J. Vis. Commun. Image R. 38 (2016) 18–28

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

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

SVD-based self-embedding image authentication scheme using quick response code features [☆]

Wen-Chuan Wu [*], Zi-Wei Lin

Department of Computer Science and Information Engineering, Aletheia University, 32 Zhenli St., Taipei 25103, Taiwan

ARTICLE INFO

Article history:
Received 19 October 2015
Accepted 8 February 2016
Available online 12 February 2016

Keywords:
Image authentication
Fragile watermarking
Tamper detection
Self-embedding
Quick response code
Singular value decomposition
Differential prediction
Data recovery

ABSTRACT

Image authentication is a type of technique for the content protection of digital images. This technique is able to detect and locate tampered regions on a digital image. In this paper, two self-embedding image authentication approaches are proposed to involve distinctive singular values. Both of them extract self-characteristics of an image as the crucial authentication information for that image. Subsequently, this information is converted into the two dimensional code format and that codes are then embedded into digital image pixels. With the capability of error correction in two dimensional codes, the extracted authentication data, even being detected with a tamper, still can be completely restored and errorless. As well, it can be utilized to detect whether an image has been tampered with or not. According to experimental results, the proposed approaches are superior to other schemes for images that have been modified to a certain attack extent because the authentication data could be completely extracted in more effective way, and the tampered regions could be identified more accurately. In addition, the proposed approaches utilize these complete self-characteristics to restore tampered regions into their original states.

1. Introduction

The rapid development of digital and network technologies indeed aroused a drastic increase in the number of information technology (IT) users. With just their handheld mobile devices, people can either search for information online and acquire new knowledge at any time and in any place, or share information instantly with others on social network websites. Digital media such as images, audio files, and videos are digital content most commonly found online [13]. People store their own digital works on cloud platforms, thereby increasing the visibility of their works to other Internet users. Although digital information can be edited, stored, distributed, and shared easily, it can also be tampered with, modified, and copied by attackers who engage in illegal activities. In particular, two highly similar digital images cannot be differentiated with the naked eye [12]; therefore, the safety of digital media content in easily accessible network environment has gradually received much attention [1,2,12,13,16].

Cryptography is a conventional technique [2] used to protect digital and sensitive data. Specifically, mathematical formulae and encryption keys are applied to convert ordinary information into unintelligible text (also called ciphertext). Unless they know the corresponding key, other people cannot decrypt the ciphertext and get the plaintext. This approach enables confidential information to be disseminated secretly. However, meaningless ciphertext is prone to malicious attacks. Moreover, decryption computation is complicated and time-consuming, rendering it inapplicable to process voluminous digital images and videos. Digital watermarking [1] is a method of using embedding techniques to protect the intellectual property of digital media; it embeds signatures or marks representing the ownership of a digital content creator. When disputes regarding ownership arise, such marks can be used to identify copyright ownership [14]. Given the broadening scope of its application, digital watermarking can be classified as robust watermarking and fragile watermarking [1]. Robust watermarking can easily block off various types of digital attacks and is used to verify ownership of work, whereas fragile watermarking is used to determine whether an embedded watermark has been destroyed and it detects whether data have been sabotaged.

Fragile watermarking, also known as image authentication, is a type of digital image data protection technique used to confirm the integrity of image media [18]. When image data are transmitted or stored using a network, image authentication can be used to detect whether an image has been tampered with; this process is called

[☆] This paper has been recommended for acceptance by M.T. Sun.

[*] Corresponding author.

E-mail addresses: au4387@au.edu.tw (W.-C. Wu), freelifetw29@gmail.com (Z.-W. Lin).

http://dx.doi.org/10.1016/j.jvcir.2016.02.005
1047-3203/© 2016 Elsevier Inc. All rights reserved.

tamper detection. Subsequently, the tampered portion of an image can be restored to its original state; this process is referred to as data recovery. Currently, research investigating image authentication techniques primarily focuses on active and passive authentication schemes [17], as shown in Fig. 1. Active authentication involves protecting an image from being counterfeited before it is transmitted on the network. In this scheme, an authentication data is used to determine whether an image has been sabotaged and counterfeited. By contrast, passive authentication requires no additional information; it uses an image's inherent features or any abnormalities in the image content to detect traces of digital tampering.

The least significant bit (LSB) flipping method [15] in 1995 is the earliest active anti-forgery authentication method proposed by Walton et al., who applied checksum to perform modular operation on the most significant bits (MSBs) of each image pixel. The calculated results were then used as image authentication information, embedding them in the LSB of each pixel. However, this approach provided no safety mechanisms, allowing counterfeiters to skillfully maintain the checksum value of an image unchanged without altering the LSB. Wong et al. proposed a novel block-based image authentication technique [19] to address the shortcomings of Walton et al.'s method and provide a more secure protection mechanism. In 2009, Wu and Ren adopted chaotic map and Sudoku rules to develop an image authentication scheme [20]. Chen and Wang [9] employed fuzzy c-means clustering to generate the association among image blocks. This association was then used as an image's unique authentication data. Subsequently, Chan [3] utilized error-correcting hamming codes to adjust image pixel bits for tamper detection of authentication data.

In addition to pixel bit operation, there are some research works tried to solve problem by compression and transformation operations. Cruz-Ramos et al. specifically protected the region of interest (ROI) on an image by proposing an image authentication scheme [7] based on discrete cosine transform (DCT) and self-embedding processing. Wu and Hsieh [16] and Chuang et al. [6] both adopted vector quantization compression technique to detect tampered parts of an image. They also used compression data to restore the tampered portion. Furthermore, Chuang et al. [6] improved the quality of the recovered image using multi-copies and majority voting methods. In [17,18], two active image authentication schemes were proposed based on block truncation coding (BTC) and singular value decomposition (SVD), respectively. However, the tampered regions cannot be restored well and the problem of detected misjudgments was still unsolved in both proposed schemes [17,18]. Therefore, Chen and Chen [4] developed a novel scheme, using two-dimensional quick response codes to express authentication data. This scheme provided added protection to authentication data; thus, even if an image was tampered with and the QR code data were somewhat damaged, the extracted authentication data remained intact and accurate.

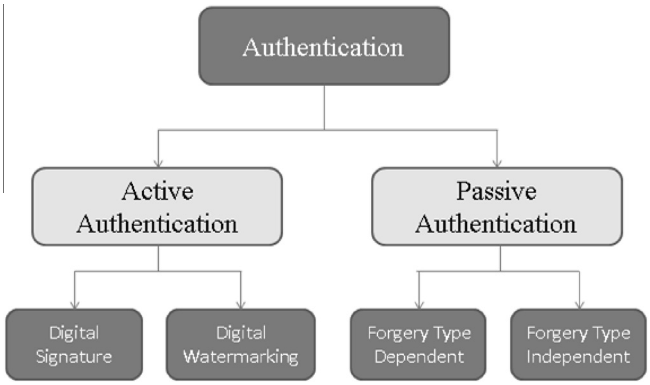

Fig. 1. Image authentication techniques [18].

However, this approach proposed by Chen and Chen required the original image in order to accurately indicate the location of the tampered regions on the image. Later, Dadkhah et al. [10] presented an improved SVD-based authentication scheme for tamper localization and self-recovery. Merely, its self-recovery using an average intensity of blocks is slightly powerless. Therefore, we will propose two improvements to overcome the shortcomings of Wu et al.'s scheme [18], Chen and Chen's scheme [4] and Dadkhah et al.'s scheme [10]. By making using of the error correction capability of QR codes, we can avoid possibly detected misjudgments and secure the authentication data against attacks so as to enhance the image qualities. The rest of this paper is organized as follows: Section 2 introduces quick response code, singular value decomposition, and Chen and Chen's scheme. The proposed schemes are presented in Section 3. Section 4 shows the experimental results of proposed scheme, followed by a conclusion in Section 5.

2. Related works

In this section, we will provide some background knowledge of our novel schemes by reviewing several related works. First, in Sections 2.1 and 2.2, the basic concepts of QR code and SVD are introduced, respectively. Then in Section 2.3, a brief review of the earlier image authentication scheme [4] based on QR codes is presented.

2.1. Quick response code

A quick response (QR) code is a type of matrix or two dimensional (2D) barcode. It is an extension of the conventional one dimensional barcode, which only uses spaces and vertical lines to express information. But, a QR code records more data using an additional dimension. Recently, numerous applications for QR codes have been developed. General smartphone users can scan that QR code using a decoder to obtain the information embedded in the code. Such an approach is faster and more convenient compared with the conventional method of typing data manually. Fig. 2 illustrates the structural design [5] of QR codes developed in Japan. The dark gray part represents the data storage area, which has a capacity for storing a maximum of 4296 English characters or 984 Chinese characters, and is frequently used to transmit personal contact details, web addresses, and product information.

In addition, QR codes feature point positioning and error correction mechanisms, enabling users to scan image patterns from different angles to read data. Even if a part of the QR code is damaged, the content can still be read out with the decoder. A QR code has four error correction levels that namely L, M, Q, and H represent error correction rates of 7%, 15%, 25%, and 30%, respectively.

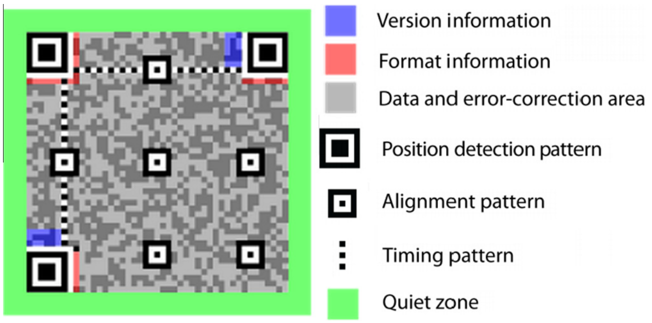

Fig. 2. Structural design of a QR code [5].