私立東海大學資訊工程與科學研究所

碩士論文

指導教授：林祝興 博士

Dr. Chu-Hsing Lin

基於數位樣板的二元文件影像完整性保護技術

Integrity Protection of Binary Document Images Based on Digital Patterns

研究生：林育瑩 撰

(Yu-Ying Lin)

中　華　民　國　九　十　七　年　六　月

Abstract

It is more difficult to protect binary document images than color or grayscale images. Because binary document images are often in black and white format and there is thus less redundancy that can be exploited for embedding additional information. In this thesis, a scheme for integrity protection of binary document images based on digital patterns is proposed. The image skeleton and the inverse skeleton are found through thinning and the skeleton signature is combined with watermark information. The result is encrypted asymmetrically and hidden in embeddable locations of the image. A series of attack experiments are conducted to demonstrate that the approach is capable of detecting tampering. Even single malicious pixel modifications can be detected. The approach is computationally more efficient than previous approaches.

Keywords: integrity protection, digital watermark, flippability, thinning, digital pattern, skeleton

摘要

在此研究論文當中，我們將提出一個基於影像樣板的二元文件影像完整性保護架構，二元影像較困難於灰階影像及彩色影像，因為二元影像只由黑色及白色像素所構成，因此對於嵌入方面便更顯得困難。架構上我們將二元文件影像的黑及白樣板透過細線化的方法取出，且和使用者的浮水印資訊做組合後透過非對稱的加密方法加密，之後再將加密資訊嵌入到原有的二元文件影像中可嵌入的位置，供日後完整性的判定。對於實驗部份我們提供了一系列的攻擊方式，而實驗結果顯示此方法架構能有效的偵測出此二元文件影像是否遭受竄改攻擊，甚至連最細微攻擊也都能有效的偵測出，另外，和先前的方法做比較上，除了能有效的偵測出是否遭受竄改之外，此方法的計算複雜度也較先前的方法來的要好。

關鍵詞：完整性保護、數位浮水印、可翻轉性、細線化、數位樣板、骨架

致 謝

本篇論文之所以能順利完成，要感謝的人實在很多，首先要感謝我的指導老師 林祝興教授以及劉榮春老師，兩年來在學業上悉心指導，獲益良多，使我在學術研究的領域中有所成長。另外，也感謝口試委員們撥冗指正論文中錯誤與提供許多寶貴的意見，使本篇論文能更加完整。

在學期間也感謝實驗室學長姐仁傑、彥菱、佳男、君維與嘉仁關於研究和課業上給予很多建議與幫助；實驗室同學懋樺、掄元、衍緯、嘉瀚及亞太影印店的惠娟為我加油打氣與安慰；學弟妹們建廷、美君、志捷與宗哲在我沮喪時適時給予鼓勵與歡笑；謝謝你們。

研究生生涯使我成長許多，家人的鼓勵與支援是我最大的精神支柱，僅將此論文獻給我最敬愛的父親、母親、姐姐與姊夫，與所有關心我的親友們，以及永遠給我最大支持與陪伴我走過風風雨雨的欣珮。今日，終於完成碩士學位。在此，致上我最大的感謝與祝福予所有的師長、家人、朋友與學弟妹們，願目前本研究能對未來研究者有所裨益。

林育瑩　謹上 2008/7

東海大學碩士學位論文考試審定書

東海大學資訊工程與科學系 研究所

研究生 林 育 瑩 所提之論文

基於數位樣板的二元文件影像完整性保護技術

經本委員會審查，符合碩士學位論文標準。

學位考試委員會
召 集 人 _____ 簽章

委 員 _____

_____

_____

_____

指 導 教 授 _____ 簽章

中華民國 97 年 6 月 27 日

Contents

Figures

Tables

Chapter1
Introduction

Electronic documents published on the Internet are vulnerable to unsolicited modifications by unauthorized parties. In order to protect intellectual property rights and authenticate the originality of intellectual properties, a digital watermark is embedded in digital documents. Digital watermarking validates the integrity of multimedia documents. The multimedia content owner embeds watermarks in content before publishing. Legitimate users can then validate the integrity of the document and detect document tampering by extracting the embedded watermark and validating it.

However, it is more difficult to protect binary images of text documents than color or grayscale images. Text document images are often in binary black and white format and thus, there is less redundancy that can be exploited for embedding additional information. Consequently, to embed hidden information into a text document and then subsequently use it to verify the integrity of the document has become the focus of several studies [1-14].

Yang and Kot [9, 16] proposed a scheme for text document authentication based on watermarks. Their method defines three connectivity-preserving functions that define the “flippability” of a pixel. A blind data hiding technique is used to preserve the connectivity of pixels in a local neighborhood. Lin, Chou, and Chen [15] proposed an integrity protection method for text document by computing skeletons. Lin et al.’s method defines the all-black and all-white blocks to compute the skeletons of characters. In this thesis, we propose a strategy based on the black skeleton and the white, or inverse, skeleton of a binary document. Based on the idea of image thinning,

a novel method for protecting the integrity of text documents is proposed.

The strategy can be outlined as follows: First, two skeletons are computed by thinning, namely, obtaining the black skeleton (skeleton) and the white skeleton (inverse skeleton) of a document. Then the odd/even value is calculated for each image block and embedding locations are chosen. Next, by using a one-way hash function, a hash code is computed from the combination of the black and white skeletons. Next, an exclusive-OR operator is applied to the hash code and the watermark. The result of the above hash operation is then encrypted by using the verifier's public key, and following the encryption operation, the final result is embedded in the chosen embedding blocks.

If the document contents are altered, then the image topology, and hence the black and white image skeletons are also altered. A legitimate user can then validate the integrity of the document by extracting and verifying the watermark. Our experiments show that even very tiny alterations to the document result in blurry watermarks that are easy to detect.

The remainder of this thesis is organized as follows. Previous work is briefly reviewed in Chapter 2 and the Yang and Kot's text document authentication scheme is described in Chapter 3. The proposed method is described in Chapter 4. Experimental results and analysis of computational complexity of the method are presented in Chapter 5. Conclusions are made in Chapter 6.

Chapter 2
Preliminaries

In this chapter, we will discuss visible watermarking technology and invisible watermarking technology.

2.1 Visible watermarking

Visible digital watermarking technology shows embedded watermarks, that is, they can be seen by human eyes directly. The characteristic of visible watermark is that people can know directly who owns the intellectual property without further operations. The purpose of this kind of watermark is clear. It gives the information to the users straightforwardly, and the users directly recognize the source of information and the ownership. For example, visible watermark is shown on the paper bill, and TV stations show their company logos on the broadcasting images.

But this kind of watermark has two major shortcomings. First, it visually destroys the original image by declaring the information of ownership. Second, it is easy to tamper the watermark, that is, the visible watermark lacks security.

2.2 Invisible watermarking

Invisible watermarking technology include four classes of digital watermarking technologies: fragile watermarking technology, robust watermarking technology, spatial domain watermarking technology, and frequency domain watermarking technology.

Invisible watermarking technology is the mainstream of watermark study at present. This kind of watermark provides privacy and is difficult to be deleted. It can

be seen as one kind of information hidden technologies. Compared with the visible watermark, invisible watermark also shows characteristic of hidden information in addition to features applicable to intellectual property protection.

Seen on the application side, watermark technology can be divided as fragile watermarking and robust watermarking. Seen on the technological side, watermark technology can be divided as spatial domain watermarking and frequency domain watermarking. We discuss these watermarks in the following sections.

2.2.1 Fragile watermarking

Fragile watermarking technology is mainly used to verify the integrity of the stego image. If the stego image is altered by mistakes or from image attacks, the extracted watermark has miscellaneous or even fuzzy information. And then we can know the integrity of the stego image is somehow destroyed. Also by extracting watermark, we might be able to know the causes of mistakes or attacks. Some study utilizes fragile nature of this kind of watermark to examine the status of networks. By observing state of the embedded watermark after transmitted via the network, One can learn clearly whether the communication network at this moment is reliable or not.

2.2.2 Robust watermarking

Robust watermarking technology is used to embed the owner’s watermark in the host image to protect ownership. The embedded watermark needs to be able to resist various kinds of attacks, such as unintentionally destruction from compressing, communication mistakes taking place in the course of transmission, or hostile attacks trying to damage the image.

2.2.3 Spatial domain watermarking

This kind of watermark is embedded in the spatial domain. If the embedded information needs to be invisible, people will embed watermarks in parts that are not easily perceived by the human eye. To embed watermarks in the spatial domain, people slightly change the digital binary data of host image and embed the watermark information directly.

Advantages of the spatial watermark technology are that the embedding process is simple and fast, but large amount of information is allowed to be embedded in the host image. The drawbacks of this watermark technology are that it is vulnerable to geometric attacks and is easily destroyed by common digital signal processing operations, in other words, it is fragile. Fragile watermarking exploits this fragile characteristic of the spatial watermarks. By embedding watermark information in the spatial domain into document images, we can effectively verify the integrity of the document by retrieving and verifying the embedded watermark information.

2.2.4 Frequency domain watermarking

Frequency domain watermarking transforms data in the spatial domain to frequency domain before embedding watermarks in the host image. The watermark is embedded by revising the coefficient of host image, and this result from this embedding process is transform by an inverse transforming process to have stego image in the spatial domain.

Further, locations to embed the watermark depend on the kind of watermark application. Because the low and middle frequency ranges are more difficult to be destroyed, these frequency ranges are suitable for robust watermarking technology. The high frequency range is easier to be destroyed, thus this frequency range suits for fragile watermarking technology. There are several kinds of frequency band

transformations, for example, discrete wavelet transforms (DWT), discrete cosine transforms (DCT), and discrete Fourier transforms (DFT), etc.

Chapter 3
Yang and Kot's Text Document Authentication Scheme

Yang and Kot [9, 16] proposed a scheme for text document authentication through embedded watermarks. The method employs a blind data hiding technique that preserves the connectivity of pixels in a local neighborhood. A flippability decision method is used for finding pixels that possess the flippability property. Flippable pixels are used for embedding watermarks.

3.1 Flippability Decision

The flippability of a pixel depends on the transitions from the pixel to its eight neighbors in a 3×3 block. As shown in Figure 1, the eight neighbors of the central pixel $p(i, j)$ in a 3×3 block are namely w1, w2, w3, w4, w5, w6, w7, and w8.

(i-1, j-1) W_6	(i-1, j) W_7	(i-1, j+1) W_8
(i, j-1) W_5	(i, j) P	(i, j+1) W_1
(i+1, j-1) W_4	(i+1, j) W_3	(i+1, j+1) W_2

Figure 1 A 3×3 block and the flippability of the central pixel p

Yang and Kot' defined the following three connectivity-preserving functions.

$$N_{VHW} = \sum_{i=1,3} \overline{p} \cdot \overline{w}_i \cdot \overline{w}_{i+4} \; and \; N_{VHB} = \sum_{i=1,3} p \cdot w_i \cdot w_{i+4} \qquad (1)$$

$$N_{IR} = \sum_{i=1}^{4} \overline{p} \cdot w_{2i} \cdot \overline{w}_{2i-1} \cdot \overline{w}_{2i+1} \qquad (2)$$

$$N_C = \sum_{i=1}^{4} p \cdot w_{2i} \cdot w_{2i+1} \cdot w_{2i+2} \cdot w_{2i+3} \cdot w_{2i+4} \qquad (3)$$

Where NVHW and NVHB are the number of vertical and horizontal transitions, NIR is the number of interior right angle transitions and NC is the number of transitions from the center pixel to the sharp corners. The central pixel is flippable if these three values remain constant before and after flipping the central pixel. Moreover, a central pixel is also flippable if Equation (1) and Equation (2) remains constant, or if Equation (1) and Equation (3) remains constant. The central pixel P in such blocks is marked as an embeddable pixel, since the value of P can be flipped without changing the properties of the block.

3.2 Embeddable Blocks

The steps for choosing the embeddable blocks are summarized as follows.

Step 1 Partition the image into equal-size square blocks.

Step 2 Compute the flippability of the determined pixels according to the flippability criteria captured by Equations (1-3).

Step 3 Once a pixel is identified as “flippable,” the block is marked as “embeddable.” The current “flippable” pixel is identified as an “embeddable” pixel.

Step 4 Proceed to the next block.

Step 5 Repeat step 2 to step 4 until all of the blocks are processed.

3.3 Embedding Steps

Watermark embedding is performed as follows (see Figure 2).

Step 1 Find the "embeddable" locations using the procedure outlined in the previous paragraph.

Step 2 Generate an intermediate image Y_1 by setting all the "embeddable" pixels to zero.

Step 3 Compute a Hash value Ho from the intermediate image Y_1 using a hash function H(), namely $H_o = H(Y_1)$.

Step 4 Encrypt the hash value H_o using the private key K_s of the document owner to generate the content signature of the document $W_s = E_k(H_o, K_s)$, where E_k is an encryption algorithm.

Step 5 Perform XOR (Exclusive OR) or concatenation of W_s with the payload watermark W_p to generate the hard authenticator watermark W_r, e.g., $W_r = W_p \,||\, W_s$, where "||" is the concatenation operator.

Step 6 Embed W_r in the "embeddable" blocks according to whether there are an odd or even number of black or white pixels in the block.

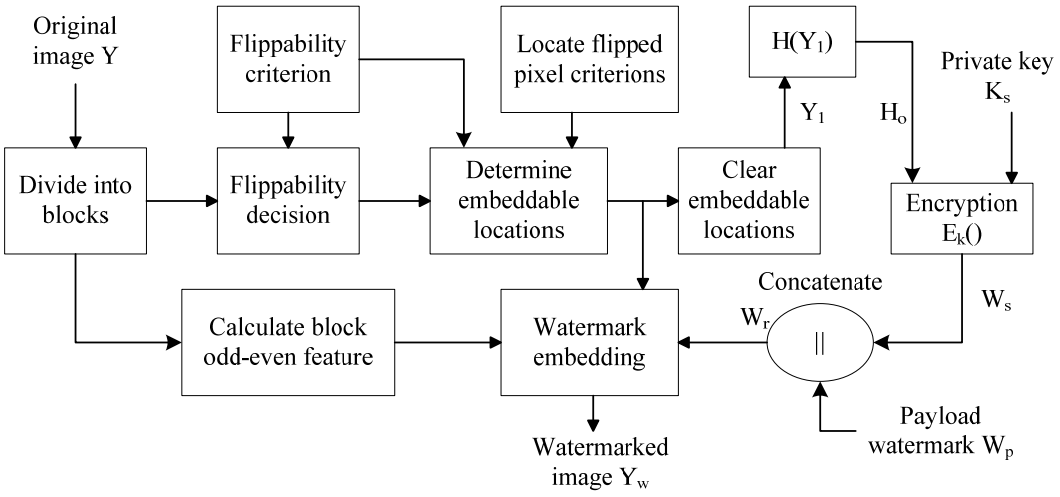


Figure 2 Yang and Kot's watermark embedding method

3.4 Authentication Steps

Authentication is performed as follows (see Figure 3).

Step 1 The first three steps are the same as for the embedding procedure, i.e., first the "embeddable" locations are found, the intermediate image Y_1' is generated and finally the hash value of the watermarked image H_w is computed.

Step 2 Extract the watermark W_r' based on the odd-even feature of the number of black or white pixels in the "embeddable" blocks, split it into two parts: the content signature W_s' and the payload watermark W_p'.

Step 3 Decrypt W_s' to obtain the hash value of the original image using the public key K_p, e.g., compute $H_o' = D_k(W_s', K_p)$, where D_k is the decryption algorithm.

Step 4 Compare W_p with W_p' and H_w with H_o'. If H_o' matches H_w and W_p' matches W_p, the authenticity and integrity of the image is confirmed.

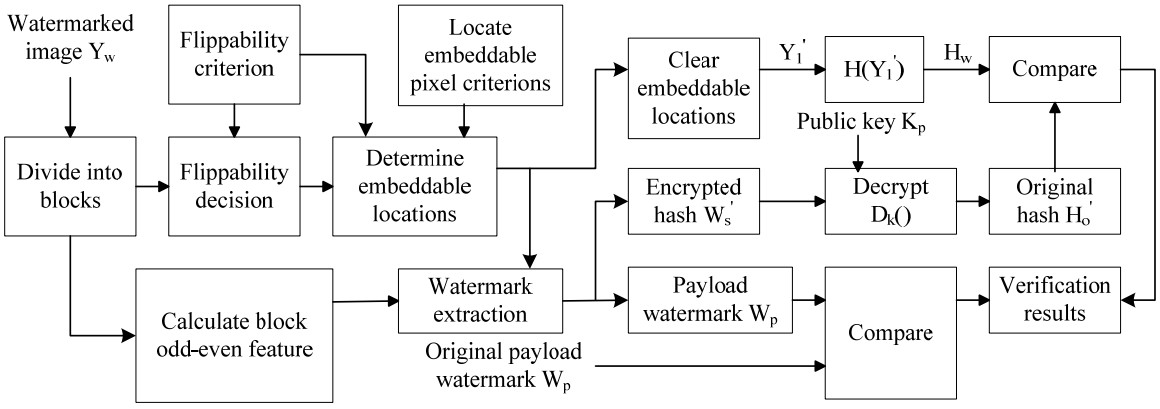


Figure 3 Yang and Kot's Authentication method

Chapter 4
Proposed Schemes

This chapter describes the proposed document protection scheme based on the image topology. The topology or skeleton of a document image is computed using image thinning. The watermark embedding and extracting procedures are identical to those proposed by Lu, Kot and Cheng [8].

4.1. Skeleton extraction

First, the document image skeletons must be computed and then the watermark embedded into the appropriate pixel locations. Zhang and Suen's algorithm [17] is used for extracting the black skeleton (skeleton) and the white skeleton (inverse skeleton) of a document. The thinning strategy is based on the two functions X(p) and B(p) for a square block, say of 3×3 pixels. In this block, shown in Figure 4, the central pixel p has eight neighbors. X(p) denotes the number of value changes, from 0 to 1, by scanning in the order of p1, p2 , p3,…, p8 (a clockwise scanning of pixels surrounding p). B(p) denotes the number of nonzero neighbors to p, that is, B(p)= p1+p2+p3…+p8. Note that 1s represent image object pixels and 0s represent image background pixels.

P_1	P_2	P_3
P_8	P	P_4
P_7	P_6	P_5

Figure 4 The central pixel p has eight neighbors

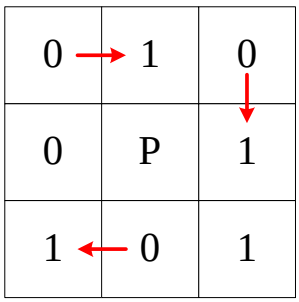


Figure 5 Shows an example where X(p)=3 and B(p)=4

Figure 5 shows an example where X(p)=3 and B(p)=4. Zhang and Suen's algorithm is iterative. The value of the current iteration depends on that of the previous iteration. It is computationally fast and simple to implement. For each iteration, the central pixel p in a 3×3 block of pixels is set to zero if its neighbors satisfy some conditions. By repeatedly applying the following two alternating steps with their indicated conditions, most of the pixels can be set to zero and the resulting image represents the image skeleton.

The first iteration	The second iteration
1. X(p) =1	1. X(p) =1
2. 2 <= B(p)<= 6	2. 2 <= B(p)<= 6
3. $p_2 * p_4 * p_6 = 0$	3. $p_2 * p_4 * p_8 = 0$
4. $p_4 * p_6 * p_8 = 0$	4. $p_2 * p_6 * p_8 = 0$

In the first iteration, illustrated in Figure 6, p4 must be zero, or p6 must be zero, or both p2 and p8 must be zero in order for both conditions 3 and 4 to be satisfied simultaneously. Similarly, in the second iteration, illustrated in Figure 7, p2 must be zero or p8 must be zero or both p4 and p6=0 must be zero for both conditions 3 and 4 to be satisfied simultaneously. Black pixels are used in Figures 6 and 7 to represent 1, white pixels indicate 0 and gray pixels indicate "don't care."

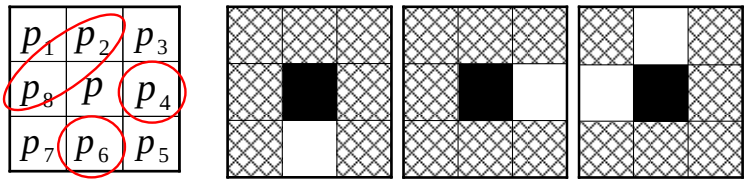


Figure 6 If p_4=0 or p_6=0 or (p_2=p_8=0) in the first iteration, then p can be removed

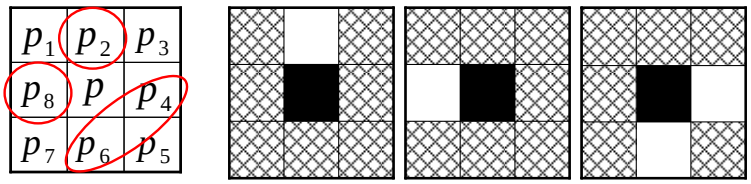
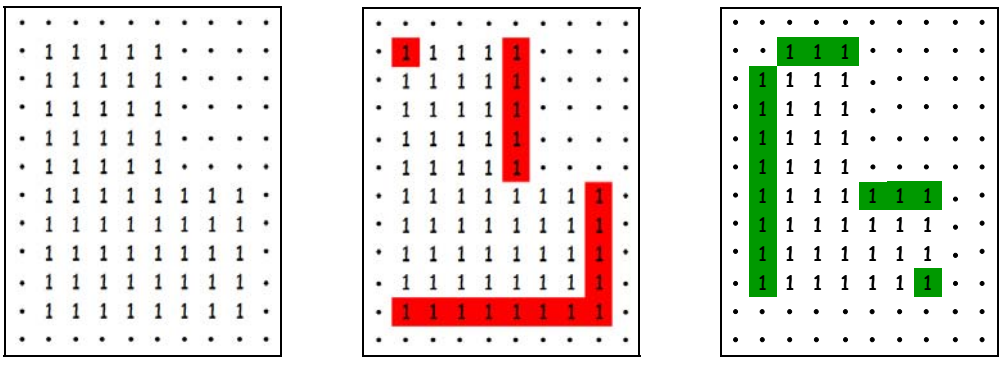
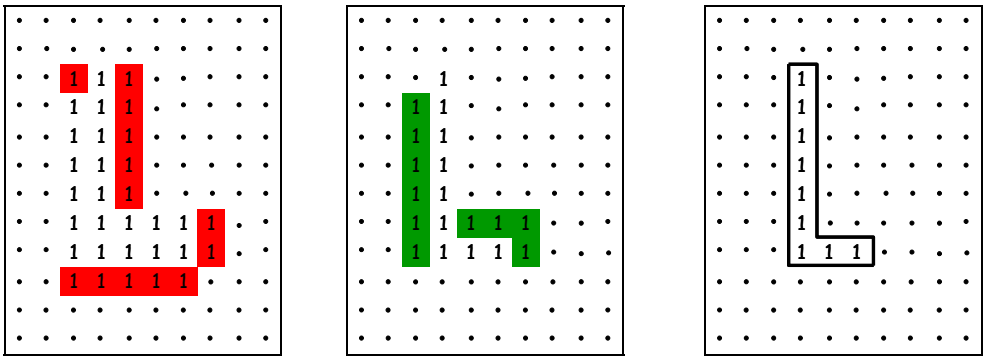


Figure 7 If p_2=0 or p_8=0 or (p_4=p_6=0) in the second iteration, then p can be removed

Figure 6 shows that pixel p can be set to zero (removed) if the 3×3 block satisfies the conditions for the first iteration. Similarly, Figure 7 shows that pixel p can be set to zero if the block satisfies the indicated conditions for the second iteration. Figure 8 illustrates a larger example: Figure 8-(a) shows the original image which is partitioned into 3×3 blocks of pixels where each block is processed individually. Figure 8-(b) highlights pixels set to zero after the first iteration. Figure-(c) highlights pixels set to zero after the second iteration. Next, Figures 8-(d) and 8-(e) show the effects of applying the first and second iterations again, respectively. Finally, Figure 8-(f) shows the result after the two alternating iterations have been repeatedly applied to the document image. The result is the skeleton of the original image.



(a) (b) (c)



(d) (e) (f)

Figure 8 (a) The original image (b) Pixels set to zero after the first iteration (c) Pixels set to zero after the second iteration (d) Pixels set to zero after repeating the first iteration (e) Pixels set to zero after repeating the first iteration (f) The image skeleton

The strategy presented herein relies on both the skeleton and the inverse skeleton being computed using the same method. The following pseudo code illustrates the procedure.

If p=1 && (2<=B(p)<=6) && X(p)=1
if(p_2 =0|| p_4 =0|| p_6 =0)&&(p_4 =0|| p_6 =0|| p_8 =0)
then set p=0
else
if(p_2 =0|| p_4 =0|| p_8 =0)&&(p_2 =0|| p_6 =0|| p_8 =0)
then set p=0

4.2. Watermark embedding process

This section describes the watermark embedding process (see Figure 9):

Input: Host document, watermark W_p, and verifier's public key K_P.

Output: The stego document (watermarked document).

Step 1 Compute the skeleton and the inverse skeleton of the document image with Zhang and Suen's algorithm.

Step 2 Combine the skeleton and the inverse skeleton to form a single skeleton

(combined skeleton).

Step 3 Generate the hash code IH of the single skeleton using a one-way hash function.

Step 4 Apply an exclusive-OR operation on the hash code and the watermark.

Step 5 Encrypt the result of the Step (4) using the verifier's public key to obtain the result IE, where $I_E = E_{K_p}(W_P \oplus I_H)$.

Step 6 Divide the cover document into blocks, and then calculate the odd/even value and choose the embeddable locations.

Step 7 Embed the information IE in the embeddable blocks.

Step 8 Output the stego document.

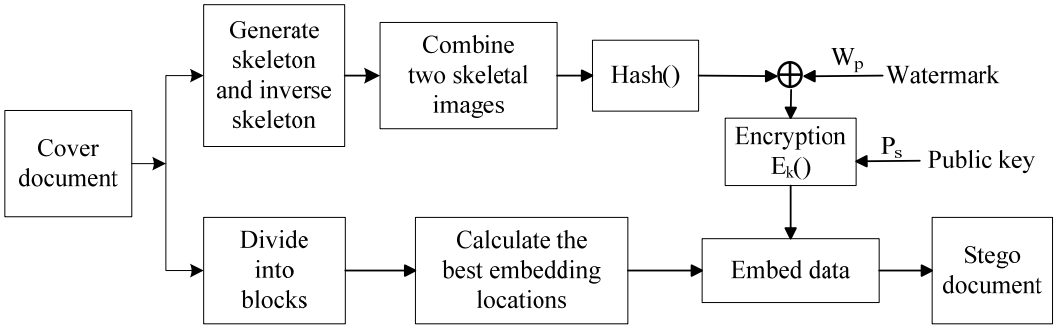


Figure 9 Watermark embedding process

If the number of black pixel in a block is odd, then a 1 is embedded. Otherwise, if the number of black pixel is even, then a 0 is embedded. All-black or all-white blocks are not used, as pixel changes in such blocks are visually perceivable.

Figure 10 shows an example of an odd block, i.e., it has 5 black pixels, and a 1 is therefore embedded by leaving the centre pixel white. However, a 0 is to be embedded then pixel P is changed from white to black such that the number of black pixels rise from 5 to 6, and becomes even.

Furthermore, the embeddable locations need to be found. Non-skeleton locations are defined as embeddable candidates. Figure 11 shows an example the embeddable candidates marked in gray.

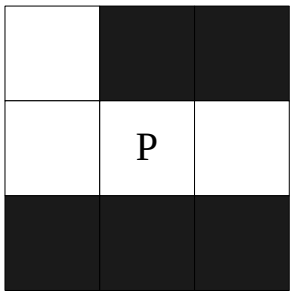


Figure 10 A one is coded by leaving the central pixel white in this block since it has an odd number of pixels (5)

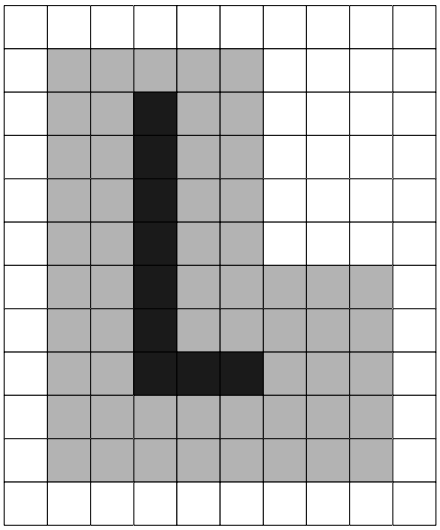


Figure 11 The gray area indicates the embeddable candidates

4.3. Authentication of Integrity

This section outlines the authentication process of the proposed scheme (see Figure 12).

Input: The stego document and the private key K_S of the verifier.

Output: The watermark.

Step 1 Generate the skeleton and the inverse skeleton using Zhang and Suen's algorithm.

Step 2 Combine the skeleton and the inverse skeleton into a single skeleton (combined skeleton).

Step 3 Compute a Hash value I'_H from the single skeleton.

Step 4 Divide the stego document into blocks and determine the embedding locations.

Step 5 Extract the embedded data.

Step 6 Decrypt the above data using the corresponding private key to obtain I'_E.

Step 7 The watermark is obtained by performing an exclusive-OR on the encrypted data I'_E and the hash code I'_H.

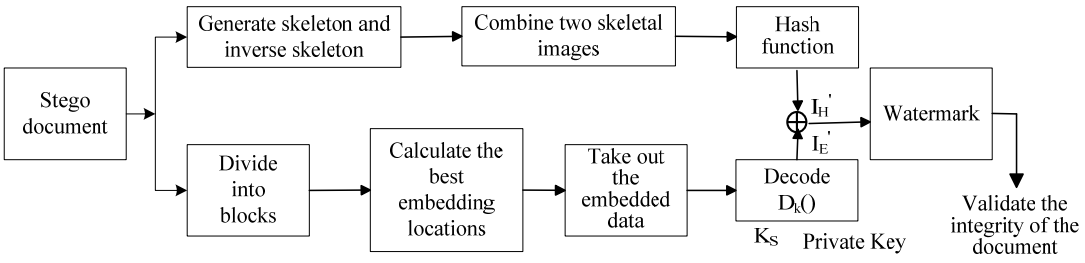


Figure 12 Integrity authentication process

Chapter 5
Experimental Results

The experimental evaluation was conducted using Windows XP with JBuilderX IDE, Java Advanced Imaging (JAI) package library and JDK 1.6.0. PhotoShop 8.0 was used for image tampering. Watermarks were embedded in both English-language and Chinese language documents, including both typed hand handwritten documents. A series of attacks were performed by adding black and white noise to the documents to test whether the alterations could be detected successfully.

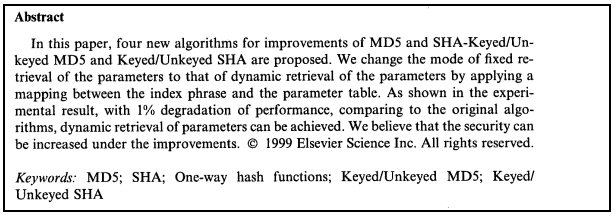
The experiments demonstrate that the proposed method is capable of effectively protecting the integrity of different classes of documents. The attacker is unable to obtain the embedded information. In addition, even single pixel document modifications are detected using the proposed strategy.

To ensure that the proposed scheme is promising, we conduct a series of experiments. As an example, we show some of the experimental results as follows. Figure 13 shows a host document image. Figure 14 shows the extracted black and white skeletons. Figure 15 shows the watermark to be embedded. Figure 16 is the stego document. (or watermarked document)

For attacking experiment, in Figure 18 we first do some changes to the stego document, e.g., add a noise point to the character “k”. In the verification stage, we found that the extracted watermark has been blurred seriously, shown in Figure 19. Further, Figure 20 and Figure 22 show changes of a character, respectively. Figure 21 and Figure 23 show the result of deleting some characters.

We also do experiments on non-textual documents. We transform *Lena* to binary image, as shown in Figure 24. Figure 25 is the stego image. Figure 26 shows the

changes made on the area of the eyes. We see the extracted watermark has been blurred seriously from Figure 27.

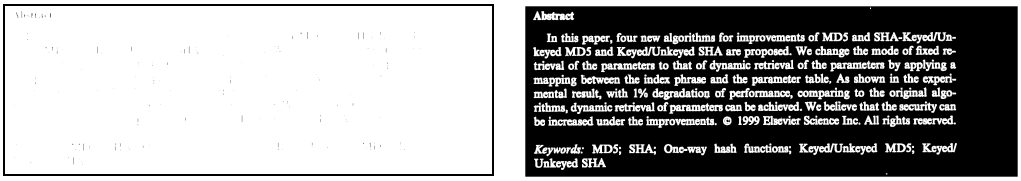


Abstract

In this paper, four new algorithms for improvements of MD5 and SHA-Keyed/Unkeyed MD5 and Keyed/Unkeyed SHA are proposed. We change the mode of fixed retrieval of the parameters to that of dynamic retrieval of the parameters by applying a mapping between the index phrase and the parameter table. As shown in the experimental result, with 1% degradation of performance, comparing to the original algorithms, dynamic retrieval of parameters can be achieved. We believe that the security can be increased under the improvements. © 1999 Elsevier Science Inc. All rights reserved.

Keywords: MD5; SHA; One-way hash functions; Keyed/Unkeyed MD5; Keyed/Unkeyed SHA

Figure 13 Host document



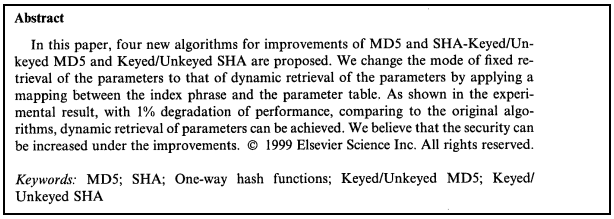
Abstract

In this paper, four new algorithms for improvements of MD5 and SHA-Keyed/Unkeyed MD5 and Keyed/Unkeyed SHA are proposed. We change the mode of fixed retrieval of the parameters to that of dynamic retrieval of the parameters by applying a mapping between the index phrase and the parameter table. As shown in the experimental result, with 1% degradation of performance, comparing to the original algorithms, dynamic retrieval of parameters can be achieved. We believe that the security can be increased under the improvements. © 1999 Elsevier Science Inc. All rights reserved.

Keywords: MD5; SHA; One-way hash functions; Keyed/Unkeyed MD5; Keyed/Unkeyed SHA

Figure 14 The black (lift) and white (right) skeletons

Figure 15 The watermark



Abstract

In this paper, four new algorithms for improvements of MD5 and SHA-Keyed/Unkeyed MD5 and Keyed/Unkeyed SHA are proposed. We change the mode of fixed retrieval of the parameters to that of dynamic retrieval of the parameters by applying a mapping between the index phrase and the parameter table. As shown in the experimental result, with 1% degradation of performance, comparing to the original algorithms, dynamic retrieval of parameters can be achieved. We believe that the security can be increased under the improvements. © 1999 Elsevier Science Inc. All rights reserved.

Keywords: MD5; SHA; One-way hash functions; Keyed/Unkeyed MD5; Keyed/Unkeyed SHA

Figure 16 The stego document of Figure 13

Figure 17 The extracted watermark of Figure 16

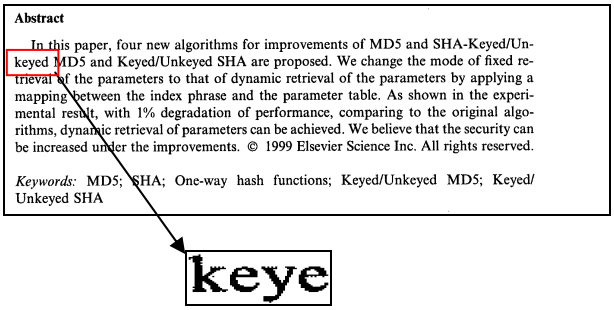


Figure 18 Adding noise point to the host document

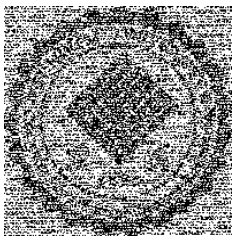


Figure 19 The extracted watermark from Figure 18

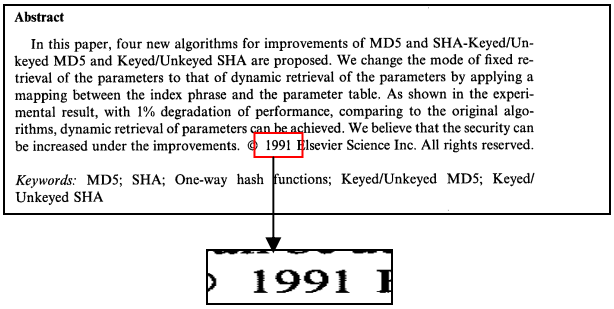


Figure 20 The word "1999" is changed to "1991"

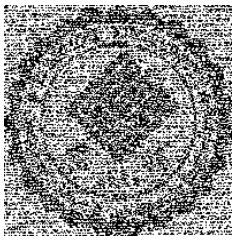


Figure 21 The extracted watermark from Figure 20

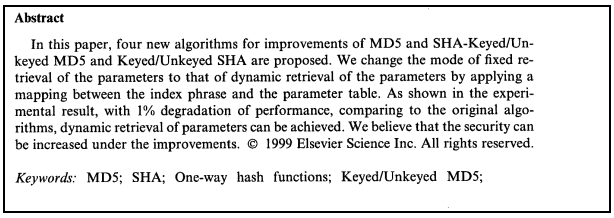


Figure 22 The "keyed/Unkeyed SHA" is cropped

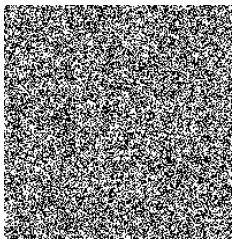


Figure 23 The extracted watermark from Figure 22

Figure 24 The host image

Figure 25 The stego image

Figure 26 Host image (Left) and eyes are changed (Right)

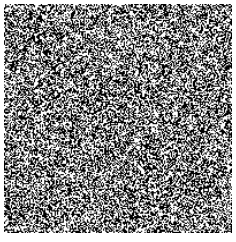


Figure 27 The extracted watermark from Figure 26

Figure 28 shows the experimental results obtained for English documents. Figure 28-(a) shows the document image. Figure 28-(b) shows the embedded watermark. Figure 28-(c) shows the extracted skeleton and the inverse skeleton, respectively. Figure 28-(d) shows the stego-document (watermarked document.) The watermark is significantly affected by flipping just one single pixel in the stego-document. Figure 28-(e) and Figure 28-(f) show the two extracted watermark when a black and a white pixel in the skeleton part of the image are flipped, respectively. Both watermarks are noticeably blurred and the effect is visible to the naked eye. Moreover, by flipping one black pixel and one white pixel simultaneously the resulting watermark is completely unrecognizable.

It is natural to expect that changes to the skeleton part of the image are detected since these parts are used to compute the hash value. However, imagine that the attacker knows the method and decide to attack the non-skeleton part of the image. To simulate such attacks a pixel is flipped in a non-skeleton part of the image. The results demonstrate that the method is able to withstand these attacks effectively. There are four situations:

(1) A flipped pixel in the non-skeleton part that influences both of the skeleton and the inverse skeleton will completely destroy the extracted watermark as shown in Figure 28-(h).

(2) A flipped pixel in the non-skeleton part that influences the skeleton blurs the extracted watermark as shown in Figure 28-(i).

(3) Similarly, a flipped pixel in the non-skeleton part that influences the inverse skeleton blurs the extracted watermark as shown in Figure 28-(j).

(4) Two contiguous pixels flipped in the non-skeleton part must influence either the skeleton or the inverse skeleton and blur the extracted watermark as shown in Figure 28-(k). The change of two consecutive pixels could represent the insertion or removal

of a full stop symbol. The full stop is the smallest printable character and it occupies two contiguous pixels in some resolutions.

However, it is not easy to locate a single flipped pixel in the non-skeleton part of the image that does not affect either the skeleton or the inverse skeleton. However, it is not meaningful to just change a single pixel in a document. The simultaneous change of two pixels are more realistic as a full stop is represented with 2 pixels in font size 12 and 4 pixels in font size 14 for very low resolution images (shown in Figure 29-(a) and 29-(b)). Furthermore, a full stop is the smallest printable character that it would be meaningful to change. The experiments show that the addition, or removal, of a full stop character influences either the skeleton, or the inverse skeleton. Consequently, the extracted watermark becomes blurred.

Furthermore, a series of attacks on Chinese printed document and handwritten documents were performed. Figure 30 shows the experimental results for Chinese documents. Figure 30-(a) shows the 365×365 pixel cover document, Figure 30-(b) shows the watermark, and Figure 30-(c) shows the skeleton (left) and the inverse skeleton (right), respectively. Figure 30-(d) shows the stego document before tampering (left) and the extracted watermark (right) and Figure 30-(e) shows the result after adding one black pixel in the inverse skeleton (left) and the blurred extracted watermark (right). Similarly, Figure 30-(f) shows the result of adding one white pixel in the skeleton (left) and the resulting blurred watermark (right). By simultaneously adding one white pixel in the skeleton and one black pixel in the inverse skeleton (left) then the extracted watermark becomes completely blurred (right) as shown in Figure 30-(g). Similarly, Figure 30-(h) shows that if a noisy pixel is added in the non-skeleton part such that it affects the inverse skeleton and the skeletons then the extracted watermark is completely destroyed. Figure 30-(i) shows that if a noisy pixel is added in the non-skeleton part of the image that influences the

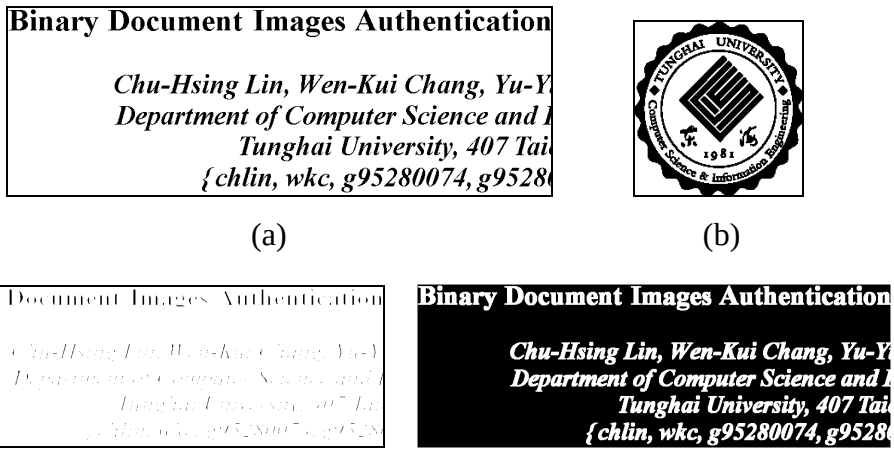
skeleton, then the extracted watermark is blurred. Similarly, Figure 30-(j) shows that if a noisy pixel is added in the non-skeleton part that affects the inverse skeleton, then the extracted watermark becomes blurred. Figure 30-(k) demonstrates that if two contiguous pixels are changed in the non-skeleton part, it affects either the skeleton or the inverse skeleton and the extracted watermark becomes blurred.

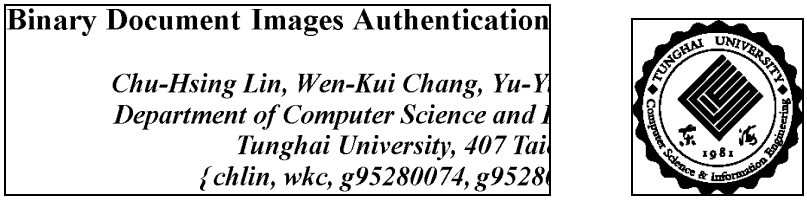
Figure 31 shows experimental results for handwritten documents and the findings are consistent with those found for the typed English and Chinese documents.

The results are summarized in Table 1 which lists Pearson's correlation coefficients between the original watermark (W) and the extracted watermark (W').when the document images are subjected to various attacks. The following definition was used:

$$Corr(W,W') = \frac{\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}(W_{(i,j)} - \overline{W})(W'_{(i,j)} - \overline{W'})}{\sqrt{\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}(W_{(i,j)} - \overline{W})^2}\sqrt{\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}(W'_{(i,j)} - \overline{W'})^2}} \qquad (4)$$

Where $\overline{W}$ and $\overline{W'}$ are the average pixel values of the original watermark and of the extracted watermark. The correlation coefficient ranges from -1 to 1. A value of 1 indicates that a linear equation describes the relationship perfectly and positively; a value of 0 indicates no correlation; and -1 signals perfect negative correlation.




Binary Document Images Authentication
Chu-Hsing Lin, Wen-Kui Chang, Yu-Y
Department of Computer Science and I
Tunghai University, 407 Tai
{chlin, wkc, g95280074, g9528

(d)


Binary Document Images Authentication
Chu-Hsing Lin, Wen-Kui Chang, Yu-Y
Department of Computer Science and I
Tunghai University, 407 Tai
{chlin, wkc, g95280074, g9528

(e)


Binary Document Images Authentication
Chu-Hsing Lin, Wen-Kui Chang, Yu-Y
Department of Computer Science and I
Tunghai University, 407 Tai
{chlin, wkc, g95280074, g9528

(f)


Binary Document Images Authentication
Chu-Hsing Lin, Wen-Kui Chang, Yu-Y
Department of Computer Science and I
Tunghai University, 407 Tai
{chlin, wkc, g95280074, g9528

(g)


Binary Document Images Authentication
Chu-Hsing Lin, Wen-Kui Chang, Yu-Y
Department of Computer Science and I
Tunghai University, 407 Tai
{chlin, wkc, g95280074, g9528

(h)


Binary Document Images Authentication
Chu-Hsing Lin, Wen-Kui Chang, Yu-Y
Department of Computer Science and I
Tunghai University, 407 Tai
{chlin, wkc, g95280074, g9528

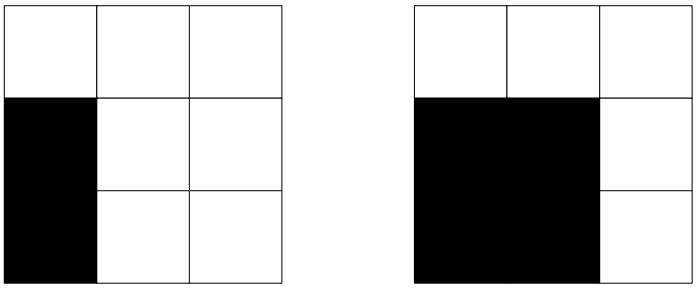
(i)


Binary Document Images Authentication
Chu-Hsing Lin, Wen-Kui Chang, Yu-Y
Department of Computer Science and I
Tunghai University, 407 Tai
{chlin, wkc, g95280074, g9528

(j)

(k)

Figure 28 Attacks experiment on a 911 × 315 pixels typed English document (a) Document image, (b) Watermark, (c) The skeleton (left) and the inverse skeleton (right), (d) Stego document (left) and the extracted watermark (right), (e) Black pixel in white skeleton attack (left) and the extracted watermark (right), (f) White pixel in black skeleton attack (left) and the extracted watermark (right), (g) A white and a black pixel in the skeleton attack (left) and the extracted watermark (right), (h) A noisy pixel in the non-skeleton part that affects the skeleton and the inverse skeleton (left) and the extracted watermark (right), (i) A noisy pixel in the non-skeleton part that affects the skeleton (left) and the extracted watermark (right), (j) A noisy pixel in the non-skeleton part that affects the inverse skeleton (left) and the extracted watermark (right), (k) Two contiguous pixels in the non-skeleton part that affects the skeleton or the inverse skeleton (left), and the extracted watermark (right).



(a) (b)

Figure 29 (a) A full stop can be represented using 2 pixels in font size 12 (b) And with 4 pixels in font size 14.

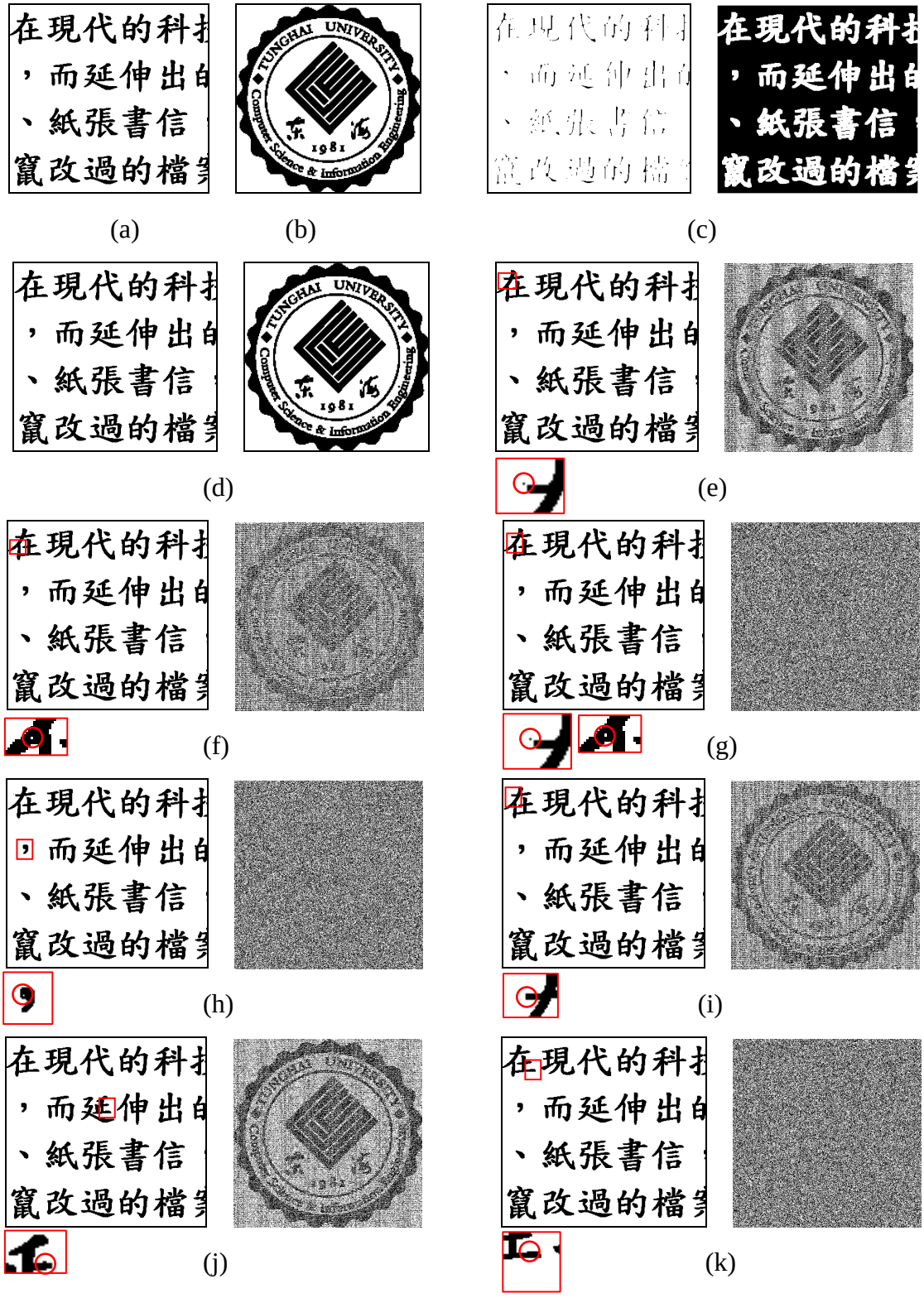
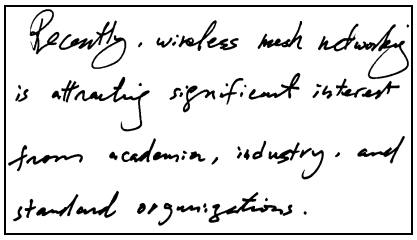
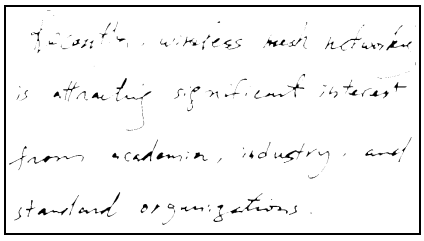


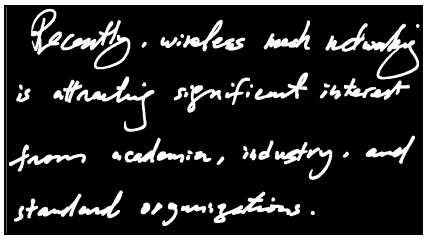
Figure 30 Attack experiment on a 365×365 pixels typed Chinese document(a) Document image, (b) Watermark, (c) The skeleton (left) and the inverse skeleton (right), (d) Stego document (left) and the extracted watermark (right), (e) Black pixel in white skeleton attack (left) and the extracted watermark (right), (f) White pixel in

black skeleton attack (left) and the extracted watermark (right), (g) A white and a black pixel in the skeleton attack (left) and the extracted watermark (right), (h) A noisy pixel in the non-skeleton part that affects the skeleton and the inverse skeleton (left) and the extracted watermark (right), (i) A noisy pixel in the non-skeleton part that affects the skeleton (left) and the extracted watermark (right), (j) A noisy pixel in the non-skeleton part that affects the inverse skeleton (left) and the extracted watermark (right), (k) Two contiguous pixels in the non-skeleton part that affects the skeleton or the inverse skeleton (left), and the extracted watermark (right).

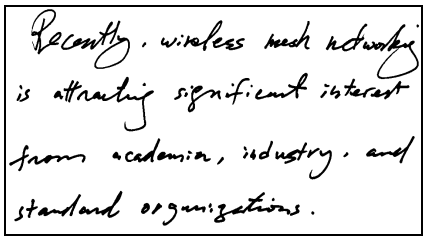


(a) (b)

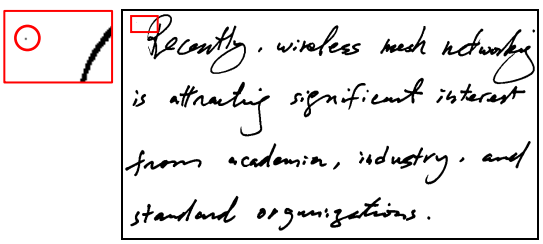


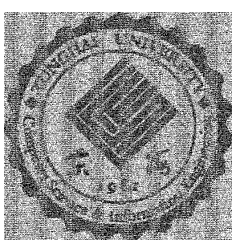


(c)

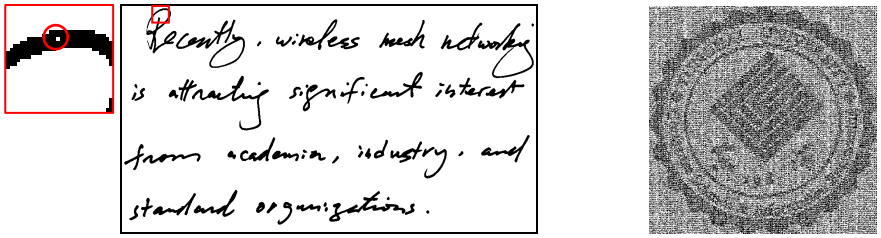


(d)

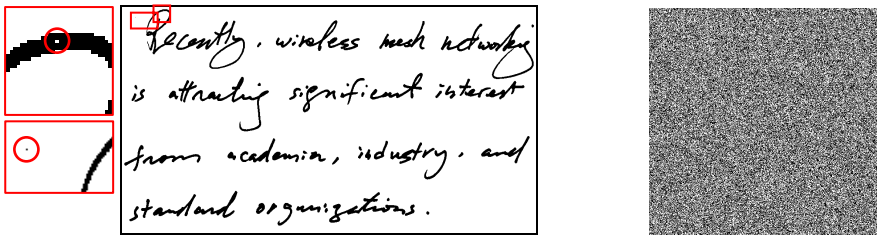




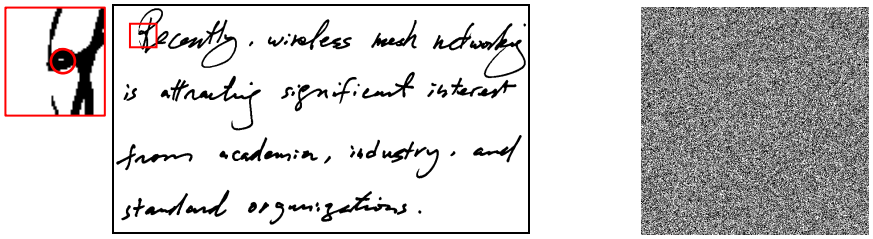
(e)


Recently, wireless mesh networking
is attracting significant interest
from academia, industry, and
standard organizations.

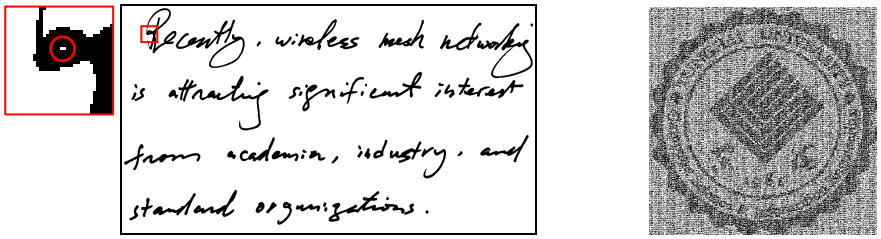
(f)


Recently, wireless mesh networking
is attracting significant interest
from academia, industry, and
standard organizations.

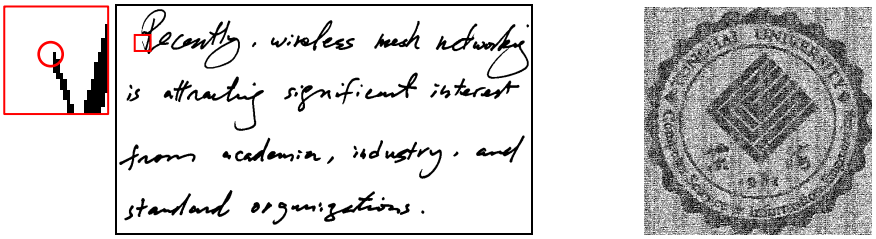
(g)


Recently, wireless mesh networking
is attracting significant interest
from academia, industry, and
standard organizations.

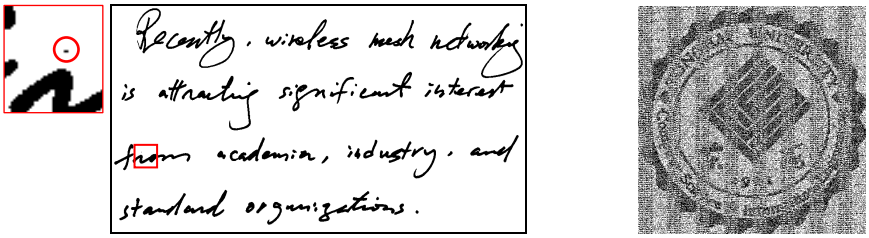
(h)


Recently, wireless mesh networking
is attracting significant interest
from academia, industry, and
standard organizations.

(i)


Recently, wireless mesh networking
is attracting significant interest
from academia, industry, and
standard organizations.

(j)



(k)

Figure 31 Attacks experiment on an 1125×624 pixels typed handwritten document(a) Document image, (b) Watermark, (c) The skeleton (left) and the inverse skeleton (right), (d) Stego document (left) and the extracted watermark (right), (e) Black pixel in white skeleton attack (left) and the extracted watermark (right), (f) White pixel in black skeleton attack (left) and the extracted watermark (right), (g) A white and a black pixel in the skeleton attack (left) and the extracted watermark (right), (h) A noisy pixel in the non-skeleton part that affects the skeleton and the inverse skeleton (left) and the extracted watermark (right), (i) A noisy pixel in the non-skeleton part that affects the skeleton (left) and the extracted watermark (right), (j) A noisy pixel in the non-skeleton part that affects the inverse skeleton (left) and the extracted watermark (right), (k) Two contiguous pixels in the non-skeleton part that affects the skeleton or the inverse skeleton (left), and the extracted watermark (right).

Table 1 Pearson's correlation coefficient of attacks on various documents

Attacks		English	Chinese	Handwritten
Add one black pixel in the inverse skeleton		0.274	0.261	0.298
Add one white pixel in the skeleton		0.226	0.146	0.201
Change one pixel in both the skeleton and the inverse skeleton simultaneously		0	0.003	0.001
Add one noise pixel in the non-skeleton part and that would:	Influence both the skeleton and the inverse skeleton	0.002	0	-0.003
	Influence only the skeleton	0.183	0.183	0.233
	Influence only the inverse skeleton	0.283	0.330	0.303
Add two contiguous pixels and that affects either the skeleton or the inverse skeleton		0.316	0.003	0.254

Computational Complexity

The computational complexities of the components of the method are summarized in Table 2 together with the complexity of Yang and Kot method for reference. The computation of X(p) involves 8 logical ANDs. Furthermore, 7 additions are needed to compute B(p). Next, the two iterations comprise 16 logical AND operators. The calculation of odd and evenness has a time complexity of O(M×N) where M and N denotes the width and height of the document image. Nx×Ny is the total number of blocks and Nd is the determined pixels per block, e.g., Nd = 1 for a 3×3 block. Clearly, the proposed method has a lower time-complexity than the method proposed by Yang and Kot.

Table 2 Comparisons of computation cost

Method	Operations	Required Computations
The Proposed Method	Generate skeleton	(M-2)×(N-2)×7 addition
		(M-2)×(N-2)×24 AND
	Calculate odd-even feature	M×N Increment
Yang and Kot's Method	Calculate transitions	Nx×Ny×Nd×24 AND
		Nx×Ny×Nd×12 NOT
		Nx×Ny×Nd×24 addition
	Calculate odd-even feature	M×N Increment

Comparisons of Embeddable blocks

As to binary document image, some image may not have locations that satisfy flippability decision. But every binary document images can utilize thinning to obtain skeletons. So the part of non-skeleton by using flippability decision may be still the embeddable blocks in our method. The proposed method can use in each binary document image, but the Yang and Kot's method can not.

Chapter 6
Conclusions

This paper presents a novel method for protecting the integrity of binary documents. By computing the skeleton and the inverse skeleton and using a watermark, the integrity of a document can be effectively protected. Experimental evaluations confirm that even a small change made to a document is easily detected visually from the extracted watermark. However, an attacker familiar with the method may try to attack the non-skeleton part of the document since the non-skeleton parts are not used for computing the hash code. Four possible types of non-skeleton part attacks are therefore examined experimentally and the method successfully detects tampering in these situations too. The computational complexity of the strategy is lower than previous strategies and the parallel nature of the thinning algorithm allows for fast hardware implementations. Finally, a balance must be struck in terms of block size. If the block size is too large, there may be too few skeletons and inverse skeletons to use for coding information. On the contrary, if the block size is too small, there are more skeletons to process.

Chapter 7
Future works

Nowadays ever-increasing amount of data are transmitted through the Internet, and they are in danger of being tampered. So protection of the integrity of the data becomes very important. At present, few methods have been described that successfully address important issues of file verification, and detection of document tampering.

In this thesis, we propose a method to authentication the integrity of binary document image. The experiment shows that even very small alterations to the document result in blurry watermarks that are easy to detect. But we can not recover the stego image any more. So in the future, in addition to detecting tampering of binary document, we need a method to protect and recover binary document images from tampering. And this study will be more completed.

Bibliography

[1] Takaaki Yamada, Yasuhiro Fujii, Islao Echizen, Kouichi Tanimoto and Satoru Tezuka, “Print Traceability Systems Framework using Digital Watermarks: for Binary Images,” *2004 IEEE international Conference on Systems*, Man and Cybernetics, Vol. 4, Oct. 2004, pp.3285-3290.

[2] Y. U. Chao and Xudong Zhang, “Watermark Embedding in Binary Image for Authentication,” *The Seventh International Conference on Signal Processing (ICSP'04)*, Vol. 1, Sept. 2004, pp.865-868.

[3] C. E. Zhang and Z. D. Qiu, “Fragile Watermarking with Quality Control for Binary Images,” *Proceedings of 2005 International Conference on Machine Learning and Cybernetics*, Vol. 8, Aug. 2005, pp.4952-4956.

[4] Y. C. Tseng, Y. Y. Chen and H. K. Pan, “A Secure Data Hiding Scheme for Binary Images,” *IEEE Trans. on Communications*, vol. 50, no. 8, Aug. 2002, pp.1227-1231.

[5] H. Y. Kim and R. L. Queiroz, “A Public-Key Authentication Watermarking for Binary Images”, *Proceedings IEEE International Conference on Image Processing*, Singapore, 2004, pp.3459-3462.

[6] H. Y. Kim and R. L. de Queiroz, “Alteration-Locating Authentication Watermarking for Binary Images,” *2004 International Workshop on Digital Watermarking*, Seoul Korea, LNCS Vol. 3304, 2004, pp.125-136.

[7] H. Y. Kim, “A New Public-Key Authentication Watermarking for Binary Document Images Resistant to Attacks,” *IEEE International Conference on Image Processing (ICIP 2005)*, Genoa, Italy, Vol. 2, Sept. 2005,pp.II-1074-7.

[8] H. Lu, A. C. Kot and J. Cheng, “Secure Data Hiding in Binary Document Images for Authentication,” *Proceedings of the 2003 International Symposium on*

Circuits and Systems, Bangkok, Thailand, Vol. 3, May 2003, pp.806-809.

[9] H. Yang and A. C. Kot, "Data Hiding for Text Document Image Authentication by Connectivity-Preserving," *Proceedings of the IEEE International Conference on Acoustics*, Speech, and Signal Processing 2005, Philadelphia, PA, USA, Vol. 2, March 18-23, pp.505-508.

[10] M. Wu, E. Tang and B. Liu, "Data Hiding in Digital Binary Image," *Proceedings IEEE International Conference on Multimedia and Expo*., New York, 2000, pp.393-396.

[11] P. W. Wong and N. D. Memon, "Secret and Public Key Image Watermarking Schemes for Image Authentication and Ownership Verification," *IEEE Transactions on Image Processing*, Vol. 10, No. 10, Oct. 2001, pp.1593-1601.

[12] H. Yang and A. C. Kot, "Data Hiding for Bi-level Documents using Smoothing Techniques," *Proceedings IEEE International Symposium on Circuits Systems (ISCAS'04)*, May 2004, Vol. 5, pp.692-695.

[13] Q. Mei, E. K. Wong and N. Memon, "Data Hiding in Binary Text Document," Proceedings, Vol. 4314, SPIE, 2001, pp.369-375.

[14] C. H. Lin, W. K. Chang, Y. Y. Lin and L. Y. Cheng, "Binary Document Images Authentication by Thinning Digital Patterns," *The Third International Conference on Intelligent Information Hiding and Multimedia Signal*, Kaohsiung, Taiwan, Vol.26-28, Nov, 2007, pp.485-488.

[15] C. H. Lin, J. S. Chou and Y. W. Chen, "Integrity Protection of Document Assets by Computing Skeletons," *The Second International Conference on Innovative Computing, Information and Control (ICICIC 2007)*, Kumamoto, Japan, Sept. 2007, pp.285-285 .

[16] H. Yang and A. C. Kot, "Pattern-Based Data Hiding for Binary Image Authentication by Connectivity-Preserving," *IEEE Transactions on Multimedia*,

Vol. 9, No. 3, April 2007, pp.475-486.

[17] T. Y. Zhang and C. Y. Suen, “A Fast Parallel Algorithm for Thinning Digital Patterns,” *Communications of the ACM*, March 1984, pp.236-239.

[18] M. Wu and B. Liu, “Data Hiding in Binary Image for Authentication and Annotation,” *IEEE Transactions on Multimedia*, Vol. 6, No 4, Aug. 2004, pp.528-538.

[19] M. A. Qadir and I. Ahmad, “Digital Text Watermarking: Secure Content Delivery and Data Hiding in Digital Documents,” *Aerospace and Electronic Systems Magazine*, Issue 11, Vol. 21, Nov. 2006, pp.18-21.

[20] M. A. Qadir and I. Ahmad, “Digital Text Watermarking: Secure Content Delivery and Data Hiding in Digital Documents,” Security Technology, 2005. *CCST '05. 39th Annual 2005 International Carnahan Conference* on Oct. 2005, pp.101-104.

[21] Y. Fu and T. S. Huang, "Image Classification Using Correlation Tensor Analysis," *IEEE Transactions on Image Processing (TIP)*, Vol. 17, No. 2, Feb. 2008, pp.226-234.