't be revealed, i.e., the cheat becomes harder. However, the contrast of revealed secret image becomes quite low by increasing the number of subpixels; being uncompliant with Req. 1 becomes uncompliant with Req. 2. Both conventional and proposed cheat-prevention VSS described in this chapter meet Req. 1.

A successful cheat-prevention VSS prevents any party from deceiving an honest party, and it is summarized [80] that an efficient and robust cheat-prevention scheme should has the following properties in addition to Reqs. 1, 2, and 3:

4. Each party verifies shares presented by other participants.

5. The verification image of each party is different and confidential.

6. A cheat-prevention scheme should be applicable to any VSS method.

5.3 Conventional Cheat-Prevention VSS Schemes

This section reviews two conventional schemes [53,80] for cheat-prevention VSS. In a cheat-prevention VSS, each of all n parties $\mathbf{P}$ holds two images for satisfying Req. 4; one (share image S_i) is for secret recovery and the other (verification image share V_i) is for verification.

Before revealing the secret image, party P_i can check others' share image S_j by stacking V_i and S_j, i.e., $V_i + S_j$ where $j = 1, 2, \ldots, n$ and $j \neq i$. If this stacked image $\left(V_i + S_j\right)$ reveals verification image V^i of P_i, which is set in advance, share

image S_j is judged to be authentic, if not, S_j is forged. It is noted that verification image V^i of P_i should be know to P_i only.

5.3.1 Conventional Scheme 1

Based on given $\mathbf{S}^0$ and $\mathbf{S}^1$ which are the $n \times m$-sized basic matrices for share image generation in a black-and-white VSS method, this scheme [80] firstly creates four $n \times (m + 2)$-sized basic matrices $\mathbf{T}^0$, $\mathbf{T}^1$, $\mathbf{R}^0$, and $\mathbf{R}^1$ as

$$\mathbf{T}^0 = \left[\begin{array}{c|c} 10 & \\ \vdots & \mathbf{S}^0 \\ 10 & \end{array}\right], \mathbf{T}^1 = \left[\begin{array}{c|c} 10 & \\ \vdots & \mathbf{S}^1 \\ 10 & \end{array}\right], \tag{5.3}$$

$$\mathbf{R}^0 = \left[\begin{array}{c|c} 10 & \\ \vdots & 0 \\ 10 & \end{array}\right], \mathbf{R}^1 = \left[\begin{array}{c|c} 01 & \\ \vdots & 0 \\ 01 & \end{array}\right], \tag{5.4}$$

where $\mathbf{T}^0$ and $\mathbf{T}^1$ are used for generating share S_i and $\mathbf{R}^0$ and $\mathbf{R}^1$ are used for generating verification image share V_i, respectively.

This scheme generates share image S_i as follows:

1. For each white pixel in the secret image, put the i-th row of $\mathbf{T}^0$ to S_i as $(m + 2)$-length subpixels.

2. For each black pixel in the secret image, put the i-th row of $\mathbf{T}^1$ to S_i as $(m + 2)$-length subpixels.

According to verification image V^i of party P_i, this scheme generates verification image share V_i as follows:

1. For each white pixel in V^i, put the i-th row of $\mathbf{R}^0$ to V_i as $(m + 2)$-length subpixels.

2. For each black pixel in V^i, put the i-th row of $\mathbf{R}^1$ to V_i as $(m + 2)$-length subpixles.

By adding two columns consisting of one 0 and one 1 to $\mathbf{S}^0$ and $\mathbf{S}^1$, stacking shares by colluded parties cannot disclose $\mathbf{S}^0$ or $\mathbf{S}^1$. In addition, a generation of fake shares with taking account into the verification image share of the honest party (parties) becomes much harder. It is noted that columns in $\mathbf{T}^0$, $\mathbf{T}^1$, $\mathbf{R}^0$, and $\mathbf{R}^1$ are differently permuted at each pixel of the secret image before generating share images to be more secure.

Figure 5.3 shows an example of this cheat-prevention VSS scheme [80] when it is applied to $(2,3)$-threshold VSS [66]. It is shown that party P_i can see his/her own verification image V^i by stacking V_i and S_j where S_j is the image share from party P_j. It is also shown that stacking shares shows the secret image.

5.3.2 Conventional Scheme 2

It was found that cheat-prevention in conventional scheme 1 [80] described in the previous section is breakable when adversaries use complementary verification images [81]. As shown in Eq. (5.4), verification image share V_i has subpixels in which the first column is '1' for white pixels and subpixels in which the second column is '1' for black pixels. All other $(m+1)$ columns are zeros. From this fact, if two complementary verification images are used by two malicious parties, they can fool conventional scheme 1.

A tangible example is given here with three parties P_1, P_2, and P_3 in the conventional scheme 1 on $(2,3)$-threshold VSS with Eq. (5.1). It is assumed that P_1 and P_2 are collusive cheaters and P_3 is the victim. Column permutation of $\mathbf{T}^0$, $\mathbf{T}^1$, $\mathbf{R}^0$, and $\mathbf{R}^1$ are omitted here for simplicity, and the permutation does not prevent P_1 and P_2 from deceiving P_3. The attack is illustrated as follow:

1. P_1 and P_2 choose complimentary verification images V^1 and V^2 as shown in Fig. 5.4 (a) and (b), respectively.

2. Each party receives the share and verification image shares.

3. P_1 and P_2 stack their verification image shares V_1 and V_2 to determine the positions of the added columns in $\mathbf{R}^0$ and $\mathbf{R}^1$ by focusing the position of '1.'

It is easily determined that the first and second columns are added to zero matrices to form $\mathbf{R}^0$ and $\mathbf{R}^1$ as shown in Eq. (5.4).

4. The basic matrices $\mathbf{T}^0$ and $\mathbf{T}^1$ can be uniquely determined because the first and second rows of $\mathbf{T}^0$ and $\mathbf{T}^1$ which for S_1 and S_2 are known and the positions of the added columns in $\mathbf{T}^0$ and $\mathbf{T}^1$ which are the same as those in $\mathbf{R}^0$ and $\mathbf{R}^1$ are known.

5. Subpixels in S_3 are now determined from the third row of $\mathbf{T}^0$ and $\mathbf{T}^1$.

6. According to the third row of $\mathbf{T}^0$ and $\mathbf{T}^1$ and the positions of added columns, fake share images F_1 and F_2 which for P_1 and P_2, respectively, can be forged.

As shown in Figs. 5.4 (g) and (h), P_3 confirms own verification image V^3 (shown in Fig. 5.4 (c)) from $V_3 + F_1$ and $V_3 + F_2$ as from $V_3 + S_3$ shown in Fig. 5.4 (f). However, $S_3 + F_1$ and $S_3 + F_2$ reveal the fake secret image (shown in Fig. 5.4 (e)) instead of the secret image (shown in Fig. 5.4 (d)) as shown in Figs. 5.4 (i) and (j).

From the fact clarified in the literature [81], another requirement is further introduced to cheat-prevention scheme:

7. Added columns cannot be estimated even collusive cheaters use complimentary verification images.

The literature [81] has proposed a scheme to meet Req.7 where the scheme is referred to as conventional scheme 2 in this chapter. In order to foil up u collusive cheaters, $(u + 1)$ of zero columns and one of 1 column, i.e., $(u + 2)$ columns are added to the basic matrices with m-columns. This remedy is considered as increasing the columns of basic matrices, and it is achieved at the cost of higher pixel expansion which is against Reqs. 1 and 2 as shown in Fig. 5.5, and the literature also points out this problem by itself [81].

5.3.3 Conventional Scheme 3

A new visual structure called 'black pattern' is introduced to the conventional scheme [82] to prevent cheating between participants. A black pattern is a rectangle filled with black pixels and some black patterns appear by stacking verification image share V_i and share image S_j as shown in Figs. 5.6 (g), (h), and (i). It is noted that the dealer instead of participants decides the number and positions of black patterns for each participant.

This conventional scheme 3 [82] has two disadvantages: The scheme is only applicable to $(2, n)$-threshold VSS and participants are not allowed to choose their verification images freely. The former does not satisfy Req.6, whereas conventional schemes 1 [80] and 2 [81] meet Req.6. On the latter, this kind of limitation can prevent collusive cheaters from estimating added columns even in conventional scheme 1 [80]; Cheaters cannot choose complimentary verification images freely under such limitation.

The next section proposes a new cheat-prevention VSS scheme which overcomes the problems: Req. 7 is not satisfied (in conventional scheme [80]) and Req. 1 is not satisfied (in conventional scheme 2 [81]). In addition, the proposed scheme is applicable to (k, n)-threshold VSS.

5.4 Proposed Scheme

This section gives details of the proposed scheme in which randomness is introduced to share generation instead of increasing the number of columns of basic matrices for meeting Req. 7; preventing cheaters with complimentary verification images from estimating added columns. Let $\mathbf{S}^0$ and $\mathbf{S}^1$ be the $n \times m$-sized basic matrices for share generation in a black-and-white VSS method in which each party P_i holds share image S_i where $i = 1, 2, \ldots, n$ and a pixel in a secret image is expanded to m subpixels in a share image.

5.4.1 Algorithm

Firstly, the proposed scheme creates four $n \times (m + 2)$-sized basic matrices $\mathbf{T}^0$, $\mathbf{T}^1$, $\mathbf{R}^0$, and $\mathbf{R}^1$ as the same as conventional scheme 1 [80], i.e., as Eqs. (5.3) and (5.4). In addition, party-dependent $(m + 2)$-length row vector $\mathbf{r}_i^0$ is obtained from $\mathbf{t}_i^0$ which is the i-th row of $\mathbf{T}^0$ where $i = \{1, 2, \ldots, n\}$;

$$\mathbf{t}_i^0 = \left[\begin{array}{cc|c} 1 & 0 & \mathbf{s}_i^0 \end{array} \right], \tag{5.5}$$

where $\mathbf{s}_i^0$ is the i-th row of $\mathbf{S}^0$. With the assumption that the number of 1's in $\mathbf{s}_i^0$ is l where $0 < l < m$, the number of 1's in $\mathbf{t}_i^0$ is $(l + 1)$. One 1 is randomly chosen from $(l + 1)$ of 1's, and l of 1's are set to zero to obtain new $(m + 2)$-length row vector $\mathbf{r}_i^0$ which contains exact one 1 at each pixel of the verification image.

Then, $\mathbf{T}^0$ and $\mathbf{T}^1$ are used for generating share images S_i as in the conventional schemes [53,80]. In contrast, according to the pixel value of secret and verification images, verification image share generation can be divided into 4 cases as,

1. The focal pixel in the secret and verification images are black.
2. The focal pixel in the secret and verification images are black and white, respectively.
3. The focal pixel in the secret and verification images are white and black, respectively.
4. The focal pixel in the secret and verification images are white.

Each $(m + 2)$-length subpixels in verification image share V_i are generated as follows:

Cases 1, 2, or 3 Use $\mathbf{R}^0$ and $\mathbf{R}^1$ as in the conventional scheme 1 [80]. That is, put the i-th row of $\mathbf{R}^0$ and $\mathbf{R}^1$ to V_i as $(m + 2)$-length subpixels, for white and black pixels in verification image V^i, respectively.

Case 4 Put party-dependent row vector $\mathbf{r}_i^0$ to V_i as $(m + 2)$-length subpixels.

5.4.2 Example

A tangible example of the proposed scheme is given by using (2, 3)-threshold VSS method with Eq. (5.1). Then, from Eqs. (5.1) and (5.3), $\mathbf{T}^0$ is given as

$$\mathbf{T}^0 = \left[\begin{array}{c|c} 10 & \\ \vdots & \mathbf{S}^0 \\ 10 & \end{array}\right] = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \end{bmatrix}, \tag{5.6}$$

and $\mathbf{t}_i^0 = [1\ 0\ 1\ 0\ 0]$ regardless of i. The proposed scheme randomly replaces 1's in $\mathbf{t}_i^0$ with 0 to generate party-dependent row vector $\mathbf{r}_i^0$:

$$\mathbf{r}_i^0 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{or} \quad \mathbf{r}_i^0 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \end{bmatrix}. \tag{5.7}$$

When malicious parties try to attack the proposed scheme based on the description in Section 5.3.2, i.e., with complementary verification images, expanded subpixels in stacked verification image shares of malicious parties are either [1 1 0 0 0] or [0 1 1 0 0]. So, it is impossible to identify the position of added columns exactly in the proposed scheme.

5.4.3 Discussion

This section discusses the pixel expansion efficiency and decrypt-able randomness of the proposed scheme.

Pixel Expansion Efficiency

Assume that w columns are added to $n \times m$-sized base matrices of VSS method to create two $n \times (m + w)$-sized base matrices in a cheat-prevention VSS scheme where $w \geq 1$.

To meet Req. 1, it is desired that $w = 1$, and the size of pixel expansion is $m + w = m + 1$. Then, the added column must be a zero vector, because stacking verification image share V_i and share image S_j ($V_i + S_j$) should become either black or white where $1 \leq i, j \leq n$ and $i \neq j$. On the other hand, if the added

column consists of one, a white pixel of verification image V^i becomes black when V_i and S_j are stacked.

When $w = 1$, a black pixel of V^i is expanded to $(m + 1)$-length subpixels consisting of one of 1 and m of zeros in verification image share V_i and a white pixel of V^i is expanded to subpixels compounded of $(m + 1)$ of zeros in V_i. That is, V_i leaks V^i without stacking with S_j. It goes against Req. 5. So, the number of added columns are at least two, i.e., $w \geq 2$.

From this perspective, the proposed scheme which adds two columns to $n \times m$-sized basic matrices achieves the most efficient pixel expansion, i.e., the proposed scheme satisfies Req. 1. So, the proposed scheme overcomes the problem in conventional scheme 2 [81].

Decrypt-Able Randomness

As discussed in Section 5.4.3, the most efficient pixel expansion is to add 2 columns to $n \times m$-sized basic matrices. It is assumed again that Eq. (5.1) is used, then, from Eqs. (5.3) and (5.4), $\mathbf{T}^0$, $\mathbf{T}^1$, $\mathbf{R}^0$, and $\mathbf{R}^1$ are as follows:

$$\mathbf{T}^0 = \left[\begin{array}{cc|ccc} 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \end{array}\right], \qquad \mathbf{T}^1 = \left[\begin{array}{cc|ccc} 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{array}\right], \tag{5.8}$$

$$\mathbf{R}^0 = \left[\begin{array}{cc|ccc} 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{array}\right], \qquad \mathbf{R}^1 = \left[\begin{array}{cc|ccc} 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{array}\right]. \tag{5.9}$$

In conventional scheme 1 [80], it is easy to tell that the proportion of white pixels to black pixels is 3/2 in each 5-length subpixels in $V_i + S_j$, if the corresponding pixel in V^i is white. In contrast, the proportion is 2/3, if the corresponding pixel in V^i is black. Note that the proportion doesn't change even a column permutation is applied to matrices.

In case 4 which is defined in Section 5.4.1, 5-length subpixels in V_i are [1 0 | 0 0 0], those in S_j [1 0 | 1 0 0], and thus $V_i + S_j$ becomes [1 0 | 1 0 0] in conven-

tional scheme 1 [80] where $i \neq j$. Meanwhile, $\mathbf{r}_i^0$ could be either [1 0 | 0 0 0] or [0 0 | 1 0 0] in the proposed scheme by introducing randomness, even the promotion of white pixels to black pixels in 5-length subpixels in $V_i + S_j$ is 2/3, i.e., it is decrypt-able even randomness is introduced. For other cases, randomness could change the proportion, and it is the reason that randomness is introduced only to case 4.

As the key point of the attack to conventional scheme 1 [80] is to determine the position of added columns [81], the proposed scheme introduces randomness in generating verification image shares to make the accurate estimation of the added columns impossible, i.e., the proposed scheme meets Req. 7. Thus, the proposed scheme overcomes the problem in conventional scheme 1 [80].

Accidental Correct Estimation of Added Columns

Though it is quite difficult, there is a possibility that random guessing gives the correct estimation of the positions of added columns in the proposed scheme and even in conventional scheme 2 [81]. It is assumed here that verification and secret images randomly consist of equiprobable white and black pixels. The proposed scheme introduces randomness to Case 4, and in Case 4 in $(2, 3)$-threshold VSS, which was discussed in Section 5.4.2, the possibility of correct guessing of added columns becomes 1/2. So, for a $X \times Y$-sized image, the possibility of correctly guessing all positions of added pixels is $\left(\frac{1}{2}\right)^{\frac{XY}{4}}$. Similarly, that in conventional scheme 2 [81] is $\left(\frac{1}{18}\right)^{\frac{XY}{2}}$.

Based on this possibility, the proposed scheme is inferior to conventional scheme 2 [81]. The proposed scheme, however, is superior in the contrast of decrypted images to conventional scheme 2. This situation is the same as that slightly weakening the security could be a choice to improve the visual contrast in VSS [75, 76].

5.4.4 Features

The features of the proposed scheme are summarized here.

Cheat-Prevention Functionality Improvement

The problem of conventional scheme 1 [80] is due to all rows in $\mathbf{R}^0$ are the same and simultaneously all rows in $\mathbf{R}^1$ are the same. That is, all parties receives verification image share V_i's in which subpixels corresponding to black pixels in verification image V^i are the same regardless of party and simultaneously subpixels corresponding to white pixels in V^i are the same regardless of party. This fact allows malicious parties to collude for deceiving an honest party by using complementary verification images [81]. Conventional scheme 2 [81] expands pixels much more, whereas the proposed scheme introduces party-dependent subpixels to V_i's. Both strategies prevent malicious parties from estimating $\mathbf{R}^0$ and $\mathbf{R}^1$, i.e., from deceiving an honest party as well.

Consequently, the proposed scheme is superior in the cheat-prevention functionality to conventional scheme 1 [80].

Improvement in Pixel Expansion and Contrast of Recovered Images

The problem of conventional scheme 2 [81] is due to increasing zero columns to prevent malicious parties from deceiving an honest party, c.f., Figs. 5.3 and 5.5. On the other hand, the proposed scheme simply introduces randomness to the share generation process. The proposed scheme, thus, keeps the subpixel size as small as possible and it results in keeping the contrast of the recovered secret image as that in conventional scheme 1 [80]. Although the security is weakened in the proposed scheme than that in the conventional scheme [81], the pixel expansion efficiency and contrast of decrypted images are improved. Other literatures [75, 76] also show that it is a reasonable choice to improve contrast in VSS.

Consequently, the proposed scheme is superior in pixel expansion efficiency

to conventional scheme 2 [81].

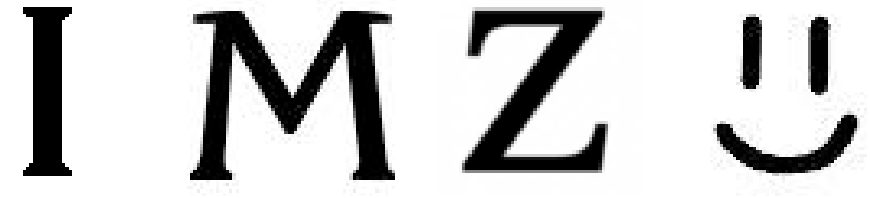
5.5 Experimental Results

The proposed scheme is implemented on $(2, 3)$-threshold VSS method in this experiment. Verification images are those shown in Figs. 5.4 (a), (b), and (c), respectively. The secret and fake secret images are those shown in Figs. 5.4 (d) and (e), respectively.

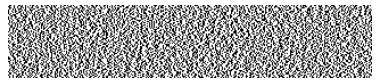
Figures 5.7 (a), (b), and (c) show secret image shares S_1, S_2, and S_3, respectively, and Figs. 5.7 (d), (e), and (f) are verification image shares V_1, V_2, and V_3, respectively. Figs.5.7 (g), (h), and (i) are revealed verification images. Figs.5.7 (j), (k), and (l) are revealed secret images. As added pixels can't be accurately estimated, so it is impossible to generate fake secret share.

5.6 Conclusions

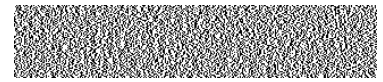
This chapter has improved the visual secret sharing schemes with cheat-prevention. The proposed scheme has better performance than conventional scheme 1 [80] in cheat-prevention functionality and less pixel expansion than conventional scheme 2 [81]. The proposed scheme can be applied to (k, n)-threshold VSS different from a latest scheme [82] which is only suitable for $(2, n)$-threshold VSS. The effectiveness of the proposed scheme has been confirmed through experimental results.



(a) Verification image V^1. (b) Verification image V^2. (c) Verification image V^3. (d) Secret image.

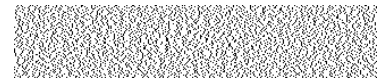


(e) Share image S_1.

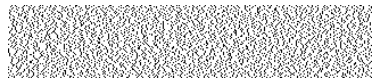


(f) Share image S_2.

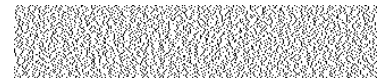
(g) Share image S_3.



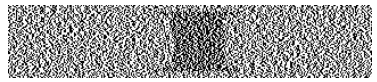
(h) Verification image share V_1.



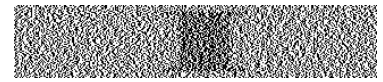
(i) Verification image share V_2.



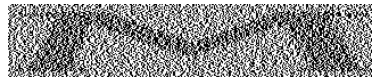
(j) Verification image share V_3.



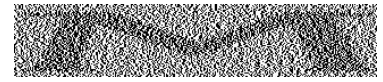
(k) $V_1 + S_2$.



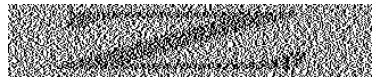
(l) $V_1 + S_3$.



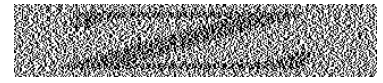
(m) $V_2 + S_3$.



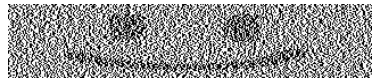
(n) $V_2 + S_1$.



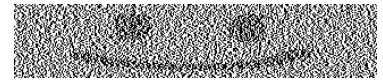
(o) $V_3 + S_1$.



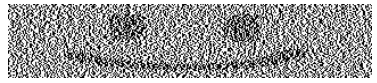
(p) $V_3 + S_2$.



(q) $S_1 + S_2$.



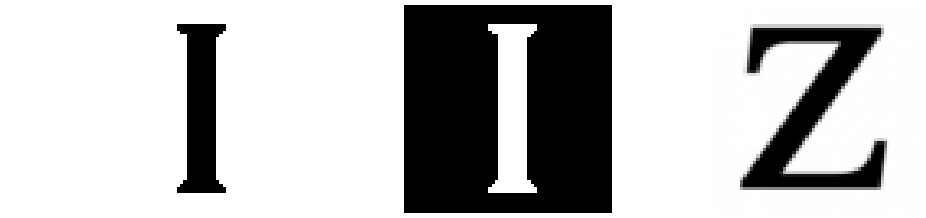
(r) $S_2 + S_3$.



(s) $S_1 + S_3$.

(t) $S_1 + S_2 + S_3$.

Figure 5.3: An example of conventional cheat-prevention VSS scheme 1 [80] on $(2, 3)$-threshold VSS [66]. Image shares and verification image shares are five times larger in width to verification and secret images, i.e., $m + 2 = 5$.



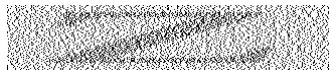
(a) Verification image V^1.

(b) Verification image V^2.

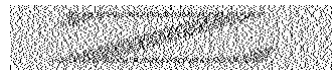
(c) Verification image V^3.

(d) Secret image.

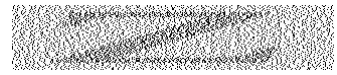
(e) Fake secret image.



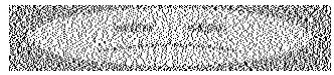
(f) $V_3 + S_3$.



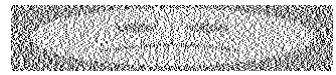
(g) $V_3 + F_1$.



(h) $V_3 + F_2$.

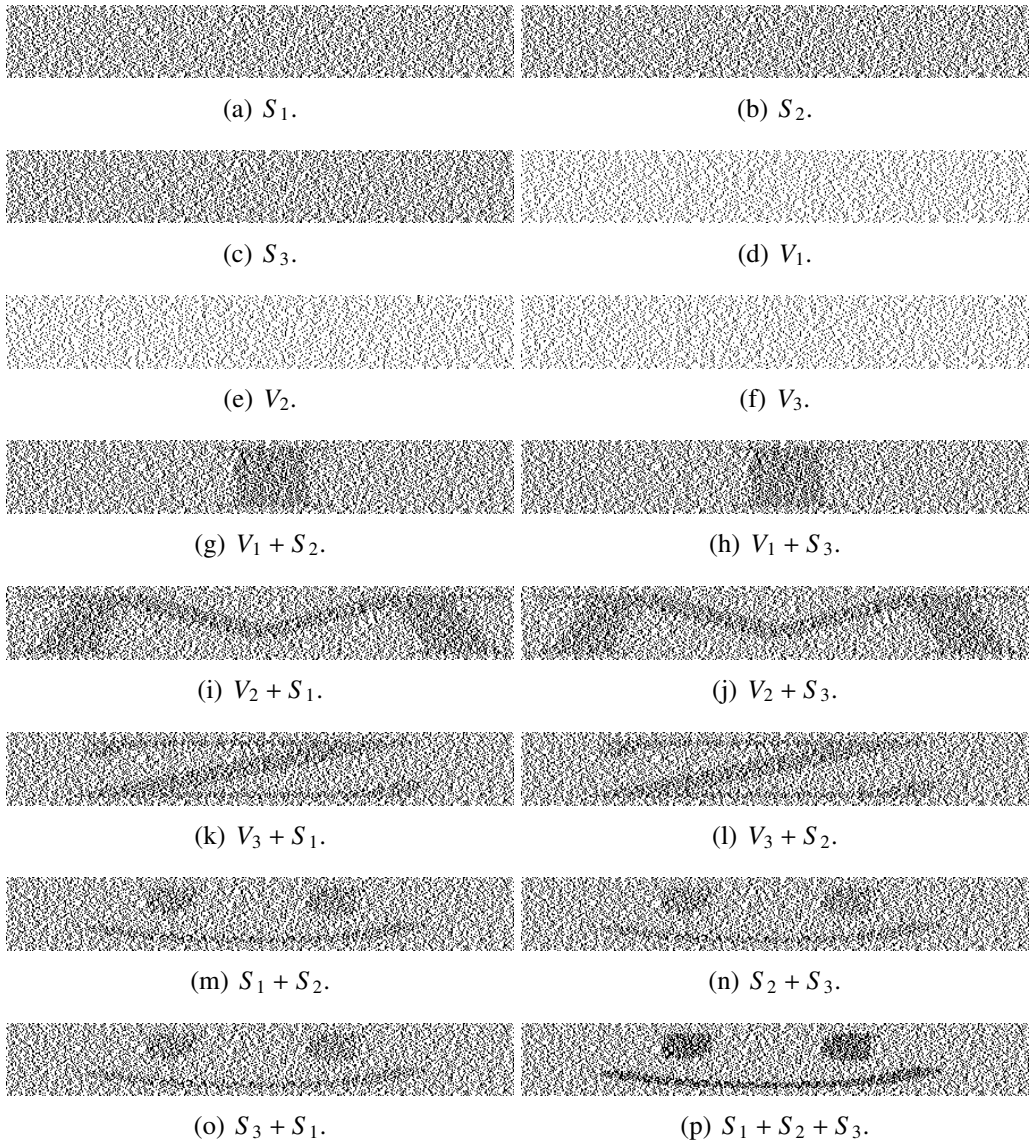


(i) $S_3 + F_1$.



(j) $S_3 + F_2$.

Figure 5.4: Attack [81] to conventional scheme 1 [80].



(a) S_1. (b) S_2.

(c) S_3. (d) V_1.

(e) V_2. (f) V_3.

(g) $V_1 + S_2$. (h) $V_1 + S_3$.

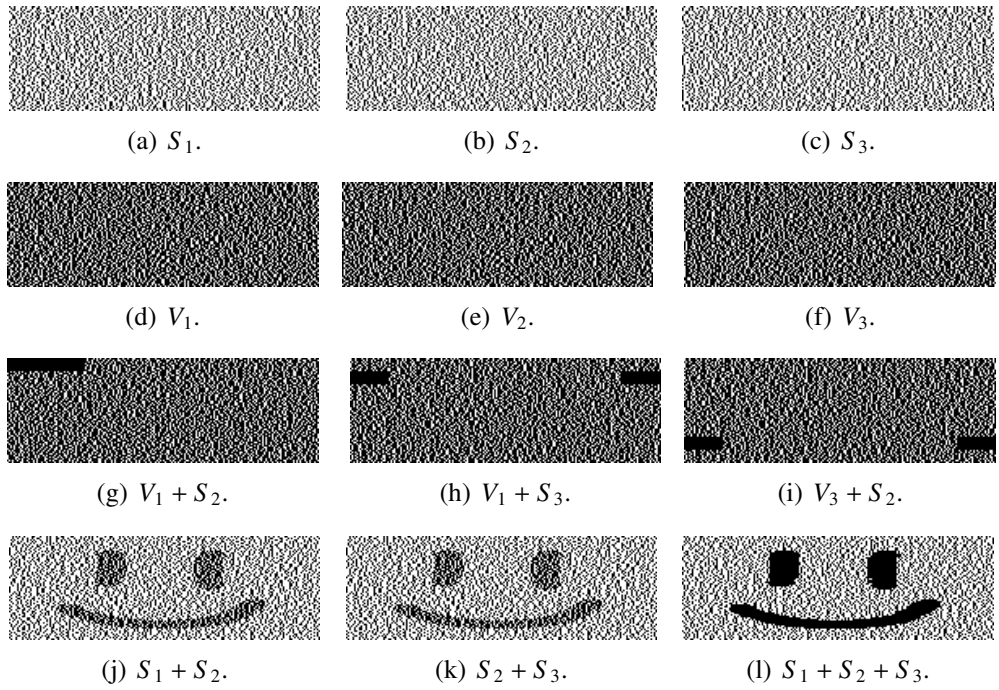
(i) $V_2 + S_1$. (j) $V_2 + S_3$.

(k) $V_3 + S_1$. (l) $V_3 + S_2$.

(m) $S_1 + S_2$. (n) $S_2 + S_3$.

(o) $S_3 + S_1$. (p) $S_1 + S_2 + S_3$.

Figure 5.5: An example of conventional scheme 2 [81] on $(2, 3)$-threshold VSS method [66] with Eq. (5.1). Pixels in the secret image are expanded to seven subpixles under the condition that foiling up two collusive parties, i.e., $m + (u + 1) + 1 = 3 + 3 + 1 = 7$. The contrast of the recovered secret images are low.



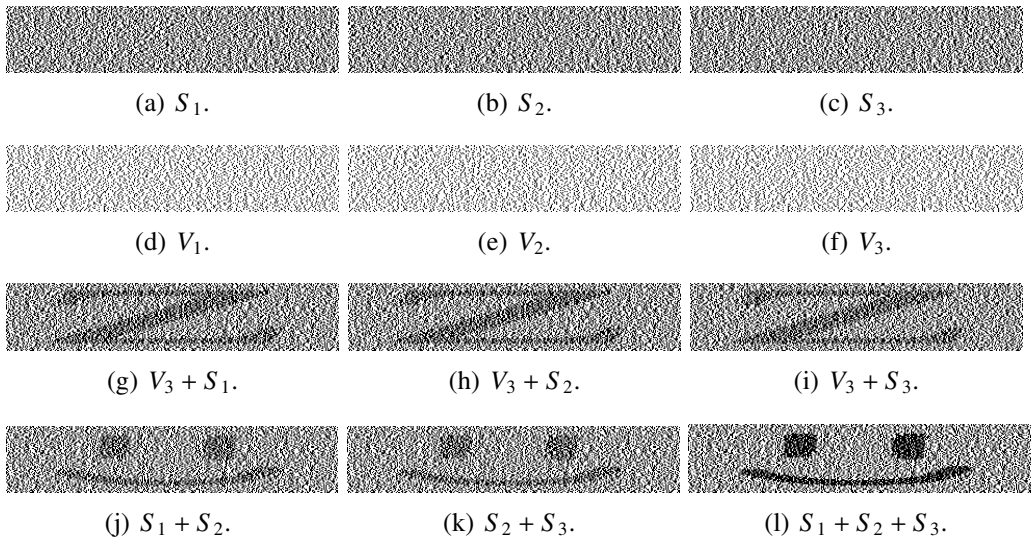
(a) S_1. (b) S_2. (c) S_3.

(d) V_1. (e) V_2. (f) V_3.

(g) $V_1 + S_2$. (h) $V_1 + S_3$. (i) $V_3 + S_2$.

(j) $S_1 + S_2$. (k) $S_2 + S_3$. (l) $S_1 + S_2 + S_3$.

Figure 5.6: An example of conventional scheme [82] on $(2, 3)$-threshold VSS [82].



(a) S_1. (b) S_2. (c) S_3.

(d) V_1. (e) V_2. (f) V_3.

(g) $V_3 + S_1$. (h) $V_3 + S_2$. (i) $V_3 + S_3$.

(j) $S_1 + S_2$. (k) $S_2 + S_3$. (l) $S_1 + S_2 + S_3$.

Figure 5.7: An example of the proposed scheme on $(2, 3)$-threshold VSS method [66].

Chapter 6

Conclusions

In this thesis, visually encrypted images for rights protection and authentication is studied. Visually encrypted images approach image trading system and visual cryptography. In image trading system, visual encryption protects privacy of customer better than the conventional schemes do. In visual cryptography, it provides a way to authenticate shares presented by other share holders. Through consideration of new expression and perspective of visually encrypted images, new schemes are proposed in image trading system and visual cryptography.

6.1 Results and Contribution

Chapter 2 In Chapter 2, visually encrypted images are introduced. First, the generation of amplitude-only image is discussed. There are two types of them by domains, which are discrete Fourier transformation based amplitude-only image and discrete cosine transformation based amplitude-only image. Secondly, amplitude-only image with random signs are discussed. Thirdly, secret sharing, visual cryptography and their relationship are roughly reviewed.

Chapter 3 In Chapter 3, an image trading system using amplitude-only images for privacy- and copyright-protection is proposed. In the proposed system, copyright of image is protected by fingerprinting embedded into the amplitude-only

image; the privacy of customer is also conserved. Because it is quite difficult to estimate the content of original image from amplitude-only image. The proposed scheme can protect privacy better than the conventional schemes. Furthermore, the proposed scheme has better performance in fingerprinting against normal attacks than conventional schemes.

Chapter 4 Chapter 4 is an extension of image trading system in chapter 3. As mentioned above, while transmitting or storing images with enormous data, compression (reversible or non-reversible) is often requested. Distortion is large when compression is introduced into the image trading system in chapter 3. In Chapter 4, an image trading system with efficient compression is proposed. In the proposed system, while generating amplitude-only image, random sign matrix is introduced; by dong so, distortion brought by compression is reduced. In the proposed system, fingerprinting can be extracted with higher accuracy than conventional systems when images are lossy compressed.

Chapter 5 Chapter 5 proposes a cheat-prevention visual secret sharing sheme with efficient pixel expansion. Generally, while generating secret image shares, matrix **M** is used. In conventional scheme, cheat-prevention is achieved by adding 2 columns to the basic matrix **M**. However, special attack will break this scheme, in other word, cheat will be successful. In others, special attack will fail to cheat. However, basic matrix **M** is much more expanded which leads to lower visibility of revealed secret image. In the proposed scheme, basic matrix **M** is analyzed. The problems which lead the conventional schemes fail is carefully studied. By adding randomness to generating matrices, the proposed scheme preserve the ability of cheating immune and enhance the contrast of revealed secret image.

6.2 Open Problem

The employment of visually encrypted images has revealed a new direction in image trading system for copyright protection and privacy conservation. It has also provided a new way to authenticate. The methods described in this thesis provide a starting point to develop new approaches. Several possibilities are: (1) more robust system for fingerprinting technique (2) less pixel expansion with higher contrast of revealed secret image.

Bibliography

[1] G. Short, “Can Felony Penalties for Copyright Infringement Curtail the Copying of Computer Software?”, 10 Santa Clara Computer & High Tech. L.J. 221, 1994.

[2] Copy Protection: A History and Outlook http://www.studio-nibble.com/countlegger/01/HistoryOfCopyProtection.html

[3] Rosen, Jeffrey, “The Web Means the End of Forgetting” New York Times, July 19, 2010

[4] R. Richardson, 2008 CSI Computer Crime and Security Survey at i.cmpnet.com.

[5] Delfs, Hans & Knebl, Helmut,“Symmetric-key encryption”. Introduction to cryptography: principles and applications. Springer, 2007. ISBN 9783540492436.

[6] M. Nabeel,N. Shang, and E. Bertino, “Privacy preserving policy-based content sharing in public clouds,” IEEE Transactions on Knowledge and Data Engineering 25 (11) , art. no. 6298891 , pp. 2602–2614.

[7] A. Alexanyan, H. Aslanyan, and J. Rolim, “Symmetric-key encryption scheme based on the strong generating sets of permutation groups,” 2013 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2013 , art. no. 6529543 , pp. 470-474.

[8] P.T. Liu, "Secure symmetric key fuzzy Identity-Based Encryption," Applied Mechanics and Materials 321-324 , pp. 2665-2668, 2013.

[9] S. Dutta, C. Kumar, and S. Chakraborty, "A symmetric key algorithm for cryptography using music," International Journal of Engineering and Technology 5 (3) , pp. 3109–3115, 2013.

[10] D. Pugila, H. Chitrala, S. Lunawat, and P.M. Durai Raj Vincent, "An efficeient encrpytion algorithm based on public key cryptography," International Journal of Engineering and Technology 5 (3) , pp. 3064-3067, 2013.

[11] X. Zhang, C. Xu, W. Zhang, W Li, "Threshold public key encryption scheme resilient against continual leakage without random oracles," Frontiers of Computer Science , pp. 1-14, 2013.

[12] S.S. Al-Riyami, K.G. Paterson, "Certificateless public key cryptography," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 2894 , pp. 452-473, 2003.

[13] R. Canetti, S. Halevi, and J. Katz, "A forward-secure public-key encryption scheme," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 2656 , pp. 255-271, 2003.

[14] D. Naccache, J. Stern, "New public key cryptosystem based on higher residues," Proceedings of the ACM Conference on Computer and Communications Security , pp. 59-66, 1998.

[15] A. Herzberg, M. Jakobsson, S. Jarecki, H. Krawczyk, M. Yung, "Proactive public key and signature systems," Proceedings of the ACM Conference on Computer and Communications Security , pp. 100-110, 1997.

[16] S. Ye, Y. Lue, J. Zhao, and S.S. Cheung, "Anonymous biometric acess control," EURASIP Journal on Information Security, vol. 2009, Article ID 865259, 2009.

[17] S.C. Draper, A. Khisti, E. Martinian, A. Vetro, J.S. Yedidia, "Using distributed source coding to secure fingerprint biometrics," ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings 2 , art. no. 4217362 , pp. II129-II132.

[18] Y. Luo, S. Ye, S.-C.S. Cheung, "Anonymous subject identification in privacy-aware video surveillance," IEEE International Conference on Multimedia and Expo, ICME 2010 , art. no. 5583561, pp. 83-88, 2010.

[19] Y. Luo, S.-C.S. Cheung, S. Ye, "Anonymous biometric access control based on homomorphic encryption," IEEE International Conference on Multimedia and Expo, ICME 2009 , art. no. 5202677 , pp. 1046-1049, 2009.

[20] F. Han, J. Hu, X. Yu, "A biometric encryption approach incorporating fingerprint indexing in key generation," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 4115 LNBI -III , pp. 342-351.

[21] C. Orlandi, A. Piva, and M. Barni, "Obivious neural network computing via homomorphic encryption," EURASIP Journal on Information Security, vol. 2007, 2007.

[22] R. Agrawal, R. Srikant, "Privacy-preserving data mining," SIGMOD Record (ACM Special Interest Group on Management of Data) 29 (2) , pp. 439-450, 2000.

[23] J. Vaidya, C. Clifton, "Privacy preserving association rule mining in vertically partitioned data," Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mini ng , pp. 639-644, 2002.

[24] M. Kantarcioglu, C. Clifton, "Privacy-preserving distributed mining of association rules on horizontally partitioned data," IEEE Transactions on Knowledge and Data Engineering 16 (9) , pp. 1026-1037, 2004.

[25] Y. Lindell, B. Pinkas, "Privacy preserving data mining," Journal of Cryptology 15 (3) , pp. 177-206, 2003.

[26] W. Du, Z. Zhan, "Using randomized response techniques for privacy-preserving data mining," Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining , pp. 505-510, 2003.

[27] J.M. Shapiro, "Embedded image coding using zerotrees of wavelets coefficients," *IEEE Trans. Signal Process.*, vol.41, pp.3445–3462, Dec. 1993.

[28] A. Said and W.A. Pearlman, "A new, fast, and efficient image codec based on set partitioning in hierarchical trees," *IEEE Trans. Image Process.*, vol.5, pp.1303–1310, Sep. 1996.

[29] H. Cheng and X.B. Li, "Partial encryption of compressed images and videos," *IEEE Trans. Signal Process.*, vol.48, pp.2439–2451, Aug. 2000.

[30] S. Liu, M. Fujiyoshi, and H. Kiya, "A Commutative Scheme of Perceptual Cryptography and Image Compression for JPEG 2000," Proc. International Technical Conference on Circuits/Systems, Computers and Communications, no.E-W1-04, 2012.

[31] L. Tang, "Methods for encrypting and decrypting MPEG video data efficiently," Proceedings of the ACM International Multimedia Conference & Exhibition , pp. 219-229, 1996.

[32] C.-P. Wu, C.-C.J. Kuo, "Design of integrated multimedia compression and encryption systems," IEEE Transactions on Multimedia 7 (5) , pp. 828-839, 2005.

[33] P.P. Dang, P.M. Chau, "Image encryption for secure Internet multimedia applications," IEEE Transactions on Consumer Electronics 46 (3) , pp. 395-403, 2000.

[34] M. Johnson, P. Ishwar, V. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," IEEE Transactions on Signal Processing 52 (10) , pp. 2992-3006, 2004.

[35] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption and watermarking in video compression," IEEE Transactions on Circuits and Systems for Video Technology 17 (6) , pp. 774-778, 2007.

[36] I. Ito and H. Kiya, "Phase Scrambling and Its Application to Image Matching," IEICE Trans., vol.J92-A, no.7, pp.459469, July 2009.

[37] H. Kiya and I. Ito, "Image Matching between Scrambled Images for Secure Data Management," Proc. EURASIP European Signal Processing Conference, no.L4-3.5, Lausanne, Switzerland, 28th August, 2008.

[38] Y.J. Lee, K.R. Park, S.J. Lee, K. Bae, and J. Kim, "A new method for generating an invariant iris private key based on the fuzzy vault system," IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics 38 (5) , pp. 1302-1313, 2008.

[39] D. Moon, Y. Chung, S.B. Pan, K. Moon, and K.I. Chung, "An efficient selective encryption of fingerprint images for embedded processors," ETRI Journal 28 (4) , pp. 444-452, 2006.

[40] S.H. Moi, N.B.A. Rahim, P. Saad, P.L. Sim, Z. Zakaria, and S. Ibrahim, "Iris biometric cryptography for identity document," SoCPaR 2009 - Soft Computing and Pattern Recognition , art. no. 5368674 , pp. 736-741, 2009.

[41] Y. Zhao, L. Zhuo, M. Niansheng, J. Zhang, and X. Li, "An object-based unequal encryption method for H.264 compressed surveillance videos," 2012

IEEE International Conference on Signal Processing, Communications and Computing, ICSPCC 2012 , art. no. 6335618 , pp. 419-424, 2012.

[42] Y.-C. Zeng, C.-Y. Hsu, Y.-F. Luo, H.-Y. Chou, and H.-Y.M. Liao, "Object detection in encryption-based surveillance system," APSIPA ASC 2010 - Asia-Pacific Signal and Information Processing Association Annual Summit and Conference , pp. 86-94, 2010.

[43] K.-Y. Chu, Y.-H. Kuo, and W.H. Hsu, "Real-time privacy-preserving moving object detection in the cloud," Proceedings of the 2013 ACM Multimedia Conference , pp. 597-600, 2013.

[44] M. Fujiyoshi, K. Kuroiwa, and H. Kiya, "A Scrambling Method for Motion JPEG Videos Enabling Moving Objects Detection from Scrambled Videos" Proc. IEEE International Conference on Image Processing, no.MP-L5.6, pp.773776, San Diego, CA, the U.S., 13th October, 2008.

[45] I.J. Cox, M.L. Miller, J.A. Bloom, J. Fridrich, and T. Kalker, Digital watermarking and steganography, 2nd ed., Morgan Kaufmann Publishers, 2008.

[46] M. Kuribayashi, "Recent fingerprinting techniques with cryptographic protocol," Signal Processing, S. Miron, ed., InTech, 2010.

[47] B. Schneier, Applied cryptography: protocols, algorithms, and source code in C, 2nd ed., John Wiley & Sons, 1996.

[48] M. Okada, Y. Okabe, and T. Uehara, "Semi-blind fingerprinting utilizing ordinary existing watermarking techniques," Proc. IWDW, LNCS, vol.5703, pp.14–28, 2009.

[49] M. Okada, Y. Okabe, and T. Uehara, "Security analysis on privacy-secure image trading framework using blind watermarking," Proc. IEEE International Symposium on Applications and the Internet, pp.243–246, 2009.

[50] M. Okada, Y. Okabe, and T. Uehara, "A privacy-secure content trading system for small content providers using semi-blind digital watermarking," Proc. Computer Science and Its Application, 2009.

[51] M. Okada, Y. Okabe, and T. Uehara, "Privacy-secure image sharing system for a purchaser and recorded subject using semi-blind fingerprinting," Procedia Social and Behavioral Sciences 2, pp.137–142, 2010.

[52] M. Okada, Y. Okabe, and T. Uehara, "A web-based privacy-secure content trading system for small content providers using semi-blind digital watermarking," Proc. IEEE CCNC, 2010.

[53] Y. Sengoku and H. Hioki, "An image segmentation method for privacy and copyright-aware image trading system," IEICE Tech. Rep., vol.111, no.496, EMM2011-67, pp.19–24, Mar. 2012.

[54] R. Achanta and S. Susstrunk, "Saliency detection using maximum symmetric surround," Proc. IEEE ICIP, pp.2653–2656, 2010.

[55] S.C. Liu, M. Fujiyoshi, and H. Kiya, "A Use of amplitude-Only Images for Privacy- and Copyright Image Trading System," IEICE Tech. Rep., vol.112, no.188, EMM2012-46, pp.63–68, Aug. 2012.

[56] I. Ito and H. Kiya, "Phase-only correlation based matching in scrambled domain for preventing illegal matching," LNCS Trans. Data Hiding and Multimedia Security V, vol.6010/2010, pp.51–69, Jun. 2010.

[57] I. Ito and H. Kiya, "One-Time Key Based Phase Scrambling for Phase-Only Correlation between Visually Protected Images," EURASIP J. Information Security, vol.2009, no.841045, Jan. 2010.

[58] I.J. Cox, J. Kilian, F.T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Process., vol.6, no.12, pp.1673–1687, Dec. 1997.

[59] P. Meerwald, "Digital image watermarking in the wavelet transform domain," Master's Thesis, Department of Scientific Computing, University of Salzburg, Austria, Jan. 2001.

[60] T. Tachibana, M. Fujiyoshi, and H. Kiya, "A Watermarking scheme retaining the desired image quality in order to be applicable to watermarks with various distributions," IEICE Trans. Inf. & Sys. (Japanese edition), vol.J87-D-II, no.3, pp.850–859, Mar. 2004.

[61] T. Tachibana, M. Fujiyoshi, and H. Kiya: "A digital watermarking scheme that preserves image quality and is applicable to watermark sequences from a variety of distribution s", Systems and Computers in Japan, **37**, pp.90–100 (Jul. 2006)

[62] F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn, "Attacks on copyright marking systems", Proc. Information Hiding, LNCS, vol.1525, pp.219–239, 1998.

[63] F.A.P. Petitcolas, "Watermarking schemes evaluation," IEEE Signal Process. Magazine, vol.17, no.5, pp.58–64, Sep. 2000.

[64] Kakadu software version 6.4.

[65] A. Shamir, "How to share a secret," Commun. ACM, vol.22, pp.612–613, Nov. 1979.

[66] M. Naor and A. Shamir, "Visual cryptography," Proc. IACR EUROCRYPT, LNCS, vol.950, pp.1–12, 1994.

[67] I. Biehl and S. Wetzel, "Traceable visual cryptography," Proc. Int. Conf. Information Communication Security, LNCS, vol.1334, pp.61–71, 1997.

[68] T. Hofmeister, M. Krause, and H.-U. Simon, "Contrast-optimal k out of n secret sharing schemes in visual cryptography," Theoret. Comput. Sci., vol.240, no.2, pp. 471–485, 2000.

[69] S. Cimato, R.D. Prisco, and A.D. Santis, "Optimal colored visual cryptography schemes," Designs, Codes and Cryptography, vol.35, pp.311–335, 2005.

[70] T. Ishihara and H. Koga, "A visual secret sharing scheme for color images based on meanvalue-color mixing," IEICE Trans. Fundamentals, E86-A, no.1, pp.194–197, 2003.

[71] H. Koga and T. Ishihara, "A general method for construction of (t, n)- threshold visual secret sharing schemes for color images," Designs, Codes and Cryptography, vol.61, no.2, pp.223–249, 2011.

[72] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson, "Extended capabilities for visual cryptography," Theor. Comput. Sci., vol.250, pp.143–161, Jan. 2001.

[73] C.-C. Chang and T.-X. Yu, "Sharing a secret gray image in multiple secret," Proc. International Symposium on Cyber Worlds, pp.1–8, 2002.

[74] M. Iwamoto, L. Wang, K. Yoneyama, N. Kunihiro, and K. Ohta, "Visual secret sharing schemes for multiple secret images allowing the rotation of shares," IEICE Trans. Fundamentals, vol.E89, no.5, pp.1382–1395, 2006.

[75] M. Iwamoto, "A weak security notion for visual secret sharing schemes," IEEE Trans. Information Forensics and Security, vol.7, no.2, pp.372–382, 2012.

[76] M. Iwamoto, "Security notions of visual secret sharing schemes," Proc. IWAIT, pp.95–100, 2013.

[77] S. Cimato, A. De Santis, A.L. Ferrara, and B. Masucci, "Ideal contrast visual cryptography schemes with reversing," Inf. Process. Lett., vol.93, no.4, pp.199–206, 2005.

[78] P.A. Eisen and D.R. Stinson, "Threshold visual cryptography with specified whiteness levels of reconstructed pixels," Designs, Codes, and Cryptography, vol.25, no.1, pp.15–61, 2002.

[79] D.S. Tsai, T.H. Chen, and G. Horng, "A cheating prevention scheme for binary visual cryptography with homogeneous secret images," Pattern Recog., vol.40, no.8, pp. 2356–2366, Aug. 2007.

[80] C.M. Hu and W.G. Tzeng, "Cheating prevention in visual cryptography," IEEE Trans. Image Process., vol.16, no.1, pp. 36–45, Jan. 2007.

[81] Y.C. Chen, G. Horng, and D.S Tsai, "Comment on 'Cheating Prevention in Visual Cryptography' " IEEE Trans. Image Process., vol.21, no.7, pp.3319–3323, July 2012.

[82] Y.C. Chen, D.S Tsai, and G. Horng "A new authentication based cheating prevention scheme in Naor-Shamir's visual cryptography" J. Vis. Commu. Image R., vol.23, pp.1225-1233, Nov. 2012.