J. Vis. Commun. Image R. 24 (2013) 1099–1105

Contents lists available at SciVerse ScienceDirect

J. Vis. Commun. Image R.

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

A blind image copyright protection scheme for e-government ☆

Shi-Jinn Horng [a,b,*], Didi Rosiyadi [b,f], Tianrui Li [a], Terano Takao [c], Minyi Guo [d], Muhammad Khurram Khan [e]

[a] *School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China*
[b] *Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology, Taiwan, ROC*
[c] *Department of Computational Intelligence and Systems Science, Tokyo Institute of Technology, Tokyo, Japan*
[d] *Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China*
[e] *Center of Excellence in Information Assurance, King Saud University, Saudi Arabia*
[f] *Research Center for Informatics, Indonesian Institute of Sciences (LIPI), Indonesia*

ARTICLE INFO

Article history:
Received 5 October 2012
Accepted 9 July 2013
Available online 19 July 2013

Keywords:
Blind
Quantizing value
Discrete cosine transform
Singular value decomposition
E-government
Genetic algorithm
Pick signal to noise ratio
Minimum square error

ABSTRACT

An efficient blind copyright protection for e-government document images is proposed through a combination of the discrete cosine transform (DCT) and the singular value decomposition (SVD) based on genetic algorithm (GA). This combination could lead the watermarked image to be resistant to various attacks as well as to improve its performance, security and robustness. DCT, in this case, is applied to the entire image and mapped by a zigzag manner to four areas from the lowest to the highest frequencies. SVD, meanwhile, is applied in each area and then the singular value of DCT-transformed host image, subsequently, is modified in each area with the quantizing value using GA to increase the visual quality and the robustness. The host image is not needed in the watermark extraction and it is more useful than non-blind one in real-world applications. Experiment results demonstrate that the proposed method outperforms other existing methods under several types of attacks.

1. Introduction

E-government refers to the use of information technology by governmental offices to provide better services for people and business and to facilitate cooperation among governmental institutions. To safeguard important information in a government, e-government information security that plays a critical role in a successful implementation for e-government and transaction-based services, is required. Here, confidential information, authenticity, integrity and non-repudiation are some of the security issues in e-government that are under discussion. Confidential information should not be accessible to any unauthorized users. On the other side, authenticity should be verified by a person or a project claiming to be an originator and vice versa when information is received. For integrity, the information, once stored or sent, should appear exactly on retrieval or received at the other end of a communication network. At last, for non-repudiation, the sender after sending/authorizing a message should not be able to deny at the time of having done so [3,15]. In response, a new technology, called digital watermarking, must be in place to protect the integrity of digital information and to safeguard the intellectual property rights in order to prevent and counter these issues. Tracking the printing of the document sources, tampering proofing and assessments, copying control, and doing finger printing, additionally, are necessary to do in e-government then.

Digital watermarking technique has been used in access control, copyright information, and authentication [13,14]. Watermarking itself that includes singular value decomposition (SVDs), discrete cosine transforms (DCTs), discrete wavelet transforms (DWTs), and discrete fractional Fourier transforms (DFFTs) can be grouped into two approaches; one is the spatial domain and the other is the transform domain. In the former approach, watermarking was through a direct embedment into the pixel locations, while in the latter approach, it is through the embedment of the watermark by changing the frequency components. The watermark has to gratify several requirements such as non-blind, semi-blind and blind schemes. Non-blind schemes require both the original image and the secret key(s) for watermark extraction. The semi-blind one, on the other side, requires both secret key(s) and watermark sequences, while the blind one can only use the secret key(s) [2,4,5].

☆ This work was supported in part by the National Science Council under contract number NSC-99-2916-I-011-002-A1, and it was also partially supported by the 111 Project under the Grant No. 111-2-14 and One Hundred Person Project 2012, Sichuan Province.

* Corresponding author.

E-mail addresses: horngsj@yahoo.com.tw (S.-J. Horng), didi.rosiyadi@gmail.com (D. Rosiyadi), trli@swjtu.edu.cn (T. Li), terano@plum.plala.or.jp (T. Takao), guo-my@cs.sjtu.edu.cn (M. Guo), mkhurram@ksu.edu.sa (M.K. Khan).

1047-3203/$ - see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.jvcir.2013.07.008

In this paper, an efficient blind copyright protection for e-government document images is presented through a combination of DCT and SVD based on GA. The rest of this paper is organized as follows: Section 2 is to present the related works; Section 3 presents the explanation of the proposed watermarking scheme – followed by Section 4 presenting the proposed experimental results. Section 5 as the last section provides the conclusion of this paper.

2. Related works

In previous researches, several watermarking schemes had been proposed for non-blind DCT-SVD watermarking, some of which were optimized by genetic algorithm (GA) for digital image watermarking, for example in [1,2] in which the SVD watermarking schemes were based on genetic algorithm. Meanwhile, Lai et al. [1] proposed a novel image-watermarking scheme using SVD and micro-genetic algorithm (micro-GA). Here, to embed the watermark image, the modification of the singular values of the cover image was through the multiple scaling factors in which the proper values of scaling factors were efficiently optimized and obtained by means of the micro-GA.

Veysel et al. [2] proposed a novel optimal watermarking scheme based on SVD using GA. To embed the watermark image, the singular values (SV) of the host image were modified through an optimization using GA to obtain the highest possible robustness without losing any transparency. The non-blind hybrid-watermarking schemes based on genetic algorithm have been proposed in [3], in this case, by combining the DCT and the SVD using a control parameter to avoid a false positive problem. An optimization process of the scaling factor key α was conducted based on GA.

Some blind schemes, meanwhile, have been used in [4–6,8–10,12,16–18]. In [4], a blind watermarking algorithm for digital image based on DCT and SVD is proposed and demonstrates that the watermarking is robust to the common signal processing techniques such as JPEG compressing noise and low pass filter. Kim et al. [5], furthermore, introduced a blind DWT-SVD watermarking scheme only requiring a secret key in the detection phase. This scheme, in turn, is suitable for internet applications that have no any original cover to receivers. Ma and Shen [6] also proposed a blind watermark scheme based on SVD using Arnold chaos encryption for performing the watermark. With the SVD technology, the pixel value of the watermark was subsequently embedded into the blocks of the largest singular value by quantization. By so doing, it enabled to detect the watermark without any original image. In [16], the proposition of a blind watermarking scheme was by using the wave atom; while in [17] it was by using the new non-tensor product wavelet filters banks constructed using a number of special symmetric matrices. This, as a result, enabled to capture the singularities in all directions.

Makhloghi et al. [7] conducted a research on digital image watermarking using SVD in order to obtain a watermark robust towards several attacks. Modaghegh et al. [8] proposed an adjustable watermarking method based on SVD, the parameters of which were adjusted using the GA in consideration of image complexity and attack resistance, and in the change of the fitness function. Wang and Min [9] proposed a blind watermarking algorithm for color images based on SVD in DWT domain. Here, the blue component of the original color image was decomposed with DWT and the low-frequency coefficients were then transformed by block-SVD. Subsequently, a binary watermark, scrambled by logistic chaotic, was embedded by quantizing the singular values of primitive image. Here, the performance of the watermark extraction was extracted without any original image. Tong et al. [10] proposed a blind digital image-watermarking scheme based on SVD and FastICA algorithm. According to the favorable stability property of singular value, the watermark is inserted into the singular values of the image's DCT coefficients, regarded as two sources, mixed through the instantaneous mixing model of ICA. Meanwhile, the FastICA algorithm is introduced in an extraction procedure through which the watermark can be efficiently derived, even with the unknown original image and the mixing procedure.

Zhao and Ho [11] have resulted in a method of digital image watermark using DCT. Agarwal and Prabhakaran [18] with the basic idea to find a cluster tree from the clusters of 3-D points proposed a robust blind watermarking mechanism for building generic copyright schemes for 3-D models. The technique, when applied to 3-D meshes, also achieved robustness against retriangulation and progressive compression techniques. Lin et al. [12,13] presented a blind watermarking method using a maximum wavelet coefficient quantization. The wavelet coefficients of a host image were grouped into blocks of variable size. Lin et al. in this method embedded a watermark in different sub-bands and used each block to embed either the watermark bit 0 or the watermark bit 1.

Even though some of the researches mentioned above have ever used the genetic algorithm based hybrid DCT-SVD technique, none of them has conducted a research using hybrid DCT-SVD technique for the type of information about the blind watermark and optimizing the value of singular factor of watermark using genetic algorithm in the e-government document images. Therefore, a new combined blind copyright protection scheme for E-government document images is proposed in this paper. Several existing schemes have been fairly compared in order to strengthen the statement that the proposed scheme comes to be a new combination scheme.

In Table 1, the proposed scheme is compared to other related schemes proposed in Makhloghi et al. [7], Lin et al. [13], You et al. [17] and Zhao and Ho [11], respectively. Table 1 summarizes the classification of five related watermarking schemes. The watermarking schemes are classified based on the following criteria: (1) information type of watermark, (2) domain type (e.g. class and description), (3) watermark type, and (4) typical uses of watermarks. From Table 1, it is found that all watermarking schemes for comparison are having similarity in four aspects; those are the information type as a blind watermarking scheme, the domain type as a transform domain, the watermark type as visual one, and the typical uses of watermarks as the copyright protection.

Afterwards, the significant differences with the reference [3] are listed as follows:

Table 1
The classification of five related watermarking schemes.

The criterion	Information type of watermark	Domain type		Watermark type	Typical uses of watermarks
		Class	Description		
Proposed Scheme	Blind	Transform	SVD-DCT based on GA	Visual watermark	Copyright protection
Makhloghiet al. [7]	Blind	Transform	SVD	Visual watermark	Copyright protection
Lin et al. [12]	Blind	Transform	SD-WCQ	Visual watermark	Copyright protection
You et al. [17]	Blind	Transform	DNWT and SD-DNWT	Visual watermark	Copyright protection
Zhao and Ho [11]	Blind	Transform	Wavelet-Based Contourlet Transform (WBCT)	Visual watermark	Copyright protection