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; Wang, 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 $I_m$ 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:

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 $s_{b_1}$ and $s_{b_2}$, as shown in Fig. 1, and then all bits in $w_i$ are set to zero. The block with the signature structure is illustrated in Fig. 2(a).

$$ DH_{b_i} = D_e(S_i), i = 1, 2, ..., r. $$

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 $H_{b_i}$ 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.

- $A = \{s_{b_i} \mid$ a set of the pairs $H_{b_i}$ and $DHB_i$ do not match $\}$.
- $B = \{s_{b_i} \mid$ a set of the pairs $H_{b_i}$ and $DHB_i$ match $\}$.
- $C = \{s_{b_i} \mid$ a set of probable altered sub-blocks $\}$. In other words, $C = A - B$. Here, $-$ denotes a difference set operation.

For example, if all $H_{b_i}$ and $DHB_i$ match except for $H_{b_1}$ and $DHB_1$, we know that the block $b_2$ has been altered. According to rules, $A = \{s_{b_1}, s_{b_2}, s_{b_3}\}$, $B = \{s_{b_1}, s_{b_2}, s_{b_3}, s_{b_4}\}$, and $C = A - B = \{s_{b_1}\}$. Therefore, we obtain a probable altered sub-block $s_{b_1}$. 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 Figs. 6-10 represent altered sub-blocks.

**Case 1: Sub-block $S_{b_1}$ 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

- $A = \{s_{b_1}, s_{b_2}\}$.
- $B = \{s_{b_1}, s_{b_2}, s_{b_3}, ..., s_{b_r}\}$.

The probable tampered sub-block is $C = A - B = \{s_{b_1}\}$. In the straightforward method (described in Section 2), the detected tampered sub-blocks are $s_{b_1}$ and $s_{b_2}$. 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 $s_{b_1}$ and $s_{b_2}$ 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

- $A = \{s_{b_1}, s_{b_2}, s_{b_3}\}$.
- $B = \{s_{b_4}, s_{b_5}, s_{b_6}, ..., s_{b_r}\}$.

The probable tampered sub-block is $C = A - B = \{s_{b_1}, s_{b_2}\}$. In the straightforward method (described in Section 2), the detected tampered sub-blocks are $s_{b_1}$ and $s_{b_2}$, and its length is 172 pixels. However, the length of the detected
Fig. 2: Blocks with Signature S

Fig. 3: Embed a Signature in to an Image

Fig. 4: Extract a Signature from a Protected Image
**Tang et al.**: An Image Authentication Scheme Based on Digital Signatures

![Image](a.png)

**(a)**

![Image](b.png)

**(b)**

![Image](c.png)

**(c)**

![Image](d.png)

**(d)**

Fig. 5: Experimental Result

![Image](a.png)

![Image](b.png)

![Image](c.png)

![Image](d.png)

**Fig. 6: An Example of Altering Sub-block sb,**

![Image](a.png)

![Image](b.png)

**Fig. 7: An Example of Altering Sub-blocks sb, and sb2.**

![Image](a.png)

![Image](b.png)

**Fig. 8: An Example of Altering Sub-blocks sb2 and sb3.**

![Image](a.png)

**Fig. 9: An Example of Altering Sub-blocks sb3 and sb4.**

![Image](a.png)

![Image](b.png)

**Fig. 10: An Example of Altering Sub-blocks sb4 and sb5.**

Method. Therefore, if two consecutive sub-blocks sb2 and sb2, in different blocks b, and b2, respectively, are altered, the proposed scheme gives the better performance than the straightforward method.

**Case 4: Sub-block b2 is altered (shown in Fig. 9):**

Here the blocks b1 and b2 do not match, while b2 and other blocks do match. Therefore we have

- A = {sb1, sb2, sb3, sb4}
- B = {sb1, sb5, sb6, ..., sb7, sb8, ... , sb10}.

The probable tampered sub-block is C = A - B = {sb1, sb2, sb3}.

Under the straightforward method, the detected tampered sub-blocks are sb1, sb2, sb3, and sb4, 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 sb2 in a block b1 is tampered, then the straightforward method is better than our method.

**Case 5: Sub-block sb2 is altered (shown in Fig. 10):**

Block b2 does not match in Step 5 of Section 2, while b1, b3, and other blocks do match. By applying rules from Step 6 of section 2, we have

- A = {sb1, sb2, sb3}
- B = {sb1, sb2, sb3, sb4, sb5, sb6, ..., sb10}.

The probable tampered sub-block is C = A - B = {sb1, sb2, sb3}.

In the straightforward method, the detected tampered sub-blocks are sb1, sb2, sb3, and sb4. The length of detected tampered pixels is 344, whereas the length of detected tampered pixels is 258 under the proposed method. We conclude that if two sub-blocks in a block are altered, then the straightforward method is better than our 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.

![Image of altered sub-blocks](image)

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

![Image of altered sub-blocks](image)

**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**


