Pakistan Journal of Applied Sciences 2(5): 553-557, 2002

An Image Authentication Scheme Based on Digital Signatures

Yuan-Liang Tang, Min-Shiang Hwang, Ching-Rong Yang
Department of Information Management, Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng, Taichung County, Taiwan 413, R.O.C.

Abstract: It is important to protect digital pictures and detect tampered image locations in digital Cyberspace. In this paper, we propose an image authentication scheme based on digital signature. The proposed scheme is capable of detecting if certain blocks of an image have been altered. The block can be as small as 86 image pixels.

Key Words: Authentication, Cryptography, Digital Signature, Image Authentication

Introduction

It is necessary to protect digital media because information such as images; audio/video data, text, and software are transmitted via the Internet (Chen, Chang, and Hwang, 1998; Hwang, Chang, and Hwang, 1999; Hwang, Chang, and Hwang, 2000; Chang, Hwang, and Hwang, 2000; Chang, Hwang, and Chen, 2001). Consider the following case. When an image is used as a piece of evidence in the prosecution of a crime, the court must make sure that the evidence has not been altered. Without this guarantee, the image cannot be used as legal evidence. Such an image can be a matter of life and death in a criminal case. The ability to accurately verify the authenticity of an image, as well as detecting the altered locations in a tampered image is extremely important. When an image is transferred over the network, hackers may intercept it and make changes to it. Similarly, an image file produced by a digital camera (Friedman, 1993) may be doctored for certain purposes.

Recently, many approaches (Friedman, 1993; Wong, 1998; Wu, 1998) have been proposed to solve the problem of image authentication, including the legal use of images and trusted camera and medical image archiving.

In these methods, the owner or receiver of the image must have a prior knowledge about the image size (Wong, 1998) or its look-up table (Wu, 1998). For example, Wong proposed a public key watermark (Wong, 1998) for image verification and authentication. This approach can not only authenticate an image, but also identify the tampered location. However, one of the drawbacks is that the smallest detectable block is 172 pixels. It is thus desirable to develop a scheme that can effectively detect altered blocks smaller than 172 pixels.

In this paper, we introduce a new method for image authentication, which is able to detect an altered image block as small as 86 pixels.

An effective authentication and verification scheme should have the following features:

- Determine if the image or data has been modified.
- Enable a defense for any attack.
- Be independent from the image size or the look-up table.

Our method used the RSA cryptosystem (Chang and Hwang, 1996) to generate and put a signature into the Least Significant Bits (LSB) of each block. This scheme can be applied to a "secure" digital camera (Friedman, 1993) for authenticating and detecting altered image pixels.

This paper is organized as follows. Section 2 introduces the basic idea of how to encrypt image blocks into LSB. Section 3 provides some experimental results. The analysis is performed in section 4, and section 5 gives the concluding remarks.

Proposed Scheme: The main idea is to perform a set of operations to detect altered blocks. The scheme is based on the RSA signature with 512 bits (Atkins, 1994). Five hundred and twelve bits are used for protecting each image block. This method can detect altered locations as sub-blocks. The following discussions are focused on gray level images. For color images, the same technique applies.

Let I_{mn} be a gray level image of size m by n pixels. The Most Significant Bits (MSB) and Least Significant Bits (LSB) of each pixel in our scheme are 5 and 3 bits, respectively. Since each signature block is 512 bits in the RSA cryptosystem, we require 172 pixels (as a block) to input a signature. The total numbers of MSBs and LSBs in a block (172 pixels) are 860 and 516 bits, respectively. In a straightforward method, we can hash the 860 bits (an MSB block) to 516 bits. A signature can then be made with 516 bits and placed into the LSB block using the RSA cryptosystem. If the block has not been altered, the MSBs of the signature will be equal to the LSBs. If the MSB of the signature are not equal to the LSBs, we can be certain that a portion of this block has been altered. This straightforward method can determine only whether the block (172 pixels) has been altered or not. The proposed scheme (described below) can be used to detect an altered image with size as small as 86 pixels. The proposed scheme is described here in the following six steps:

Step 1: Collect and Construct the First Block: According to the RSA standard, at least 512 bits are necessary for an encryption to effectively resist any attack. Because the LSB is defined as 3 bits/pixel, 172 pixels must be collected to form a signature (172 * 3=516 bits). Now every first 5 bits (MSB) of the 172 pixels are collected to form the block b_1, which represents the image data. The final 3 bits (LSB) of each pixel are collected to form w_1, i.e. the signature. In our method, b_1 is further divided into two 86 pixel sub-blocks, denoted sb_1 and sb_2, as shown in Fig. 1, and then all bits in w_1 are set to zero. The block with the signature structure is illustrated in Fig. 2(a).

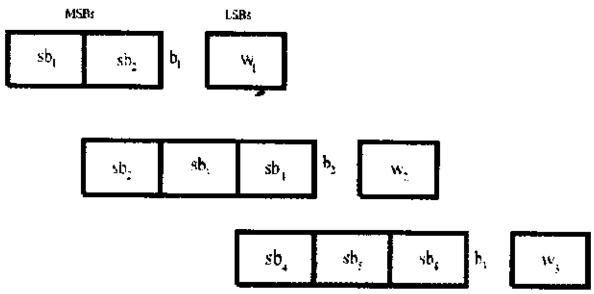

Fig. 1: Blocks with MSBs and LSBs

Step 2: Collect and Construct the Second Block: We denote the second to the last block as b_2 to b_r, respectively, where $r = \lceil m * n/172 \rceil$. Every block b_r is divided into three sub-blocks ($sb_{2(r-1)}$, sb_{2r-1}, sb_{2r}). An example of blocks with a signature structure is shown in Fig. 2(a) and (b). The steps for embedding a signature into an image are shown in Fig. 3.

In the previous steps 1 and 2, the block $b_1 = sb_1 + sb_2$, $b_2 = sb_2 + sb_3 + sb_4$, $b_r = sb_{2(r-1)} + sb_{2r-1} + sb_{2r}$, where + denotes concatenation. Since, the size of sub-block sb_i is equal to 86 pixels, the number of pixels in b_1 is 172 and the number of pixels in the others b_i, i=2,..., r, are equal to 258.

Step 3: Choose One-way Hash Function: Let H be a one-way hash function, such as MD5 (Rivest, 1992). H can be formulated as:

$$Hb_i = H(b_i), i = 1,2,\ldots,r. \qquad (1)$$

Here, the length of b_1 is 860 bits (=172 * 5); The lengths of b_i, 2= i= r, are 1290 bits (=258 * 5); The lengths of Hb_i, i=1,2, ..., r, are 516 bits.

Step 4: Generate and Embed the Signature: The RSA cryptosystem is used to generate the digital signature S_i as follows.

$$S_i = E_d(Hb_i), i = 1,2,\ldots,r. \qquad (2)$$

Where d is the system's private key and E is the RSA algorithm (Rivest, Shamir, and Adleman, 1978) with 516 bits. The length of S_i is 516 bits. The signatures S_i are embedded into w_i, i=1, 2, , r.

Step 5: Verify Image: When an image is received, it is necessary to perform an authentication process and determine if and where the image has been altered. The authentication process consists of 6 consecutive tasks as delineated in Fig. 4. The first three tasks are the same as in Step 1. i.e., the hash values HB_i', i=1, 2,..., r are obtained. The fourth task uses the RSA cryptosystem (Rivest, 1978) to recover the signature S_i as follows.

$$DHb_i = D_e(S_i), i = 1,2,\ldots,r. \qquad (3)$$

Where e is the system's public key and D is the RSA deciphering algorithm. If the image has not been altered, each pair of Hb_i' and DHb_i should match. Otherwise, the image has been altered.

Step 6: Identify the Tampered Location: The following rule is used to confine the altered location. We define three sets as follows.

- A = {sb_i | a set of the pairs Hb_i' and DHb_i do not match.}.
- B = {sb_j | a set of the pairs Hb_j' and DHb_j match.}.
- C = {sb_k | a set of probable altered sub-blocks.}. In other words, C = A - B. Here, - denotes a difference set operation.

For example, if all Hb_i' and DHB_i' match except for Hb_2' and DHB_2', we know that the block b_2 has been altered. According to rules, A = {sb_2, sb_3, sb_4}, B= {sb_1, sb_2, sb_4, sb_5,...}, and, C = A – B = {sb_3}. Therefore, we obtain a probable altered sub-block sb_3. This means that the altered locations can be detected at a range of 86 pixels.

Results and Discussion

The experimental result is shown in Fig. 5. We used the "Lena" image (256 * 256 pixels) as the test image. Fig. 5(a) shows an original image. Fig. 5(b) shows an image with a signature embedded into the original image. Fig. 5(c) shows an image with a black eyeball that has been altered. Fig. 5(d) shows how an image can be detected using our scheme. The large black background area in Fig. 5(d) represents the location that has not been altered, whereas the small black & white area at the middle represents a location that has probably been altered. Here, the length of the tampered area is 86 pixels.

Analysis: In this section we analyze some tampered image cases. The shaded sub-blocks in Fig.s 6-10 represent altered sub-blocks.

Case 1: Sub-block Sb_1 Is Altered (Shown in Fig. 6): Block b_1 does not match in Step 5 of Section 2, while b_2, b_3, and other blocks do match. By applying rules from step 6 of section 2, we have

- A = {sb_1, sb_2}.
- B = {sb_2, sb_3, sb_4,..., sb_r}.

The probable tampered sub-block is C = A – B = {sb_1}. In the straightforward method (described in Section 2), the detected tampered sub-blocks are sb_1 and sb_2. The length of detected tampered is 172 pixels. In comparison, the length of the detected tampered pixels is only 86 under the proposed scheme.

Case 2: Sub-blocks sb_1 and sb_2 are Altered (Shown in Fig. 7): Blocks b_1 and b_2 do not match in Step 5 of Section 2, while b_3 and other blocks do match. By applying rules from step 6 of section 2, we have

- A = {sb_1, sb_2, sb_3, sb_4}
- B = {sb_4, sb_5, sb_6, ..., sb_r}.

The probable tampered sub-block is C = A - B= {sb_1, sb_2, sb_3}.

In the straightforward method (described in Section 2), the detected tampered sub-blocks are sb_1 and sb_2 and its length is 172 pixels. However, the length of the detected

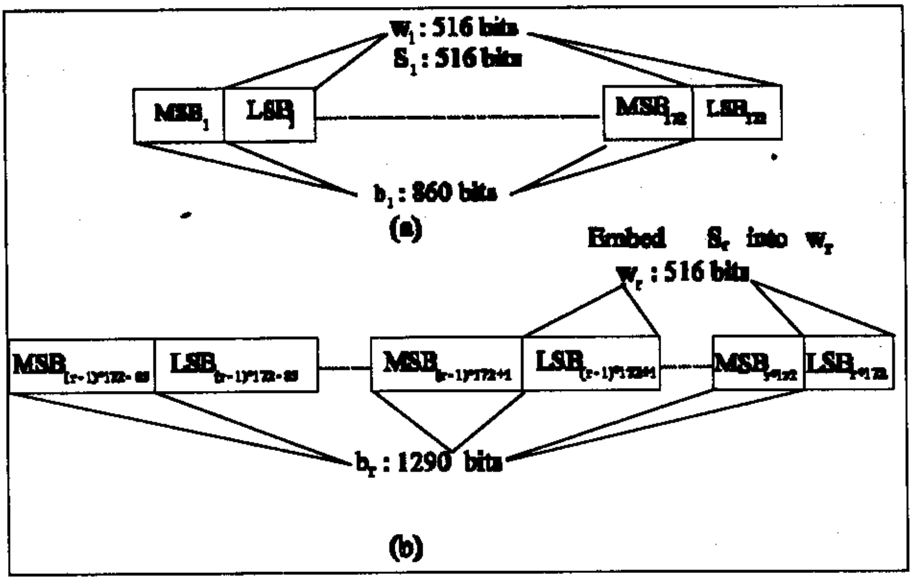

Fig. 2: Blocks with Signature S_i

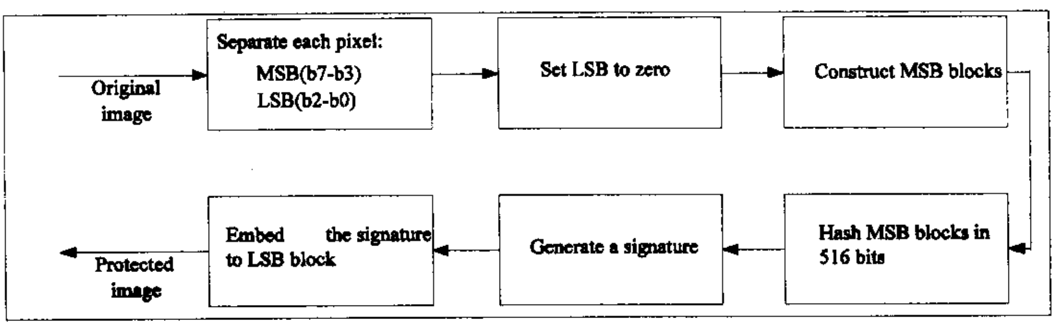

Fig. 3: Embed a Signature in to an Image

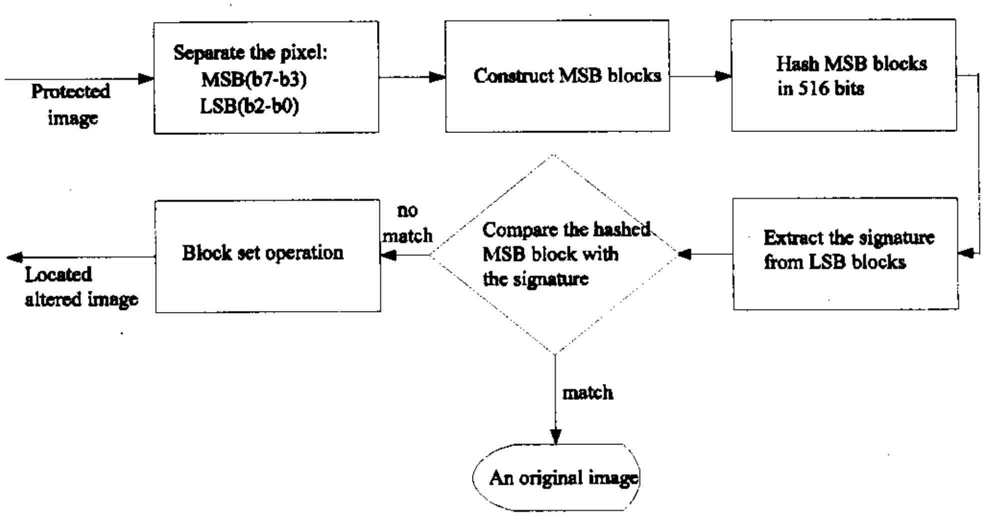

Fig. 4: Extract a Signature from a Protected Image

(a) (b) (c) (d)

Fig. 5: Experimental Result

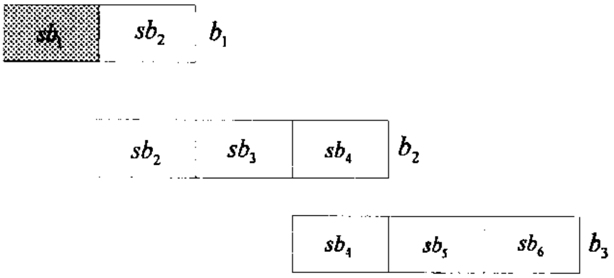

Fig. 6: An Example of Altering Sub-block sb_i

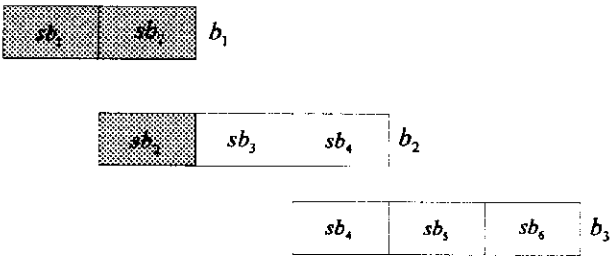

Fig. 7: An Example of Altering Sub-blocks sb_i and sb_2

tampered is 258 pixels using the proposed method. We conclude that if two sub-blocks in a block are altered, then the straightforward method is better than our method.

Case 3: Sub-blocks sb_2 and sb_3 are Altered (shown in Fig. 8): Blocks b_1 and b_2 do not match in Step 5 of Section 2, while b_3 and other blocks do match. By applying rules from step 6 of section 2, we have

- A = {sb_1, sb_2, sb_3, sb_4}
- B = {sb_4, sb_5, sb_6, ..., sb_r }.

The probable tampered sub-block is C = A - B= {sb_1, sb_2, sb_3}.

In the straightforward method, the detected tampered sub-blocks are sb_1, sb_2, sb_3, and sb_4. The length of detected tampered pixels is 344, whereas the length of detected tampered pixels is 258 under the proposed method. Therefore, if two consecutive sub-blocks sb_{2i} and sb_{2i+1} in different blocks b_i and b_{i+1}, respectively, are altered, the proposed scheme gives the better performance than the straightforward method.

Case 4: Sub-block b_2 is altered (shown in Fig. 9): Here the blocks b_1 and b_2 do not match, while b_3 and other blocks do match. Therefore we have

- A = {sb_1, sb_2, sb_3, sb_4}
- B = {sb_4, sb_5, sb_6, ..., sb_r }.

The probable tampered sub-block is C = A - B= {sb_1, sb_2, sb_3}.

Under the straightforward method, the detected tampered sub-blocks are sb_1, sb_2, sb_3, and sb_4, and its length of detected tampered pixels is 344 pixels. However, the length of the detected tampered pixels is 258 pixels using our method. We conclude that if a sub-block sb_{2i} in a block b_i is tampered, then the straightforward method is better than our method.

Case 5: Sub-block sb_3 is Altered (shown in Fig. 10): Block b_2 does not match in Step 5 of Section 2, while b_1, b_3, and other blocks do match. By applying rules from step 6 of section 2, we have

- A = {sb_2, sb_3, sb_4}
- B = {sb_1, sb_2, sb_4, sb_5, sb_6, ..., sb_r }.

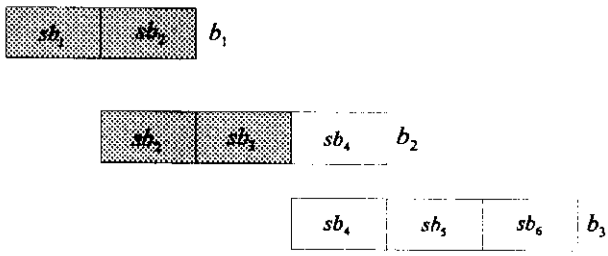

Fig. 8: An Example of Altering Sub-blocks sb_2 and sb_3

The probable tampered sub-block is C = A - B= {sb_3}.

In the straightforward method (described in Section 2), the detected tampered sub-blocks are sb_3 and sb_4. The length of detected tampered pixels is 172 pixels. However, the length of the detected tampered pixels is 86 pixels using our method. We conclude that if a sub-block sb_{2i-1} in a block b_i is altered, then our method is better than the straightforward method.

Although, our method is not better the straightforward method in some cases, the main merit of our scheme is that our scheme can detect a tampered location within 86 pixels.

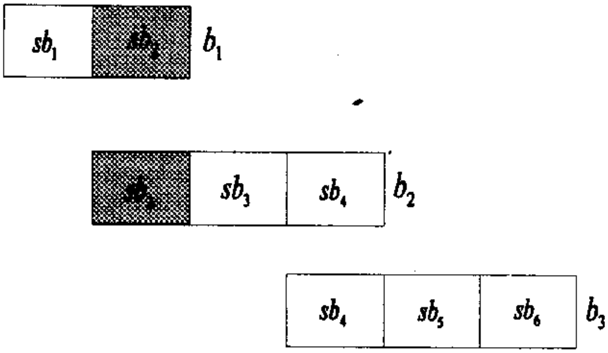

Fig. 9: An Example of Altering Sub-block sb_2

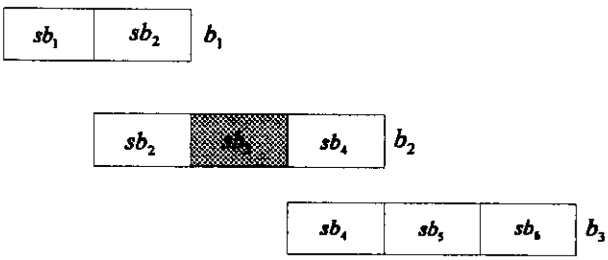

Fig. 10: an Example of Altering Sub-block sb_3

Conclusion

In this paper, we have proposed a new method for image authentication, which can detect a tampered block with size as small as 86 image pixels. In the proposed scheme, a prior knowledge is not necessary for detecting tampering in an image.

Acknowledgement

The authors wish to thank many anonymous referees for their suggestions to improve this paper. Part of this research was supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC90-2213-E-324-004.

References

B. Schneier, 1996. "Applied Cryptography." John Wiley & Sons Press.

C. C. Chang and M. S. Hwang, 1996. "Parallel Computation of The Generating Keys For RSA Cryptosystems," IEE Electronics Letters, 32: 1365-1366.

C. C. Chang, K. F. Hwang, and M. S. Hwang, 2000. "A Digital Watermarking Scheme Using Human Visual Effects", Informatica, 24: 505-511.

C. C. Chang, M. S. Hwang, and T. S. Chen, 2001. "A New Encryption Algorithm For Image Cryptosystems," Journal of Systems and Software, 58: 83-91.

D. Atkins, M. Graff, A. K. Lenstra, and P. C. Leyland, 1994. "The Magic Words Are Squeamish Ossifrage," In Advance in Cryptology, Asiacrypt '94, 263-277.

G. L. Friedman, 1993. "The Trustworthy Digital Camera: Restoring Credibility to The Photographic Image," IEEE Transactions on Consumer Electronic, 905--910.

M. S. Hwang, C. C. Chang, and K. F. Hwang, 1999. "A Watermarking Technique Based on One-way Hash Functions," IEEE Transactions on Consumer Electronics, 45: 286-294.

M. S. Hwang, C. C. Chang, and K. F. Hwang, 2000. "Digital Watermarking of Images Using Neural Networks", J. of Electronic Imaging, 9: 548-555.

M. Wu and B. Liu, 1998. "Watermarking For Image Authentication," Proceedings of the IEEE International Conference on Image Processing, 437-441.

P. W. Wong, 1998. "A Public-Key Watermark For Image Verification and Authentication," Proceedings of the IEEE International Conference on Image Processing, 455-459.

R. L. Rivest, 1992. "The MD5 Message Digest Algorithm," RCF 1321.

R. L Rivest, A. Shamir, L. Adleman, 1978. "A Method For Obtaining Digital Signatures And Public-Key Cryptosystems," Communications of the ACM, 21: 120-126.

T. S. Chen, C. C. Chang, and M. S. Hwang, 1998. "A Virtual Image Cryptosystem Based Upon Vector Quantization," IEEE Transactions on Image Processing, 7: 1485-1488.