

資訊科學與工程研究所

碩 士 論 文

以修改型灰階視覺密碼為基礎的
非對稱性浮水印技術

Asymmetric Watermarking Scheme Based on
Modified Gray Visual Cryptography



研 究 生：蔡盛同

指 導 教 授：薛元澤 教授

中 華 民 國 九 十 五 年 六 月


以修改型灰階視覺密碼為基礎的 非對稱性浮水印技術

學生：蔡盛同

指導教授：薛元澤

國立交通大學資訊科學學系（研究所）碩士班

摘要



近年來，隨著電腦科技發展迅速和生活數位化，資訊的傳遞量與日俱增，資訊安全已成為一個重要的議題，目前雖然有很多方法能用來保護智慧財產權和機密資料，但傳統的加密和解密過程需耗費大量時間和複雜的計算，而M. Naor及A. Shamir在1994年提出了一個新的密碼學領域，即所謂的視覺密碼學[7]。它有別於傳統的加密和解密技術，不須要任何密碼學的知識，也沒有複雜的計算過程，只須將機密訊息分解成多張雜亂無章的分享影像（投影片）。在解密時，直接將這些分享影像進行重疊，並利用人類視覺系統便可從中取得原來的機密訊息。這個技術徹底的改進了傳統密碼學在解密過程中須大量複雜計算的缺點。

本論文主要是提出一個非對稱的修改型灰階視覺密碼模型結合公開金

鑰和秘密金鑰的概念所創新的方案，簡稱為PPKA Watermarking Scheme，其中非對稱的修改型灰階視覺密碼模型是結合Y.C. Hou, and P.M. Chen提出的非對稱浮水印 [5] 和Bo-Cheng Shen提出的灰階視覺密碼模型 [28] 的概念，加以改進而成的。此方案由於必須要先後加入公開浮水印及秘密浮水印，又要保持原本影像的品質及認證機制的完備，經過一系列實驗測試，修正後，便提出了修正型的PPKA (MPPKA)Watermarking Scheme來達到一些需求。然而，此方案還有一些需要改進之處，值得我們繼續探討。

在本論文的最後，我們將會提出一個最佳化的PPKA (OPPKA) Watermarking Scheme，兼具了維持原本影像的品質不變，認證機制的健全及對於攻擊抵抗能力的強健性等優點。在此，我們希望本研究對於智慧財產權的保護能提供一個更簡潔便利的方法。

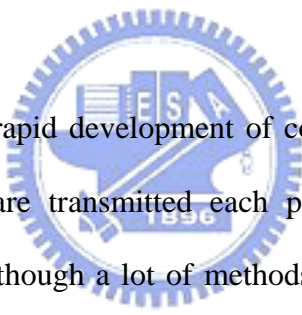
Asymmetric Watermarking Scheme Based on Modified Gray Visual Cryptography

student : Sheng-Tong Cai

Advisors : Dr.Yuang-Cheh Hsueh

Institute of Computer and Information Science
National Chiao Tung University

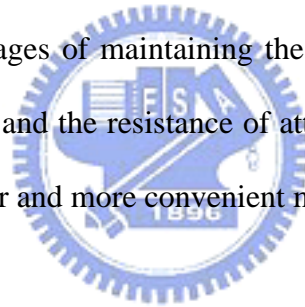
ABSTRACT



In recent years, with the rapid development of computer technology and digitized life, more and more information are transmitted each passing day. Information security has become an important topic. Although a lot of methods can be used for copyright protection and secret information at present, traditional encryption and decryption need to consume a lot of time and complicated calculations, however, M. Naor and A. Shamir addressed a new cryptography domain, called Visual Cryptography [7]. Without any knowledge of cryptography, and without performing complicated calculations, the Visual Cryptography is different from traditional encrypted and decrypted technology. It only needs to split the secret messages into several shares (slides) which looked like random noises. When decrypting, it directly superimposes these shares to obtain original secret messages by human visual system. This technique thorough improves the drawbacks that traditional cryptography needs a lot of complex calculations in the process of decryption.

This thesis mainly addresses a new scheme which combines an asymmetric modified gray visual cryptography model with the concept of Public Key and Private Key, abbreviated to PPKA Watermarking Scheme. An asymmetric modified gray visual cryptography model is created by improving the concept which combines an asymmetric watermark [5] addressed by Y.C. Hou, and P.M. Chen with gray visual cryptography model [28] by Bo-Cheng Shen. Because this scheme must embed Public Watermark and Private Watermark in turn, it also maintains the quality of original image and completes the authentication mechanism. Hence, we address a Modified PPKA (MPPKA) Watermarking Scheme to reach some requirements after a series of experimental tests and modifications. However, this scheme still has some places that need to improve, it is worthy of our continued discussion.

At the end of this thesis, we will address an Optimal PPKA (OPPKA) Watermarking Scheme which has the advantages of maintaining the quality of original image, completing the authentication mechanism, and the resistance of attacks is robust, etc. Here, we hope that this research can offer a simpler and more convenient method for copyright protection.



誌謝

我在這裡要感謝我的指導教授 薛元澤教授，兩年來對我孜孜不倦的教誨，教導我研究學問的方法及待人處世道理，讓我畢生受益無窮，以及我的口試委員 張隆紋教授與 陳玲慧教授，二位老師不吝指教，讓這篇論文更加完善。

我還要感謝吳昭賢學長，給予我論文研究及寫作方面等的各種建議，感謝何昌憲同學、王蕙綾同學、高薇婷同學在這兩年內與我共同努力，互相砥礪。另外，我要感謝呂盈賢學弟、江仲庭學弟、林明志學弟、劉裕泉學弟、顏佩君學妹及王慧縈學妹陪我度過這段快樂的實驗室生活。

僅將此論文獻給我親愛的家人與朋友，我的父母及妹妹，感謝他們在這段期間給我的關心、支持與鼓勵，祝福他們永遠健康快樂

CONTEXTS

ABSTRACT (CHINESE)	i
ABSTRACT (ENGLISH)	iii
ACKNOWLEDGEMENT	v
CONTEXTS	vi
LIST OF FIGURES	viii
LIST OF TABLES	xii
CHAPTER 1 : Introduction	1
1.1 Motivation	1
1.2 Backgrounds	1
1.3 Thesis Organization	3
CHAPTER 2 : Previous Research	4
2.1 Brief Introduction to Digital Images	4
2.1.1 Data Formations of Digital Images	4
2.1.2 Definition of Digital Image Quality	5
2.2 Digital Watermarking	5
2.2.1 Spatial Domain Watermarking Technique	12
2.2.2 Frequency Domain Watermarking Technique	15
2.3 Basic Notions	19
2.3.1 Public Key and Private Key Watermarking System	19
2.3.2 Symmetric and Asymmetric Watermarking Scheme	20
2.4 Visual Cryptography	23
CHAPTER 3 : The Proposed Method	26

3.1 Overview of Gray Visual Cryptography Scheme	26
3.2 Public Key and Private Key Asymmetric (PPKA) Watermarking Scheme.....	30
3.2.1 Modified1 Gray Visual Cryptography (MGVC1) Model.....	33
3.2.2 Modified2 Gray Visual Cryptography (MGVC2) Model.....	41
3.3 Modified Public Key & Private Key Asymmetric (MPPKA) Watermarking Scheme .	53
3.4 Optimum Public Key & Private Key Asymmetric (OPPKA) Watermarking Scheme .	60
3.5 Schemes Comparison and Discussion	68
CHAPTER 4 : Experimental Results and Discussion	69
4.1 Attack Experiments	69
4.2 Results Discussion.....	79
CHAPTER 5 : Conclusions and Furture Works	80
5.1 Conclusions	80
5.2 Future works	80
References	81



LIST OF FIGURES

Fig.2-1	Image frequency distribution	16
Fig.2-2	Three-dimensions Haar function DWT	18
Fig.2-3	General blind symmetric watermarking scheme.....	22
Fig.2-4	General asymmetric watermarking scheme.....	23
Fig.3-1	(a) Cover image, (b) Public watermark, and (c) Private watermark.....	33
Fig.3-2	Split a Public watermark into Public Share1 (a) and Public Share2 (b) according to the Modified Visual Cryptography model.....	34
Fig.3-3	Aim at Public Share2 compares (a) Y.C. Hou and P.M. model with (b) MGVC1 Model.....	35
Fig.3-4	Compare the visibility of the extracted watermark in (a) Y.C. Hou and P.M. model with (b) MGVC1 Model.....	36
Fig.3-5	Splitting the Public watermark into (a) Public Share1 and (b) Public Share2 in MGVC1 Model.....	37
Fig.3-6	Public-Cover image in MGVC1 Model and PSNR= 33.08.....	37
Fig.3-7	Public-random image in MGVC1 Model	38
Fig.3-8	(a) Private Share1 and (b) Private Share2 in MGVC1 Model	38
Fig.3-9	Public-Private random image in MGVC1 Model	39
Fig.3-10	Compare (a) Original image with (b) Public-Private Stego-image in MGVC1 Model, and PSNR= 28.315.....	39
Fig.3-11	The extracted Public Watermark in MGVC1 Model	40
Fig.3-12	Public-Private random Stego-image in MGVC1 Model.....	40
Fig.3-13	The extracted Private Watermark in MGVC1 Model	41
Fig.3-14	Split a Public Watermark into (a) Public Share1 and (b) Public Share2 according to an original image in the third Gray Visual Cryptography model.	43
Fig.3-15	Public-Cover image in the third Gray Visual Cryptography model and	

	PSNR=30.07	44
Fig.3-16	Public-random image in the third Gray Visual Cryptography mode.....	44
Fig.3-17	Split a Private Watermark into (a) Private Share1 and (b) Private Share2 refer to the original image in the third Gray Visual Cryptography model.....	45
Fig.3-18	Public-Private random image in the third Gray Visual Cryptography model	45
Fig.3-19	Compare (a) Original image with (b) Public-Private Stego-image in the third Gray Visual Cryptography model, and PSNR= 26.36	46
Fig.3-20	Split a Public Watermark (Fig.3-1(b)) into (a) Public Share1 and (b) Public Share2 according to an original image (Fig.3-1(a)) in MGVC2 Model.....	48
Fig.3-21	Public-Cover image in MGVC2 Model and PSNR= 35.808.....	48
Fig.3-22	Public-random image in MGVC2 Model	49
Fig.3-23	(a) Private Share1 and (b) Private Share2 in MGVC2 Model	49
Fig.3-24	Public-Private random image in MGVC2 Model	50
Fig.3-25	Compare (a) Original image with (b) Public-Private Stego-image in MGVC2 Model, and PSNR= 32.325.....	50
Fig.3-26	Compare the visibility of the extracted Public Watermark (a) MGVC1 Model with (b) MGVC2 Model.....	51
Fig.3-27	Public-Private random Stego-image in MGVC2 Model.....	52
Fig.3-28	Compare the visibility of the extracted Private Watermark (a) MGVC1 Model with (b) MGVC2 Model.....	52
Fig.3-29	Random-cover image in MPPKA Watermarking Scheme	54
Fig.3-30	Split a Public Watermark into (a) Public Share1 and (b) Public Share2 according to Random-original image (Fig.3-29) in MPPKA Watermarking Scheme	55
Fig.3-31	Public-random image in MPPKA Watermarking Scheme	55
Fig.3-32	Public-Cover image in MPPKA Watermarking Scheme and PSNR= 35.808.....	56

Fig.3-33	Private-random image in MPPKA Watermarking Scheme	56
Fig.3-34	Split a Private Watermark into (a) Private Share1 and (b) Private Share2 according to Private-random image in MPPKA Watermarking Scheme.	57
Fig.3-35	Public-Private random image in MPPKA Watermarking Scheme	57
Fig.3-36	Public-Private Stego-image in MPPKA Watermarking Scheme and PSNR=29.86.....	58
Fig.3-37	Random Public-Private Stego-image in MPPKA Watermarking Scheme	58
Fig.3-38	Extracted Public Watermark in MPPKA Watermark Scheme	59
Fig.3-39	Public-Private random Stego-image in MPPKA Watermarking Scheme.....	59
Fig.3-40	Extracted Private Watermark in MPPKA Watermarking Scheme.....	60
Fig.3-41	Random-cover image in OPPKA Watermarking Scheme.....	62
Fig.3-42	Split the Public Watermark into (a) Public Share1 (random-cover image) and (b) Public Share2 in OPPKA Watermarking Scheme.	63
Fig.3-43	Public-random image in OPPKA Watermarking Scheme.....	63
Fig.3-44	Public-Cover image (cover image) in OPPKA Watermarking Scheme.....	63
Fig.3-45	Private- random image in OPPKA Watermarking Scheme	64
Fig.3-46	Split the Public Watermark into (a) Private Share1 (Private-random image) and (b) Private Share2 in OPPKA Watermarking Scheme.....	64
Fig.3-47	Public-Private random image (Private-random image) in OPPKA Watermarking Scheme.....	65
Fig.3-48	Public-Private Stego-image (cover image) in OPPKA Watermarking Scheme..	65
Fig.3-49	Random Public-Private Stego-image in OPPKA Watermarking Scheme.....	66
Fig.3-50	Extracted Public Watermark in OPPKA Watermark Scheme	66
Fig.3-51	Public-Private random Stego-image in OPPKA Watermarking Scheme	67
Fig.3-52	Extracted Private Watermark in OPPKA Watermarking Scheme	67
Fig.4-1	(a) input image, (b) Public watermark, and (c) Private watermark.....	69

Fig.4-2	JPEG compression Attack : Compression rate set to 80%	70
Fig.4-3	Distortion Attack	71
Fig.4-4	Mosaic Attack : X axis set to 3, Y axis set to 3	72
Fig.4-5	Blur Attack : Degree set to strong.....	73
Fig.4-6	Jitter Attack: Move upward set to eight pixels	74
Fig.4-7	Cut1 Attack: Cut right-down parts of Stego-image	75
Fig.4-8	Cut2 Attack: Cut the important parts of Stego-image	76
Fig.4-9	Clarity Attack: degree sets to 8.....	77
Fig.4-10	Noise Attack: Variances set to 10	78



LIST OF TABLES

Table.2-1	A (2, 2)-visual threshold scheme.....	25
Table.3-1	Basic Visual Cryptography model.....	28
Table.3-2	Modified Visual Cryptography model addressed by Y.C. Hou and P.M. Chen.....	29
Table.3-3	The third Gray Visual Cryptography models by Bo-Cheng Shen.....	42
Table.3-4	Modified2 Gray Visual Cryptography (MGVC2) Model	47
Table.3-5	Comparisons in PPKA, MPPKA, and OPPKA Watermarking scheme.....	68



CHAPTER 1

Introduction

1.1 Motivation

Due to Internet rapid development, more and more digital information are easy to distribute, duplicate and modify. This has led to the need for effective copyright protection techniques. Various watermarking schemes have been addressed in recent years. Digital watermarking can be seen as one research direction of information hiding or steganography [8][9][10][11], so it is important to find an optimum watermarking scheme such that the process of embedding and extracting of watermarks is simpler, and the hidden information is difficult to embezzle and destroy .

Visual Cryptography is addressed from M. Naor and A. Shamir in 1994 [7], the purpose is to decrypt the ciphertext by human visual system. Because of its simplicity, the model can be used by anyone without any knowledge of cryptography and without performing any cryptographic computations. Because visual cryptography has these advantages, we will adopt this model as the parts of our research methods later.

In this thesis, in order to find an optimum watermarking scheme which is more robust, safer, and easier to access by a dedicated extracting method, we will modify original visual cryptography models to address a series of gray visual cryptography models which combine the asymmetric watermarking method with the concepts of Public Key and Private Key.

1.2 Backgrounds

Watermarking is closely related to the fields of information hiding and steganography. These three fields have a great deal of overlap and share many technical approaches. However, there are fundamental philosophical differences that affect the requirements and thus the

design of a technical solution. In this section, we discuss these differences.

Information hiding (or data hiding) is a general term encompassing a wide range of problems beyond that of embedding messages in content. The term hiding here can refer to either marking the information imperceptible (as in watermarking) or keeping the existence of the information secret. Some researches in this field can be found in the International Workshops on Information Hiding, which have included papers on such topics as maintaining anonymity while using a network [13] and keeping part of a database secret from unauthorized users [14]. These topics definitely fall outside our definition of watermarking.

Steganography is a term derived from the Greek words "steganos graohia", which means "covered writing". It is the art of concealed communication. The very existence of a message is secret.

We refer to a specific song, video, or picture or to a specific copy of such as a *Work* [12]. The original unwatermarked Work is sometimes referred to as the *cover Work*, in that it hides or "covers" the watermark. We define *watermarking* as the practice of imperceptibly altering a Work to embed a message about that Work. Systems for inserting messages in Works can thus be divided into watermarking systems, in which the message is related to the cover Work, and non-watermarking systems, in which the message is unrelated to the cover Work. They can also be independently divided into steganographic systems, in which the very existence of the message is kept secret, and non-steganographic systems, in which the existence of the message need not be secret.

By distinguishing between embedded data that relates to the cover Work and hidden data that does not, we can anticipate the different applications and requirements of the data-hiding method. However, the actual techniques used for watermarking may be very similar, or in some cases identical, to those used in non-watermarking systems. Thus, although this thesis focuses on watermarking techniques, most of these techniques are applicable to other areas of information hiding.

1.3 Thesis Organization

The remainder of this thesis is organized as follows. In chapter 2, we will briefly introduce the digital images and digital watermarking, then describe the related techniques and concepts, and finally introduce visual cryptography.

In chapter 3, we will survey the research of gray visual cryptography schemes, and then address a new concept of Public Key and Private Key Asymmetric (PPKA) Watermarking Scheme by utilizing Modified1 Gray Visual Cryptography (MGVC1) Model and Modified2 Gray Visual Cryptography (MGVC2) Model. In order to optimize this scheme, then we address Modified Public Key and Private Key Asymmetric (MPPKA) Watermarking Scheme and Optimum Modified Public Key and Private Key Asymmetric (OPPKA) Watermarking Scheme. Finally we will compare these PPKA, MPPKA, and OPPKA Watermarking schemes.

In chapter 4, we adopt a series of attacked experiments on OPPKA Watermarking Scheme to prove its robustness and then discuss experimental results.

In chapter 5, the conclusions and future works will be stated.



CHAPTER 2

Previous Research

In this chapter, we will simply introduce digital images in section 2.1. In section 2.2, digital watermarking techniques between spatial domain and frequency domain will be introduced. In section 2.3, the concept of basic notions about public key and secret key watermarking techniques and asymmetric watermarking scheme will be introduced. Finally, we will describe basic visual cryptography in section 2.4.

2.1 Brief Introduction to Digital Images

In this section, we will describe two data formations of digital images in 2.1.1. In section 2.1.2, the definition of digital image quality will be introduced.

2.1.1 Data Formations of Digital Images

Generally, a picture or photograph appeared on a computer is referred to as a digit image. We can divide digital image data formations into spatial domain and frequency domain in according to their stored method.

Spatial domain data formation is used most frequently. Basically, every digital image is made up by a lot of pixels in this data formation. For example, size 256×256 of a picture is made up of 65536 pixels, and every pixel has a number value which expresses the color of this point, the range of number value is from 0 to 255 (this thesis is mainly based on gray-level picture), shown color from black to white.

Data of a digital image is usually stored by a two-dimensional array, every pixel corresponds to one element of a two- dimensional array, and this stored method is referred to as the spatial domain data formation of the digital image.

Besides spatial domain data formation, frequency domain data formation also can be

used to express the digital image. The image of spatial domain can be seen by our naked eye. However, a frequency domain image is the result of an image converted from spatial domain to frequency domain. Through such conversion, the portion of different frequency of the image will be leach, and generated a lot of high and low frequency. Common conversion methods are Discrete Cosine Transformation (DCT) and Discrete Wavelet Transformation (DWT). In this thesis, we adopt the spatial domain data formation as our research method.

2.1.2 Definition of Digital Image Quality

When an image is compressed or embedded the digital watermark, we will find that the resulted image is different from the original one. Because the difference between them is not easily described, researchers usually use PSNR (Peak Signal to Noise Ratios) as a measure of image distortion tool. Define it as follows [28].

$$PSNR = 10 \log \frac{\sum_{i=0}^{N-1} \sum_{j=0}^{M-1} 255^2}{\sum_{i=0}^{N-1} \sum_{j=0}^{M-1} (x_{ij} - \hat{x}_{ij})^2}$$

In the formula above, x_{ij} and \hat{x}_{ij} express respectively the coordinate (i, j) of the pixels in the original picture and modified picture. M and N respectively express the width and height of the picture. Hence, the greater $PSNR$ value is, the smaller the difference between them. In generally, if $PSNR$ is approximately 30 then the quality of modified image which can be accepted. Besides $PSNR$, we must use match up the visual observation, due to some important positions of a picture may be destroyed seriously, but $PSNR$ is still greater than 30.

2.2 Digital Watermarking

Digital watermarking can be seen as one research direction of information hiding or steganography. The information (digital watermarking) is to be embedded is called

embedded-information, and the information to carry the embedded information is called *cover*-information. Both the information combined together that are called *stego*-information.

The main purpose of digital watermarking is to prevent illegal copying, modifying, and even spreading widely. Digital watermarking becomes a more popular technique in recent years due to the increasing importance of the copyright protection of electronic documents and media to attach day by day. Hence, a good robust digital watermarking must have following characteristics [15] [16] [17] [18].

1. Robustness:

Robustness refers to the ability to detect the digital watermarking after common signal processing operations. Examples of common operations on images include spatial filtering, lossy compression, printing and scanning, and geometric distortions (rotation, translation, scaling, and so on). Video watermarks may need to be robust to many of the same transformations, as well as to recording on video tape and changes in frame rate, among other influences. Audio watermarks may need to be robust to such process as temporal filtering, recording on audio type, and variations in playback speed that result in wow and flutter. Not all digital watermarking applications require robustness to all possible signal processing operations. Rather, a digital watermark need only survive the common signal processing operation likely to occur between the time of embedding and the time of detection. Clearly this is application dependent. For example, in TV and radio broadcast monitoring, the digital watermark need only survive the transmission process. In the case of broadcast video, this often includes lossy compression, digital-to-analog conversion, and analog transmission resulting in low-pass filtering, additive noise, and some small amount of horizontal and vertical translation. In general, watermarks for this application need not survive rotation, scaling, high-pass filtering, or any of a wide variety of degradations that occur only prior to the embedding of the watermark or after its detection. Thus, for example, a digital watermarking for broadcast monitoring need not be robust to VHS recording.

In some cases, robustness may be completely irrelevant, or even undesirable. In fact, an important branch of watermarking research focuses on fragile watermarks. A fragile watermark is one designed so that it is not robust. Relevant the fragile watermark are not discussed here, in this thesis, we will regard the robustness digital watermarking as our discussed target.

2. Security:

Security of a digital watermarking refers to its ability to resist hostile attacks. A hostile attack is any process specifically intended to destroy the watermark's purpose. The types of attacks we might be concerned about fall into three broad categories below.

i. Unauthorized removal:

Unauthorized removal refers to attacks that prevent a Work's watermark from being detected. It is common to distinguish between two forms of unauthorized removal: elimination attacks and masking attacks. Intuitively, elimination of a watermark means that an attacked work cannot be considered to contain a watermark at all. That is, if a watermark is eliminated, it is not possible to detect it even with a more sophisticated detector. Note that eliminating a watermark does not necessarily mean reconstructing the original, unwatermarked work. Rather, the goal of the adversary is to make a new work that is perceptually similar to the original, but will never be detected as containing a watermark. Masking attacks means that the attacked work can still be considered to contain the watermark, but the mark is undetectable by existing detectors. More sophisticated detectors might be able to detect it. For example, many image watermark detectors cannot detect watermarks that have been rotated slightly. Thus, an adversary may apply a rotation that is slight enough to be unnoticeable, with the distorted image therefore having acceptable fidelity. Because the watermark detector is sensitive to rotations, the watermark will not be detected. Nevertheless, the watermark could still be detected by a more sophisticated detector capable of correcting for the rotation. Therefore we can think of the watermark as still being present.

One another interesting form of unauthorized removal as a collusion attack. Here, the attacker obtains several copies of a given work, each with a different watermark, and combines them to produce a copy with no watermark. This is primarily a concern in transaction tracking, which entails putting a different watermark in each copy. With existing watermarking systems, it is generally believed that a fairly small number of copies suffice to make a collusion attack successful [19] [20] [21]. How serious this problem is depends on the contest in which transaction tracking is being used. However, in the studio dailies application, it is very unlikely that any one employee will be able to obtain many different copies of a given film clip; therefore, collusion attacks are of less concern.

ii. Unauthorized embedding:

Unauthorized embedding, also referred to as forgery, refers to acts that embed illegitimate watermarks into works that should not contain them. Here, we are not concerned with whether an adversary can render a watermark undetectable, in that doing so would cause the detector to, correctly, identify a work as inauthentic. However, if an adversary has the ability to perform unauthorized embedding, she can cause the detector to falsely authenticate an invalid work.

iii. Unauthorized detection:

Unauthorized detection, or passive attacks, can be broken down into three levels of severity. The most severe level of unauthorized detection occurs when an adversary detects and deciphers an embedded message. This is the most straight forward and comprehensive form of unauthorized reading. A less severe form of attack occurs when an adversary can detect watermarks, and distinguish one mark from another, but cannot decipher what the marks mean. Because watermarks refer to the works in which they are embedded, the adversary might be able to divine the meanings of the marks by comparing them to their cover works. The least severe form of attack occurs when an adversary is able to determine that a watermark is present, but it is neither able to decipher a message nor distinguish between

embedded messages.

In conclusion, unauthorized removal and embedding are referred to as active attacks because these attacks modify the cover work. Unauthorized detection does not modify the cover work and is therefore referred to as a passive attack. In general, passive attacks are of more concern in steganography than in watermarking, but there are watermarking applications in which they might be important. For example, suppose we have a broadcast monitoring reports. An adversary who can read our watermarks could set up a competing service, without having to incur the cost of embedding. The relative importance of these attacks depends on the application. In fact, there are situations in which the watermark has no hostile enemies and need not be secure against any type of attack. This is usually the case when a watermark is used to provide enhanced functionality to consumers. However, for applications that do require some level of security, it is important to understand the distinctions between these types of attack.



3. Capacity:

Capacity means that different digital watermarking techniques can embed watermarks of different sizes on the same image. If the digital watermarking technique can embed the bigger watermark or embed more than one watermark, it will make the technical application aspect of watermark more widely and also more robust. Data payload of the digital watermarking is closely related to embedding watermark algorithm and influence the quality of the image after embedding watermark directly at the same time. So a better algorithm must embed many digital watermarking but not reduce the quality of the image.

4. Unambiguous:

Unambiguous means that extract digital watermarking from stego-information must recognize clearly, in order to identify copyright ownership, and can not ambiguous lest it cause disputing about copyright ownership.

5. Universal:

Universal means that the embedding digital watermarking algorithm should be generally suitable for different multimedia information, such as the picture, image and sound so on. Although in course of embedding is not same, the same algorithm is used on different Medias, but its' result should be the same.

6. Imperceptibility:

Imperceptibility also referred to as transparency, means that the quality between the original information and stego-information must minimally difference after the embedding watermark, that is to say, the digital watermarking should not perceptible by the hummus vision system.

7. Statistically Undetectable:

Statistically Undetectable means that it is possible to detect the digital watermark by statistic method. That is to say, the statistic characteristic should be the same between the original information and stego-information after embedding the digital watermarking.

8. Embedding effectiveness:

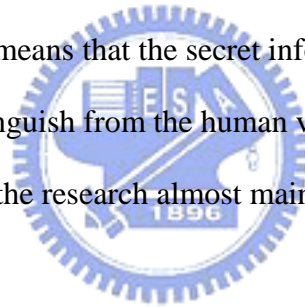
The effectiveness is the probability of detection immediately after embedding. This definition implies that a watermarking system might have an effectiveness of less than 100%. Although 100% effectiveness is always desirable, this goal often comes at a very high cost. Depending on the application, we might be willing to sacrifice some effectiveness for better performance with respect to other characteristics. For example, consider a stock photo house that needs to embed proof of ownership watermarks in thousands of images each day. Such a system might have a very high fidelity requirement, and it may be the case that certain images cannot successfully watermark within those fidelity constraints. The photo house may then have to decide whether to allow the images to remain unmarked, and thus unprotected, or allow the introduction of more distortion to maintain a 100% effectiveness rate. In some case, the former choice is preferable. In some cases, the effectiveness of a watermarking system may be determined analytically. It can also be estimated empirically by simply embedding a

watermark in a large test set of images. The percentage of output images that result in positive detections will approximate the probability of effectiveness, provided the number of images in the set is sufficiently large and is drawn from the same distribution as the expected application images.

However, more and more researches of the digital watermarking techniques are addressed in recent years. In general, we may qualify the digital watermarking techniques depending on the attributes approximately below.

1. Distinguish with the vision characteristic:

Digital watermarking can be divided into visible and invisible. Visible digital watermarking means that it declares the picture mark or characters of ownership, showing on the protected image and can distinguish from the human visual system directly. On the contrary, invisible digital watermarking means that the secret information is hidden in the protected image, which is unable to distinguish from the human visual system directly, must need special method to extract it. Recently, the research almost mainly emphasizes on invisible digital watermarking.



2. Distinguish by the resisting of the digital watermarking:

Digital watermarking can be divided into robust and fragile according to the resisting of the digital watermark. Robust digital watermarking means that if the watermark is subjected to attacks, it still maintains undeleted and not be degraded characteristics. That is to say, robust watermarks have the property that it is infeasible to remove them or make them useless without destroying the object at the same time. It has been inferred by Cox et al. that the mark should be embedded in the most perceptually significant components of the object. On the contrary, fragile digital watermarking means that the watermark is sensitive to attacks, easy to delete and damage, even it is subjected to slightly modify so that the hidden information will be destroyed. Fragile digital watermarking can be used to authenticate the content and hence prove that an object has not been “doctored” and might be useful if digital images are used as

evidence in court. Note this thesis mainly focuses on robust digital watermarking.

3. Distinguish by imbedding the way:

Digital watermarking can be divided into spatial domain and frequency domain. Spatial domain digital watermarking refers to embedding a watermark by modifying the pixels of the original image. In addition, frequency domain watermarking refers to transforming the original image into some kind of frequency form, then embedding the watermark by modifying the frequency coefficient, and finally transforming it back into the image again.

4. Distinguish by extracting digital watermarking whether needs original image:

Digital watermarking can be divided into blind and non-blind. Blind digital watermarking refers to extracting the watermark, when marked and unmarked original images are not necessary. On the contrary, non-blind digital watermarking means that the extraction function requires the unmarked original image.

Hence, digital watermarking techniques mainly utilize the properties that it is not sensitive to border regions or smooth areas for the human visual system, and it is not easy to notice a little detail change of the image, in order to hide the watermark. Recently the most classification of digital watermarking is mainly divided into the spatial domain and frequency domain. We introduce them in section 2.3.1 and section 2.3.2 respectively below.

2.2.1 Spatial Domain Watermarking Technique

Spatial domain watermarking technique utilizes the properties that it is not easy to recognize a slight change of the image for the human visual system, and it does not destroy the quality of the original image, in order to embed a watermark is to modify a little pixels of the image directly. That is to say, the most advantage of spatial domain watermarking technique is that it definitely maintains the quality of the image after embedding the watermark. Its related methods are described below.

1. Least Significant Bit (LSB):

"LSB" is the abbreviation of "Least Significant Bit", which is the embedding technique that is developed earliest and also utilized widely. It is addressed by Schyndel, Tirkel, and Osborne [22] in 1994 at first, mainly uses direct embedded and M-sequences embedded methods, which embed digital watermarking into less important bit, in general, almost modify the pixels of the least significant bit. Gray-level image usually uses 8-bits to record the gray-value of every pixel, so different gray-value represents different color. Embedding the hidden information into the least significant bit, that is the minimum impact on the quality of the cover-image, and embedding payload is 1/8 sizes of the image. Of course, we can embed not only one bit, but in opposition the quality of image is degraded after embedding. At most we can modify the least three significant bits, the quality of the original image will maintain according to the experimental result.

In order to increase the capacity of embedding by LSB, there are two methods can reach: the first method is fixed-sized LSB embedding, that is to say, fixed increasing capacity of embedding every pixel. The general image is fixed embedded hidden information into three bits, which is not perceptual for human visual system according to the experimental analysis. But this method is easy to extract the hidden watermark by illegal users. Walton [23] addressed improved methods that utilized pseudo random number generator to control the embedding position of the image. However, the resistance of these methods is very weak for attacks, for example, it may cause the digital watermarking is too degraded to recognize even incurs simple image processing such as image compressed and blur so on.

The second method is variable-sized LSB embedding, that is to say, it is decided the capacity of embedding hidden information into every pixel according to consider the characteristics itself of every pixel. Hence, if we do not consider its' undetected and robustness, embedding payload can achieve more than 50% image size by combing the above two methods.

In conclusion, the disadvantage of LSB embedding technique is that the resistance is very

weak for the generality of attacks, and it is also very sensitive to noise. It is aimed to this disadvantage, the hidden information embedded into the higher bits of the image, but not degrade the quality of the image a lot, hence, Chin-Chen Chang [24] addressed a distortion reduction method, mainly utilize pseudo random number generator to find out the embedding locations and bits, due to the embedding bits may be higher bits, so it must adjust the pixel values to reduce the differences between the original image and the image after embedding.

2. Image Quadtree:

Digital watermarking should be embedded the median frequency band according to frequency domain concept, because embedding the watermark into low frequency band is easy to discover and embedding the watermark into high frequency band is easy to destroy by compressing distortion. That is to say, after the image transforms into frequency domain, the high frequency band represents the areas of high pixel value changing in the image, which is often abandoned firstly by image compressed, hence the watermark is not be embedded into the high frequency band. However, low frequency band represents the smooth areas in the image, which be fewer subjected to attack, if we embed the watermark into the low frequency band, so that a little pixel values change may let the quality of the origin image changed obviously. Hence, the digital watermark almost embedded into the media frequency band when we consider the robustness and invisible prosperities. In the past, the general methods are addressed that transform the original image into frequency domain first, and then embed the watermark into median frequency band. Yuan-Fu Zhao [25] addressed a method called image quadtree, which find out the median frequency band in the spatial domain. In this method, he utilized spanning tree concept to transform the pixel values of the original image to the quadtree that embedded the watermark into some leaves nodes. In the image quadtree, the higher level leaf node represents the bigger image region; the variation of the color level neighborhood is smaller, represents the low frequency band of the original image. On the contrary, the lower level leaf node represents the smaller image region and the variation of the

color level neighborhood is smaller, represents the higher frequency band of the original image. So it is suitable to embed the watermark into the middle level leaf node which represents the median frequency band. Its disadvantage is that need the original image to find out the median frequency which embedded the watermark. Spatial domain watermarking technique still has many other methods, we list the methods which corresponding this thesis for the basis purpose.

2.2.2 Frequency Domain Watermarking Technique

Frequency domain watermarking technique mainly refers to transform the original image into frequency domain, by adjusting the coefficient after transforms in order to embed into watermark, and then return to the original image in the spatial domain. The main transform techniques have discrete cosine transform (DCT), fast Fourier transform (FFT), discrete wavelet transform (DWT), simply introduced as follows [28].

1. Discrete cosine transforms (DCT):

DCT technique refers to utilize discrete cosine to transform the image information from spatial domain into frequency domain, but in opposite, transform the image information from frequency domain into spatial domain, called inverse DCT (IDCT). The main idea is to divide the original image into 8x8 sizes of image blocks which not overlapped. After for all pixels of every image block in the spatial domain minus 128, then execute DCT by utilizing Formula 2.1 below, in order to get one frequency image block which the number of pixels is the same as that in the spatial image block. Finally, the frequency information transformed with IDCT by utilizing Formula 2.2 below, and then adding the value 128 to every pixel, that can get the original image.

$$d(i, j) = \frac{1}{\sqrt{2N}} c(i)c(j) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x, y) \cos\left[\frac{(2x+1)i\pi}{2N}\right] \cos\left[\frac{(2y+1)j\pi}{2N}\right] \quad (\text{Formula 2.1})$$

$$f(x, y) = \frac{1}{\sqrt{2N}} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} c(i)c(j) d(i, j) \cos\left[\frac{(2x+1)i\pi}{2N}\right] \cos\left[\frac{(2y+1)j\pi}{2N}\right] \quad (\text{Formula 2.2})$$

$$\left\{ \begin{array}{l} i = 0, c(i) = \frac{1}{\sqrt{2}} \\ i = 1, 2 \dots, c(i) = 1 \end{array} \right. \quad \left\{ \begin{array}{l} j = 0, c(j) = \frac{1}{\sqrt{2}} \\ j = 1, 2 \dots, c(j) = 1 \end{array} \right.$$

$f(x, y)$: Pixel value in the spatial domain x, y : Location in the spatial domain

$d(i, j)$: Pixel value in the frequency domain i, j : Location in the frequency domain

N : Size of the original image

After the information of the original image transforms into frequency domain, its frequency distribution from high frequency to low frequency is the same to from above the left to below the right in Fig.2-1. Among them, the value in the most upper-left corner is called DC coefficient, represents the lowest frequency (0), other frequency coefficients are called AC coefficient. Median and low frequency represent the most important portions in the original image, and also the region which influences on the quality of the image, so mostly image processing is keep this region as far as possible.

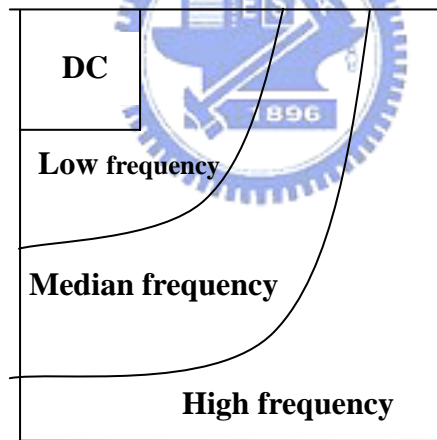


Fig.2-1 Image frequency distribution

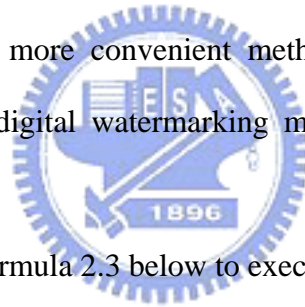
The procedure of embedding watermark divided four steps, described below in turn.

- i. Random rearranging in the original image and digital watermark.
- ii. Cutting the image into 8×8 size of image block, and executes DCT to obtain the coefficient of DCT.
- iii. Choosing the coefficient of the median frequency band, and modify it in order to embed the watermark.

iv. Executing IDCT to the modified coefficients, so that return to the spatial domain.

2. Fast Fourier Transform (FFT):

Discrete Fourier Transform (DFT) has developed for a long time, often applied to digital signal processing, which transformed signals into frequency domain in order to analyze characteristics of the frequency. Traditional DFT utilized limitless length waveform of sin function and cosine function, which combined approximately original waveform of signal according to different amplitudes in different frequency. Apply this method to image processing, so as to obtain a frequency spectrum decomposition of original image. But traditional DFT will consume a large amount of time when making operation. Hence, now researches almost utilize Fast Fourier Transform (FFT) to obtain frequency spectrum corresponds to signal. Base on this method, not only the speed in computing frequency spectrum, but also provide a more convenient method on digital signal processing. The procedure of embedding the digital watermarking mainly divides into three steps, shown below respectively in turn.



- i. Original image utilizes Formula 2.3 below to execute FFT.
- ii. Modify the coefficients of frequency in the frequency spectrum in order to embed the digital watermarking.
- iii. Transform these coefficients of frequency back into the spatial domain.

$$\begin{aligned}
 F(k) &= \sum_{n=0}^{N-1} f(n)e^{-j\left(\frac{2\pi}{N}\right)nj} & k = 0,1,\dots,N-1 \\
 &= \sum_{n=0}^{N-1} f(n)W_n^{nk} & W_n = e^{-j\frac{2\pi}{N}}
 \end{aligned}
 \tag{Formula 2.3}$$

3. Discrete Wavelet Transforms (DWT):

Now there are many methods about Discrete Wavelet Transforms in research, this thesis will introduce a simpler method, called Haar function. Main idea is to consider all pixels as the independent number separately, and make adding and minusing operation in order to

obtain the frequency of this image, among of them the portion of addition represents average, and the portion of subtraction represents variation. However, there are approximately two steps in Haar function: horizontal division and vertical division. The values of addition portion store on the half-left portion, and the value of subtraction portion store on the half-right portion when making horizontal division. The values of subtraction portion store on the upper-half portion, and the value of subtraction portion store on the below-half portion when making vertical division. After the first horizontal division and vertical division, we call it one-dimensions DFT. So repeat them in order to obtain the low frequency image block and frequency distribution of the original image below in Fig.2-2. Among them, the value in the most upper-left gray frequency block that represent the lowest frequency block and the most important portion of the image.

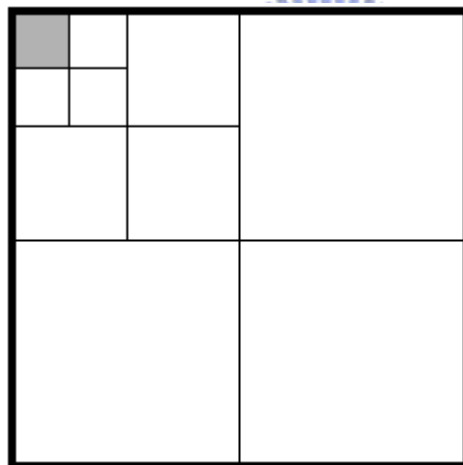


Fig.2-2 Three-dimensions Haar function DWT

The procedure of embedding watermark divided four steps, described below in turn.

- i. Make DWT to the original image.
- ii. Choose the frequency bands of embedding watermark.
- iii. Find out the less important frequency bands in frequency bands which chose in ii, and modify the pixels of some points in order to embed the digital watermark.
- iv. Transform these coefficients of frequency back into the spatial domain.

In collusion, most frequency domain watermarking techniques in the principle of

embedding watermark actions are similar to the spatial domain watermarking techniques, the difference between them are only modify the pixels or the coefficients of frequency domain. However, the frequency domain watermarking technique needs a lot of computations on transform to find out the location of median frequency bands.

2.3 Basic Notions

In this section, we will simply introduce public key and private key techniques in 2.3.1. In section 2.3.2, we will describe symmetric and asymmetric watermarking scheme.

2.3.1 Public Key and Private Key Digital Watermarking System

In order to making digital watermarking systems safer now, some systems already introduce cryptography techniques among them. On the basis of using the different cryptography techniques, we divided them into public key digital watermarking system and private key digital watermarking system respectively.

In the private key digital watermarking system, sender and receiver own a same secrete key together and use a traditional private key generator, which generates a very long series of pseudo random number sequence, that can choose which bit positions to embed or extract the digital watermark.

For the public key digital watermarking system, if Tom and John have no chance to own a same private key together, but John have a public key of Tom, so John can use Tom's public key to encrypt secret messages that he wanted to transfer, then embedded these cipher text into original system according to embedding digital watermarking methods. Only Tom owns a decrypt key, so he can extract these secret messages.

Watermarking algorithms also can be classified into fragile watermarking and robust watermarking [32] [33]. The public-key watermarking algorithm can be more effective to face the attacks. Also it has more potential value of applications. Some public-key fragile

watermarking algorithms are proposed. The Wong's algorithm [31], which based on public key cryptography, is a typical one. However, there are few public-key robust watermarking algorithms proposed since they are requested to survive severe tampering. In Wong's algorithm, any subtle change in watermarked media will make the decrypt failure. Thus Wong's method can not be applied simply to obtain a robust watermarking algorithm.

2.3.2 Symmetric and Asymmetric Watermarking Scheme

Symmetric watermarking scheme means the key used for watermark embedding must be available at the watermark detector, which uses the same sequence for embedding and detecting, has the security problem that with only the detector [4], an attacker can easily estimate and remove the embedded watermark [29] [30]. That's to say, symmetric means that the detection process makes use of the parameters used by the embedding process. The knowledge of these parameters allows pirates to forge illegal contents by modifying or removing watermark. This set of parameters is called the secret key and must be stored safely. This is not possible in consumer electronics. Tamper proof device is too expensive.

This is the reason why the cryptography domain has been recently studied [34] [35] [36]. They should be robust symmetric techniques with a detector needing a set of parameters called the public key different from the embedding's secret key. Knowing the public key, it should be neither possible to deduce the private key nor possible to remove the watermark.

One particular problem with state-of-the-art watermarking schemes is that they are symmetric [3]. The keys necessary for watermark embedding and detection are identical. Thus, the watermark detector knows all critical parameter of the watermarking scheme that also allows efficient removal of the embedded watermark. Using watermark technology for copy protection, the watermark detector needs to implement in many cheap consumer devices all over the world. A symmetric watermarking scheme presents a security risk, since the detector has to know the required private key. However, cheap tamper-proof devices are

hardly producible, and thus, pirates can obtain the private key from such devices and use them to outwit the copy protection mechanism. For this reason, we would like to develop a watermarking scheme where detection of the watermark is possible with a public key that does not give enough information to impair the embedded watermark. Such a scheme is called asymmetric.

However, in general, most researchers focus on symmetric watermarking, i.e., it is different or takes lots of efforts to embed, change, remove, and extract a watermark. This will make image authentication more laborious and limit the applications of digital watermarking. Thus, asymmetric watermarking is addressed. It demands that a watermark is easy to extract, but only authorized people can embed, change, or remove this watermark.

First, we will explain our notation and describe a general point of view on watermarking schemes below. For a better understanding of the differences between symmetric and asymmetric schemes, we will describe both of them [3].

We view digital watermarking as a communications problem, where the watermark information $b \in \beta$, with β denoting the finite set of all possible watermark messages, is transmitted over a hostile channel. The host signal \underline{x} serves as the carrier for the watermark information. In this paper, we adopt vector notation for signals that is

$\underline{x} = [x[0], x[1], \dots, x[N-1]]^T$ with $x[i]$ being the i th signal sample. We do not focus on a specific data type. The signal \mathbf{x} can denote audio, image or video data, or any transform domain representation of such multimedia data. In practice, watermarking schemes have to be optimized for the specific features of different host signals. Here, our intention is to compare basic concepts without considering details that are strongly dependent on the specific multimedia data.

Any modification of the host signal \underline{x} does affect its quality, thus an assessment of watermarking schemes is not possible without defining a quality measurement. Good quality

measurements are again strongly dependent on the data at hand. However, as a rough approximation, the *mean squared error* (MSE) between the original host signals and any modified signal can be used as a quality measurement.

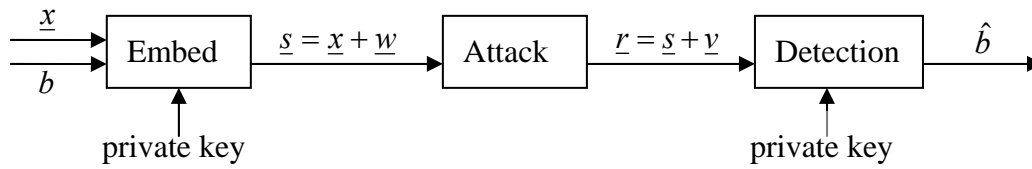


Fig.2-3 General blind symmetric watermarking scheme

Fig.2-3 depicts a general blind symmetric watermarking scheme [3]. The term “blind” indicates that the host signal \underline{x} is not known at the watermark detector. The watermark information b is embedded into the host signal \underline{x} dependent on a private key. All modifications introduced by the embedding process are denoted by the watermark signal \underline{w} , so that the public signal \underline{s} can be expressed as $\underline{s} = \underline{x} + \underline{w}$. The distortion introduced by the embedding of the watermark is given by $D_E = E \{ (s - x)^2 \} = E \{ w^2 \}$. Here, $E \{ \cdot \}$ denotes expectation.

The public signal \underline{s} is subject to a variety of different *attacks*. We use the term *attack* for any signal processing that, intentionally or not, reduces the reliability of watermark detection. The modifications introduced by the attack(s) can be summarized by the additive, but not necessarily independent, signal \underline{v} . Of course, an attack is useless if the attacked signal $\underline{r} = \underline{s} + \underline{v}$ has such poor quality that its value is lost. Thus, the quality of the attacked signal must be sufficiently good. Many watermarking schemes can be successfully attacked by desynchronizing the embedded watermark relative to the watermark signal the detector is looking for. We do not consider desynchronized attacks formally, but point out where synchronization is a particularly difficult problem. Assuming synchronization, the quality of the attacked signal \underline{r} is measured relative to the original host signal \underline{x} . We measure the

distortion of an attacked signal by $D_A = E \{ (r - x)^2 \}$.

Finally, the detector computes an estimate \hat{b} of the transmitted watermark information b according to the private key and the received signal \underline{r} . The probability $\Pr(\hat{b} \neq b)$ of false detection should be as small as possible.

The constraints on the qualities D_E and D_A are strongly dependent on the given data and the application in mind. However, it is reasonable to assume that the allowable D_A is at least at the order of D_E , and in many cases even much larger. We use the ratio $D_{A,\min}/D_E$ as a robustness criteria, with $D_{A,\min}$ being the minimal distortion for a successful attack. Chen and Wornell [37] introduced the term “distortion penalty” for $D_{A,\min}/D_E$.

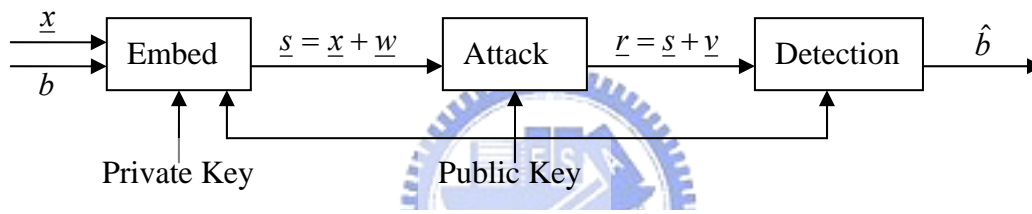


Fig.2-4 General asymmetric watermarking scheme

Fig.2-4 depicts a general asymmetric watermarking scheme. With aid of a private and a public key, the watermark is embedded into the host signal \underline{x} . The significant difference to the symmetric scheme depicted in Fig.2-3 is that all entities, embedding, attack and detection, have access to the public key necessary for watermark detection. Obviously, an attacker can try to use the knowledge of the public key to destroy the embedded watermark information.

2.4 Visual Cryptography

Visual cryptography is a new cryptography idea, which addressed from M. Naor and A. Shamir in 1994 [7], the purpose is to decrypt the ciphertext by human visual system. By their method, a shared image can be reconstructed by stacking some authorized shadow

images without performing a lot amount of complex computation. Any subset of unauthorized shadow images can not infer any knowledge about the shadow image. Visual cryptography is also an extended type of (t, n) -threshold scheme which is also named the (t, n) -visual threshold scheme. In [7], the shadow of each participant is a transparency showing random dots. The shared secret is an image composed of black and white pixels. Any t out of these n shadows can make the shared secret recognized through the human visual system when they are stacked together. Any $t-1$ (or less) shadows stacked together can generate no knowledge about the shared secret. In this section, we shall take a $(2, 2)$ -visual threshold scheme (Table.2-1) created by M. Naor and A. Shamir for example.

The image stored in the computer system can be considered a composition of pixels. Let each pixel be stored in d bits. Then, a 2^d gray-level image can be shown by using a set of pixels. The watermark pattern discussed in this section is composed of black or white pixels. It only uses one bit to express each pixel. Table.2-1 illustrates a simple $(2, 2)$ -threshold scheme based on M. Naor and A. Shamir's idea [7]. It also specifies the algorithm to encode each pixel in the shared image. This algorithm is applied to each pixel in the shared image in order to generate the corresponding subpixels in its corresponding two shadows. Each pixel P in the shared image is divided into two subpixels in each of these two shadows. If P is white, then the dealer randomly selects one of the last two rows in Table.2-1 below. Then the dealer puts two-subpixel blocks from Column 2 and 3 to corresponding positions in shadow 1 and 2, respectively.

Let's consider the result when these two shadows are stacked together. For each pixel P in the shared image, if P is black, then it generates a share with two black subpixels when these two shadows are stacked together. If P is white, then it generates a share with one black with one black subpixel and one white subpixel when these two shadows are stacked together. The result is a collection of two black/white subpixels, which are printed in close proximity to each other so that the human visual system averages their individual black/white contributions.

Through the human visual system, the share with two black subpixels will be recognized as a share dot while the block with one black subpixel and one white subpixel will be recognized as a white dot. Obviously, we can readily recognize if an image is the shared image with our visual system when these two shadows are stacked together.

















Pixel	Share1	Share2	Share1 superimposes on Share2
	 (1, 0)	 (0, 1)	 (1, 1)
	 (0, 1)	 (1, 0)	 (1, 1)
	 (1, 0)	 (1, 0)	 (1, 0)
	 (0, 1)	 (0, 1)	 (0, 1)

Table.2-1 A (2, 2)-visual threshold scheme

Note: bit "1" denotes black and bit "0" denotes white.

CHAPTER 3

The Proposed Method

In this chapter, we will introduce a new watermarking scheme of gray images by utilizing the concepts of the public key and private key. At first, in section 3.1, we will overview some gray visual cryptography schemes, and then find the problems in order to improve in next sections. In section 3.2 and 3.3, two kinds of new watermarking schemes, called PPKA and MPPKA Watermarking Schemes, will be described in detail. Finally, in section 3.4, we will discuss the applications of Public Key and Private Key Asymmetric Watermarking Schemes.

3.1 Overview of Gray Visual Cryptography Scheme

Gray-level images can be divided into 8 bit plane. In LSB method, a watermark is mainly embedded into less important low bit planes. But due to the locations of embedding watermark are not important bits, the resistances of attacks are very weak.

Since traditional digital watermarking techniques need a lot of computations, Y.C. Hou [26] tried to use visual cryptography which has the property that complex computations are not needed embedding a watermark. At the same time, he utilized to higher bit planes in the image to encrypt a watermark. The process of encryption, mainly utilized the highest bit plane in the image as Share1, and then utilized Share1 to generate Share2 according to the embedded watermark [26]. The process of decryption only extracts the highest bit plane superimposed on Share2 directly to extract the hidden information of the watermark [26]. His method [26] mainly utilizes expanding visual cryptography to encrypt, and generates Share2 which is double sizes of the original image, hence the stored spaces are also double. In order to solve this question, W.L. Zhou [27] addressed the non-expand visual cryptography to

encrypt and reduce the storing information.

Because these methods above utilized the highest bit plane in the image as Share1, the resistances of attacks are quite strong. Moreover, since the original image is not modified at all, it may be easy for someone to make mistake that the copyright is owned by himself.

In addition to the methods above, Y.C. Hou, and P.M. Chen [5] addressed another digital watermarking technique base on visual cryptography. Their digital watermarking technique mainly modified the pixels of the bottom image to embed Share1. A base visual cryptography model is in Table.3-1 below. In their scheme [5], they made a little modification of Naor and Shamir scheme [7] (Table.3-1), because they want to hide the Share1 into cover-image, 50% of black subpixels on Share1 will change the cover-image significantly, this will leave clue of embedded watermark. Hence, according to Table.3-1 [7], Y.C. Hou, and P.M. Chen [5] make a little modification and describe it follows.

The black subpixels of Share1 are changed to gray color with gray-scale equals to 247. The white subpixels of Share2 that are split by black pixel are changed to gray color with gray-scale equals to 247, but the white subpixels of Share2 that are split by white pixel remain white (gray-scale equals to 255) unchanged (Table.3-1). The color of the rest subpixels on the Share1 and Share2 are the same as Naor and Shamir does.

Then we introduce splitting watermark and embedding watermark methods respectively [5], as follows.

1. Splitting watermark method refers to split the watermark into Share1 and Share2. If the pixel of the watermark is white, then two corresponding subpixels in Share1 and Share2 are randomly assigned to gray and black color respectively (the other subpixel is transparent). The positions of gray and black subpixels in Share1 and Share2 are the same. If the pixel of the watermark is black, then we randomly assign two corresponding subpixels in Share1 and Share2 to be gray. The remaining subpixels in Share1 and Share2 have white and block color respectively. The splitting result Share1 will be embedded into the cover-image and the other

result Share2 will be the key image used to extract the embedded watermark.

2. Embedding watermark method is equivalent to superimpose Share1 over cover-image to obtain the stego-image. That's to say, if the subpixels in Share1 are gray, then the gray values of the corresponding subpixels in the cover-image decrease by 8, otherwise it remains unchanged. The reason of decreasing by 8 is that the white subpixels of Share2 that are split by black pixel are changed to gray color with gray-scale equal to 247 in Table.3-2, that is to say, if we utilize the subpixel with gray-scale equal to 247 to superimpose the original subpixel, the superimposed image quite approximates to the result of decreasing the original gray image by 8, because the subpixel with gray-scale decreases from 255 to 247 and the subpixel of 255 is transparent by human visual system.











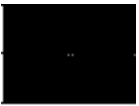


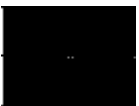
Pixel	Share1	Share2	Share1 superimposes Share2
			
			
			
			

Table.3-1 Basic Visual Cryptography model


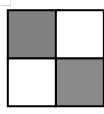


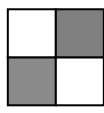
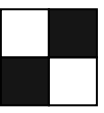


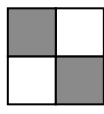


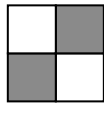

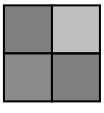
Pixel	Share1	Share2	Share1 superimposes Share2
			
			
			
			

Table.3-2 Modified Visual Cryptography model addressed by Y.C. Hou, and P.M. Chen

Although there are some advantages of using this watermarking scheme [5], such as the process of embedding is simpler than those transformations, e.g. DCT, FFT, DWT, etc, which are most used by the watermarking scheme in the frequency domain, and the extraction of watermark can easily performed by superimposing the key shared over the stego-image, there are still some problems according to my experimental results, describe as follow.

1. Splitting watermark into two shares with random patterns, but one of the splitting results, Share2, will leave very tiny clue of embedded watermark.
2. Extracted watermark is not very distinguishable and difficult to recognize by human visual system.

Aim at above watermarking scheme addressed by Y.C. Hou, and P.M. Chen [5], Bo-Cheng Shen addressed another new model, which also used modified pixels of gray-level image method, called Gray Visual Cryptography models [28]. In Gray Visual Cryptography models, already further improve a little the visibility of extracted watermark, but the quality of the stego-image obviously reduces a little (its PSNR decreases from 33 to 30), that is to say,

if we need to embed more than one digital watermarking for widely applications, the method addressed by Bo-Cheng Shen [28] seem unable to achieve this purpose, so there will be some improvements on the Gray Visual Cryptography models.

Hence, this thesis mainly further modifies those methods of Gray Visual Cryptography model in order to satisfy the property which can embed more than one digital watermarking into cover-image for widely applications, in next sections, there will be described in more detail.

3.2 Public Key and Private Key Asymmetric (PPKA) Watermarking Scheme

With the rapid internet development, more and more digital information are transmitted and exchanged on Internet. The importance of copyright protection grows with each passing day; hence, we need the more robustness and multipurpose digital watermarking scheme. And the concept of public key and private key also becomes widespread application on cryptography domain. In previous section 2.2, we have simply described the basic concepts of public key, private key, and the asymmetric watermarking scheme. Here, we will try to address a new watermarking scheme, called Public Key and Private Key Asymmetric Watermarking Scheme, abbreviated to PPKA Watermarking Scheme, which combines the concepts of public key and private key with an asymmetric watermarking scheme based on the modified gray visual cryptography models. The following is the skeleton of PPKA Watermarking Scheme.

This scheme divided into Embedding Watermark mechanism and Authentication mechanism, we describe them respectively as follows.

1. Embedding Watermark mechanism:

The first phase is Embedding Public Watermark mechanism. First, we split the Public Watermark into Public Share1 and Public Share2. Public Share1 will be embedded into the

cover-image and Public Share2 will be the key image which is considered as a Public Key that will be used to extract the Public Watermark. Next, we embed Public Share1 into cover-image, then processing it randomly by using a random function γ to generate an image, called the Public-random image, which will be used in the second phase.

The second phase is Embedding Private Watermark mechanism. Similarly, we split the Private Watermark into Private Share1 and Private Share2. Private Share1 will be embedded into the cover-image and Private Share2 will be the key image which is considered as a Private Key that will be used to extract the Private Watermark. Next, we embed Private Share1 into Public-random image, then processing it re-randomly by using a re-random function γ^{-1} to generate an image, called the Public-Private Stego-image.

2. Authentication mechanism:

We divide this mechanism into Public Watermark Authentication mechanism and Private Watermark Authentication mechanism, and describe them respectively below.

Public Watermark Authentication mechanism is to embed Public Share2 into Public-Private Stego-image to extract the Public Watermark. Private Watermark Authentication mechanism is to process Public-Private Stego-image randomly by a random function γ , then embed Private Share2 into it to extract the Private Watermark. The algorithms of Embedding Watermark mechanism, Public Watermark Authentication mechanism, and Private Watermark Authentication mechanism described respectively below.

1. Algorithm: Embedding Watermark mechanism

Input: three $2^n \times 2^n$ gray-level images represent the cover-image, Public Share1, and Private Share1 respectively; two functions represent random function γ and re-random function γ^{-1} respectively.

Output: $2^n \times 2^n$ gray-level Public-Private Stego-image

Step1: Split the Public Watermark into Public Share1 and Public Share2, and then embed Public Share1 into the cover-image to create the Public-Cover image.

Step2: Process Public-Cover image randomly by a random function γ to generate Public-random image.

Step3: Split a Private Watermark into Private Share1 and Private Share2, and then embed Private Share1 into Public-random image to generate Public-Private random image.

Step4: Process Public-Private random image re-randomly by using a re-random function γ^{-1} to generate the Public-Private Stego-image.

2. Algorithm: Public Watermark Authentication mechanism

Input: two $2^n \times 2^n$ gray-level images represent Public-Private Stego-image and Public Share2 respectively

Output: one $2^{n-1} \times 2^{n-1}$ gray-level image represent Public Watermark

Step1: Embed Public Share2 into Public-Private Stego-image to extract the Public Watermark.

3. Algorithm: Private Watermark Authentication mechanism

Input: two $2^n \times 2^n$ gray-level images represent Public-Private Stego-image and Private Share2 respectively

Output: one $2^{n-1} \times 2^{n-1}$ gray-level image represent Private Watermark

Step1: Process the Public-Private Stego-image randomly by a random function γ to generate a Public-Private random Stego-image.

Step2: Embed Private Share2 into Public-Private random Stego-image to extract the Private Watermark.

It is worthy of our notice that random processing in the course of Embedding Watermark mechanism is necessary, because it makes the hidden watermarks secure, and leave fewer clues of embedded watermarks. However, we also consider the quality of Public-Private Stego-image after embedding two watermarks and the visibility of the extracted Public Watermark and Private Watermark, so we will try to adopt optimum methods aimed at the Embedding Watermark mechanism in PPKA Watermarking Scheme. In next sections, we will

discuss them in more detail.

In section 3.2.1, we address the first model of the Modified Gray Visual Cryptography, which improves the problem that leave tiny clues of embedded watermarks in the Modified Visual Cryptography model addressed by Y.C. Hou, and P.M. Chen [5]. However, the extracted watermark is too distinguishable to recognize by human visual system. In section 3.2.2, we will address the second model of the Modified Gray Visual Cryptography to optimize the visibility of the extracted watermark.

3.2.1 Modified1 Gray Visual Cryptography (MGVC1) Model

In section 3.1, we have introduced the Modified Visual Cryptography model [5], first, we utilize this model to implement PPKA Watermarking Scheme. In this thesis, we use a 256×256 size of Lena picture in Fig.3-1 (a) as our cover image, a 128×128 size of Public Watermark in Fig.3-1 (b), a 128×128 size of Private Watermark in Fig.3-1 (c), a random function γ and a re-random function γ^{-1} , that we preset its random seed value to zero. Every dot of a watermark corresponds to four dots of the original image.

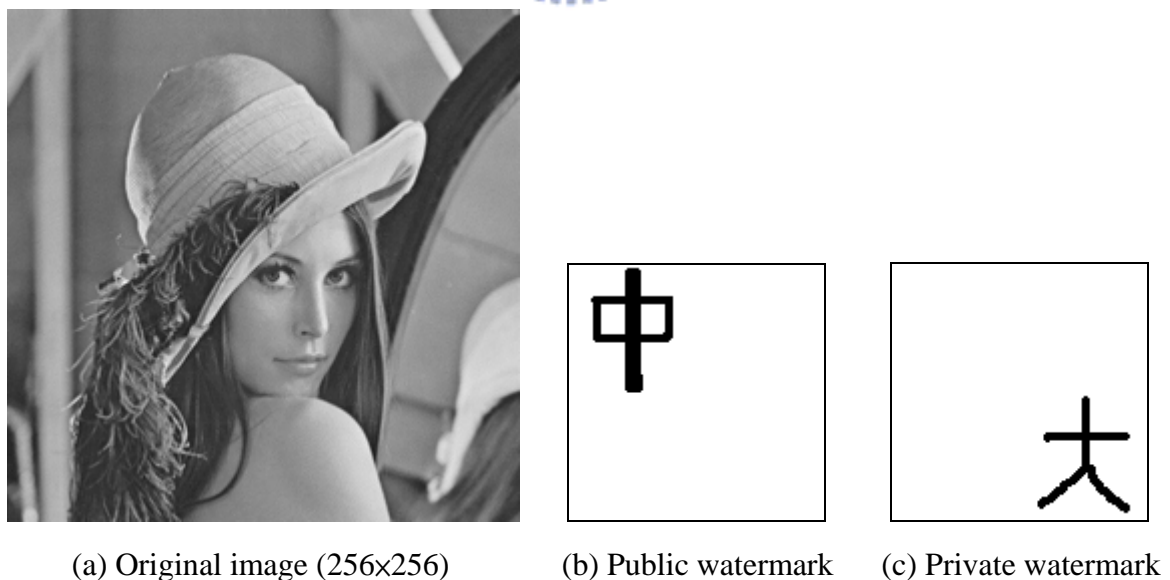


Fig.3-1 (a) Cover image, (b) Public watermark, and (c) Private watermark (128×128)

First we split a Public watermark (Fig.3-1 (b)) into Public Share1 (Fig.3-2 (a)) and

Public Share2 (Fig.3-2(b)) according to the Modified Visual Cryptography model [5] shown in Table.3-2. Experimental results below.

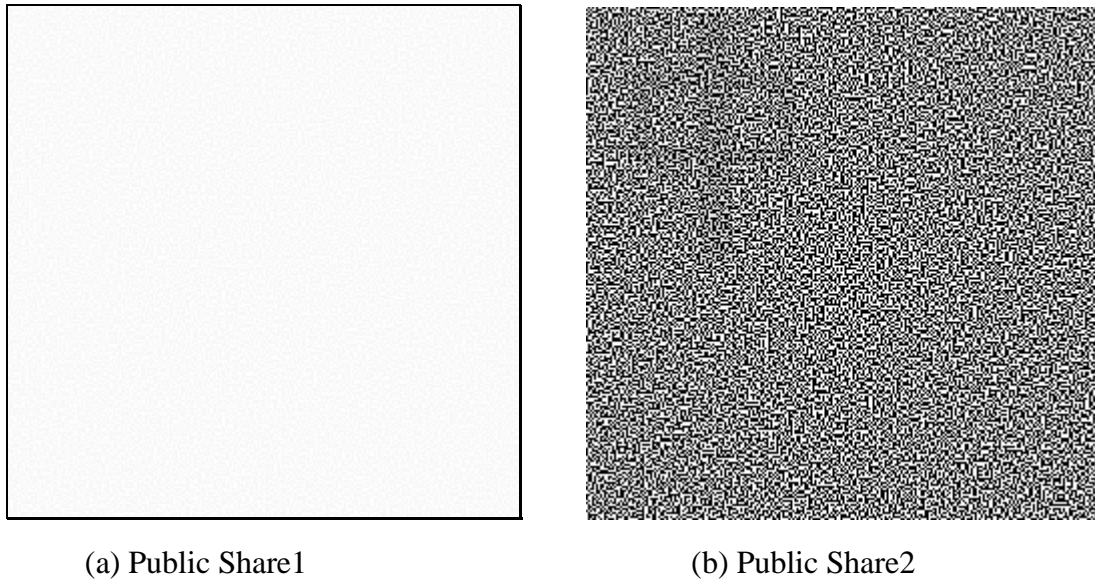
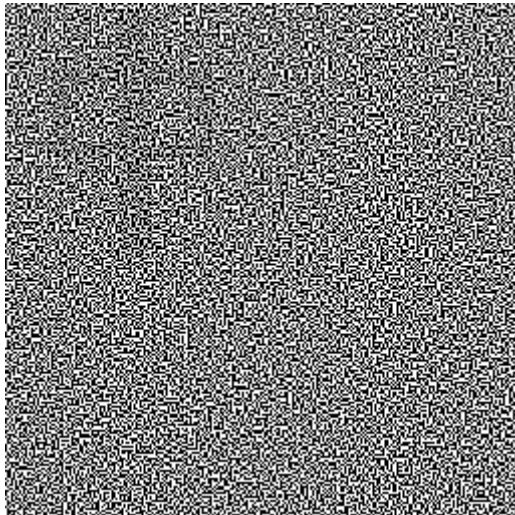


Fig.3-2 Split a Public watermark into (a) Public Share1 and (b) Public Share2 according to the Modified Visual Cryptography model.

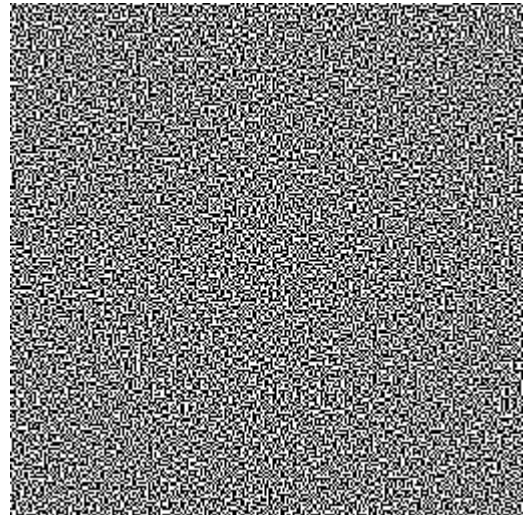
By Fig.3-2(b) above, if we observe carefully, there will be tiny clue of embedded watermark by human visual system. Hence, in order to solve this problem, we will modify their visual cryptography model (in Table.3-2) a little bit. The new modified model will be called the Modified1 Gray Visual Cryptography Model, abbreviated to MGVC1 Model. The details are described as follows.

The black subpixels of Share1 are changed to gray color with gray-scale equals to 247. The white subpixels of Share2 that are split by black pixel are changed to gray color with gray-scale equals to 251, but the white subpixels of Share2 that are split by white pixel remain white (gray-scale equals to 255) (Table.3-1). The color of the rest subpixels on the Share1 and Share2 are the same as those in the model of Naor and Shamir.

Fig.3-3(a) and (b) show the Public Share2 keys produced by the model of Y.C. Hou and P.M [5] and MGVC1 Model respectively.



(a) Y.C. Hou and P.M. model



(b) MGVC1 Model

Fig.3-3 Aim at Public Share2 compares (a) Y.C. Hou and P.M. model with (b) MGVC1 Model

By Fig 3-3(a) and (b) above, if we observe carefully, compares (a) with (b), we will find (a) Y.C. Hou and P.M. model leave tiny clue of embedded watermark by human visual system. Next, we can compare the visibility of the extracted watermark in Y.C. Hou and P.M. model with MGVC1 Model, as follow in Fig3-4 (a) and (b) respectively. For the human visual system, the clarity of the extracted watermark between them is quite similar (very blur). Hence, generally speaking, the security of this MGVC1 Model is better than Y.C. Hou and P.M. model a little.



(a) Y.C. Hou and P.M. model



(b) MGVC1 Model

Fig.3-4 Compare the visibility of the extracted watermark in (a) Y.C. Hou and P.M. model with (b) MGVC1 Model

The reason that we address this MGVC1 Model is that we want to leave no clue of the embedded watermark and not to find by human visual system, hence, we try to make the white subpixels of Share2 that are split by black pixel are changed to gray color with gray-scale equals to 251, that is to say, reduce the differences of white pixel and black pixel of Share2, i.e. compare the pixel value 251 with 247, by far, 251 is closer to 255, which is more transparent.

Then, we adopt MGVC1 Model to experiment on PPKA Watermarking Scheme. The process of the implementation is as follows.

First, we split the Public watermark into Public Share1 and Public Share2. They are shown in Fig.3-5 (a) and (b), respectively.

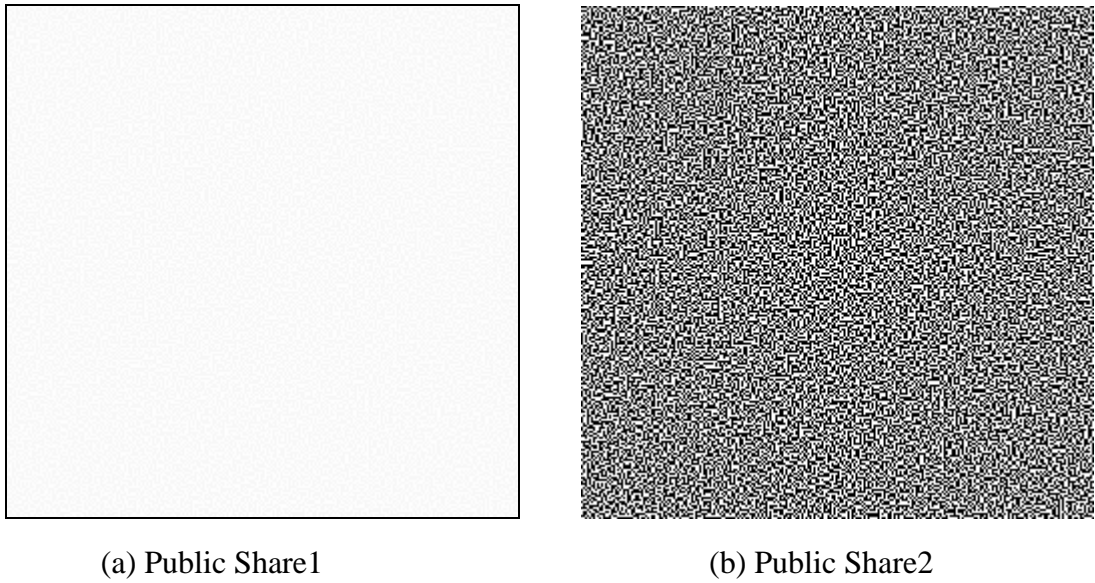


Fig.3-5 Split the Public watermark into (a) Public Share1 and (b) Public Share2 in MGVC1 Model

Next, we experiment on the embedding Public and Private watermark system as follows.

Step1: Embed Public Share1 into cover-image to create Public-Cover image.



Fig.3- 6 Public-Cover image in MGVC1 Model and PSNR= 33.08

Step2: Process Public-Cover image randomly by using a random function γ to create Public-random image.

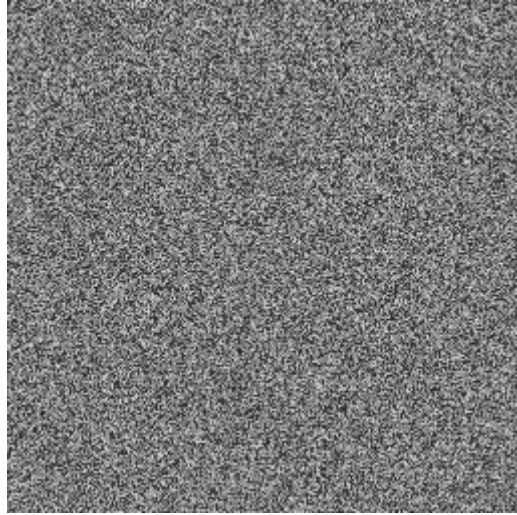


Fig.3-7 Public-random image in MGVC1 Model

Step3: Split a Private Watermark into Private Share1 and Private Share2 according to Public-random image, and embed Private Share1 into Public-random image at the same time to create Public-Private random image in Fig.3-9.



(a) Private Share1

(b) Private Share2

Fig.3-8 (a) Private Share1 and (b) Private Share2 in MGVC1 Model

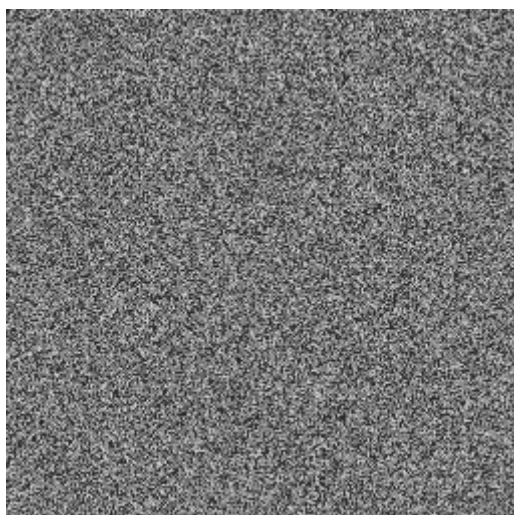


Fig.3-9 Public-Private random image in MGVC1 Model

Step4: Process Public-Private random image re-randomly by using a re-random function γ^{-1} in order to return to Public-Private Stego-image in Fig.3-10 (b). So far, this system has finished.



(a) Original image

(b) Public-Private Stego-image

Fig.3-10 Compare (a) Original image with (b) Public-Private Stego-image in MGVC1 Model, and PSNR= 28.315

Finally, we experiment on Public and Private Watermark Authentication mechanism below.

1. Public Watermark Authentication mechanism:

Step1: Embed the Public Share2 into Public-Private Stego-image, finally extract Public

Watermark in Fig.3-11.



Fig.3-11 The extracted Public Watermark in MGVC1 Model

2. Private Watermark Authentication mechanism:

Step1: Process Public-Private Stego-image randomly by a random function γ to create a Public-Private random Stego-image in Fig.3-12

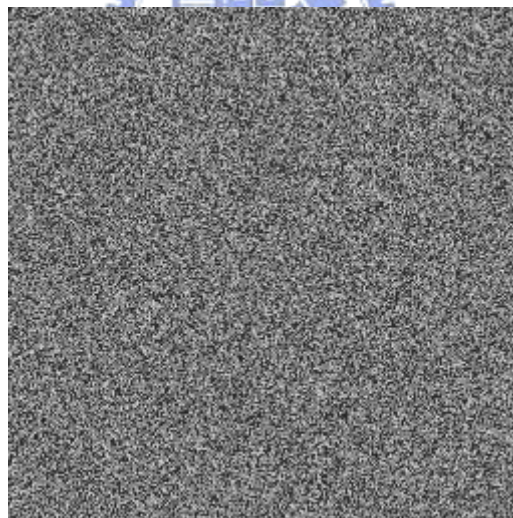


Fig.3-12 Public-Private random Stego-image in MGVC1 Model

Step2: Embed Private Share2 into Public-Private random Stego-image, finally extract Private Watermark in Fig.3-13.

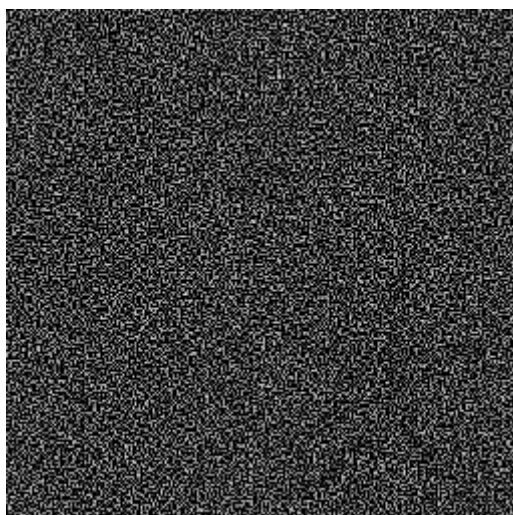


Fig.3-13 The extracted Private Watermark in MGVC1 Model

By Fig.3-10, Fig.3-11, and Fig.3-13 above, we can observe three problems in MGVC1 Model, described them as follows.

1. The PSNR of a result image (Public-Private Stego-image) has reduced to 28.315, under 30 a little, i.e. the quality of a result image is not ideal by human visual system.
2. The clarity of the extracted Public Watermark is not ideal for copyright authentication.
3. The visibility of the extracted Private Watermark is very difficult to recognize by human visual system.

Hence, MGVC1 Model still has a great improvement on PPKA Scheme, in next sections. We will try to address another suitable model step by step to solve these problems.

3.2.2 Modified2 Gray Visual Cryptography (MGVC2) Model

In order to solve those problems described in section 3.2.1, first, we try to utilize the third Gray Visual Cryptography model [28] because it has the best clarity of extracted watermark by human visual system. We summarize this model in Table.3-3 below. (+ represents “superimpose”)


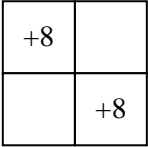
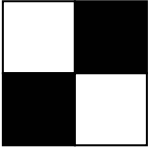
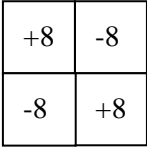
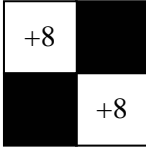
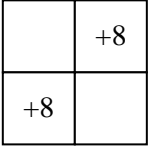
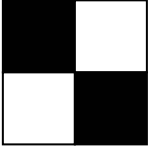
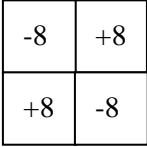
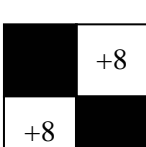

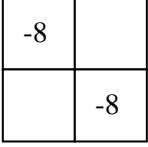
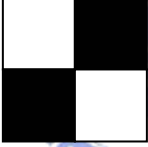
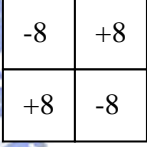
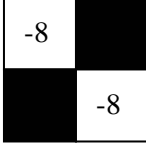
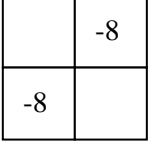
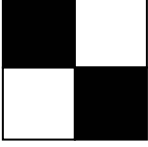
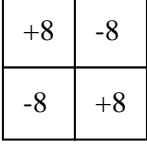
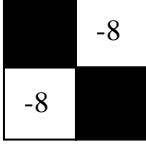
Pixel	Share1	Share2	Share1 +Original image	Share2 +Original image
	 two whitest of four dots			
	 two whitest of four dots			
	 two blackest of four dots			
	 two blackest of four dots			

Table.3-3 The third Gray Visual Cryptography models by Bo-Cheng Shen

In Table.3-3, the splitting, embedding, and extracting watermark principles are similar as those in Table.3-2. The difference between them is the splitting watermark in Table.3-3 need to refer to the original image. For example, if the pixel of the watermark is white, we choose the first or the second row of Table.3-3, and then choose the two whitest subpixels correspond

to the original image, embedding the pixels of them increased by 8 into the Share1 according to the position of the original image, and embedding the pixels of zero into the Share2 according to the other two positions of the original image. Similarly, if the pixel of watermark is black, we choose the third or the fourth row of Table.3-3, and then choose the two blackest subpixels correspond the original image, embedding the pixels of them decreased by 8 into the Share1 according to the positions of the original image, and embedding the pixel of zero into the Share2 according to the other two positions of the original image.

Then, we try to utilize the third Gray Visual Cryptography model [28] to experiment on PPKA Watermarking Scheme. The process of implementations is as follows.

First, we split the Public watermark into Public Share1 and Public Share2 according to the original image (Fig.3-1(a)). Experimental results are shown in Fig.3-14 (a) and (b) respectively.

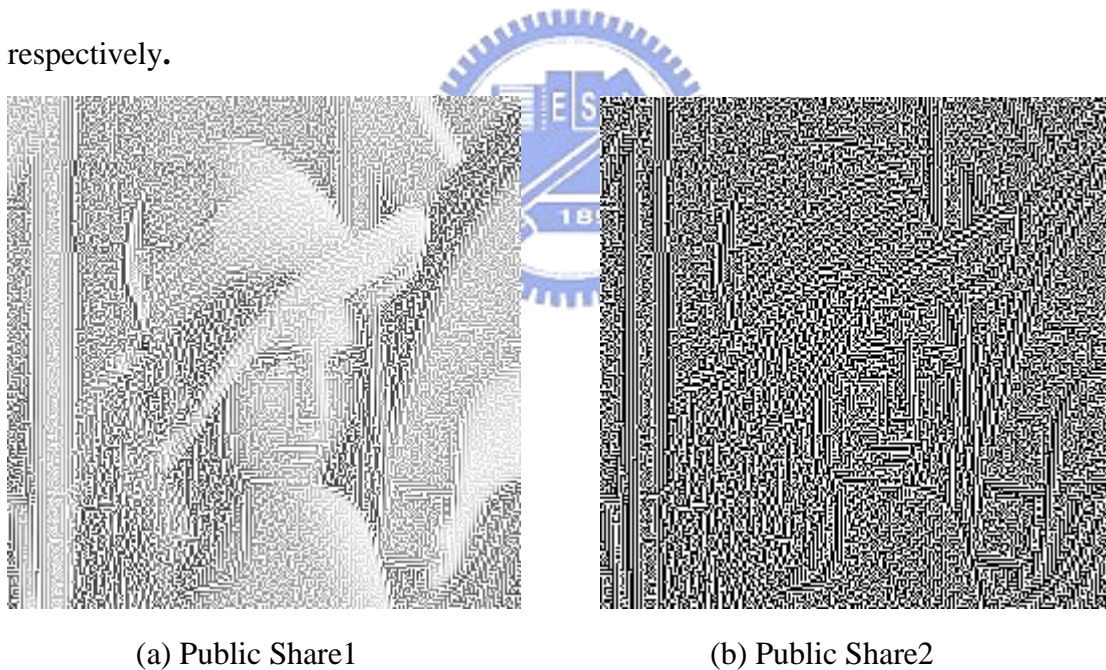


Fig.3-14 Split a Public Watermark (Fig.3-1(b)) into (a) Public Share1 and (b) Public Share2 according to an original image (Fig.3-1(a)) in the third Gray Visual Cryptography model.

Next, we experiment on the embedding Public and Private watermark system as follows.

Step1: Embed Public Share1 into cover-image to generate Public-Cover image.



Fig.3-15 Public-Cover image in the third Gray Visual Cryptography model and PSNR=30.07

Step2: Process Public-Cover image randomly by using a random function γ to create Public-random image.

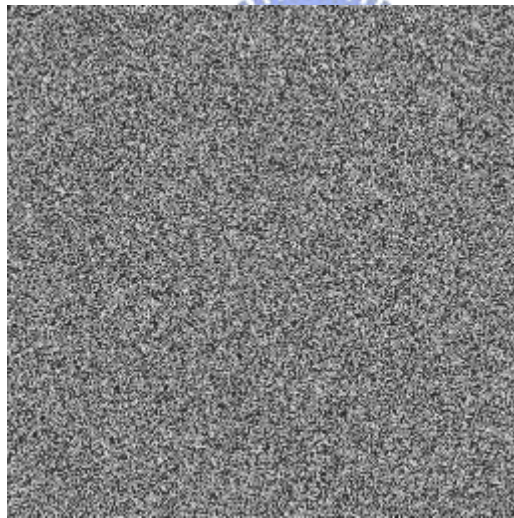


Fig.3-16 Public-random image in the third Gray Visual Cryptography mode

Step3: Split a Private Watermark into Private Share1 and Private Share2 according to Public-random image, and embed Private Share1 into Public-random image at the same time to create Public-Private random image.

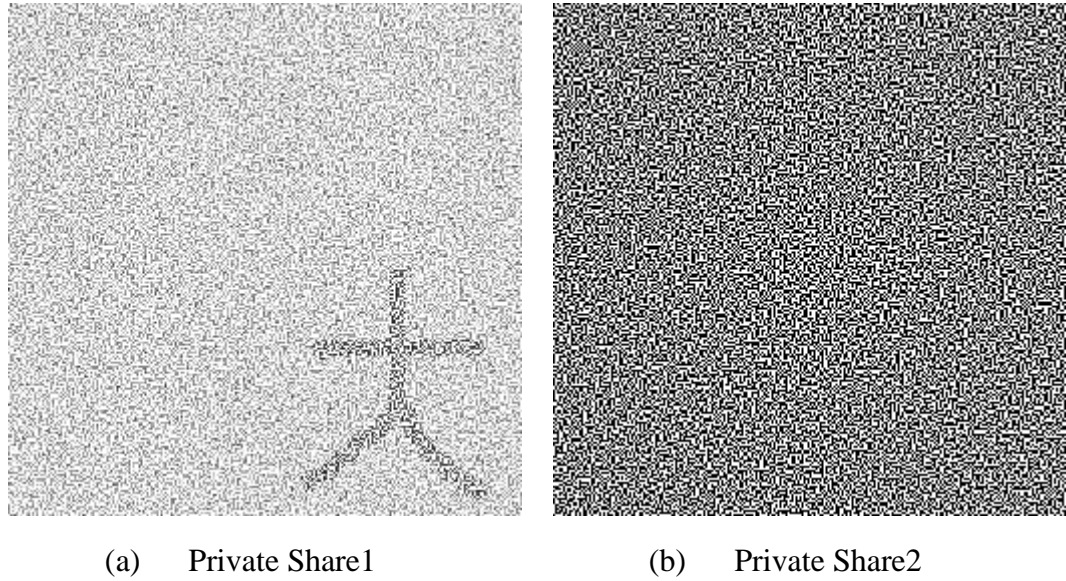


Fig.3-17 Split a Private Watermark into (a) Private Share1 and (b) Private Share2 refer to the original image in the third Gray Visual Cryptography model

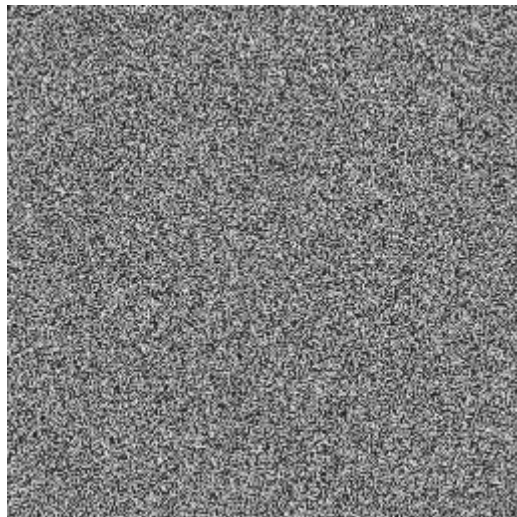


Fig.3-18 Public-Private random image in the third Gray Visual Cryptography model

Step4: Process Public-Private random image re-randomly by using a re-random function γ^{-1} in order to return to Public-Private Stego-image in Fig.3-19 (b). So far, this system has finished.



(a) Original image



(b) Public-Private Stego-image

Fig.3-19 Compare (a) Original image with (b) Public-Private Stego-image in the third Gray Visual Cryptography model, and PSNR= 26.36

By Fig.3-19 (a) and (b) above, we obviously find that the quality of the result image (Public-Private Stego-image) in this embedding Public and Private Watermark system is not ideal by human visual system and PSNR also is decreased below 30, so we try to modify this Gray Visual Cryptography model [28] to optimize the PPKA scheme, and then address another Model, called Modified2 Gray Visual Cryptography Model, abbreviated to MGVC2 Model, described this model in Table.3-4. (+ represents “superimpose”)

In Table.3-4, about splitting, embedding, and extracting watermark principle is the same in Table.3-3. But we make a little modification aimed at Table.3-3, described as follow.

If the pixel of the watermark is white, we choose the first or the second row of Table.3-4, and then choose the two whitest subpixels correspond to the original image, embedding the pixel of them increased by 4 into the Share1 according to the position of an original image. If the pixel of the watermark is black, we choose the third or the fourth row of Table.3-4, and then choose the two blackest subpixels correspond to the original image, embedding the pixel of them decreased by 6 into the Share1 according to the position of original image. The other pixels are the same principle as Table.3-3 does.


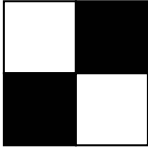
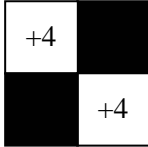
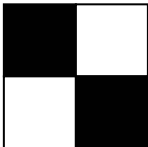
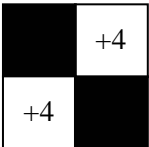

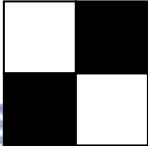
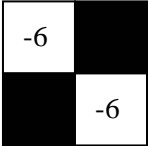
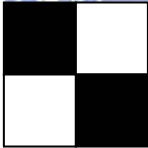
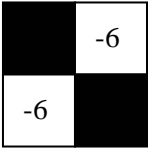
Pixel	Share1	Share2	Share1 + Original image	Share1 + Share2 +Original image								
	<table border="1"> <tr><td>+4</td><td></td></tr> <tr><td></td><td>+4</td></tr> </table> <p>two whitest</p>	+4			+4		<table border="1"> <tr><td>+4</td><td>-4</td></tr> <tr><td>-4</td><td>+4</td></tr> </table>	+4	-4	-4	+4	
	+4											
	+4											
+4	-4											
-4	+4											
<table border="1"> <tr><td></td><td>+4</td></tr> <tr><td>+4</td><td></td></tr> </table> <p>two whitest</p>		+4	+4			<table border="1"> <tr><td>-4</td><td>+4</td></tr> <tr><td>+4</td><td>-4</td></tr> </table>	-4	+4	+4	-4		
	+4											
+4												
-4	+4											
+4	-4											
	<table border="1"> <tr><td>-6</td><td></td></tr> <tr><td></td><td>-6</td></tr> </table> <p>two blackest</p>	-6			-6		<table border="1"> <tr><td>-6</td><td>+6</td></tr> <tr><td>+6</td><td>-6</td></tr> </table>	-6	+6	+6	-6	
	-6											
	-6											
-6	+6											
+6	-6											
<table border="1"> <tr><td></td><td>-6</td></tr> <tr><td>-6</td><td></td></tr> </table> <p>two blackest</p>		-6	-6			<table border="1"> <tr><td>+6</td><td>-6</td></tr> <tr><td>-6</td><td>+6</td></tr> </table>	+6	-6	-6	+6		
	-6											
-6												
+6	-6											
-6	+6											

Table.3-4 Modified2 Gray Visual Cryptography (MGVC2) Model

The reason that we make this modification is that we want to optimize the quality of the result image and maintain the clarity of extracted watermark.

Then, we adopt MGVC2 Model to experiment PPKA Watermarking Scheme, the process of experiment as follows.

First, we split the Public watermark into Public Share1 and Public Share2. Experimental result in Fig.3-20 (a) and (b) respectively.

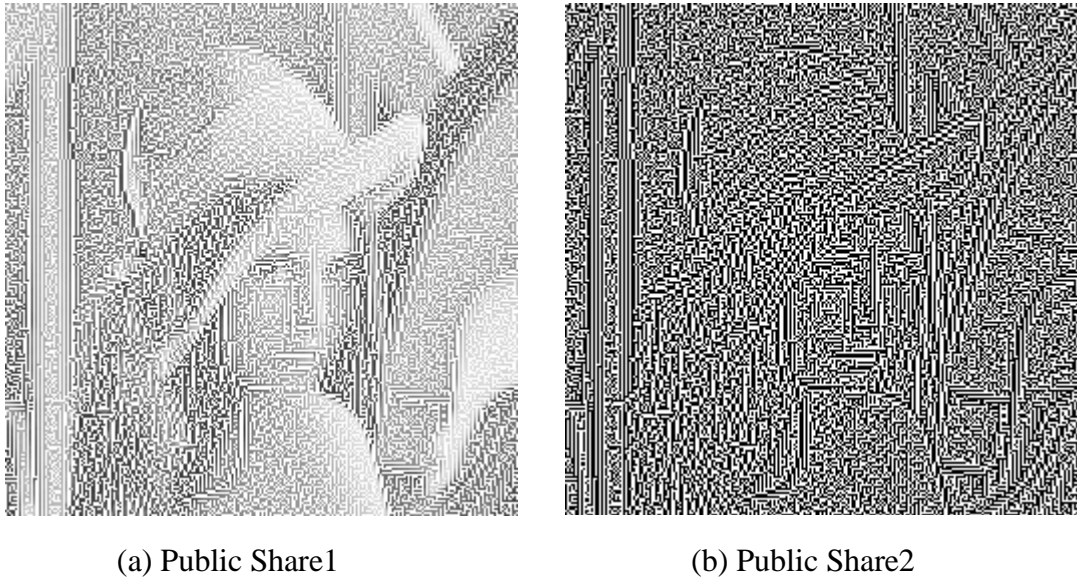


Fig.3-20 Split a Public Watermark (Fig.3-1(b)) into (a) Public Share1 and (b) Public Share2 according to an original image (Fig.3-1(a)) in MGVC2 Model.

Next, we experiment on the embedding Public and Private Watermark system as follows.

Step1: Embed Public Share1 into cover-image generates Public-Cover image.



Fig.3-21 Public-Cover image in MGVC2 Model and PSNR= 35.808

Step2: Process Public-Cover image randomly by a random function γ to create Public-random image.

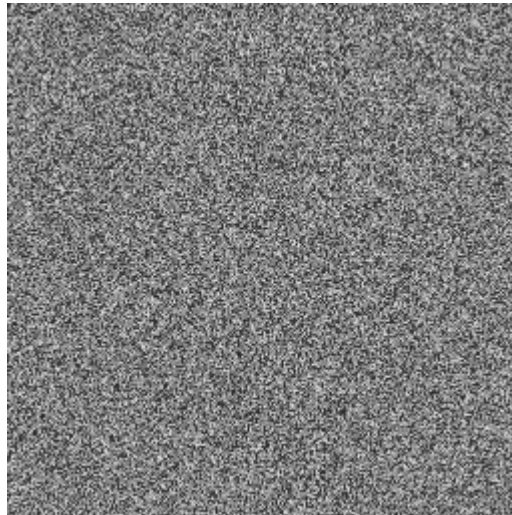
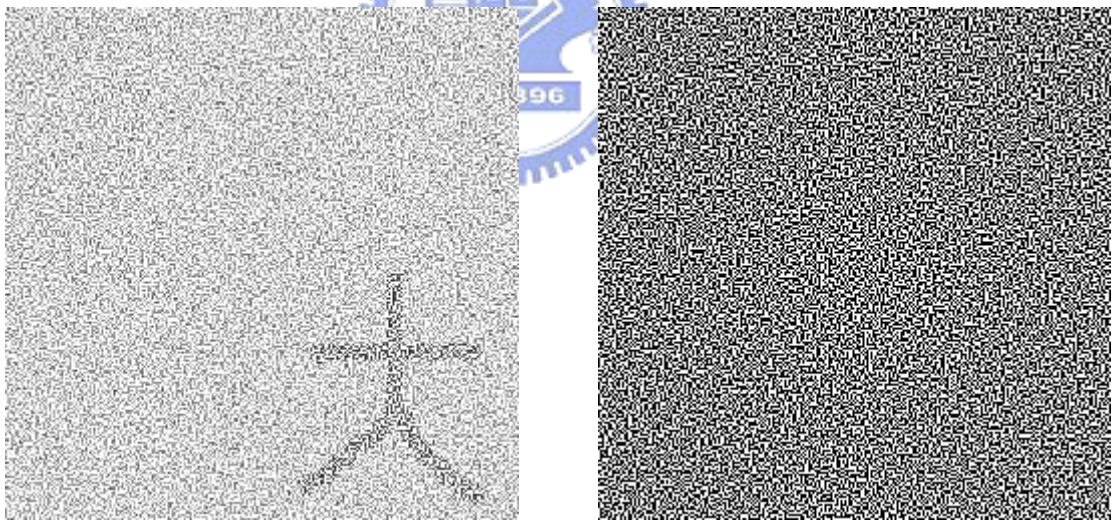


Fig.3-22 Public-random image in MGVC2 Model

Step3: Split a Private Watermark into Private Share1 and Private Share2 according to Public-random image, and embed Private Share1 into Public-random image at the same time to generate Public-Private random image.



(a) Private Share1

(b) Private Share2

Fig.3-23 (a) Private Share1 and (b) Private Share2 in MGVC2 Model

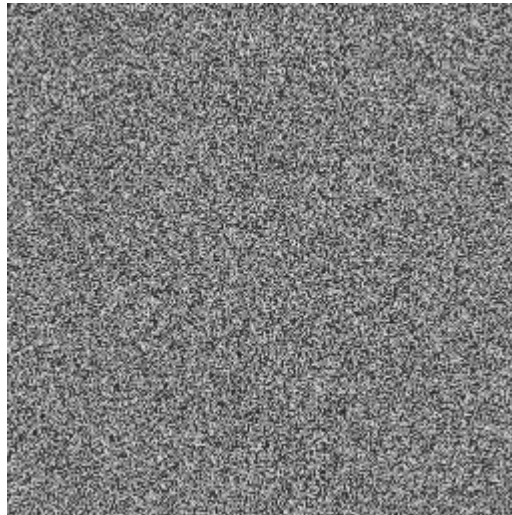


Fig.3-24 Public-Private random image in MGVC2 Model

Step4: Process Public-Private random image re-randomly by using a re-random function γ^{-1} to return to Public-Private Stego-image in Fig.3-25 (b), So far, this system has finished.



(a) Original image

(b) Public-Private Stego-image

Fig.3-25 Compare (a) Original image with (b) Public-Private Stego-image in MGVC2 Model, and PSNR= 32.33

By Fig 3-25 (a) and (b) above, we obviously find that the quality of a result image (Public-Private Stego-image) in this embedding Public and Private Watermark system is acceptable by human visual system and PSNR also above 30, hence, about the clarity of result

image, MGVC2 Model is suitable to the third Gray Visual Cryptography Model [28] for PPKA Watermarking Scheme.

Finally, we experiment on Public and Private Watermark Authentication mechanism.

1. Public Watermark Authentication mechanism:

Step1: embed the Public Share2 into Public-Private Stego-image, finally extract Public Watermark in Fig.3-26 (b)

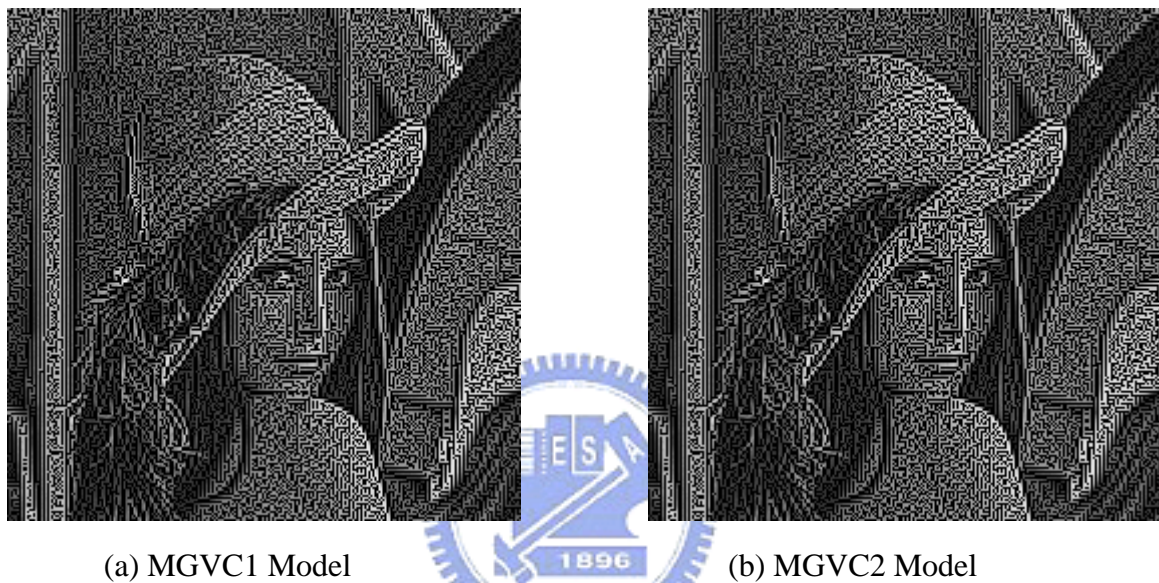


Fig.3-26 Compare the visibility of the extracted Public Watermark (a) MGVC1 Model with (b) MGVC2 Model

2. Private Watermark Authentication mechanism:

Step1: Process Public-Private Stego-image randomly by a random function γ to generate a Public-Private random Stego-image.

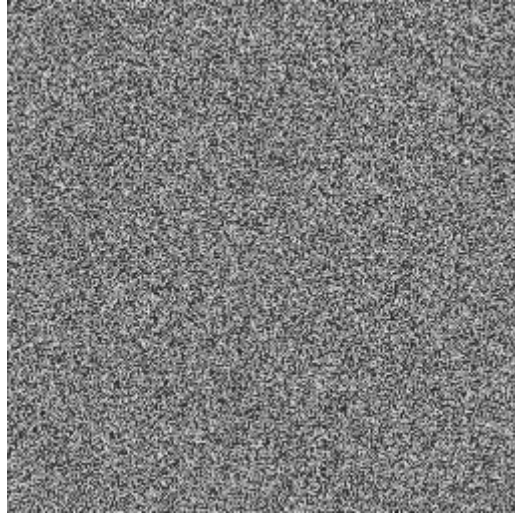
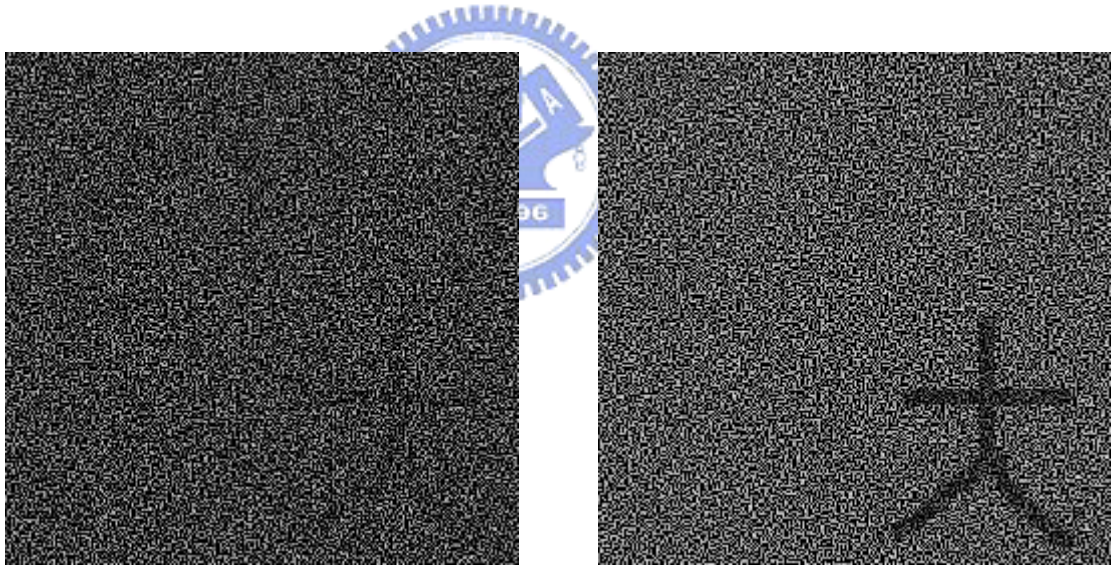


Fig.3-27 Public-Private random Stego-image in MGVC2 Model

Step2: Embed Private Share2 into Public-Private random Stego-image, finally extract Private Watermark in Fig.3-28 (b).



(a) MGVC1 Model

(b) MGVC2 Model

Fig.3-28 Compare the visibility of the extracted Private Watermark (a) MGVC1 Model with (b) MGVC2 Model

By Fig.3-25, Fig.3-26 and Fig.3-28 above, aimed at three disadvantages of MGVC1 Model (see in section 3.2.1), we address MGVC2 Model to compare with it as follows.

1. The PSNR of a result image in MGVC2 Model is 32.33 (greater than 30), i.e. the quality of a result image is acceptable by human visual system.

2. The clarity of the extracted Public Watermark in MGVC2 Model is as similar as that of MGVC1 Model (very blur), so MGVC2 Model is not ideal for copyright authentication.
3. The visibility of the extracted Private Watermark in MGVC2 Model obviously improve a lot, hence, MGVC2 Model is very distinguishable to recognize by human visual system.

In conclusion, MGVC2 Model already solves two problem of MGVC1 Model, but the clarity of extracted Public Watermark is still not ideal for copyright authentication. In the next section, we will address the Modified PPKA scheme to solve this problem.

3.3 Modified Public Key and Private Key Asymmetric (MPPKA)

Watermarking Scheme

In previous section 3.2.2, we utilize MGVC2 Model to embed Public Watermark and Private Watermark, the extracted Private Watermark obviously is more distinguishable than the extracted Public Watermark, why use the same MGVC2 Model to embed watermark, the clarity of the extracted watermark between them is quite different? After we think carefully, we can find the fact that before embedding the Private Watermark, we need to process the stego-image randomly, lead the extracted Private Watermark become more distinguishable. Base on this principle, we try to modify PPKA Scheme to optimize the clarity of the extracted Public Watermark. We call it Modified PPKA Watermark Scheme, abbreviated to MPPKA Watermarking Scheme, and describe it below.

1. Embedding Watermark mechanism

First, we process the cover-image randomly by using a random function γ to generate random-cover image, then split Public Watermark into Public Share1 and Public Share2 by utilizing MGVC2 Model.

Next, we embed Public Share1 into random-cover image to generate the Public-random image, and process the Public-random image re-randomly by using a re-random function γ^{-1} to generate the Public-Cover image. So far, we have embedded the Public Watermark into

cover-image. The rest processes of this MPPKA Watermarking Scheme are the same as those of PPKA Watermarking Scheme.

2. Public Watermark Authentication mechanism

First, we process the result image randomly by using a random function γ to create random-result image, then embed the Public Share2 into random-result image to extract the Public Watermark.

3. Private Watermark Authentication mechanism is the same as PPKA Watermarking Scheme.

Next, we experiment on MPPKA Watermarking Scheme as follows.

1. Embedding Watermark mechanism

First, the process of embedding Public Watermark as follows.

Step1: Randomize the cover image by using a random function γ to create random-cover image as follows.



Fig.3-29 Random-cover image in MPPKA Watermarking Scheme

Step2: Split the Public Watermark into Public Share1 and Public Share2 according to random-cover image, and embed Public Share1 into random-cover image to generate Public-random image as follows.

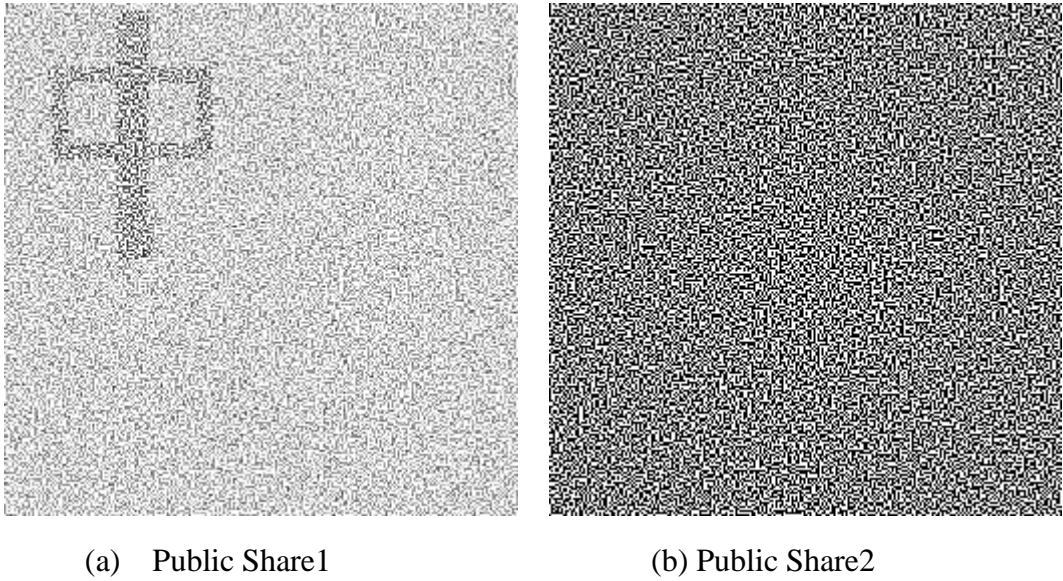


Fig.3-30 Split a Public Watermark into (a) Public Share1 and (b) Public Share2 according to Random-original image (Fig.3-29) in MPPKA Watermarking Scheme

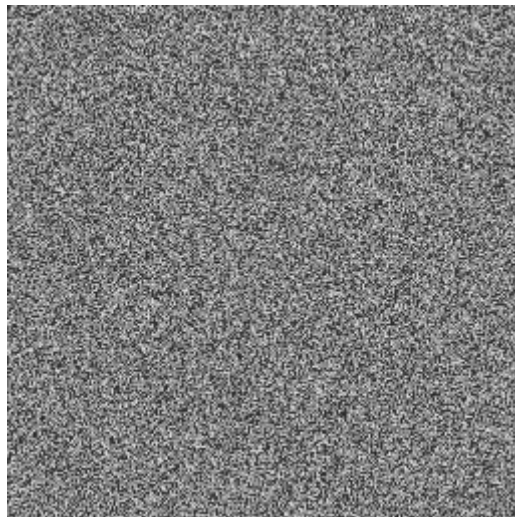


Fig.3-31 Public-random image in MPPKA Watermarking Scheme

Step3: Re-randomize Public-random image by using a re-random function γ^{-1} to generate Public-Cover image as follows.



Fig.3-32 Public-Cover image in MPPKA Watermarking Scheme and PSNR= 35.808

Next, the process of embedding Private Watermark as follows.

Step1: Randomize Public-Cover image by using a random function γ to generate Private-random image as follows.

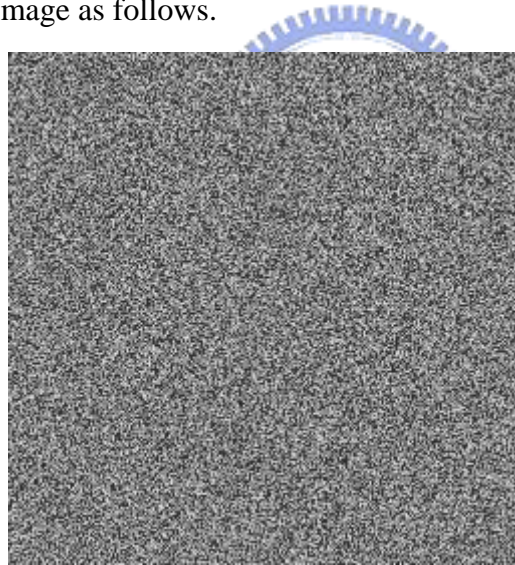


Fig.3-33 Private-random image in MPPKA Watermarking Scheme

Step2: Split the Private Watermark into Private Share1 and Private Share2 according to Private-random image, and embed Private Share1 into Private-random image to create Public-Private random image as follows.

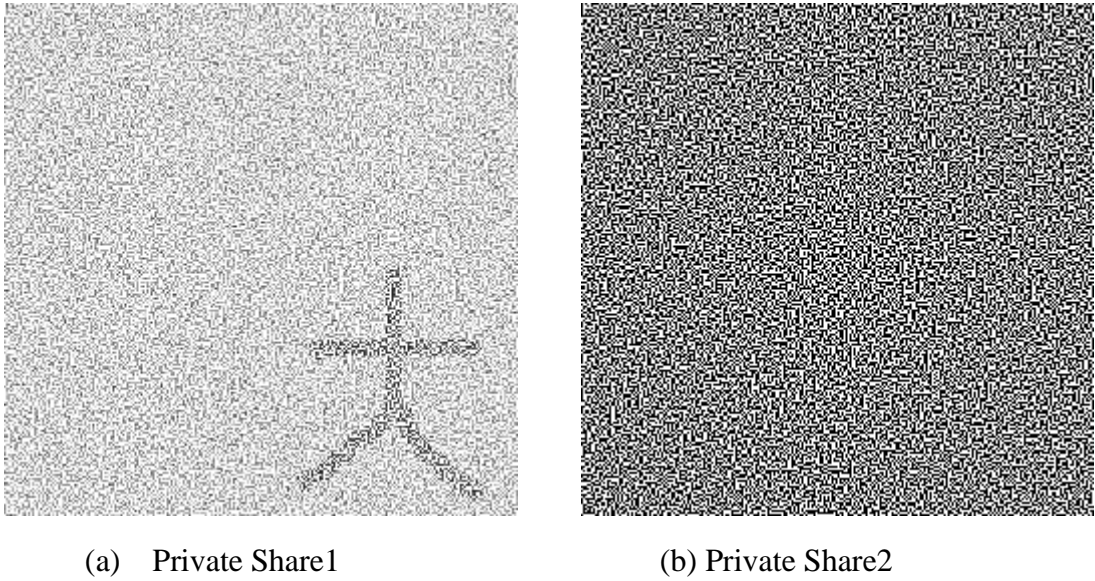


Fig.3-34 Split a Private Watermark into (a) Private Share1 and (b) Private Share2 according to Private-random image (Fig.3-23) in MPPKA Watermarking Scheme.

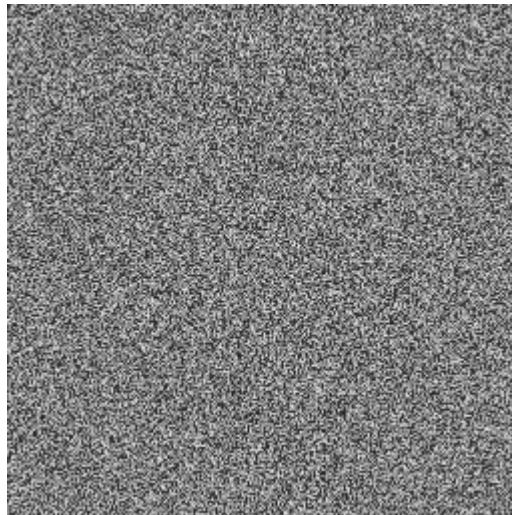


Fig.3-35 Public-Private random image in MPPKA Watermarking Scheme

Step3: Re-randomize Public-Private random image by using a re-random function γ^{-1} generate Public-Private Stego-image.



Fig.3-36 Public-Private Stego-image in MPPKA Watermarking Scheme and PSNR= 29.86

2. Public Watermark Authentication mechanism

Step1: Process the Public-Private Stego-image randomly by a random function γ to create a Random Public-Private Stego-image as follows.

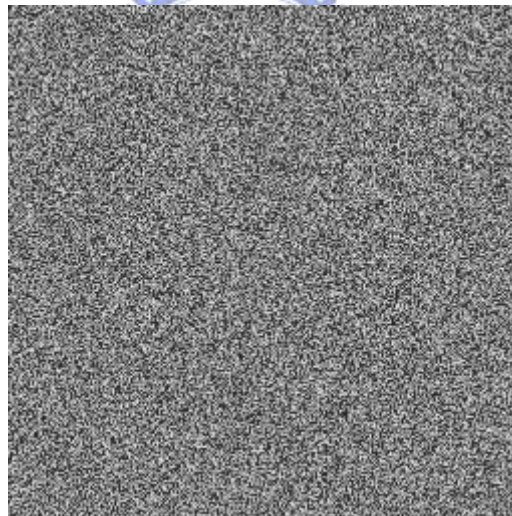


Fig.3-37 Random Public-Private Stego-image in MPPKA Watermarking Scheme

Step2: Embed Public Share2 into Random Public-Private Stego-image to extract Private Watermark in Fig.3-38.

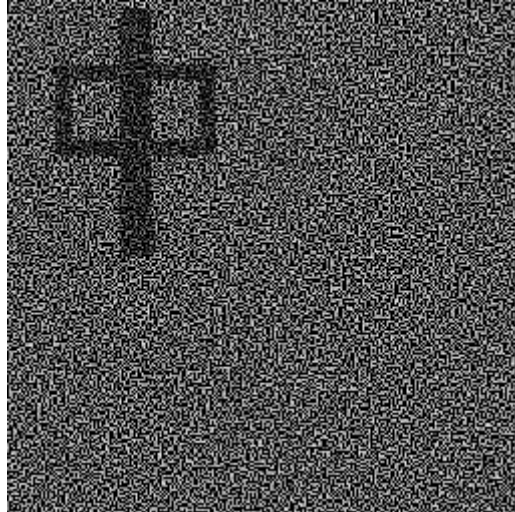


Fig.3-38 Extracted Public Watermark in MPPKA Watermark Scheme

3. Private Watermark Authentication mechanism

Step1: Process the Public-Private Stego-image randomly by a random function γ to create the Public-Private random Stego-image as follows.

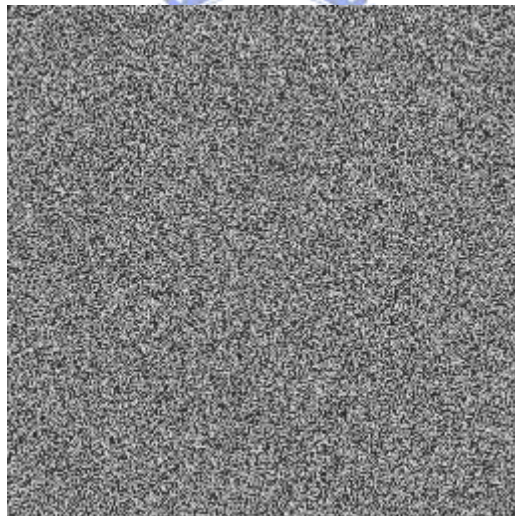


Fig.3-39 Public-Private random Stego-image in MPPKA Watermarking Scheme

Step2: Embed Private Share2 into Public-Private random Stego-image to extract the Private Watermark in Fig.3-40.

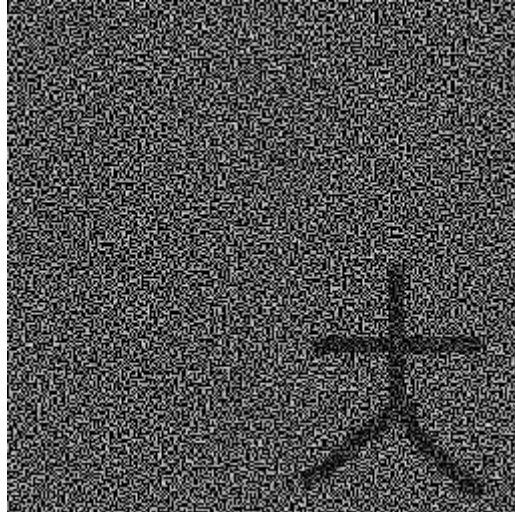


Fig.3-40 Extracted Private Watermark in MPPKA Watermarking Scheme

By Fig.3-36, Fig.3-38 and Fig.3-40 above, aimed at three problems of MGVC1 Model (section 3.2.1), we address MPPKA Watermarking Scheme to compare with PPKA Watermarking Scheme as follows.

1. The PSNR of the result image in MPPKA Watermark Scheme is 29.86 (under 30 a little), i.e. the quality of the result image is just passable by human visual system.
2. The clarity of extracted Public Watermark in MPPKA Watermark Scheme obviously improves a lot, so MPPKA Watermark Scheme suits for copyright authentication (Fig.3-38).
3. The visibility of extracted Private Watermark in MPPKA Watermark Scheme is the same as that in PPKA Watermark Scheme. It is easy to recognize by human visual system.

In conclusion, we adopt MGVC2 Model to experiment on MPPKA Watermark Scheme, seem to solve some problems (section 3.2.1), but the PSNR of the result image is not very ideal (under 30 a little), in the next section, we will address another scheme to optimize MPPKA Watermark Scheme, i.e. increase the PSNR of the result image, etc.

3.4 Optimum Public Key and Private Key Asymmetric (OPPKA) Watermarking Scheme

In this section, in order to optimize MPPKA Watermarking Scheme (section 3.3), we

address another scheme, called the Optimum Public Key and Private Key Watermark Scheme, abbreviated to OPPKA Watermark Scheme, which is described as follows.

The skeleton of this scheme is similar to MPPKA Watermarking Scheme, only difference is in the Embedding Watermark mechanism, and we describe it as follows.

The first phase is Embedding Public Watermark mechanism. First, we randomize the cover image by using a random function γ to create random-cover image, then split Public Watermark into Public Share1 and Public Share2 as follows.

Algorithm: Splitting Public Watermark

Input: a $2^{n-1} \times 2^{n-1}$ bi-level Public Watermark, and a $2^n \times 2^n$ gray-level random-cover image

Output: Public Share1 and Public Share2, each has the size of $2^n \times 2^n$

Step1: We use the random-cover image as our Public Share1.

Step2: Perform Step3 until Public Share2 is created.

Step3: If the pixel of the Public Watermark is white, then we embed white color into two subpixels in Public Share2 which corresponds to the two whitest subpixels in Public Share1 and embed black color into the other subpixels in Public Share2. If the pixel of the Public Watermark is black, then we embed white color into two subpixels in Public Share2 which corresponds to the two blackest subpixels in Public Share1 and embed black color into the other subpixels in Public Share2.

Next, we directly re-randomize the Public-random image by using a re-random function γ^{-1} to generate the Public-Cover image because Public Share1 is equivalent to Public-random image. So far, embedding Public Watermark mechanism has finished. It is worthy of our notice that the Public-Cover image is equivalent to the cover image. That is to say, the quality of the stego-image is the same as the cover image after embedding the Public Watermark into the cover image.

Embedding Private Watermark mechanism is the same as that of Embedding Public Watermark mechanism. Hence, the result image is equivalent to the cover image.

Next, we experiment on MPPKA Watermarking Scheme as follows.

1. Embedding Watermark mechanism

First, the process of embedding Public Watermark as follows:

Step1: Randomize the cover image by using a random function γ to create random-cover image as follows.

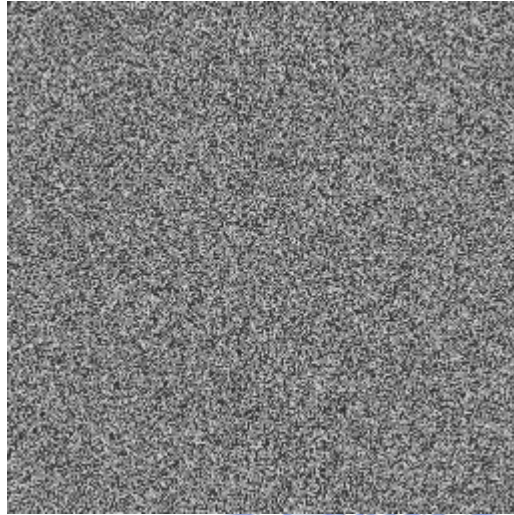
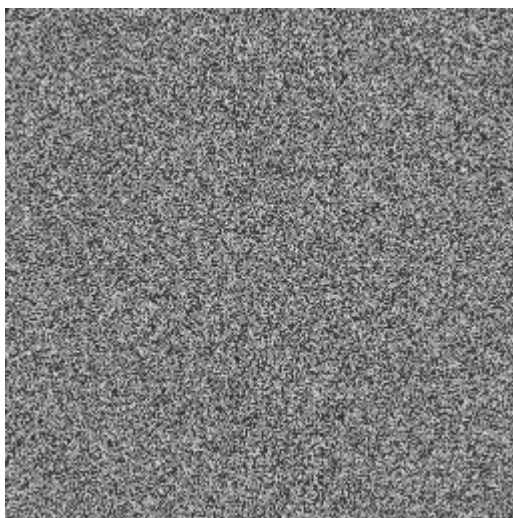
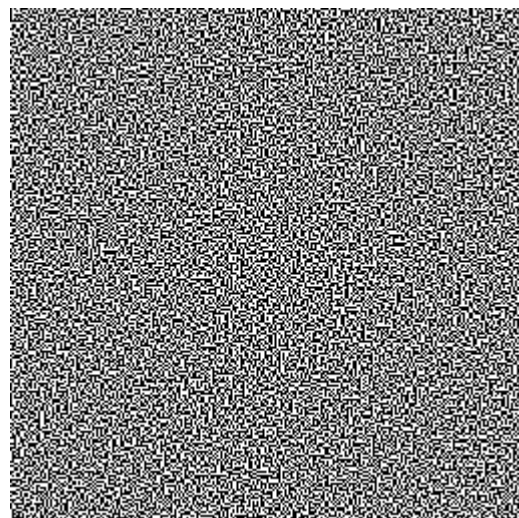


Fig.3-41 Random-cover image in OPPKA Watermarking Scheme

Step2: Split the Public Watermark into Public Share1 and Public Share2 according to random-cover image, and embedding Public Share1 into random-cover image to generate Public-random image, which is equivalent to random-cover image, because we use the random-cover image as Public Share1, as follows.



(a) Public Share1 (random-cover image)



(b) Public Share2

Fig.3-42 Split the Public Watermark into (a) Public Share1 (random-cover image) and (b) Public Share2 in OPPKA Watermarking Scheme.

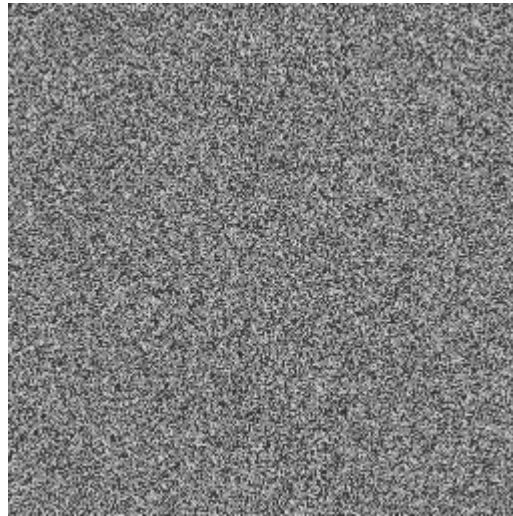


Fig.3- 43 Public-random image (random-cover image) in OPPKA Watermarking Scheme

Step3: Re-randomize Public-random image by using a re-random function γ^{-1} to generate Public-Cover image which is equivalent to the cover image below.

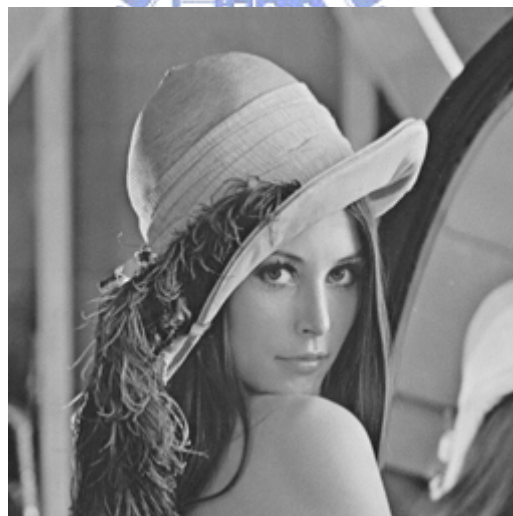


Fig.3-44 Public-Cover image (cover image) in OPPKA Watermarking Scheme

Next, the process of embedding Private Watermark as follows.

Step1: Randomize Public-Cover image by using a random function γ to create Private-random image as follows.

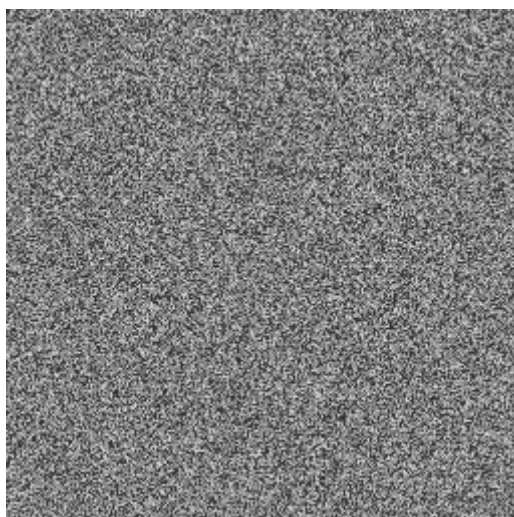
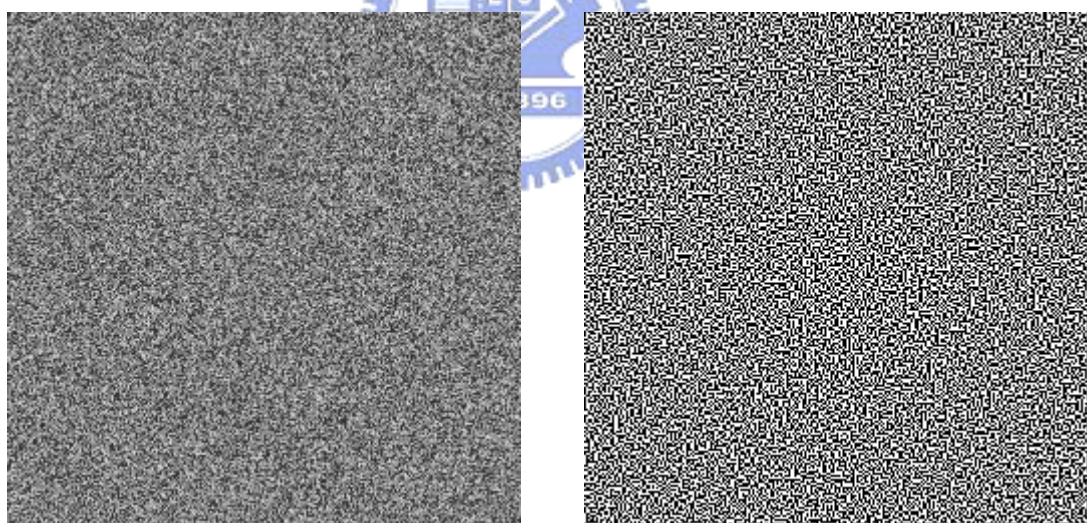


Fig.3-45 Private- random image in OPPKA Watermarking Scheme

Step2: Split the Private Watermark into Private Share1 and Private Share2 according to Private-random image, and embed Private Share1 into Private-random image to generate Public-Private random image which is equivalent to Private-random image, because we use the Private-random image as Private Share1 as follows.



(a) Private Share1 (Private-random image)

(b) Private Share2

Fig.3-46 Split the Public Watermark into (a) Private Share1 (Private-random image) and (b) Private Share2 in OPPKA Watermarking Scheme.

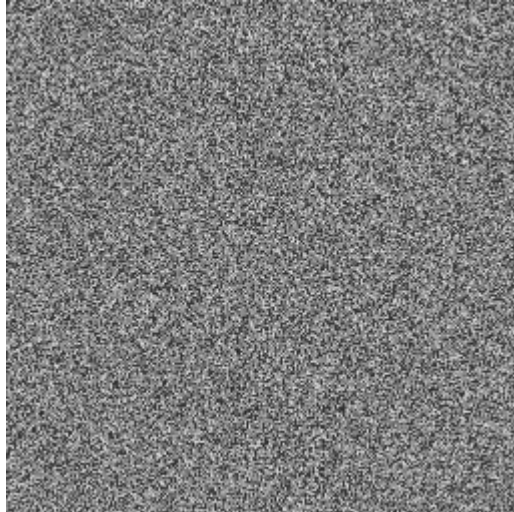


Fig.3-47 Public-Private random image (Private-random image) in OPPKA Watermarking Scheme

Step3: Re-randomize Public-Private random image by using a re-random function γ^{-1} to create Public-Private Stego-image which is equivalent to cover image below.

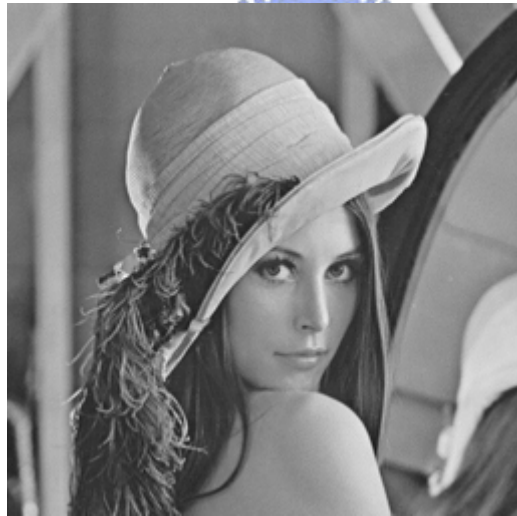


Fig.3-48 Public-Private Stego-image (cover image) in OPPKA Watermarking Scheme

2. Public Watermark Authentication mechanism

Step1: Process the Public-Private Stego-image randomly by a random function γ to create the Random Public-Private Stego-image as follows.

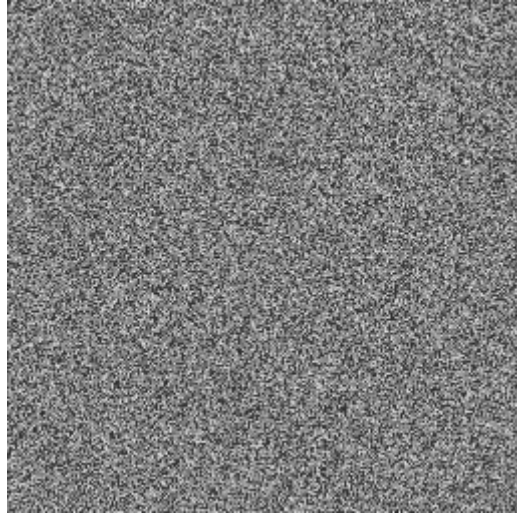


Fig.3-49 Random Public-Private Stego-image in OPPKA Watermarking Scheme

Step2: Embed Public Share2 into Random Public-Private Stego-image to extract the Private Watermark in Fig.3-50.

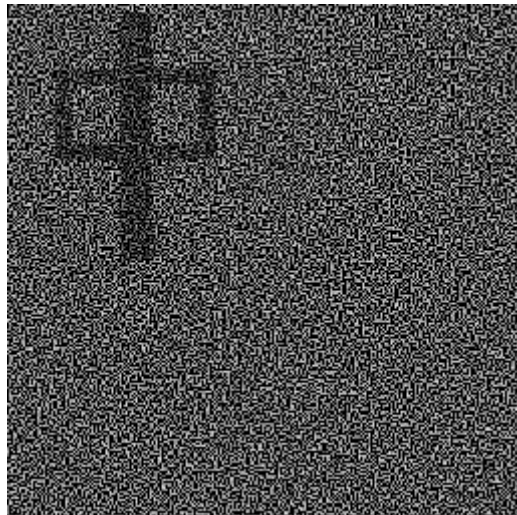


Fig.3-50 Extracted Public Watermark in OPPKA Watermark Scheme

3. Private Watermark Authentication mechanism

Step1: Process the Public-Private Stego-image randomly by a random function γ to create the Public-Private random Stego-image as follows.

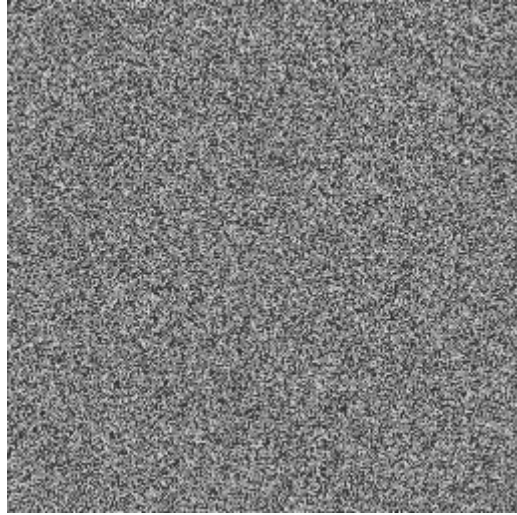


Fig.3-51 Public-Private random Stego-image in OPPKA Watermarking Scheme

Step2: Embed Private Share2 into Public-Private random Stego-image to extract the Private Watermark in Fig.3-52.

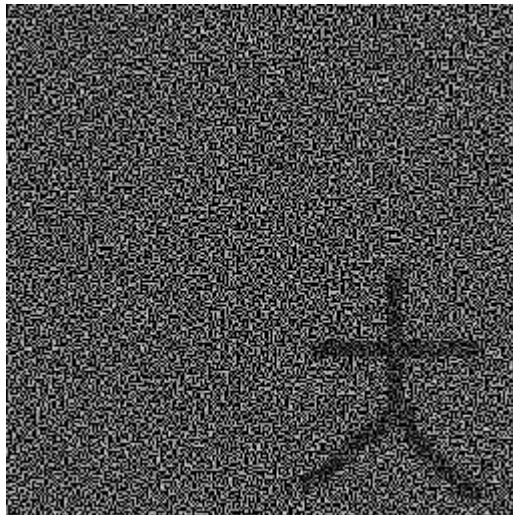


Fig.3-52 Extracted Private Watermark in OPPKA Watermarking Scheme

By Fig.3-48, Fig.3-50 and Fig.3-52 above, aimed at three problems of MGVC1 Model (section 3.2.1), we address OPPKA Watermarking Scheme to compare with MPPKA Watermarking Scheme as follows.

1. The result image is equivalent to the cover image (Fig.3-48), so the quality of the result image is optimum, and we have improved the problem that the PSNR of MPPKA Watermarking Scheme is not very ideal by human visual system.
2. The clarity of extracted Public Watermark (Fig.3-50) and extracted Private Watermark in

OPPKA Watermarking Scheme (Fig.3-52) are the same as those by MPPKA Watermarking Scheme (Fig.3-38 and Fig.3-40). Obviously it is easy to recognize by human visual system.

By Fig.3-46 and Fig.3-48 above, we conclude that the quality of the result image (Public-Private Stego-image) in OPPKA Watermarking Scheme is better than MPPKA Watermarking Scheme. Hence, in the next section, we will discuss the difference between them (PPKA, MPPKA, and OPPKA Watermarking Scheme).

3.5 Schemes Comparison and Discussion

In this section, we will compare these PPKA, MPPKA, and OPPKA Watermarking schemes in following criterions in Table.3-5, and discuss them below.

Scheme (Model) Criterion	PPKA		MPPKA	OPPKA
	MGVC1	MGVC2	MGVC2	
Refer to cover image	No	Yes	Yes	Yes
Leave clue of extracted Public Watermark in Public Share1	No	Tiny	No	No
Leave clue of extracted Private Watermark in Private Share1	No	Tiny	No	No
Leave clue of extracted Public Watermark in Public Share2	No	Tiny	No	No
Leave clue of extracted Private Watermark in Private Share2	No	No	No	No
PSNR of the result image	28.315	32.325	29.86	optimum
Visibility of extracted Public Watermark	Worse	Worse	Good	Good
Visibility of extracted Private Watermark	Worse	Good	Good	Good

Table.3-5 Comparisons in PPKA, MPPKA, and OPPKA Watermarking schemes

In this chapter, we try to experiment on above schemes step by step. Finally, we address the OPPKA Watermarking scheme, which has the best quality of the result image, and the extracted watermarks are very clarity by human visual system obviously. In the next chapter, various attacks will experiment on this OPPKA Watermarking Scheme to test its robustness.

CHAPTER 4

Experimental Results and Discussion

In section 4.1, we will utilize some image processing to simulate various attacks on the OPPKA Watermarking Scheme to improve its robustness. Then we will discuss various attacks experimental results in section 4.2.

4.1 Attack Experiments

This thesis utilizes PhotoImpact 10.0 as image processing tool. We adopt the OPPKA Watermarking Scheme as the attacked target to maintain optimum visibility. The following is the illustration aimed at various attacks.

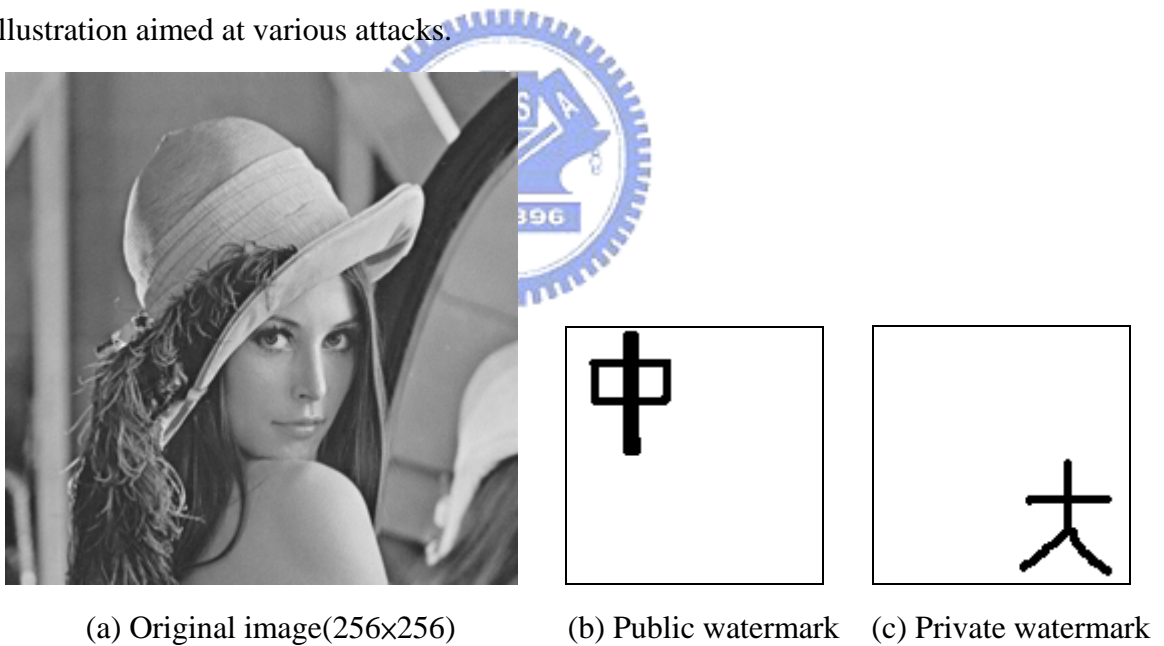
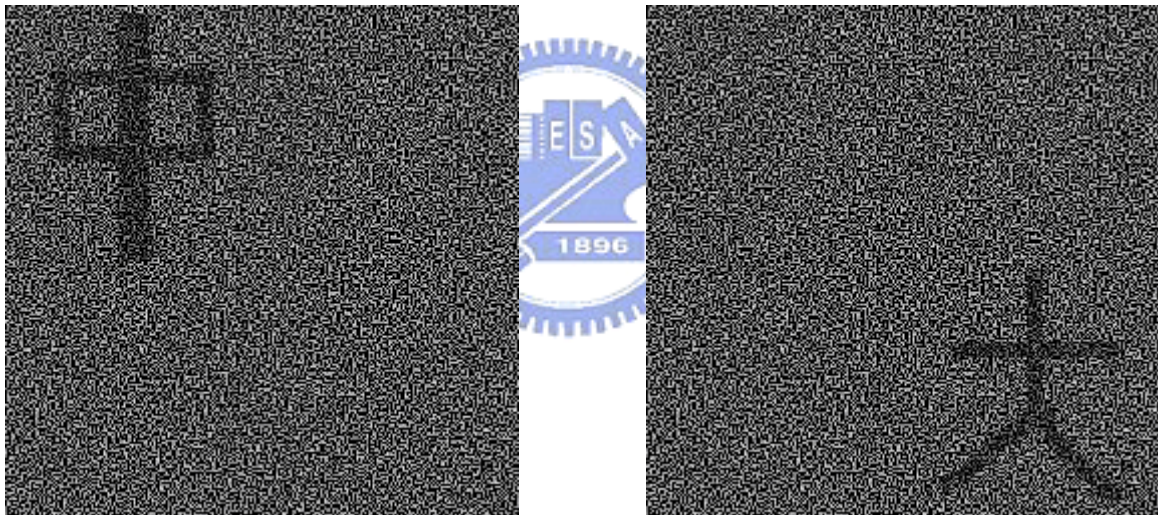


Fig.4-1 (a) input image, (b) Public Watermark, and (c) Private Watermark (128x128)

1. JPEG compression attack: Compression rate sets to 80%



(a) Public-Private Stego- image



(b) Extracted Public Watermark

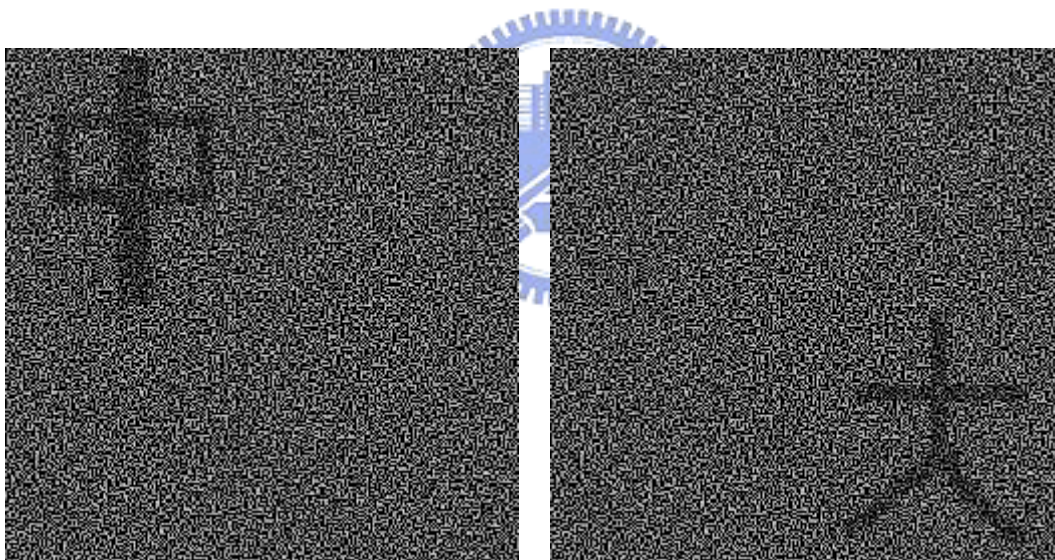
(c) Extracted Private Watermark

Fig.4-2 JPEG compression Attack : Compression rate sets to 80%

2. Distortion attack: Ruling distortion



(a) Public-Private Stego- image



(b) Extracted Public Watermark

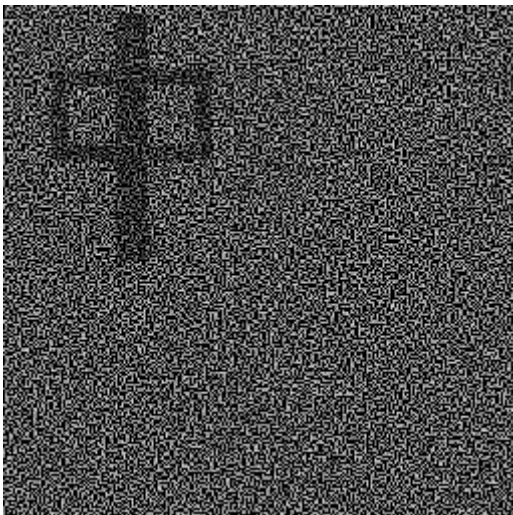
(c) Extracted Private Watermark

Fig.4-3 Distortion Attack : Ruling distortion

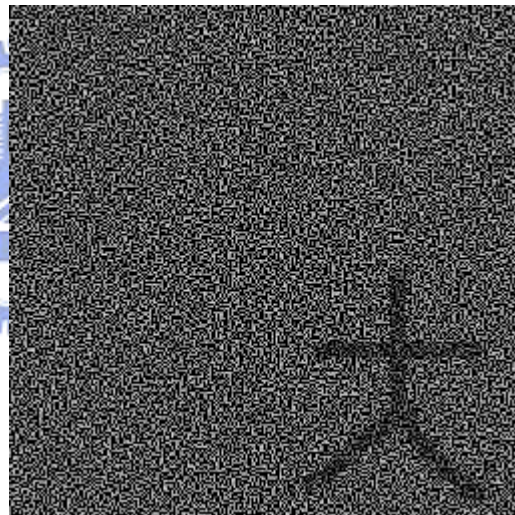
3. Mosaic attack: X axis sets to 3, Y axis sets to 3



(a) Public-Private Stego- image



(b) Extracted Public Watermark



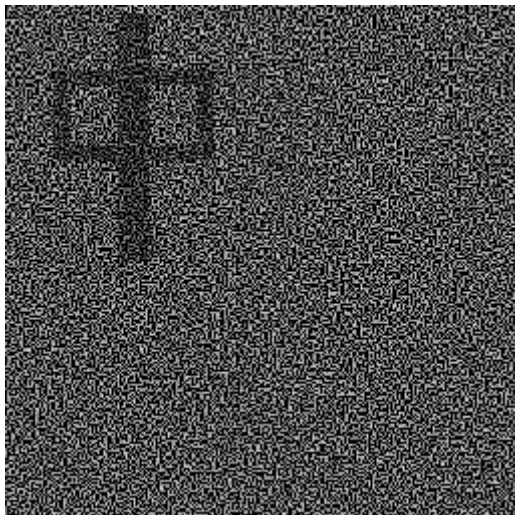
(c) Extracted Private Watermark

Fig.4-4 Mosaic Attack : X axis sets to 3, Y axis sets to 3

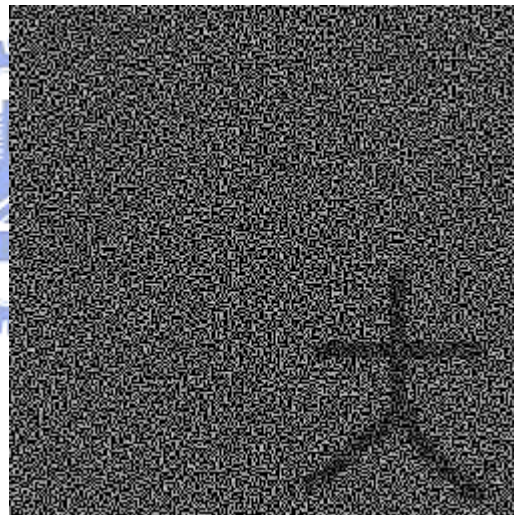
4. Blur attack: Degree sets to strong



(a) Public-Private Stego- image



(b) Extracted Public Watermark



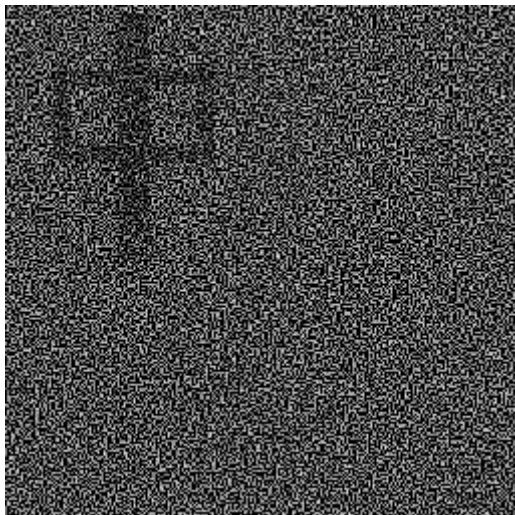
(c) Extracted Private Watermark

Fig.4-5 Blur Attack : Degree sets to strong

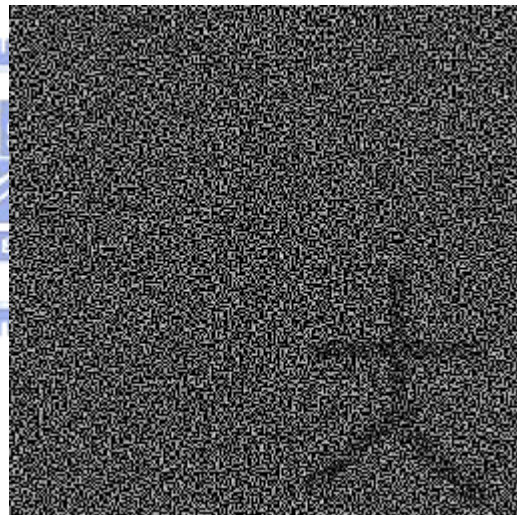
5. Jitter attack: Move upward sets to eight pixels



(a) Public-Private Stego- image



(b) Extracted Public Watermark



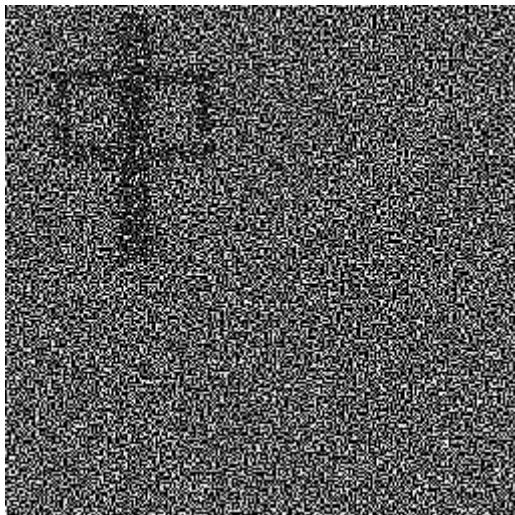
(c) Extracted Private Watermark

Fig.4-6 Jitter Attack: Move upward sets to eight pixels

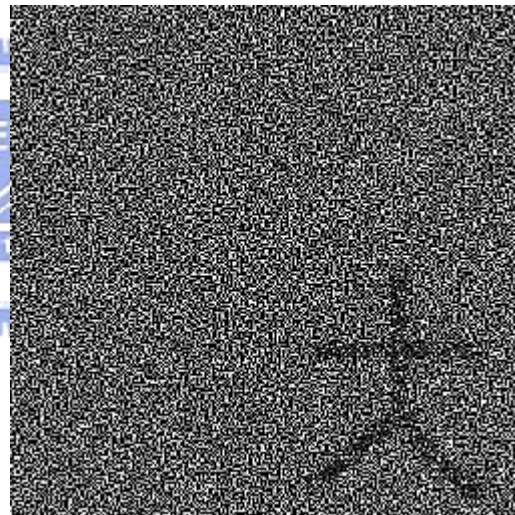
6. Cut1 attack: Cut right-down parts of Stego-image



(a) Public-Private Stego- image



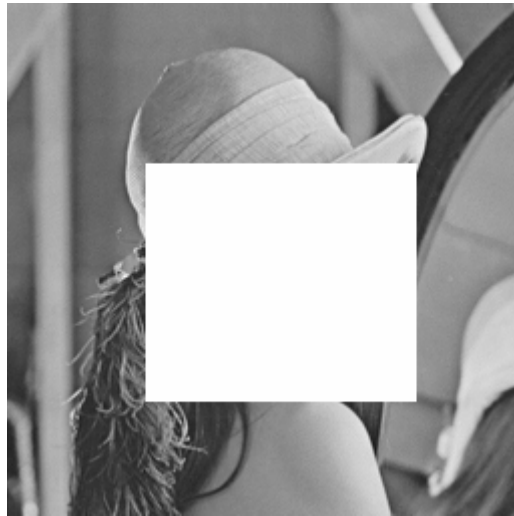
(b) Extracted Public Watermark



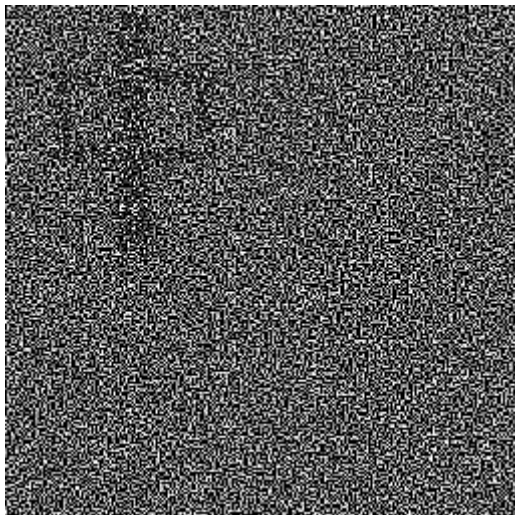
(c) Extracted Private Watermark

Fig.4-7 Cut1 Attack: Cut right-down parts of Stego-image

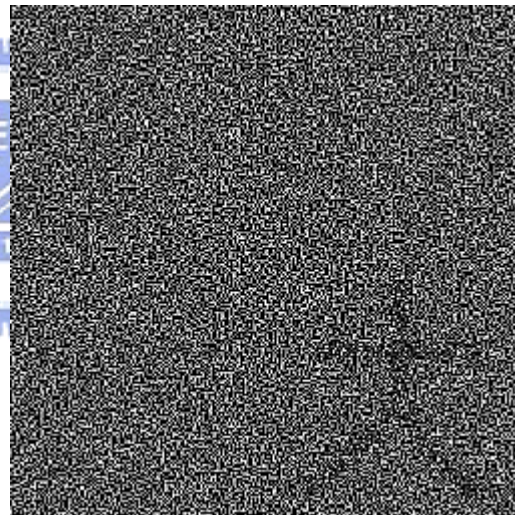
7. Cut2 attack: Cut the important parts of Stego-image



(a) Public-Private Stego- image



(b) Extracted Public Watermark



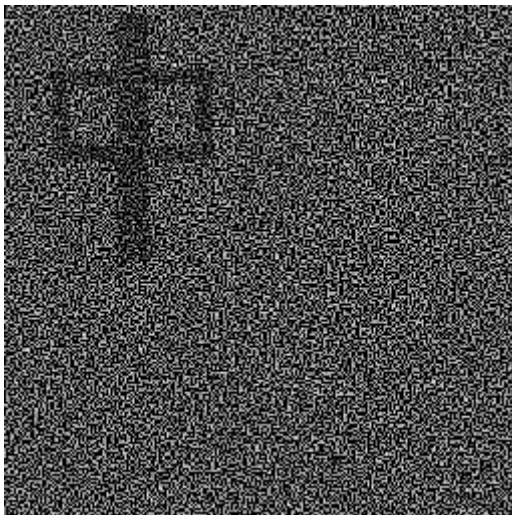
(c) Extracted Private Watermark

Fig.4-8 Cut2 Attack: Cut the important parts of Stego-image

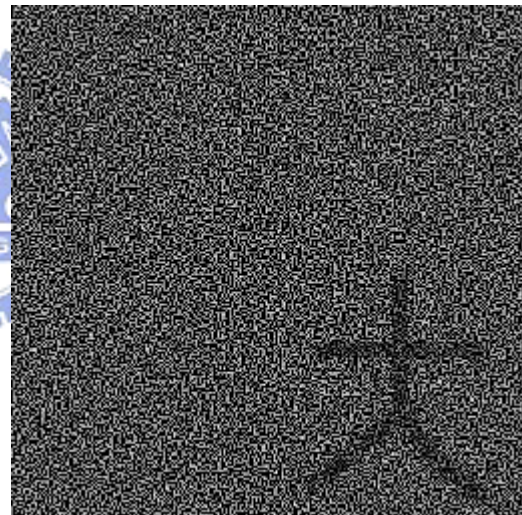
8. Clarity attack: Degree sets to 8



(a) Public-Private Stego- image



(b) Extracted Public Watermark



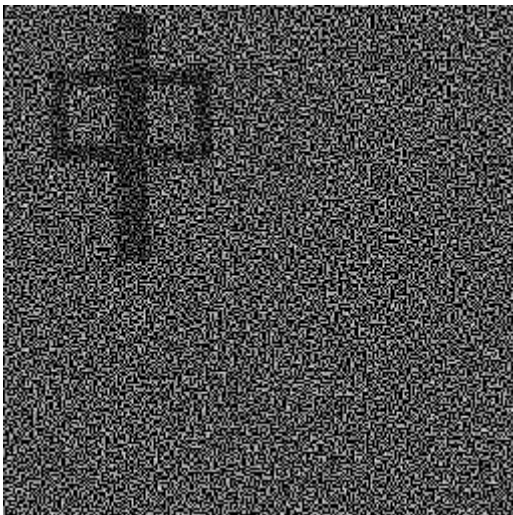
(c) Extracted Private Watermark

Fig.4-9 Clarity Attack: Degree sets to 8

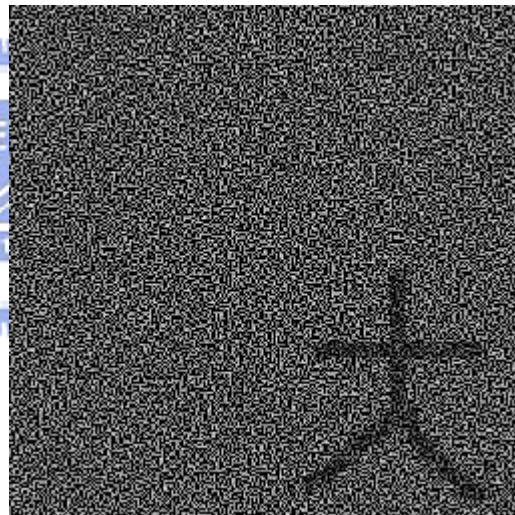
9. Noise attack: Variances set to 10.



(a) Public-Private Stego- image



(b) Extracted Public Watermark



(c) Extracted Private Watermark

Fig.4-10 Noise Attack: Variances set to 10

4.2 Results Discussion

In previous section 4.1, we observe that when OPPKA Watermarking Scheme is subjected to various attacks, the visibility of the extracted watermark still very clear besides cut attacks. Because cut attacks may remove some hidden information, this will make the clarity of the extracted watermark degrade a little. However, it is still recognizable by human visual system. Hence, by above attack experiment results, we conclude that the OPPKA Watermarking Scheme has strong resistance against various attacks, that is to say, it regards as a robust watermarking scheme.



CHAPTER 5

Conclusions and Future Works

5.1 Conclusions

In this thesis, at first, we address the PPKA Watermarking Scheme, and utilize two kinds of the Modified Gray Visual Cryptography to experiment on this scheme respectively. By experimental results, we find that the extracted of Public Watermark is difficult to recognize by human visual system. Hence, we try to modify the PPKA Watermarking Scheme, and then address the MPPKA Watermarking Scheme to solve this problem. Although the MPPKA Watermarking Scheme obviously improves a lot on the above problem, the PSNR of the result stego-image is not very ideal for human visual system. Finally, we address the OPPKA Watermarking Scheme to optimize the above scheme. By a series of attack experiments on the OPPKA Watermarking Scheme, we conclude that the OPPKA Watermarking Scheme is also a robust Watermarking Scheme.

In the next section, we will further discuss the applications of OPPKA Watermarking Scheme. Then we try to improve its function and more efficient in the future research.

5.2 Future works

Future works can be directed to the following topics. First, we will improve our scheme to apply the full-color image, not only gray-level image, because a lot of full-color images are now in widespread use. Second, we will enhance the capacity and universal in this scheme, in order to make its application more extensive. Third, we hope this scheme can combine other watermarking techniques to increase its function more complete and more efficient. Finally, how to make this scheme more robust is also our research target in the future.

References

- [1] Teddy Furon and Pierre Duhamel, "Robustness of asymmetric watermarking technique" in *Image Processing*, 2000. Proceedings. 2000 International Conference on.
- [2] Teddy Furon and Pierre Duhamel, "An Asymmetric Watermarking Method" in *IEEE Transactions on Signal Processing*, vol. 51, no. 4, April 2003.
- [3] Joachim J. Eggers¹, Jonathan K. Su¹, and Bernd Girod², "Asymmetric watermarking schemes" in Sicherheit in Mediendaten Berlin, Germany, Sep. 19, 2000.
- [4] Tae Young Kim, Hyuk Choi, Kiryung Lee, and Taejeong Kim, "An asymmetric watermarking system with many embedding watermarks corresponding to one detection watermark" in *IEEE Signal Processing Letters*, vol. 11, no. 3, March 2004.
- [5] Y.C. Hou, and P.M. Chen (2000), "An Asymmetric Watermarking Scheme based on Visual Cryptography", *Signal Processing Proceedings*, 2000. WCCC-ICSP 2000. 5th International Conference, 2, 992–995.
- [6] Yanjun Hu, Li Gao, Xiaoping Ma and Zhigeng Pan, Li Li, "A Public-key Asymmetric Robust Watermarking Algorithm Based on Signal" in WSCG POSTERS *proceedings WSCG'2004, February 2-6, 2004*, Plzen, Czech Republic. Copyright UNION Agency – Science Press.
- [7] Naor, M. and Shamir, A., "Visual Cryptography", *Advances in Cryptography, Advances in Cryptology: Eurocrypt'94*, Springer-Verlag, Berlin, 1995, pp 1-12.
- [8] Anderson, Rose(Ed.), *Information Hiding*, Lecture Notes in Computer Science 1174, (Proceedings of First International Workshop on Information Hiding, Cambridge, U.K.)Spring-Verlag, 1996.
- [9] Bender, W, Gruhl, D., Morimoto, N., and Lu, A., Techniques for data hiding, IBM System Journal, Vol. 35, No. 3&4, pp.313-336, 1996.
- [10] Memon, Nasir and Wong, P. W., Protecting Digital Media Content, Comum, of ACM,

Vol 41, No 7, pp.35-43, July 1998.

[11] Popa, Richard, An Analysis of Stegonographic Techniques, *Master Thesis of Det. Of CS&SE, Facult of automatics and Computers, The Politehnica University of Timisoara*, 1998.

[12] United State Code, Tittle 17.

[13] D. Kesdogan, J. Ebner, and R. Buschks. "Stop-and Go MIXes Providing Probabilistic Anonymity in an Open System," in *Proceedings of the Second International Information Hiding Workshop*, pp.83-98, 1998.

[14] I. S. Moskowitz and L. W. Chang. "An Entropy-based Framework for Database Inference," in *Proceedings of the Third International Information Hiding Workshop*, pp.405-418, 1999.

[15] F. Hartung and M. Kutter. "Multimedia Watermarking Techniques," *Proceedings of the IEEE*, 87(7):1079-1107, 1999.

[16] I. J. Cox and M. L. Miller. "A Review of Watermarking and the Importance of Perceptual Modeling," in *Proceedings of SPIE, Human Vision & Electronic Imaging II*, volume 3016, pp. 92-99, 1997.

[17] F. A. P. Petitcolas, R. Anderson, and M. G. Kuhn. "Information Hiding: A Survey," *Proceedings of the IEEE*, 87(7):1062-1077, 1999.

[18] R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp. "Perceptual Watermarks for Digital Images and Video," *Proceedings of the IEEE*, 87(7):1108-1126, 1999.

[19] H. S. Stone. *Analysis of Attacks on image Watermarks with Randomized Coefficients*. Technical Report TR 96-045, NEC Research Institute, 1996.

[20] J. Kilian, F. T. Leghton, L. R. Matheson, T. Shamoon, and R. E. Tarjan. *Resistance of Watermarked Documents to Collusional Attacks*. Technical Report TR 97-167, Princeton, NJ: NEC Research Institute, 1997.

[21] F. Ergun, J. Kilian, and R. Kumar. "A Note on the Limits of Collusion-resistant

Watermarks,” in *Advances in Cryptology: EUROCRYPT’99*, pp. 140-149. Berlin; New York: Springer-Verlag,1999.

[22] R.G. van Schyndel, A.Z. Tirkel, and C.F. Osborne (1994), “A Digital Watermark,” *Proc. IEEE Int. Conf. Image Processing*, Austin, TX, Nov, 2, 86-90.

[23] S. Walton (1995), “Image Authentication for a Slippery New Age,” *Dr. Dobb’s Journal*.

[24] M.S. Hwang, C.C. Chang, and K.F. Hwang (1999), “A Watermarking Technique Based on One-Way Hash Function,” *IEEE Transactions on Consumer Electronics*, 45(2), 286-294.

[25] Yuan-Fu Zhao, “Information Hiding Techniques of Research”, Master Thesis of National Central University, June 1999.

[26] Y.C. Hou, C.X. Chen, “Non-Perceptual Watermarking Technique based on Gray Visual Cryptography “, The sixth Information Management and Practice Seminar.

[27] Zhi-lun Zhou, “Watermarking Technique based on the non-extended visual cryptography“, Master Thesis of National Central University, June 2002.

[28] Bo-Cheng Shen, “Watering Technique based on Gray Visual Cryptography”, Master Thesis of National Central University, June 1999.

[29] F. Hartung and B. Girod, “Fast public-key watermarking of compressed video,” in *Proc. IEEE Intl. Conf. Image Processing*, vol. 1, Oct. 1997,pp. 528–531.

[30] J. J. Eggers, J. K. Su, and B. Girod, “Asymmetric watermarking schemes,” in *Tagungsband Des GI Workshops Sicherheit in Mediendaten*, Berlin, Germany, Sept. 2000, pp. 107–123.

[31] Ping Wah Wong, N. Memon, Secret and public key image watermarking schemes for image authentication and ownership verification ,*IEEE Transactions on Image Processing*, vol:10,2001, pp.1593 –1601

[32] F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn, Information Hiding – *A Survey*, *Proc. IEEE* 87(1999), pp.1062-1078

- [33] Vinayak, Dangui, EE368A : Final Project Robust watermarking of digital images,
Availabe:http://ise0.stanford.edu/class/ee368a_proj01/dropbox/project05/presentation.html.
- [34] T.Furon and P. Duhamel “An Asymmetric Public Detection Watermarking Technique”
in *Proc. Of the 3rd Int. Work. On Information Hiding, Dresden*, Sept 1999.
- [35] R.G. van Schyndel, A.Z. Tirkel, and I.D. Svalbe “Key Independent Watermark
Detection” in *ICMCS'99*, Florence, Italy, 1999.
- [36] J. Eggers and B. Girod “Robustness of Public Key Watermarking Scheme”, *VD
Watermarking Workshop*, Erlangen, Germany, Oct 1999.
- [37] B. Chen and G. W. Wornell. Dither modulation: a new approach to digital watermarking
and information embedding. In *Proc. of SPIE Vol. 3657: Security and Watermarking of
Multimedia Contents*, San Jose, January 1999.

