A REVERSIBLE IMAGE AUTHENTICATION SCHEME BASED ON CHAOTIC FRAGILE WATERMARK

Di Xiao[1,2] and Frank Y. Shih[2]

[1]College of Computer Science and Engineering
Chongqing University
Chongqing 400044, P. R. China
xiaodi_cqu@hotmail.com

[2]College of Computing Sciences
New Jersey Institute of Technology
Newark, NJ 07102, USA
shih@njit.edu

ABSTRACT. *Although a variety of watermark-based image authentication schemes have been proposed so far, most of them have to leave some permanent distortions in the original image for embedding the watermark information. In this paper, we propose a novel reversible image authentication scheme to allow complete recovery of the cover image after the extraction of the embedded watermark. In the embedding process, the original image is partitioned into blocks; the chaotic watermark of each block is computed and embedded into the block itself in a reversible way. In the extracting process, the watermarked image is partitioned into blocks; the embedded watermark of each block is extracted and the block itself is fully recovered. Then we compute the new chaotic watermark of each recovered block and perform comparison with the extracted one. Therefore, we can detect whether the original image is modified. If it is, then the modification can be located. Besides, by the use of chaotic watermark, the complicated nonlinear and sensitive dependence within image feature, secret key, and watermark is established to ensure the watermarking security. Theoretical analysis and computer simulation have verified the successful achievement of the proposed image authentication scheme.*
Keywords: Fragile watermark, Authentication, Reversible watermark, Chaos, Hash

1. **Introduction.** With recent rapid development of information technology, digital multimedia has been widely used in many applications. However, the rising information security problems, such as malicious alternation and forgery, have become increasingly serious. Fragile digital watermarking is used to accomplish data authentication, and a variety of fragile watermark-based image authentication schemes have been developed [14]. Among them, the seminal fragile watermarking scheme proposed by Yeung and Mintzer [21] is based on the parity of pixel values and uses the error diffusion to keep proper average color. Fridrich [7] and Holliman and Memon [8] respectively analyzed its security drawback and proposed their attack and improvement. Since the function of the fragile watermarking scheme is to authenticate the integrity of the media, the watermark should reflect the content of the media, which is quite different from its counterpart in the robust watermarking scheme.

The hierarchical block-based watermarking scheme proposed by Celik et al. [2] not only includes the information of the corresponding block, but also possesses the relative information of higher-level blocks. Chan and Chang [3] introduced the (7, 4)-Hamming code into the image authentication area. Liu et al. [11] employed permutation transform and