Digital Signal Processing 33 (2014) 134–147

Contents lists available at ScienceDirect

Digital Signal Processing

www.elsevier.com/locate/dsp

A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition

Nasrin M. Makbol, Bee Ee Khoo *

School of Electrical and Electronic Engineering, Universiti Sains Malaysia, Malaysia

ARTICLE INFO

Article history:
Available online 2 July 2014

Keywords:
Digital image watermarking
Integer wavelet transform
Singular value decomposition
Wilcoxon signed rank test
Digital signature

ABSTRACT

In this paper, a new robust and secure digital image watermarking scheme that can be used for copyright protection is proposed. The scheme uses the integer wavelet transform (IWT) and singular value decomposition (SVD). The grey image watermark pixels values are embedded directly into the singular values of the 1-level IWT decomposed sub-bands. Experimental results demonstrate the effectiveness of the proposed scheme in terms of robustness, imperceptibility and capacity due to the IWT and SVD properties. A challenge due to the false positive problem which may be faced by most of SVD-based watermarking schemes has been solved in this work by adopting a digital signature into the watermarked image. The proposed digital signature mechanism is applied to generate and embed a digital signature after embedding the watermarks; the ownership is then authenticated before extracting watermarks. Thus, the proposed scheme achieved the security issue where the false positive problem is solved, in addition to that, the scheme is considered as a blind scheme. A computer simulation is used to verify the feasibility of the proposed scheme and its robustness against various types of attacks and to compare it with some previous schemes. Furthermore, the statistical Wilcoxon signed rank test is employed to certify the effectiveness of the proposed scheme.

© 2014 Elsevier Inc. All rights reserved.

1. Introduction

With the rapid global expansion of the Internet, the growth of digital technologies has become a basic requirement, and these technologies provide numerous advantages for transferring data across the World Wide Web. The easy editing, transfer and tracing of digital data and the ability to copy data without degrading the content are some advantages. However, a number of problems have emerged along with these advantages, one of which is the ease with which digital data can be perfectly and rapidly copied, which necessitates copyright protection. Thus, digital watermarking was suggested as an attractive solution to protect copyright. Although it was the main reason for the introduction of digital watermarking, copyright protection is not the only application of this technology, which has been expanded to fingerprinting, broadcast monitoring and authentication applications.

Digital watermarking is the process of concealing secret information in a digital medium. This information should be imperceptibly embedded in a way that allows it to be extracted or detected later for security purposes. Different types of digital watermarking methods for various media have been developed and classified into three classes: robust, fragile and semi-fragile. These classes are application-dependent. Additional classes of such technologies are blind, semi-blind and non-blind, which are based on the information required for the extraction or detection process. The alternative classifications rely on the domain where the secret information will be embedded and are further classified as spatial domain techniques and transform domain techniques. Low complexity and easy implementation are the advantages of each spatial watermarking technique. Despite these benefits, spatial watermarking methods are fragile against image processing operations. However, transform watermarking techniques; such as discrete cosine transform (DCT) [1,2], discrete wavelet transform (DWT) [3], redundant discrete wavelet transform (RDWT) [4,5], radon transform [6], lifting wavelet transform (LWT) [7] and etc., are preferred due to their desirable properties. These schemes embed a watermark by modulating the coefficients magnitude in a transform domain, allowing more information to be embedded, thus resulting in greater robustness against both image processing attacks (e.g., JPEG compression and noise attacks) and malicious attacks (e.g., rotation, scaling and translation attacks).

All digital watermarking schemes consist of two processes: the embedding process and the extracting or detecting process. Each

* Corresponding author.
E-mail addresses: Nasrin.ld08@student.usm.my (N.M. Makbol), beekhoo@usm.my (B.E. Khoo).

http://dx.doi.org/10.1016/j.dsp.2014.06.012
1051-2004/© 2014 Elsevier Inc. All rights reserved.

watermarking scheme must satisfy a number of requirements. The basic requirements related to any watermarking system are robustness, capacity and data payload, imperceptibility and security. Robustness refers to the scheme's resistance against several attacks, including image processing attacks and geometrical attacks. Robustness varies from one operation to another and from one scheme to another. All schemes cannot resist all attacks, and hence, their resistance is application-dependent [8]. The second requirement is capacity and data payload. The data payload indicates number of watermark bits that encoded within a message [9] while the watermark capacity indicates the amount of information in the selected medium (e.g., image, video or audio), for example in an image, if multiple watermarks are embedded, then the sum of all individual watermark's data payload is the watermarking capacity [10]. The similarity between the original medium and its watermarked version is known as imperceptibility. Imperceptibility is sometimes referred to as fidelity or perceptual transparency [9]. The peak signal-to-noise ratio (PSNR) is a metric that is used to evaluate imperceptibility performance. A higher PSNR indicates a higher imperceptibility. Generally in the watermarking world, a minimum PSNR of 38 dB is considered acceptable [11]. A trade-off always exists among the robustness, capacity and imperceptibility; for example, increasing the embedding capacity in an image may enhance its robustness while simultaneously degrading its imperceptibility and vice versa. Therefore, researchers have increased their efforts to develop techniques that find a compromise between these conflicting parameters. Thus, many robust techniques with high embedding capacities and good imperceptibilities have been developed. The security term is used to describe a technique that resists many hostile attacks [9], indicating that a robust scheme can survive common image processing operations, but may not be secure against malicious attacks. The security aspect of the singular value decomposition (SVD)-based schemes should be monitored, specifically, the problem of false positive, thus will serve the security requirement.

Currently, improving the robustness against attacks by protecting the visual quality is considered the core motivation of most existing watermarking schemes. Hence, the incentive to develop hybrid schemes that combine two or more transforms to utilise the properties of these transforms and achieve the required goals has arisen. A few years ago, a number of robust hybrid watermarking schemes based on SVD were developed [12,13,4,14,3,5,7,15]. SVD is a technique that can be used to mathematically extract the algebraic properties from an image. Considering an image as a matrix A, SVD of A can be represented as follows:

$$SVD(A) = USV^T \tag{1}$$

U, S and V^T are matrices. SVD-based digital watermarking schemes embed a watermark by modifying either the singular values (S) or the orthogonal vectors U and V. One of the advantages to employing SVD in digital watermarking schemes is the good stability of its singular values, meaning that the visual quality of the image can be preserved even for large singular value changes, which may occur during the attacks. Although, most SVD-based watermarking schemes have proven their robustness, they have failed to resolve their rightful ownership [12,13,4,14,3,5]. These schemes suffered from the false positive problem, in which a fake watermark was detected from the content of where a different watermark was embedded. Two causes of this problem are stated in this paper. The first involves the modification of the singular values of the host with the singular values of the watermark as occurred with the schemes developed by Ganic et al. [13], Lagzian et al. [4] and Rastegar et al. [14]. All of these schemes followed the same embedding steps except for the wavelet transform types used, which were the DWT by [13], RDWT by [4], and finite Radon transform (FRAT) and DWT by [14]. The embedding process was performed by modifying the singular values of each sub-band of the host image with the singular values of the watermark. Here, the false positive problem might have occurred due to exposing the watermark to the SVD process, as was explained clearly by Xiao et al. [16]. The second cause of this problem is due to the following embedding process:

$$S + \alpha W = U_W S_W V_W^T \tag{2}$$

as occurred with [12,3,5]. This process requires the embedding of the watermark (W) into the singular values (S) of the host image after multiplying it by scaling factor α. Next, the result is transformed using SVD to obtain new matrices named as U_W, S_W and V_W^T to distinguish between them and the matrices results due to applying SVD on the original host image. The challenge in such an embedding process results from adopting U_W and V_W^T as secret keys for the extraction process. Usually, U and V can preserve major information about an image. Therefore, the attacker can claim ownership using forged singular vectors U_F and V_F to obtain a unique forged watermark regardless of the extracted singular values [17,18]. Thus, the schemes follow the same embedding technique are vulnerable to the false positive problem [17–19]. Examples of these schemes include Liu et al. [12], Lai et al. [3] and Makbol et al. [5]. In Liu et al. [12], the host image was transformed using SVD, and the watermark was then directly embedded into the singular values of the host image using Eq. (2). In Lai et al. [3], the authors decomposed the host image into four sub-bands (LL, LH, HL and HH) using the DWT and then applied SVD to only the LH and HL sub-bands. Finally, the watermark image was divided into two-halves and then embedded into the singular values of LH and HL, respectively, using Eq. (2). However, Makbol et al. [5] decomposed the host image into four sub-bands (LL, LH, HL and HH) using the RDWT instead of the DWT proposed by Lai et al. [3]. Each sub-band was the same size as the host image due to the RDWT decomposition analysis. After this analysis, the SVD was applied to all sub-bands, and four grey-scale watermark images with the same host image size were embedded in the singular values of the sub-bands by means of Eq. (2). Notably, the above-mentioned schemes that suffered from the false positive problem exhibited good performance against attacks, especially our previously reported scheme (Makbol et al. scheme [5]). With the Makbol et al. scheme [5], we approached the problem by ignoring the exposure of the watermark to SVD, but the security weakness due to the false positive detection is emerged due to the adopted embedding equation that addressed by Eq. (2). However, Makbol's scheme outperformed some of the state of the art schemes in all watermarking requirements (robustness, embedding capacity and imperceptibility). In this study, we met all of the watermarking requirements, especially robustness. Moreover, we attempted to overcome the lack of security due to the false positive problem by discovering a suitable solution that also satisfied the other watermarking requirements. Several solutions to this issue have been suggested, such as those proposed by Loukhaoukha et al. [20] and Gupta et al. [21]. Loukhaoukha et al. [20] reported two solutions, the first of which was to apply a one-way hash function on U and V. Accordingly, these terms received two hashing values, H_U and H_V, which were then stored into a private key. This proposed solution was presented and implemented by Loukhaoukha et al. [7]. First, these authors applied a 2-level LWT on a host image and then selected any sub-band (LH2, HL2 or HH2). The authors then computed the inverse LWT and applied SVD to the results, obtaining U, S and V. SVD was also applied to a watermark, obtaining U_W, S_W and V_W. Embedding was accomplished by modifying the singular values (S) of the host image using the singular values (S_W) of the watermark. Loukhaoukha et al. [7] solved the false positive problem by

Download English Version:

https://daneshyari.com/en/article/564660

Download Persian Version:

https://daneshyari.com/article/564660

Daneshyari.com