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

Lien-Yi Weng (翁連奕)[1] and Wen-Hsiang Tsai (蔡文祥)[1, 2]
[1]Department of Computer & Information Science
National Chiao Tung University, Hsinchu, Taiwan 300
[2]Department of Computer Science & Information Engineering
Asia University, Taichung, Taiwan 413
E-mails: gis92534, whtsai@cis.ncu.edu.tw

Abstract

A method for authentication of grayscale document images against print-and-scan attacks by a semi-fragile watermarking technique is proposed. A line, taken as a fragile authentication signal, is embedded in each character or word block in a grayscale document image to create a stego-image. The line is embedded at a best position in the block which arouses the least visual awareness. During the authentication process, the authentication signals are extracted by a line fitting technique to acquire the embedded line in each block of a stego-image in suspicion. The integrity of the document images can be verified by comparing the difference between the embedded authentication signals and the extracted ones. Security of the authentication signals is improved by the use of a key in determining the slope of each embedded line. Experimental results show the feasibility of the proposed approach.

Keywords: digital watermarking, image authentication, document image, copyright protection, print-and-scan operations.

1. Introduction

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

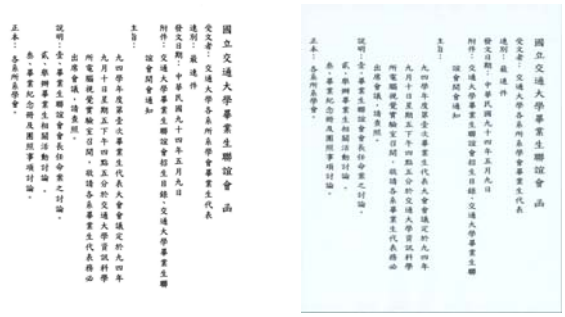
Digital watermarking is a technique which may be used to embed a watermark into an image to protect the owner's copyright of the image or to authenticate the image (i.e., to check the integrity or fidelity of the image). A watermarked image is also called a stego-image. The watermark signals must be robust against print-and-scan operations, that is, it is hoped that after applying such operations on a stego-image, the embedded watermark signals still can be detected and extracted. Some researches about watermarking techniques for copyright protection against print and scan attacks have been proposed in recent years. In [1-2], a watermark is embedded in a ring in the discrete Fourier transform domain. Lefebvre et al. [3] proposed a method, which combines an additive watermarking algorithm in the spatial domain and a synchronization template in the Fourier domain.

The definition of print-and-scan operation is to print a digital image and rescan the result to become another digital version. Because of the rapid development of electronic products, printers and scanners are commonly used for distributions and reproductions of documents. It is popular to transform an image between the digital format and the printed copy. Some distortions may occur during the transformation; therefore, for copyright protection and integrity checking, it is necessary to design a scheme to solve this problem. It means that print-and-scan operations are regarded as normal behaviors to process an image, and they cannot be considered as tampering operations, but we still want to be sure whether the image resulting from rescanning is genuine in every part, i.e., to be sure of the integrity of the image. On the other hand, illegal users might attempt to eliminate the digital watermark embedded behind a digital image by print-and-scan attacks, hoping that no watermark will ever exist in the rescanning result. So an authentication scheme with a certain degree of robustness against print-and-scan operations is desirable.

After an image suffers from print-and-scan operations, two types of distortions will emerge in the reproduced version, namely geometric transformations and pixel value distortions. Geometric transformations include translation, rotation, cropping, scaling, etc. And distortions of pixel values are caused by (1) luminance, contrast, gamma correction, and chrominance variations; (2) blurring of neighboring pixels; and so on. These are typical effects of printers and scanners, but they affect the visual quality of a reproduced image [4]. Figure 1 shows an image and a reproduced version of it. In this study, we deal mainly with grayscale document images.

The remainder of this paper is organized as follows. In Section 2, the idea of the proposed method of image authentication against the print-and-scan operation is briefly described. In Section 3, the process

of embedding authentication signals is introduced. Section 4 includes a description of the process of authentication signal extraction. And in Section 5, some experimental results are given to show the feasibility of the proposed method. Finally, in Section 6, some discussions and a summary are made.



(a) (b)

Fig. 1 A grayscale document image and a reproduced image with degraded quality. (a) Chinese document image. (b) Reproduced image of (a) with quality of 100 dpi.

2. Idea of Proposed Method for Authentication

In the proposed procedure of authentication signal embedding, a document image is first divided into non-overlapping blocks. Different from processing an image in the unit of fixed-sized pixel block, we take a character or word as a basic block by after segmenting the document image into such blocks by a connected component merging technique. Second, we embed in each block a line as a semi-fragile watermark by decreasing the gray values of the pixels in the block. In order to enhance the security of authentication, the coefficients of the line equation are created by the use of a secrete key and an reduced halftone gray (RHG) value, which, as defined in [6], is used to assign a gray value G to a binary image block.

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

3. Authentication Signal Embedding

3.1 Pre-processing stage

There are two stages in the procedure of authentication signal embedding, namely, (1) preprocessing; and (2) authentication signal generation and embedding.

A. Bi-level thresholding

The first step in the pre-processing stage is to remove noise and distortion. For this, we apply bi-level thresholding to increase the effectiveness of a region growing technique applied later for image segmentation. We set a threshold value to partition the 256 gray values into 2 pixel values, 0 and 255, and the corresponding pixels are called black and white ones, respectively.

B. Division of image into blocks by region growing

If we process an image in terms of blocks of a fixed size, the blocks will be changed after the image suffers from scaling, shrinking, or other attacks. So, it is not suitable to utilize fixed-sized blocks to process an image against scaling. Instead, we utilize the region growing technique in the data embedding and extraction processes to determine the size of each block, so that the blocks segmented out in the data embedding process will have no difference from those segmented out in the data extraction processes, achieving the goal of processing the same set of image blocks in the two processes. Region growing is a procedure that groups pixels or subregions into large regions based on predefined criteria. The basic concept is to start with a set of "seed" points and from them grow regions by appending to each seed those neighboring pixels that have properties similar to the seed [7].

C. Merging blocks

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

Case 1: Several blocks are overlapping.

If a block b_1 and another block b_2 are overlapping, then we merge the two blocks to establish a new one b_3.

Case 2: Several blocks are neighboring.

If the distance between the center of a block b_1 and that of another b_2 are smaller than a threshold T_i, then we merge the two blocks into a new one b_3. Fig. 2 shows an example in this case. Fig. 2(a) is an image and its blocks acquired after region growing and (b) is an image suffering from enlarging operations and its blocks acquired after region growing. As we can see, if an image suffers from scaling, the total number of blocks we obtain will be different from that of the original image.

D. An example

In Fig. 2(c), c_1, c_2, c_3 and c_4 are the center of blocks 1, 2, 3, 4, respectively; d_2, d_3 and d_4 are the distances between the center of the first block c_1 and c_2, c_3 and c_4, respectively. If d_2, d_3 or d_4 is smaller then T_i, then we merge the two blocks. After merging blocks, the total number of blocks is identical to the original one. Fig. 2(d) shows the result after merging blocks. As can be seen, merging blocks can solve the above-mentioned problem.

E. Increasing gray values of all black pixels

Because we embed authentication signals by modifying the gray values of pixels (described later), we increase the gray values of total black pixels (originally 0) to be a new value T_s as the final step of preprocessing.

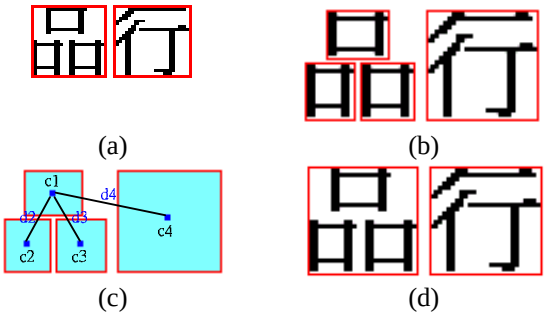


Fig. 2 Block merging. (a) Chinese document image with total number of blocks equal to 2. (b) Enlarged image of (a) with total number of blocks equal to 4. (c) Block distances of (b). (d) The resulting image of (b) after block merging with total number of blocks equal to 2.

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

In this section, we describe how to create and embed authentication signals into blocks segmented in the preprocessing stage. The main idea is to embed a semi-fragile watermark value into each block as an authentication signal. And the value is the *slope* of a line which is created artificially and embedded in the block. The line is created by modifying the gray values of the black pixels in the block through which the embedded line passes. For the purpose of increasing the robustness, we choose the best position for the line according to a certain criterion. The details are described below.

A. Acquiring equation of embedded line

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

$$y = mx + b \tag{1}$$

where m is the slope of the line, and b is the shift of the line with respective to the y-axis.

In our method, we create the value of m in terms of two elements: a key and the RHG value. The key, held by the sender and the receiver, is used to enhance the security of authentication as mentioned previously. It can be promised that even the algorithm is known by a thief, without a correct key the thief can not produce the authentication signals to cheat the algorithm during the authentication process.

On the other hand, the RHG value of a given block O is defined to a gray value G which is computed according to the following *reduced halftone gray function*:

$$G = \frac{(T - B)}{T} \times level \tag{2}$$

where *level* is a pre-selected integer meaning to divide the total gray range into *level* intervals, T is the total number of pixels in the block O and B is the number of black pixels in O. Equation (2) was proposed by Huang and Tsai [6]. Because the *RHG* is based on the use of fixed-sized blocks and can not be applied to our method directly, we revise it to meet our goal of allowing the use of arbitrary-sized blocks.

With the key and the RHG values ready for use, we compute the slope of the embedded line in each block by the following equation:

$$m = (\text{key value} + \text{RHG value})_{mod\ R} \tag{3}$$

where R is a value used to control the range of m so that the line slope will not become uncontrollable. By modifying the slope m of the embedded line, we can embed an authentication signal into each block.

B. Finding the best position to embed a line

After calculating the slope of the embedded line, it is needed to find the best position to embed a line. A technique we use here is to adjust the shift value b of the equation of the line to embed a line which arouses the *least awareness* while maintaining a certain degree of *robustness*. The way we adopt for this purpose is to find the line position with the *largest number of lining-up black pixels* through which the embedded line passes.

Because all the black pixels in a document image have been assigned the gray values of T_s during the preprocessing stage, we embed the authentication signals in each block by modifying back to 0 the gray value of T_s of each pixel on the line determined as described previously. Then, during the authentication process, we only need to extract the pixels with the least gray values (i.e., 0) in each block to recover the embedded line.

C. An example

Fig. 3 shows an example of selecting the best position to embed a line. In this example we set m in Equation (1) to be m =1. Fig. 3(a) shows a block after applying a region growing technique, and (b) is an example of shifting b to seek the best position to embed the line. After adjusting all possible values of b, the best position found to embed the line is shown in Fig. 3(c). Fig. 3(d) shows that the result of modifying the gray values of the black pixels through which the embedded line passes.

4. Image Authentication Process

The process of image authentication is essentially a reverse version of the embedding process. Since the embedded authentication signal is the line created by the key and the RHG value, we can judge an image in suspicion as being tampered with or not by checking the difference between the generated slope m and the extracted slope m' from the image.

More specifically, first the given suspicious image is

partitioned into non-overlapping blocks by region growing, as done in the data embedding process. Then the process of merging neighboring or overlapping smaller blocks into larger ones is conducted. In each block, pixels with the smallest gray values 0 are collected and line fitting is applied to them to extract the authentication signal which is the slope m' of the fitted line:

$$m' = \frac{n\sum_{i=1}^{n} x_i y_i - \sum_{i=1}^{n} x_i \sum_{i=1}^{n} y_i}{n\sum_{i=1}^{n} x_i^2 - (\sum_{i=1}^{n} x_i)^2} \quad (4)$$

where n is the total number of pixels, x_1, x_2, …, x_n and y_1, y_2, …, y_n are the x-coordinates and y-coordinates of the collected pixels.

On the other hand, we collect the two coefficients of the key and the RHG value to compute the original slope value m according to (3). By comparing the difference between m and m', we can judge an image in suspicion as being tempered with or not in each block.

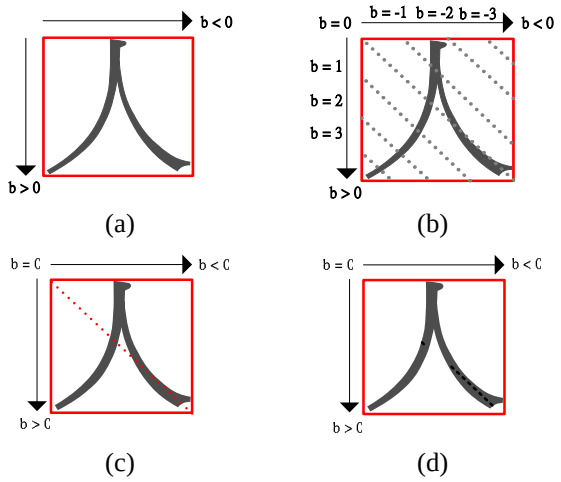


Fig. 3 An example of finding the best position to embed a line. (a) A character. (b) and (c) Shifting the line by changing b to seek the best position to embed the line. (d) Modifying the gray values of the black pixels in the character.

5. Experimental Results

Some experimental results of applying the proposed method are shown here. Figs. 4(a) and (b) are the grayscale images of a Chinese document and an English document, respectively, both with the size of 400 × 500. And the stego-images resulting from embedding authentication signals are shown in Figs. 4(c) and (d), respectively. Figs. 4(e) and (f) are respective reproduced stego-images of Figs. 4(c) and (d) suffering from print-and-scan operations, which were printed at 400 dpi and scanned at 100 dpi using an HP LaserJet 4200 printer and a MICROTEC Scanmaker 9800XL flatbed scanner. The corresponding PSNR values are shown in Table 1.

Two images resulting from tampering with Figs. 4(e) and (f), respectively, are shown in Figs. 5(a) and (b) with resolutions of 100 dpi. And Figs. 5(c) and (d) show the authentication results after applying the proposed authentication process. The red parts indicate the detected areas of tampering. From this result, we see that even if an image is subject to print-and-scan operations before they are tempered with, we can still detect the integrity of the image.

6. Discussions and Conclusions

We have presented a novel scheme to embed authentication signals in grayscale document images, which has robustness against print-and-scan operations. The main idea is to embed a line in each image block as a semi-fragile watermark. The equation of the embedded line is created by a key and an RHG value to increase the security. The authentication signal is the slope of the embedded line. The line is embedded by modifying to be 0 the gray values of the black pixels through which the line passes. And we only have to collect the smallest gray values of the pixels in each block and apply a line fitting technique to extract the embedded line and its slope. We can verify the integrity of each block of the image by comparing the difference between the extracted line slope and the original one. If someone tampers with a stego-image, the RHG value of some of the blocks will be changed, and the extracted slopes of these blocks will not be kept the same as the generated slopes of the blocks. The experimental results prove the feasibility of the proposed method, that is, prove that the embedded authentication signals can survive print-and-scan operations.

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

References

[1] V. Solachidis and L. Pitas, “Circularly symmetric watermark embedding in 2-D DFT domain,” *IEEE Transactions on Image Processing*, Vol. 10, Issue 11, pp. 1741-1753, Nov. 2001.

[2] Y. C. Chiu and W. H. Tsai. “Copyright protection by watermarking for color images against print-and-scan operations using coding and synchronization of peak locations in discrete Fourier transform domain,” *Proceedings of 2004 Conference on Computer Vision, Graphics and Image Processing*, Hualien, Taiwan, Aug. 2004.

[3] F. Lefebvre, A. Gueluy, D. Delannay, and B. Macq, “A print and scan optimized watermarking scheme,” *Proceedings of 2001 IEEE Fourth Workshop on Multimedia Signal Processing*, Cannes, France, pp. 511-516, Oct. 3-5, 2001.

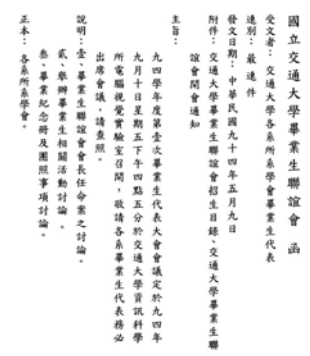
[4] C. Y. Lin and S. F. Chang, “Distortion Modeling and Invariant Extraction for Digital Image Print-and-Scan Process,” *Proceedings of International Symposium on Multimedia*

Information Processing (ISMIP), Taipei, Taiwan, Dec. 1999.

[5] D. J. Fleet and D. J. Heeger, "Embedding invisible information in color images," *Proceedings of IEEE International Conference on Image Processing*, Santa Barbara, CA USA, Vol. 1, pp. 532-535, Oct. 26-29, 1997.

[6] Pei. Ying. Huang and Wen-Hsiang. Tsai, "New and Integrated Techniques for Information Hiding in Images for Copyright Protection, Covert Communication, and Tampering Detection," *M. S. Thesis*, Department of Computer and Information Science, National Chiao Tung University, Hsinchu, Taiwan, Republic of China, June 2003.

[7] R.C. Gonzalez and R. E. Woods, "Digital Image Processing," second edition, 2002, pp. 135-136.


國立交通大學畢業生聯誼會 函

(a)


Homeland Security
Emergency Preparedness
Office of Emergency Response

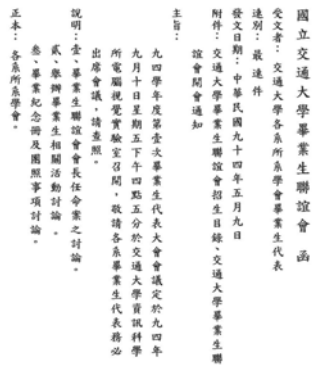
Dear Team Leaders, AO and Team Members,

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

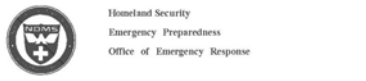
The new Direct Deposit Form is now called the FEPP. I have attached a PDF file with the 1199A form. This can be printed and filled out. Please include on the bottom on line at our website under federal forms; go to forms library, type in Direct Deposit in the search area.

Sincerely.

(b)


國立交通大學畢業生聯誼會 函

(c)


Homeland Security
Emergency Preparedness
Office of Emergency Response

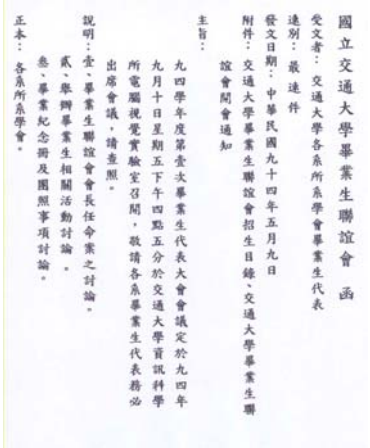
Dear Team Leaders, AO and Team Members,

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

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

Sincerely.

(d)


國立交通大學畢業生聯誼會 函

(e)


Homeland Security
Emergency Preparedness
Office of Emergency Response

Dear Team Leaders, AO and Team Members,

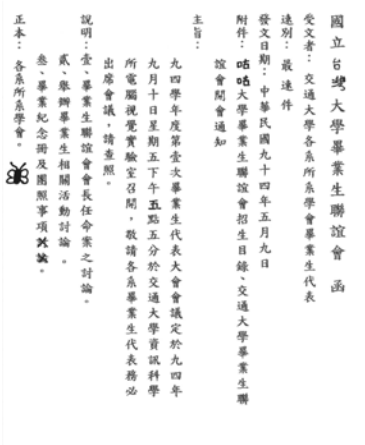
During this time of transition from the Department of Health and Human Services to FEMA, we need the following information form each approved team member in the NDMS database:
A new Direct Deposit Form is to be filled out with an original signature form the approved team member.

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

Sincerely.

(f)

Fig. 4 Input grayscale document images and output stego-images with authentication signals. (a) A grayscale Chinese document image. (b) A grayscale English document image. (c) and (d) stego-images of (a) and (b) after embedding authentication signals, respectively. (e) and (f) stego-images of (c) and (d) suffering from print-and-scan operations.



(a)

(b)

(c)

(d)

Fig. 5 Some images which were tampered with and corresponding authentication results. (a) and (b) Images resulting from tampering with Figures 4(e) and (f), respectively. (c) and (d) Authentication results.

Table 1 The PSNR values of the stego-images after embedding authentication signals.

	Chinese Document Images	**English Document Images**
PSNR	**22.8**	**22.3**