Measurement 88 (2016) 287–296

Contents lists available at ScienceDirect

Measurement

journal homepage: www.elsevier.com/locate/measurement

Image tamper detection and recovery using adaptive embedding rules

Ching-Sheng Hsu [a], Shu-Fen Tu [b,*]

[a] Department of Information Management, Ming Chuan University, No. 5, Deming Rd., Gueishan District, Taoyuan City 333, Taiwan
[b] Department of Information Management, Chinese Culture University, No. 55, Huagang Rd., Shihlin District, Taipei City 11114, Taiwan

ARTICLE INFO

Article history:
Received 30 January 2015
Accepted 25 March 2016
Available online 1 April 2016

Keywords:
Digital watermarking
Fragile watermarking
Image authentication
Tamper detection

ABSTRACT

Many image tamper detection methods implement authentication and recovery in units of blocks; however, these methods do not consider the characteristics of blocks to distinguish watermark embedding and detection modes, thus resulting in poor hiding effects. We suggest that embedding an excessive number of bits within a region with only a slight change in an image to record recovery information is unnecessary. In addition, more recovery information is required in a region with major changes to improve recovery quality. Therefore, this study used smoothness to distinguish the types of image blocks, and employ different watermark embedding, tamper detection, and recovery strategies for different block types to enhance hiding efficiency, authentication, and recovery effects. The experimental results regarding the authentication error rate and image quality showed that the proposed scheme has satisfactory performance.

1. Introduction

Because of the advancement in computer and Internet technologies, transmitting, circulating, and exchanging digital information and digital works (e.g., text, images, sound, and video) have become more convenient and frequent. However, digitized information or work is likely to be tampered and altered. The consequences can be disastrous if a receiver cannot authenticate information [1]. For examples, a tampered medical image may prompt an insurance settlement dispute; a tampered picture in a news article may distort facts; a tampered evidential image for a criminal case may cause misjudgements [2]. Therefore, verifying the integrity of digital images has become a popular and crucial research subject.

Image integrity verification can be implemented using digital signatures [3] or digital watermarking. The digital signature method involves extracting the feature information of digital images and saving it as independent authentication information. Whether a digital image is tampered can be verified if the authentication information is determined. However, the part that is tampered cannot be known. By contrast, digital watermarking enables not only identifying whether an image is tampered, but also locating the tampered part. Therefore, digital watermarking is more practical than using digital signatures. A digital watermark used for image authentication is called a fragile watermark [2,4–12]. A watermark-based image authentication scheme contains two phases: the first is watermark embedding and the second is tampering detection. In watermark embedding, an image feature is converted to a watermark, which is then hidden in the image. In tampering detection, the hidden watermark is extracted to determine whether the image has been tampered and the location of the tampered part. Some fragile watermarking schemes can even recover the tampered part.

[*] Corresponding author. Tel.: +886 2 2861 0511x35932; fax: +886 2 2861 8805.
E-mail address: dsf3@ulive.pccu.edu.tw (S.-F. Tu).

http://dx.doi.org/10.1016/j.measurement.2016.03.053
0263-2241/© 2016 Elsevier Ltd. All rights reserved.

Watermark embedding and detection can be technically divided into the frequency and spatial domains. The technology of the frequency domain uses transfer functions (e.g., fast Fourier transform, discrete cosine transform, and discrete wavelet transform) to convert pixel gray levels of the spatial domain to coefficients of the frequency domain and then hides the watermark in these coefficients [1,13–16]. The technology of the spatial domain directly modifies the pixel gray level to embed and detect a watermark. In addition, this type of technology usually hides the watermark in the least significant bits (LSBs) of the image to avoid damaging the image [17,18]. Many spatial-domain fragile watermarking schemes entail embedding watermarks and detecting whether an image has been tampered block by block. Obviously, the amount of information that a block can hide is restricted by the block size. A large block can carry a large amount of information, leading to a low error rate of tamper detection; however, the ability of this scheme to precisely locate the tampering part becomes poor [19]. Some methods involve implementing tamper detection directly in pixels, increasing the detection precision; however, the space for hiding information is small [20]. To balance the hiding space and detection precision, block authentication and pixel authentication are combined in some methods [12].

A practical image tamper detection method should detect the integrity of an image, locate the tampered part, and then recover the tampered part. Many image tamper detection methods entail watermark embedding, tamper authentication, and recovery in units of blocks [9,11]. However, in these methods, the characteristics of a block can be utilized are not used to increase the efficiency of information hiding and tampering authentication. We believe that the recovery information of the blocks with slight changes can be encoded in fewer bits, and that of the blocks with uneven chages can be encoded in more bits to enhance recovery quality. Accordingly, an excessive amount of space to store the recovery information of smooth blocks is unnecessary, and space can be saved for storing the recovery information of texture blocks. Therefore, this study used smoothness to distinguish the types of image blocks and design different strategies for watermark embedding, tamper detection, and recovery for different block types to increase the efficiency of watermark embedding and improve the results of tampering detection and recovery.

2. The proposed scheme

Most image authentication schemes involve encoding authentication and recovery information in fixed bits regardless of the characteristics of blocks. Some blocks requiring more authentication and recovery information fail to obtain adequate information, and some blocks requiring low information are allotted information exceeding their demand. In our scheme, the encoding rule of the authentication and recovery information of a block is determined using its smoothness level. For different encoding rules, the strategies for embedding watermarks, tampering detection, and recovery are distinguished accordingly.

Suppose that the original image is an $M \times N$ lossless gray level image, where M and N are the height and width of the image, respectively. The original image is divided into nonoverlapping blocks of 2×2 pixels, which are denoted as small blocks, and each 4×4 small block is grouped as a large block. Smoothness is used to distinguish the type of each large block. The smoothness level of a large block is determined by its pixel value variance. Each large block with the top one-third variance is categorized as a nonsmooth block, and the rest are smooth blocks. In addition, a small block belonging to a nonsmooth large block is categorized as a nonsmooth block. Similarly, a small block belonging to a smooth large block is categorized as a smooth block. Fig. 1(b) designates the nonsmooth and smooth blocks shown in Fig. 1(a) in white and black colors, respectively. The image tamper detection and recovery scheme proposed in this study is detailed as follows.

2.1. Watermark embedding method

In the proposed scheme, the watermark contains authentication information, block types, and recovery information and is embedded in the LSBs of pixels. The spatial-domain layouts of smooth and nonsmooth small blocks are shown in Fig. 2, where each row represents eight bits b_7, b_6, …, b_0 of a pixel. The notations in Fig. 2 are explained as follows. H_s is the authentication information of a small block, H_b is the authentication information of a large block, R_s is the recovery information of a small block, R_b is the recovery information of a large block, and C is the type of a large block ($C = 0$ represents the smooth type and $C = 1$ represents the nonsmooth type). The watermark embedding procedure is described as follows.

Step 1: Divide the entire image into $k = M \times N/64$ nonoverlapping large blocks. In addition, divide the entire image into $M \times N/4$ nonoverlapping small blocks.

Step 2: Divide the entire image into 16 equal-sized zones Z_0, Z_1, …, Z_{15} (Fig. 3), where each zone contains k small blocks. Let

$$A = \begin{bmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,k-1} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,k-1} \\ \vdots & \vdots & \vdots & \vdots \\ a_{15,0} & a_{15,1} & \cdots & a_{15,k-1} \end{bmatrix}, \tag{1}$$

where $a_{i,j}$ is the number of j-th small blocks in the i-th zone Z_i. The k small blocks in the Z_i are numbered as $(a_{i,0}, a_{i,1}, \ldots, a_{i,k-1})$. Then, use a virtual random number generator with seed SK to disarrange the elements in each row vector of matrix A and generate a stochastic correspondence matrix

$$A' = \begin{bmatrix} a'_{0,0} & a'_{0,1} & \cdots & a'_{0,k-1} \\ a'_{1,0} & a'_{1,1} & \cdots & a'_{1,k-1} \\ \vdots & \vdots & \vdots & \vdots \\ a'_{15,0} & a'_{15,1} & \cdots & a'_{15,k-1} \end{bmatrix}. \tag{2}$$