Segment-based and reversible techniques in data hiding for binary images

Gao, Yupeng

2007

Gao, Y. (2007). Segment-based and reversible techniques in data hiding for binary images. Master's thesis, Nanyang Technological University, Singapore.

<https://hdl.handle.net/10356/3513>

<https://doi.org/10.32657/10356/3513>

Nanyang Technological University

Downloaded on 26 Apr 2023 16:33:38 SGT

SEGMENT-BASED AND REVERSIBLE TECHNIQUES IN DATA HIDING FOR BINARY IMAGES

GAO YUPENG

SCHOOL OF ELECTRICAL & ELECTRONIC ENGINEERING

NANYANG TECHNOLOGICAL UNIVERSITY

2007

Segment-based and Reversible Techniques in Data Hiding for Binary Images

GAO YUPENG

SCHOOL OF ELECTRICAL & ELECTRONIC ENGINEERING

A thesis submitted to the Nanyang Technological University
in fulfillment of the requirement for the degree of
Master of Engineering

2007

Statement of Originality

I hereby certify that the work embodied in this thesis is the result of original research and has not been submitted for a higher degree to any other University or Institution.

.....

Date

.....

Gao Yupeng

Acknowledgments

First of all, I would like to express my sincere gratitude to my supervisor, Prof. Kot Chichung, Alex, for his precious time, patient guidance, invaluable experience, helpful instructions on this research and persistent encouragement through the tough time of my study towards the Master of Engineering degree. His knowledge, wisdom, kindness and spirit have benefited me for these years and will benefit me for my whole life.

I am very grateful to Dr. Liu Jun for guiding me, giving me valuable and detailed instructions on my research. Taking this opportunity, I would also like to thank specially my colleague Ms Yang Huijuan, for her great help on reviewing my thesis, and thank the fellow colleagues and graduate students Chen Jianping, Zeng Jiancheng, Cheng Jun and Cao Hong, with whom I always had helpful discussions and shared ideas. I also take pleasure to thank the technicians in Workstation Resource Lab Mr. Chu Chun Chung and Ms. Teo Boon Ping, who provided me a lot of technical supports whenever I needed.

Finally, I want to thank my loved parents for teaching me the importance of hard work and perseverance, and for their love and encouragement. I would like to thank my sister Gao Yuyan and my dear girlfriend Liu Wenjing, for their love, care and support. Without them I could never accomplish this thesis. I would also like to thank all my friends to give me the strength to go on.

Thanks again to all people who have helped me in one way or another.

Table of Contents

CHAPTER 1	
INTRODUCTION	1
1.1 Motivation	1
1.2 Objectives.....	3
1.3 Major Contributions of the Thesis.....	4
1.4 Organization of the Thesis	4
 CHAPTER 2	
DIGITAL WATERMARKING BASICS	6
2.1 A General Framework of Watermarking	6
2.2 Digital Image Watermarking Requirements and Categories	9
2.2.1 Perceptibility	9
2.2.2 Robustness	10
2.2.3 Watermark Extraction.....	11
2.2.4 Watermarking Domain	11
2.2.5 Reversibility	12
2.2.6 Watermark Security.....	12
2.2.7 Embedding Capacity.....	13
2.2.8 Complexity.....	13
 CHAPTER 3	
LITERATURE REVIEW ON DATA HIDING IN BINARY IMAGES	14
3.1 Previous Work for Binary Images	14
3.2 The Proposed Algorithms and Assumptions.....	18

CHAPTER 4	
PROPOSED SEGMENT-BASED WATERMARKING METHOD	21
4.1 Proposed Segment-based Watermarking Method	21
4.1.1 Introduction to Block-based Watermarking Method.....	21
4.1.2 Overview of the Proposed Segment-based Watermarking Method.....	23
4.1.3 Check “adding” and “reducing” Property.....	26
4.1.4 Embeddability of a Segment	33
4.2 Performance Evaluation on Proposed Segment-based Watermarking Method.....	35
4.2.1 Test Images and Distortion Measure	36
4.2.2 Experimental Results of the Proposed Segment-based Watermarking Method.....	38
4.2.3 Performance Comparison of Embedding Methods for Binary Images	43
4.3 Summary	51
 CHAPTER 5	
PROPOSED PATTERN-BASED REVERSIBLE WATERMARKING METHOD	52
5.1 Proposed Pattern-based Reversible Watermarking Method	52
5.1.1 Embedding Data	55
5.1.2 Embedding Pattern Information	57
5.2 Experimental Results of the Proposed Reversible Watermarking Method.....	63
5.3 Summary	69

CHAPTER 6	
SECURE AUTHENTICATION SYSTEM.....	70
6.1 Digital Signature Authentication System.....	70
6.2 Watermarking Authentication System.....	72
6.2.1 Authentication System Based On the Segment-based Data	
Hiding Algorithm	73
6.2.2 Authentication System Based On the Pattern-based Reversible	
Data Hiding Algorithm	75
6.3 Experimental Results	77
6.4 Summary	77
 CHAPTER 7	
CONCLUSION AND RECOMMENDATIONS	82
7.1 Conclusion.....	82
7.2 Recommendations	83
 BIBLIOGRAPHY	85
 APPENDIX I	
PARTIAL MATLAB CODE.....	94
 APPENDIX II	
EXAMPLE IMAGES	97

Summary

With the fast development of computer and internet, digital media is becoming more and more popular and begins to replace the traditional analog media in many areas. In the mean time, copyrights and authenticity of digital media are critical due to the ease of forging, distribution and modification of digital media. Therefore, digital watermarking is proposed to solve these problems. In the past, a lot of watermarking algorithms were proposed for copyright protection of digital media. Nowadays authenticity of digital media, especially authenticity of digital images, is gaining more interests from researchers. Most watermarking algorithms in this area are proposed for grayscale or color images, only a few are proposed for binary images. The existing watermarking methods for binary images either have low embedding capacity or have poor visual quality of watermarked images.

In order to solve the above-mentioned problems, we propose two fragile watermarking methods for binary images for the purpose of authentication in this thesis. The first method is a segment-based watermarking method. In the embedding process, a sequence of continuous black pixels segment is searched in a binary image from top to bottom, and then from left to right. After a segment is located, the pre-defined masks are used to check two ends of the segment to determine the properties of the segment for embeddability. For embeddable segments, a black pixel is added or removed at either end of the segment by using the odd or even number of black pixels in the segment to embed bit “1” or “0”. Since the modified locations are the selected corner pixels of the characters, this method can achieve low distortion for the marked image. The method also has a

higher embedding capacity than some of the existing binary watermarking methods.

A pattern-based reversible watermarking method is also proposed in this thesis. This method searches existent patterns in the cover image, and creates non-existent patterns from the existent ones to embed the message data. In the extraction process, the hidden message data is extracted and the watermarked image is restored to its original.

The performance of our proposed methods is evaluated in terms of the embedding capacity and the visual quality of the watermarked image. Distance-Reciprocal Distortion Measure (DRDM) is used to measure the visual quality of the watermarked binary document image. Experimental results show that the proposed segment-based watermarking method can achieve a good visual quality and higher embedding capacity than some binary document watermarking methods reported in literature. Furthermore, two watermarking authentication systems based on our proposed methods are also presented in this thesis. They can be used to detect any modification made to the watermarked document image and to verify the authenticity of the document image.

List of Figures

Figure 2.1: Generic Digital Watermark Embedding Process	8
Figure 2.2: Generic Digital Watermark Extraction Process.....	8
Figure 4.1: One of Commonly Used Blocks for Watermarking in Block-based Methods.....	23
Figure 4.2: A Simple Binary Image.....	23
Figure 4.3: An Image with Four Segments	24
Figure 4.4: Embedding Process	25
Figure 4.5: Extraction Process.....	25
Figure 4.6: A Segment with Five Black Pixels	27
Figure 4.7: An Example of Mask(A)	30
Figure 4.8: Generation Process of Binary Document Images	36
Figure 4.9: Hiding Effect on a Single Letter “a”	38
Figure 4.10: A Portion of a Document Image Containing Randomly Generated Words.....	41
Figure 4.11: A Regular Document Image	41
Figure 4.12: Embedding Rate of Document Images with Different Font Sizes and Resolutions	43
Figure 4.13: Original English Image and Watermarked Images by Our Segment-based Watermarking Method and Other Methods	46
Figure 4.14: Original Chinese Image and Watermarked Images by Our Segment-based Watermarking Method and Other Methods	47
Figure 4.15: Watermarked Images by Randomly Flipping the Edge Pixels..	48
Figure 4.16: Four Masks Used for Comparing Different Watermarking Methods	50
Figure 5.1: An A4 Size Binary Document Image (1275×1649 pixels)	53
Figure 5.2: Histogram of Patterns within a 3×3 Block.	54

Figure 5.3: Architecture Overview of the Reversible Data Hiding	54
Figure 5.4: Constitution of Record R	62
Figure 5.5: Components in i^{th} Block	62
Figure 5.6: Bit Sequence in a 3×3 Block	63
Figure 5.7: A Portion of the Original Text Image	65
Figure 5.8: A Portion of the Watermarked Image with 789 Bits Embedded .	65
Figure 5.9: Enlarged Portion of the Watermarked Image	66
Figure 6.1: Overview of Digital Signature.....	71
Figure 6.2: Watermarking Authentication System Based on Proposed Segment-based Method	74
Figure 6.3: Watermarking Authentication System Based on Proposed Reversible Method	76
Figure 6.4: Authentication Results	78
Figure 6.5: Authentication Results.....	79
Figure 6.6: Authentication Results.....	80
Figure 6.7: Authentication Results.....	81

List of Tables

Table 4.1: Sixteen Non-overlapping Categories Representing the Properties of a Segment	34
Table 4.2: Embedding Capacity of the Proposed Segment-based Method	40
Table 4.3: Embedding Capacity of Different Watermarking Methods for Binary Document Images	44
Table 4.4: Distortion Measure Results of Different Watermarking Methods for Binary Document Images.....	48
Table 4.5: Embedding Capacity of the Segment-based Method and the Block-based Method Based on the Same Masks	50
Table 5.1: Distribution of Patterns within a 3×3 Block	64
Table 5.2: Five Marker-pairs Used in the Experiment	67
Table 5.3: Embedding Capacity of Different Computer-generated Document Images	68

CHAPTER 1

INTRODUCTION

1.1 Motivation

With the fast development of computer and internet techniques, digital multimedia (image, video and audio) is becoming more and more popular and it is replacing the traditional analog one in many applications [1]. Comparing to analog multimedia, digital multimedia has the following advantages: simple editing, easy distribution, higher quality, and so on. However, these advantages also bring the dark side of the digital multimedia. People can easily distribute and modify pictures, movies and MP3 songs by using internet and some special softwares. The copyright and the authenticity of the digital contents are threatened.

In order to protect the copyright and the authenticity of the digital media, digital watermarking is proposed. It is a process in which some specified information is embedded in the digital media to be protected and subsequently the specified information can be extracted from the watermarked digital media. The specified information is called *watermark*, and the digital media to be protected is called *cover media*. After the embedding process, a new digital media containing the watermark is obtained and it is called *watermarked media*. The watermarked media should have little difference from the cover media. The watermark must be able to be extracted from the watermarked media, and no watermark is expected from the cover media and other unwatermarked media. For copyright protection, the watermark will be destroyed only if the watermarked media is badly destroyed. This kind of watermarking is called *robust watermarking*. To ensure the

CHAPTER 1. INTRODUCTION

authenticity of the digital media, the extracted watermark will be different from the embedded one if the content of the watermarked media is modified. This kind of watermarking is called *fragile watermarking*. In this thesis, *data hiding*, *digital watermarking* and *steganography* are used interchangeably. Nevertheless, strictly speaking, there are some differences between them, as described below:

- ◆ Data hiding: also called *information hiding*, is a general term encompassing a wide range of problems beyond that of embedding messages in content. The term *hiding* here can refer to either making the information imperceptible or keeping the existence of the information secret [48].
- ◆ Digital watermarking: initially this term only stands for the copyright protection applications, in which embedding capacity, robustness and perceptibility are the three important properties. Its focus is the media itself and the data embedded is related to the cover media. Nowadays this term means any process which embeds some data in the media.
- ◆ Steganography: its original purpose is to transmit information secretly [2]. Its focus is the hidden information. Here it refers to the algorithms designed for ensuring the integrity and authenticity of digital media.

Our main purpose is to hide information in binary images, mainly in text images, to ensure their integrity and authenticity.

In the literature, only a few data hiding methods were proposed for binary text/document images while many have been proposed for grayscale and color images. However, the methods proposed for grayscale and color images cannot be applied to binary text images directly. It is a challenging task to embed information in binary text images because there are only black and white pixels in them.

CHAPTER 1. INTRODUCTION

Information can be embedded by flipping pixels from black to white or vice versa, but the changes will be noticeable if the embedding process is not done properly. Comparing to grayscale and color images, binary images occupy less storage space while the visual quality maintains. Among the existing data hiding methods for binary images, some of them embed data in binary text images without causing perceptual distortion but their embedding capacity is small. Some methods have a large embedding capacity but the original images are distorted too much after embedding. Motivated by those facts, in this thesis, we propose a novel segment-based data hiding method. It has a large capacity and at the same time the distortion can be controlled to keep a good perceptual quality of the watermarked images.

Furthermore, only one of the existent data hiding methods for binary images is reversible [71]. This method does not always work properly as the original image cannot always be reconstructed in the extraction process. Motivated by this fact, we also propose a reversible data hiding method for binary document image in this thesis. This method can embed data in binary document images without causing noticeable distortion. After the data is extracted, the original image can be reconstructed from the watermarked image.

1.2 Objectives

The first objective of this thesis is to develop a novel embedding method for binary images with minimum distortion, but with large capacity. The proposed method is applied to a secure authentication system for ensuring the integrity and authenticity of binary images. The second objective is to develop a reversible data hiding method due to the fact that there are few reversible data hiding methods for binary

CHAPTER 1. INTRODUCTION

images in literature. This method is more suitable for binary document image, and it focuses on reversibility and visual quality of the watermarked image.

1.3 Major Contributions of the Thesis

The major contributions in this thesis are the two novel data hiding methods proposed for digital binary images. One is a segment-based data hiding method, which has a large capacity with less visual distortion comparing to some existing methods. Its processing speed is also fast enough to be used in real time applications. The other one is a pattern-based reversible data hiding method, in which the original image can be reconstruct by providing the watermarked image in the extraction process. Both methods can be employed in a secure authentication system. Moreover, we analyze our proposed methods in terms of embedding capacity and visual quality of the watermarked images generated by them. Experimental results are shown in this thesis to support our claims.

1.4 Organization of the Thesis

We present in the next Chapter a general framework of a digital watermarking system, which includes the embedding process and the extraction process. The watermarking requirements are also presented. We categorize watermarking algorithms according to various requirements. Previous data hiding methods for binary images are reviewed in Chapter 3. Some assumptions of our proposed algorithms are also described. We present our proposed segment-based watermarking method in Chapter 4. The experimental results and performance comparison among the segment-based data hiding method and some existing data hiding methods are also included. In Chapter 5, we present the pattern-based

CHAPTER 1. INTRODUCTION

reversible data hiding method and the experimental results. We start Chapter 6 with digital signature authentication system, which is the state-of-the-art solution for authenticity of digital images. Then we present the watermarking authentication systems based on our proposed algorithms. Finally, conclusions are drawn and recommendations for future research work are presented.

CHAPTER 2

DIGITAL WATERMARKING BASICS

In this chapter, a general framework of digital watermarking is presented. Usually a digital watermarking algorithm consists of watermark embedding process and watermark extraction process. In addition, the requirements of digital image watermarking and classifications of different methods are also described.

2.1 A General Framework of Watermarking

Digital watermarking is the practice of hiding a message about a digital image, audio clip, video clip, or other work of media within that work itself [48]. The hidden message, known as watermark, can be used for various purposes like copyright protection or content authentication. Generally a digital watermarking algorithm (*invisible watermarking*) consists of two parts: watermark embedding process at the sender side and watermark extraction process at the receiver side. Some digital watermarking algorithms (*visible watermarking*) only have watermark embedding process. The typical processes are presented and explained below.

Watermark Embedding Process

The generic watermark embedding process [3] is shown in Figure 2.1. The inputs consist of the cover media, the watermark and an optional secret/public key. The cover media is the digital media we want to protect or authenticate. It can be a digital image, digital audio, digital video or digital document. The watermark is the

CHAPTER 2. DIGITAL WATERMARKING BASICS

information being embedded in the cover media. It could be a number, a text string, an image, or a combination of the above. A secret or public key can be used to make the watermark more secure. An unauthorized party could not extract the watermark if he does not know the key. The watermarking techniques using a secret or public key are usually referred to as *secret* or *public watermarking* [4, 5].

Watermark Extraction Process

The generic watermark extraction process [3] is illustrated in Figure 2.2. The inputs consist of the test media, the optional cover media and the optional secret/public key. If the extraction process requires the cover media, it is usually called *non-blind watermarking* algorithm. Otherwise, it is called *blind watermarking* algorithm. The outputs consist of the retrieved watermark and the optional original cover media. The retrieved watermark can be classified into three forms. The first form is to tell whether there is a watermark in the test media. It is not required to extract the watermark exactly the same as the embedded one. The second form is the exact watermark, such as a number, a text, etc. The third form is a watermark which may be a little different from the embedded one. When the watermark is a logo, we can identify it although it is degraded. The extraction algorithm is called *reversible watermarking* algorithm if it can reconstruct the original cover media.

CHAPTER 2. DIGITAL WATERMARKING BASICS

Figure 2.1: Generic Digital Watermark Embedding Process.

Figure 2.2: Generic Digital Watermark Extraction Process.

2.2 Digital Image Watermarking Requirements and Categories

Different applications have different requirements on digital watermarking algorithms. In this section, we shall review some of the requirements for digital image watermarking algorithms, and classify the watermarking algorithms according to the requirements.

2.2.1 Perceptibility

According to perceptibility, watermarking algorithms can be classified into *visible watermarking algorithm* [8, 14-16] and *invisible watermarking algorithm* [6, 17]. Visible watermarking algorithm is popular in an early stage of digital watermarking. It makes the watermark visible in the watermarked image so that one can easily know whom the watermarked image belongs to. However, it is very easy for an adversary to remove the watermark because the location of the watermark is known. In addition, the visible watermark will destroy the visual quality of part of the image. Therefore, nowadays most watermarking algorithms are invisible algorithms.

Invisible watermarking techniques embed the watermark invisibly in the image, and the watermark embedding process should not introduce any perceptible artifacts into the cover image. It is difficult to tell whether or not and where an image contains the watermark if invisible watermarking algorithms are used, and the watermark is spread over the whole image. As a result, the security of invisible watermarking algorithms is higher than that of visible watermarking algorithms. The methods proposed in this thesis are invisible watermarking algorithms.

2.2.2 Robustness

Watermarking algorithms can be classified into *robust watermarking algorithm*, *fragile watermarking algorithm* and *semi-fragile watermarking algorithm* based on watermark robustness. The robust watermarking is used to protect the copyright of the digital image [18], therefore an ideal robust watermark should resist any kind of attack. But it is also impossible as there is no absolute robustness for digital watermarking. What a robust watermark can do is to discourage illegal copies, or to increase pirates' cost to do so. An attack to an image can be viewed as any method that will change the existing form of the image (e.g. image scaling) or modify the pixel values of the image (e.g. JPEG compression). Stirmark and Checkmark, which include most well-known attacks so far, are the two main benchmarking tools used to test the robustness of a watermarking method [19, 20].

A fragile watermark is a mark that is readily altered or destroyed when the cover image is modified through a linear or nonlinear transformation [21]. The fragile watermarking can be used to authenticate and detect any modification to the digital images [22-26]. The methods proposed in this thesis belong to fragile watermarking algorithms.

Another type of algorithm called semi-fragile watermarking is proposed recently [27-30]. Its robustness is between robust watermarking and fragile watermarking. A semi-fragile watermark is also sensitive to most attacks but can survive some pre-defined attacks (e.g., JPEG compression). Therefore, it can be used to tolerate incidental distortions but reject malicious modifications.

2.2.3 Watermark Extraction

According to the way of watermark extraction, watermarking algorithms can be classified into *source extraction algorithm* [16] and *destination extraction algorithm*. Source extraction algorithms, which are also called private or non-blind watermarking [6], require both the original cover image and the test image to extract the watermark. They cannot be used in authentication applications because there is no original cover image at the receiver side in those applications. Destination extraction algorithms, which are also called public or blind watermarking, need a key instead of the original cover image for watermark extraction. The size of the key is usually much smaller than that of the original cover image. The methods proposed in this thesis are destination extraction algorithms.

2.2.4 Watermarking Domain

Watermarking algorithms can be classified into *spatial domain algorithm* [17, 22, 32-34] and *transform (frequency) domain algorithm* [16, 31] according to watermarking domain. Spatial domain algorithms embed watermark by changing the pixel values of the cover image directly, while transform domain algorithms embed watermark by changing the coefficients of the transformed cover image in transform domain. The commonly used transforms include Discrete Cosine Transform, Hadamard Transform, etc. Usually embedding watermark in transform domain is more robust than embedding watermark in spatial domain. Transform domain algorithms are mainly used for grayscale and color image watermarking [35] because they may cause high distortion when applying to binary image

CHAPTER 2. DIGITAL WATERMARKING BASICS

watermarking [36], so spatial domain algorithms are often used for binary image watermarking. The methods proposed in this thesis belong to spatial domain algorithms.

2.2.5 Reversibility

According to reversibility, watermarking algorithms can be classified into *non-reversible watermarking algorithm* and *reversible watermarking algorithm*. Non-reversible watermarking algorithms cannot reconstruct original cover image at the time they extract the watermark from the watermarked image. Original cover images are desirable in some applications such as medical and military imaging. Therefore, reversible watermarking algorithms are useful. Here reversibility means that the marked image can be reversed to the original cover image without any distortion after the hidden data are retrieved [37-47]. Our proposed segment-based data hiding method is non-reversible, while the proposed pattern-based watermarking method is reversible.

2.2.6 Watermark Security

Watermark security is another important requirement for digital watermarking algorithms. The watermark should not be replaced by the adversary. In order to protect the watermark, a secret key should be used to control the insertion of the watermark in the cover image [48].

2.2.7 Embedding Capacity

Embedding capacity measures the amount of information that can be hidden in the cover image [49]. Some applications of watermarking need a small capacity such as embedding person's name in the cover image. However, some applications require a large capacity such as embedding an image in the cover image. It is good for a fragile watermarking algorithm to have a large capacity and at the same time keeping the nice visual quality of the watermarked image.

2.2.8 Complexity

Computational complexity of the watermark embedding and extraction processes is another requirement. It is important that the algorithms must operate efficiently in some real-time applications.

CHAPTER 3

LITERATURE REVIEW ON DATA HIDING IN BINARY IMAGES

In this chapter, we briefly review the existing binary image watermarking algorithms, and describe some assumptions of our proposed digital watermarking algorithms.

3.1 Previous Work for Binary Images

Many digital watermarking methods for grayscale and color images have been discussed in [7-13]. In this thesis we only focus on binary document images, so the works on other types of binary images like halftone image [74, 75] are out of the scope of this thesis. An overview on the recent development of document image watermarking has been given in [50, 51]. According to the embedding methods, binary document watermarking algorithms can be roughly divided into two groups: *space shifting algorithms* and *pixel flipping algorithms*. We will talk about them briefly in the following.

Space Shifting Algorithms

In document images there are many spaces, such as spaces between paragraphs, between text lines, between words, and between characters. Watermarking methods [17, 52-59] belonging to this group embed information by modifying these spaces instead of flipping the pixel values (from black to white, or vice versa)

CHAPTER 3. LITERATURE REVIEW ON DATA HIDING IN BINARY IMAGES

in binary document images. Space shifting algorithms can achieve good visual quality and robustness, but they have a smaller embedding capacity than pixel flipping algorithms.

Pixel Flipping Algorithms

Watermarking algorithms belonging to this group embed data by modifying the pixel values in binary images, which can be further divided into two sub-groups: character feature modification and block-based watermarking algorithm.

◆ Character Feature Modification

Brassil *et al.* [32-34] proposed some watermarking algorithms which embed data by modifying the top pixels of the vertical endlines in some letters like ‘b’, ‘d’ and ‘h’. However, the modification is sensitive to human eyes. Hu [60] proposed a document image watermarking method which divides the document into weight-invariant partitions in the spatial domain using the neighborhood pixel ratio. Watermark is embedded in different partitions. This method is used for copyright protection. Amamo and Misaki [61] proposed a feature calibration scheme for embedding data in document images. It partitions an image symmetrically into two sets. The watermark is embedded in one set. In the extraction process, the watermark is extracted by comparing the differences between the two sets. The embedding capacity of the method is not high. Mei *et al.* [62] proposed a data hiding method to embed data by using a fixed set of pairs of five-pixel long boundary patterns. Flipping the pixel in one pattern in each pair will result in the other pattern in the same pair. The visual quality of the watermarked image is good

CHAPTER 3. LITERATURE REVIEW ON DATA HIDING IN BINARY IMAGES

because the flipped pixels lie at the boundary of a character. Flipping pixels at this area is not sensitive to human eyes.

Tsai *et al.* [71] proposed the only reversible data hiding method for binary images using PWLC (Pair-wise Logical Computation) to the best of our knowledge. PWLC scans the cover image in the raster order, e.g. from top to bottom then from left to right, and looks for the sequences “000000” or “111111” near to the image boundaries. It converts “000000” to “001000” if a bit “0” is embedded and to “001100” if a bit “1” is embedded. Similarly, it converts “111111” to “110111” if a bit “0” is embedded and to “110011” if a bit “1” is embedded. However, how to identify the original sequence and the modified sequence in watermark extraction process is not described in the paper. For example, if a sequence “110011” is found in the extraction process, how to differentiate that it is the sequence existing in the original cover image or it is the sequence converted from “111111” after embedding process.

◆ Block-based Watermarking Method

Wu *et al.* [63] proposed a method to embed data in blocks of binary images by employing the shuffling technique. An embedding score for each pixel within a block can be calculated and this score determines whether the pixel can be flipped or not. The shuffling technique is used to ensure at least one flippable pixel in each block in shuffled domain. If the shuffling key is not selected properly, relatively large distortion will appear for small size blocks. In order to control the visual quality, a larger block size is required, e.g., 12-pixel $\times$ 12-pixel.

Lu *et al.* [64, 65] proposed a novel objective distortion measure called Distance-Reciprocal Distortion Measure (DRDM) for binary document images.

CHAPTER 3. LITERATURE REVIEW ON DATA HIDING IN BINARY IMAGES

This measure is based on the reciprocal of distance from the flipped pixel to its surrounding pixels. They also proposed a data hiding method based on DRDM. One bit can be embedded in a fixed-size non-uniform block by modifying the odd/even feature of the block. If a pixel in the block needs to be flipped, the one with minimum DRD value, which causes minimum distortion, will be flipped. This method can generate watermarked images with good visual quality, but the capacity depends on the block size.

Tseng *et al.* [66, 67] proposed a secure data hiding method with high capacity for binary images. The method enables us to embed as many as r bits ($2^{r+1} - 1 \leq m \times n$) of data into a $m \times n$ block by flipping maximum two pixels. Whether a block can be used to embed data is determined by the data to be hidden, the block itself, a key matrix and a weight matrix. The key matrix and the weight matrix are only known to the sender and the receiver, which makes the method secure. The capacity of the method is high but the distortion of the watermarked image is not controlled well. Hirohisa [68] proposed a watermarking scheme based on [66, 67]. The new scheme adopts new key matrices and new ways to decide whether a block can be used to embed data, so the capacity is increased and at the same time the visual quality of the watermarked image can be better controlled.

Yang and Kot [69] proposed a method to embed data in binary images using noise suppression patterns in 5×5 neighborhood. It has a moderate embedding capacity and the watermarked image has good perceptual quality. Retrieval of the watermark does not require the original image. However the secret key and the location map information are needed for the retrieval. In [73] they proposed another blind data hiding method for document images by using the connectivity-preserving patterns in a local neighborhood. They use three criteria

CHAPTER 3. LITERATURE REVIEW ON DATA HIDING IN BINARY IMAGES

to determine the flippability of a pixel in a 3×3 moving window which is centered at the pixel. After that they use some rules to determine the embeddability of the block containing the moving window, and data is only embedded in embeddable blocks. The method can achieve good visual quality with reasonable embedding capacity.

In summary, pixel flipping algorithms can achieve higher capacity but less visual quality than space shifting algorithms. Most block-based watermarking method can achieve high capacity and reasonable visual quality simultaneously by flipping pixels which are not sensitive to human eyes. They are more suitable for authentication of binary document images since this application requires the capacity to be at least 1024 bits for any size of image. However, block-based watermarking methods have a common problem that they lost much capacity by dividing the cover image into blocks with fixed sizes. Block-based watermarking methods usually embed one bit in each block if they can find an embeddable location in the block. If two or more embeddable locations exist in one block, only one of them can be used for embedding and others are discarded.

3.2 The Proposed Algorithms and Assumptions

By reviewing the existing algorithms, it can be seen that there are not many data hiding methods for binary document images. Due to the problem existing in block-based watermarking methods, we propose a fragile segment-based watermarking method in this thesis. It can achieve higher embedding capacity than block-based methods and at the same time it can achieve good visual quality, due to the fact that it embeds data by flipping the corner pixels of a character.

CHAPTER 3. LITERATURE REVIEW ON DATA HIDING IN BINARY IMAGES

Another observation can be made by reviewing the existing algorithms is that there isn't any applicable reversible data hiding method for binary document image. This will limit the application of digital watermarking. Therefore, we propose a pattern-based reversible watermarking method for document images in this thesis, which is implemented using Matlab program.

Some assumptions of the proposed algorithms are discussed below:

- **Applicable images**

The algorithms proposed in this thesis are applicable to all kinds of binary images. However, the experiments and analysis made in this thesis are mainly on binary text images.

- **Robustness**

The proposed methods in this thesis are fragile watermarking methods for authentication purpose, so robustness is not our concern and there is no robustness test in this thesis.

- **Noise**

In this thesis, we consider the whole scheme only in digital domain and assume there is no noise during any transmission.

- **The watermark**

In this thesis, we use a randomly generated bit stream of "0"s and "1"s as the watermark in our experiments. If we use meaningful watermarks, such as names, numbers or images, similar results will be obtained.

- **Security concerns for the application**

We focus on the embedding and extraction process in this thesis. Although we employ some cryptographic methods, we do not discuss them in detail.

CHAPTER 3. LITERATURE REVIEW ON DATA HIDING IN BINARY IMAGES

- **Simulation environment**

In our experiments, the simulation results are obtained from the computer with 2.8GHz CPU (Pentium 4) and 512MB memory. The computer is running in Windows XP operation system. MATLAB 6.5 and Visual C++ 6.0 are used to conduct the experimental simulation.

CHAPTER 4

PROPOSED SEGMENT-BASED WATERMARKING METHOD

In this chapter, a segment-based watermarking method for binary images is proposed. The performance of the proposed method is evaluated in terms of visual quality of the watermarked images and embedding capacity when applying to binary document images. After that, we compare our segment-based watermarking method with some other existing methods on visual quality and embedding capacity by applying them to the same binary document images. The data being embedded in the images in our experiments is the random sequence of “1”s and “0”s.

4.1 Proposed Segment-based Watermarking Method

In this section, we will first introduce block-based watermarking method briefly, and then we present the overview of the proposed segment-based watermarking method, after that we discuss the details of how the method works.

4.1.1 Introduction to Block-based Watermarking Method

From previous chapters, we know that capacity and visual quality of the watermarked image are the two main requirements for fragile binary document image watermarking. In order to achieve a high capacity, block-based watermarking method is the better choice than space shifting method. Block-based

CHAPTER 4. PROPOSED SEGMENT-BASED WATERMARKING METHOD

watermarking methods work in the following way. They divide the original image into blocks with fixed size and then use some rules to check whether data could be embedded in or extracted from these blocks [63, 69, 73]. These blocks could be non-overlapping or overlapping at most one column horizontally or one row vertically with each other. In order to achieve good visual quality of the watermarked image, usually the pixels (black pixels or white pixels) being flipped locate at the corners of each character. Figure 4.1 shows one of the blocks that are most commonly used for embedding data in block-based watermarking methods. P could be a black pixel or a white pixel. Data is embedded in the block by flipping P from black to white or vice versa, depending on the bit to be hidden. However, the drawback of block-based methods is that the number of corner pixels they can find is quite dependent on how the image is divided into blocks. In most cases they cannot locate all the corner pixels. Therefore, the capacity of block-based methods is limited. This problem is illustrated in Figure 4.2. If block-based watermarking methods divide the image starting from the first column, as shown within the red boundary, no data can be embedded although there is one embeddable block in the image. Therefore, we manage to solve this problem by finding out all the corner pixels first, and then we use pre-defined masks to check whether these pixels can be used for embedding. In this way we can use a larger amount of pixels to embed data and achieve a higher capacity without lowering the visual quality of the watermarked image.

CHAPTER 4. PROPOSED SEGMENT-BASED WATERMARKING METHOD

Figure 4.1: One of Commonly Used Blocks for Watermarking in Block-based Methods.

Figure 4.2: A Simple Binary Image.

4.1.2 Overview of the Proposed Segment-based Watermarking Method

In the embedding process, our proposed method searches for all the segments in an image, and then uses the pre-defined masks to check the properties of each segment. After that, the embeddability of each segment is determined by its properties. Lastly, the data is embedded by modifying the length of the embeddable segments. Here, a *segment* is defined as a row of continuous black pixels, and the length of the segment is the number of black pixels it contains.

CHAPTER 4. PROPOSED SEGMENT-BASED WATERMARKING METHOD

Figure 4.3 shows four segments, S1 to S4. In the extraction process, whether data can be extracted from a segment depends on the property of that segment, which is decided by the same masks used in the embedding process. Figure 4.4 and Figure 4.5 demonstrate the embedding and extraction process of the method, respectively.

Figure 4.3: An Image with Four Segments.

The embedding process can be summarized in the following 4 steps.

Step 1: Searching for a segment in a given binary image, from left to right and then top to bottom. Go to Step 2 if a segment is found.

Step 2: Checking the leftmost and rightmost black pixels of the segment and their immediate white pixels. Finding out whether the segment has “adding” or “reducing” property, and then go to Step 3.

Step 3: Checking the embeddability of the segment according to its “adding” and “reducing” properties. If the segment is not embeddable, then the current bit cannot be embedded, then go to Step 1 and continue the previous searching. Otherwise, go to Step 4.

Step 4: Updating the image by making the number of black pixels of the current segment to be even if a bit “0” is embedded, or making it to be odd if a bit “1” is

CHAPTER 4. PROPOSED SEGMENT-BASED WATERMARKING METHOD

embedded. Go to Step 1 to continue the search. The embedding process will stop after all the data bits are embedded.

Figure 4.4: Embedding Process.

Figure 4.5: Extraction Process.

CHAPTER 4. PROPOSED SEGMENT-BASED WATERMARKING METHOD

The extraction process can be summarized in the following 3 steps.

Step 1: Searching for a segment in a test binary image, from left to right and then top to bottom. Go to Step 2 if a segment is found.

Step 2: Checking whether the segment has the “adding” property. If it does, go to Step 3; else go to Step 1 and continue searching.

Step 3: Extracting data bit according to the odd/even feature of the segment. A bit “1” is extracted if the length of the segment is odd, and a bit “0” is extracted if the length of the segment is even. Repeat Step 1 to Step 3 until all the bits are extracted.

4.1.3 Check “adding” and “reducing” Property

The “adding” and “reducing” properties of a segment are explained by using Figure 4.6. It shows a given segment with five black pixels. B_L and B_R are the leftmost black pixel and the rightmost black pixel of the segment, respectively. W_L and W_R are their immediate white pixels, respectively. If either W_L or W_R or both can be flipped to black, then the segment has the “adding” property. That is to say, black pixel(s) can be added to the segment. If either B_L or B_R or both can be flipped to white, then the segment has the “reducing” property. That is to say, black pixel(s) can be reduced from the segment. If a segment has only one black pixel, B_L and B_R point to the same pixel and the segment does not have the “reducing” property. It is also possible that a segment has neither the “adding” nor the “reducing” property.

CHAPTER 4. PROPOSED SEGMENT-BASED WATERMARKING METHOD

	W_L	B_L				B_R	W_R		

Figure 4.6: A Segment with Five Black Pixels.

The “adding” and “reducing” properties of a segment can be determined using the following four masks: Mask(A), Mask(B), Mask(C) and Mask(D).

x	x	1	x
0	0	$P_{(i,j)}$	1
x	x	0	x

Mask(A)

x	0	0	0
0	0	$P_{(i,j)}$	1
x	x	1	x

Mask(B)

x	1	x
1	$P_{(i,j)}$	0
x	0	x

Mask(C)

0	0	0
1	$P_{(i,j)}$	0
x	1	x

Mask(D)

Mask(A) and Mask(B) are used to check the left end of a segment, and Mask(C) and Mask(D) are used to check the right end of a segment. In order to ensure that the processed segment is not affected by the modification of next segment, the masks used to check the left end of a segment are different from those used to check the right end due to the fact that our method processes the segments in an image one by one from left to right. The discussion is given in the next section. If

CHAPTER 4. PROPOSED SEGMENT-BASED WATERMARKING METHOD

either end of a segment satisfies one of the four Masks, the segment has the “adding” or “reducing” property.

Assuming row number and column number start from 1, we can define the following parameters for the Masks:

i: row number, $2 \leq i \leq \text{image_height} - 1$.

j: column number, $3 \leq j \leq \text{image_width} - 2$.

1: black pixel.

0: white pixel.

x: don't care value, which can be either 1 or 0.

$P_{(i,j)}$: the pixel value at position (i, j) where we want to reduce or add a black pixel. $P_{(i,j)}$ could be either 1 or 0.

The elements in Mask(A) and Mask(B) can be represented in the following way:

$P_{(i-1,j-2)}$	$P_{(i-1,j-1)}$	$P_{(i-1,j)}$	$P_{(i-1,j+1)}$
$P_{(i,j-2)}$	$P_{(i,j-1)}$	$P_{(i,j)}$	$P_{(i,j+1)}$
$P_{(i+1,j-2)}$	$P_{(i+1,j-1)}$	$P_{(i+1,j)}$	$P_{(i+1,j+1)}$

We can write down the mathematical expressions for Mask(A) and Mask(B) as following:

$$\text{Mask(A): } L1_{(i,j)} = \bar{P}_{(i,j-2)} \wedge \bar{P}_{(i,j-1)} \wedge P_{(i,j+1)} \quad (4.1)$$

$$L2_{(i,j)} = P_{(i-1,j)} \wedge \bar{P}_{(i+1,j)} \quad (4.2)$$

CHAPTER 4. PROPOSED SEGMENT-BASED WATERMARKING METHOD

$$\text{Mask(B): } L1_{(i,j)} = \bar{P}_{(i,j-2)} \wedge \bar{P}_{(i,j-1)} \wedge P_{(i,j+1)} \quad (4.1)$$

$$L3_{(i,j)} = \bar{P}_{(i-1,j-1)} \wedge \bar{P}_{(i-1,j)} \wedge \bar{P}_{(i-1,j+1)} \wedge P_{(i+1,j)} \quad (4.3)$$

where $\bar{P}$ is the negation of P , ' $\wedge$ ' is the bitwise “AND” operation.

Therefore, the condition for the “adding” and “reducing” property of a segment on its left end can be expressed mathematically below.

$$\begin{aligned} C_L &= (L1 \wedge L2) \vee (L1 \wedge L3) \\ &= L1 \wedge (L2 \vee L3) \end{aligned} \quad (4.4)$$

where ' $\vee$ ' is the bitwise “OR” operation. When $C_L = 1$, $P_{(i,j)}$ is flippable.

Similarly, the mathematical expressions for Mask(C) and Mask(D) are:

$$\text{Mask(C): } R1_{(i,j)} = \bar{P}_{(i,j+1)} \wedge P_{(i,j-1)} \quad (4.5)$$

$$R2_{(i,j)} = P_{(i-1,j)} \wedge \bar{P}_{(i+1,j)} \quad (4.6)$$

$$\text{Mask(D): } R1_{(i,j)} = \bar{P}_{(i,j+1)} \wedge P_{(i,j-1)} \quad (4.5)$$

$$R3_{(i,j)} = \bar{P}_{(i-1,j-1)} \wedge \bar{P}_{(i-1,j)} \wedge \bar{P}_{(i-1,j+1)} \wedge P_{(i+1,j)} \quad (4.7)$$

And the condition for the “adding” and “reducing” property of a segment on its right end can be expressed mathematically below.

$$\begin{aligned} C_R &= (R1 \wedge R2) \vee (R1 \wedge R3) \\ &= R1 \wedge (R2 \vee R3) \end{aligned} \quad (4.8)$$

when $C_R = 1$, $P_{(i,j)}$ is flippable.

In order to extract data correctly, we must ensure that modifying the current processing segment will not affect the “adding” property of the processed

CHAPTER 4. PROPOSED SEGMENT-BASED WATERMARKING METHOD

segments. Due to the fact that our method processes the segments in an image from left to right and from top to bottom, what we need to show is that in the embedding process, the flip of $P_{(i,j)}$ will not affect the “adding” property of a segment on row $(i-1)$ and the previous segment on row i .

Proposition I: Adding/reducing one black pixel at the LEFT-end of the segment on row i will neither affect the “adding” property of the previous segment that at most ends at $(i, j-3)$ on row i , nor the “adding” property of the segment on row $(i-1)$.

Discussion:

We will first show that this is true for Mask(A). Figure 4.7 shows one situation for Mask(A). Segment 1 is the segment we are checking at the moment and $P_{(i,j)}$ could be its leftmost black pixel or the immediate white pixel to its leftmost black pixel. Segment 2 and segment 3 have been processed. Segment 2 lies on the row $(i-1)$ and segment 3 lies on the row i . Segment 4 lies on row $(i+1)$, which is not processed yet.

Figure 4.7: An Example of Mask(A).

CHAPTER 4. PROPOSED SEGMENT-BASED WATERMARKING METHOD

We only need to examine the following 4 locations: $(i, j-2)$, $(i-1, j-2)$, $(i-1, j-1)$ and $(i-1, j+1)$, since they might be the immediate white pixels next to the leftmost or rightmost black pixel of a segment and determine the “adding” property of that segment. If we can show flipping $P_{(i,j)}$ will not affect the flippability of those four locations, we will show that the statement is correct for $\text{Mask}(A)$. Let us examine them one by one.

- a)** The pixel at location $(i, j-2)$ might be an immediate white pixel to the rightmost black pixel of a segment. In Figure 4.7, it is an immediate white pixel to the rightmost black pixel of segment 3. If we take $(i, j-2)$ as the location we are checking, we can write down the “adding” conditions for segment 3 by using equation (4.5), (4.6) and (4.7):

$$R1_{(i,j-2)} = \overline{P}_{(i,j-1)} \wedge P_{(i,j-3)}$$

$$R2_{(i,j-2)} = P_{(i-1,j-2)} \wedge \overline{P}_{(i+1,j-2)}$$

$$R3_{(i,j-2)} = \overline{P}_{(i-1,j-3)} \wedge \overline{P}_{(i-1,j-2)} \wedge \overline{P}_{(i-1,j-1)} \wedge P_{(i+1,j-2)}$$

From $R1$, $R2$ and $R3$, we can observe that the “adding” property of segment 3 does not depend on $P_{(i,j)}$. Therefore, flipping $P_{(i,j)}$ will not affect the “adding” property of segment 3.

- b)** The pixel at location $(i-1, j-2)$ might be an immediate white pixel either to the leftmost black pixel of a segment or to the rightmost black pixel of a

CHAPTER 4. PROPOSED SEGMENT-BASED WATERMARKING METHOD

segment. If it is an immediate white pixel to the rightmost black pixel of a segment, we can write down the “adding” conditions for that segment by using equation (4.1), (4.2) and (4.3):

$$L1_{(i-1, j-2)} = \overline{P}_{(i-1, j-4)} \wedge \overline{P}_{(i-1, j-3)} \wedge P_{(i-1, j-1)}$$

$$L2_{(i-1, j-2)} = P_{(i-2, j-2)} \wedge \overline{P}_{(i, j-2)}$$

$$L3_{(i-1, j-2)} = \overline{P}_{(i-2, j-3)} \wedge \overline{P}_{(i-2, j-2)} \wedge \overline{P}_{(i-2, j-1)} \wedge P_{(i, j-2)}$$

From L1, L2 and L3, we can observe that the “adding” property of the segment does not depend on $P_{(i, j)}$. Therefore, flipping $P_{(i, j)}$ will not affect its “adding” property. Similarly, the conclusion is also true if the pixel at location $(i-1, j-2)$ is an immediate white pixel to the leftmost black pixel of a segment.

- c) The pixel at location $(i-1, j-1)$ might be an immediate white pixel to the leftmost black pixel of a segment. In Figure 4.7, it is the immediate white pixel to the leftmost black pixel of segment 2. We can write down the “adding” conditions for segment 2 by using equation (4.1), (4.2) and (4.3):

$$L1_{(i-1, j-1)} = \overline{P}_{(i-1, j-3)} \wedge \overline{P}_{(i-1, j-2)} \wedge P_{(i-1, j)}$$

$$L2_{(i-1, j-1)} = P_{(i-2, j-1)} \wedge \overline{P}_{(i, j-1)}$$

CHAPTER 4. PROPOSED SEGMENT-BASED WATERMARKING METHOD

$$L3_{(i-1, j-1)} = \overline{P}_{(i-2, j-2)} \wedge \overline{P}_{(i-2, j-1)} \wedge \overline{P}_{(i-2, j)} \wedge P_{(i, j-1)}$$

As a result, flipping $P_{(i, j)}$ will not affect the “adding” property of segment 2.

- d)** The pixel at location $(i-1, j+1)$ might be an immediate white pixel to the rightmost black pixel of a segment. In Figure 4.7, it is the immediate white pixel to the rightmost black pixel of segment 2. We can write down the “adding” conditions for that segment by using equation (4.5), (4.6) and (4.7):

$$R1_{(i-1, j+1)} = \overline{P}_{(i-1, j+3)} \wedge \overline{P}_{(i-1, j+2)} \wedge P_{(i-1, j)}$$

$$R2_{(i-1, j+1)} = P_{(i-2, j+1)} \wedge \overline{P}_{(i, j+1)}$$

$$R3_{(i-1, j+1)} = \overline{P}_{(i-2, j)} \wedge \overline{P}_{(i-2, j+1)} \wedge \overline{P}_{(i-2, j+2)} \wedge P_{(i, j+1)}$$

As a result, flipping $P_{(i, j)}$ will not affect the “adding” property of segment 2.

Similarly, we can show that **Proposition I** is also correct for Mask(B). Furthermore, we can use similar ways to show that it is correct that adding/reducing one black pixel at the RIGHT-end of the segment on row i will neither affect the “adding” property of the previous segment on row i , nor the “adding” property of the segment on row $(i-1)$.

4.1.4 Embeddability of a Segment

In the embedding process shown in Figure 4.4, after checking the “adding” and “reducing” properties of a segment, we also need to check the embeddability of the

CHAPTER 4. PROPOSED SEGMENT-BASED WATERMARKING METHOD

segment in order to determine whether it can be used to embed one bit. The rule of thumb is that if a segment is used to embed one bit, it should have the “adding” property after embedding process; if a segment is not used for embedding, it should not have the “adding” property after embedding process. In our method, one segment is used to embed one bit only.

From the previous Section 4.1.3, we know that four masks are used to check both ends of a segment to find out whether a black pixel can be added or reduced at the specific end. If we use “+” to represent that a black pixel can be added at the specific end, “-” to represent that a black pixel can be removed, and “none” to represent that a black pixel can neither be added nor be removed, a segment should belong to one of the following 16 non-overlapping categories shown in Table 4.1.

Table 4.1: Sixteen Non-overlapping Categories Representing the Properties of a Segment.

No.	Representation	No.	Representation
1	none, none	9	+, +
2	+, -	10	-, -
3	+&-, +&-	11	+&-, none
4	+, +&-	12	none, +&-
5	+&-, -	13	+, none
6	-, +	14	none, +
7	-, +&-	15	-, none
8	+&-, +	16	none, -

CHAPTER 4. PROPOSED SEGMENT-BASED WATERMARKING METHOD

We can use Figure 4.6 to explain the meaning of the above categories. The sign before comma describes the left end of a segment, and the sign after comma describes the right end of a segment. Therefore, in category 2 the signs “+, -” means W_L can be flipped to black pixel and B_R can be flipped to white pixel. In category 6, “+&-, none” means both W_L and B_L can be flipped but neither W_R nor B_R can be flipped. As long as a segment has a “+” sign, it has “adding” property. The partial MATLAB codes and sentences shown in Appendix I are used to illustrate how a segment is used to embed a data bit (1 or 0). L_s is the length of a segment, which is equal to the number of black pixels in the segment. From the process shown in Appendix I we can observe that if a segment is used for embedding, it always has the “adding” property after embedding process; if a segment is not used for embedding, it always does not have the “adding” property after embedding. This ensures that all the hidden data can be extracted correctly in the extraction process. Another observation is that sometimes although a black pixel is added to a segment, no bit is embedded, which is a drawback of our method.

4.2 Performance Evaluation on Proposed Segment-based Watermarking Method

In this section, the test images and distortion measure are introduced first, followed by the experimental results and comparison among the proposed method and other existing methods.

CHAPTER 4. PROPOSED SEGMENT-BASED WATERMARKING METHOD**4.2.1 Test Images and Distortion Measure****Generation of Test Binary Document Images**

Figure 4.8 demonstrates how we generate the binary document images used in our experiments. First we generate a Microsoft Word file. The font format of all texts used in our experiments is Times New Roman. Then Adobe Acrobat 5.0 is used to print the word file as a PDF file. After that, the PDF file is saved as a “tiff” image. Different DPI (dots per inch) like 72 dpi, 96 dpi, 150 dpi, 300 dpi and 600 dpi can be selected during the saving process. This resolution will determine the quality of the resultant “tiff” images. The higher the resolution is, the better the quality is. The “tiff” image is then saved as a monochrome image using Window’s PAINT program.

Figure 4.8: Generation Process of Binary Document Images.

Distortion Measure for Binary Document Images

Distance-Reciprocal Distortion Measure (DRDM) [64], which is an objective distortion measure for binary document images, is used to measure the watermarked image quality when we compare our method with other embedding

CHAPTER 4. PROPOSED SEGMENT-BASED WATERMARKING METHOD

methods. The average DRD value can be calculated from [64] using the following equation.

$$\text{ave_DRD} = \frac{\sum_{k=1}^S \text{DRD}_k}{S} \quad (4.9)$$

where S is the number of flipped pixels in the watermarked image $g(x, y)$, and the distortion DRD_k measured for the k^{th} flipped pixel in $g(x, y)$ is given by

$$\text{DRD}_k = \sum_{i,j} [D_k(i, j) \times W_{N5}(i, j)] \quad (4.10)$$

where $1 \leq i, j \leq 5$ in our experiments, and the $(i, j)^{\text{th}}$ element of the difference matrix D_k is given by

$$D_k(i, j) = |B_k(i, j) - g[(x, y)_k]| \quad (4.11)$$

where B_k is a 5×5 block in the original image $f(x, y)$, and the normalized weight matrix which is of size 5×5 is given by

$$W_{N5} = \begin{bmatrix} 0.0256 & 0.0324 & 0.0362 & 0.0324 & 0.0256 \\ 0.0324 & 0.0512 & 0.0724 & 0.0512 & 0.0324 \\ 0.0362 & 0.0724 & 0 & 0.0724 & 0.0362 \\ 0.0324 & 0.0512 & 0.0724 & 0.0512 & 0.0324 \\ 0.0256 & 0.0324 & 0.0362 & 0.0324 & 0.0256 \end{bmatrix}$$

A smaller average DRD value means a better image quality.

4.2.2 Experimental Results of the Proposed Segment-based Watermarking Method

Figure 4.9 shows the enlarged original image and watermarked image of the letter “a”, and the difference between them. The font size of the letter “a” is 12, and the DPI value is 300.

Figure 4.9: Hiding Effect on a Single Letter “a”.

It can be observed that the watermarked image is very similar to the original image, and all the flipped pixels lie at the corners of the letter. If the original image is not shown and the watermarked image is not zoomed in, it is very hard to see that some information has been hidden in the image.

Table 4.2 shows the results for evaluating the embedding capacity of our method. The results are obtained from embedding random bits in A4 size (1653×2338

CHAPTER 4. PROPOSED SEGMENT-BASED WATERMARKING METHOD

pixels) document images with different DPIs varying from 72 dpi to 300 dpi and different font sizes varying from 10 to 13. Each image contains English words generated randomly from [70]. The mean values of R_e (embedding rate), N_{es} (number of segments used for embedding), N_s (number of total segments) and N_w (number of words) are calculated from 100 various images in each category (e.g. font 10 & 72 dpi, font 11 & 200 dpi). R_e is the ratio between N_{es} and N_s . From Table 4.2 we can obtain the embedding rate for different font sizes and different resolutions. For a binary document image with font size 12 and 200 dpi, the embedding rate is about 0.41. That means if there are 100 segments in the image, 41 bits can be embedded in the image. The very small standard deviation of R_e indicates that our results are accurate. The values of N_{es} , N_s and N_w are for the purpose of reference. Figure 4.10 shows a portion of one document image used in our experiments with font size 12 and 200 dpi.

Table 4.2 can be used to roughly calculate the maximum number of bits that can be embedded in a given document image. Our method does not concern about the dimensions of the document images but the number of segments in that image. For example Figure 4.11 shows an A4 size binary document image with font size 12 and 200 dpi, whose dimension is 1653×2338. It contains 57,517 segments. The embedding rate for document image with font size 12 and 200 dpi shown in Table 4.2 is 0.4067. Then we can calculate the embedding capacity to be about 23,392 bits. The embedding capacity from experiment is 23,226. The two results do not differ too much.

CHAPTER 4. PROPOSED SEGMENT-BASED WATERMARKING METHOD

Table 4.2: Embedding Capacity of the Proposed Segment-based Method.

Fonts Size		Resolution of Image				
		72dpi	96dpi	150dpi	200dpi	300dpi
Font size 10	Mean of R_e	0.2145	0.2908	0.3674	0.3924	0.4090
	Standard deviation of R_e	0.002209	0.002262	0.002042	0.002035	0.002214
	Mean of N_{es}	5555	10746	24393	34353	56751
	Mean of N_s	25896	36952	66393	87545	138756
	Mean of N_w	431	431	431	431	431
Font size 11	Mean of R_e	0.2140	0.3013	0.3744	0.4024	0.4176
	Standard deviation of R_e	0.002270	0.002468	0.002134	0.001934	0.002080
	Mean of N_{es}	5430	12084	25135	34806	55290
	Mean of N_s	25373	40106	67133	86497	132400
	Mean of N_w	389	389	389	389	389
Font size 12	Mean of R_e	0.2234	0.3215	0.3837	0.4067	0.4064
	Standard deviation of R_e	0.002097	0.02403	0.00235	0.002338	0.002321
	Mean of N_{es}	6757	11888	25469	34796	53485
	Mean of N_s	30247	36978	66378	85557	131608
	Mean of N_w	354	354	354	354	354
Font size 13	Mean of R_e	0.2838	0.3153	0.3689	0.3965	0.3960
	Standard deviation of R_e	0.002371	0.002160	0.002236	0.002343	0.002258
	Mean of N_{es}	7791	12871	24838	33285	52318
	Mean of N_s	27453	40823	67331	83947	132116
	Mean of N_w	326	326	326	326	326

CHAPTER 4. PROPOSED SEGMENT-BASED WATERMARKING METHOD

In the table, R_e denotes the embedding rate which is given by $\frac{N_{es}}{N_s}$, N_{es} denotes the number of segments used for embedding in an A4 size image, N_s denotes the number of segments in an A4 size image and N_w denotes the number of words in an A4 size image.

adown beslaver contund dissocial doting ebullioscope e
inwrought liberalism misapprehension negotiation niveous
uninteresting unmoral unthinkable alcaic cerecloth clincher c
enjoyment hexaglot infundibuliform misadventure picaroon
sharpeners shoplifting spinney tympani undertaker undisturbed
anticlinal athanor comtation correctitude debased depopula
eleemosynary enshrine extemporaneously fumigation good
menacing nonsuccess saltatoric spiroid averseness bairn bomb
checkmake culdelampe disclaimer fakir fourwheeler kilderk

Figure 4.10: A Portion of a Document Image Containing Randomly Generated Words.

Figure 4.11: A Regular Document Image.

CHAPTER 4. PROPOSED SEGMENT-BASED WATERMARKING METHOD

Figure 4.12 shows the plot of embedding rates of document images with different font sizes and resolutions shown in Table 4.2. For a fixed font size, it can be observed that the embedding rate below 200 dpi increases very fast. Above 200 dpi the embedding rate increases slowly or stays flat. The reason is that when resolution goes up, N_s increases proportionally but the increment of N_{es} becomes smaller and smaller. This can be explained as follows. Each character in the document image is represented by single-line black pixels at 72 dpi, so the number of corner pixels that can be flipped is very limited. This leads to a small N_{es} . As the resolution increases, the character is represented by multi-line black pixels, and more and more corner pixels that can be flipped appear. Below 200 dpi the width and height of each character will increase less than 3 times comparing to the characters at 72 dpi. The increasing rate is less than the height of our Masks which is 3-pixel high, thus the impact on finding N_{es} by using the Masks is greater when the resolution of the characters changes from 72 dpi to a higher DPI which is smaller than 200. Above 200 dpi the increasing rate of the resolution is larger than three, so the influence to our Masks becomes smaller and smaller, and we believe that the curves in Figure 4.12 will change their directions from going up to going flat and finally to going down. That means N_{es} will become constant at some resolution R_c . Another observation is that when the font size increases, the effect of resolution on embedding rate becomes smaller, and R_c could also becomes smaller.

CHAPTER 4. PROPOSED SEGMENT-BASED WATERMARKING METHOD

Figure 4.12: Embedding Rate of Document Images with Different Font Sizes and Resolutions.

4.2.3 Performance Comparison of Embedding Methods for Binary Images

In this section we will compare our segment-based watermarking method with other methods in terms of embedding capacity and watermarked image quality. We compare our proposed method with four other block-based embedding methods, which are Yang and Kot's denoise method [69], Yang and Kot's

CHAPTER 4. PROPOSED SEGMENT-BASED WATERMARKING METHOD

connectivity-preserving method [73], Min Wu *et. al*'s method [63] and DRDM-based method [65]. In order to compare the embedding capacity, we apply the five watermarking methods to the same binary document images. One English document image and one Chinese document image are used as the cover images in our experiments. Table 4.3 shows the number of maximum bits that can be embedded in the images by using each of the methods. It can be seen that our proposed segment-based method has the highest embedding capacity in both cases.

Table 4.3: Embedding Capacity of Different Watermarking Methods for Binary Document Images.

Watermarking methods	Embedding Capacity for English Document Image (bits)	Embedding Capacity for Chinese Document Image (bits)
Yang and Kot's denoise method	503	528
DRDM, block size 10×10	588	730
Min Wu <i>et. al</i> 's method, block size 12×12	784	784
Yang and Kot's connectivity-preserving method, block size 4×4	1237	1320
Our proposed segment-based method	1348	1713

CHAPTER 4. PROPOSED SEGMENT-BASED WATERMARKING METHOD

Figure 4.13 and Figure 4.14 show the original images and the watermarked images produced by different watermarking methods. It is very hard to tell the difference in visual quality of the watermarked images by using our naked eyes. Therefore we use DRDM to measure the visual quality of the watermarked images objectively. We fix the length of data to be embedded in the image shown in Figure 4.13 (a) and Figure 4.14 (a) as 503 bits and 528 bits respectively for each method. Table 4.4 shows the DRDM values of the watermarked English and Chinese document images for different watermarking methods. The number in the bracket represents the rank where 1 means the best visual quality and 6 means the worst visual quality. In Table 4.4 we also added in an additional row called “randomly embedding” to show the worst DRDM value. It is observed that the DRDM value is not linear. Randomly embedding means we embed random data by only flipping the edge pixels in the image. As we all know, a watermarking method will seldom flip a white pixel to black if all the surrounding pixels of the white pixel are white, or vice versa. Thus randomly flipping the edge pixels will be the worst case and that will give the worst DRDM value. The watermarked image by randomly embedding is presented in Figure 4.15.

CHAPTER 4. PROPOSED SEGMENT-BASED WATERMARKING METHOD

During the past
edit card transact
of the increase i
binary images?
ry of image fea
ble. The goal of

(a) Original Image Which is of Size
336×336 Pixels.

During the past
edit card transact
of the increase i
binary images?
ry of image fea
ble. The goal of

(b) Watermarked Image by Yang and
Kot's Denoise Method.

During the past
edit card transact
of the increase i
binary images?
ry of image fea
ble. The goal of

(c) Watermarked Image by DRDM
Method.

During the past
edit card transact
of the increase i
binary images?
ry of image fea
ble. The goal of

(d) Watermarked Image by Min Wu *et al.*'s Method.

During the past
edit card transact
of the increase i
binary images?
ry of image fea
ble. The goal of

(e) Watermarked Image by Yang and
Kot's Connectivity-preserving Method.

During the past
edit card transact
of the increase i
binary images?
ry of image fea
ble. The goal of

(f) Watermarked Image by Proposed
Segment-based Method.

Figure 4.13: Original English Image and Watermarked Images by Our

Segment-based Watermarking Method and Other Methods.

CHAPTER 4. PROPOSED SEGMENT-BASED WATERMARKING METHOD

5. 根据清洁发展
规定，缔约方会
(2001-2002 年)
(a) 执行理事会
(b) 执行理事会
议。尤其是关于

(a) Original Image Which is of Size 336×336 Pixels.

5. 根据清洁发展
规定，缔约方会
(2001-2002 年)
(a) 执行理事会
(b) 执行理事会
议。尤其是关于

(b) Watermarked Image by Yang and Kot's Denoise Method.

5. 根据清洁发展
规定，缔约方会
(2001-2002 年)
(a) 执行理事会
(b) 执行理事会
议。尤其是关于

(c) Watermarked Image by DRDM Method.

5. 根据清洁发展
规定，缔约方会
(2001-2002 年)
(a) 执行理事会
(b) 执行理事会
议。尤其是关于

(d) Watermarked Image by Min Wu *et al.*'s Method.

5. 根据清洁发展
规定，缔约方会
(2001-2002 年)
(a) 执行理事会
(b) 执行理事会
议。尤其是关于

(e) Watermarked Image by Yang and Kot's Connectivity-preserving Method.

5. 根据清洁发展
规定，缔约方会
(2001-2002 年)
(a) 执行理事会
(b) 执行理事会
议。尤其是关于

(f) Watermarked Image by Proposed Segment-based Method.

Figure 4.14: Original Chinese Image and Watermarked Images by Our Segment-based Watermarking Method and Other Methods.

CHAPTER 4. PROPOSED SEGMENT-BASED WATERMARKING METHOD

Table 4.4: Distortion Measure Results of Different Watermarking Methods for Binary Document Images.

Watermarking methods	Number of Bits Embedded	DRDM Value of English Image	DRDM Value of Chinese Image
DRDM, block size 10×10	503	0.363 (1)	0.323 (1)
Our proposed segment-based method	503	0.494 (2)	0.495 (2)
Yang and Kot's denoise method	503	0.501 (3)	0.496 (3)
Yang and Kot's connectivity-preserving method, block size 4×4	503	0.513 (4)	0.543 (5)
Min Wu <i>et. al</i> 's method	503	0.532 (5)	0.517 (4)
Randomly Embedding	503	0.600 (6)	0.570 (6)

During the past
edit card transact
of the increase i
binary images?
ry of image fea
ble. The goal of

(a) English Image.

5. 根据清洁发展
规定，缔约方会
(2001-2002 年)
(a) 执行理事会
(b) 执行理事会
议 书 其 是 关 于

(b) Chinese Image.

Figure 4.15: Watermarked Images by Randomly Flipping the Edge Pixels.

CHAPTER 4. PROPOSED SEGMENT-BASED WATERMARKING METHOD

It can be observed from Table 4.4 that our method ranks the second best visual quality according to DRDM values. It is not surprising that the watermarking method based on DRDM ranks No. 1 according to DRDM values. That is because different watermarking methods make use of different masks to embed data, and DRDM assigns different values to those masks when it measures the visual quality of the watermarked images. The watermarking method based on DRDM uses only the masks with small DRDM values for embedding. If the same masks are used in the proposed segment-based method to embed 503 bits in the binary English image and embed 528 bits in the binary Chinese image, we can obtain similar results. And we believe this is also true for other block-based methods.

In order to compare our proposed segment-based watermarking method with other block-based watermarking methods fairly, we can use the following way. We can use the same masks, which are shown in Figure 4.16, in both the proposed segment-based method and the block-based method to embed data in the images shown in Figure 4.13 (a) and Figure 4.14 (a). Thus the visual quality of the watermarked images generated by the two kinds of methods will be the same. As a result, the method with a higher embedding capacity gains the advantage. Table 4.5 shows the maximum bits to be embedded by using the two methods. It is obvious that our proposed segment-based method has a higher embedding capacity, and we can conclude that our claim is correct that our method can make use of more corner pixels than block-based methods. The embedding capacity of the block-based method is obtained by dividing the cover image into overlapping 3×3 blocks and scanning each block using the four masks. Each block overlaps a column with its left and right blocks horizontally, and overlaps a row with its upper and lower blocks vertically.

CHAPTER 4. PROPOSED SEGMENT-BASED WATERMARKING METHOD

Figure 4.16: Four Masks Used for Comparing Different Watermarking Methods.

Table 4.5: Embedding Capacity of the Segment-based Method and the Block-based Method Based on the Same Masks.

Watermarking methods	Number of Bits Embedded in English Image	Number of Bits Embedded in Chinese Image
Block-based method	350	239
Our proposed segment-based method	601	487

CHAPTER 4. PROPOSED SEGMENT-BASED WATERMARKING METHOD

4.3 Summary

The proposed segment-based watermarking method for binary images is presented in this chapter. It searches a segment in a binary image from left to right and top to bottom. After a segment is found, our method uses some pre-defined masks to check two ends of the segment to determine the properties of the segment for embeddability. For embeddable segments, our method adds or reduces a black pixel at either end of the segment and uses the odd or even number of black pixels in the segment to embed bit “1” or “0”. The modified locations are the corner pixels in the binary images. Therefore, it can achieve the purpose of high embedding rate and low distortion for the marked image. This method can be applied to any kind of binary images and the fast computation speed and low complexity make the method suitable for real-time implementation. Retrieval of the hidden data does not require the presence of the original binary image.

We also evaluated our proposed segment-based watermarking method in terms of the embedding capacity and the visual quality of the watermarked image. A table including embedding rates for binary document images with different font sizes and different resolutions is presented. It can be used to estimate the embedding capacity of the proposed segment-based watermarking method. In addition, we compared our segment-based method with some block-based methods. We fix the visual quality of the watermarked images by using the same masks adopted in both our segment-based method and the block-based method to embed data. The result is that the proposed segment-based method can embed more data than the block-based method.

CHAPTER 5

PROPOSED PATTERN-BASED REVERSIBLE WATERMARKING METHOD

In this chapter we present the proposed pattern-based reversible watermarking method. We also evaluate its performance in terms of visual quality of the watermarked images and embedding capacity by applying it to binary document images. The test images and distortion measure used in this chapter are the same as those used in Chapter 4.

5.1 Proposed Pattern-based Reversible Watermarking

Method

From literature we cannot see any practical implementation of reversible data hiding method for binary document images. Reversible data hiding is essential in some applications like military and medical areas. In this chapter, we present a pattern-based reversible data hiding method for binary document images, and we have implemented it using Matlab 6.5. Our method works well with A4 size binary document images.

Consider an A4 size text image given in Figure 5.1, we subdivide the image into non-overlapping blocks with size 3-pixel $\times$ 3-pixel. There are a total of 512 possible pixel patterns. Figure 5.2 shows the distribution of these patterns. It can be

[illegible]

M. Eng. Thesis

Figure 5.2: Histogram of Patterns within a 3×3 Block.

Figure 5.3: Architecture Overview of the Reversible Data Hiding.

CHAPTER 5. PROPOSED PATTERN-BASED REVERSIBLE WATERMARKING METHOD

Number of non-existent patterns selected and the types of patterns chosen are stored using Y bits in the pattern-section. The record containing its length, the locations of the flipped pixels coded in R in Figure 5.3, and the message to be hidden are embedded in the message-section. Combining both sections will generate the desired marked text image. The pattern-section location has to be predefined and the pattern pair information has to be extracted first. Subsequently, the hidden message can be extracted correctly. The flipped pixel location, as part of the hidden message extracted is used to recover the original text image. We employed the secured feature in [67] in our implementation.

5.1.1 Embedding Data

In the embedding process, we label an existent pattern used for embedding as Marker_I, and a non-existent pattern generated from Marker_I after embedding as Marker_II. Marker_I is converted to Marker_II depending on the data to be hidden, which form a marker-pair. In the extraction and recovery process, hidden data are extracted and Marker_II is converted back to Marker_I.

The embedding process can be summarized in 7 steps.

Step 1: Divide the image into two sections, one is called message-section which is used to hide message and the other is called pattern-section which is used to hide marker/pattern information. The pattern-section is known to both issuers and receivers. To make the pattern-section secure, the receiver will generate a pair of correlated private key and public key, and send the public key to the sender. Then the sender encrypts the information about pattern-section using the public key and sends it back to the receiver. In this

CHAPTER 5. PROPOSED PATTERN-BASED REVERSIBLE WATERMARKING METHOD

case, only the receiver can extract the correct information by using the private key. Usually a few fixed rows of pixels in the header, footer or corners of the text images are sufficient to hide pattern information. The remaining pixels in the text images are for hiding message.

Step 2: Divide the message-section of the image into non-overlapping blocks of size $m \times n$. There are totally $2^{m \times n}$ possible patterns. Sort the distributions of the pixel patterns within an $m \times n$ block in descending order of appearance.

Step 3: For each pattern $P_i, i = 1, 2, \dots, K$, that belongs to the first K patterns on the list, flip one at a time each pixel in P_i to obtain a new pattern Q_i . If Q_i does not exist in the original image, P_i is labelled as Marker_I and Q_i is labelled as a set of candidates for Marker_II. If more than one such Q_i patterns exist in this flipping process, DRDM [64] is used to select one Q_i with minimum distortion in hiding data. The P_i and the selected Q_i composes a marker-pair.

Step 4: Sort all the marker-pairs in ascending order according to their DRD values. The marker-pair with the smallest DRD value corresponding to smallest distortion is used for embedding first.

Step 5: Convert the information to be hidden into a bit stream, which is then embedded by changing Marker_I to Marker_II to hide a bit '1'. For bit '0', no change is made.

Step 6: Embed identity of the used marker-pairs in the pattern-section.

Step 7: Embed the locations of the flipped pixels in the message-section using Step 5. If larger capacity is needed, more marker-pairs and those P_i patterns higher on the list are chosen for embedding additional data.

CHAPTER 5. PROPOSED PATTERN-BASED REVERSIBLE WATERMARKING METHOD

The extraction process is just the reverse of the embedding process. We can extract the hidden data and restore the watermarked image to the original image in the extraction process.

5.1.2 Embedding Pattern Information

The marker/pattern information is embedded in the pattern-section using the hiding method proposed in [67]. We choose this method because it makes the pattern information secure by employing a key matrix and a weight matrix shared only by the sender and the receiver. It can embed many bits in one block by flipping at most two pixels. This helps to reduce the number of bits required to record the locations of the flipped pixels, which is used to restore the pattern-section.

Secure Data Hiding Scheme for Binary Images

In this part, we will introduce the major portion of reference [67]. The inputs to [67] are as follows.

- 1) F is a host binary image (i.e., bitmap), which is to be modified to embed data.

Here, F is partitioned into blocks of size $m \times n$. For simplicity, we assume that the size of F is a multiple of $m \times n$.

- 2) K is a secret key shared by the sender and the receiver. It is a randomly selected bitmap of size $m \times n$.

- 3) r is the number of bits to be embedded in each $m \times n$ block of F . The value of r satisfies $2^r - 1 \leq m \times n$.

- 4) W is a secret-weight matrix shared by the sender and the receiver. It is an integer matrix of size $m \times n$ whose content satisfies the following requirements:

CHAPTER 5. PROPOSED PATTERN-BASED REVERSIBLE WATERMARKING METHOD

each element of $\{1, 2, \dots, 2^r - 1\}$ appears at least once in W , i.e., $\{[W]_{ij}, i = 1 \dots m, j = 1 \dots n\} = \{1, 2, \dots, 2^r - 1\}$.

- 5) B is critical information consisting of kr bits to be embedded in F , where k is the number of $m \times n$ blocks in F .

After defining all the inputs, the embedding steps can be described as following.

- 1) Compute $F_i \oplus K$, where F_i is a $m \times n$ image block of the host image F and ' $\oplus$ ' means bitwise exclusive-OR.
- 2) Compute $\text{SUM} [(F_i \oplus K) \otimes W]$, where ' $\otimes$ ' is the component-wise multiplication operator on two equal-size integer matrices.
- 3) From the matrix $F_i \oplus K$, compute for each $w = 1 \dots 2^r - 1$ the following set:

$$S_w = \left\{ (j, k) \mid \left([W]_{j,k} = w \wedge [F_i \oplus K]_{j,k} = 0 \right) \vee \left([W]_{j,k} = 2^r - w \wedge [F_i \oplus K]_{j,k} = 1 \right) \right\} \quad (5.1)$$

Intuitively, S_w represents the set containing each matrix index (j, k) , such that complementing $[F_i]_{j,k}$ would increase the sum in step 2 by w .

- 4) Define a weight difference as:

$$d \equiv (b_1 b_2 \dots b_r) - \text{SUM} [(F_i \oplus K) \otimes W] \pmod{2^r} \quad (5.2)$$

where $b_1 b_2 \dots b_r$ denotes the r data bits. If $d = 0$, F_i does not need to be changed.

Otherwise, the following steps are executed to transform F_i into F_i' , which is the modified image block. For ease of presentation, defining $S_w = S_{w'}$ for any $w \equiv w' \pmod{2^r}$.

- a) Randomly select an $h \in \{0, 1, \dots, 2^r - 1\}$, such that $S_{hd} \neq \emptyset$ and

$$S_{-(h-1)d} \neq \emptyset.$$

- b) Randomly select a $(j, k) \in S_{hd}$ and complement the bit $[F_i]_{j,k}$.

CHAPTER 5. PROPOSED PATTERN-BASED REVERSIBLE WATERMARKING METHOD

c) Randomly select a $(j, k) \in S_{-(h-1)d}$ and complement the bit $[F_i]_{j,k}$.

Thus, the data is embedded in the host image. The data can be extracted by

$$\text{SUM}[(F_i' \oplus K) \otimes W] \equiv b_1 b_2 \dots b_r \pmod{2^r} \quad (5.3)$$

Embedding Pattern Information by Employing Secure Data Hiding Scheme

According to [67], we define the following inputs to the scheme:

- 1) G is the pattern-section, and it is partitioned into blocks of size 8×8 .
- 2) K is a secret key shared by the sender and the receiver. It is a random selected bitmap of size 8×8 . In our implementation, we choose

$$K = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

- 3) W is a secret weight matrix shared by the sender and the receiver, which is an integer matrix of size 8×8 whose content satisfies some requirements. Please refer to [67] for the requirements. Here we choose

CHAPTER 5. PROPOSED PATTERN-BASED REVERSIBLE WATERMARKING METHOD

$$W = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 \\ 25 & 26 & 27 & 28 & 29 & 30 & 31 & 32 \\ 33 & 34 & 35 & 36 & 37 & 38 & 39 & 40 \\ 41 & 42 & 43 & 44 & 45 & 46 & 47 & 48 \\ 49 & 50 & 51 & 52 & 53 & 54 & 55 & 56 \\ 57 & 58 & 59 & 60 & 61 & 62 & 63 & 1 \end{bmatrix}$$

- 4) X is the number of bits to be embedded in each 8×8 block of G . The value of X must satisfies $2^X - 1 \leq 8 \times 8$, here we choose $X = 5$.
- 5) E is the marker information consisting of $N \times X$ bits, where N is the number of 8×8 blocks used for embedding in G . If the length of E , Y (bits), is not the multiple of X , we append zeros to the end of E .

After defining all the inputs, the embedding process of pattern information can be roughly described by the following 4 steps:

- 1) Perform a bitwise exclusive-OR on G_i and K , $G_i \oplus K$, where G_i is an image block of G and ' $\oplus$ ' means bitwise exclusive-OR.
- 2) Sum all elements in the matrix $(G_i \oplus K) \otimes W$, $\text{SUM}[(G_i \oplus K) \otimes W]$, where ' $\otimes$ ' is the component-wise multiplication operator on two equal-size integer matrices.
- 3) From the matrix $G_i \oplus K$, compute for each $w = 1 \dots 2^X - 1$ the following set:

$$S_w = \left\{ (j, k) \mid \left([W]_{j,k} = w \wedge [G_i \oplus K]_{j,k} = 0 \right) \vee \left([W]_{j,k} = 2^X - w \wedge [G_i \oplus K]_{j,k} = 1 \right) \right\} \quad (5.4)$$

CHAPTER 5. PROPOSED PATTERN-BASED REVERSIBLE WATERMARKING METHOD

Intuitively, S_w represents the set containing each matrix index (j,k) , such that complementing $[G_i]_{j,k}$ would increase the sum in step 2 by w .

4) Define a weight difference as

$$d \equiv (e_1 e_2 \dots e_x) - \text{SUM}[(G_i \oplus K) \otimes W] \pmod{2^x} \quad (5.5)$$

If $d = 0$, G_i does not need to be changed to embed X bits. If $d \neq 0$, we can use d to select suitable S_w and flip at most two pixels in G_i according to the index (j,k) in S_w to embed X bits. More details on how to choose S_w can be found in [67].

After embedding the marker information, we calculate the total number of bits needed to restore the pattern-section. We use Y (shown in Figure 5.3) to represent the total number of bits used to store the marker information, R (shown in Figure 5.3) to represent the record of the flipped pixels locations used to hide Y in the marked pattern-section. The length (in bits) of R , R_{Length} can be computed by

$$R_{Length} = \sum_{i=1}^N B_i \quad (5.6)$$

where $N = \left\lceil \frac{Y}{X} \right\rceil$ is the number of blocks used to hide marker information, $\lceil \cdot \rceil$ is the ceiling function and B_i is the number of bits used to record the locations in the i^{th} 8×8 block.

A graphical representation of R is shown in Figure 5.4. F_l is a flag used to denote whether any bit is flipped in the 1st block; H_l indicates one or two pixels are

CHAPTER 5. PROPOSED PATTERN-BASED REVERSIBLE WATERMARKING METHOD

flipped; C_i records the position of the flipped pixels. Figure 5.5 shows the components in i^{th} block. It can be seen that B_i has the following 3 possible values:

1. If $F_i = 0$, that means no pixel is flipped in the i^{th} block, so there is no H component and C component in it as well, and $B_i = 1$.
2. If $F_i = 1$ and $H_i = 0$, that means one pixel is flipped in the i^{th} block, so the length of C_i is 6 bits, recoding x and y positions of the flipped pixel in the block, and $B_i = 8$.
3. If $F_i = 1$ and $H_i = 1$, that means two pixels are flipped in the i^{th} block, so the length of C_i is 12 bits and $B_i = 14$.

Figure 5.4: Constitution of Record R .

Figure 5.5: Components in i^{th} Block.

5.2 Experimental Results of the Proposed Reversible Watermarking Method

In our experiment, a number of binary test document images which contain different language fonts and four various resolutions (72, 96, 150 and 300dpi) were used to study the distribution for different patterns within a 3×3 block. The font size is fixed at 12. The generation process of the test images has been illustrated in Figure 4.8 in Chapter 4. We define the bit sequence shown in Figure 5.6, where b1 is the Most Significant Bit (MSB) and b9 is the Least Significant Bit (LSB). We label each pattern as b1b2...b9.

b1	b2	b3
b4	b5	b6
b7	b8	b9

Figure 5.6: Bit Sequence in a 3×3 Block.

Table 5.1 shows the distribution for the patterns within a 3×3 block. We use sixteen text images with different font types and resolutions to check the distributions of existent versus non-existent patterns. These images are shown in Appendix II. It can be observed that there are more than 20% non-existent patterns out of 512 possible patterns in these text images. There are plenty of non-existent

CHAPTER 5. PROPOSED PATTERN-BASED REVERSIBLE WATERMARKING METHOD

patterns to choose from and the creation of the marker-pair in text images is not difficult.

Table 5.1: Distribution of Patterns within a 3×3 Block.

Image name (font type_resolution)	Image size in pixel value (Height × Width)	Percentage of non-existent patterns
English_72dpi	791×612	34.18%
English_96dpi	1055×816	45.31%
English_150dpi	1649×1275	46.29%
English_300dpi	3299×2550	62.70%
Arabic_72dpi	791×612	44.34%
Arabic_96dpi	1055×816	51.37%
Arabic_150dpi	1649×1275	50.39%
Arabic_300dpi	3299×2550	58.01%
Chinese_72dpi	791×612	21.68%
Chinese_96dpi	1055×816	21.48%
Chinese_150dpi	1649×1275	21.48%
Chinese_300dpi	3299×2550	39.84%
Croatian_72dpi	791×612	26.37%
Croatian_96dpi	1055×816	35.74%
Croatian_150dpi	1649×1275	41.60%
Croatian_300dpi	3299×2550	58.59%

Usually, images with resolution below 150dpi have a large quantity of quantization noise. Our method works well for A4 size images with resolution equal or above 150dpi. Figure 5.7 shows a portion of the original document image with resolution 150dpi, which is of size 1649×1275. Figure 5.8 shows the same

CHAPTER 5. PROPOSED PATTERN-BASED REVERSIBLE WATERMARKING METHOD

portion of the watermarked image, in which 789 bits are embedded. The visual quality of the watermarked A4 size document image is acceptable and the average DRD value is 0.435.

Figure 5.7: A Portion of the Original Text Image.

Figure 5.8: A Portion of the Watermarked Image with 789 Bits Embedded.

CHAPTER 5. PROPOSED PATTERN-BASED REVERSIBLE WATERMARKING METHOD

Figure 5.9 demonstrates the enlarged portion of the watermarked image, in which the black pixels are the pixels being flipped. It can be seen that some flipped pixels lie on the straight lines of the characters so that some noise are created after converting Marker_Is to Marker_IIs. The reason is that Marker_IIs are the patterns that should not appear in a clean computer-generated document image. Therefore we have to sacrifice some quality and capacity in order to achieve reversible data hiding. Table 5.2 illustrates the five marker-pairs used for data hiding. They have smaller DRD values than any other marker-pairs so the watermarked image results in a better visual quality but not achieving the highest embedding capacity. If other marker-pairs with higher appearance were chosen for embedding, more data could be embedded but the visual quality of the watermarked image might not be so good. There is always a trade-off between the embedding capacity and the visual quality of the watermarked image.

Figure 5.9: Enlarged Portion of the Watermarked Image.

Table 5.2: Five Marker-pairs Used in the Experiment.

	Marker_I	Marker_II
Marker-pair 1
Marker-pair 2
Marker-pair 3
Marker-pair 4
Marker-pair 5

Table 5.3 shows more experimental results by applying the proposed method on some images listed in Table 5.1. We fix the average DRD value at 0.5 and examine the embedding capacity of different images. The value of R_{length} is calculated by using equation (5.3). We assume the chances of $B_i = 1$, $B_i = 8$, and $B_i = 14$ are equal and $N = \left\lceil \frac{Nm \times 13}{5} \right\rceil$ for 13 bits being used to record one marker-pair and five bits being embedded in one block in the pattern-section. Marker_I is recorded using 9 bits, and Marker_II is recorded using 4 bits that are sufficient to indicate the different bit from Marker_I, hence, a total of 13 bits are used. For example, for the image English_150dpi, $N = 58$, $R_{length} = 58 \times (1+8+14)/3 = 445$ with the

CHAPTER 5. PROPOSED PATTERN-BASED REVERSIBLE WATERMARKING METHOD

assumption that there is an equal chance for $B_i = 1$, $B_i = 8$, and $B_i = 14$. Furthermore, we can use a length of 20 bits as a header to indicate the length of n .

From Table 5.3 we can observe that for an A4 size document image with full contents, our method can embed a large number of bits for authentication purpose. However, for the images with few contents like Arabic_150dpi and Arabic_300dpi, our method is not applicable because the appearance of marker-pairs with small distortion is small. There is not enough space for embedding sufficient information for authentication.

Table 5.3: Embedding Capacity of Different Computer-generated Document Images.

Image	Size	N_m	n	R_{length}	$n - R_{length}$
English_150dpi	1275×1649	22	2199	445	1754
English_300dpi	2550×3299	17	1682	345	1337
Arabic_150dpi	1240×1753	11	265	223	42
Arabic_300dpi	2479×3507	Not	Not	Not	Not
Chinese_150dpi	1275×1649	12	758	246	512
Chinese_300dpi	2550×3299	8	864	161	703
Croatian_150dpi	1240×1753	14	1950	284	1666
Croatian_300dpi	2479×3507	17	2107	345	1762

In the table, N_m is the number of marker-pairs used, n is the total number of bits embedded in the image, R_{length} is the number of bits used to record the location information and $n - R_{length}$ is the embedding capacity. “Not” means that the embedding was not possible.

5.3 Summary

In this chapter, we presented the proposed pattern-based reversible watermarking method. The method searches for the existent patterns and creates non-existent patterns for hiding data. The original image can be reconstructed after the hidden data are extracted. If all possible patterns exist for a 3×3 block, the block size can be increased to search for non-existent patterns for data embedding. But this will take more processing time and more space to store the marker-pairs. Capacity can be increased by choosing an existent pattern with the highest number of occurrence in an image. There is always a trade off between capacity and the quality of the marked image if the chosen pattern does not have a small DRDM value. We also evaluated the proposed watermarking method in terms of the embedding capacity and the visual quality of the watermarked image. The embedding capacity of the reversible method is lower than most binary watermarking methods. However, the reduction in capacity is the trade off due to the reversibility requirement. The reversible method is suitable for a document image with a large size, in which the noise is not noticeable to human eyes and the embedding capacity is acceptable.

CHAPTER 6

SECURE AUTHENTICATION SYSTEM

In this chapter, we present a secure binary document authentication system based on our proposed algorithms. It consists of two processes: watermark embedding process and watermark authentication process. We also compare it with the traditional digital signature authentication system.

6.1 Digital Signature Authentication System

The state-of-the-art solution for binary document authentication is digital signature. The signature generation process and authentication process are shown in Figure 6.1 (a) and Figure 6.1(b), respectively.

The generation process of the digital signature can be summarized as follows:

Step 1: $h = H(I)$. A hash function is used to generate the message digest h from the original image I .

Step 2: $S = E(h, k_{private})$. An encryption function is used to generate the signature S with a private key $k_{private}$.

Step 3: The signature is appended to the original image, and we obtain the resultant image with a digital signature inside.

The authentication process can be summarized as follows:

Step 1: $h' = H(I')$. Generate the message digest h' from the test image I' .

CHAPTER 6. SECURE AUTHENTICATION SYSTEM

Step 2: $h = D(S, k_{public})$. Decrypt the appended signature using the public key which is corresponding to the private key used in generation process to obtain the message digest h .

Step 3: Compare h and h' . If they are equal, the test image is authenticated; else it is not authenticated.

(a) Generation Process.

(b) Authentication Process.

Figure 6.1: Overview of Digital Signature.

CHAPTER 6. SECURE AUTHENTICATION SYSTEM

Comparing to watermarking authentication system, digital signature has the following weaknesses:

1. In digital signature, the signature is attached to the image instead of being embedded in the image. The attachment of the digital signature can be easily detected due to the changes in image size.
2. Digital signature is not as flexible as watermarking when used to authenticate the digital image. Some unintended errors which do not affect the content of the image will lead the authenticity to failure.

6.2 Watermarking Authentication System

The watermarking authentication system for binary images was proposed by Kim and Afif [22]. They use a known seed to generate a set of pseudo-random locations L , and embed the encrypted hash value at these locations. The hash value is calculated after clearing all the pixels belonging to L .

In the above-mentioned authentication system, the host image is divided into two parts: the first part is used to calculate the hash value, and the second part is used to embed the watermark (usually the encrypted hash value). In most cases, the embedding capacity of the second part is larger than the size (1024 bits in our experiment) of encrypted hash value, so the pixel values at those locations which are not used for embedding can be modified freely. This allows the unintended modification in watermarking authentication system. Those pixels lie at the boundaries of the characters, so they will not affect the contents of the image.

6.2.1 Authentication System Based On the Segment-based Data Hiding Algorithm

The proposed segment-based data hiding algorithm can be used in this kind of system. Figure 6.2 shows the embedding process and the authentication process for our proposed segment-based algorithm. The hash function and the public key encryption used here is 128-bit MD5 algorithm and RSA (R. Rivest, A. Shamir and L. Adleman) public-key cryptosystem, respectively. For more information about encryption function, please refer to [72].

The embedding steps are as follows:

Step 1: Generate a new image I_{new} by clearing the even rows of the original image I .

Step 2: $h = H(I_{new})$. Calculate the hash value of I_{new} .

Step 3: $W_{xor} = h \oplus w$. Calculate the Exclusive OR (XOR) value of the hash value and the watermark.

Step 4: $W_{encrypt} = E(W_{xor}, k_{private})$. Encrypt W_{xor} by using public key encryption with a private key.

Step 5: Embed $W_{encrypt}$ in the even rows of the original image by using the proposed segment-based data hiding method. The image size remains the same after watermark embedding process.

The authentication steps are as follows:

Step 1: Generate a new image I'_{new} by clearing the even rows of the test image I' .

Step 2: $h' = H(I'_{new})$. Calculate the hash value of I'_{new} .

CHAPTER 6. SECURE AUTHENTICATION SYSTEM

(a) Watermark Embedding Process.

(b) Watermark Authentication Process.

Figure 6.2: Watermarking Authentication System Based on Proposed Segment-based Method.

CHAPTER 6. SECURE AUTHENTICATION SYSTEM

Step 3: Extract the watermark W' from the even rows of the test image by using the proposed segment-based watermarking method.

Step 4: $W_{decrypt} = D(W', k_{public})$. Decrypt W' by using public key encryption with a public key.

Step 5: $W_{retrieve} = h' \oplus W_{decrypt}$. Calculate the Exclusive OR (XOR) value of the hash value and the decrypted watermark to obtain the retrieved watermark.

Step 6: Compare the retrieved watermark with the original watermark. If they are same, the image is authenticated. Otherwise, the authentication failed. If the watermark is an image, we can authenticate the image by viewing the retrieved watermark, and the original watermark is not required.

6.2.2 Authentication System Based On the Pattern-based Reversible Data Hiding Algorithm

In the above mentioned authentication system, only the part of the image that is used to generate hash value can be authenticated. The other part of the image that is used to embed the watermark has been cleared before calculating the hash, and it cannot be authenticated. In order to authenticate the whole image, we can adopt the proposed reversible watermarking method in the authentication system. The watermark embedding and authentication processes are shown in Figure 6.3. The embedding and authentication steps are similar to those used in Figure 6.2 except in this case the image is not divided into two parts and the whole image can be authenticated.

CHAPTER 6. SECURE AUTHENTICATION SYSTEM

(a) Watermark Embedding Process.

(b) Watermark Authentication Process.

Figure 6.3: Watermarking Authentication System Based on Proposed Reversible Method.

6.3 Experimental Results

Figure 6.4 shows the experimental results when we apply the presented authentication system on a digital document image. Figure 6.4 (a) shows the watermarked image, and Figure 6.4 (b) shows the modified image with the word “black” in the title changed to “back”. It can be seen that in Figure 6.4 (d) the extracted watermark from the modified watermarked image is very different from the original watermark shown in Figure 6.4 (c). The modified image can not be authenticated. Figure 6.5, Figure 6.6 and Figure 6.7 show more experimental results.

6.4 Summary

In this chapter, we introduced digital signature, which is the traditional way used to authenticate binary images, and the watermarking authentication systems based on our proposed methods. The watermarking authentication system has many advantages over the digital signature authentication system. The former embeds information in the image, and the image size is unchanged. The latter attach data after the image so that the image size increases and it is easy for others to notice there is something hidden inside the image. The former can be used to authenticate the main content of the image as well as the whole image. But the latter can only be used to authenticate the whole image. Watermarking authentication system becomes popular these days due to these reasons. The experimental results show the watermarking authentication systems based on our proposed methods are effective.

(a) Watermarked Image.

(b) Modified Watermarked Image.

(c) Watermark Embedded in (a). (d) Extracted Watermark from (b).

Figure 6.4: Authentication Results.

II - L'IMPLANTATION GEOGRAPHIQUE

L'organisation de l'entreprise française est divisée en 20 régions. Des calculateurs ont été installés dans les régions importantes. On trouve ainsi des machines Bull 300 TI à programmes câblés dans les régions de Nancy, Nantes, Limoges pour la comptabilité téléphonique. A l'avenir, si la plupart des fichiers sont à être gérés en temps différé, un certain nombre de fichiers, voire mis à jour en temps réel, les abonnés, le fichier des renseignements des abonnés contiendront des quantités de données. Le volume total de caractères à gérer pour quelques 500 000 abonnés a été évalué.

(a) Watermarked Image.

II - L'IMPLANTATION GEOGRAPHIQUE

L'organisation de l'entreprise française est divisée en 20 régions. Des calculateurs ont été installés dans les régions importantes. On trouve ainsi des machines à Lille. Bordeaux, Toulouse et Montpellier. Bull 300 TI à programmes câblés dans les régions de Nancy, Nantes, Limoges pour la comptabilité téléphonique. A l'avenir, si la plupart des fichiers sont à être gérés en temps différé, un certain nombre de fichiers, voire mis à jour en temps réel, les abonnés, le fichier des renseignements des abonnés contiendront des quantités de données. Le volume total de caractères à gérer pour quelques 500 000 abonnés a été évalué.

(b) Modified Watermarked Image in Which the First Comma on the Fifth Line Changed to Full Stop.

NTU

(c) Watermark Embedded in (a). (d) Extracted Watermark from (b).

Figure 6.5: Authentication Results.

Keynote Presentations Professor Ravi Sa
 initiated the workshop with a keynote pres
 term usage control is a generalisation of a
 ongoing controls and mutability. Tradit
 authorisation decisions on users' access to
 that have to be fulfilled by the subject fo
 object-independent environmental require
 today's dynamic, distributed environment
 decision factors for richer and finer contr
 authorisation decisions are generally made

(a) Watermarked Image.

Keynote Presentations Professor Ravi Sa
 initiated the workshop with a keynote pres
 term usage control is a generalisation of a
 ongoing controls and mutability. Tradit
 authorisation decisions on users' access to
 that have to be fulfilled by the subject fo
 object-independent environmental require
 today's dynamic, distributed environment
 decision factors for richer and finer contr
 authorisation decisions are generally made

(b) Modified Watermarked Image in Which the Letter "o" in the First Word "Keynote" Is Exchanged With the Letter "o" in the Second Word "Presentations".

(c) Watermark Embedded in (a). (d) Extracted Watermark from (b).

Figure 6.6: Authentication Results.

Keynote Presentations Professor Ravi Sa
 initiated the workshop with a keynote pres
 term usage control is a generalisation of a
 ongoing controls and mutability. Tradit
 authorisation decisions on users' access to
 that have to be fulfilled by the subject fo
 object-independent environmental require
 today's dynamic, distributed environment
 decision factors for richer and finer contr
 authorisation decisions are generally made

(a) Watermarked Image.

Keynote Presentations Professor Ravi Sa
 initiated the workshop with a keynote pres
 term usage control is a generalisation of a
 ongoing controls and mutability. Tradit
 authorisation decisions on users' access to
 that have to be fulfilled by the subject fo
 object-independent environmental require
 today's dynamic, distributed environment
 decision factors for richer and finer contr
 authorisation decisions are generally made

(b) Modified Watermarked Image in Which the Word "and" in the Second Line from Bottom Is Shifted to the Left.

 NTU

(c) Watermark Embedded in (a). (d) Extracted Watermark from (b).

Figure 6.7: Authentication Results.

CHAPTER 7

CONCLUSION AND RECOMMENDATIONS

7.1 Conclusion

In this thesis, we proposed two fragile watermarking methods for binary images, especially for binary document images, for the purpose of image authentication. The first method is a segment-based watermarking method. In the embedding process, a sequence of continuous black pixels segment is searched in a binary image from top to bottom, and then from left to right. After a segment is located, pre-defined masks are used to check two ends of the segment to determine the properties of the segment for embeddability. For embeddable segments, a black pixel is added or removed at either end of the segment by using the odd or even number of black pixels in the segment to embed bit “1” or “0”. Since the modified locations are the selected corners pixels of the characters, it can achieve the purpose of high embedding rate and low distortion for the marked image. A pattern-based reversible watermarking method is also proposed in this thesis. This method searches existent patterns in the cover image, and creates non-existent patterns from the existent ones to embed data. In the extraction process, the hidden data is extracted and the watermarked image is restored to its original.

The performance of our proposed methods is evaluated in terms of the embedding capacity and the visual quality of the watermarked image.

CHAPTER 7. CONCLUSION AND RECOMMENDATIONS

Distance-Reciprocal Distortion Measure (DRDM) is used to measure the visual quality of the watermarked binary document image. Experimental results show that the proposed segment-based watermarking method can achieve higher embedding capacity than other block-based binary document watermarking methods with the same visual quality of the watermarked images. A table including embedding rates of document images with different font sizes and different resolutions is also shown in our experimental results. It can be used to predict the embedding capacity of a binary document image roughly. Experimental results also show that the proposed pattern-based reversible watermarking method can be applied to almost all document images. As long as we increase the dimension of the existent pattern, we can always find the corresponding non-existent patterns.

Furthermore, a watermarking authentication system based on our proposed methods is also presented in this thesis. The system can be used to detect any modification to the document image and to verify the authenticity of the document image.

7.2 Recommendations

Some recommendations for future research are discussed below.

- The embedding capacity of the segment-based method is reduced by half when it is used in the authentication system. Further research could be done on finding a better way to employ this method in an authentication system. A possible solution is to use our method to find out all the segments first. Then we use some new masks to check the pixels at the two ends of the segments. In stead of using the “add” and “reduce” properties and the odd/even feature of the segment to embed data, we flip the end

CHAPTER 7. CONCLUSION AND RECOMMENDATIONS

pixels of the segments to embed data. Each segment will be able to embed maximum two bits.

- Our experimental results are mainly obtained heuristically. More theory work should be developed in the future.
- The pattern-based reversible method is currently only suitable for binary document images. More experiments can be done on other types of binary images, and we can further develop this method for other binary images based on the experimental results.
- In our pattern-based reversible method, DRDM is used to measure the distortion of each marker-pair and put them in an ascending order according to their DRD values. The process of sequencing them is quite time-consuming, so we can set a threshold value in advance. As long as the DRD value of a marker-pair is less than the threshold value, it can be used for embedding. This will save a lot of processing time. Furthermore, more research can be done on finding out a better way to hide marker-pair information in order to reduce the length of bits used to store the marker-pair information.

BIBLIOGRAPHY

- [1] J. J. Eggers, R. Bäuml, R. Tzschoppe and J. Huber, “Applications of Information Hiding and Digital Watermarking,” *ECDL 2001*, Workshop Generalized Documents, September 8, 2001, Darmstadt, Germany.
- [2] N. Provos and P. Honeyman, “Hide and seek: an introduction to steganography,” *IEEE Security & Privacy* (2003), 1(3):32-44.
- [3] F. Shu, “Orthogonal Transform Watermarking Techniques For Authentication Of Digital Images and Documents,” M.Eng. dissertation, Nanyang Technological University, Singapore, 2005.
- [4] P. W. Wong, “A public key watermark for image verification and authentication,” *IEEE Int. Conf. Image Processing*, vol. 1, pp. 455-459, 1998.
- [5] P. S. L. M. Barreto, H. Y. Kim and V. Rijmen, “Toward a secure public-key blockwise fragile authentication watermarking,” *IEEE Proc. Vision, Image and Signal Processing*, vol. 149, no. 2, pp. 57-62, 2002.
- [6] S. Katzenbeisser and F. A. P. Petitcolas, *Information hiding techniques for steganography and digital watermarking*, Artech House, 2000.
- [7] C. Podilchuk and W. Zeng, “Image-adaptive watermarking using visual models,” *IEEE J. Select. Areas Commun*, vol. 16, pp. 525-539, May 1998.
- [8] R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, “Perceptual watermarks for digital images,” *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1108-1126, July 1999.
- [9] N. Memon and P. W. Wong, “Protecting digital media content,” *Commun. of the ACM*, vol. 41, pp. 35-43, July 1998.

BIBLIOGRAPHY

- [10] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "Information hiding - a survey," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1062-1078, July 1999.
- [11] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1079-1107, July 1999.
- [12] S. Voloshynovskiy, F. Deguillaume, O. Koval and T. Pun, "Information-theoretic data-hiding: recent achievements and open problems," *International Journal of Image and Graphics*, vol. 5, no. 1 (2005) 1-31.
- [13] W. Bender, D. Gruhl, N. Morimoto and A. Lu, "Techniques for data hiding," *IBM Systems Journal*, vol. 35, pp. 313--336, 1996.
- [14] G. W. Braudaway, K. A. Magerlein and F. Mintzer, "Protecting publicly available images with a visible image watermark", *Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques (R. L. van Renesse, ed.)*, vol. 2659, pp. 126-133, Feb. 1996.
- [15] M. S. Kankanhalli, Rajmohan and K. R. Ramakrishnan, "Adaptive visible watermarking of images," *IEEE Proc. of ICMCS'99, Florence, Italy*, vol. 1, pp. 568-573, June 1999.
- [16] S. P. Mohanty, K. R. Ramakrishnan and M. S. Kankanhalli, "An adaptive DCT domain visible watermarking technique for protection of publicly available images," *ICMPS'2000*, pp. 195-198, 2000.
- [17] H. Yang and A. C. Kot, "Text document authentication by integrating inter character and word spaces watermarking," *ICME'2004*, pp. 955-958, Taiwan, June 2004.
- [18] J. Zhao and E. Koch, "Embedding robust labels into images for copyright protection," *Proc. International Congress on Intellectual Property Rights for*

BIBLIOGRAPHY

- Specialized Information, Knowledge and New Technologies*, pp. 242-251, Aug. 1995.
- [19] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "Attacks on copyright marking systems," *Information hiding, second international workshop, IH98*, Portland, Oregon, U.S.A., LNCS 1525, Springer-Verlag, ISBN 3-540-65386-4, pp. 219-239, Apr. 1998.
- [20] F. A. P. Petitcolas, "Watermarking schemes evaluation," *IEEE. Signal Processing*, vol. 17, no. 5, pp. 58-64, Sept. 2000.
- [21] M. Yeung and F. Mintzer, "Invisible watermarking for image verification," *Journal of Electronic Imaging*, vol. 7, no. 3, pp. 578-591, July 1998.
- [22] H. Y. Kim and A. Afif, "Secure authentication watermarking for binary images," *IEEE, SIBGRAPI'03*, pp. 199-206, Oct. 2003.
- [23] Y. Yuan and C. T. Li, "Fragile watermarking scheme exploiting nondeterministic block-wise dependency," *Proc. IEEE, ICPR'04*, pp. 849-852, Cambridge, UK, Aug. 2004.
- [24] E. T. Lin and E. J. Delp, "A review of fragile image watermarks," *ACM Multimedia '99, Multimedia Contents*, Orlando, FL, pp. 25-29, Oct. 1999.
- [25] H. Lu, A. C. Kot and J. Cheng, "Secure data hiding in binary document images for authentication," *Proceedings of the 2003 IEEE International Symposium on Circuits and Systems (ISCAS 2003)*, Bangkok, Thailand, vol. 3, pp. 806-809, May 2003 (invited paper).
- [26] H. Lu, A. C. Kot and R. Susanto, "Binary Image Watermarking through Biased Binarization," in *Proceedings of the 2003 IEEE International Conference on Multimedia & Expo (ICME 2003)*, Baltimore, Maryland, July 2003.

BIBLIOGRAPHY

- [27] S. H. El-Din and M. Moniri, "Fragile and semi-fragile image authentication based on image self-similarity El-Din," *IEEE, ICIP'2002*, vol. 2, pp. 897-900, Sept. 2002.
- [28] Zhe-Ming Lu, Dian-Guo Xu, Chun-He Liu and Sheng-He Sun, "Semi-fragile image watermarking method based on index constrained vector quantisation," *Electronics Letters*, vol. 39, issue: 1, pp. 35-36, Jan. 2003.
- [29] Qibin Sun, Shih-Fu Chang, K. Maeno and M. Suto, "A new semi-fragile image authentication framework combining ECC and PKI infrastructures," *IEEE, ISCAS'2002*, vol.2, pp. II-440 - II-443, May 2002.
- [30] Qibin Sun and Shih-Fu Chang, "Semi-fragile image authentication using generic wavelet domain features and ECC," *IEEE, ICIP'2002*, vol. 2, pp. II-901 - II-904, Sept. 2002.
- [31] Y. Wang, J. F. Doherty and R. E. V. Dyck, "A wavelet-based watermarking algorithm for ownership verification of digital images," *IEEE Trans. on Image Processing*, vol. 11, issue. 2, pp. 77-88, Feb. 2002.
- [32] J. T. Brassil, S. Low, N. Maxemchuk and L. O'Gorman, "Watermarking document images with bounding box expansion," *Information hiding: first international workshop, Lecture Notes in CS, Springer*, vol. 1174, pp. 227-236, 1996.
- [33] J. T. Brassil, S. Low, N. F. Maxemchuk and L. O'Gorman, "Electronic marking and identification techniques to discourage document copying," *IEEE Journal on Selected Areas in Commun.*, vol. 13, no. 8, Oct. 1995.
- [34] J. T. Brassil, S. Low and N. F. Maxemchuk, "Copyright protection for the Electronic Distribution of Text Documents," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1181-1196, July 1999.

BIBLIOGRAPHY

- [35] M. Barni, F. Bartolini and A. Piva, "Multichannel watermarking of color images," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 12, issue: 3, pp. 142-156, Mar. 2002.
- [36] H. Lu, X. Shi, Y. Q. Shi, A. C. Kot and L. Chen, "Watermark embedding in DC components of DCT for binary images," *Proceedings of the IEEE International Workshop on Multimedia Signal Processing (MMSP 2002)*, US Virgin Islands, pp. 300-303, Dec. 2002.
- [37] Y. Q. Shi, Zhicheng Ni, Dekun Zou, Changyin Liang and Guorong Xua, "Lossless data hiding: fundamentals, algorithms and applications," *ISCAS 2004*, page(s): II - 33-6, vol.2, 23-26 May, 2004.
- [38] Zhicheng Ni, Y. Q. Shi, Ansari, N. and Wei Su, "Reversible data hiding," *ISCAS 2003*, page(s): II-912 - II-915, vol.2, 25-28 May, 2003.
- [39] A. Van Leest, M. van der Veen and Bruekers, F., "Reversible image watermarking," *ICIP 2003*, page(s): II - 731-734, 14-17 Sept. 2003.
- [40] Jun Tian, "Reversible data embedding using a difference expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, volume 13, issue 8, page(s):890 – 896, Aug. 2003.
- [41] A. M. Alattar, "Reversible watermark using difference expansion of triplets," *ICIP 2003*, page(s): I - 501-4, vol.1, 14-17 Sept. 2003.
- [42] A. M. Alattar, "Reversible watermark using difference expansion of quads," *IEEE International Conference on Acoustics, Speech, and Signal Processing, 2004(ICASSP '04)*, page(s): iii - 377-80, vol.3, 17-21 May 2004.
- [43] D. M. Thodi, and J. J. Rodriguez, "Prediction-error based reversible watermarking," *International Conference on Image Processing, 2004(ICIP '04)*, page(s):1549 – 1552, vol. 3, 24-27 Oct. 2004.

BIBLIOGRAPHY

- [44] M. U. Celik, G. Sharma, A. M. Tekalp and E. Saber, "Reversible data hiding," *International Conference on Image Processing*. 2002, page(s): II-157 - II-160, vol.2, 22-25 Sept. 2002.
- [45] Hiuk Jae Shim, Jinhaeng Ahn and Byeungwoo Jeon, "DH-LZW: lossless data hiding in LZW compression," *International Conference on Image Processing*, 2004(ICIP '04), page(s):2195 – 2198, Vol. 4, 24-27 Oct. 2004.
- [46] J. Fridrich, J. Goljan and R. Du, "Invertible Authentication," *Proceedings of SPIE, Security and Watermarking of Multimedia Contents III*, vol. 3971, pp. 197-208, San Jose, Jan. 2001.
- [47] Yanjiang Yang and Feng Bao, "An invertible watermarking scheme for authentication of Electronic Clinical Brain Atlas," *IEEE International Conference on Acoustics, Speech, and Signal Processing*, 2003(ICASSP '03), page(s): III - 533-6, vol.3, 6-10 April 2003.
- [48] I. J. Cox, M. L. Miller and J. A. Bloom, *Digital watermarking*, Morgan Kaufmann Publishers, 2002.
- [49] E. T. Lin and E. J. Delp, "A review of data hiding in digital images," in *Proceedings of the Image Processing, Image Quality, Image Capture Systems Conference (PICS '99)*, Savannah, Georgia, April 1999, pp. 274–278.
- [50] M. Chen, E. K. Wong, N. Memon and S. Adams, "Recent developments in document image watermarking and data hiding," *Proc. SPIE Conference on Multimedia Systems and Applications IV*, vol. 4518, pp. 166-176, Aug. 2001.
- [51] J. C. Zeng, "Steganography for Font-dependant Binary Documents," M.Eng. dissertation, Nanyang Technological University, Singapore, 2005.

BIBLIOGRAPHY

- [52] S. H. Low, N. F. Maxemchuk and A. M. Lapone, "Document identification for copyright protection using centroid detection," *IEEE Transactions on Communications*, vol. 46, no. 3, pp. 372-383, Mar. 1998.
- [53] S. H. Low and N. F. Maxemchuk, "Performance comparison of two text marking methods," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 561-572, May 1998.
- [54] N. F. Maxemchuk and S. H. Low, "Marking text documents," *Proc. IEEE International Conference on Image Processing*, vol. 3, pp. 26-29, Oct. 1997.
- [55] D. Huang and H. Yan, "Interword distance changes represented by sine waves for watermarking text images," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 11, no. 12, pp. 1237-1245, Dec. 2001.
- [56] Y. Liu, J. Mant, E. Wong, and S. H. Low, "Marking and detection of text documents using transform-domain techniques," *Proc. SPIE Conference on Security and Watermarking of Multimedia Contents III*, vol. 3657, pp. 317-328, Jan. 1999.
- [57] I. J. Cox, J. Kilian, F. T. Leighton and T. Shamoan, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, no.12, Dec. 1997.
- [58] D. Zou and Y. Q. Shi, "Formatted text document data hiding robust to printing, copying and scanning," *IEEE International Symposium on Circuits and Systems (ISCAS 2005)*, page(s):4971 – 4974, Vol. 5, 23-26 May 2005.
- [59] N. Chotikakamthorn, "Document image data hiding techniques using character spacing width sequence coding," *Proc. IEEE International Conference on Image Processing*, vol. 32, pp. 250-254, 1999.

BIBLIOGRAPHY

- [60] S. Hu, "Document Image Watermarking Algorithm Based on Neighborhood Pixel Ratio," *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '05)*, Volume 2, Page(s):841 – 844, March 18-23, 2005.
- [61] T. Amamo and D. Misaki, "A Feature calibration method for watermarking of document images," *Proc. the 5th International Conference on Document Analysis and Recognition*, pp. 91-94, Sept. 1999.
- [62] Q. G. Mei, E. K. Wong and N. D. Memon, "Data hiding in binary text documents," *Proc. of SPIE Conference on Security and Watermarking of Multimedia Contents III*, vol. 4314, pp. 369-375, Aug. 2001.
- [63] M. Wu, E. Tang and B. Liu, "Data hiding in digital binary image," *Proc. IEEE International Conf. on Multimedia and Expo*, vol. 1, pp. 393-396, 2000.
- [64] H. Lu, A. C. Kot and Y. Q. Shi, "Distance-reciprocal distortion measure for binary document images," *IEEE Signal Processing Letters*, vol. 11, no. 2, pp. 228-231, Feb. 2004.
- [65] H. Lu, J. Wang, A. C. Kot and Y. Q. Shi, "An objective distortion measure for binary document images based on human visual perception," *Proceedings of the Sixteenth International Conference on Pattern Recognition (ICPR 2002)*, Quebec City, vol. 4, pp. 239-242, Aug. 2002.
- [66] Y.-C. Tseng and H.-K. Pan, "Secure and Invisible Data Hiding in 2-Color Images," *Proceedings of INFOCOM 2001*, 2001, pp. 887-896.
- [67] Y.-C. Tseng, Y.-Y. Chen and H.-K. Pan, "A Secure Data Hiding Scheme for Binary Images," *IEEE Transactions on Communications*, vol. 50, pp. 1227-1231, Aug. 2002.

BIBLIOGRAPHY

- [68] HIOKI Hirohisa, “A Modified CPT Scheme for Embedding Data into Binary Images”, *Proc. of Pacific Rim Workshop on Digital Steganography 2003*, pp.32-44, Jul. 2003.
- [69] Huijuan Yang and A. C. Kot, “Data hiding for bi-level documents using smoothing technique,” *Proceedings of the 2004 International Symposium on Circuits and Systems (ISCAS '04)*, page(s):692-695, vol.5, 23-26 May 2004.
- [70] <http://unique-name.perceptus.ca/random-word.php>
- [71] C-L Tsai, K-C Fan, C-D Chung and T.C. Chuang, “Data Hiding of Binary Images Using Pair-wise Logical Computation Mechanism,” in *Proc. IEEE International Conference on Multimedia and Expo, ICME 2004*, vol. 2, pp. 951-954, 2004.
- [72] B. Schneier, *Applied Cryptography*, second edition, John Wiley & sons, 1996
- [73] Huijuan Yang and A. C. Kot, “Data Hiding For Text Document Image Authentication by Connectivity-Preserving,” *IEEE International Conference on Acoustics, Speech, and Signal Processing*, volume 2, page(s):505 – 508, March 18-23, 2005.
- [74] Zhang Guannan and Wang Shuxun, “A private watermarking for halftone image by stochastic error diffusion,” *International Conference on Signal Processing, 2004*, volume 3, page(s):2362 – 2365, 31 Aug. - 4 Sept. 2004.
- [75] Ming Sun Fu and O. C. Au, “A robust public watermark for halftone images,” *ISCAS 2002*, volume 3, page(s):639 – 642, 26-29 May 2002.

APPENDIX I

PARTIAL MATLAB CODE

Checking two sides of a segment

if the segment belongs to category 1

do nothing and go to next segment; no bit is embedded

else if it belongs to one of category 2, 3, 4, 5, 6, 7, 8

if ($L_s \bmod 2$) $\neq$ data bit

reduce a black pixel at either side with “-” sign and go to next
segment to embed NEXT data bit; one bit has been embedded

else

do nothing and go to next segment to embed NEXT data bit; one
bit has been embedded

end

else if it belongs to category 9

if ($L_s \bmod 2$) $\neq$ data bit

add a black pixel at either side and go to next segment to embed
NEXT data bit; one bit has been embedded

else

do nothing and go to next segment to embed NEXT data bit; one
bit has been embedded

end

else if it belongs to category 10

if ($L_s \bmod 2$) $\neq$ data bit

APPENDIX I. PARTIAL MATLAB CODE

```
        reduce a black pixel at either side and go to next segment to  
        embed NEXT data bit; one bit has been embedded  
  
    else  
        go to next segment to embed CURRENT data bit; NO bit has been  
        embedded  
  
    end  
  
    else if it belongs to one of category 11, 12  
        if ( $L_s \bmod 2$ )  $\neq$  data bit  
            reduce a black pixel at the side with “-” sign and go to next  
            segment to embed NEXT data bit; one bit has been embedded  
        else  
            go to next segment to embed NEXT data bit; one bit has been  
            embedded  
        end  
  
    else if it belongs to one of category 13, 14  
        if ( $L_s \bmod 2$ )  $\neq$  data bit  
            add a black pixel at the side with “+” sign and check the “adding”  
            property of this segment again;  
            if the segment has “adding” property  
                go to next segment to embed NEXT data bit; one bit has been  
                embedded  
            else  
                go to next segment to embed CURRENT data bit; NO bit has  
                been embedded  
            end  
        end
```

APPENDIX I. PARTIAL MATLAB CODE

```
    else
        go to next segment to embed NEXT data bit; one bit has been
        embedded
    end
else if it belongs to one of category 15, 16
    if ( $L_s$  modulo 2)  $\neq$  data bit
        reduce a black pixel at the correct side and go to next segment to
        embed NEXT data bit; one bit has been embedded
    else
        go to next segment to embed CURRENT data bit; NO bit has been
        embedded
    end
end
```

APPENDIX II

EXAMPLE IMAGES

Security for wireless and mobile networks – Key management in wireless/mobile/ad hoc environments, secure access control protocols, secure wireless/mobile/ad hoc routing, denial of service, privacy and anonymity, and prevention of traffic analysis.

Methods and tools for efficient security assessment/ certification/verification of products – Processes, techniques and tools that could effectively and efficiently test and verify the security claims of products. This will inspire confidence both in the product and the overall system, as well as to enable well-founded and steady improvements in the development of security products.

Data storage security at the system level – Edge computing entails the distribution of data to servers at the “edge” of the network that perform tasks on behalf of the master server. Issues that must be addressed include authentication of query results, secure and efficient propagation of updates, steganographic storage schemes and counter-measures against traffic analysis, distributed storage volumes that provide security and resilience, and also access control and authentication of the edge storage servers.

Security management (including usability) – Security management technologies should adapt to changes in non-intrusive detection, identification and verification technologies. This would encompass the need to analyse and respond to network related needs.

Underlying technologies – Cryptography, mathematical proofs, confidentiality, integrity and availability of the data. Development of tamper-proof/resistant devices/techniques to ensure the security of implementation as well as the ability to sense and respond to tamper.

4. HIGHLIGHTS OF WORKSHOP PRESENTATIONS

Keynote Presentations Professor Ravi Sandhu from George Mason University, USA, initiated the workshop with a keynote presentation on next generation access control. The term usage control is a generalisation of access control to cover obligations, conditions, ongoing controls and mutability. Traditionally, access control has dealt only with authorisation decisions on users’ access to target resources. Obligations are requirements that have to be fulfilled by the subject for allowing access. Conditions are subject and object-independent environmental requirements that have to be satisfied for access. In today’s dynamic, distributed environment, obligations and conditions are also crucial decision factors for richer and finer controls on usage of digital resources. Traditional authorisation decisions are generally made at the time of requests but hardly recognise ongoing controls for relatively long-lived access or

(Times New Roman, font size 12)

Figure1: English_72dpi.

APPENDIX II. EXAMPLE IMAGES

Security for wireless and mobile networks – Key management in wireless/mobile/ad hoc environments, secure access control protocols, secure wireless/mobile/ad hoc routing, denial of service, privacy and anonymity, and prevention of traffic analysis.

Methods and tools for efficient security assessment/ certification/verification of products – Processes, techniques and tools that could effectively and efficiently test and verify the security claims of products. This will inspire confidence both in the product and the overall system, as well as to enable well-founded and steady improvements in the development of security products.

Data storage security at the system level – Edge computing entails the distribution of data to servers at the “edge” of the network that perform tasks on behalf of the master server. Issues that must be addressed include authentication of query results, secure and efficient propagation of updates, steganographic storage schemes and counter-measures against traffic analysis, distributed storage volumes that provide security and resilience, and also access control and authentication of the edge storage servers.

Security management (including usability) – Security management technologies should adapt to changes in non-intrusive detection, identification and verification technologies. This would encompass the need to analyse and respond to network related needs.

Underlying technologies – Cryptography, mathematical proofs, confidentiality, integrity and availability of the data. Development of tamper-proof/resistant devices/techniques to ensure the security of implementation as well as the ability to sense and respond to tamper.

4. HIGHLIGHTS OF WORKSHOP PRESENTATIONS

Keynote Presentations Professor Ravi Sandhu from George Mason University, USA, initiated the workshop with a keynote presentation on next generation access control. The term usage control is a generalisation of access control to cover obligations, conditions, ongoing controls and mutability. Traditionally, access control has dealt only with authorisation decisions on users' access to target resources. Obligations are requirements that have to be fulfilled by the subject for allowing access. Conditions are subject and object-independent environmental requirements that have to be satisfied for access. In today's dynamic, distributed environment, obligations and conditions are also crucial decision factors for richer and finer controls on usage of digital resources. Traditional authorisation decisions are generally made at the time of requests but hardly recognise ongoing controls for relatively long-lived access or

(Times New Roman, font size 12)

Figure 2: English_96dpi.

APPENDIX II. EXAMPLE IMAGES

Security for wireless and mobile networks – Key management in wireless/mobile/ad hoc environments, secure access control protocols, secure wireless/mobile/ad hoc routing, denial of service, privacy and anonymity, and prevention of traffic analysis.

Methods and tools for efficient security assessment/ certification/verification of products – Processes, techniques and tools that could effectively and efficiently test and verify the security claims of products. This will inspire confidence both in the product and the overall system, as well as to enable well-founded and steady improvements in the development of security products.

Data storage security at the system level – Edge computing entails the distribution of data to servers at the “edge” of the network that perform tasks on behalf of the master server. Issues that must be addressed include authentication of query results, secure and efficient propagation of updates, steganographic storage schemes and counter-measures against traffic analysis, distributed storage volumes that provide security and resilience, and also access control and authentication of the edge storage servers.

Security management (including usability) – Security management technologies should adapt to changes in non-intrusive detection, identification and verification technologies. This would encompass the need to analyse and respond to network related needs.

Underlying technologies – Cryptography, mathematical proofs, confidentiality, integrity and availability of the data. Development of tamper-proof/resistant devices/techniques to ensure the security of implementation as well as the ability to sense and respond to tamper.

4. HIGHLIGHTS OF WORKSHOP PRESENTATIONS

Keynote Presentations Professor Ravi Sandhu from George Mason University, USA, initiated the workshop with a keynote presentation on next generation access control. The term usage control is a generalisation of access control to cover obligations, conditions, ongoing controls and mutability. Traditionally, access control has dealt only with authorisation decisions on users' access to target resources. Obligations are requirements that have to be fulfilled by the subject for allowing access. Conditions are subject and object-independent environmental requirements that have to be satisfied for access. In today's dynamic, distributed environment, obligations and conditions are also crucial decision factors for richer and finer controls on usage of digital resources. Traditional authorisation decisions are generally made at the time of requests but hardly recognise ongoing controls for relatively long-lived access or

(Times New Roman, font size 12)

Figure 3: English_150dpi.

APPENDIX II. EXAMPLE IMAGES

Security for wireless and mobile networks – Key management in wireless/mobile/ad hoc environments, secure access control protocols, secure wireless/mobile/ad hoc routing, denial of service, privacy and anonymity, and prevention of traffic analysis

Methods and tools for efficient security assessment/ certification/verification of products – Processes, techniques and tools that could effectively and efficiently test and verify the security claims of products. This will inspire confidence both in the product and the overall system, as well as to enable well-founded and steady improvements in the development of security products.

Data storage security at the system level – Edge computing entails the distribution of data to servers at the “edge” of the network that perform tasks on behalf of the master server. Issues that must be addressed include authentication of query results, secure and efficient propagation of updates, steganographic storage schemes and counter-measures against traffic analysis, distributed storage volumes that provide security and resilience, and also access control and authentication of the edge storage servers.

Security management (including usability) – Security management technologies should adapt to changes in non-intrusive detection, identification and verification technologies. This would encompass the need to analyse and respond to network related needs

Underlying technologies – Cryptography, mathematical proofs, confidentiality, integrity and availability of the data. Development of tamper-proof/resistant devices/techniques to ensure the security of implementation as well as the ability to sense and respond to tamper.

4. HIGHLIGHTS OF WORKSHOP PRESENTATIONS

Keynote Presentations Professor Ravi Sandhu from George Mason University, USA, initiated the workshop with a keynote presentation on next generation access control. The term usage control is a generalisation of access control to cover obligations, conditions, ongoing controls and mutability. Traditionally, access control has dealt only with authorisation decisions on users’ access to target resources. Obligations are requirements that have to be fulfilled by the subject for allowing access. Conditions are subject and object-independent environmental requirements that have to be satisfied for access. In today’s dynamic, distributed environment, obligations and conditions are also crucial decision factors for richer and finer controls on usage of digital resources. Traditional authorisation decisions are generally made at the time of requests but hardly recognise ongoing controls for relatively long-lived access or

(Times New Roman, font size 12)

Figure 4: English_300dpi.

APPENDIX II. EXAMPLE IMAGES

Figure 5: Arabic_72dpi.

APPENDIX II. EXAMPLE IMAGES

Figure 6: Arabic_96dpi.

APPENDIX II. EXAMPLE IMAGES

Figure 7: Arabic_150dpi.

APPENDIX II. EXAMPLE IMAGES

Figure 8: Arabic_300dpi.

APPENDIX II. EXAMPLE IMAGES

C. 请缔约方会议采取的行动

5. 根据清洁发展机制模式和程序第3 和4 段的规定以及第17/CP.7 号决定第 6 段的规定，缔约方会议不妨在第八届会议上审查和注意执行理事会的第一次年度报告(2001-2002 年)，并通过作出有关以下各项的决定向执行理事会提供指导意见：

(a) 执行理事会就本报告附件所载议事规则提出的建议；

(b) 执行理事会根据第17/CP.7 号决定包括清洁发展机制模式和程序的规定提出的建议，尤其是关于本报告附件二所载用于含平标准的清洁发展机制小规模项目活动的简化模式和程序的建议；

(c) 酌情指定执行理事会根据《京都议定书》第十二条第5 款和清洁发展机制模式和程序附录A 所载认证标准认证的经营实体。

6. 缔约方会议不妨将执行理事会的权限延至第八届会议以后，以便经理事会认证的经营实体在得到缔约方会议指定之前予以暂时指定。

7. 缔约方会议第八届会议不妨再请缔约各方向《公约》补充活动信托基金出资，支持与尽快启动清洁发展机制有关的活动，包括拟订清洁发展机制登记册。

二、执行理事会处理的组织事项

8. 执行理事会在本报告所涉时期内举行了五次会议，包括对各个议程项目加以辅助说明的文件在内的各次执行理事会会议的议程、议程说明以及报告已列入《公约》清洁发展机制的网站(<http://unfccc.int/cdm/ebmeet.html>)，可公开查阅。理事会各次会议的报告载有理事和候补理事的出席情况，并说明了遵行法定人数规定的情况。

A. 就职宣誓

9. 在承担执行理事会的职务之前，理事会的全体理事和候补理事按照清洁发展机制模式和程序第8 段(e) 分段签署了宣誓就职书。

宋体,12

Figure 9: Chinese_72dpi.

APPENDIX II. EXAMPLE IMAGES

C. 请缔约方会议采取的行动

5. 根据清洁发展机制模式和程序第3 和4 段的规定以及第17/CP.7 号决定第 6 段的规定，缔约方会议不妨在第八届会议上审查和注意执行理事会的第一次年度报告(2001-2002 年)，并通过作出有关以下各项的决定向执行理事会提供指导意见：

(a) 执行理事会就本报告附件所载议事规则提出的建议；

(b) 执行理事会根据第17/CP.7 号决定包括清洁发展机制模式和程序的规定提出的建议，尤其是关于本报告附件二所载用于合乎标准的清洁发展机制小规模项目活动的简化模式和程序的建议；

(c) 酌情指定执行理事会根据《京都议定书》第十二条第5 款和清洁发展机制模式和程序附录A 所载认证标准认证的经营实体。

6. 缔约方会议不妨将执行理事会的权限延至第八届会议以后，以便经理事会认证的经营实体在得到缔约方会议指定之前予以暂时指定。

7. 缔约方会议第八届会议不妨再请缔约各方向《公约》补充活动信托基金出资，支持与尽快启动清洁发展机制有关的活动，包括拟订清洁发展机制登记册。

二、执行理事会处理的组织事项

8. 执行理事会在本报告所涉时期内举行了五次会议。包括对各个议程项目加以辅助说明的文件在内的各次执行理事会会议的议程、议程说明以及报告已列入《公约》清洁发展机制的网站(<http://unfccc.int/cdm/ebmeet.html>)，可公开查阅。理事会各次会议的报告载有理事和候补理事的出席情况，并说明了遵行法定人数规定的情况。

A. 就职宣誓

9. 在承担执行理事会的职务之前，理事会的全体理事和候补理事按照清洁发展机制模式和程序第8 段 (e) 分段签署了宣誓就职书。

宋体,12

Figure 10: Chinese_96dpi.

APPENDIX II. EXAMPLE IMAGES

C. 请缔约方会议采取的行动

5. 根据清洁发展机制模式和程序第3 和4 段的规定以及第17/CP.7 号决定第 6 段的规定，缔约方会议不妨在第八届会议上审查和注意执行理事会的第一次年度报告(2001-2002 年)，并通过作出有关以下各项的决定向执行理事会提供指导意见：

(a) 执行理事会就本报告附件所载议事规则提出的建议；

(b) 执行理事会根据第17/CP.7 号决定包括清洁发展机制模式和程序的规定提出的建议，尤其是关于本报告附件二所载用于合乎标准的清洁发展机制小规模项目活动的简化模式和程序的建议；

(c) 酌情指定执行理事会根据《京都议定书》第十二条第5 款和清洁发展机制模式和程序附录A 所载认证标准认证的经营实体。

6. 缔约方会议不妨将执行理事会的权限延至第八届会议以后，以便经理事会认证的经营实体在得到缔约方会议指定之前予以暂时指定。

7. 缔约方会议第八届会议不妨再请缔约各方向《公约》补充活动信托基金出资，支持与尽快启动清洁发展机制有关的活动，包括拟订清洁发展机制登记册。

二、执行理事会处理的组织事项

8. 执行理事会在本报告所涉时期内举行了五次会议。包括对各个议程项目加以辅助说明的文件在内的各次执行理事会会议的议程、议程说明以及报告已列入《公约》清洁发展机制的网站(<http://unfccc.int/cdm/ebmeet.html>)，可公开查阅。理事会各次会议的报告载有理事和候补理事的出席情况，并说明了遵行法定人数规定的情况。

A. 就职宣誓

9. 在承担执行理事会的职务之前，理事会的全体理事和候补理事按照清洁发展机制模式和程序第8 段 (e) 分段签署了宣誓就职书。

宋体,12

Figure 11: Chinese_150dpi.

APPENDIX II. EXAMPLE IMAGES

C. 请缔约方会议采取的行动

5. 根据清洁发展机制模式和程序第3 和4 段的规定以及第17/CP.7 号决定第 6 段的规定，缔约方会议不妨在第八届会议上审查和注意执行理事会的第一次年度报告(2001-2002 年)，并通过作出有关以下各项的决定向执行理事会提供指导意见：

(a) 执行理事会就本报告附件所载议事规则提出的建议；

(b) 执行理事会根据第17/CP.7 号决定包括清洁发展机制模式和程序的规定提出的建议，尤其是关于本报告附件二所载用于合乎标准的清洁发展机制小规模项目活动的简化模式和程序的建议；

(c) 酌情指定执行理事会根据《京都议定书》第十二条第5 款和清洁发展机制模式和程序附录A 所载认证标准认证的经营实体。

6. 缔约方会议不妨将执行理事会的权限延至第八届会议以后，以便经理事会认证的经营实体在得到缔约方会议指定之前予以暂时指定。

7. 缔约方会议第八届会议不妨再请缔约各方向《公约》补充活动信托基金出资，支持与尽快启动清洁发展机制有关的活动，包括拟订清洁发展机制登记册。

二、执行理事会处理的组织事项

8. 执行理事会在本报告所述时期内举行了五次会议。包括对各个议程项目加以辅助说明的文件在内的各次执行理事会会议的议程、议程说明以及报告已列入《公约》清洁发展机制的网站(<http://unfccc.int/cdm/ebmeet.html>)，可公开查阅。理事会各次会议的报告载有理事和候补理事的出席情况，并说明了遵行法定人数规定的情况。

A 就职宣誓

9. 在承担执行理事会的职务之前，理事会的全体理事和候补理事按照清洁发展机制模式和程序第8 段(c) 分段签署了宣誓就职书。

宋体,12

Figure 12: Chinese_300dpi.

APPENDIX II. EXAMPLE IMAGES

EMU Ne, demokracija Da**Zauzmite stajalište za demokraciju a protiv eura!**

Da za EMU će nagristi demokraciju. Želimo veću suradnju među neovisnim državama umjesto veću vlast na nivou Europske Unije (EU). Europska Monetarna Unija (EMU) pretvara EU u Sjedinjene Europske Države, što bi povećavalo nemoć ljudi i njihov osjećaj da su po strani kao i proširavalo jaz između izabranih povjerenika i glasača.

Članstvom u EMU također bi se odrekli i mogućnosti korištenja kamata i monetarne politike kao oruđa u gospodarstvu. Želimo i ubuduće imati mogućnost da koristimo to oruđe tada kada mi u zajednici to želimo, na primjer da bi spasili radnih mjesta i zaštitili školstvo, zdravstvo i društvenu skrb. Predati za uvijek to oruđe središnjoj banci u Frankfurtu bi bilo nedemokratski i krajnje neodgovorno prema budućim generacijama.

EMU više pogađa ljude koji su već ugroženi u društvu

Grupe kod kojih je nezaposlenost veća, sigurnost radnog odnosa manja a plaće niže dok je osjećaj da su po strani najveći, biće najviše pogođeni negativnim posljedicama EMU. Ako nestane mogućnost korištenja kamata i monetarne politike kao oruđa u gospodarstvu, opasnost je veća da će loše ekonomsko stanje biti i duže i jače, kao što je slučaj sa trenutnom krizom u Njemačkoj. Nemojte se zavaravati da će središnja banka u Frankfurtu prilagođavati svoju politiku prema željama malih država poput Švedske.

EMU jača pritisak na EU u pogledu zajedničke gospodarske politike. Takva politika pogađa one koji su već ugroženi u društvu. EMU-om se smanjuju mogućnosti mnogih ljudi da utječu kako na društvo tako i na svoj osobni položaj u njemu.

EMU je krajnje rizičan projekt

Zato najveći središnji sindikat u Švedskoj, LO, podneo zahtjev vladi da se odvajaju novčana sredstva koja bi se mogla koristiti u slučaju lošeg ekonomskog stanja u budućnosti. Socijaldemokrati su to odbili. EMU je u tolikoj mjeri rizičan projekt da gospodarstvenici i političari od krajnje desnice do krajnje ljevice, kao i više ministara pa čak i bivši guverneri Švedske državne banke, su protiv EMU.

EMU sprječava globalnu solidarnost

Da li stvarno mislite da bi Sjedinjene Europske Države bile više solidarne od Sjedinjenih Američkih Država? Teško je povjerovati da bi to mogao biti slučaj. Prije bi glasovi poput glasa Njemačke u pogledu otpora prema ratu u Iraku kao i glasa Švedske u pogledu trgovine najsiromašnijih država, potpuno ušutkali. EU na primjer koristi mjeru sankcija protiv Zimbabve-a, ali ne i protiv Izraela koji krši uvjete u svojim trgovinskim ugovorima sa EU.

EU također ne preuzima odgovornost ni za globalna pitanja zaštite čovjekova okoliša nego misli najprije na to kako će stvoriti prednosti velikim poduzećima unutar EU. Istodobno uopće ne mari za razvitak siromašnih država.

EU sa većom vlašću će, na žalost, samo pojačavati sebičnost unutar EU kao i središte na brzi dobit poduzeća unutar EU.

Uzmite sigurno za gotovo pa glasajte Ne za EMU na referendumu 14. rujna.

Svi građani koji imaju pravo glasa na općinskim izborima mogu glasati i na referendumu o EMU. Ne morate biti švedski državljanin.

www.mp.se/emu

Figure 13: Croatian_72dpi.

APPENDIX II. EXAMPLE IMAGES

EMU Ne, demokracija Da**Zauzmite stajalište za demokraciju a protiv eura!**

Da za EMU će nagristi demokraciju. Želimo veću suradnju među neovisnim državama umjesto veću vlast na nivou Europske Unije (EU). Europska Monetarna Unija (EMU) pretvara EU u Sjedinjene Europske Države, što bi povećavalo nemoć ljudi i njihov osjećaj da su po strani kao i proširavalo jaz između izabranih povjerenika i glasača.

Članstvom u EMU također bi se odrekli i mogućnosti korištenja kamata i monetarne politike kao oruđa u gospodarstvu. Želimo i ubuduće imati mogućnost da koristimo to oruđe tada kada mi u zajednici to želimo, na primjer da bi spasili radnih mjesta i zaštitili školstvo, zdravlje i društvenu skrb. Predati za uvijek to oruđe središnjoj banci u Frankfurtu bi bilo nedemokratski i krajnje neodgovorno prema budućim generacijama.

EMU više pogađa ljude koji su već ugroženi u društvu

Grupe kod kojih je nezaposlenost veća, sigurnost radnog odnosa manja a plaće niže dok je osjećaj da su po strani najveći, biće najviše pogođeni negativnim posljedicama EMU. Ako nestane mogućnost korištenja kamata i monetarne politike kao oruđa u gospodarstvu, opasnost je veća da će loše ekonomsko stanje biti i duže i jače, kao što je slučaj sa trenutnom krizom u Njemačkoj. Nemojte se zavaravati da će središnja banka u Frankfurtu prilagođavati svoju politiku prema željama malih država poput Švedske.

EMU jača pritisak na EU u pogledu zajedničke gospodarske politike. Takva politika pogađa one koji su već ugroženi u društvu. EMU-om se smanjuju mogućnosti mnogih ljudi da utječu kako na društvo tako i na svoj osobni položaj u njemu.

EMU je krajnje rizičan projekt

Zato najveći središnji sindikat u Švedskoj, LO, podneo zahtjev vladi da se odvajaju novčana sredstva koja bi se mogla koristiti u slučaju lošeg ekonomskog stanja u budućnosti. Socijaldemokrati su to odbili. EMU je u tolikoj mjeri rizičan projekt da gospodarstvenici i političari od krajnje desnice do krajnje ljevice, kao i više ministara pa čak i bivši guverneri Švedske državne banke, su protiv EMU.

EMU sprječava globalnu solidarnost

Da li stvamo mislite da bi Sjedinjene Europske Države bile više solidarne od Sjedinjenih Američkih Država? Teško je povjerovati da bi to mogao biti slučaj. Prije bi glasovi poput glasa Njemačke u pogledu otpora prema ratu u Iraku kao i glasa Švedske u pogledu trgovine najsiromašnijih država, potpuno ušutkali. EU na primjer koristi mjeru sankcija protiv Zimbabve-a, ali ne i protiv Izraela koji krši uvjete u svojim trgovinskim ugovorima sa EU.

EU također ne preuzima odgovornost ni za globalna pitanja zaštite čovjekova okoliša nego misli najprije na to kako će stvoriti prednosti velikim poduzećima unutar EU. Istodobno uopće ne mari za razvitak siromašnih država.

EU sa većom vlašću će, na žalost, samo pojačavati sebičnost unutar EU kao i središte na brzi dobit poduzeća unutar EU.

Uzmite sigurno za gotovo pa glasajte Ne za EMU na referendumu 14. rujna.

Svi građani koji imaju pravo glasa na općinskim izborima mogu glasati i na referendumu o EMU. Ne morate biti švedski državljanin.

www.mp.se/emu

Figure 14: Croatian_96dpi.

APPENDIX II. EXAMPLE IMAGES

EMU Ne, demokracija Da**Zauzmite stajalište za demokraciju a protiv eura!**

Da za EMU će nagristi demokraciju. Želimo veću suradnju među neovisnim državama umjesto veću vlast na nivou Europske Unije (EU). Europska Monetarna Unija (EMU) pretvara EU u Sjedinjene Europske Države, što bi povećavalo nemoć ljudi i njihov osjećaj da su po strani kao i proširavalo jaz između izabranih povjerenika i glasača.

Članstvom u EMU također bi se odrekli i mogućnosti korištenja kamata i monetarne politike kao oruđa u gospodarstvu. Želimo i ubuduće imati mogućnost da koristimo to oruđe tada kada mi u zajednici to želimo, na primjer da bi spasili radnih mjesta i zaštitili školstvo, zdravstvo i društvenu skrb. Predati za uvijek to oruđe središnjoj banci u Frankfurtu bi bilo nedemokratski i krajnje neodgovorno prema budućim generacijama.

EMU više pogađa ljude koji su već ugroženi u društvu

Grupe kod kojih je nezaposlenost veća, sigurnost radnog odnosa manja a plaće niže dok je osjećaj da su po strani najveći, biće najviše pogođeni negativnim posljedicama EMU. Ako nestane mogućnost korištenja kamata i monetarne politike kao oruđa u gospodarstvu, opasnost je veća da će loše ekonomsko stanje biti i duže i jače, kao što je slučaj sa trenutnom krizom u Njemačkoj. Nemojte se zavaravati da će središnja banka u Frankfurtu prilagođavati svoju politiku prema željama malih država poput Švedske.

EMU jača pritisak na EU u pogledu zajedničke gospodarske politike. Takva politika pogađa one koji su već ugroženi u društvu. EMU-om se smanjuju mogućnosti mnogih ljudi da utječu kako na društvo tako i na svoj osobni položaj u njemu.

EMU je krajnje rizičan projekt

Zato najveći središnji sindikat u Švedskoj, LO, podneo zahtjev vladi da se odvajaju novčana sredstva koja bi se mogla koristiti u slučaju lošeg ekonomskog stanja u budućnosti. Socijaldemokrati su to odbili. EMU je u tolikoj mjeri rizičan projekt da gospodarstvenici i političari od krajnje desnice do krajnje ljevice, kao i više ministara pa čak i bivši guverneri Švedske državne banke, su protiv EMU.

EMU sprječava globalnu solidarnost

Da li stvarno mislite da bi Sjedinjene Europske Države bile više solidarne od Sjedinjenih Američkih Država? Teško je povjerovati da bi to mogao biti slučaj. Prije bi glasovi poput glasa Njemačke u pogledu otpora prema ratu u Iraku kao i glasa Švedske u pogledu trgovine najsiromašnijih država, potpuno ušutkali. EU na primjer koristi mjeru sankcija protiv Zimbabve-a, ali ne i protiv Izraela koji krši uvjete u svojim trgovinskim ugovorima sa EU.

EU također ne preuzima odgovornost ni za globalna pitanja zaštite čovjekova okoliša nego misli najprije na to kako će stvoriti prednosti velikim poduzećima unutar EU. Istodobno uopće ne mari za razvitak siromašnih država.

EU sa većom vlašću će, na žalost, samo pojačavati sebičnost unutar EU kao i središte na brzi dobit poduzeća unutar EU.

Uzmite sigurno za gotovo pa glasajte Ne za EMU na referendumu 14. rujna.

Svi građani koji imaju pravo glasa na općinskim izborima mogu glasati i na referendumu o EMU. Ne morate biti švedski državljanin.

www.mp.se/emu

Figure 15: Croatian_150dpi.

APPENDIX II. EXAMPLE IMAGES

EMU Ne, demokracija Da**Zauzmite stajalište za demokraciju a protiv eura!**

Da za EMU će nagristi demokraciju. Želimo veću suradnju među neovisnim državama umjesto veću vlast na nivou Europske Unije (EU). Europska Monetarna Unija (EMU) pretvara EU u Sjedinjene Europske Države, što bi povećavalo nemoć ljudi i njihov osjećaj da su po strani kao i proširavalo jaz između izabranih povjerenika i glasača.

Članstvom u EMU također bi se odrekli i mogućnosti korištenja kamata i monetarne politike kao oruđa u gospodarstvu. Želimo i ubuduće imati mogućnost da koristimo to oruđe tada kada mi u zajednici to želimo, na primjer da bi spasili radnih mjesta i zaštitili školstvo, zdravstvo i društvenu skrb. Predati za uvijek to oruđe središnjoj banci u Frankfurtu bi bilo nedemokratski i krajnje neodgovorno prema budućim generacijama.

EMU više pogađa ljude koji su već ugroženi u društvu

Grupe kod kojih je nezaposlenost veća, sigurnost radnog odnosa manja a plaće niže dok je osjećaj da su po strani najveći, biće najviše pogođeni negativnim posljedicama EMU. Ako nestane mogućnost korištenja kamata i monetarne politike kao oruđa u gospodarstvu, opasnost je veća da će loše ekonomsko stanje biti i duže i jače, kao što je slučaj sa trenutnom krizom u Njemačkoj. Nemojte se zavaravati da će središnja banka u Frankfurtu prilagođavati svoju politiku prema željama malih država poput Švedske.

EMU jača pritisak na EU u pogledu zajedničke gospodarske politike. Takva politika pogađa one koji su već ugroženi u društvu. EMU-om se smanjuju mogućnosti mnogih ljudi da utječu kako na društvo tako i na svoj osobni položaj u njemu.

EMU je krajnje rizičan projekt

Zato najveći središnji sindikat u Švedskoj, LO, podneo zahtjev vladi da se odvajaju novčana sredstva koja bi se mogla koristiti u slučaju lošeg ekonomskog stanja u budućnosti. Socijaldemokrati su to odbili. EMU je u tolikoj mjeri rizičan projekt da gospodarstvenici i političari od krajnje desnice do krajnje ljevice, kao i više ministara pa čak i bivši guverneri Švedske državne banke, su protiv EMU.

EMU sprječava globalnu solidarnost

Da li stvarno mislite da bi Sjedinjene Europske Države bile više solidarne od Sjedinjenih Američkih Država? Teško je povjerovati da bi to mogao biti slučaj. Prije bi glasovi poput glasa Njemačke u pogledu otpora prema ratu u Iraku kao i glasa Švedske u pogledu trgovine najsiromašnijih država, potpuno usutkali. EU na primjer koristi mjeru sankcija protiv Zimbabve-a, ali ne i protiv Izraela koji krši uvjete u svojim trgovinskim ugovorima sa EU.

EU također ne preuzima odgovornost ni za globalna pitanja zaštite čovjekova okoliša nego misli najprije na to kako će stvoriti prednosti velikim poduzećima unutar EU. Istodobno uopće ne mari za razvitak siromašnih država.

EU sa većom vlašću će, na žalost, samo pojačavati sebičnost unutar EU kao i središte na brzi dobit poduzeća unutar EU.

Uzmite sigurno za gotovo pa glasajte Ne za EMU na referendumu 14. rujna.

Svi građani koji imaju pravo glasa na općinskim izborima mogu glasati i na referendumu o EMU. Ne morate biti švedski državljanin.

www.mp.se/emu

Figure 16: Croatian_300dpi.