

國立交通大學

資訊科學系

碩士論文

在文件影像中作資訊隱藏之研究



A Study on Information Hiding in Document Images

研究生：翁連奕

指導教授：蔡文祥 教授

中華民國九十四年六月

在文件影像中作資訊影藏之研究
A Study on Information Hiding in Document Images

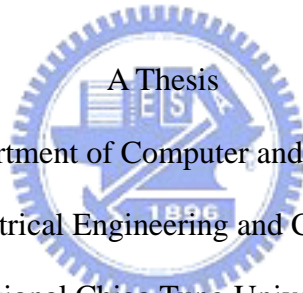
研究生：翁連奕

Student : Lien-Yi Weng

指導教授：蔡文祥

Advisor : Wen-Hsiang Tsai

國立交通大學
資訊科學研究所
碩士論文



Submitted to Department of Computer and Information Science

College of Electrical Engineering and Computer Science

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Master

in

Computer and Information Science

June 2005

Hsinchu, Taiwan, Republic of China

中華民國九十四年六月

在文件影像中做資訊影藏之研究

研究生：翁連奕 指導教授：蔡文祥 博士

國立交通大學資訊科學研究所

摘要

由於數位影像技術的快速發展，數位影像很可能被非法竄改、編輯與複製。因此有必要去發展能保護數位影像的方法。在本論文中，我們針對公文影像提出了數種數位浮水印的技術以達到能夠保護版權並指出影像被竄改之處的目的。針對灰階公文影像，我們利用數位浮水印提出了一種影像驗證的方法，且我們希望即使此影像被列印與掃描後，其驗證資訊還能被準確的抽取出來，同時若影像被破壞後，我們也能指出被破壞的區域。另外我們也提出了一種在公文影像上加入強韌性浮水印的方法，以達到保護版權的目的。針對黑白公文影像，我們提出了一個資訊隱藏的方法，因此可藉由嵌入在影像內的浮水印來保護其版權。最後，我們提出了一套整合性的資訊隱藏的方法來同時藏入浮水印與驗證訊號，其特色為不但可以從影像中抽取出隱藏的資訊，同時若影像遭受到竄改時，我們也可指出影像被竄改之處。相關的實驗結果證明其所提的方法是可行的。

A Study on Information Hiding in Document Images

Student: Lien-Yi Weng

Advisor: Dr. Wen-Hsiang Tsai

Department of Computer and Information Science
National Chiao Tung University

ABSTRACT

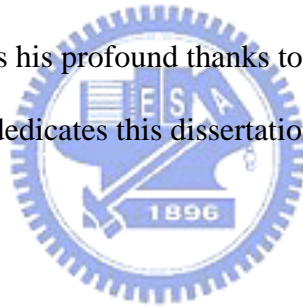
Because of the rapid development of image processing, it often occurs that digital images are duplicated or edited without authorization. As a result, it is desired to develop a scheme to protect the copyright and to verify the integrity of digital images. In this study, we propose several watermarking techniques for digital document images for copyright protection and image authentication. For grayscale document images, a method based on semi-fragile watermarking against print-and-scan operations for image authentication is proposed, which is useful for verifying the fidelity and integrity of document images. Then a method for copyright protection of document images is proposed, which embeds a robust watermark into a document image, based on the use of edge direction histograms with circular interpretation. For color images, a method for image authentication is also proposed. Generation of authentication signals and the positions for embedding them are controlled by two keys. A suspicious image can be verified for tampering proof by comparing the difference between the embedded authentication signals and those generated by the two keys. For binary images, a data hiding method for copyright protection is proposed, which embeds up to three bits in a 4×4 image block by rearranging the black pixels in the pre-selected 2×2 image block in the 4×4 block. A method for integration of watermark and authentication signals is finally proposed. Good experimental results prove the feasibility of the proposed methods.

ACKNOWLEDGEMENTS

The author is in hearty appreciation of the continuous guidance, discussions, support, and encouragement received from his advisor, Dr. Wen-Hsiang Tsai, not only in the development of this thesis, but also in every aspect of his personal growth.

Thanks are due to Mr. Chih-Jen Wu, Mr. Tsung-Yuan Liu, Mr. Shi-Yi Wu, Mr. Ming-Che Chen, Mr. Shi-Chei Hung and Mr. Yuei-Cheng Chuang for their valuable discussions, suggestions, and encouragement. Appreciation is also given to the colleagues of the Computer Vision Laboratory in the Department of Computer and Information Science at National Chiao Tung University for their suggestions and help during his thesis study.

Finally, the author also extends his profound thanks to his family for their lasting love, care, and encouragement. He dedicates this dissertation to his parents.



CONTENTS

ABSTRACT (in Chinese)	i
ABSTRACT (in English)	ii
ACKNOWLEDGEMENTS	iii
CONTENTS	iv
LIST OF FIGURES	vii
LIST OF TABLES	xi
Chapter 1 Introduction	1
1.1 Motivation.....	1
1.2 Review of Related Works.....	2
1.3 Overview of Proposed Methods.....	4
1.3.1 Definitions of Terms	4
1.3.2 Brief Descriptions of Proposed Methods	5
1.4 Contributions.....	10
1.5 Thesis Organization	10
Chapter 2 Integrity Authentication of Grayscale Document Images Surviving Print-And-Scan Attacks	12
2.1 Introduction.....	12
2.1.1 Problem Definition.....	12
2.1.2 Properties of Document Images Attacked by Print-And-Scan Operations	13
2.1.3 Properties of Grayscale Document Images.....	14
2.2 Idea of Proposed Authentication Method	16
2.3 Authentication Signal Generation and Embedding.....	16
2.3.1 Pre-processing Stage	17
2.3.2 Creation and Embedding of Semi-Fragile Authentication Signals by Line Embedding	20
2.3.3 Detailed Algorithm.....	25
2.4 Image Authentication process	26
2.4.1 Extraction of Authentication Signals Using A Line Fitting Technique	26
2.5 Experimental Results	30
2.6 Discussions and Summary	33
Chapter 3 Copyright Protection for Grayscale Document Images Using Edge	

Direction Histograms with Circular Interpretation	35
3.1 Introduction.....	35
3.1.1 Motivation.....	36
3.1.2 Problem Definition.....	36
3.1.3 Definition of Edge Direction Histograms	37
3.1.4 Definition of Circular Interpretation.....	40
3.2 Idea of Watermark Embedding Method.....	40
3.3 Watermark Embedding Process	41
3.3.1 Proposed Technique Using Edge Direction Histograms with Circular Interpretation to Embed Watermarks	41
3.3.2 Detailed Algorithm.....	46
3.4 Watermark Extraction Process	49
3.4.1 Extraction of Watermarks	49
3.4.2 Detailed Algorithm.....	49
3.5 Experimental Results	52
3.6 Discussions and Summary	55
Chapter 4 A Fragile Authentication Method for Color Images	57
4.1 Introduction.....	57
4.2 Proposed Idea of Embedding Authentication Signals.....	58
4.3 Authentication Signal Embedding Process	58
4.3.1 Embedding of Authentication Signals	58
4.3.2 Detailed Algorithm.....	61
4.4 Authentication Signal Extraction Process.....	63
4.4.1 Extraction of Authentication Signals	63
4.4.2 Detailed Algorithm.....	63
4.5 Experimental Results	66
4.6 Discussions and Summary	69
Chapter 5 A Watermarking Method for Copyright Protection of Binary Images	71
5.1 Introduction.....	71
5.1.1 Properties of Binary Images.....	72
5.1.2 Problem Definition.....	72
5.2 A Watermark Embedding Method	72
5.3 Watermark Embedding Process	73
5.3.1 Embedding of Watermarks.....	73
5.3.2 Detailed Algorithm.....	79
5.4 Watermark Extraction Process	81

5.4.1	Extraction of Watermarks	82
5.4.2	Detailed Algorithm.....	82
5.5	Experimental Results	83
5.6	Discussions and Summary	87
Chapter 6	Hiding Digital Information and Authentication Signals behind Binary Images with Reduced Distortion and Enhanced Security	89
6.1	Introduction.....	89
6.1.1	Problem Definitions	90
6.1.2	Review of Employed Techniques	91
6.2	Idea of Integration Method	94
6.3	Watermark and Authentication Signals Embedding Process	95
6.3.1	Embedding of Watermarks and Authentication Signals.....	95
6.3.2	Detailed Algorithm.....	97
6.4	Watermark Extraction Process	99
6.4.1	Extraction of Watermarks and Authentication Signals	99
6.4.2	Detailed Algorithm.....	100
6.5	Experimental Results	103
6.6	Discussions and Summary	106
Chapter 7	Conclusions and Suggestions for Future Works	107
7.1	Conclusions.....	107
7.2	Suggestions for Future Works.....	109
References	110

LIST OF FIGURES

Figure 1.1	Flowchart of proposed method for embedding authentication signals in grayscale document images.	6
Figure 1.2	Flowchart of proposed method for embedding watermark signals in grayscale document images.	7
Figure 1.3	Flowchart of proposed method for embedding authentication signals in color images.	8
Figure 1.4	Flowchart of proposed method for embedding watermark signals in binary document images.	9
Figure 2.1	A grayscale document image and a reproduced image. (a) A grayscale Chinese document image. (b) A grayscale English document image. (c) Reproduced image of (a) with quality of 100dpi. (d) Reproduced image of (b).....	15
Figure 2.2	An example of using region growing technique to get basic blocks. (a) Several Chinese characters. (b) Each character becomes a block (c) Several English characters. (d) Each character becomes a block.	18
Figure 2.3	An example of block merging. (a) A Chinese document image and the total number of blocks is 2. (b) An enlarged image of (a) and the total number of blocks is 4. (c) Block distances of (b). (d) The result image of (b) after block merging. (e) An English document image and the total number of blocks is 12. (f) The result image of (e) after block merging.	19
Figure 2.4	An example of finding the best position to embed a line. (a) A character. (b) and (c) Shifting b to seek the best position to embed the authentication signal. (d) Modifying the gray values of the black pixels in the character.	23
Figure 2.5	An example of embedding a line into a block. (a) A block. (b) The result after embedding a line in (a).	25
Figure 2.6	Flowchart of proposed method for authentication signal embedding in grayscale document images.	27
Figure 2.7	Flowchart of proposed method for image authentication	29
Figure 2.8	Input grayscale document images and output stego-images with authentication signals. (a) A grayscale Chinese document image. (b) A grayscale English document image. (c) and (d) stego-images after embedding authentication signals, respectively. (e) and (f) stego-images suffer from print-and-scan operations.....	30
Figure 2.9	Some tampered images and authentication results. (a) and (b) tampered	

	images of Figures 2.8(e) and (f), respectively. (c) and (d) authentication results.	32
Figure 3.1	Encoding of edge direction. (a) Edge direction. (b) Edge direction quantized into 16 levels.	38
Figure 3.2	An example of edge direction value computation. (a) Several pixels. (b) The x -direction Sobel mask G_x .(c) The y -direction Sobel mask G_y . (d) and (e) The result of (a) after applying G_x and G_y mask, respectively. (f) Edge direction using (3.1). (g) The result after quantizing the edge direction of (f) into 16 levels.	39
Figure 3.3	The edge direction histogram mapped into a circle. (a) Edge direction histogram. (b) A circle mapped by (a).	40
Figure 3.4	An illustration of the proposed watermark embedding algorithm. (a) A mother block and the COM vector V_m . (b) A child block and the COM vector V_c . (c) An example to embed a “0” with two COM vectors being counterclockwise. (d) An example to embed a “1” with two COM vectors being clockwise.....	45
Figure 3.5	The range of V_c	46
Figure 3.6	An illustration of changing the edge direction by modifying the gray values of pixels.	46
Figure 3.7	Flowchart of the proposed watermark embedding process.....	48
Figure 3.8	A flowchart of the proposed extraction watermark process.....	51
Figure 3.9	An example of line-based block watermarking in a Chinese document image. (a) and (b) Images before and after watermarking. (c) The degree value of the angle of the COM vector V_m in the mother block. (d) and (e) The degree values of the angles before and after embedding a watermark signal.	53
Figure 3.10	An example of line-based block watermarking in an English document image. (a) and (b) Images before and after watermarking. (c) The degree value of the angle of the COM vector V_m in the mother block. (d) and (e) The degree values of the angles before and after embedding a watermark signal.	54
Figure 4.1	An example of 9×9 image blocks. (a) A 9×9 block. (b) Each 3×3 block in the 9×9 block.....	59
Figure 4.2	An example of selecting the mother and child blocks. (a) Indices of a 3×3 block. (b) The selection of the mother and child blocks.....	60
Figure 4.3	An illustration of changing the edge direction by modifying the gray values of pixels.	61
Figure 4.4	A flowchart of the proposed authentication signal embedding method...	65

Figure 4.5	A flowchart of the proposed authentication process.....	66
Figure 4.6	An example of results of applying proposed authentication method. (a) An image of “Painting”. (b) The stego image after embedding authentication codes. (c) Tampered image “Painting”. (d) Authentication result.....	67
Figure 4.7	An example of results of applying proposed authentication method. (a) An image of “Lena”. (b) The stego-image after embedding authentication codes. (c) A tampered image of “Lena”. (d) Authentication result.....	68
Figure 4.8	An example of results of applying proposed authentication method. (a) An image of “Jet”. (b) The stego-image after embedding authentication codes. (c) A tampered image of “Jet”. (d) Authentication result.	69
Figure 5.1	An example of 4×4 image blocks. (a) A 4×4 block. (b) Each 2×2 block in the 4×4 block.....	73
Figure 5.2	An example of Case B. (a) A 4×4 block. (b) The rearrangeable 2×2 block (in the red block) of the 4×4 block. (c) The 4×4 block after embedding “00” the bit stream of watermark. (d) The 4×4 block after embedding “01” the bit stream of watermark. (e) The 4×4 block after embedding “10” the bit stream of watermark. (f) The 4×4 block after embedding “11” the bit stream of watermark.....	78
Figure 5.3	An example of Case C. (a) A 4×4 block. (b) The rearrangeable 2×2 block (in the red block) of the 4×4 block. (c) The 4×4 block after embedding “00” the bit stream of watermark. (d) The 4×4 block after embedding “01” the bit stream of watermark. (e) The 4×4 block after embedding “10” the bit stream of watermark. (f) The 4×4 block after embedding “11” the bit stream of watermark. (g) The 4×4 block after embedding “000” the bit stream of watermark. (h) The 4×4 block after embedding “111” the bit stream of watermark.	79
Figure 5.4	Flowchart of proposed method for watermark embedding process.....	81
Figure 5.5	Flowchart of proposed extraction process.	83
Figure 5.6	Input binary images, output stego-images with watermark signals, the differences, and the watermark image. (a) A binary image of “Lena”. (b) A binary image of “Monkey”. (c) and (d) The stego-images after embedding watermark signals. (e) and (f) The difference between the original binary image and the stego-image.....	84
Figure 5.7	Input binary document images, output stego-images with watermark signals, and the differences. (a) A Chinese binary document image. (b) An English binary document image. (c) and (d) The stego-images after embedding the watermark signals. (e) and (f) The difference between the	

	original binary image and the stego-image, respectively.....	86
Figure 6.1	An example of embedding authentication codes. (a) and (b) A 3×3 block. (c) and (d) Select a code holder to embed an authentication code for (a) and (b). (e) and (f) The result after embedding the authentication code. (g) and (h) The 3×3 block corresponding to (e) and (f).....	92
Figure 6.2	An example of SEC_p and ΔSEC_p . (a)-(c) Some examples of SEC_p . (d) An example of SEC_p . (e) An example of SEC_p'	94
Figure 6.3	An example of authentication signal embedding process in a 9×9 block (a) A 9×9 block and the number index. (b) An example of 9×9 block. (c) The corresponding binary value of (b). (d) An example of embedding an authentication signal into P_6 . (e) The result after embedding authentication signals.....	96
Figure 6.4	An example of watermark signal embedding procedure. (a) The positions for embedding authentication signals. (b) The result after embedding watermark signals.	97
Figure 6.5	Flowchart of proposed method for authentication and watermark signal embedding in binary document images.	99
Figure 6.6	Flowchart of proposed method for authentication and watermark signal extraction process.....	102
Figure 6.7	An embedded watermark image, input binary document images, output stego-images with authentication and watermark signals, and the differences. (a) A binary watermark image. (b) A binary Chinese document image. (c) A binary English document image. (d) and (e) Stego-images after embedding authentication and watermark signals. (f) and (g) The difference pixels before and after embedding authentication and watermark signals.	103
Figure 6.8	Some tampered images, authentication results and embedded watermark images. (a) and (b) Images tampered with. (c) and (d) Authentication results. (e) and (f) Embedded watermark images extracted from (a) and (b), respectively.....	105

LIST OF TABLES

Table 2.1	The PSNR values of the stego-images after embedding authentication signals.	33
Table 3.1	The PSNR values of recovered images after embedding watermarks.	55
Table 3.2	Various attacks and signal detection result	55
Table 4.1	The PSNR values of the stego-images after embedding the authentication signals.	69
Table 5.1	An example of reference table.	76
Table 5.2	The statistics about the embedded bits and the difference pixels for the stego-images after embedding watermark signals.	87



Chapter 1

Introduction

1.1 Motivation

With the rapid development of digital signal processing, many kinds of digital multimedia are produced and used widely nowadays, such as digital images, texts, audio, and so on. On the other hand, because of the rapid growth of the Internet, the exchange of information prevails. As a result, it becomes easy to duplicate and edit digital media without authorization. How to develop techniques to protect the copyright of digital media and verify their integrity is then a great concern. In our study, we will focus on dealing with copyright protection and authentication of digital document images.

Document images are those coming from scanning printed or typewritten documents. A document image is usually text-dominated and reveals a clear separation between the background and the foreground. Many researches have been proposed to achieve the goal of copyright protection and authentication of images. Digital watermarking is the most common way. For copyright protection, a digital watermark is embedded into an image imperceptibly. Image copyright can be protected by extracting the embedded signals. For image authentication, by embedding authentication signals and detecting whether they are destroyed, image integrity and fidelity can be verified.

However, compared with common color images, document images have the characteristic of containing more contrasted contents which are mostly black and white texts. Papers aiming to solve the problems of copyright protection of document images are few according to our survey. In this study, we propose several methods

dealing with the problem of copyright protection and authentication for document images.

In addition, the robustness of stego-images, which are images with embedded data, plays an import role in data hiding fields. Attacks may be applied to the stego-images in order to destroy the embedded watermark signals, and it is hoped that even if a stego-image suffers from attacks, the embedded watermark signals can still be detected and extracted correctly.

The capacity of a cover-image is another main concern. Of course, we hope that the capacity for embedding watermark signals is as large as possible, but in fact it is a trade-off problem. When the robustness is increased, the capacity is decreased. During the embedding process, we aim at making a compromise between the capacity and the robustness for document images.

1.2 Review of Related Works

There have been fewer researches on watermarking techniques for document images than for other types of images according to our survey. However, because of the rapid development of digital signal processing, more and more digital text document files are spread out, such as e-books and digital library contents. As a result, techniques of document image watermarking become more important in applications of copyright protection and image authentication.

Document images can be successively decomposed into pixels, strokes, characters, words, lines, and blocks. In our survey, there are mainly three levels of document components into which signals can be embedded, namely, character-level, stroke feature-level, and pixel-level [3].

Character-level embedding means to use lines, words, or characters as a block unit

to embed data. Brasil, Low, and Maxemchuk [22] developed line-shift coding and word-shift coding algorithms for this purpose. Line-shift coding means to move a line up or down to embed data, while the line immediately above or below are left unmoved. These unmoved adjacent lines serve as reference locations in the decoding process. Word-shift coding is to displace a word to the left or right to embed data, while the words immediately adjacent are left unmoved and serve as reference locations [22]. Huang and Yan [24] proposed a word-shift algorithm which adjusts inter-word spaces to represent a sine wave, which can be seen as a watermark for copyright protection.

Feature-level embedding means to modify the features of text documents, such as stroke, width, and serif shape, to embed watermark signals [23]. A drawback of this method is that the extraction of character features needs to be accurate during the extraction procedure.

Main applications of the pixel-level embedding algorithms include grayscale or binary document images. Because of the limited data embedding capacity, it is difficult to hide data into binary images. Pixel-level algorithms for binary document images aim to embed data at less noticeable positions by using the human visual model found in [1, 2, 13]. A pixel-level embedding algorithm for grayscale document images is proposed in Bhattacharjya and Ancin [25] in which a grayscale document image is divided into non-overlapping sites consisting of 3×3 pixels. Selecting the sites to embed watermark signals is accomplished by setting a threshold at 90th percentile of the luminance histogram of all text components. And one bit is inserted into every two sites. An advantage of this technique is that it provides a large data embedding capacity. However, because the embedding method modifies the brightness of the sites, a drawback results, that is, the robustness is weak.

In this study, we develop techniques belonging to the pixel-level embedding category, and it is hoped to make a compromise between the embedding capacity and the robustness. It means that even though a stego image suffers from attacks, the embedded watermark signals can still be detected and extracted correctly.

1.3 Overview of Proposed Methods

1.3.1 Definitions of Terms

Before describing the proposed method, some definitions of the terms used in this study are given first as follows.

- 1 *Cover image*: A cover image means an image into which a watermark signal is embedded.
- 2 *Stego-image*: A stego-image means an image that is produced by embedding watermark signals into a cover image.
- 3 *Authentication signal*: An authentication signal means a fragile signal embedded into a cover image such that any alteration to the watermarked image can be detected.
- 4 *Authentication image*: An authentication image means an image that is obtained from verifying the embedded authentication signals.
- 5 *Embedding process*: An embedding process means a process to embed data into an image.
- 6 *Extraction process*: An extraction process means a process to extract hidden data from an image.
- 7 *Authentication process*: An authentication process is a process to verify whether a stego-image is tampered with or not.

1.3.2 Brief Descriptions of Proposed Methods

In this study, we focus on dealing with grayscale and binary document images. And for them, different watermarking algorithms will be proposed according to their different characteristics.

A. Integrity Authentication Technique Surviving Print-And-Scan Attacks for Grayscale Document Images

A method for authentication of grayscale document images by a semi-fragile watermarking technique against print-and-scan attacks is proposed in this study, in which a line seen as a semi-fragile watermark and used as an authentication signal is embedded in a grayscale document image to create a stego-image. A rescanned image always has pixel-value distortion and geometric transformations, like scaling, slight rotation, and a little zero padding. Therefore, a watermark embedded in a rescanned image must be provided with robustness against pixel-value distortion and geometric operation attacks. In the proposed method, the block size used for embedding authentication signals is created by a region growing method. A line is produced by a key and adopted as an authentication signal, and is embedded in each block by modifying the gray value of the pixels. By choosing the least noticeable places in each block, the authentication signals can be embedded with less distortion. The authentication signals can be extracted from the stego-image by a line fitting technique. We then judge an image in suspicion as being tampered with or not by checking the difference between the embedded authentication signals and the extracted ones. Figure 1.1 shows a flowchart of the proposed method for embedding authentication signals in grayscale document images.

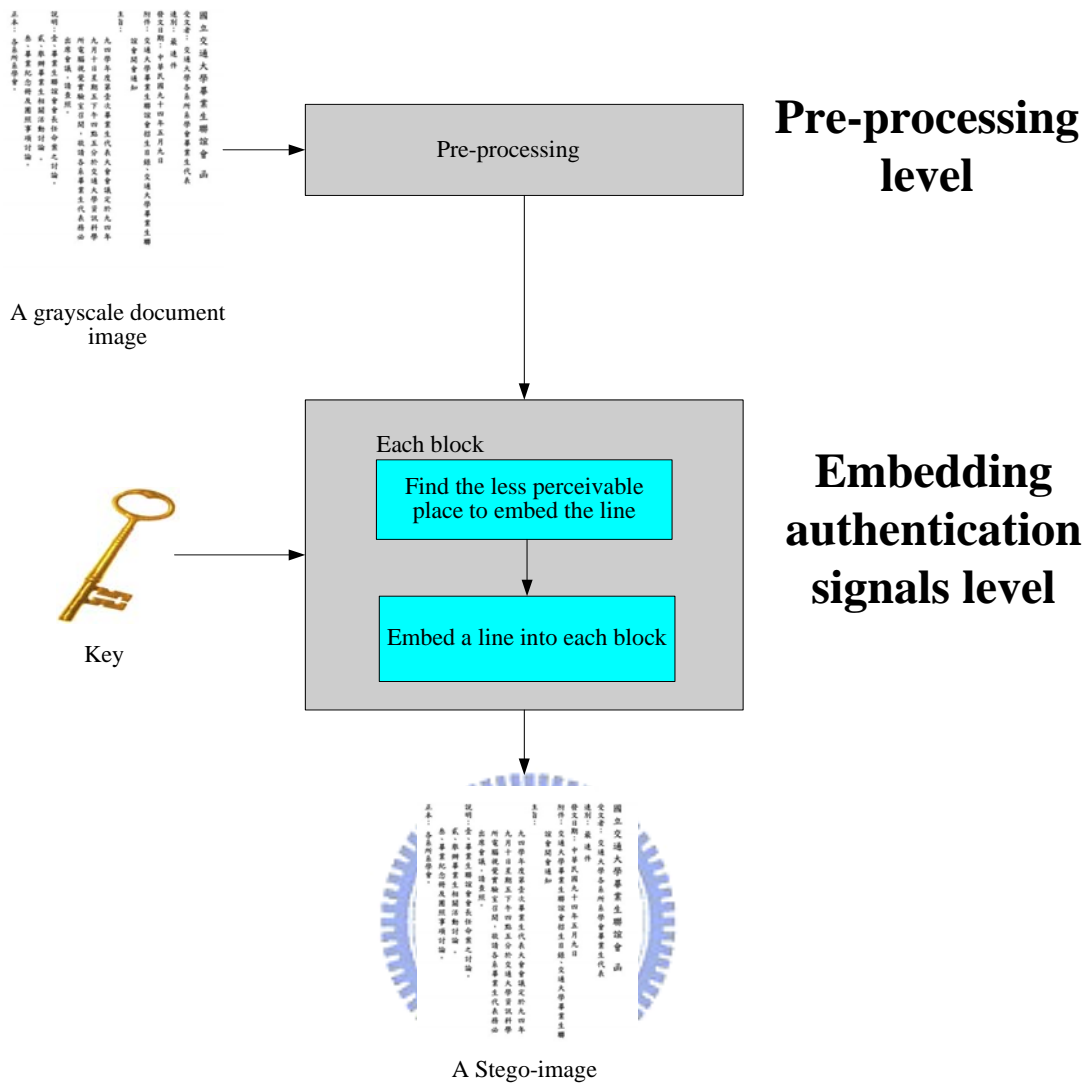


Figure 1.1 Flowchart of proposed method for embedding authentication signals in grayscale document images.

B. Copyright Protection for Grayscale Document Images Using Edge Direction Histograms with Circular Interpretation

A method for copyright protection in grayscale document images using edge direction histograms with circular interpretation is proposed. We use the relationship between mother and child blocks to hide data. A mother block can be seen as a reference block. By modifying the gray value of the pixels in a child block, watermark signals can be embedded in it. More specifically, an edge direction histogram is

created to collect all edge directions in a block to get a discrete distribution. Circular interpretation is then conducted to map an edge direction histogram into a circle. The center of mass in the edge direction histogram is calculated both in the mother and in the child blocks. By adjusting the location of the center of mass in an edge direction histogram circle of the child blocks according to the embedded data, the child blocks can carry the watermark signals. Figure 1.2 shows a flowchart of the proposed method for embedding watermark signals in grayscale document images.

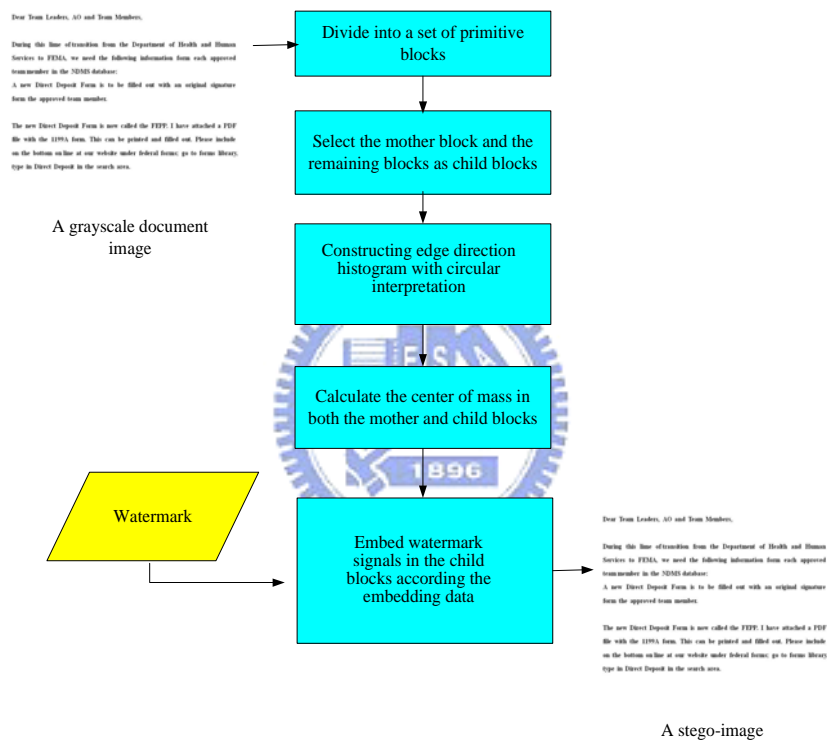


Figure 1.2 Flowchart of proposed method for embedding watermark signals in grayscale document images.

C. A Fragile Authentication Method for Color Images

A method for image authentication in color images is proposed in this study. The block size used in the proposed method is chosen to be 3×3 as the mother block from a 9×9 block. The remaining blocks in the 9×9 block are regarded as child blocks. In

the method, authentication signals and embedding locations are generated by two keys. The concept of edge direction histogram with circular interpretation is also used in this study. By modifying the location of the center of mass in the edge direction histogram circle of the child blocks, authentication codes can be embedded in them. We can then judge the stego-image in suspicion as being tampered with or not by checking the difference between the authentication codes and the extracted ones from the child blocks. Figure 1.3 shows a flowchart of the proposed method for embedding authentication signals method in color images.

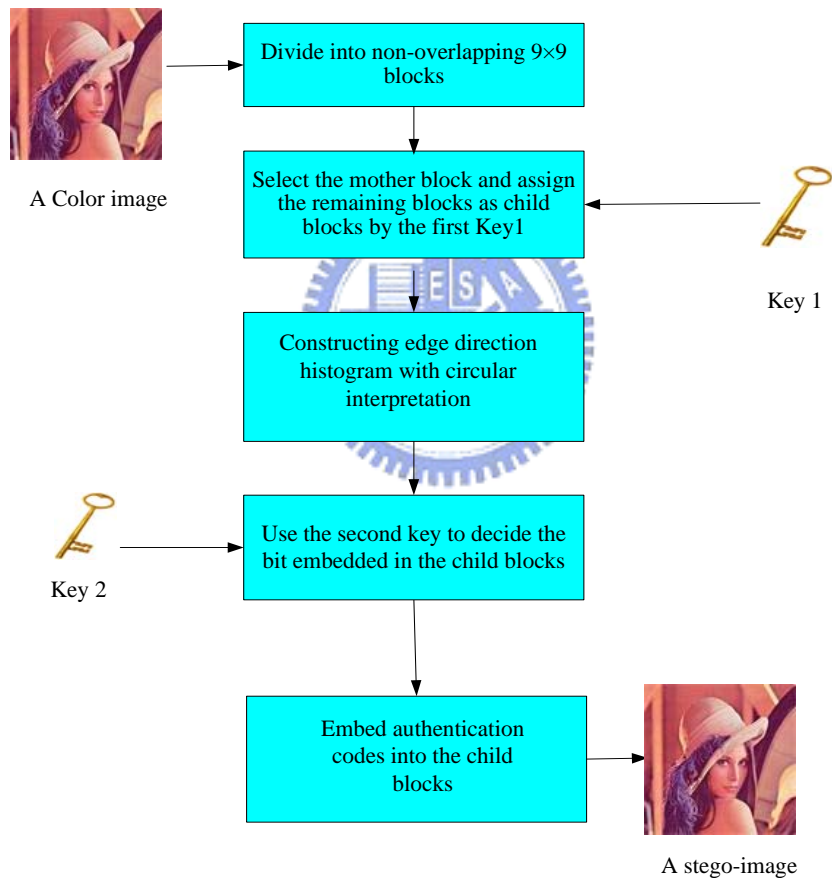


Figure 1.3 Flowchart of proposed method for embedding authentication signals in color images.

D. Watermarking Method for Copyright Protection of Binary Document Images

In this topic, we focus on watermarking for binary document images. We choose the least noticeable 2×2 block from a 4×4 block to embed watermark signals. A reference table about how to embed data is created. With the help of the reference table, we embed data into a binary document image with less distortion. During the extraction process, the watermark signals can be extracted by table lookup from the reference table. Figure 1.4 shows a flowchart of the proposed method for embedding watermark signals in binary document images.

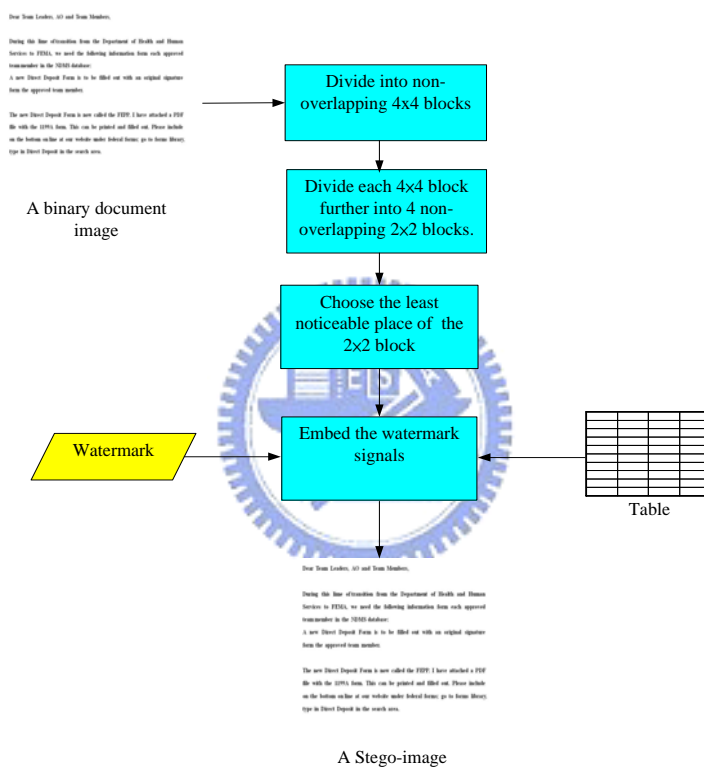


Figure 1.4 Flowchart of proposed method for embedding watermark signals in binary document images.

E. Hiding Digital Information And Authentication Signals behind Binary Images with Reduced Distortion And Enhanced Security

In this topic, a method for binary document images is proposed, which is based on Tseng and Tsai [1-2]. Because the method for embedding authentication signals in [1]

and the method for embedding watermark signals in [2] use the same block size of 3×3 , it is hoped to combine these two methods for embedding watermark and authentication signals together into a cover image, but this will cause some conflicts to occur. We propose a method to solve the conflict problem, in which, the block size for embedding authentication signals is modified to be 9×9 , and the block size for embedding watermark signals is unchanged. We then embed watermark signals into the 3×3 blocks in a 9×9 block in which the authentication signals are embedded in advance.

1.4 Contributions

In this study, several contributions have been made, as described in the following.

- 1 A novel method is proposed to embed authentication signals against print-and-scan operations in grayscale document images.
- 2 A method is proposed to embed watermark signals in grayscale document images.
- 3 A method is proposed to embed authentication signals in color images.
- 4 A method is proposed to embed data in binary document images.
- 5 A method is proposed to integrate watermark and authentication signals for binary document images.

1.5 Thesis Organization

In the remainder of this study, the proposed method about authentication of grayscale document images against print-and-scan operations is described in Chapter 2. In Chapter 3, the proposed method for embedding watermark signals into grayscale document images is described. And in Chapter 4, the proposed method for embedding

fragile authentication signals into color images is described. In Chapter 5, the proposed method for copyright protection by watermarking for binary document images is described. In Chapter 6, the proposed method to integrate watermark and authentication signals for binary document images is described. Finally, in Chapter 7, we will give some conclusions and briefly point out possible directions for future research works. In short, in Chapters 2 and 3, we deal with watermarking in grayscale document images, in Chapter 4, we deal with watermarking in color images, and finally, in Chapters 5 and 6, we deal with watermarking in binary document images.



Chapter 2

Integrity Authentication of Grayscale Document Images Surviving Print-And-Scan Attacks

In this chapter, a method for authentication of grayscale document images by a semi-fragile watermarking technique against print-and-scan attacks is proposed, in which a line seen as a semi-fragile watermark and used as an authentication signal is embedded in a grayscale document image to create a stego-image. During the authentication process, the authentication signals can be extracted by a line fitting technique to acquire the embedded line in each character of a stego-image in suspicion. The integrity of document images can be verified by comparing the difference between the embedded authentication signals and the extracted ones.

The remainder of this chapter is organized as follows. In Section 2.1, an introduction is given first. In Section 2.2, the idea of the proposed method for authentication is briefly described. In Section 2.3, the process of embedding authentication signals is introduced. Section 2.4 includes a description of the process of extracting authentication signals. And in Section 2.5, some experimental results are given to show the feasibility of the proposed method. Finally, in Section 2.6, some discussions and a summary are made.

2.1 Introduction

2.1.1 Problem Definition

Because document images such as magazines and newspapers are widespread

and they are easy to duplicate or tamper with, the issues of copyright protection and authentication of document images must be taken into consideration more seriously. For instance, if a publisher publishes their magazines per month, they might want to design a scheme to protect their copyright and to authenticate the integrity of them.

The definition of print-and-scan operation is to print an image and rescan it to become a digital version. Because of the rapid development of electronic products, printers and scanners are commonly used for distributions and reproductions of documents. It is popular to transform an image between the electronic digital format and the printed form. Some distortions may occur during the transformation; therefore, for copyright protection and integrity checking, it needs to design a scheme to solve this problem. It means that print-and-scan operations are regarded as normal behaviors to process an image, and they cannot be considered as tampering operations, but we still want to be sure whether the image resulting from rescanning is genuine in every part, i.e., to be sure the integrity of the image. So a developed scheme must have a certain degree of robustness against print-and-scan operations.

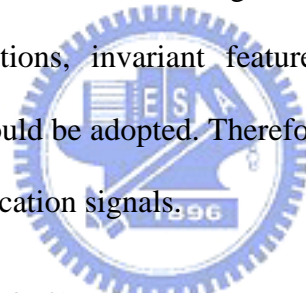
Digital watermarking is a technique to embed a watermark into an image to protect the owner's copyright of the image. And the watermark signals must be robust against print-and-scan operations. It is hoped that after applying these operations on the stego-image, the embedded watermark signals still can be detected and extracted exactly.

2.1.2 Properties of Document Images Attacked by Print-And-Scan Operations

If an image suffers from print and scan operations, there are two categories of distortions, namely geometric transformations and pixel value distortions. Geometric

transformations include translation, rotation, cropping and scaling. And distortions of pixel values are caused by (1) luminance, contrast, gamma correction, and chrominance variations, and (2) blurring of neighboring pixels. These are typical effects of printers and scanners, and while they are perceived by human eyes, they affect the visual quality of a rescanned image [9]. Geometric transformations do not cause significant effects on the visual quality but the pixel value distortions do. Figure 2.1 shows an original image and a rescanned version of it.

If we want to design a method for image authentication, embedding watermark signals is a way to achieve this goal. And the embedded authentication signal must have certain degrees of robustness against pixel-value distortions and geometric operations. In order to embed authentication signals in a grayscale document image against print-and-scan operations, invariant features of images with respect to geometric transformations should be adopted. Therefore, it's better to use semi-fragile watermarks to embed authentication signals.



2.1.3 Properties of Grayscale Document Images

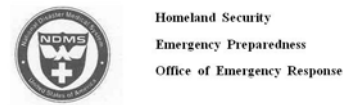
Document images are those coming from scanning printed or typewritten documents. A feature of document images is that there are many huge white blocks in background, so if we modify the gray values of pixels in the background, it is easy to be perceived. Another feature of document images is that it is usually text-dominated and reveals clear contrast between the background and the foreground. Because of pure color distribution, image processing on document images is easy to be noticed.

A grayscale image has only one channel, the gray channel. Each pixel value of this channel is an integer between 0 and 255. In the proposed method, we focus on grayscale document images, and so how to embed data in the single channel of a

grayscale document image is the main issue in this chapter.

國立交通大學畢業生聯誼會 函
 受文者：交通大學各系所系學會畢業生代表
 送別：最速件
 發文日期：中華民國九十四年五月九日
 附件：交通大學畢業生聯誼會招生目錄、交通大學畢業生聯誼會開會通知
 主旨：九四學年度第壹次畢業生代表大會會議定於九四年九月十日星期五下午四點五十分於交通大學資訊科學所電腦視覺實驗室召開，敬請各系畢業生代表務必出席會議，請查照。
 說明：壹、畢業生聯誼會會長任命案之討論。
 貳、舉辦畢業生相關活動討論。
 參、畢業紀念冊及團照事項討論。
 正本：各系所系學會。

(a)



Dear Team Leaders, AO and Team Members,

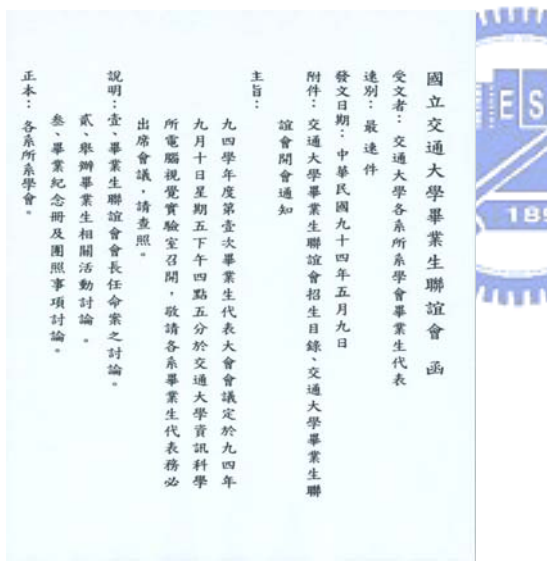
During this time of transition from the Department of Health and Human Services to FEMA, we need the following information from each approved team member in the NDMS database:

A new Direct Deposit Form is to be filled out with an original signature from the approved team member.

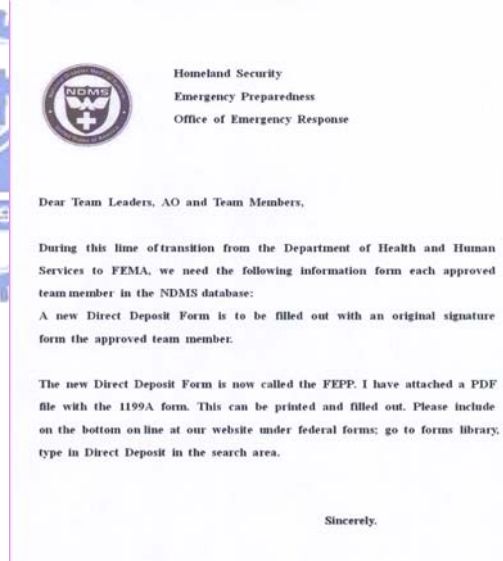
The new Direct Deposit Form is now called the FEPP. I have attached a PDF file with the 1199A form. This can be printed and filled out. Please include on the bottom on line at our website under federal forms: go to forms library, type in Direct Deposit in the search area.

Sincerely,

(b)



(c)



(d)

Figure 2.1 A grayscale document image and a reproduced image. (a) A grayscale Chinese document image. (b) A grayscale English document image. (c) Reproduced image of (a) with quality of 100dpi. (d) Reproduced image of (b).

2.2 Idea of Proposed Authentication Method

In the procedure of embedding authentication signals, a document image is first divided into non-overlapping blocks. Different processing an image in the unit of a constant block, we treat a character or a word as a basic block by a connected component merging technique. Second, to each word block, we assign a number index and then embed in it a line as a semi-fragile watermark by decreasing the gray values of these pixels in it. Coefficients of a line equation are created by (1) a secret key, (2) an RHG value [10] which is used to assign a gray value G to a binary image block, and (3) the block number index, in order to enhance the security of authentication.

As for the extraction of authentication signals, the pre-processing procedure of acquiring blocks is the same as the embedding one. And then we extract the least gray value of pixels in each block and apply a line fitting technique to obtain an equation of a line. In addition, we calculate another equation of a line by the key, the RHG value and the number index for each block. By comparing the difference between embedded line and calculated one in each block, we can verify the integrity of a grayscale document image.

2.3 Authentication Signal Generation and Embedding

In order to generate authentication signals for a grayscale document image, in our method, it is needed to do some pre-processing for the sake of reducing distortion. So there are two stages of tasks in our method, which are the pre-processing stage and the authentication signal embedding stage.

2.3.1 Pre-processing Stage

A. Bi-level thresholding:

The first step in the pre-processing stage is to remove noise and distortion. We apply a bi-level thresholding to increase the sensitivity of a region growing technique applied later. We set a threshold value to divide 256 pixel values into 2 pixel values, 0 and 255, and the corresponding pixels may be called *black* and *white* ones, respectively.

B. Division of image into blocks by connected component merging:

If we process an image in terms of blocks of a fixed size, the blocks will be changed after the image suffers from scaling or shrinking. So, it is not suitable to utilize blocks of a fixed size to process an image against scaling. We utilize a technique of connected component merging or the so-called region growing in the data embedding and extraction processes to determine the size of a block, so the blocks defined in the data extraction and embedding processes have identical ranges. Region growing is a procedure that groups pixels or subregions into large regions based on predefined criteria. The basic concept is to start with a set of “seed” points and from them grow regions by appending to each seed those neighboring pixels that have properties similar to the seed [5]. Figure 2.2 shows an example of a character segmented as a basic block by the region growing method.

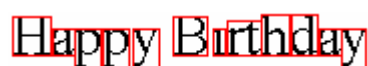
電腦視覺實驗室

(a)



(b)

Happy Birthday



(c)

(d)

Figure 2.2 An example of using region growing technique to get basic blocks. (a) Several Chinese characters. (b) Each character becomes a block (c) Several English characters. (d) Each character becomes a block.

C. Merging blocks:

The objective of merging blocks is to merge overlapping or neighboring smaller blocks into a larger one. If an image suffers from enlarging, gaps in characters will be enlarged. This means that a block may be divided into several parts and the total number of blocks after region growing will be different from the original one. So it is needed to devise a technique to solve this problem caused by image enlarging. We use a block merging technique to solve this problem. Two cases need be treated here.

Case1: Several blocks are overlapping:

If a block b_1 and another block b_2 are overlapping, then we merge the two blocks to establish a new one.

Case2: Several blocks are neighboring:

If the distance between the center of a block b_1 and the center of another

block b_2 are smaller than a threshold T_i , then we merge the two blocks into a new one. Figure 2.3 shows an example in this case. Figure 2.3 (a) is an image and its blocks acquired after region growing and (b) an image suffers from enlarging operations and its blocks acquired. As we can see, if an image suffers from scaling, the total number of blocks we obtain will be different from that of the original image.

In Figure 2.3(c), c_1 , c_2 , c_3 and c_4 are the center of blocks 1, 2, 3, 4, respectively; d_2 , d_3 and d_4 are the distance between the center of the first block c_1 and c_2 , c_3 and c_4 , respectively. If d_2 , d_3 or d_4 are smaller than T_i , then we merge the two blocks. After merging blocks, the total number of blocks is identical to the original one. Figure 2.3 (d) shows an example after merging blocks. Figure 2.3(e) and (f) show another example of merging blocks.

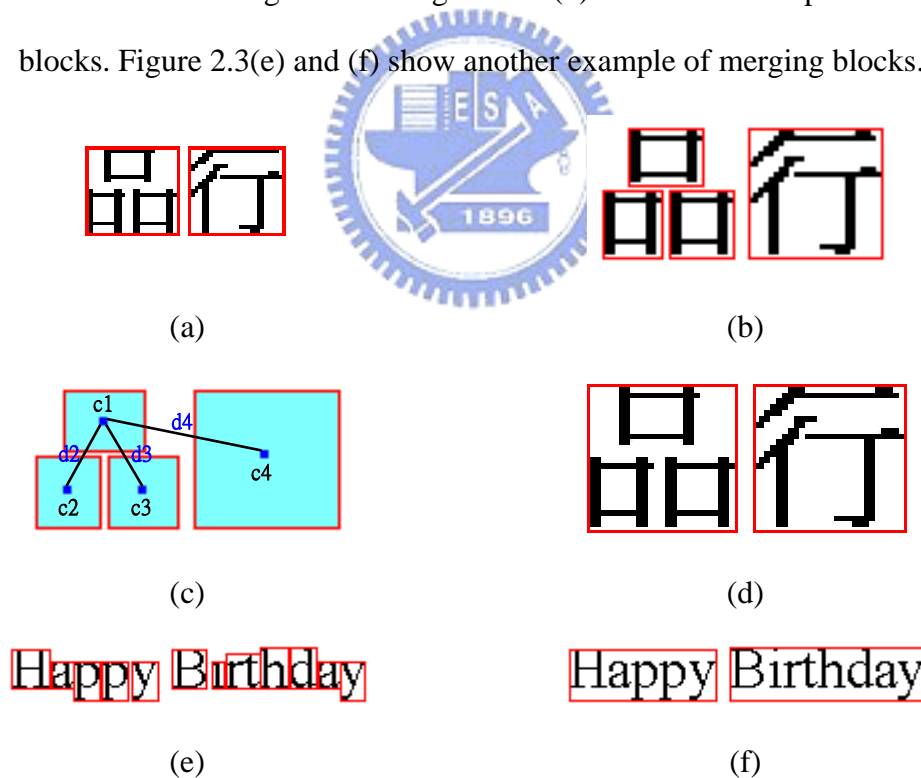


Figure 2.3 An example of block merging. (a) A Chinese document image and the total number of blocks is 2. (b) An enlarged image of (a) and the total number of blocks is 4. (c) Block distances of (b). (d) The result image of (b) after block merging. (e) An English document image and the total number of blocks is 12. (f) The result image of (e) after block merging.

D. Assignment of a number index to each block:

The reason of assigning each block a number index as a parameter to establish an equation of a line for embedding is to increase the security of authentication. In our method, after collecting all image blocks, we give a number index to each block. We do this for all blocks from the top-left to the bottom-right of the image.

E. Increasing the gray values of total black pixels:

Because the equation of the embedded line in each block is to modify the gray values of the black pixels which the embedded line has passed through to 0, in order to distinguish the embedded black pixels from original black pixels, we need to increase the gray values of total black pixels to a threshold T_s .

2.3.2 Creation and Embedding of Semi-Fragile Authentication Signals by Line Embedding

The objective of the pre-processing stage is to decrease created distortions. In this section, we describe how to create and embed authentication signals into each block. The technique we describe below is the core skill. The main idea is to embed a value as a semi-fragile watermark into each block. And the value is the slope of a line. For the purpose of increasing the robustness, we will choose the best position to embed an authentication signal into each block. It seems a better choice to consider embedding data in black pixels in each block. After choosing the best position to hide an authentication signal in each block, we embed the slope of a line into each block by modifying the gray values of the black pixels through which the embedded line passes. The detail of semi-fragile watermark embedding is described below.

A. Acquiring the equation of the embedded line:

In order to enhance the security of authentication, we use a key, the RHG value and the block number index as parameters to build up the equation of the embedded line. An equation of a line is as follows:

$$y = mx + b \quad (2.1)$$

where x denotes a value of an x -coordinate, and y means similarly, m is a slope of a line, and b is a constant which means the shift of the y -axis.

In our method, the slope of the line m is the main coefficient to control the slope of the embedded line. We create the value of m in terms of three elements: a key, the RHG value, and the block number index. After m is determined, b is used to adjust the shift of the embedded line to reduce the awareness by human eyes.

(1) A key:



A key held by the sender and the receiver is used to enhance the security of authentication as mentioned previously. It can be promised that even the algorithm is known by a thief, without a correct key he/she can not produce the authentication signals to cheat the algorithm during the authentication process.

(2) The RHG value:

The RHG value aims to assign a gray value G by the following reduced halftone gray function:

$$G = \frac{(T - B)}{T} \times level \quad (2.2)$$

where $level$ means to divide total pixels into $level$ parts, T is the total number of pixels and B is the number of black pixels. Equation (2.2) was proposed by Huang and Tsai

[10]. Because the *RHG* is based on the use of blocks of a fixed size and can not be applied to our method directly, we revise it to meet our goal of allowing the use of arbitrary-sized blocks.

(3) The block number index

We assign each block a number index to represent it. The numbers are assigned in a raster scan order. The block number index is also a key parameter to build up the equation of a line. The reason is to avoid malicious attacks by altering the positions of blocks.

After computing the three main elements, we compute the slope of the embedded line by the following equation:

$$m = f(\text{key}, \text{RHG value}, \text{block number index}) \quad (2.3)$$

Because the size of a block is not infinite and the capacity to embed the slope m into each block is restricted, the slope m of the embedded line can not be too large. As a result, we need to limit the range of m . In our method, the function f is described as follows:

$$m = (\text{key} + \text{RHG value} + \text{block number index}) \% \text{range} \quad (2.4)$$

where *range* is used to control the range of m . By modifying the slope m of the embedded line, we can embed an authentication signal into each block.

B. Finding the best position to embed a line

After calculating the slope of the embedded line, it is needed to find the best position to embed a line. A technique we use here is to adjust the constant value b of the equation of the line described in (2.1) to seek the best position to embed a line which arouses the least awareness. We shift the position of the embedded line by

modifying the constant value b .

In our method, the black pixels with gray value T_s in each block are used to carry an authentication signal by modifying their gray values to 0. And the selection of black pixels for embedding an authentication signal is by checking whether the embedded line passes through. Because it is hoped that the authentication signal have a certain degree of robustness, we choose more places to embed it to increase the robustness. So, we find the position with the largest number of lining-up black pixels which the embedded line passes through to embed the authentication signal. The position of the most number of lining-up black pixels to embed the line is selected by modifying b and can be seen as the best position with the best robustness.

Figure 2.4 shows an example of selecting the best position to embed a line. In this example we set m in Equation (2.1) to be $m = 1$. Figure 2.4(a) shows a block after applying a region growing technique, and (b) is an example of shifting b to seek the best position to embed the line. After adjusting all possible values of b , we can find the best position to embed the line, as shown in Figure 2.4(c). Figure 2.4(d) shows that after selecting the value of b , we modify the gray values of the black pixels through which the embedded line passes in the block.

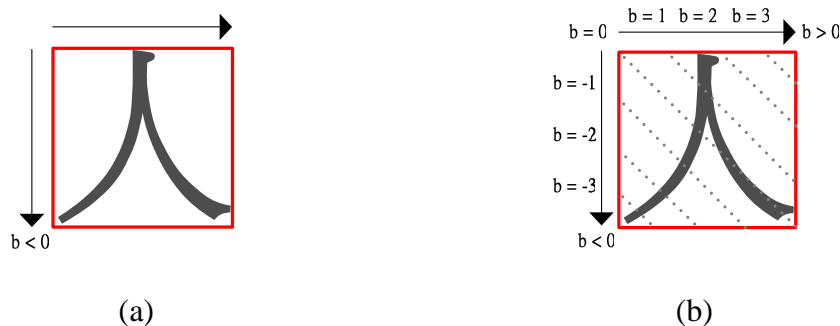


Figure 2.4 An example of finding the best position to embed a line. (a) A character. (b) and (c) Shifting b to seek the best position to embed the authentication signal. (d) Modifying the gray values of the black pixels in the character.

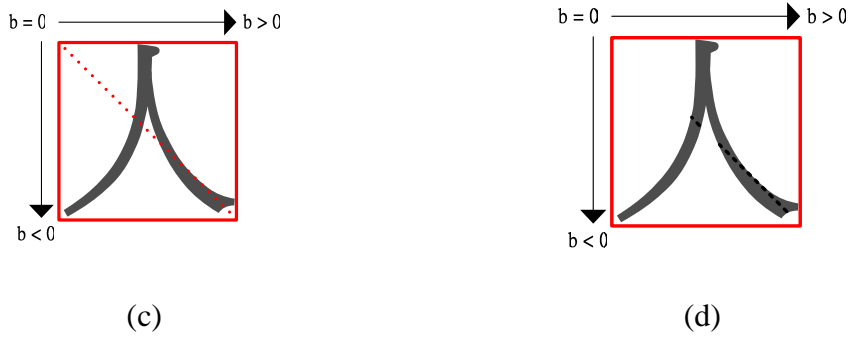
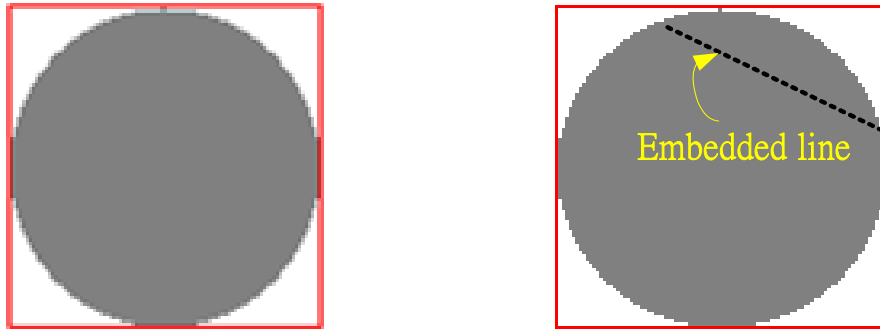


Figure 2.4 An example of finding the best position to embed a line. (a) A character. (b) and (c) Shifting b to seek the best position to embed the authentication signal. (d) Modifying the gray values of the black pixels in the character (continued).

C. Embedding a line into each block

In order to increase the robustness, we select the best position to embed a semi-fragile watermark in each block. Because all the black pixels in a document image raise the gray values to T_s during the pre-processing stage, we can distinguish the authentication signal embedded in the black pixels in each block from the original black pixels by modifying the gray values of the black pixels which are selected for embedding the authentication signals. By decreasing to 0 the gray values of the black pixels through which the line has passed, we can embed a line into each block. So, during the authentication process, we only need to extract the least gray values of pixels in each block to recover the equation of the embedded line. Figure 2.5 shows an example of this step.



(a)

(b)

Figure 2.5 An example of embedding a line into a block. (a) A block. (b) The result after embedding a line in (a).

2.3.3 Detailed Algorithm

The inputs to the proposed method for embedding authentication signals include a grayscale document image I and a key K . The output is a stego-image S . The algorithm for the process can be briefly expressed as follows. Figure 2.6 shows a flowchart of the process.

Algorithm 1: *Authentication signal embedding process.*

Input: A given grayscale document image I and a key K used in the authentication signal embedding process.

Output: A stego image S .

Steps:

- 1 Pre-Processing of a document image I :
 - 1.1 Apply bi-level thresholding to I using a threshold T_i .
 - 1.2 Divide I into character blocks by a connected component merging

technique.

- 1.3 For each block D_i , merge overlapping or neighboring smaller blocks into a larger one.
- 1.4 Assign each block D_i a number index S_i in a raster scan order from top left to bottom right.
- 1.5 Increase the gray values of all the black pixels in I to be T_s .
- 2 For each block D_i , build up the equation of a line to be embedded.
 - 2.1 Assign the RHG value according to (2.2).
 - 2.2 Use K , S_i and the RHG value to calculate a slope m of a line according to (2.3).
 - 2.3 Find the best position to embed the line by shifting a constant of b .
 - 2.4 Embed the line into D_i by modifying the gray values of the black pixels through which the line passes.
- 3 Take the final result as the desired stego-image S .

2.4 Image Authentication process

In the embedding process, the embedded authentication signal is the line created by the key, the RHG value, and the number index. Therefore, we can judge an image in suspicion as being tampered with or not by checking the difference of authentication signals between the generated slope m and the extracted slope m' .

2.4.1 Extraction of Authentication Signals Using A Line Fitting Technique

The proposed method for image authentication is essentially similar to the embedding one but in a reverse order. A suspicious image is first divided into non-overlapping

blocks by a connect component merging technique, and then merging neighboring or overlapping smaller blocks into a larger one similar to the pre-processing of the embedding process. For each block, we collect the least gray values of the pixels and apply a line fitting technique to extract the authentication signals.

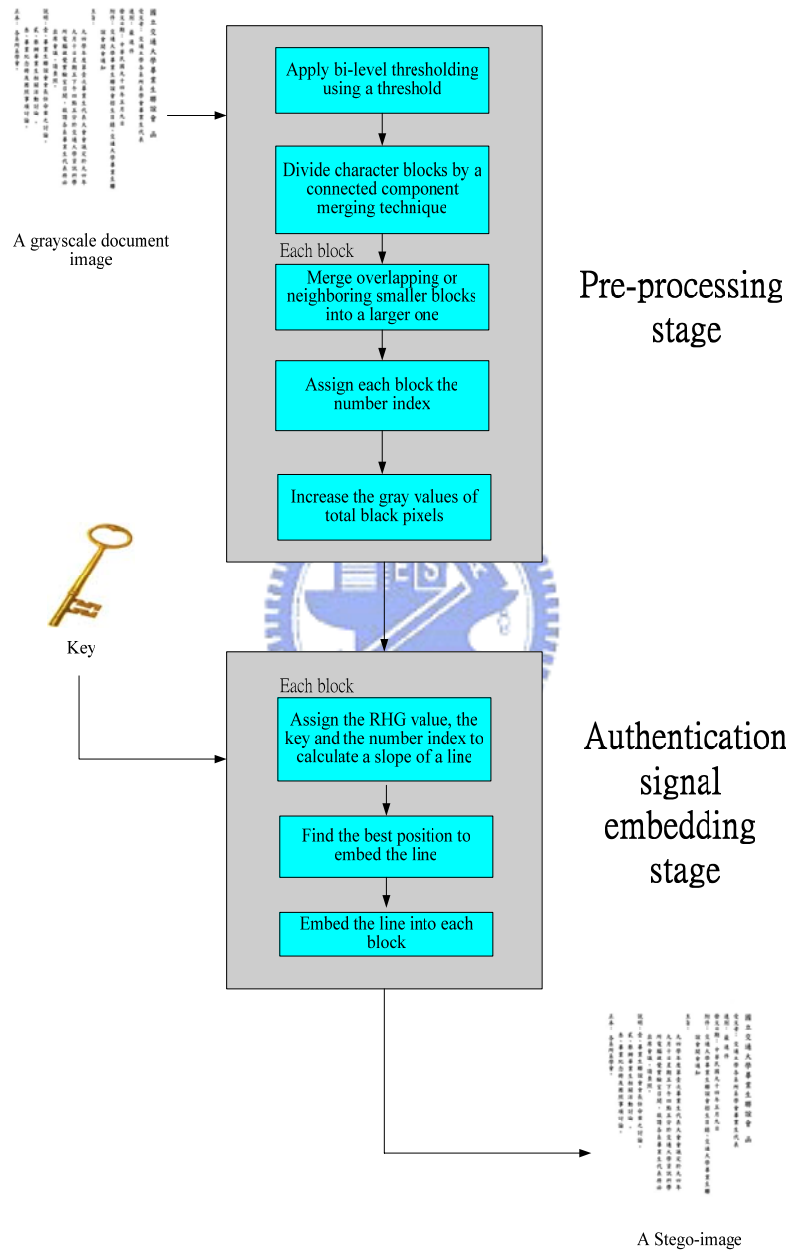


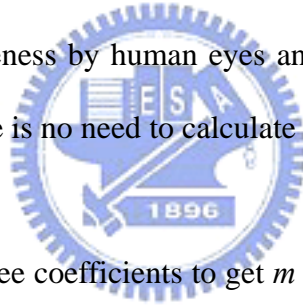
Figure 2.6 Flowchart of proposed method for authentication signal embedding in grayscale document images.

A. Applying a line fitting technique to extract the embedded line.

During the embedding process, modifying to be 0 the gray values of the black pixels which the line has passed through is the core technique to embed a semi-fragile watermark into each block. So, during the image authentication procedure, all we need to do is to collect the least gray values of the pixels in each block and extract the embedded line by a line fitting technique which is described as follows:

$$m' = \frac{n \sum_{i=1}^n x_i y_i - \sum_{i=1}^n x_i \sum_{i=1}^n y_i}{n \sum_{i=1}^n x_i^2 - (\sum_{i=1}^n x_i)^2} \quad (2.5)$$

where m' means the slope of a line, n is the total number of pixels and X : $[x_1, x_2, x_3 \dots x_n]$; Y : $[y_1, y_2, y_3 \dots y_n]$. One thing needed to remind again is that b in (2.1) is only used for decreasing the awareness by human eyes and is irrelevant to the embedded authentication signals, so there is no need to calculate this constant.



We still have to collect three coefficients to get m according to (2.4) which are the key, RHG value, and the number index. By comparing the difference between m and m' , we can judge an image in suspicion as being tempered with or not in each block. Figure 2.7 is a flowchart of the proposed method for image authentication.

Algorithm 2: *Image authentication process.*

Input: A given stego-image S and the key K identical to that used in the embedding process.

Output: An authentication image A .

Steps:

- 1 Pre-Processing of a document image S

- 1.1 Divide S into character blocks by a connected component merging technique.
- 1.2 For each block D_i , merge overlapping or neighboring smaller blocks into a larger one.
- 1.3 Assign each block D_i a number index S_i .
- 2 For each block D_i , perform the following operations.
 - 2.1 Collect the least gray values of pixels, and apply line fitting to the pixels to get m' according to (2.5)
 - 2.2 Assign the RHG value according to (2.2)
 - 2.3 Use K , S_i , and RHG to calculate the slope m of the line according to (2.4).
 - 2.4 if $m \neq m'$, then regard D_i as being tampered with and mark the block at the same location in A with red color.
- 3 Take the final result as the desired authentication image A .

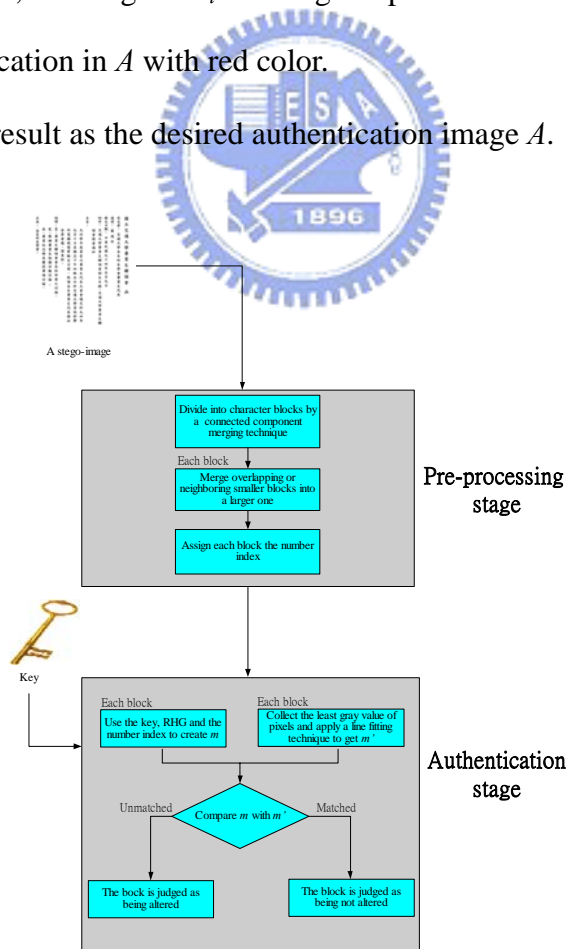


Figure 2.7 Flowchart of proposed method for image authentication

2.5 Experimental Results

Some experimental results of applying the proposed method are shown here. Figure 2.8(a) and (b) are two grayscale Chinese and English document images, respectively, both with size of 400×500. And the stego-images resulting from embedding authentication signals are shown in Figure 2.8(c) and (d), respectively. Figure 2.8(e) and (f) are two stego-images suffering from print-and-scan operations, which were printed at 400dpi and scanned at 100dpi using an HP LaserJet 4200 printer and a MICROTEC Scanmaker 9800XL flatbed scanner. The corresponding PSNR values are shown in Table 2.1. Two tampered images suffering from print-and-scan operations are shown in Figure 2.9(a) and (b) with resolutions of 100dpi. And Figure 2.9(c) and (d) show the authentication results. The red parts indicate the detected tampered areas. By experiments, even if an image is subject to print-and-scan operations, we can still detect the integrity of a stego-image. The experimental results show that the embedded authentication signals have the semi-fragile property and can survive print-and-scan operations.

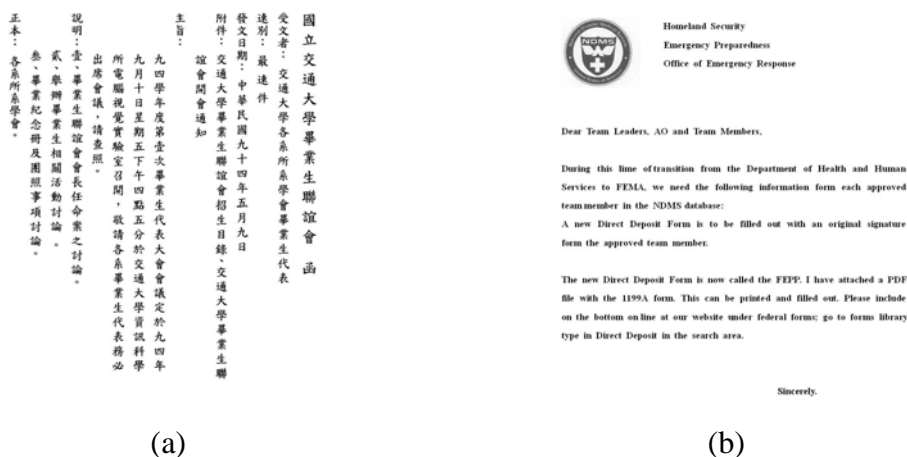


Figure 2.8 Input grayscale document images and output stego-images with authentication signals. (a) A grayscale Chinese document image. (b) A grayscale English document image. (c) and (d) stego-images after embedding authentication signals, respectively. (e) and (f) stego-images suffer from print-and-scan operations.

國立交通大學畢業生聯誼會 函
 受文者：交通大學各系所系學會畢業生代表
 速別：最速件
 發文日期：中華民國九十四年五月九日
 附件：交通大學畢業生聯誼會招生目錄、交通大學畢業生聯誼會開會通知
 主旨：九四學年度第壹次畢業生代表大會會議定於九十四年九月十日星期五下午四點五十分於交通大學資訊科學所電腦視覺實驗室召開，敬請各系畢業生代表務必出席會議，請查照。
 說明：壹、畢業生聯誼會會長任命案之討論。
 貳、舉辦畢業生相關活動討論。
 參、畢業紀念冊及團照事項討論。
 正本：各系所系學會。

(c)



Homeland Security
 Emergency Preparedness
 Office of Emergency Response

Dear Team Leaders, AO and Team Members,

During this time of transition from the Department of Health and Human Services to FEMA, we need the following information from each approved team member in the NDMS database:

A new Direct Deposit Form is to be filled out with an original signature from the approved team member.

The new Direct Deposit Form is now called the FEPP. I have attached a PDF file with the 1199A form. This can be printed and filled out. Please include on the bottom on line at our website under federal forms; go to forms library, type in Direct Deposit in the search area.

Sincerely,

(d)

國立交通大學畢業生聯誼會 函
 受文者：交通大學各系所系學會畢業生代表
 速別：最速件
 發文日期：中華民國九十四年五月九日
 附件：交通大學畢業生聯誼會招生目錄、交通大學畢業生聯誼會開會通知
 主旨：九四學年度第壹次畢業生代表大會會議定於九十四年九月十日星期五下午四點五十分於交通大學資訊科學所電腦視覺實驗室召開，敬請各系畢業生代表務必出席會議，請查照。
 說明：壹、畢業生聯誼會會長任命案之討論。
 貳、舉辦畢業生相關活動討論。
 參、畢業紀念冊及團照事項討論。
 正本：各系所系學會。

(e)



Homeland Security
 Emergency Preparedness
 Office of Emergency Response

Dear Team Leaders, AO and Team Members,

During this time of transition from the Department of Health and Human Services to FEMA, we need the following information from each approved team member in the NDMS database:

A new Direct Deposit Form is to be filled out with an original signature from the approved team member.

The new Direct Deposit Form is now called the FEPP. I have attached a PDF file with the 1199A form. This can be printed and filled out. Please include on the bottom on line at our website under federal forms; go to forms library, type in Direct Deposit in the search area.

Sincerely,

(f)

Figure 2.8 Input grayscale document images and output stego-images with authentication signals. (a) A grayscale Chinese document image. (b) A grayscale English document image. (c) and (d) stego-images after embedding authentication signals, respectively. (e) and (f) stego-images suffer from print-and-scan operations (continued).

國立台灣大學畢業生聯誼會 函

受文者：交通大學各系所系學會畢業生代表

速別：最速件

發文日期：中華民國九十四年五月九日

附件：咄咄大學畢業生聯誼會招生目錄、交通大學畢業生聯誼會開會通知

主旨：九四學年度第壹次畢業生代表大會會議定於九四年九月十日星期五下午五點五十分於交通大學資訊科學所電腦視覺實驗室召開，敬請各系畢業生代表務必出席會議，請查照。

說明：壹、畢業生聯誼會會長任命案之討論。
貳、舉辦畢業生相關活動討論。
參、畢業紀念冊及團照事項討論。

正本：各系所系學會。

Homeland Security
Emergency Preparedness
Office of Emergency Response

Dear Team Leaders, AO and Team Members,

During this time of transition from the Department of Health and Human Services to FEMA, we need the following information form each approved team member in the ~~NIDSS~~ database:


A new Direct Deposit Form is to be filled out with an original signature form the approved team member.

The new Direct Deposit Form is now called the FEPP. I have attached a PDF file with the 1199A form. This can be printed and filled out. Please include on the bottom ~~office~~ at our website under federal forms; go to forms library, type in Direct Deposit in the search ~~box~~

Sincerely, NCTU

(a)


(b)


國立  大學畢業生聯誼會 函


受文者：交通大學各系所系學會畢業生代表

速別：最速件

發文日期：中華民國九十四年五月九日

附件：  大學畢業生聯誼會招生目錄、交通大學畢業生聯誼會開會通知


主旨：九四學年度第壹次畢業生代表大會會議定於九四年九月十日星期五下午  點五十分於交通大學資訊科學所電腦視覺實驗室召開，敬請各系畢業生代表務必出席會議，請查照。

說明：壹、畢業生聯誼會會長任命案之討論。
貳、舉辦畢業生相關活動討論。
參、畢業紀念冊及團照事項  。



正本：各系所系學會。




Homeland Security
Emergency Preparedness
Office of Emergency Response

Dear Team Leaders, AO and Team Members,

During this time of transition from the Department of Health and Human Services to FEMA, we need the following information form each approved team member in the  database:

A new Direct Deposit Form is to be filled out with an original signature form the approved team member.

The new Direct Deposit Form is now called the FEPP. I have attached a PDF file with the 1199A form. This can be printed and filled out. Please include on the bottom  at our website under federal forms; go to forms library, type in Direct Deposit in the search 

Sincerely,   

(c)

(d)

Figure 2.9 Some tampered images and authentication results. (a) and (b) tampered images of Figures 2.8(e) and (f), respectively. (c) and (d) authentication results.

Table 2.1 The PSNR values of the stego-images after embedding authentication signals.

	Chinese Document Images	English Document Images
PSNR	22.8	22.3

2.6 Discussions and Summary

In this chapter, we have presented an authentication scheme to embed authentication signals against print-and-scan operations in grayscale document images. The main idea of our method is to embed a line as a semi-fragile watermark into each block of a grayscale document image. And the equation of the embedded line is created by a key, an *RHG* value, and a block number index to increase the security of authentication. Because the line is embedded by modifying to 0 the gray values of the black pixels which the line has passed through during the image authentication process, we only need to collect the least gray values of the pixels in each block and apply a line fitting technique to extract the embedded line. We can verify the integrity of the image to be tampered with or not by comparing the difference between the generated slope m and the extracted slope m' . If someone tampers with a stego-image, the *RHG* value or the block number index will be changed. The extracted slope m' of the embedded line from the tampered image will then not be the same as the generated slope m . Therefore, the tampered areas can be detected and located.

In our method, we use a linear equation of the first order to embed an authentication signal; we also can use a polynomial equation in the same way to increase the security.

It is common to print document files. And the print-and-scan operation should not be considered as a tampering operation, though it is a huge attack so far as the

resulting image quality is concerned. The experimental results prove our proposed method to be useful and that the embedded authentication signals can survive print-and-scan operations.



Chapter 3

Copyright Protection for Grayscale Document Images Using Edge Direction Histograms with Circular Interpretation

The proposed method for copyright protection of grayscale document images is described in this chapter. The main idea is based on two techniques, namely, *edge direction histograms (EDH)* and *circular interpretation*, and we will describe these two terms later. These techniques are employed to embed watermark signals into grayscale document images.

The remainder of this chapter is organized as follows. In Section 3.1, an introduction and the term definitions are first given. The idea of the proposed watermarking method is presented in Section 3.2. The watermark embedding process and the watermark extraction process are shown in Section 3.3 and Section 3.4, respectively. In Section 3.5, several experimental results are illustrated. Finally, in Section 3.5, some discussions and a summary are made.

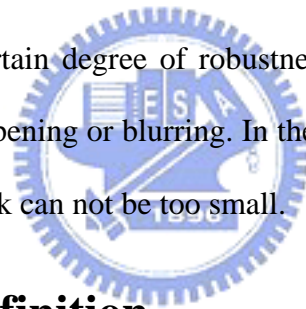
3.1 Introduction

Digital watermarking is a technique for embedding a watermark into an image to protect the owner's copyright of the image. However, the stego-images are easy to be modified, thus destroying the watermark signals. As a result, the stego-images need to be robust to avoid malicious attacks. There are many existing robust methods to embed watermark signals into an image, but the capacity offered by each of these

methods is relative small. We all know that this involves a tradeoff problem. When the robustness is increased, the capacity is decreased. In this study, we aim at making a compromise between the capacity and the robustness for grayscale document images.

3.1.1 Motivation

Because digital text document files such as e-books and digital library files are spread easily and gained popularity, and because they are easy to duplicate or tamper with, how to protect these precious files is a main concern in recent years. A watermark scheme is a way to achieve this goal to protect the copyright of these documents. In our method, we deal with grayscale document images which come from scanning printed or typewritten documents. And it is hoped that the embedded watermark signals have a certain degree of robustness for copyright protection and can survived attacks like sharpening or blurring. In the meantime, it is desired that the capacity to embed a watermark can not be too small.



3.1.2 Problem Definition

The properties of grayscale document images are described in Section 2.1.2. In short, a document image is usually text-dominated and reveals clear contrast between the background and the foreground. And a text document image has a hierarchical structure: a page image can be successively decomposed into blocks, lines, words, characters, strokes, and pixels [3].

In this chapter, we describe a method to embed a robust watermark with less distortion into a document image for copyright protection. We use a technique based on the use of the edge directional histogram with circular interpretation to embed the watermark signals. The algorithm is based on the fact that texts have similar shapes in

their edge direction histograms [3] which will be described later, and that texts appears widely in document images.

3.1.3 Definition of Edge Direction Histograms

An edge direction histogram (EDH) collects all edge directions in a block and shows a discrete distribution. Edge direction values may be computed by the Sobel edge operator [4]. After applying the Sobel edge operator to a grayscale document image, a watermark can be embedded in a block utilizing the resulting edge values, as described in Kim and Oh [3]. In our method, first we apply the Sobel operator to get an edge direction image and then quantize it into 16 levels. We then quantize the directions into 16 codes. Figure 3.1 shows the encoding of edge directions. More specifically, we acquire edge directions by the Sobel x-mask and y-mask to get the edge values of the x and y directions, respectively, and then apply the arc tangent operator to obtain the degree values of the directions. Finally, we quantize the degree values into 16 levels. Figure 3.2 is an example of edge direction value computation. Figure 3.2(a) shows the gray values of pixels in a 3×3 block, (b) and (c) are the Sobel masks G_x and G_y of the x -direction and the y -direction, respectively. Figure 3.2(d) and (e) are the results of (a) after applying the Sobel x and y masks. Figure 3.2(f) is an edge direction image which is created by the following formula:

$$G_d = \tan^{-1}(G_y/G_x). \quad (3.1)$$

Because the range of arc tangent is from $-90^\circ \sim +90^\circ$, it is necessary to modify the degree of arc-tangent to be from 0° to 360° as shown in Figure 3.2(f). Finally, Figure 3.2(g) shows the result of (f) after quantizing the edge direction values into 16 levels.

An EDH with direction levels in the range $[0, 15]$ is a discrete function $H(r_k)=n_k$, where r_k is the k th edge direction level and n_k is the number of edge directions after

applying the Sobel masks. Like the definition of histogram, an EDH also needs to be normalized by dividing each of its values by the total number of edge directions, denoted by sum . As a result, a normalized EDH is given by $p(r_k)=n_k/sum$, for $k = 0, 1, \dots, 15$, where $p(r_k)$ are an estimate of the probability of edge direction level r_k . The sum of all the components of the normalized EDH is equal to 1. Different from the general definition of histogram, because we can apply the Sobel operator to each block to get an edge direction histogram, there are many edge direction histograms in an image.

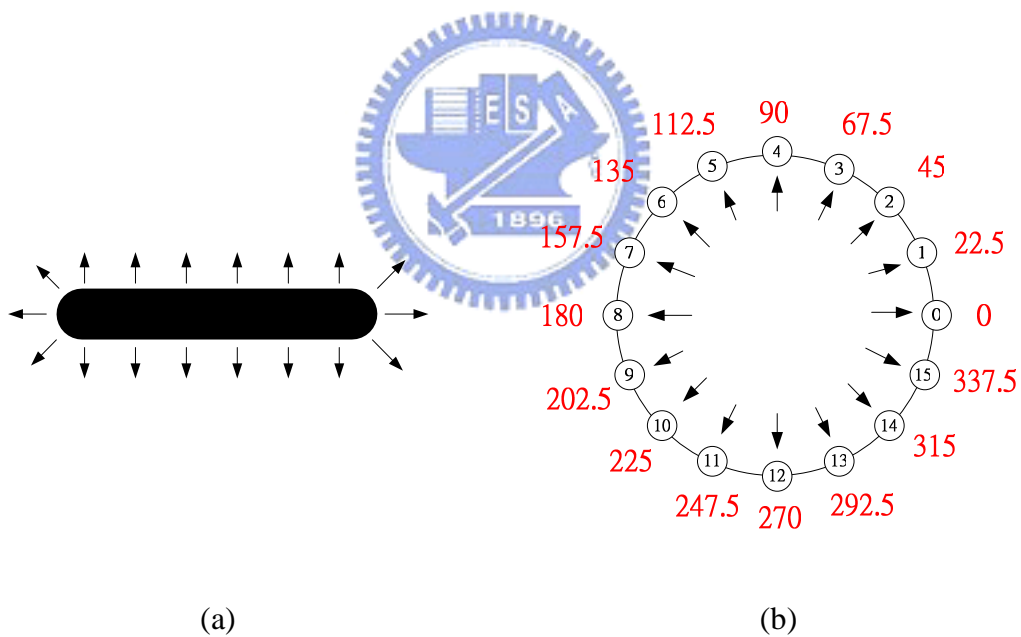


Figure 3.1 Encoding of edge direction. (a) Edge direction. (b) Edge direction quantized into 16 levels.

70	0	0	0	0
71	81	78	75	74
72	78	79	71	74
70	83	77	73	71

(a)

-1	0	1
-2		2
-1	0	1

 G_x

1	2	1
0		0
-1	-2	-1

 G_y

(b)

(c)

81	-133	-6	-4	-75
240	-49	-19	-13	-221
320	28	-30	-20	-290
244	21	-27	-17	-217

$$G_x(2,2) = 70 \cdot -1 + 71 \cdot -2 + 72 \cdot -1 + 0 \cdot 1 + 78 \cdot 2 + 79 \cdot 1 = -49$$

(d)

-223	-311	-312	-302	-223
-82	-237	-307	-295	-219
0	-2	2	8	8
222	307	307	295	219

$$G_y(2,2) = 70 \cdot 1 + 0 \cdot 2 + 0 \cdot 1 - 72 \cdot 1 - 78 \cdot 2 - 79 \cdot 1 = -237$$

(e)

290	246.8	268.9	269.2	251.4
341.1	258.3	266.5	267.5	224.7
0	355.9	176.2	158.2	178.4
42.3	86.1	95	93.3	134.7

Edge Direction

$$G_d(2,2) = \tan(G_y/G_x) = 78.3$$

$$G_d(2,2) + 180 = 258.3$$

(f)

13	11	12	12	11
15	11	12	12	10
0	0	8	7	8
2	4	4	4	6

Quantized Directions

(g)

Figure 3.2 An example of edge direction value computation. (a) Several pixels. (b) The x -direction Sobel mask G_x . (c) The y -direction Sobel mask G_y . (d) and (e) The result of (a) after applying G_x and G_y mask, respectively. (f) Edge direction using (3.1). (g) The result after quantizing the edge direction of (f) into 16 levels.

3.1.4 Definition of Circular Interpretation

The meaning of circular interpretation is to map a histogram into a circle [6]. In our method, an edge direction histogram with circular interpretation means to map an EDH to a circle, which is called EDH circle. The position of an EDH value on the circle is a weight proportional to the occurrence of the edge strength. The position of the center of mass in the EDH circle is the result of the weight distribution, as shown in Figure 3.3(b) where C_1 is the center of the mass of the circle. Figure 3.3 shows an example of circular interpretation and the center of mass in the EDH circle.

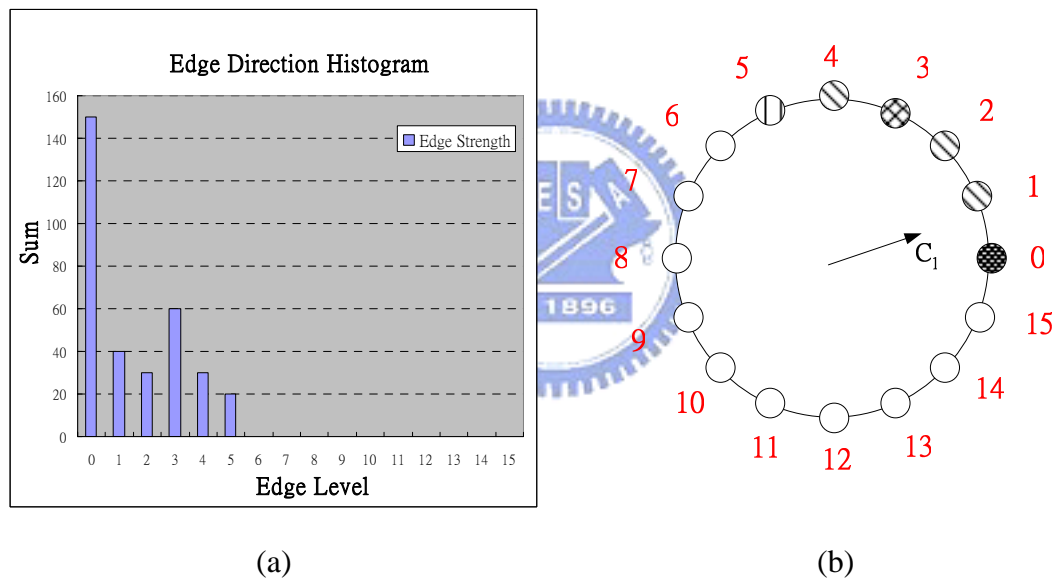


Figure 3.3 The edge direction histogram mapped into a circle. (a) Edge direction histogram. (b) A circle mapped by (a).

3.2 Idea of Watermark Embedding Method

The proposed watermark embedding method is based on a pixel-level watermarking algorithm for grayscale document images. It means that a watermark can be embedded by modifying the gray values of pixels. Instead of adopting the way

of processing an image in the unit of a constant-sized block, we use arbitrary-sized blocks to carry the watermark. The size of a block may be a word created by connected component merging described in Chapter 2. In this study, the text of a line is regarded as a block unit for embedding a watermark signal, though it is not limited to do so.

On the other hand, the concept of mother and child blocks is employed in this study. A mother block can be seen as a reference block and we modify the gray values of the pixels in the child block to embed signals. The center of mass in the EDH circle is calculated both in the mother and in the child blocks. By adjusting the location of the center of mass in the EDH circle in the child blocks according to the embedded data, the child blocks can carry the watermark signals.

3.3 Watermark Embedding Process

3.3.1 Proposed Technique Using Edge Direction Histograms with Circular Interpretation to Embed Watermarks

As mentioned previously, the size of a block does not need to be fixed in the proposed method. An advantage of using a fixed-sized block is that a page layout analysis program is not required. However, a drawback of using fixed-sized blocks is being less robust. It means that the embedded watermark signals can not survive attacks by line removing or cropping. In our method, we use a line to embed watermark signals.

By our experiments, because the location of the mass of center in the EDH circle of the document images of similar languages are similar and because modifying the

mass of center in the EDH circle a little does not cause a significant effect on the resulting visual quality, we can hide data by modifying the mass of center in the EDH circle slightly. The concept behind the proposed method is to use the similar location of the center of mass in the EDH circle between the mother and the child blocks with the same language. In detail, both the centers of mass in the EDH circles in the mother and in the child blocks are calculated. And then by adjusting the location of the center of mass in the EDH circle in the child block according to the embedded data, the child block can be made to carry the watermark signals.

First, we partition the image into non-overlapping blocks, choose a mother block, and assign the remaining as child blocks. The mother block could be seen as a reference block and plays an important role in the watermark embedding process. After selecting the mother and the child blocks, we apply the Sobel operators to obtain the EDHs of two blocks and then map them into a circle. The location of the center of mass in the EDH circle is a result computed from the weight distribution. Then, we calculate the vector pointing from the geometric center of the EDH circle to the center of mass (COM) of the EDH circle both in mother and child blocks. In our method, we call this vector a COM vector. The proposed method is to use the relationship between two COM vectors to embed a watermark.

More specifically, because the mother block is a reference block, the location of the COM vector will not be changed. On the contrary, we adjust the location of the COM vector in the child block to embed a watermark signal. That is, we make a slight rotation of the COM vector in a child block to embed a bit of information. In our method, if the two COM vectors from the mother block to the child block are clockwise, it is regarded to represent a “1;” otherwise, a “0.” Figure 3.4 shows an example. Figure 3.4(a) and (b) show a mother block and a child block and their COM

vectors in the EDH circles. In Figure 3.4(c) and (d), the COM vector V_m in the mother block is fixed, and the COM vector V_c in the child block is rotated to embed a watermark bit, and in this way (c) is shown to embed a “0,” and (d) to embed a “1.”

If an image suffers from attacks, a COM vector will also be changed slightly. So, In order to increase robustness, we establish a threshold θ_T to promise the relationship between the positions of COM vectors in the mother and child block. For instance, if θ from the COM vector V_m in the mother block to the COM vector V_c in the child block in Figure 3.4(c) or (d) is smaller than θ_T , then we adjust the location of the COM vector in the child block to enlarge θ . The range of V_c is shown in Figure 3.5.

The embedding rule relies on the fact that the COM vectors in the mother and child blocks are close to each other before embedding watermark signals. And the hypothesis is reasonable because the shape with one language is similar, as mentioned previously. However, there is one particular case which need be noticed. If the center of mass is equal to the center in an EDH circle, then we treat this case as $\theta < \theta_T$, and modify the COM vector to embed a watermark signal.

Now, how to rotate the COM vector in the child block is our main concern. If the direction from the COM vector of the mother block to that of the child block is counterclockwise and it is needed to embed a “1,” which is represented by a clockwise direction, or if the direction is clockwise but $\theta < \theta_T$, then we have to increase the weight of the EDH in the opposite direction to allow the COM vector in the child block to rotate in the clockwise direction.

The location of the center of mass in the EDH circle can be adjusted by changing the weight of the position of an EDH value on the circle. And the weight of the position of an EDH value can be modified by changing the gray values of the pixels with the same edge direction. Figure 3.6 is an example of changing the edge direction

by modifying the gray values of pixels in a block. After we change the value of the edges with the same directions to another value, the weight of the position of an EDH value on the EDH circle will also be changed. In Figure 3.6(a), the edge direction is 3, and if it is needed to change it to the opposite direction, for example, 2, 1, 0, 15, and so on, we may modify the gray values of the pixels to achieve our goal, as shown in (b). After doing the same procedure several times, the location of the center of mass of the child block will be modified as desired.

On the other hand, let the angle of the direction from the COM vector V_m in the mother block to the COM vector V_c in the child block be denoted as θ . If $\theta < \theta_T$, then we need to enlarge θ in order to increase the robustness.

Why the proposed watermark embedding technique is robust comes from the fact that most attacks do not break the relationship between the sharp region and the smooth region, in which we embed the watermark signal. By our experiments and observation, this embedding technique is not suitable for color images and the reason is that the sharp region is easy to be perceived by the human vision, whereas this technique is specially useful for dealing with text-dominating grayscale document images, because the location of the mass of center in the EDH circle of the document images of similar languages are similar and because modifying the mass of center in the EDH circle a little does not cause a significant effect on the resulting visual quality. The results also show that the resulting distortion in grayscale document images is less.

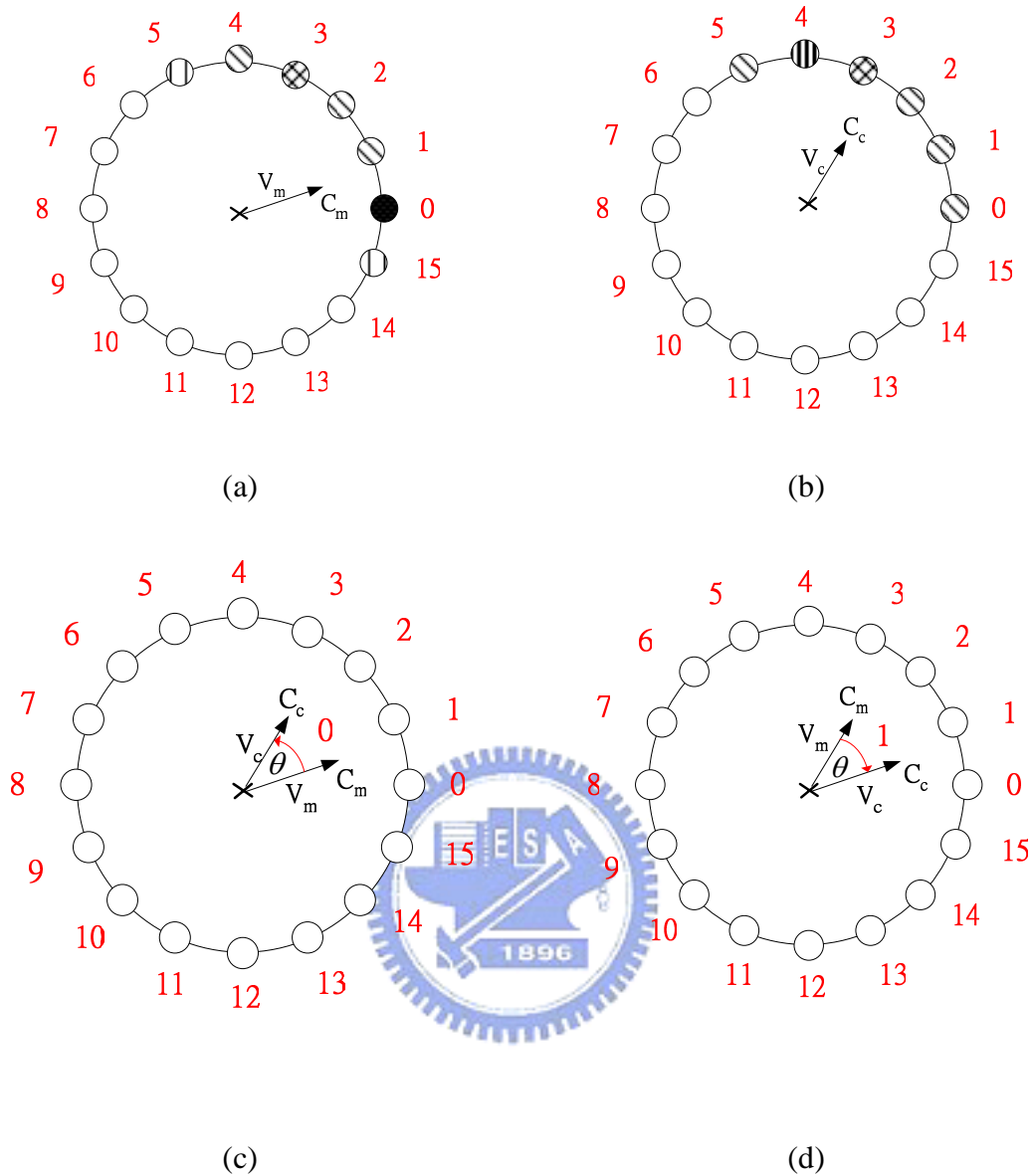


Figure 3.4 An illustration of the proposed watermark embedding algorithm. (a) A mother block and the COM vector V_m . (b) A child block and the COM vector V_c . (c) An example to embed a “0” with two COM vectors being counterclockwise. (d) An example to embed a “1” with two COM vectors being clockwise.

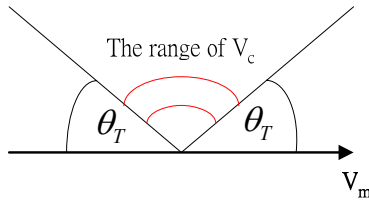


Figure 3.5 The range of V_c

70	70	70
0		70
0	0	0

Degree=63.43

Quantized Direction = 3

(a)

70	70	70
0		70
0	70	70

Degree=18.43

Quantized Direction = 1

(b)

Figure 3.6 An illustration of changing the edge direction by modifying the gray values of pixels.



3.3.2 Detailed Algorithm

The input to the proposed watermark embedding process includes a grayscale document image I and a watermark W . The output is a stego-image S . The algorithm for the process can be briefly expressed as follows. Figure 3.7 shows a flowchart of the process.

Algorithm 1: *Watermark embedding process.*

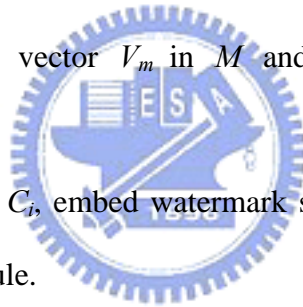
Input: A given grayscale document image I and a watermark W .

Output: A stego-image S .

Steps:

- 1 Convert W into a binary form $w_1w_2w_3\dots w_L$.

- 2 Divide I into a set of non-overlapping primitive blocks.
- 3 Select a mother block M and choose the remaining blocks $C_1, C_2 \dots C_n$ as child blocks.
- 4 For the mother block M and each child block C_i , construct the an edge direction histogram in the following way:
 - 4.1 Apply the Sobel masks and get an edge direction by (3.1).
 - 4.2 Quantize the edge direction values into 16 levels.
 - 4.3 Accumulate the number of pixels with the same edge direction levels.
 - 4.4 Compute the normalized edge direction histogram as a final EDH.
- 5 Map the EDH of the mother block M and that of each child block C_i into circles to be EDH circles.
- 6 Calculate the COM vector V_m in M and V_c in each child block C_i , respectively.
- 7 For each child block C_i , embed watermark signals, one bit per child block, using the following rule.
 - 7.1 If the bit is 0, and θ from V_m to V_c is clockwise or $\theta < \theta_T$, then modify the location of the center of mass in the EDH circle in the child block to make the two COM vectors from the mother block to the child block to be counterclockwise and $\theta > \theta_T$.
 - 7.2 If the bit is 1, and θ from V_m to V_c is counterclockwise or $\theta < \theta_T$, then modify the location of the center of mass in the EDH circle in the child block to make the two COM vectors from the mother block to the child block to be clockwise and $\theta > \theta_T$.
- 8 Take the final result as the desired stego-image S .



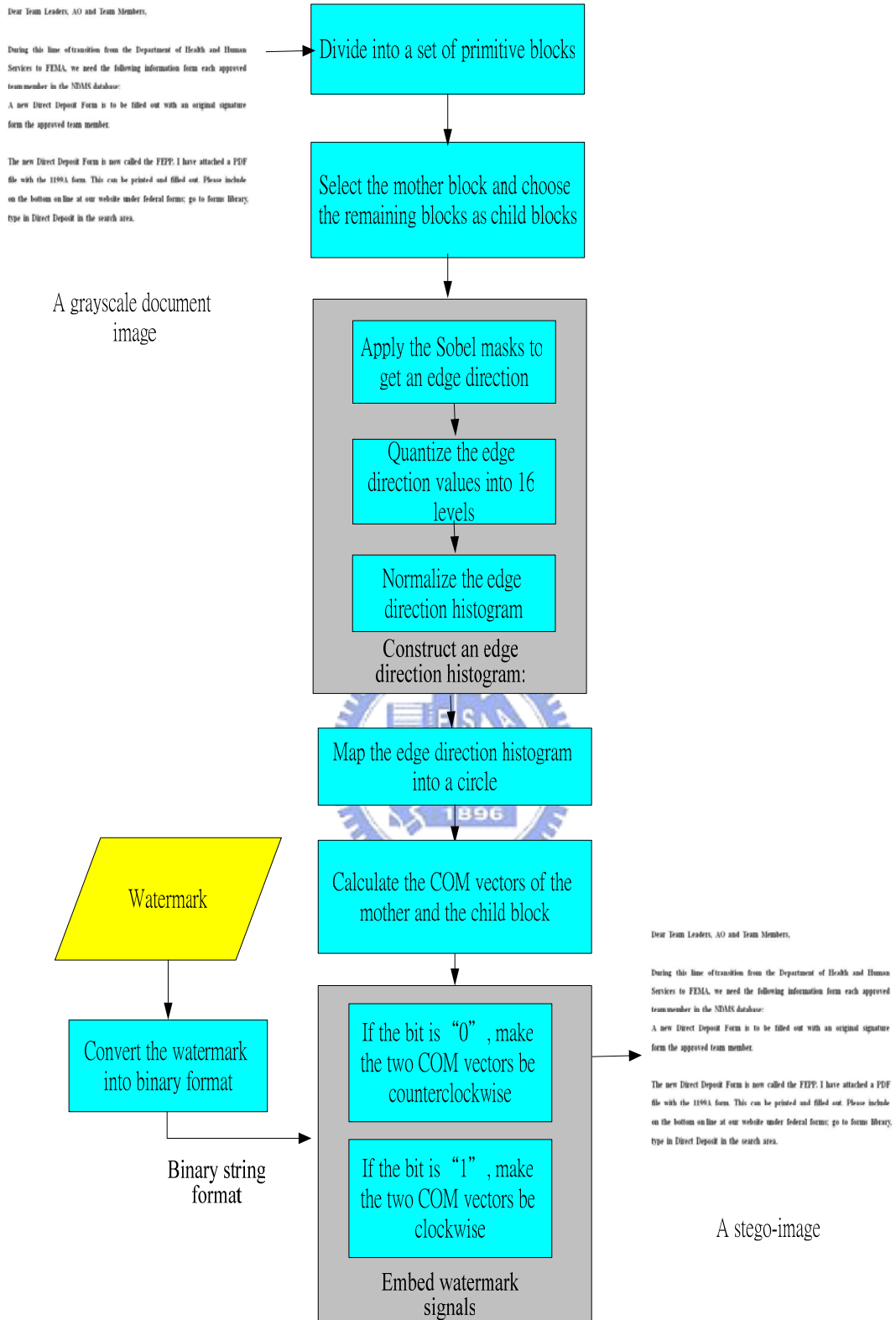


Figure 3.7 Flowchart of the proposed watermark embedding process

3.4 Watermark Extraction Process

3.4.1 Extraction of Watermarks

The watermark extraction procedure is similar to the embedding procedure but in a reverse order. In the extraction procedure, the mother block and the child blocks acquired are the same as those obtained the embedding procedure. We apply the Sobel masks to the mother and child blocks to get edge direction values, and acquire the EDH circle which is the same as that obtained in the watermark embedding procedure. The COM vectors are calculated both in the mother and child blocks. By evaluating the direction from the COM vector in the EDH circle in the mother block to the COM vector in the EDH circle in the child block and checking whether it is clockwise or counterclockwise; we can extract the watermark embedded in the child block. Figure 3.8 shows a flowchart of the proposed extraction process.

3.4.2 Detailed Algorithm

Algorithm 2: *Watermark extraction process.*

Input: A given stego-image S .

Output: A watermark W .

Steps:

- 1 Divide I into a set of non-overlapping primitive blocks as done by the watermark embedding algorithm.
- 2 Select the mother block M and child blocks in the same way as done in the embedding process.

- 3 For the mother block M and each child block C_i , construct the an edge direction histogram in the following way:
 - 3.1 Apply the Sobel masks to get an edge direction image by (3.1).
 - 3.2 Quantize the edge direction values into 16 levels.
 - 3.3 Accumulate the number of pixels with the same edge direction levels.
 - 3.4 Compute the normalized edge direction histogram as a final EDH.
- 4 Map the EDH of the mother block M and that of each child block C_i into EDH circles.
- 5 Calculate the COM vector V_m in M and V_c in each child block C_i , respectively.
- 6 For each child block C_i , extract watermark signal, one bit per child block, using the following rule:
 - 3.1 If the direction from V_m to V_c is counterclockwise, then the watermark signal is “0”.
 - 3.2 If the direction from V_m to V_c is clockwise, then the watermark signal is “1.”
- 7 Take the final result as the desired watermark W .



Dear Team Leader, AO and Team Members,

During this time of transition from the Department of Health and Human Services to FEMA, we need the following information from each approved team member in the NIMS database:
A new Direct Deposit Form is to be filled out with an original signature from the approved team member.

The new Direct Deposit Form is now called the FEPP. I have attached a PDF file with the 1199A form. This can be printed and filled out. Please include on the bottom on line at our website under federal forms; go to forms library; type in Direct Deposit in the search area.

A Stego-image

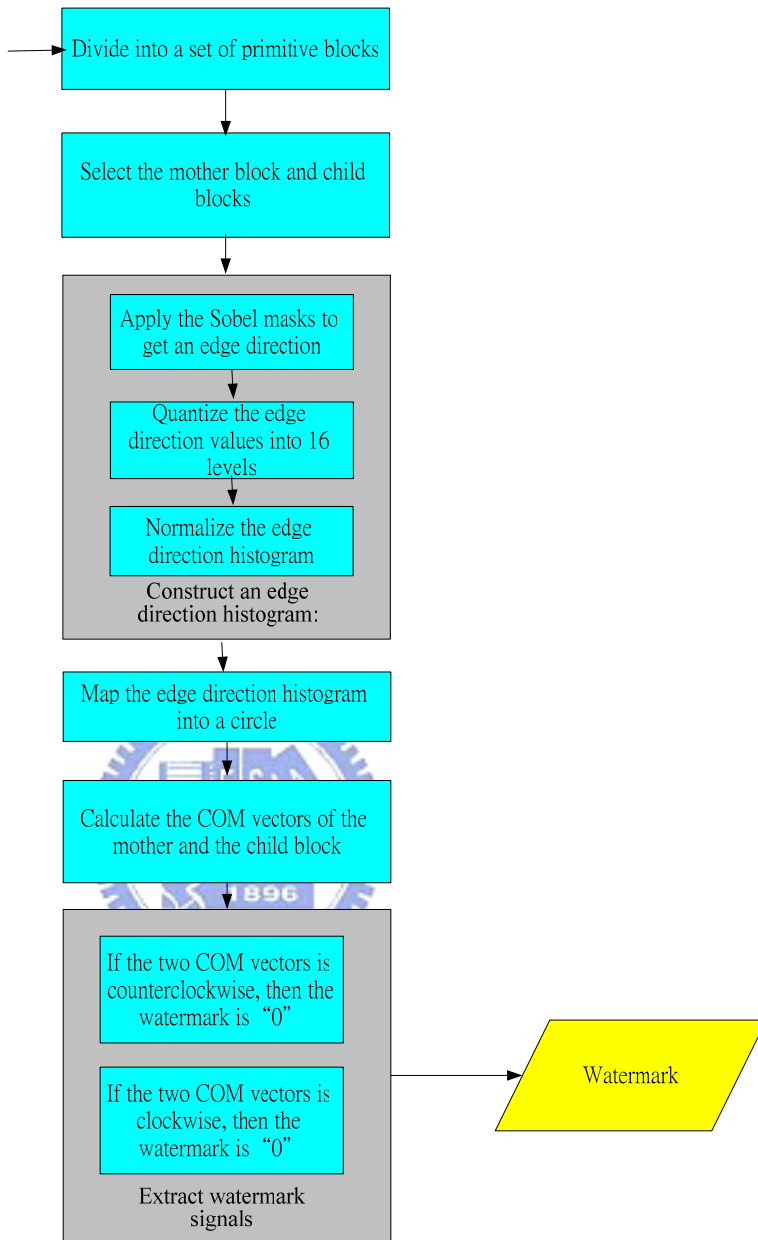


Figure 3.8 A flowchart of the proposed extraction watermark process

3.5 Experimental Results

In our method, the line-based block as a unit to embed a watermark signal is illustrated. Some experimental results of applying the proposed method are shown here. The threshold θ_T is set to be 3° . Figure 3.9 and Figure 3.10 are two grayscale Chinese and English document images, respectively, both with the size of 512×512 . And the watermark is a bit string of 101010.

Figure 3.9(a) and (b) show the grayscale Chinese document image before and after applying the proposed watermarking embedding algorithm. In addition, Figure 3.9(c) shows the degree value of the angle of the COM vector V_m in the mother block, and the mother block in this example is the first line. Figure 3.9(d) and (e) show the resulting degree values of the angle of the COM vector V_c in the child block before and after applying the watermark embedding procedure. Figure 3.10 is another example. The watermark was embedded in lines 2, 3, 4, 5, 6, 7. As we can see, the degree values of the angle of the COM vector V_m in the mother block and in the child blocks have been changed to be clockwise or counterclockwise according to the embedded signals after the watermark signal has been embedded in the child block. Table 3.1 shows the PSNR values of the stego-images after embedding the watermarks, which show that the quality of each of the stego-images is still good. And the embedded watermark is imperceptible by human vision. Table 3.2 shows various attacks and the signal detection results. The results show that the proposed embedding watermark method is robust, and the embedded watermark signals can survive several types of attacks.

北八卦山區因過度開發，造成有些自然生態慘遭破壞，經八卦山昆蟲生態農場兩年積極努力下，復育螢火蟲、樹蛙等正向的生態鏈成果豐碩，從四月下旬開始，將亮麗又熱鬧的開放教學與參觀，將成為生態教育的新樂園。

北八卦山區因過度開發，造成有些自然生態慘遭破壞，經八卦山昆蟲生態農場兩年積極努力下，復育螢火蟲、樹蛙等正向的生態鏈成果豐碩，從四月下旬開始，將亮麗又熱鬧的開放教學與參觀，將成為生態教育的新樂園。

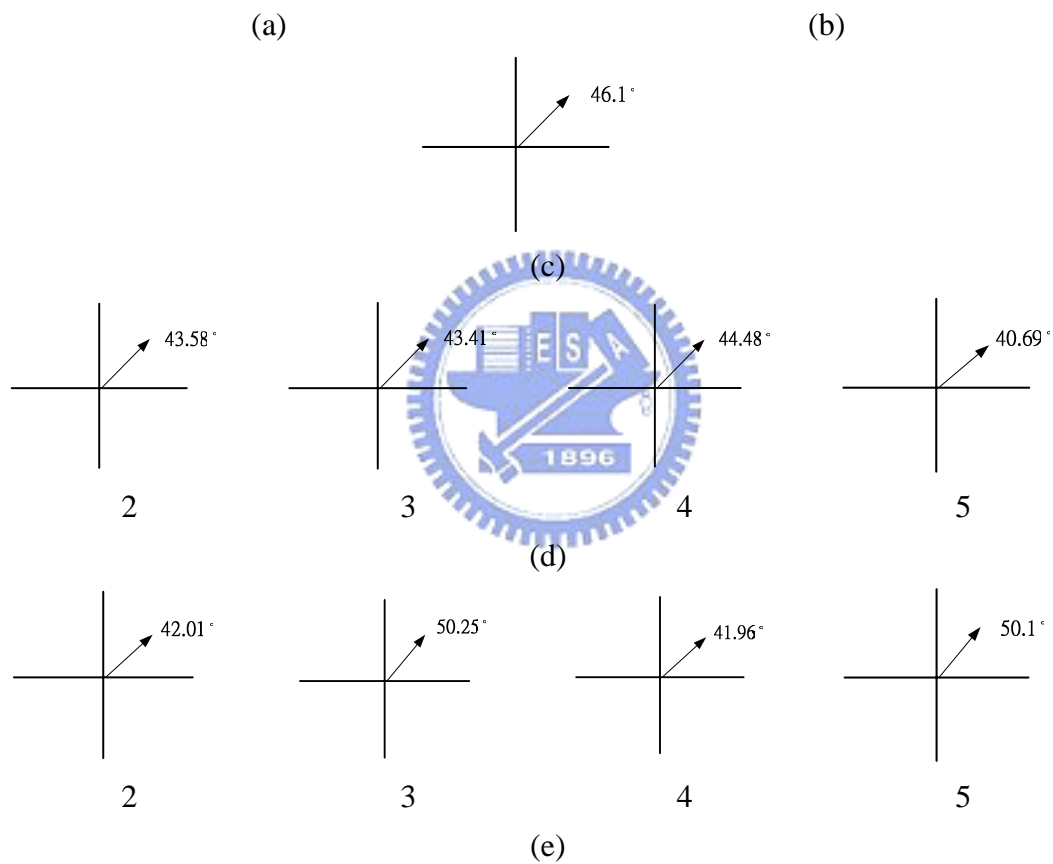


Figure 3.9 An example of line-based block watermarking in a Chinese document image. (a) and (b) Images before and after watermarking. (c) The degree value of the angle of the COM vector V_m in the mother block. (d) and (e) The degree values of the angles before and after embedding a watermark signal.

On the 80th anniversary of Malcolm X's birthday we play excerpts of the documentary, "Malcolm X: Make it Plain" produced and directed by Orlando Bagwell. It includes rare archival footage of Malcolm X as well as interviews with such figures as John Henrik Clarke, Maya Angelou, Ossie Davis and much more.

On the 80th anniversary of Malcolm X's birthday we play excerpts of the documentary, "Malcolm X: Make it Plain" produced and directed by Orlando Bagwell. It includes rare archival footage of Malcolm X as well as interviews with such figures as John Henrik Clarke, Maya Angelou, Ossie Davis and much more.

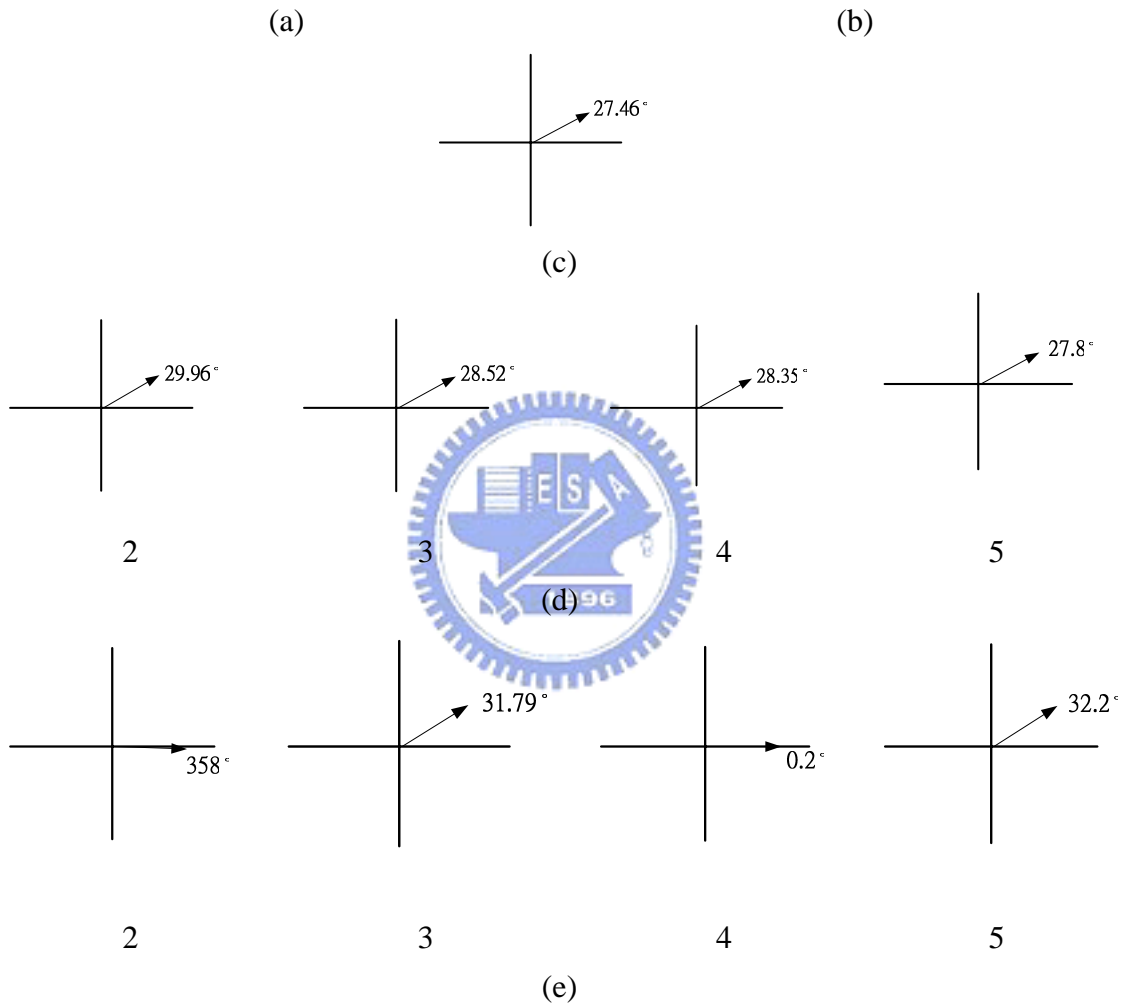


Figure 3.10 An example of line-based block watermarking in an English document image. (a) and (b) Images before and after watermarking. (c) The degree value of the angle of the COM vector V_m in the mother block. (d) and (e) The degree values of the angles before and after embedding a watermark signal.

Table 3.1 The PSNR values of recovered images after embedding watermarks.

	Chinese Document Images	English Document Images
PSNR	39.8	36.1

Table 3.2 Various attacks and signal detection result

	English document	Chinese document
No attack	1010	1010
5% Noise	1010	1010
10% Noise	1010	1010
20% Noise	1010	1111
Blurring	1010	1010
Sharpening	1010	1010
Blurring and sharpening	1010	1010

3.6 Discussions and Summary

In this chapter, we have proposed a method for embedding a watermark into a grayscale document image using edge direction histograms with circular interpretation and the relationship between the mother block and the child blocks. Because the location of the mass of center in the EDH circle of the document images of similar languages are similar and modifying the mass of center in the EDH circle a little does not cause a significant effect on the resulting visual quality, we can hide data in a grayscale document image by modifying the mass of center in the EDH circle slightly. We map the EDH into a circle and compute the center of mass from the resulting weight distribution in the EDH circle. By modifying the location of the COM vector in the child blocks, the watermark could be embedded in the child block. If θ from the COM vector in the EDH circle in the mother block to the COM vector in the EDH

circle in the child block is counterclockwise, it means to embed a “0” into the child block; on the contrary, it means to embed a “1.” The experimental results show that the distortion is less perceivable after embedding the watermark signal, and the robustness of the proposed method for different kinds of attacks proves that the watermark can survive after multiple attacks.



Chapter 4

A Fragile Authentication Method for Color Images

In this chapter, a method for authentication of color images by a fragile watermarking technique is proposed. The relationship between a mother and child blocks is used to embed an authentication signal. The authentication signals are created by the key, and the selection of the mother block is carried out with another key. The integrity of images can be verified by comparing the difference between the key and the extraction result of the authentication signals.

The remainder of this chapter is organized as follows. In Section 4.1, an introduction is given first. In Section 4.2, the idea of the proposed method is described. In Section 4.3, the process of authentication signal embedding is described. In Section 4.4, the process of authentication signal extraction is presented. Finally, in Section 4.5, some discussions and summary are made.

4.1 Introduction

Because image transmission is a major activity in today's communication and images are easy to duplicate or tamper with, it is possible for these images to be used illegally. As a result, it is necessary to design an effective algorithm for color image authentication. We propose a method here for image authentication to verify the image to be tampered with or not.

4.2 Proposed Idea of Embedding Authentication Signals

In this section, the proposed idea for image authentication in color images is described. The relationship between the mother and child blocks is used to hide data. The block size of the mother block used in the proposed method is chosen to be 3×3 . The mother block is chosen from a 9×9 block. The remaining blocks in the 9×9 block are regarded as child blocks. In this proposed method, authentication signals and embedding locations are generated by two keys. The first key is to choose the location of the mother block and assign the remaining blocks as the child blocks in each 9×9 block. And the second key is used to create authentication signals which contain 8 bits. Authentication signals will be embedded in the child blocks and called authentication codes. The concept of edge direction described in Chapter 3 is also utilized to embed authentication signals. By modifying the degree of the edge direction of the child blocks, authentication codes can be embedded in them.

4.3 Authentication Signal Embedding Process

4.3.1 Embedding of Authentication Signals

An input image is first divided into non-overlapping 9×9 blocks. Then, each 9×9 block is divided further into nine non-overlapping 3×3 blocks. Figure 4.1 shows an example of a 9×9 block and its nine 3×3 blocks.

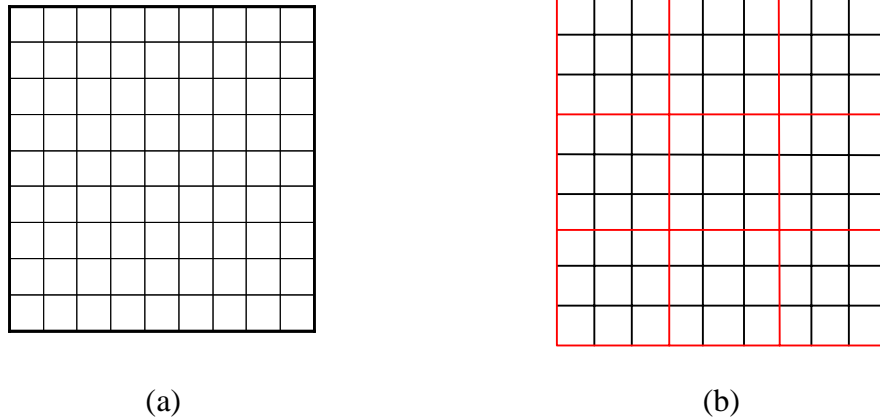


Figure 4.1 An example of 9×9 image blocks. (a) A 9×9 block. (b) Each 3×3 block in the 9×9 block.

A Selection of the location of the mother block and creation of the authentication signals using two keys.

In the proposed method, the two keys are used to enhance the security. The function of the first key K_1 is used to select the location of the mother block and assign the remaining blocks as child blocks. There are only nine 3×3 blocks in a 9×9 block. And only one block can become the mother block and the others are the child blocks. Figure 4.2 shows an example of selecting the mother and child blocks. Figure 4.2(a) is the indices of the locations of a 3×3 block and (b) shows the selection of the block with index 2 to be the mother block, and the others are the child blocks.

The function of the second key K_2 is used to create 8 bits of the authentication codes to be embedded in the child blocks. For instance, in Figure 4.2(b), if K_2 creates 8 bits which are $\{1, 0, 1, 0, 1, 0, 1, 0\}$, then we embed these authentication codes into the child blocks with indices of $\{1, 3, 4, 5, 6, 7, 8, 9\}$, respectively. So, in our method, each child block can embed one authentication code.

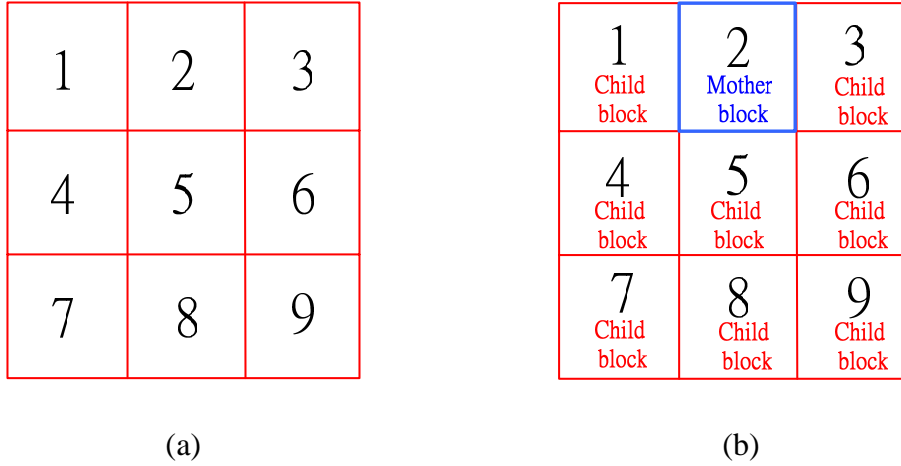


Figure 4.2 An example of selecting the mother and child blocks. (a) Indices of a 3×3 block. (b) The selection of the mother and child blocks.

B Authentication signal embedding process by edge direction.

The authentication signal embedding technique uses the edge direction. The definition of edge direction is described in Chapter 3 in detail. In short, we apply the Sobel operator to get an edge direction and then quantize it into 16 levels. The method to embed authentication signals is to adjust the edge direction according the input data. The proposed method uses the relationship of the edge direction between the mother and the child block to embed an authentication code. We call the edge direction in the mother block to be E_m , and the edge direction in the child block to be E_c . If the direction from E_m to E_c is clockwise, it represents a “1;” otherwise, a “0.”

How to modify the edge direction in the child block is our main concern. If the direction from E_m to E_c is counterclockwise and it is needed to embed a “1,” which is represented by a clockwise sign, we need to modify the gray values of the child block to make the edge direction rotate in the opposite direction. The opposite direction is the way to allow the edge direction to rotate in the clockwise direction. Figure 4.3 shows an illustration of changing the edge direction by modifying the gray values of

pixels.

During the authentication process we only need to compare the difference between the authentication codes created by K_2 and the extracted ones from the child blocks, and so verify the integrity of the stego-image. Figure 4.4 shows a flowchart of the proposed authentication embedding method.

According to our experiments, authentication signals can be embedded into the R channels without creating perceivable effects to human vision. And the gray values of the pixels in the blue and green channels are unchanged.

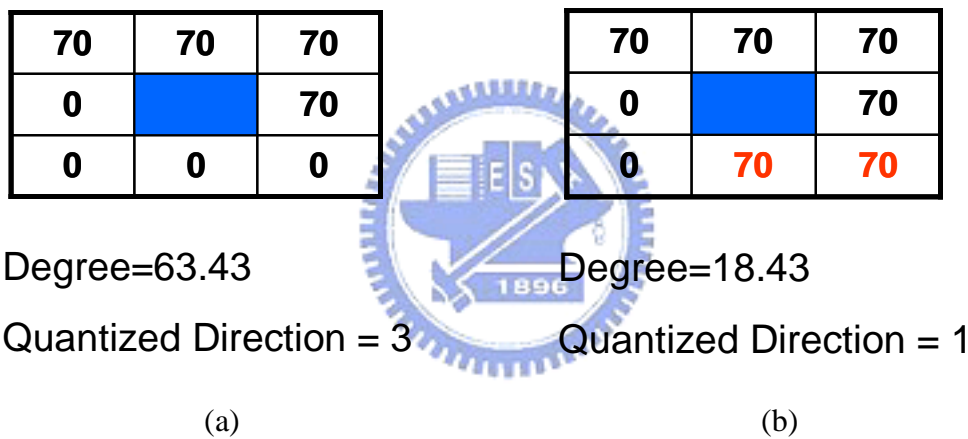


Figure 4.3 An illustration of changing the edge direction by modifying the gray values of pixels.

4.3.2 Detailed Algorithm

The input to the proposed authentication embedding process includes a color image I and two keys K_1 and K_2 . The output is a stego-image S . The algorithm for the process can be briefly expressed as follows. Figure 4.3 shows a flowchart of the algorithm.

Algorithm 1: *authentication signal embedding.*

Input: A given color image I and two keys K_1 and K_2 .

Output: A stego-image S .

Steps:

- 1 Divide I into non-overlapping 9×9 blocks.
- 2 For each 9×9 image block, divide it further into nine non-overlapping 3×3 blocks.
- 3 Select the mother block M and child blocks C_i by K_1 .
- 4 For M and each child block C_i , construct an edge direction in the following way.
 - 4.1 Apply the Sobel masks and get an edge direction
 - 4.2 Quantize the edge direction values into 16 levels.
- 5 Set the edge direction in the mother block to be E_m , and the edge direction in the child block to be E_c .
- 6 For M and each child block C_i , embed authentication codes which are created by K_2 into each child block by the following rule:
 - 6.1 If the authentication code is “1”, then set the direction from E_m to E_c to be clockwise.
 - 6.2 If the authentication code is “0”, then the direction from E_m to E_c to be counterclockwise.
- 7 Take the final result as the desired stego image S .

4.4 Authentication Signal Extraction Process

4.4.1 Extraction of Authentication Signals

The authentication signal extraction process is quite similar to the embedding procedure but in a reverse order. The two keys K_1 and K_2 are needed for the extraction process. During the authentication method, the stego image is partitioned into non-overlapping 9×9 blocks and each 9×9 block is partitioned further into nine non-overlapping 3×3 blocks. The key K_1 is used to select the mother block and assign the remaining as the child blocks. Similar to the authentication signal embedding method, we apply the Sobel operator to get an edge direction and then quantize it into 16 levels the same as the authentication signal embedding process.

By evaluating the direction from E_m to E_c to be clockwise or counterclockwise; we can know the authentication codes embedded in the child block. By comparing the difference between the authentication codes generated by K_2 and the extracted ones from the child blocks, we can verify the integrity of the stego image. Figure 4.5 shows a flowchart of the proposed authentication process.

4.4.2 Detailed Algorithm

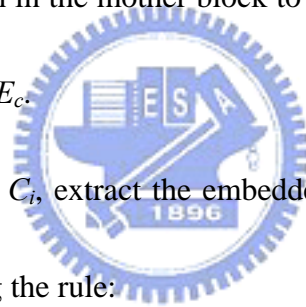
Algorithm 2: *Image authentication process.*

Input: A given stego image S and the two keys K_1 and K_2 the same as the authentication embedding process.

Output: An authentication image A .

Steps:

- 1 Divide S into non-overlapping 9×9 blocks.
- 2 For each 9×9 image block, divide it further into nine non-overlapping 3×3 blocks.
- 3 Select the mother block M and child blocks C_i by K_1 .
- 4 For M and each child block C_i , construct an edge direction in the following way.
 - 4.1 Apply the Sobel masks and get an edge direction
 - 4.1 Quantize the edge direction values into 16 levels.
- 5 Set the edge direction in the mother block to be E_m , and the edge direction in the child block to be E_c .
- 6 For each child block C_i , extract the embedded authentication codes, one bit per child block, using the rule:
 - 6.1 If the direction from E_m to E_c is counterclockwise, then the authentication code is "0".
 - 6.2 If the direction from E_m to E_c is clockwise, then the authentication code is "1".
- 7 Compare the difference between the authentication codes extracted by the child blocks and created by K_2 . If there are not the same, then regard the 9×9 image block as being tampered with and mark it red.
- 8 Take the final result as the desired authentication image A .



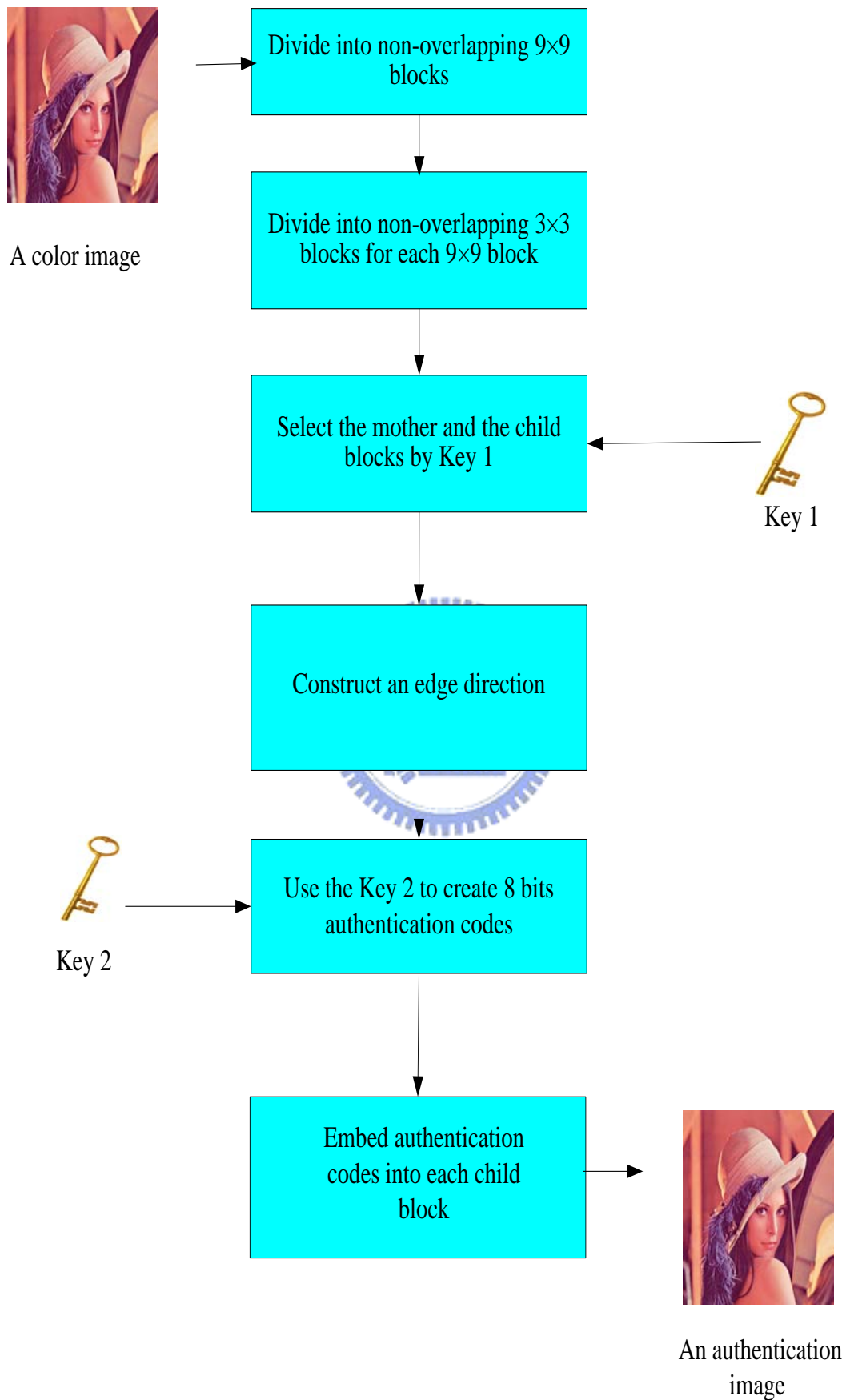


Figure 4.4 A flowchart of the proposed authentication signal embedding method.

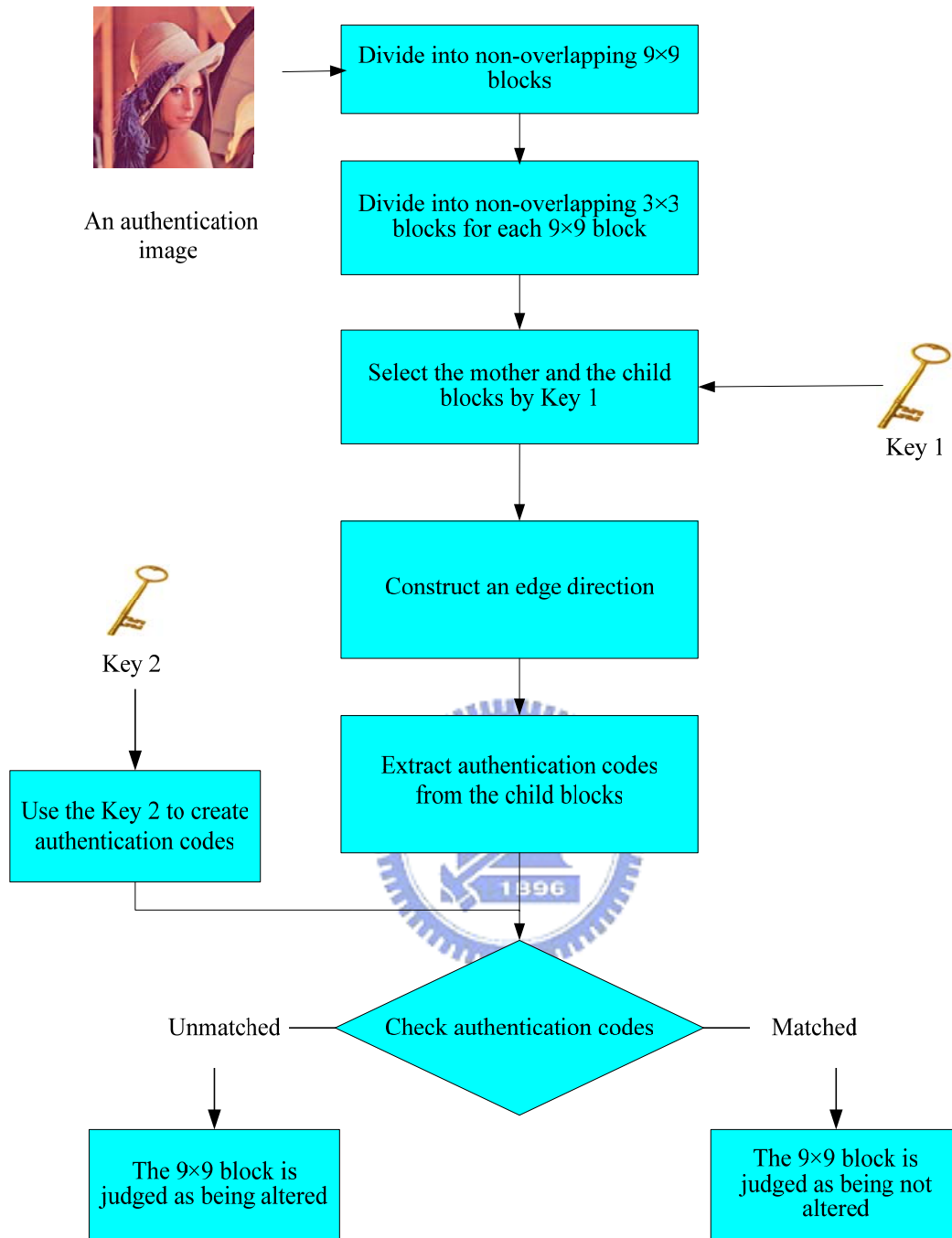


Figure 4.5 A flowchart of the proposed authentication process.

4.5 Experimental Results

In this section, some experimental results of applying the proposed method are shown. In the following example, the first Key K_1 is used to assign the number index of 1 to a block as the mother block and the remaining as the child blocks. The second

key K_2 is used to create authentication codes which are $\{0, 1, 0, 1, 0, 1, 0, 1\}$. The cover image size is 512×512 . Figure 4.6(a) is the color image of “Painting” and (b) shows the resulting stego-image after embedding the authentication codes. Figure 4.6(c) shows a tampered image with (b) and (d) showing the authentication result. And Figure 4.7 and Figure 4.8 are two others example with “Lena” and “Jet”, respectively. The corresponding PSNR values are shown in Table 4.1.

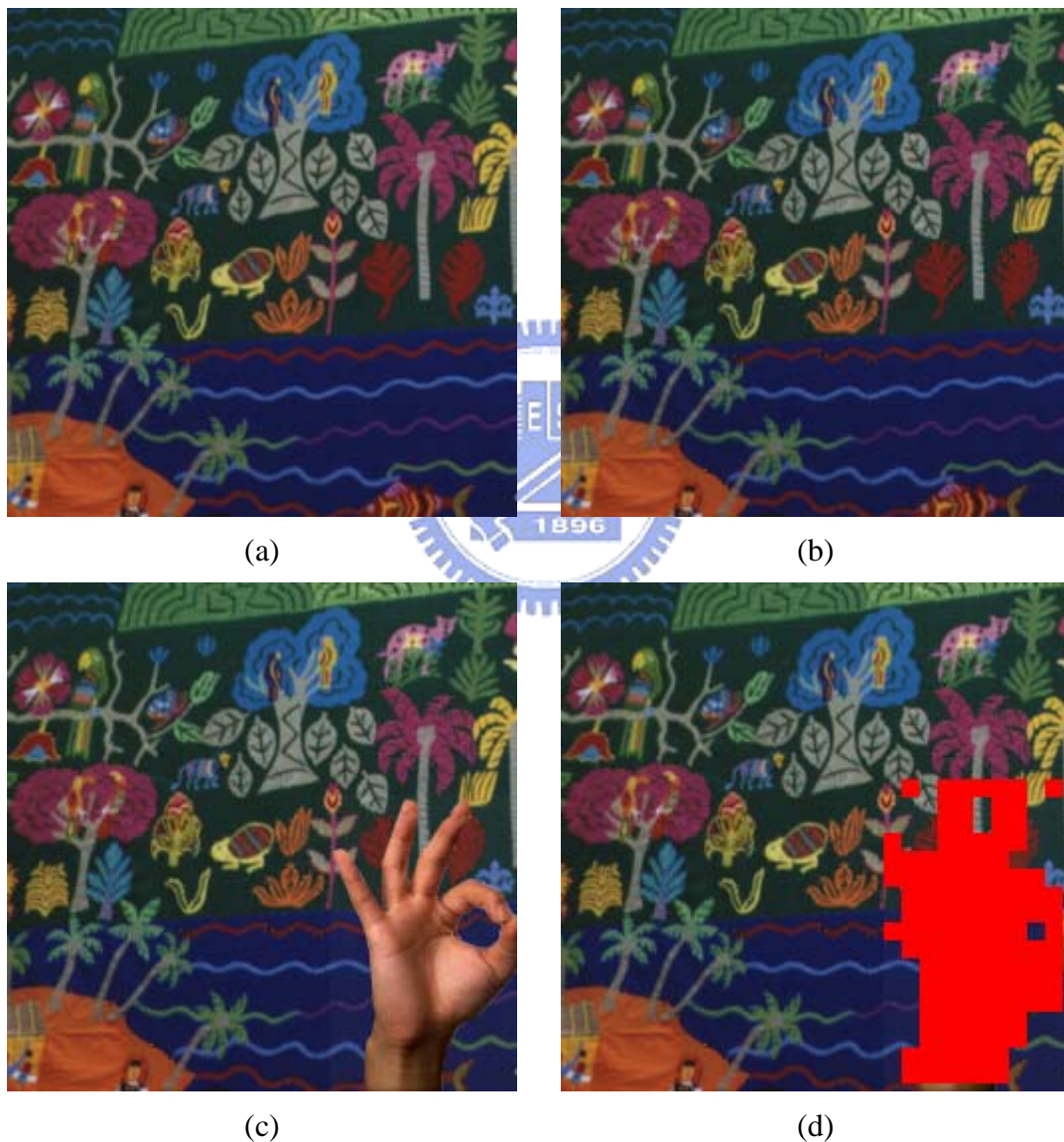


Figure 4.6 An example of results of applying proposed authentication method. (a) An image of “Painting”. (b) The stego image after embedding authentication codes. (c) Tampered image “Painting”. (d) Authentication result.



Figure 4.7 An example of results of applying proposed authentication method. (a) An image of “Lena”. (b) The stego-image after embedding authentication codes. (c) A tampered image of “Lena”. (d) Authentication result.

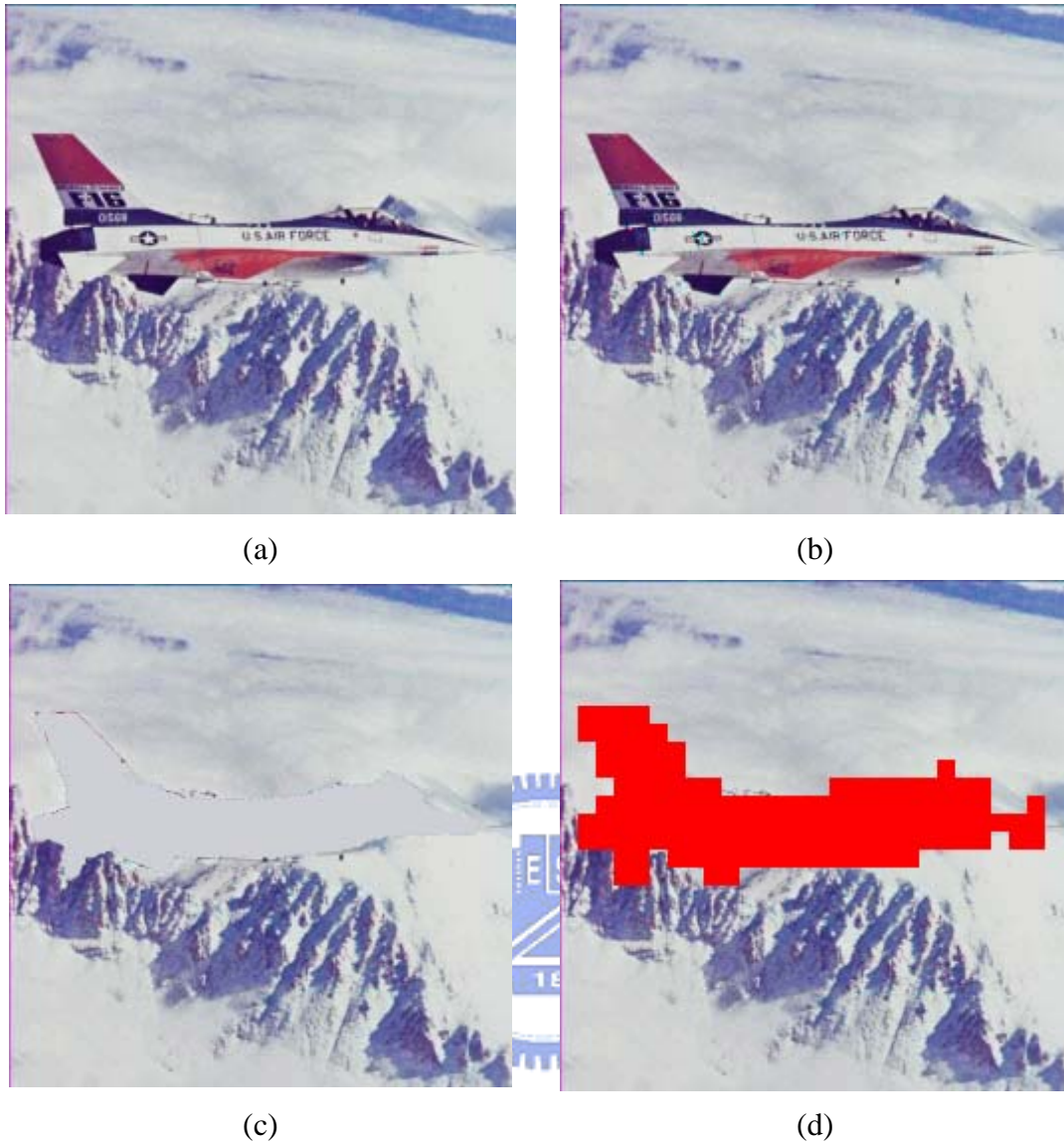


Figure 4.8 An example of results of applying proposed authentication method. (a) An image of “Jet”. (b) The stego-image after embedding authentication codes. (c) A tampered image of “Jet”. (d) Authentication result.

Table 4.1 The PSNR values of the stego-images after embedding the authentication signals.

	Painting	Lena	Jet
PSNR	34	37	35

4.6 Discussions and Summary

In this chapter, we have presented an authentication scheme to embed authentication signals into color images. We use K_1 to select the location for

embedding authentication signals and use K_2 to generate authentication codes. The proposed method uses the relationship between the mother and the child blocks to embed authentication signals. If someone tampers with the stego-image, the authentication codes extracted from the child block will be modified and can not be the same as the result of using the key K_2 . As a result, we can judge a stego-image to be tampered with and the modified areas can be detected and located.

However, because we process the cover image on the R channel which means if the tampering operations are only applied to the B or G channels, the modified areas cannot be detected by the proposed method. It may be tried to solve this problem in the future.



Chapter 5

A Watermarking Method for Copyright Protection of Binary Images

In this chapter, the proposed method for copyright protection of binary images is presented. The idea is based on rearranging all the pixels of the block by a reference table to embed binary information. Watermark retrieval can be achieved by verifying the location of the pixels of the block to extract the watermark signals.

The remainder of this chapter is organized as follows. In Section 5.1, an introduction is given first to digital watermarking and the research problem. In Section 5.2, the proposed watermarking method for copyright protection is described. In Section 5.3, the detailed algorithm of watermark embedding is presented. In Section 5.4, the detailed algorithm of watermark extraction is presented. In Section 5.5, some experimental results are given to show the feasibility of the proposed approach. Finally, in Section 5.6, some discussions and a summary are made.

5.1 Introduction

Digital Watermarking is a technique for embedding a watermark into an image to protect the owner's copyright of the image. One simple approach is to use LSB replacement, but it is not useful for binary images, since there are only two pixel values, black and white, in binary images. Therefore, the LSB does not exist in binary images. Because of the limited data embedding capacity, it is difficult to hide data into a binary image. In our survey, there have been few studies on data hiding in binary

images. The purpose of this chapter is to demonstrate how to embed watermark signals into a binary image without noticeable changes in the resulting image.

5.1.1 Properties of Binary Images

In a binary image, there are only two pixel values, 0 and 255, and the corresponding pixels may be called *black* and *white* ones, respectively. If data are embedded into a binary image, the values of the image pixels will be altered; this will usually yield noticeable artifacts in the resulting image. If we rearrange the pixels in the block in a more natural way, it is less likely for the embedded data to be noticed.

5.1.2 Problem Definition

In order to embed more data in a binary image, more pixels need to be changed. The quality of the image will then become worse. This is a trade-off problem. The proposed method for watermark embedding in binary images, therefore, is a compromise between the goal of embedding more data in a binary image and that of controlling the quality of the resulting image. Our method has the advantage of embedding 2 bits of data in a 4×4 block by rearranging the pixels via a reference table.

5.2 A Watermark Embedding Method

In this section, the proposed method for watermark embedding in a binary image is introduced. The main idea of the proposed method is to choose a suitable 2×2 block from each 4×4 block to embed watermark signals. In our method, we use the technique of *inverse halftoning*. The halftoning technique is used to convert grayscale images into binary ones. In this study, we modify the inverse halftoning technique

for generating watermark signals. Each 2×2 block of a given binary image is assigned a gray value.

5.3 Watermark Embedding Process

The watermark used for copyright protection is assumed to be a logo or a binary image, so the capacity for watermark embedding in a binary image is an important factor. If we want to embed a logo or an image into a binary image, we have to transform the logo or image into a watermark bit stream. In this section, the process of embedding a watermark bit stream into a binary image is described.

5.3.1 Embedding of Watermarks

To generate watermark signals for a binary image, the image is first divided into non-overlapping 4×4 blocks. Then, each 4×4 block is divided further into four non-overlapping 2×2 blocks. Figure 5.1 shows an example of a 4×4 block and its four 2×2 blocks.

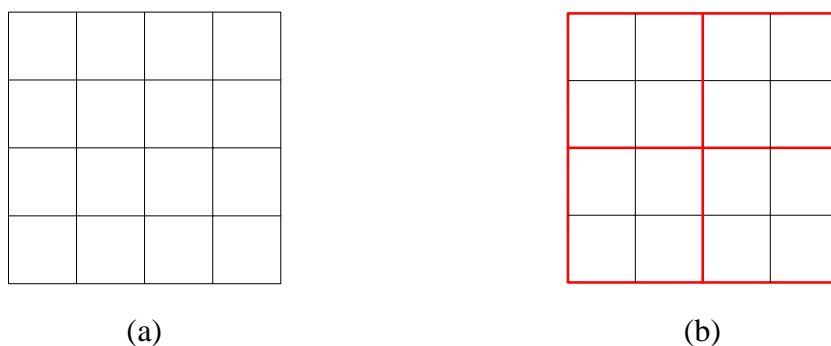


Figure 5.1 An example of 4×4 image blocks. (a) A 4×4 block. (b) Each 2×2 block in the 4×4 block.

A. Assigning Gray Values to 2×2 Blocks

In the modified inverse halftoning technique, we modify the RHG values of an image to assign a gray value to a 2×2 block, which was first proposed by Tsai and Huang [10]. The RHG value is the abbreviation of *reduced halftone gray* and an RHG function is used to convert grayscale images into binary ones. In Tsai and Huang's method, the use of the RHG function aims to process a binary image of the size of 9×9 block. However, in the proposed method, the size of a block to process a binary image is taken to be 4×4. It is, therefore, necessary to modify the RHG in a way as described here. That is, each 2×2 binary image block B is assigned a gray value G by the following RHG formula:

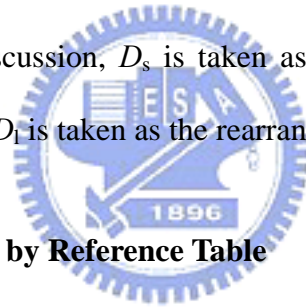
$$G = [(4-N) \times 255 / 4] \quad (5.1)$$

where N is the number of black pixels in B . The RHG value maps the range of gray values [0 255] into 4 discrete gray levels. That is, for an input N , B is assigned a gray value G which is one of the five values 0, 64, 128, 192, 256. For example, if N is 0, the RHG value is 256. If $N = 1$, then the RHG value is 192. If N is 4, the RHG value is 0. We use these RHG values to represent the gray values of each block, and then choose the candidates from the four blocks to embed watermark signals.

B. Choice of Rearrangeable Block

In order to control the quality of a binary image, we should carefully select a proper 2×2 block from a 4×4 block to embed watermark signals. Each block selected for this purpose is called a *rearrangeable block* in this study. For each 2×2 block, if their RHG value is 0 or 256 which means black or white entirely, we remove these blocks from the candidate block list. The reason is obvious, because if we make any change in an entirely black or white block, it will be easily noticed.

The way to select a proper block for embedding watermark signals is described next. One good choice of the block is that with its RHG value G_s being the smallest but not 0, and another choice is that with its RHG value G_l being the largest but not 255. A large RHG value means that there are fewer black pixels in the block, and a smaller RHG value means fewer white pixels. If we choose these blocks as a candidate to hide data, less distortion will be produced according to a human vision model. Take the smallest RHG value but not 0 as an example. It means that there are fewer white pixels in the block, so it will cause less distortion to rearrange the positions of these white pixels than to rearrange those of the black ones. Let w_s be the number of white pixels in the block D_s whose RHG value is G_s and b_l be the number of black pixels in the block D_l whose RHG value is G_l . If w_s is not larger than b_l , then according to the previous discussion, D_s is taken as the rearrangeable block in the proposed method; otherwise, D_l is taken as the rearrangeable block.



C. Rearrangement of Pixels by Reference Table








In this step, we have to set up a reference table T . The reference table is assumed to be held by the sender and the receiver, and the content of T contains the positions of the black pixels and the watermark bit stream. The value N_b in T means the number of black pixels obtained from the 2×2 rearrangeable block b . By table lookup, we will rearrange the positions of black pixels in b . Table 5.1 shows an example of the reference table.










In each 4×4 block B_i , we embed most three bits into the rearrangeable block b . The way we use to hide data is to apply combinatorial operator. The watermark bit stream $w = C(4, N_b)$ with $C(4, N_b)$ is a combinatorial number, which means the number of ways to pick N_b unordered outcomes from 4 possibilities. In this study, N_b

means the number of black pixels in b . For example, if N_b is equal to 2, we have four positions, $\{p_1, p_2, p_3, p_4\}$, from which two positions are picked to embed watermark signals, and $g = C(4,2) = 6$, which means we have 6 codes $w = \{r_1, r_2, r_3, r_4, r_5, r_6\}$ for use as watermarks, where $r_1 = \{p_1, p_2\}$, $r_2 = \{p_1, p_3\}$, $r_3 = \{p_1, p_4\}$, $r_4 = \{p_2, p_3\}$, $r_5 = \{p_2, p_4\}$, and $r_6 = \{p_3, p_4\}$. In this case, because four possibilities of combination can be used for representing two bits and we have $C(4,2) = 6$ possibilities of combination to represent two bits, the other two remaining possibilities can be used to represent one more data.

After choosing the rearrangeable block b_i , we rearrange the positions of the black pixels according to the number of black pixels by the reference table to embed the watermark bit w_i of bit stream s .

Table 5.1 An example of reference table.

Case	Number(s) of black pixels (N_b)	Positions of black pixels	Watermark bit stream $w = C(4, N_b)$
A	0		-
B	1		00
			01
			10
			11
C	2		00
			01

C	2		10
			11
			000
			111
D	3		00
			01
			10
			11
E	4		-

a. Case A and Case E:

Case A and Case E mean that the block is entirely black or white. If we change the pixels in these blocks, it is easily noticed. As a result, no data can be embedded.

b. Case B and Case D:

Case B means that there is only one black pixel in the rearrangeable block, and Case D means that there is only one white pixel in the rearrangeable block. When this is the case, because the probability of combination is equal to 4 (that is, $C(4,1) = 4$ or $C(4,3) = 4$), only two bits can be embedded. Figure 5.2 shows an example of Case B and its bit representation after embedding two bits.

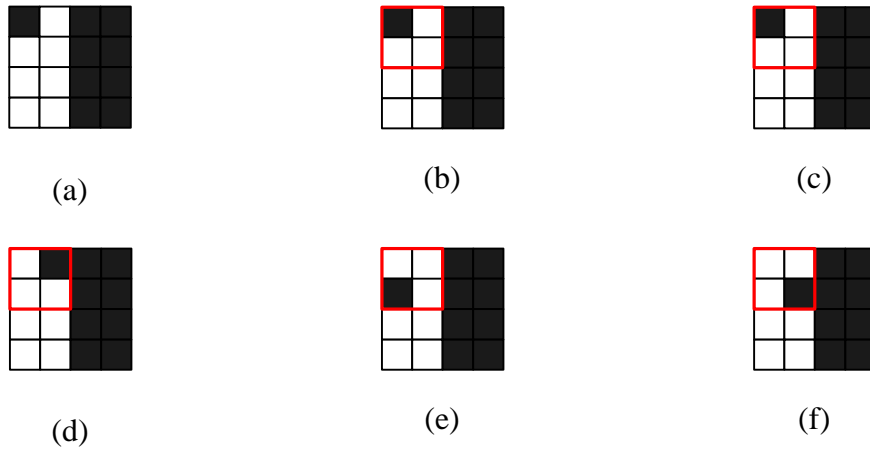


Figure 5.2 An example of Case B. (a) A 4x4 block. (b) The rearrangeable 2x2 block (in the red block) of the 4x4 block. (c) The 4x4 block after embedding “00” the bit stream of watermark. (d) The 4x4 block after embedding “01” the bit stream of watermark. (e) The 4x4 block after embedding “10” the bit stream of watermark. (f) The 4x4 block after embedding “11” the bit stream of watermark.

c. Case C:

In Case C, there are two black pixels and two white pixels, and the probability of combination is equal to 6 (that is, $C(4,2) = 6$). To embed two bits, only 4 possibilities of combination are needed. In addition to embedding two bits, it has more free space to hide one more bit. We use the remaining 2 free spaces to embed one more bit by the reference table. When this is the case, the rearrangeable block can at most hide three bits. Figure 5.3 shows an example of Case C to illustrate how to embed at most three bits.

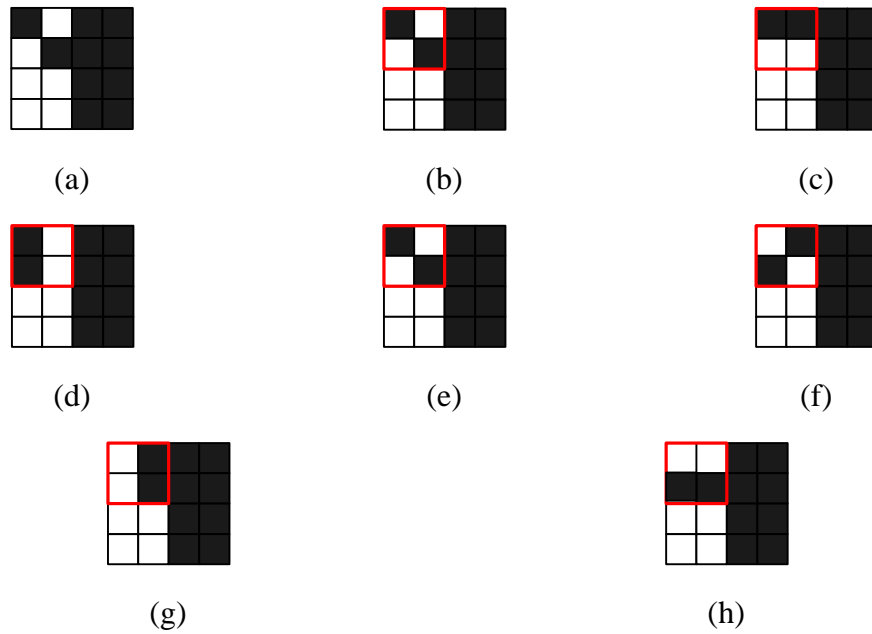


Figure 5.3 An example of Case C. (a) A 4x4 block. (b) The rearrangeable 2x2 block (in the red block) of the 4x4 block. (c) The 4x4 block after embedding “00” the bit stream of watermark. (d) The 4x4 block after embedding “01” the bit stream of watermark. (e) The 4x4 block after embedding “10” the bit stream of watermark. (f) The 4x4 block after embedding “11” the bit stream of watermark. (g) The 4x4 block after embedding “000” the bit stream of watermark. (h) The 4x4 block after embedding “111” the bit stream of watermark.

5.3.2 Detailed Algorithm

The input to the proposed watermark embedding process includes a binary image I , a watermark W , and a reference table T . The output is a stego-image S . The process is described as follows. Figure 5.4 illustrates a flowchart of the proposed watermark embedding process.

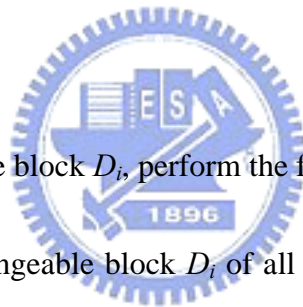
Algorithm 1: *Watermark embedding.*

Input: A given binary image I and a watermark W .

Output: A stego-image S .

Steps:

- 1 Create the reference table T .
- 2 Convert W into a binary form $w_1w_2w_3\dots w_L$.
- 3 Divide I into non-overlapping 4×4 blocks, and divide each 4×4 block B_i further into four non-overlapping 2×2 blocks.
- 4 For each 2×2 image block D_i , count the number N of the black pixels in it and assign it an RHG value G by the reduced halftone gray function described in 5.1.
- 5 For each 2×2 image block D_i , perform the following operations.
 - 5.1. Find the rearrangeable block D_i of all the four blocks in B_i , following the step of choosing the rearrangeable block -.
 - 5.2. Calculate the black pixels in D_i , and arrange pixels to embed the watermark binary stream w_i .
 - 5.3. Rearrange all the pixels of D_i to embed watermark signals according to the reference table T .
- 6 Take the final result as the desired stego-image S .



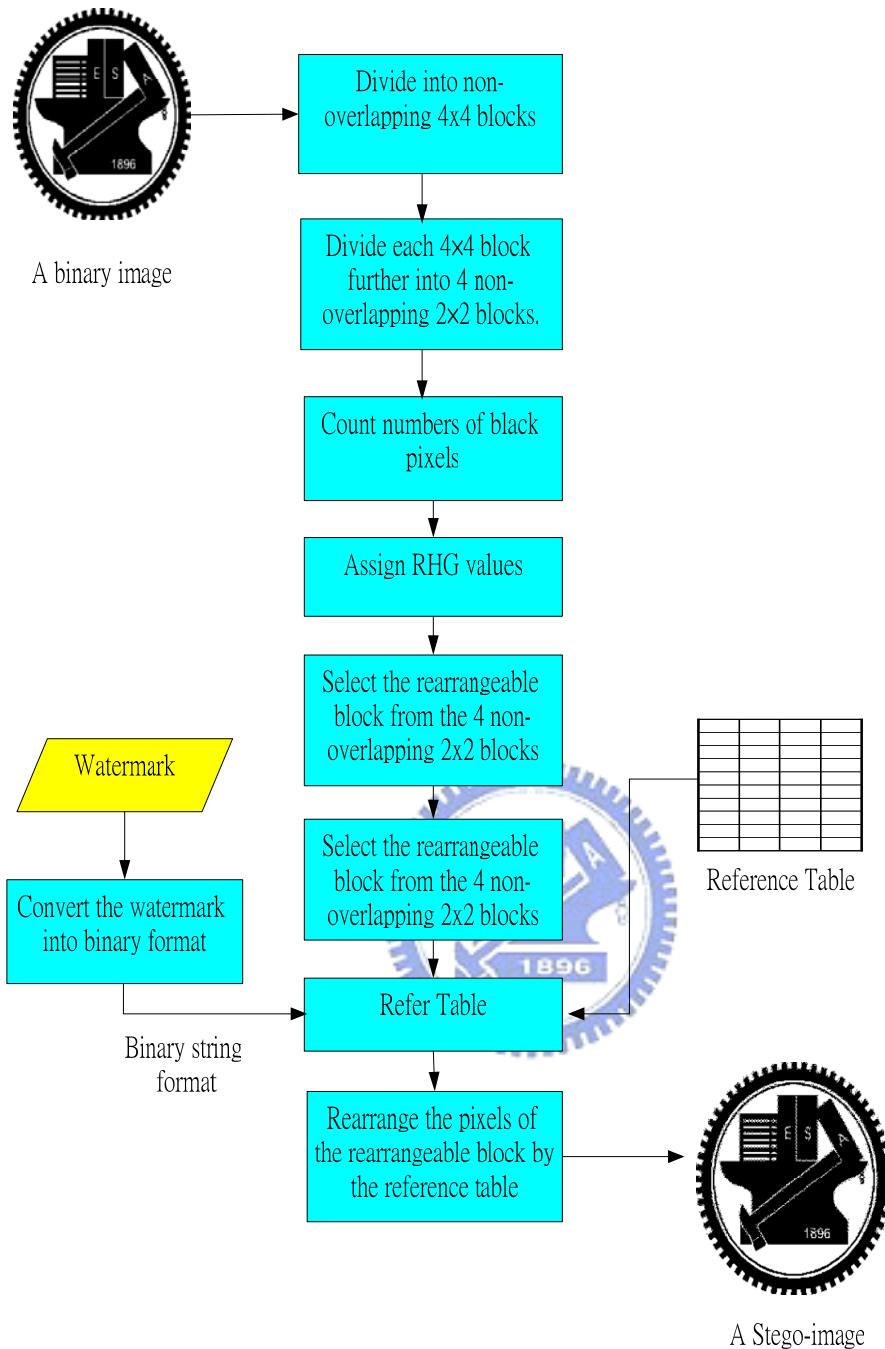


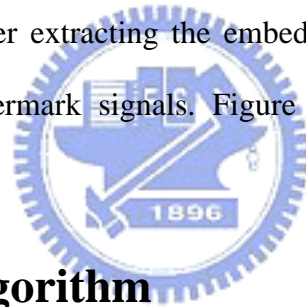
Figure 5.4 Flowchart of proposed method for watermark embedding process.

5.4 Watermark Extraction Process

In the proposed watermark extraction process, a watermark can be extracted to verify the copyright. The concept of the extraction method and the detailed extraction algorithm will be described in this section.

5.4.1 Extraction of Watermarks

In the proposed watermark extraction method, the receiver also needs the reference table T , as described in the watermark embedding method to extract the bit stream of the watermark. The extraction process is similar to the proposed embedding process but in a reverse order. A stego-image is first divided into non-overlapping 4×4 blocks. Each 4×4 block B_i is further divided into four 2×2 blocks denoted as b_i with $i = 1, 2, 3, 4$. In each 2×2 block, we assign the RHG value according to Equation (5.1) and choose the rearrangeable block b . After selecting the rearrangeable block b , we count the number of black pixels and verify the arrangement of black pixels to extract the value of the bit stream by T . That means, by table lookup, the embedded data bits in b_i can be determined. After extracting the embedded watermark bit streams, we convert them to obtain watermark signals. Figure 5.5 shows a flowchart of the proposed extraction process.



5.4.2 Detailed Algorithm

Algorithm 2: *Watermark extraction.*

Input: A given stego-image S .

Output: A watermark W .

Steps:

1. Divide S into non-overlapping 4×4 blocks, and divide each 4×4 block B_i further into four non-overlapping 2×2 blocks.
2. For each 2×2 image block b_i , count the number N of the black pixels in it and assign it an RHG value G by the reduced halftone gray function described by Equation (5.1).

3. For each 2×2 image block b_i , perform the following operations.
 - 3.1. Find the rearrangeable block b of all the four blocks in B_i , following the step of choosing a rearrangeable block.
 - 3.2. Check the positions of pixels in the rearrangeable block and by table lookup, extract the sub-stream S_j from b .
4. Reconstruct the watermark data from several sub-streams.

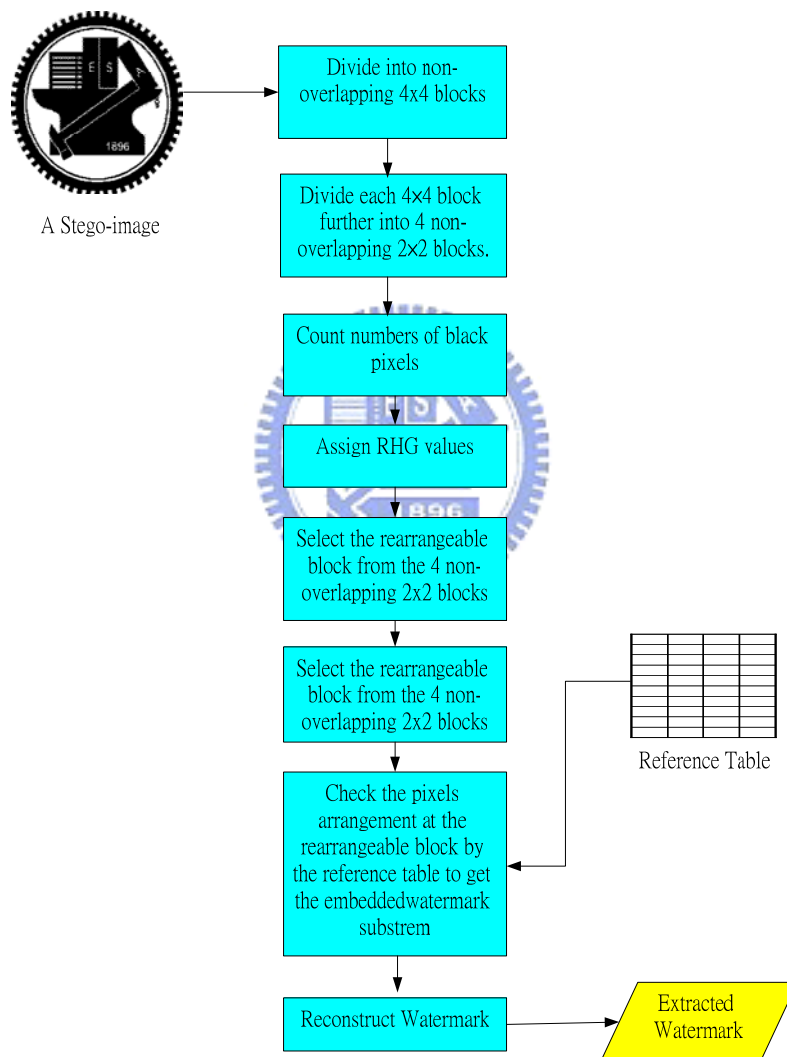


Figure 5.5 Flowchart of proposed extraction process.

5.5 Experimental Results

Several experimental results of applying the proposed method are shown here.

Figure 5.6(a) and (b) illustrate two binary images of the size 256x256. The results after embedding watermark signals are shown in Figure 5.6(c) and (d), respectively. Figure 5.6(e) and (f) show the differences in black pixels after embedding the watermark bit stream.

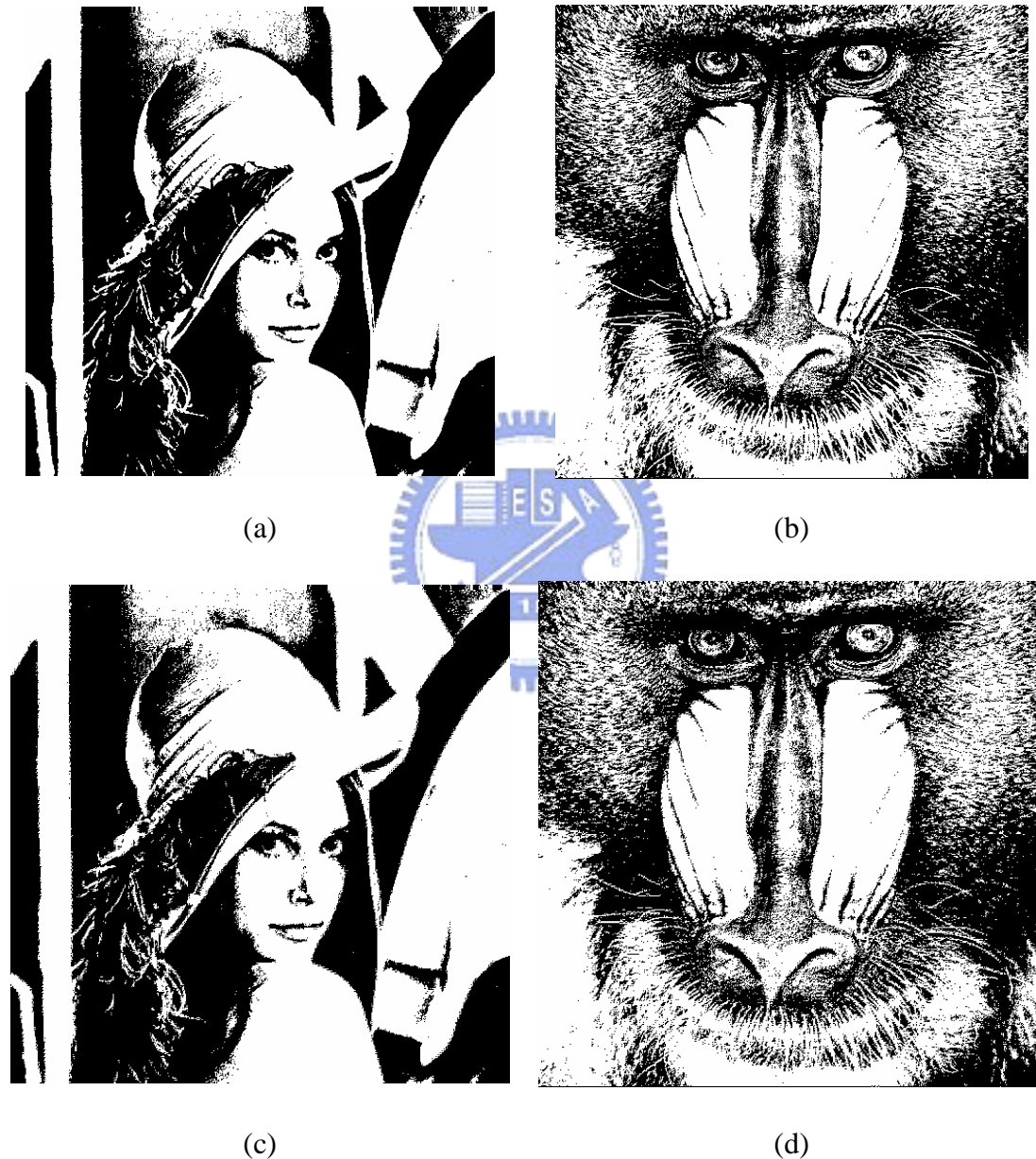


Figure 5.6 Input binary images, output stego-images with watermark signals, the differences, and the watermark image. (a) A binary image of “Lena”. (b) A binary image of “Monkey”. (c) and (d) The stego-images after embedding watermark signals. (e) and (f) The difference between the original binary image and the stego-image.

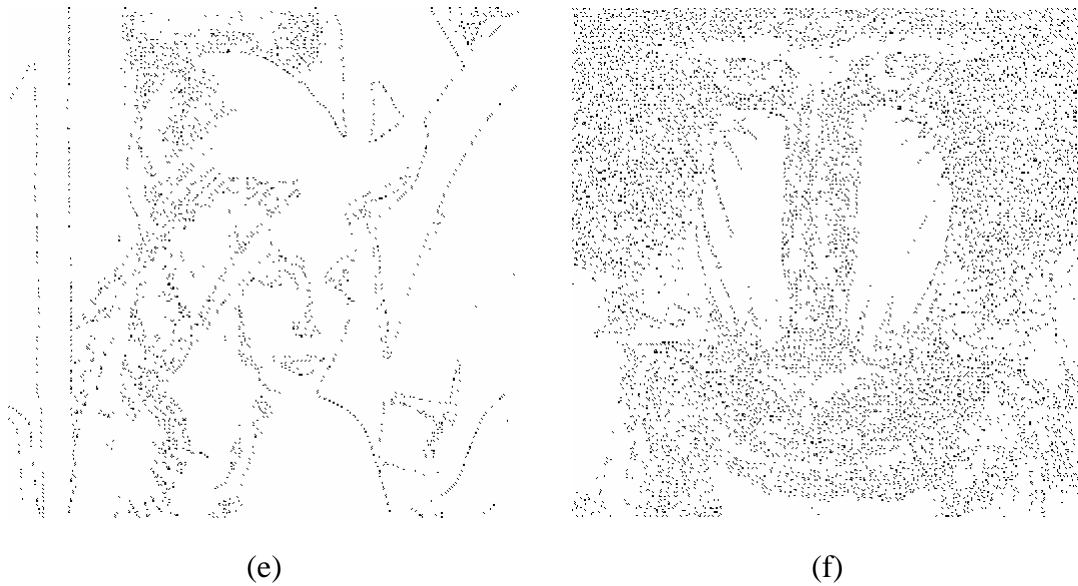


Figure 5.6 Input binary images, output stego-images with watermark signals, the differences, and the watermark image. (a) A binary image of “Lena”. (b) A binary image of “Monkey”. (c) and (d) The stego-images after embedding watermark signals. (e) and (f) The difference between the original binary image and the stego-image (continued).

Figure 5.7 shows some other examples of the results of our experiments. Figure 5.7(a) and (b) are the binary document images both of the size 512x512, and Figure 5.7(c) and (d) show the stego-image after embedding the watermark signals. Figure 5.7(e) and (f) illustrate the difference between the original image and the stego-image. Table 5.2 shows the statistics about the embedded bits and the different pixels for the stego-images after embedding the watermark signals. From these experiments, we can observe that even though the stego-image is embedded with a watermark, we can still see the words clearly. The amount of embedded bits per block ranges from 2.3 to 2.5 bits.

為推廣油桐花風姿，宣導螢火蟲護育觀念，新竹縣政府將於五月七、八日舉辦「日賞五月雪、夜訪夜精靈」螢火蟲的故鄉在內灣活動。舉辦小小螢火蟲行動劇表演、螢光大道揭幕、幸福天燈施放等，呼籲遊客在觀賞螢火蟲時，不要喧譁、亂抓螢火蟲、亂丟垃圾破壞環境。

縣府今天在內灣橫山文物館舉行記者會，縣長與觀光旅遊局長林天俊，在會中宣示愛護保育螢火蟲的決心，雙手折斷象徵抓捕螢火蟲的網子，並接受小小螢火蟲隊「愛我就不要抓我」的授證貼紙。

(a)

In November 1996 the duet Time to say goodbye by Sarah Brightman & Andrea Bocelli became in a few weeks time a big hit in Germany and later on also in several other countries of continental of Europe. And after it was performed on a T.V. programme of the National Lottery on 10 May 1997 it also become very swiftly successful in the Great Britain.

On 19 May 1997 there was an article in The Independent about the success and the background of this song and Andrea Bocelli.

(b)

為推廣油桐花風姿，宣導螢火蟲護育觀念，新竹縣政府將於五月七、八日舉辦「日賞五月雪、夜訪夜精靈」螢火蟲的故鄉在內灣活動。舉辦小小螢火蟲行動劇表演、螢光大道揭幕、幸福天燈施放等，呼籲遊客在觀賞螢火蟲時，不要喧譁、亂抓螢火蟲、亂丟垃圾破壞環境。

縣府今天在內灣橫山文物館舉行記者會，縣長與觀光旅遊局長林天俊，在會中宣示愛護保育螢火蟲的決心，雙手折斷象徵抓捕螢火蟲的網子，並接受小小螢火蟲隊「愛我就不要抓我」的授證貼紙。

(c)

In November 1996 the duet Time to say goodbye by Sarah Brightman & Andrea Bocelli became in a few weeks time a big hit in Germany and later on also in several other countries of continental of Europe. And after it was performed on a T.V. programme of the National Lottery on 10 May 1997 it also become very swiftly successful in the Great Britain.

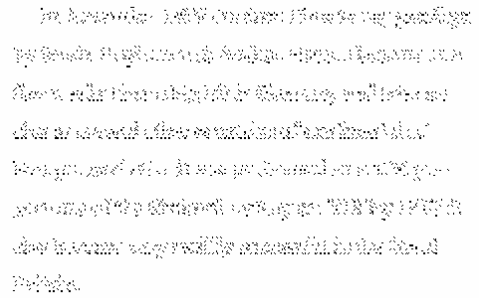
On 19 May 1997 there was an article in The Independent about the success and the background of this song and Andrea Bocelli.

(d)

Figure 5.7 Input binary document images, output stego-images with watermark signals, and the differences. (a) A Chinese binary document image. (b) An English binary document image. (c) and (d) The stego-images after embedding the watermark signals. (e) and (f) The difference between the original binary image and the stego-image, respectively.



(e)



(f)

Figure 5.7 Input binary document images, output stego-images with watermark signals, and the differences. (a) A Chinese binary document image. (b) An English binary document image. (c) and (d) The stego-images after embedding the watermark signals. (e) and (f) The difference between the original binary image and the stego-image, respectively (continued).

Table 5.2 The statistics about the embedded bits and the difference pixels for the stego-images after embedding watermark signals.

	Lena	Monkey	Chinese	English
Used blocks	3154	10299	6417	3359
Embedded bits	7287	23753	15753	8377
Different pixels	4976	16934	10624	5620

5.6 Discussions and Summary

In this chapter, we have presented a novel watermark embedding method for copyright protection in binary images. We use the RHG value to select the proper position to hide data which is called the rearrangeable block. We change the positions of black pixels in the rearrangeable blocks to obtain and embed watermark signals.

With the help of the reference table, we can embed 3 bits in a 4×4 block. So during the extraction process, we can extract the embedded watermark signal by table lookup. Experimental results demonstrate that the words in the stego-image after embedding watermark signals can still be seen clearly. As a result, our algorithm can be applied to not only binary images but also binary document images.

However, the proposed watermark embedding method does not belong to robust watermarking. This means that the embedded watermark signals are easily tampered with. In future works, efforts can be made on solving this problem.



Chapter 6

Hiding Digital Information and Authentication Signals behind Binary Images with Reduced Distortion and Enhanced Security

In this chapter, we propose a method to combine both watermark and authentication signals for binary document images. The method is based on Tzeng and Tsai [1-2]. By integrating the proposed method of [1] and [2], a watermark and an authentication signal can co-exist in a binary document image. The integrity of binary document images can be verified by extracting the authentication signals and the watermark signals can be detected for copyright protection at the same time.

The remainder of this chapter is organized as follows. In Section 6.1, an introduction is given first. In Section 6.2, the idea of the integration method is described. In Section 6.3, the watermark and authentication signal embedding processes are given. In Section 6.4, the watermark extraction process and the image authentication process are described. In Section 6.5, some experimental results are given to show the feasibility of the proposed integration method. Finally, in Section 6.6, some discussions and summary are made.

6.1 Introduction

Due to the rapid growth of digital processing, digital images are easy to be copied or even tampered with. It is necessary to devise a scheme both to protect the copyright of images and to authenticate the fidelity and integrity of them. The techniques of

embedding watermark and authentication signals together can be utilized to achieve these goals. Many researches about these techniques are proposed individually. However, few researches are about combining them in a single image.

In the proposed integration method, we focus on binary images to embed watermark and authentication signals. In a binary image, there are only two types of pixels, black and white, with values 0 and 255, respectively, and if the pixel values are changed arbitrarily, visible artifacts in the image will be created. It is the reason why there are few researches about watermarking for binary images according to our survey. In this chapter, we embed not only watermark signals for copyright protection but also authentication signals for verifying the integrity of a binary image. And it is hoped that after embedding watermark and authentication signals, the quality of the stego-image is still good.

6.1.1 Problem Definitions

Owing to the aforementioned purposes, watermark and authentication signals will be embedded simultaneously in a binary image. But this is quite difficult. A reason is that usable properties of a binary image for data embedding are limited. So, the main issue is to utilize the limited properties efficiently to embed the information properly. The embedding process should create no conflict in embedding the information of watermark and authentication signals. Furthermore, it is needed to extract all embedded information accurately from the stego-image. In this study, we propose an integration method to find usable properties and utilize them to embed watermark and authentication signals together.

6.1.2 Review of Employed Techniques

In this section, techniques employed in our methods are reviewed. These techniques are based on Tzeng and Tsai[1-2]. In Tzeng and Tsai [1], the main topic is embedding authentication signals into binary images. And in Tzeng and Tsai [2], the main topic is embedding watermark signals for copyright protection into binary images. These two techniques are introduced briefly as follows.

(A). Embedding authentication signals

In Tzeng and Tsai [1], two keys and two random number generators are used to create the authentication codes and the positions for embedding authentication signals. The size of a block used to process an image is 3×3 . The first key K_1 with the first number generator f_1 generate a sequence of random numbers as the authentication codes. The function of the second key K_2 with the second number generator f_2 is to select randomly code holders to hold the authentication codes. Then, by finding the optimal code holder g_{opt} with the minimum number of different bit values of the authentication codes and replacing the different bit values, if necessary, the authentication codes could be held by the g_{opt} .

As an example, let the pixels in a given 3×3 image block B_1 in a raster scanning order be denoted as P_1 through P_9 whose contents, when concatenated, are 011110010, as shown in Figure 6.1(a). Authentication codes $f_1(K_1)$ are 10,11,01,10 and code holders $f_2(K_2)$ are 15, 29, 82. A 2-bit authentication code $c_1=10$ generated by f_1 is to be embedded in B_1 shown in Figure 6.1(g). In Figure 6.1, the code holders created by f_2 with K_2 are $H_1=(P_1, P_5)$, $H_2=(P_2, P_9)$ and $H_3=(P_8, P_2)$. We will select a candidate from the three cold holders with the minimum number of different bit values with the authentication code. As a result, In Figure 6.1 (a), we want to embed c_1 into B_1 , and find that the code holder $H_2=(P_2,P_9)=10$ is the same as c_1 . So in B_1 there is no need to

modify the pixel value. However, in Figure 6.1(b), we want to embed c_2 into B_2 , and find that the optimal code holder $H_1=(P_1, P_5)=10$ is closest to c_2 . So in B_2 , P_5 needs to be modified to 1 in order to embed c_2 into B_2 . The result is shown in Figure 6.1(g) and (h).

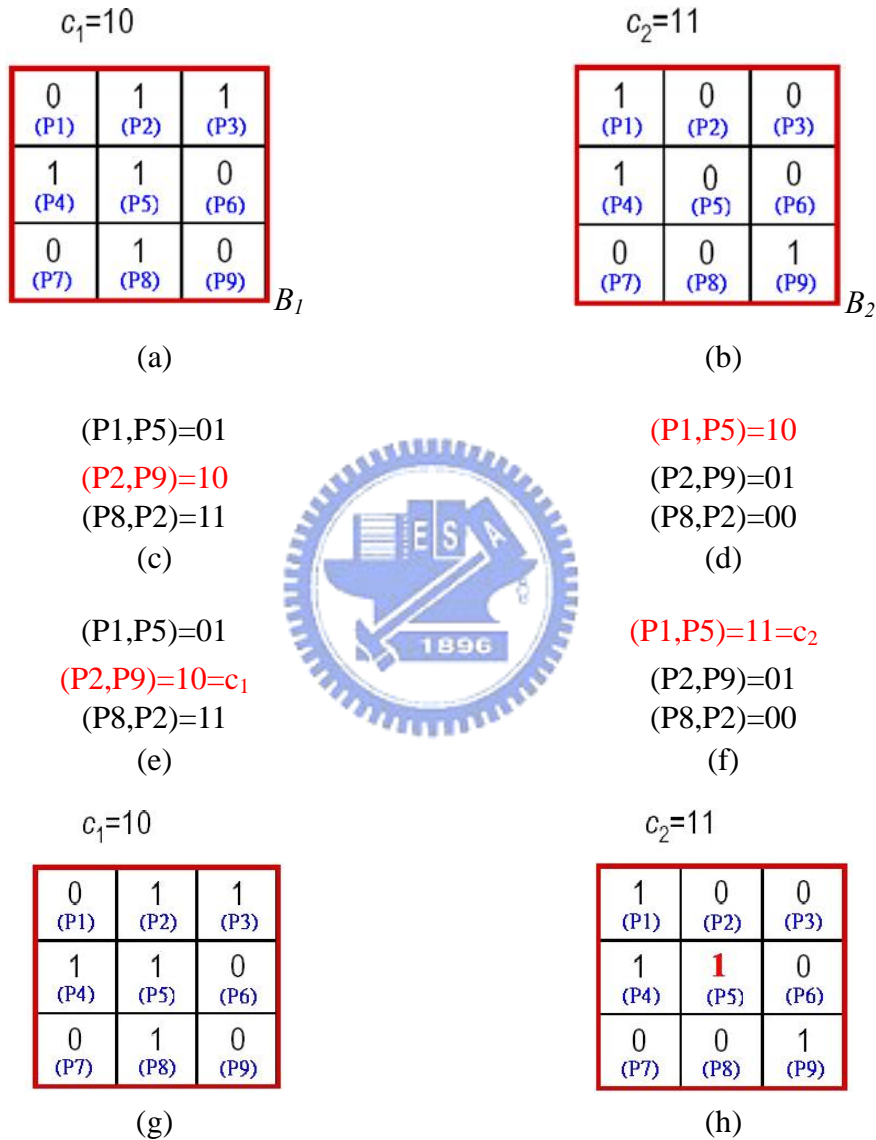


Figure 6.1 An example of embedding authentication codes. (a) and (b) A 3x3 block. (c) and (d) Select a code holder to embed an authentication code for (a) and (b). (e) and (f) The result after embedding the authentication code. (g) and (h) The 3x3 block corresponding to (e) and (f).

(B). Embedding watermark signals

In [2], a method to embed watermark signals into a binary image is described. The

concept of *surrounding edge count* (SEC) was proposed to represent data embeddability for binary images. The definition of SEC is defined as follows:

$$SEC_p = \sum_{i=1}^8 |v_i - v| \quad (6.1)$$

where v means the pixel value of centralized viewpoint of p and v_i means the pixel value of its eight neighbors. As a result, SEC_p define as the number of existing edges between p and its eight neighbors in a 3×3 block. Some examples are shown in Figure 6.2(a), (b) and (c). SEC_p is a measure of the structural randomness in a block from the centralized viewpoint of p . A characteristic of SEC is that the embeddability property can guarantee the embeddability at the embeddable bits can be preserved so that the embedded data at these bits can be extracted correctly. The definition of ΔSEC_p is shown below:

$$\Delta SEC_p = |SEC_p - SEC_p'| \quad (6.2)$$

where SEC_p' denote the SEC value after the complementation operation. ΔSEC_p is the amount of the resulting change of the numbers of edges in a 3×3 block. Figure 6.2(d) and (e) show the result of SEC_p and SEC_p' , and ΔSEC_p is equal to 8. A measure of a pixel p in a 3×3 block B to be data embeddable needs to satisfy the two conditions: (a) $\Delta SEC_p \leq \text{threshold} = T_d$; and (b) p and its eight neighbors in B have not been visited yet. The condition (a) above restricts the distortion introduced by the complementation of p 's value to be sufficiently small, so that the resulting image quality will not be affected too much. And condition (b) requires that embeddable pixels be disconnected from one another, so that pixel value changes due to secret embedding will not be clustered or propagated to cause obvious larger-size visual artifacts. The advantage of Tzeng and Tsai[2] is that pixel embeddability can be preserved after the secret hiding process.

In our proposed integration method, we will combine both (A) and (B) methods

into a binary image. Because the size of a block used in both methods is 3×3 , if we directly apply Method (A) and then apply Method (B) into a binary image, it will cause some conflicts and vice versa.

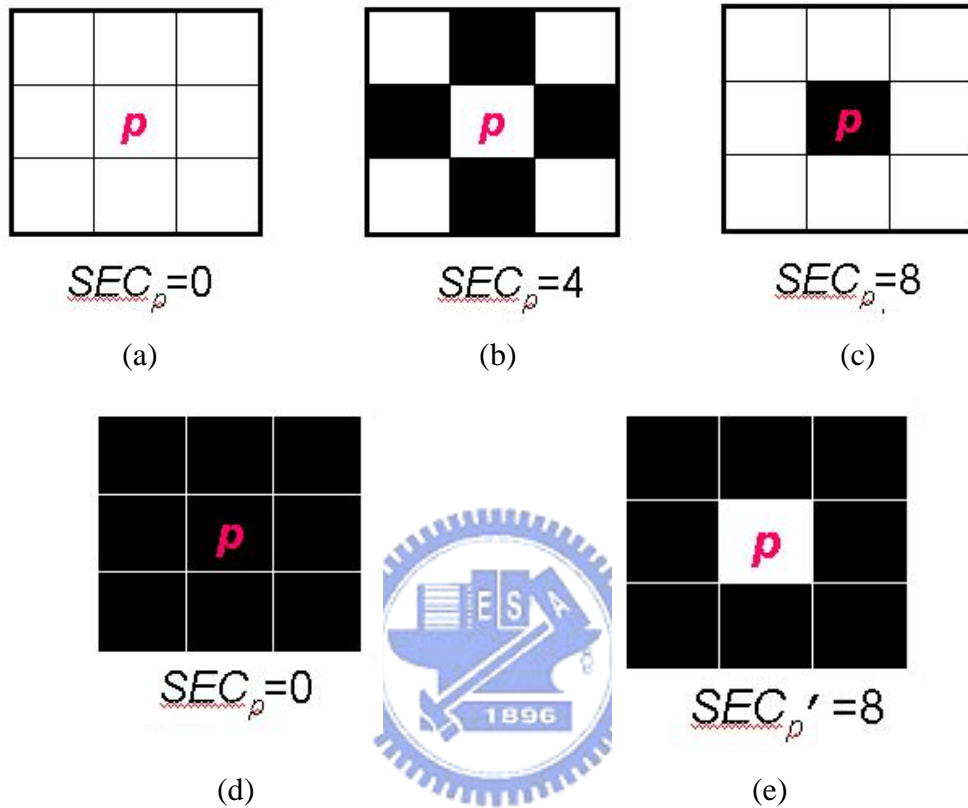


Figure 6.2 An example of SEC_p and ΔSEC_p . (a)-(c) Some examples of SEC_p .
 (d) An example of SEC_p . (e) An example of SEC'_p .

6.2 Idea of Integration Method

In this section, we will briefly describe how to embed both watermark and authentication signals into a binary image. Authentication signals are embedded first into a binary image. Different to the size of a block in [1], we process a binary image for image authentication with the size of a block being 9×9 . After processing the authentication signals, we will embed the watermark signals. The size of a block for

watermark embedding is unchanged, which is 3×3 . We mark the location to distinguish between the watermark and authentication signals. As a result, the authentication and watermark signals will be embedded independently.

6.3 Watermark and Authentication Signals Embedding Process

6.3.1 Embedding of Watermarks and Authentication Signals

Authentication signals will be embedded first, and the size of a block for embedding them is 9×9 . And each 9×9 block is partitioned further into nine 3×3 blocks. In each 3×3 block from a 9×9 block, we will give each 3×3 block a binary value to represent it according to the even or odd parity of the number of black pixels in the block. An even number of black pixels is represented by “0” and an odd number is represented by “1.” So we can treat a 9×9 block with nine 3×3 blocks as a 3×3 block to embed authentication signals, as shown in Figure 6.3(a). The authentication signals embedding algorithm is similar to [1], but using a different block size.

The positions for embedding authentication signals and the authentication codes are controlled by the two keys and two random number generators which are the same as in [1] and are briefly described in 6.1.2(A). If it is needed to embed an authentication signal into a 3×3 block, we only modify the even or odd parity of the number of black pixels according to the authentication codes. We have to mark the positions for embedding authentication signals in the 3×3 blocks, because the remaining 3×3 blocks in a 9×9 block can be used to embed watermark signals.

There is one thing needed to be addressed, that is, the central pixel does not

participate in the accumulation because the central pixel is used to embed watermark signals.

After embedding an authentication signal into the 3×3 blocks from a 9×9 block, we have to embed watermark signals in the remaining 3×3 blocks. In [2], Tzeng and Tsai only modified the center pixel in each 3×3 block. We can apply the same technique in the remaining 3×3 blocks to embed watermark signals.

Actually, it is not necessary to mark the positions of authentication signals, as watermark and authentication signals can co-exist in the same 3×3 block. However, to minimize artificial effects in a binary image, we will embed the watermark and authentication signals into different 3×3 blocks.

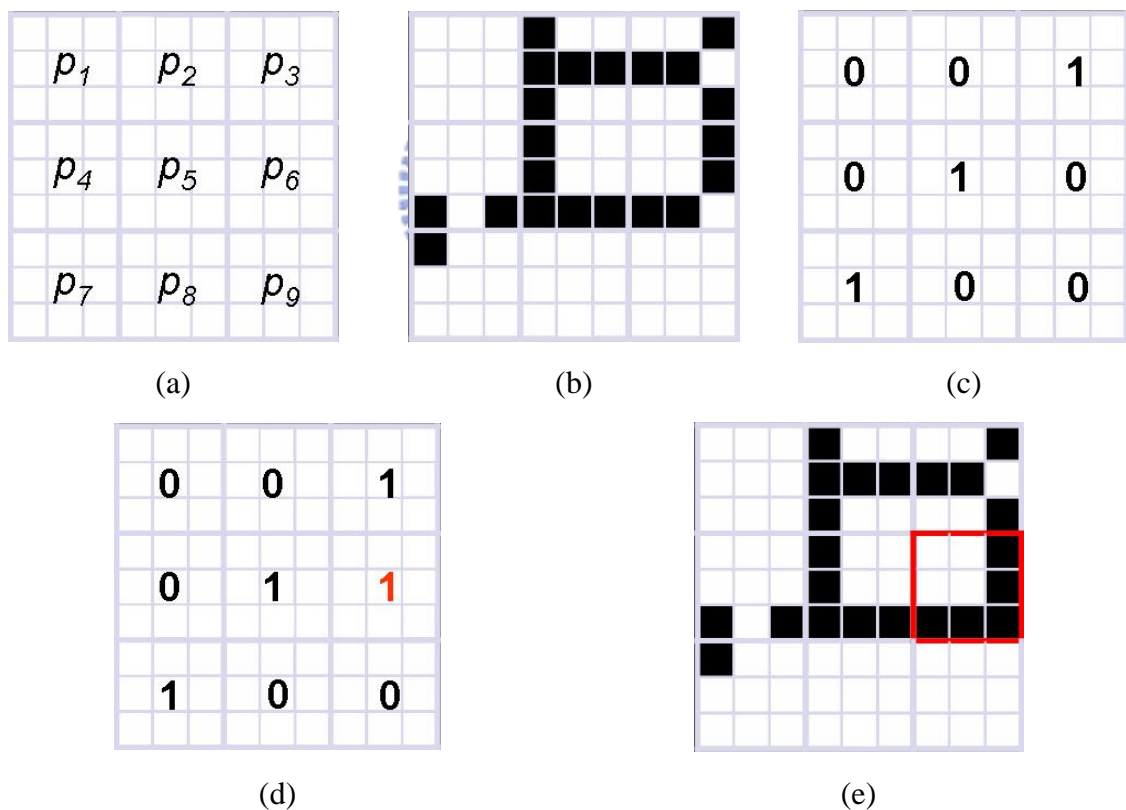


Figure 6.3 An example of authentication signal embedding process in a 9×9 block (a) A 9×9 block and the number index. (b) An example of 9×9 block. (c) The corresponding binary value of (b). (d) An example of embedding an authentication signal into P_6 . (e) The result after embedding authentication signals.

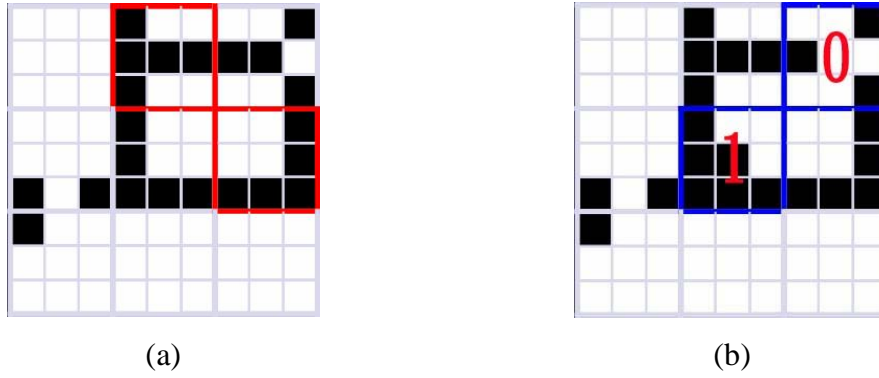


Figure 6.4 An example of watermark signal embedding procedure. (a) The positions for embedding authentication signals. (b) The result after embedding watermark signals.

Figure 6.4 shows an example of watermark signal embedding. In Figure 6.4(a), the red parts indicate the positions for embedding authentication signals and the remaining 3×3 blocks can be used to embed watermark signals. In Figure 6.4(b), because we set the threshold T_d to be 3 which means $\Delta SEC_p \leq 3$, only p_3 and p_5 meet the requirements and can embed watermark signals. Figure 6.4 (b) shows the result after embedding watermark signals “1” and “0” into p_3 and p_5 , respectively.

6.3.2 Detailed Algorithm

The input to the proposed method for integration of watermark and authentication signals include a binary image I , a watermark W , two random number generators G_1 and G_2 , and two keys K_1 and K_2 . The output is a stego-image S . The process can be briefly expressed as an algorithm as follows. Figure 6.5 illustrates a flowchart of the proposed method for authentication and watermark signal embedding in binary document images.

Algorithm 1: *Watermark and authentication signal embedding.*

Input: A given binary image I , a watermark W , two random number generators G_1 and G_2 and two keys K_1 and K_2 .

Output: A stego-image S .

Steps:

- 1 Convert W into a binary form $(w_1w_2w_3\dots w_L)$.
- 2 Generate authentication codes C by K_1 with G_1 and code holders H by K_2 with G_2 .
- 3 Divide I into non-overlapping 9×9 blocks, and divide each 9×9 block B_i further into nine non-overlapping 3×3 blocks D_i .
- 4 For each 3×3 block D_i in a 9×9 image block B_i , count the number N of the black pixels and assign it a binary value according to the even or odd parity of N .
- 5 For each B_i , perform the following operations to embed the authentication signals:
 - 5.1. Get the authentication code C_i from C .
 - 5.2. Select the code holder H_i from H with least distortion and acquire authentication codes C_i' .
 - 5.3. Modify the value in H_i by changing the number of black pixels in D_i if $C_i' \neq C_i$.
- 6 For each D_i in B_i , perform the following operations to embed the watermark signals:
 - 6.1. Count SEC value.
 - 6.2. If Δ SEC value is smaller than a threshold T_d and D_i does not embed the authentication codes, then embed the watermark signal by changing the value of center pixel p in D_i .
- 7 Take the final result as the desired stego-image S .



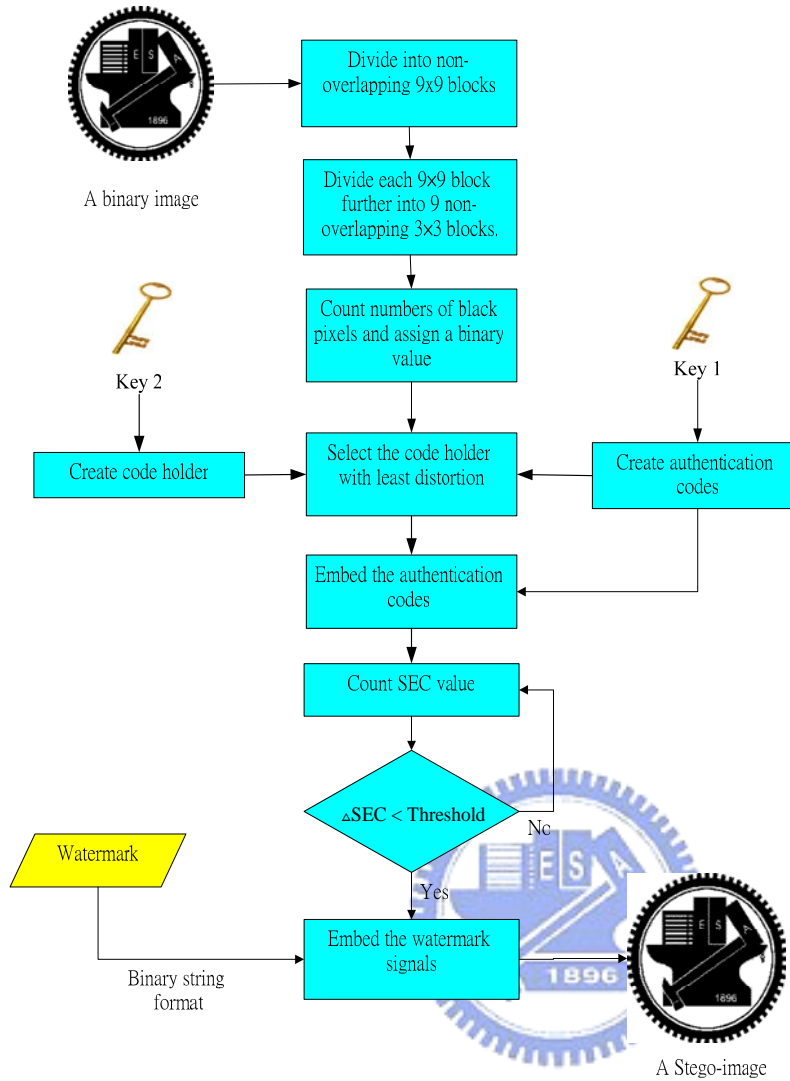


Figure 6.5 Flowchart of proposed method for authentication and watermark signal embedding in binary document images.

6.4 Watermark Extraction Process

6.4.1 Extraction of Watermarks and Authentication Signals

The embedded watermark and authentication signal extraction procedure is similar to the embedding one but in a reverse order. We extract the authentication signals first to verify the integrity of a suspicious image. If a suspicious image suffers from attacks,

the embedded authentication signals will be different from the original ones and the location of tampering can be detected.

A suspicious image is divided into non-overlapping 9×9 blocks. Then, each 9×9 block is divided further into nine non-overlapping 3×3 blocks. For each 3×3 image block B_i , the number N of black pixels in B_i is counted. And B_i is assigned a binary value according to the even or odd property of N . The authentication codes and code holders can be generated from two keys which are the same as those used in the embedding procedure. By checking the difference between the embedded authentication codes and the generated ones from the key, the 9×9 block can be judged as being altered or not. In the output images of our experiments, blocks judged as being tampered with are marked with red color.

If a stego-image does not suffer from any attack in a 9×9 block, watermark signals can be extracted from it. Because we know the locations for embedding authentication signals in the 3×3 blocks in a 9×9 block, the remaining 3×3 blocks B_W are utilized to embed watermark signals. For each B_W , the SEC value is computed and we determine if it satisfies the two conditions. If the SEC value satisfies the two conditions, a watermark signal can be extracted from B_W according to the value of the central pixel p . Figure 6.6 illustrates a flowchart of the proposed method for authentication and watermark signal extraction in binary documents.

6.4.2 Detailed Algorithm

The input to the proposed process for extracting embedded watermark and authentication signals include a stego image S , two random number generators G_1 and G_2 , and two keys K_1 and K_2 which are the same as those used in the data embedding procedure. The output is an authentication image A and a watermark W . The process

can be briefly expressed as an algorithm as follows. Figure 6.6 illustrates a flowchart of the proposed method for embedded authentication and watermark signals extraction in binary document images.

Algorithm 2: *Image authentication and watermark extraction.*

Input: A given stego image S , two random number generators G_1 and G_2 , and two keys K_1 and K_2 .

Output: An authentication image A and a watermark W .

Steps:

1. Generate authentication codes C by K_1 with G_1 and code holders H by K_2 with G_2 .
2. Divide S into non-overlapping 9×9 blocks, and divide each 9×9 block B_i further into nine non-overlapping 3×3 blocks D_i .
3. For each 3×3 block D_i in a 9×9 image block B_i , count the number N of the black pixels and assign it a binary value according to the even or odd parity of N .
4. For each B_i , perform the following operations:
 - 4.1. Get the authentication code C_i from C .
 - 4.2. Select the code holder H_i from H with least distortion and acquire authentication codes C_i' .
 - 4.3. if $C_i \neq C_i'$, regard the 9×9 image block B_i as being tampered with and mark the same location in A with red color.
5. If B_i is not tampered with, for each D_i in B_i , perform the following operations to extract the watermark signals:
 - 5.1. Count the SEC value.

- 5.2. If ΔSEC value is smaller than a threshold T_d and D_i does not embed the authentication codes, then extract the watermark signal W_i according to the value of the center pixel p in D_i .
6. Construct W from W_i .
 7. Take the final result as the desired authentication image A and the watermark W .

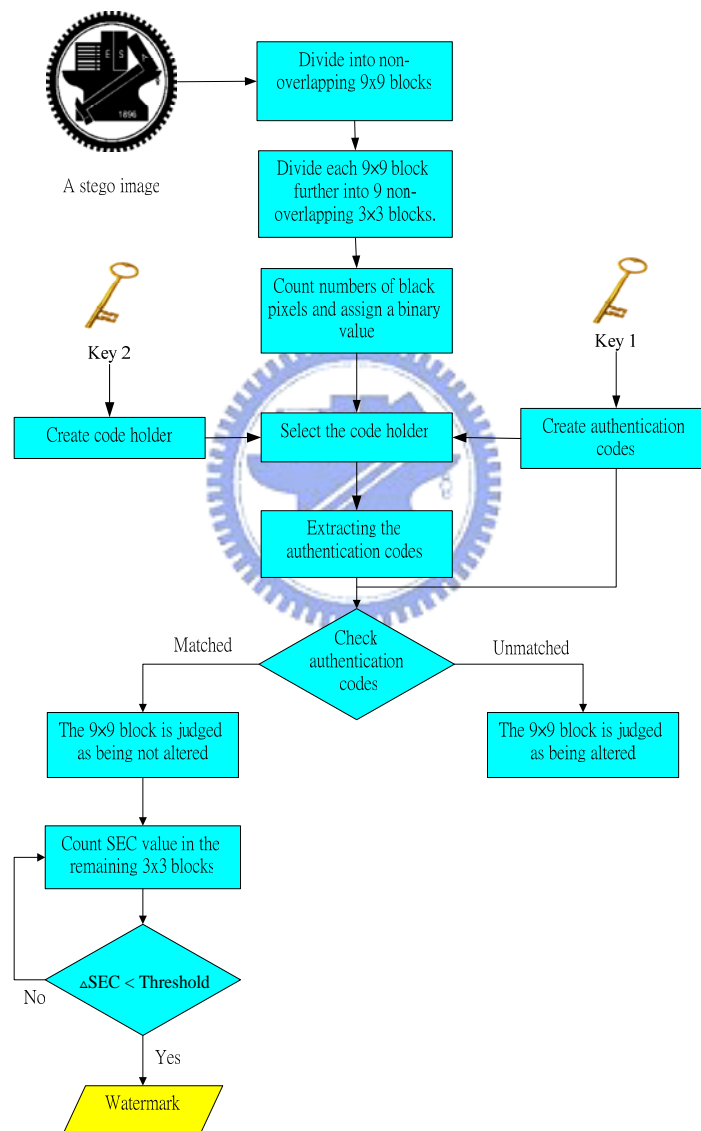


Figure 6.6 Flowchart of proposed method for authentication and watermark signal extraction process.

6.5 Experimental Results

Some experimental results of applying the proposed method for integration of authentication and watermark signals are shown here. Figure 6.7(a) is a binary watermark image with size 40×40. Figure 6.7(b) and (c) show two binary document images both with size 512×512. And the stego-images resulting from embedding authentication and watermark signals are shown in Figure 6.7(d) and (e), respectively. Figure 6.7(f) and (g) show their differences in black pixels after embedding authentication and watermark signals.



Figure 6.7 An embedded watermark image, input binary document images, output stego-images with authentication and watermark signals, and the differences. (a) A binary watermark image. (b) A binary Chinese document image. (c) A binary English document image. (d) and (e) Stego-images after embedding authentication and watermark signals. (f) and (g) The difference pixels before and after embedding authentication and watermark signals.

木柵的綠竹筍品嚐大會已經辦了14年，是熟門熟路的老饕才知道的活動：每年當地筍農挑選品質最好的新鮮竹筍，就像參加武功大會比試一樣，競爭特優的榮耀，而比賽結束之後，這些木柵地區最好的綠竹筍，就通通下鍋，擔任品嚐會的主角；品嚐會的座位每年都在開放當天就搶購一空，今年擴大舉辦，目前尚未額滿。

Taiwan's exclusion from the World Health Organisation poses an international danger because of its key role in fighting bird flu and SARS, the island's health minister said on Friday. Diplomatically isolated Taiwan is pursuing its ninth consecutive attempt to win acceptance at the WHO in the face of stern resistance from Beijing. China, which views the self-ruled island as a breakaway province, opposes its participation in most international organisations.

Health minister Hou Sheng-mou urged next week's annual assembly of the WHO to grant Taiwan observer status so that the world health body could better combat a potential influenza pandemic linked to avian flu. Experts warn such an outbreak could kill millions of people.

"If Taiwan cannot be a World Health Organisation member, that will be a loss to Taiwan ... but it will also be ... a danger to the rest of the world," Hou said in a telephone interview with Reuters. Hou feared Taiwan's continued exclusion would mean it could not receive or offer vital information in the case of a deadly disease outbreak. This could prove especially risky now. U.N health officials say the world faces a high risk of a flu pandemic stemming from Asia and are on guard for signs that a strain of bird flu is mutating into a form easily transmissible to humans. "We are facing a new world. We are threatened," Hou said. "These diseases don't respect international boundaries."

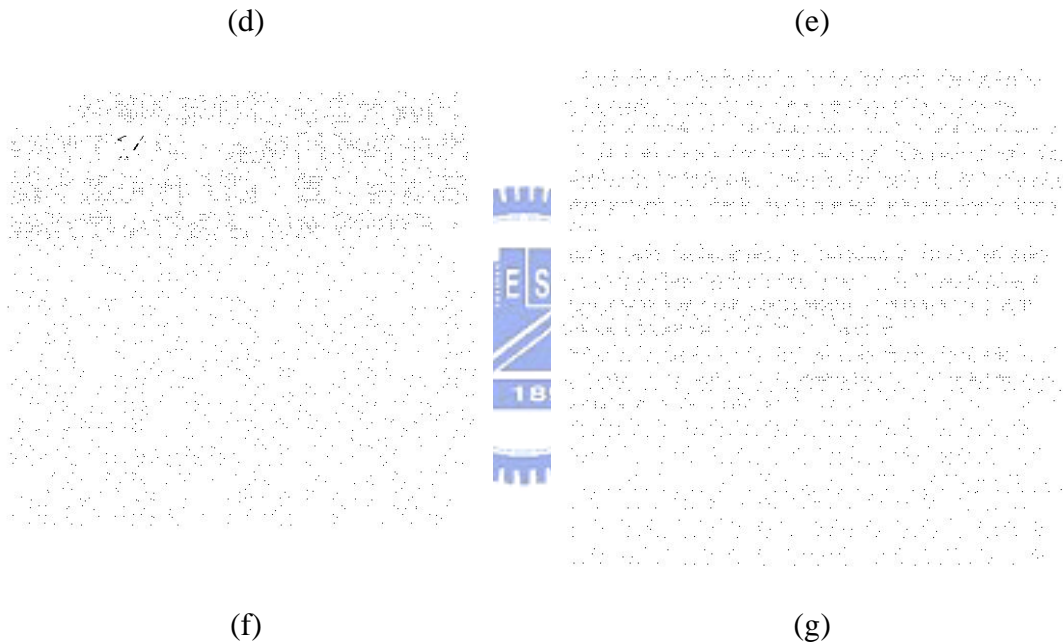


Figure 6.7 An embedded watermark image, input binary document images, output stego-images with authentication and watermark signals, and the differences. (a) A binary watermark image. (b) A binary Chinese document image. (c) A binary English document image. (d) and (e) Stego-images after embedding authentication and watermark signals. (f) and (g) The difference pixels before and after embedding authentication and watermark signals (continued).

Two images which have been tampered with are shown in Figure 6.8(a) and (b). Figure 6.8(c) and (d) show the respective authentication results. The red parts indicate the detected areas of tempering. Finally, Figure 6.8(e) and (f) show the embedded watermark image extracted from (a) and (b), respectively.

木柵的綠竹筍品嚐大會已經辦了14年，是熟門熟路的老饕才知道的活動：每年當地筍農挑選品質最好的新鮮竹筍，就像參加武功太會比試一樣，競爭特優的榮耀，而比賽結束之後，這些木柵地區最好的綠竹筍，就通通下鍋，擔任品嚐會的主角；品嚐會的座位每年都在開放當天就搶購一空，今年擴大舉辦，目前尚未額滿。

Taiwan's exclusion from the World Health Organisation poses an international danger because of its key role in fighting bird flu and SARS, the island's health minister said on Friday. Diplomatically isolated Taiwan is pursuing its ninth consecutive attempt to win acceptance at the WHO in the face of stern resistance from Beijing, China, which views the self-ruled island as a breakaway province, opposes its participation in most international organisations.

Health minister Hou Sheng-mou urged next week's annual assembly of the WHO to grant Taiwan observer status so that the world health body could better combat a potential influenza pandemic linked to avian flu. Experts warn such an outbreak could kill millions of people. "I love you so much, if Taiwan cannot be a World Health Organisation member, that will be a loss to Taiwan ... but it will also be ... a danger to the rest of the world," Hou said in a telephone interview with Reuters. Hou feared Taiwan's continued exclusion would mean it could not receive or offer vital information in the case of a deadly disease outbreak. This could prove especially risky now. U.N health officials say the world faces a high risk of a flu pandemic stemming from Asia and are on guard for signs that a strain of bird flu is mutating into a form easily transmissible to humans. "We are facing a new world. We are threatened," Hou said. "These diseases don't respect international boundaries."

(a)

(b)

木柵的綠竹筍品嚐大會已經辦了14年，是熟門熟路的老饕才知道的活動：每年當地筍農挑選品質最好的新鮮竹筍，就像參加武功太會比試一樣，競爭特優的榮耀，而比賽結束之後，這些木柵地區最好的綠竹筍，就通通下鍋，擔任品嚐會的主角；品嚐會的座位每年都在開放當天就搶購一空，今年擴大舉辦，目前尚未額滿。

Taiwan's exclusion from the World Health Organisation poses an international danger because of its key role in fighting bird flu and SARS, the island's health minister said on Friday. Diplomatically isolated Taiwan is pursuing its ninth consecutive attempt to win acceptance at the WHO in the face of stern resistance from Beijing, China, which views the self-ruled island as a breakaway province, opposes its participation in most international organisations.

Health minister Hou Sheng-mou urged next week's annual assembly of the WHO to grant Taiwan observer status so that the world health body could better combat a potential influenza pandemic linked to avian flu. Experts warn such an outbreak could kill millions of people. "I love you so much, if Taiwan cannot be a World Health Organisation member, that will be a loss to Taiwan ... but it will also be ... a danger to the rest of the world," Hou said in a telephone interview with Reuters. Hou feared Taiwan's continued exclusion would mean it could not receive or offer vital information in the case of a deadly disease outbreak. This could prove especially risky now. U.N health officials say the world faces a high risk of a flu pandemic stemming from Asia and are on guard for signs that a strain of bird flu is mutating into a form easily transmissible to humans. "We are facing a new world. We are threatened," Hou said. "These diseases don't respect international boundaries."

(c)

(d)



(e)

(f)

Figure 6.8 Some tampered images, authentication results and embedded watermark images. (a) and (b) Images tampered with. (c) and (d) Authentication results. (e) and (f) Embedded watermark images extracted from (a) and (b), respectively.

6.6 Discussions and Summary

In this chapter, we have proposed a method for embedding both authentication and watermark signals in binary document images. Because the two methods proposed by [1] and [2] used identical block sizes to embed watermark and authentication signals, if we combine these two methods for embedding watermark and authentication signals together, it will cause some conflicts to occur. In the integrated embedding process, the size of a block for embedding authentication signals is modified to be 9×9 and the size of a block for embedding watermark signals is unchanged. We treat a 9×9 block with nine 3×3 blocks as a 3×3 block to embed authentication signals by changing the number of black pixels in appropriate 3×3 blocks. The remaining 3×3 blocks can be used to embed watermark signals.

We note that in the proposed method for integration of authentication and watermark signals, we do not deal with entirely black or entirely white blocks. Therefore, if someone replaces parts of a stego-image with an entirely black or entirely white region, the region being tampered with cannot be detected. Future works can focus on solving this problem.

Chapter 7

Conclusions and Suggestions for Future Works

7.1 Conclusions

In this study, we have proposed various methods based on information hiding techniques to solve two application problems, namely, copyright protection and tampering detection for document images.

First, a method for authentication of grayscale document images has been proposed, in which a semi-fragile watermark is embedded into each block with robustness against print-and-scan attacks. The semi-fragile watermark used as the authentication signal is a straight line. The equation of a line is generated by the RHG value, the block number index, and a key in order to increase the security of authentication. By selecting the best place of embedding, a line is embedded into each block. The way to embed an authentication signal into each block is to modify the gray values of the pixels through which the embedded line passes. In the extraction process, the embedded line can be extracted by a line fitting technique. With the help of the extracted authentication signals, block areas within a suspicious image, which have been tampered with, can be detected and located, thus achieving the goal of verifying the integrity and fidelity of the image. Using this method, the semi-fragile watermark can survive print-and-scan operations.

Second, a method for copyright protection of grayscale document images by watermarking has been proposed, in which we use a technique utilizing edge direction histograms with circular interpretation to embed a watermark. The relationship

between mother and child blocks is used to hide data. A mother block can be seen as a reference block and by modifying the gray values of the pixels in the child block, watermark signals can be embedded in it. An edge direction histogram (EDH) is created to collect all edge directions in a block to get a discrete distribution. Circular interpretation is then conducted to map an EDH into a circle. By adjusting the location of the center of mass in an EDH circle of the child blocks according to the embedded data, the child blocks can carry the watermark signals. The embedded watermark signals can be extracted by checking the location of the center of mass in the mother and child blocks.

Third, a method for image authentication in color images has been proposed, in which authentication signals and embedding locations are generated by two keys. The concept of edge direction is also used in this method. By modifying the degree of the edge direction of the child blocks, authentication codes can be embedded in them. The stego-image in suspicion can be judged as being tampered with or not by checking the difference between the authentication codes and the extracted ones from the child blocks.

Fourth, a method for data hiding in binary images has been proposed. A reference table is created to hide up to three bits in each block. With the help of a reference table, data can be embedded with less distortion. In the extraction process, the watermark signals can be extracted by table lookup according to the reference table.

Finally, a method for integration of watermark and authentication signals in binary document images is proposed. It is based on the works of Tseng and Tsai [1-2] in which they proposed a method to embed watermark signals and authentication signals, respectively. Because the two methods use identical block sizes, if we combine these two methods for embedding watermark and authentication signals together in a cover

image, conflicts will occur. We thus proposed an integration method to solve the problem. It is found in this study that a watermark and an authentication signal can co-exist in a binary document image. The integrity of binary document images can be verified by extracting the authentication signals and the watermark signals can be detected for copyright protection at the same time.

7.2 Suggestions for Future Works

Data hiding methods for tampering detection and copyright protection in digital images have been proposed in this study. However, some attractive and interesting topics that are related to this study are worth further research. Several suggestions for future works are listed as follows.

1. Extending the proposed methods to other kinds of digital media, such as video, audio, and other image types.
2. Keeping the document image quality good after embedding a large amount of data.
3. Increasing the capacity of data hiding.
4. Authenticating the integrity of a stego image more precisely.
5. Authenticating the integrity of totally black or white blocks in a binary document image.

References

- [1] Chih-Hsuan Tzeng and Wen-Hsiang Tsai, "A New Approach to Authentication of Binary of Binary Images for Multimedia Communication With Images for Multimedia Communication With Distortion Reduction and Security Distortion Reduction and Security Enhancement," *IEEE COMMUNICATIONS LETTERS*, Vol. 7, No. 9, SEP. 2003, pp. 443-445.
- [2] C. H. Tzeng and W. H. Tsai, "Hiding authenticable general digital information behind binary images with reduced distortion," in *Proc. of the 2nd Workshop on Digital Archives Technologies*, Taipei, Taiwan, R. O. C, Jul. 2003, pp. 119-123.
- [3] Young-Won Kim and Il-Seok Oh, "Watermarking text document images using edge direction histograms," *Pattern Recognition Letters* Vol. 25, May 25, 2004, pp. 1243-1251.
- [4] Shapiro, L.G., Stockman, G.C., *Computer Vision*. Prentice Hall, 2001.
- [5] R.C. Gonzalez and R. E. Woods, "Digital Image Processing," second edition, 2002, pp. 135-136.
- [6] Christophe De Vleeschouwer, Jean-François Delaigle and Benoît Macq, "Circular Interpretation of Bijective Transformations in Lossless Watermarking for Media Asset Management," *IEEE TRANSACTION ON MULTIMEDIA*, Vol. 5, No. 1, MARCH 2003, pp. 97-105.
- [7] Amano, T., Misaki, D., "A feature calibration method for watermarking of document images," *Proc. ICDAR*, 1999, pp. 91-94.
- [8] Young-Won Kim, Kyung-Ae Moon and Il-Seok Oh, "A Text Watermarking Algorithm based on Word Classification and Inter-word Space Statistics," *Proceedings of the Seventh International Conference on Document Analysis and*

Recognition (ICDAR 2003), 2003.

- [9] C. Y. Lin and S. F. Chang, "Distortion Modeling and Invariant Extraction for Digital Image Print-and-Scan Process," *Proceeding of International Symposium on Multimedia Information Processing (ISMIP)*, Taipei, Taiwan, Dec. 1999.
- [10] Pei. Ying. Huang and Wen-Hsiang. Tsai, "New and Integrated Techniques for Information Hiding in Images for Copyright Protection, Covert Communication, and Tampering Detection," *M. S. Thesis*, Department of Computer and Information Science, National Chiao Tung University, Hsinchu, Taiwan, Republic of China, June 2003.
- [11] Y. C. Chiu and W. H. Tsai, "A study on Digital Watermarking and Authentication of Images for Copyright Protection And Tampering Detection," *M. S. Thesis*, Department of Computer and Information Science, National Chiao Tung University, Hsinchu, Taiwan, Republic of China, June 2004.
- [12] C. Y. Yin and W. H. Tsai, "Copyright and annotation protection in digital museums by using data hiding, watermarking, and image authentication techniques," *M. S. Thesis*, Department of Computer and Information Science, National Chiao Tung University, Hsinchu, Taiwan, Republic of China, June 2001.
- [13] Min Wu and Bede Liu, "Data Hiding in Binary Image for Authentication and Annotation," *IEEE TRANSACTIONS ON MULTIMEDIA*, Vol. 6, No. 4, AUGUST 2004, pp. 528-538.
- [14] Jeanne Chen , Tung-Shon Chen and Meng-Wen Cheng, "A New Data Hiding Method in Binary Image," *Multimedia Software Engineering* ,Proceedings. Fifth International Symposium, 2003, pp. 88 – 93.
- [15] Y. J. Cheng and W. H. Tsai, "Copyright and Integrity Protection for Images by

Removable Visible Watermarking Techniques,” *M. S. Thesis*, Department of Computer and Information Science, National Chiao Tung University, Hsinchu, Taiwan, Republic of China, June 2002.

- [16] M. Wu and B. Liu, “Watermarking for image authentication,” *Proceedings of IEEE International Conference on Image Processing*, Chicago, Illinois, Vol. 2, October 1998, pp. 437-441.
- [17] D. C. Wu and W. H. Tsai, “Embedding of any type of data in images based on a human visual model and multiple-based number conversion,” *Pattern Recognition Letter*, Vol. 20, 1999, pp. 1511-1517.
- [18] M. Wu and M. L. Miller, J. A. Bloom, and I. J. Cox, “A rotation, scale and translation resilient public watermark,” *Proceedings of 1999 IEEE International Conference on Acoustics, Speech, and Signal Processing*, Phoenix, AZ USA, Vol. 4, March 15-19, 1999, pp. 2065.
- [19] J. J. K. O’Ruanaidh and T. Pun, “Rotation, scale and translation invariant digital image watermarking,” *Proceedings of IEEE International Conference on Image Processing*, Santa Barbara, CA USA, Vol. 1, Oct. 26-29, 1997, pp. 536-539.
- [20] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, “A digital watermark,” *Proceedings of IEEE International Conference on Image Processing*, Vol. 2, 1994, pp. 86-90.
- [21] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, “A digital watermark,” in *Proc. IEEE Int. Conf. Image Processing*, Vol. II, 1994, pp. 86–90.
- [22] J. T. Brassil, S. Low and N. F. Maxemchuk, ”Copyright Protection for the Electronic Distribution of Text Documents,” *Proceedings of the IEEE*, July 1999, pp.1181-1196.
- [23] J. T. Brassil, S. Low, N. F. Maxemchuk, and L. O’Gorman, “Marking text

features of document images to deter illicit dissemination,” *Int. Conf. Pattern Recognition*, Israel, 1994, pp. 315-319.

[24] HUANG D and YAN H, "Interword Distance Changes Represented by Sine Waves for Watermarking Text Images", *IEEE Transactions on Circuits and Systems for Video Technology*, 11(12), December 2001, pp 1237-1245.

[25] A. Bhattacharjya, H. Ancin, "Data embedding in text for a copier system," *Proc. ICIP*, No.2, 1999, pp.245–249.

