Tattooing Attack: A New Type of Watermarking Attacks on Image Authentication

Jia-Hong Li, Department of Information Engineering and Computer Science, Feng Chia University, Taichung, Taiwan
Tzung-Her Chen, Department of Computer Science and Information Engineering, National Chiayi University, Chia-Yi City, Taiwan
Wei-Bin Lee, Department of Information Engineering and Computer Science, Feng Chia University, Taichung, Taiwan

ABSTRACT

Image authentication must be able to verify the origin and the integrity of digital images, and some research has made efforts in that. In this paper, we reveal a new type of malicious alteration which we call the “Tattooing Attack”. It can successfully alter the protected image if the collision of the authentication bits corresponding to the altered image and the original watermarking image can be found. To make our point, we chose Chang et al.’s image authentication scheme based on watermarking techniques for tampering detection as an example. The authors will analyze the reasons why the attack is successful, and then they delineate the conditions making the attack possible. Since the result can be generally applied into other schemes, the authors evaluate such schemes to examine the soundness of these conditions. Finally, a solution is provided for all tamper detection schemes suffering from the Tattooing Attack.

Keywords: Authentication Scheme, Image Authentication, Tampering Detection, Tattooing Attack, Watermarking

INTRODUCTION

Due to the rapid development of multimedia systems in distributed environments, the problems of illegally reproducing, tampering and distributing digital images have become more and more serious. Consequently, the research of image authentication is also becoming a very urgent issue in this decade. A secure image authentication scheme must satisfy two criteria. First, it must have the ability to detect the modifications of a protected image from all sorts of malicious tampering and non-hostile signal processing. Second, it must be able to locate the modified area correctly.

DOI: 10.4018/ijdcf.2014070103
To date, several secure image authentication schemes have been proposed (Caldelli, 2006, Celik, 2002, Chan, 2007, Chang, 2006, Chen, 2009, Lin, 2005, Liu, 2007, Wang, 2007, Wang, 2008, Zhu, 2007), but for simplicity, the scheme proposed by Chang et al. (2006), based on the watermarking technique, is used to introduce our new “Tattooing Attack”. The reasons for the success of the attack will be discussed and further extended to other schemes. In addition, when a remedy is provided and applied, it will retain all of the merits of the original scheme, and at the same time, exempting them from the threat of the Tattooing Attack.

The remainder of this paper is organized as follows: Firstly, we will review the image authentication scheme proposed by Chang et al. and then describe the Tattooing Attack applied to Chang et al.’s scheme in The security of Chang et al.’s scheme section. In The improved scheme section, we will provide the improved method. In Discussions section, the experimental results and discussions are demonstrated. Some similar examples are analyzed and the countermeasure is given in Examples analysis and countermeasure section. Finally, the conclusions are given.

REVIEW OF CHANG ET AL.’S SCHEME

To understand the “Tattooing Attack”, we take Chang et al.’s scheme (Chang, 2006) as an example, although a security problem (Phan, 2008) has been found recently. We will later show that the attack can be generalized to other image authentication schemes.

In 2006, Chang et al. (2006) proposed an image authentication scheme for grayscale images based on the fragile watermarking technique, which can assure the ownership of the image as well as detect the counterfeited part of the image. Figure 1 demonstrates the processes of Chang et al.’s scheme.

Assume that there is a grayscale image with a size of $M \times N$, where $M$ and $N$ are the pixel size of the width and the height, respectively.

First, we divide the grayscale image into $\left\lfloor \frac{M}{2} \times \frac{N}{2} \right\rfloor$ overlapping blocks each with 3×3 pixels in size. As shown in Figure 2(a), every block overlaps with its neighboring blocks and is two pixels apart. Figure 2(b) illustrates the structure of an overlapping block $b_x$. There is a central pixel $p^{x}$ for embedding the authentication data and eight surrounding pixels $p^{x}_i$, where the parameter $x$ indicates the block index and the parameter $i$ denotes the pixel index as defined in Figure 2(b).

Accordingly, the procedure of the scheme is as follows:

**Step 1:** Computing feature data

Compute a feature sequence for each block by:

$$H\left( p^{x}_1 || p^{x}_2 || \cdots || p^{x}_8 || x || ID || SK \right)$$
Antecedents of Online Privacy Protection Behavior: Towards an Integrative Model
www.igi-global.com/chapter/antecedents-online-privacy-protection-behavior/60942?camid=4v1a