A Novel Block-Based Authentication Technique for Binary Images by Block Pixel Rearrangements[1]

Pei-Ming Huang[a], Da-Chun Wu[b], and Wen-Hsiang Tsai[a,2]

[a]*Department of Computer and Information Science, National Chiao Tung University, Hsinchu 300, Taiwan, R.O.C.*

[b]*Department of information Management, National Kaohsiung First University of Science and Technology, Kaohsiung 811, Taiwan, R. O. C.*

Abstract

A novel blocked-based binary image authentication technique is proposed. The authentication signals of each 9×9 image block are placed in a selected 3×3 block within the 9×9 block. The authentication signal contains a certain relationship contributed by the standard deviation values of the other eight 3×3 blocks. Authentication signals are generated by rearranging the pixels in the selected 3×3 block. The rearrangement is designed according to a property of inverse halftoning to keep the visual change in the selected block imperceptible. By comparing the arrangement of the block pixels in a suspicious image with the extracted authentication signals, the fidelity and integrity of the image can be verified.

1. Introduction

Digital watermarking techniques can be classified into two major approaches. One is the spatial-domain approach [1-2] and the other the frequency-domain approach [3-4]. Binary images are commonly used for archiving document and logo images. It is often necessary to develop appropriate methods to verify their fidelity and integrity for security protection in various applications. So far, there were only a few studies on data hiding in *binary* images and very few researches on authentication of binary images. Wu, Tang, and Liu [5] embedded bits in image blocks by pattern matching. The method can be used both for data hiding and image authentication. The method proposed by Pan, Chen, and Tseng [6] changed pixel values in image blocks to hide secret data by mapping block contents into the secret data. And the method proposed by Tseng and Pan [7] modified the method by Pan, Chen, and Tseng [6] to control the image quality. In Koch and Zhao [8], a bit 1 or 0 was embedded in an image block by enforcing the ratio of the number of black pixels in the block to that of white ones to be larger or smaller than the value 1, respectively.

In this paper, a novel method for image authentication is proposed, which embeds authentication signals in binary images with control of the resulting image quality. The embedded authentication signals not only can be used to check not only the fidelity of a binary image but also the integrity of each block of the image.

The remainder of this paper is organized as follows. In Section 2, the proposed authentication method is described. In Section 3, some experimental results are given to show the feasibility of the proposed method. Finally, some conclusions are stated in Section 4.

2. Proposed Authentication Method

The idea of *inverse halftoning* is employed in the proposed method. The halftoning technique was proposed to convert grayscale images into binary ones and inverse halftoning can be employed to recover grayscale images from binary halftone ones. We modified the inverse halftoning technique in this study for use in authentication signal generation, as described in the following.

2.1 Authentication Signal Embedding Process

To generate authentication signals for a binary image, the image is first divided into non-overlapping 9×9 blocks. Then, each 9×9 block is divided further into nine non-overlapping 3×3 blocks.

[1] This work is supported partially by National Science Council, R.O.C. under Grant No. NSC92-2422-H-009-010 and by the MOE Program for Promoting Academic Excellency of Universities under the grant number 89-1-FA04-1-4.

[2] Corresponding author. E-mail: whtsai@cis.nctu.edu.tw

0-7803-8603-5/04/$20.00 ©2004 IEEE

A. Assigning gray values to 3×3 blocks

Each 3×3 binary image block B is then assigned a gray value G by the following *reduced halftone gray function*:

$$G = \lfloor (9 - N) \times 255 / 9 \rfloor, \qquad (1)$$

where N is the number of black pixels in B, and $\lfloor \cdot \rfloor$ means the integer floor function. The reduced halftone gray function maps the range of gray values [0 255] into 9 discrete gray levels. Such values will be called *reduced halftone gray* (*RHG*) *values*, where the term *reduced* is used to indicate that only nine discrete gray values instead of the original 256 ones are generated here from the gray scale.

B. Choice of rearrangeable block

In order to control the quality of the image with embedded authentication signals, we select 3×3 image blocks for signal embedding. Each selected block is called a *rearrangeable block* in this study. The reason for using this term will be obvious later. If a 9×9 block is neither entirely black nor entirely white, two candidate 3×3 blocks for signal embedding will be picked out of its nine 3×3 blocks. One candidate is the one with its RHG value G_s being the *smallest* but not 0, and the other candidate the one with its RHG value G_l being the *largest* but not 255. The reason to select them is explained as follows.

First, a larger RHG value means that the black pixels in the block are fewer, and a smaller RHG value means that the white pixels in the block are fewer. In the latter case, it will cause less distortion to rearrange the positions of the white pixels than to rearrange those of the black ones. Similar reasoning applies to the former case. The desired *rearrangeable block* is chosen from the two candidate blocks in this study. Let w_s be the number of white pixels in the block B_s whose RHG value is G_s, and b_l be the number of black pixels in the block B_l whose RHG value is G_l. If w_s is larger than or equal to b_l, then according to the previous discussion B_s is taken as the rearrangeable block in the proposed method; otherwise, B_l is taken as the rearrangeable block. We call this way of selecting a rearrangeable block in a 9×9 block *a rearrangeable block selection process* in the sequel.

C. Calculation of standard deviation

For each 9×9 block, a standard deviation σ of the RHG values of the eight 3×3 blocks other than the rearrangeable block is calculated. And a *standard deviation level* L is computed according to the following rule:

$$L = n$$

where n satisfies

$$(n \times 128 / 9) \geq \sigma \geq [(n - 1) \times 128 / 9]. \qquad (2)$$

Because in the gray value range [0 255], the largest integer value of the standard deviation σ is 128, the possible value of σ will fall within the range R = [0, 127]. Therefore, the possible values of L computed by the above rule will be from 1 through 9, which may be regarded to divide the standard deviation range R into 9 levels.

D. Rearrangement of pixels as authentication signal embedding

Let N be the number of black pixels in the rearrangeable 3×3 block B in a 9×9 block. We consider two cases of pixel rearrangement in B for authentication signal embedding in the following.

(a) Case 1:

If $N \leq 4$, it means that the number of black pixels in B is fewer than that of white ones. So, it is faster and so causes less distortion to rearrange the locations of the N black pixels in B than to do so for the $(9 - N)$ white ones. Therefore, we assign N new locations to the N black pixels as a way of embedding authentication signals. More specifically, we employ the value N and the standard deviation level L to design a *pixel rearrangement rule* for this purpose as follows:

$$P_i^b = \left(L \times N^i \bmod C \right) \bmod 9 \quad \text{for all } i \leq N \qquad (3)$$

where P_i^b denotes the index of the new location of the ith black pixel in B and C is a constant pre-selected in such a way that each value of P_i^b is distinct. The indices of the original locations of the nine pixels in a 3×3 block is shown in Figure 1. The value of C is chosen to be 11 according to our experimental experience in this study. Finally, we regard all the indices specified by P_i^b as the *authentication signals* embedded in the rearrangeable block B for the 9×9 block including B.

0	1	2
3	4	5
6	7	8

Figure 1. Indices of a 3×3 block.

For example, Figure 2(a) shows a 9×9 block and Figure 2(b) shows the rearrangeable 3×3 block in it, which is the one in shadow. According to the aforementioned steps, N is 2 and L is 5. By Eq. (3), we can compute P_1^b to be 1 and P_2^b to be 0. That is, the two black pixels in the rearrangeable block should be rearranged to be at positions with indices 0 and 1 according to the proposed pixel rearrangement rule of (3) described above, resulting in Figure 2(c). The indices 0 and 1 of the black pixel positions are regarded as authentication signals here.

(b) Case 2:

If $N \geq 5$, it means that the number of black pixels in B is larger than that of white ones, which is $(9 - N)$. So, it is faster and causes less distortion to rearrange the locations of the $(9 - N)$ white pixels in B than to rearrange those of the N black ones. Therefore, we assign $(9 - N)$ new locations to the $(9 - N)$ white pixels as a way of authentication signal embedding. The steps are similar to those of the previous case and are omitted here.

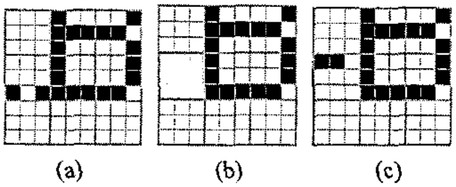


Figure 2. An example of authentication signal generation and embedding. (a) A 9×9 block. (b) The rearrangeable 3×3 block (in shadow) of the 9×9 block. (c) The 9×9 block after authentication signal embedding.

It is emphasized that the RHG value of each rearrangeable 3×3 block, after pixel rearrangement, will be kept unchanged because the pixel rearrangement is just a permutation of the pixels' positions and not an alteration of the number of black pixels or white pixels in the block. This important property makes possible the authentication signal verification work in the image authentication process, as described in the following.

2.2 Image Authentication Process

In the authentication signal embedding process, the locations of the rearranged pixels of the rearrangeable 3×3 block are taken as authentication signals. So, we can judge whether an image is tampered or not by checking whether the locations of the rearranged pixels of the 3×3 rearrangeable block, found according to the pixel rearrangement rule described previously, have been changed.

More specifically, a suspicious image is first divided into non-overlapping 9×9 blocks, and each 9×9 block is divided further into nine non-overlapping 3×3 blocks. The number N of black pixels in each 3×3 block B is counted, and the RHG value G of B computed. Then the rearrangeable 3×3 block in each 9×9 block is selected, and the standard deviation σ and the level corresponding standard deviation level L of σ of each of the remaining eight 3×3 blocks are computed. By the pixel rearrangement rules Eqs. (3) and (4) with N and L as inputs, authentication signals P_i^b or P_i^w can be computed. By checking the arrangement of all the pixels of the rearrangeable block, if the computed indices P_i^b (or P_i^w) are the same as the locations of all the black (or white) pixels of the rearrangeable block, the 9×9 block is judged as not being altered; otherwise, tampered with.

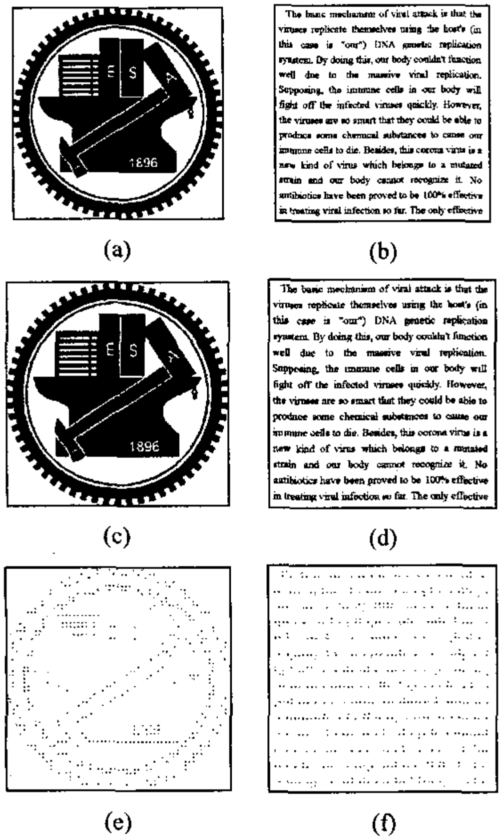
3. Experimental Results

Some experimental results of applying the proposed method are shown here. Figures 3(a) and (b) show two binary images "NCTU" and "Document" both with the size of 512×512. And the stego-images resulting from embedding authentication signals are shown in Figures 3(c) and (d), respectively. Figures 3(e) and (f) show the differences between Figures 3(a) and (b) in black pixels after embedding the authentication signals, respectively.

Two tampered images are shown in Figures 4(a) and (b). And Figures 4(c) and (d) show the respective authentication results. The red parts indicated the detected tampered blocks.

4. Concluding remarks

We have presented a novel authentication scheme to embed and verify authentication signals in binary images. We change the positions of white or black pixels in so-called rearrangeable blocks to obtain and embed authentication signals. That is, authentication signals are taken to be the indices of rearranged pixels in the rearrangeable block in each 9×9 image block. Because the authentication signals of each 9×9 image block contains a certain relationship contributed by the standard deviation of the RHG values of other eight 3×3 blocks in the 9×9 block, if somebody tampers with the stego-image, the resulting image will yield different standard deviation values and so different authentication signals in the 9x9 blocks. The result is that the arrangement of the pixels in the rearrangeable 3x3 blocks in the tampered image will be not the same as that revealed by the calculated authentication signals. By authenticating a suspicious image in this way, the tampered blocks can be detected and located, achieving the goal of verifying image fidelity and integrity.



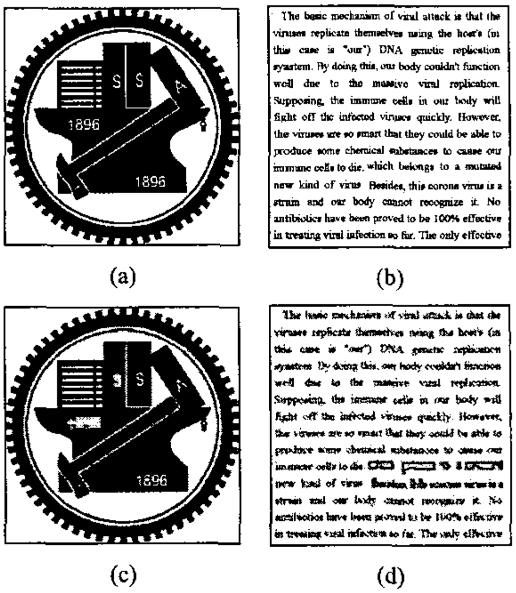
The basic mechanism of viral attack is that the viruses replicate themselves using the host's (in this case is "our") DNA genetic replication system. By doing this, our body couldn't function well due to the massive viral replication. Supposing, the immune cells in our body will fight off the infected viruses quickly. However, the viruses are so smart that they could be able to produce some chemical substances to cause our immune cells to die. Besides, this corona virus is a new kind of virus which belongs to a mutated strain and our body cannot recognize it. No antibiotics have been proved to be 100% effective in treating viral infection so far. The only effective

Figure 3. Input binary images. (a) "NCTU". (b) "Document". (c) and (d) Resulting images after embedding authentication signals, respectively. (e) and (f) The difference pixels after embedding authentication signals, respectively.

References

[1] J. Fridrich, "Robust bit extraction form images," in *Proc. IEEE ICMCS'99 Conf.* Florence, Italy, June 7–11, 1999.

[2] W. Bender, N. Morimoto, and D. Gruhl, "Method and apparatus for data hiding in images," U. S. Patent, No. 5689587, 1997.



The basic mechanism of viral attack is that the viruses replicate themselves using the host's (in this case is "our") DNA genetic replication system. By doing this, our body couldn't function well due to the massive viral replication. Supposing, the immune cells in our body will fight off the infected viruses quickly. However, the viruses are so smart that they could be able to produce some chemical substances to cause our immune cells to die. which belongs to a mutated new kind of virus Besides, this corona virus is a strain and our body cannot recognize it. No antibiotics have been proved to be 100% effective in treating viral infection so far. The only effective

Figure 4. Two tampered images and their authentication results. (a) and (b) Tampered images. (c) and (d) authentication results, respectively.

[3] I. J. Cox, J. Kilian, F. T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. on Image Processing, Vol. 6, no. 12, pp. 1673–1687, 1997.

[4] C. T. Hsu and J. L. Wu, "DCT-Based watermarking for video," IEEE Transactions on Image Processing, vol. 8, pp. 58–68, 1999.

[5] M. Wu, E. Tang, and B. Liu, "Data hiding in digital binary images," presented at the IEEE International Conference on Multimedia and Exposition, New York, 2000.

[6] H. K. Pan, Y. Y. Chen, and Y. C. Tseng, "A Secure Data Hiding Scheme for Two-Color Images," IEEE ISCC 2000, Antibes-Juan les Pins, France, pp. 750-755, July 1999.

[7] Y. C. Tseng and H. K. Pan, "Secure and invisible data hiding in 2-color images," in Proc. IEEE INFOCOM 2001 The Conference on Computer Communications, Anchorage, Alaska, U. S. A., Vol. 2, April 2001, pp. 887-896.

[8] E. Koch and J. Zhao, "Embedding robust labels into images for copyright protection," Proceedings of International Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Techniques, Munich, Germany, 1995, pp. 242–251.