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

a. Different types of watermark information, where the proposed method uses the blind watermark, while Ref. [3] uses the non-blind one.
b. Differences in the process of modifying the singular values of DCT-transformed host image on each area. This process can be clearly seen in Eq. (9).
c. The proposed scheme uses a 128×512 original image and 128×128 watermarks. Meanwhile, Ref. [3] uses a 256×1024 original image and 256×256 watermark.
d. The use of the types of attacks and their various scales (e.g. in Gaussian noise attack, the used scales are 1.5, 2.5, 3, 4.5, and 5, respectively).

3. The proposed watermarking scheme

This paper in turn is to present an efficient blind copyright protection for e-government document images through a combination of discrete cosine transform (DCT) and singular value decomposition (SVD) based on genetic algorithm (GA). The use of a blind watermarking scheme is in accordance with the considerations of the excellence of the blind scheme compared to the other schemes and its suitability for internet applications without any original cover to receivers.

Two-dimensional DCT technique and SVD technique are used in this proposed scheme. The technique of DCT refers to a technique converting a signal to be the elementary frequency components [3]. The formula of DCT technique is

$$c(r,s) = \alpha(r).\alpha(s)\sum_{x,y=0}^{N-1}\sum\left\{f(x,y).\cos\left[\frac{(2x+1)\pi r}{2N}\right]\cdot\cos\left[\frac{(2y+1)\pi s}{2N}\right]\right\} \tag{1}$$

Then, the inverse DCT is stated in Eq. (2):

$$f(x,y) = \sum_{x,y=0}^{N-1}\sum\left\{\alpha(r).\alpha(s).c(r,s).\cos\left[\frac{(2x+1)r\pi}{2N}\right]\cdot\cos\left[\frac{(2y+1)s\pi}{2N}\right]\right\} \tag{2}$$

SVD technique refers to a significant factorization in the complex matrix applied in many applications in the image processing and statistics. The formula of SVD can be seen in Eqs. (3)–(5):

$$Av_i = \sigma_i u_i \tag{3}$$

$$\text{becomes } AV = U\sum \tag{4}$$

$$\text{or } A = U\sum V^T \tag{5}$$

Here, U and V are unitary (orthogonal), Σ is the SV of A. $\sum = diag(\lambda_1, \lambda_2, \ldots, \lambda_m)$. m is the rank of matrix A, so $A = U_1.\lambda_1.V_1 + \cdots + U_m.\lambda_m.V_m$.

Subsequently, the hybrid DCT-SVD is combined from the listed techniques. The technique of combining DCT and SVD will advantageously not only make more resistant to various attacks but also can improve the performance, security and robustness of a document image. Furthermore, we use the genetic algorithm to find the optimization scaling factor of watermark image for the hybrid DCT-SVD scheme. Especially, GA has several advantages, as it, like other meta-heuristics, is particularly useful for the problems in complex, large, and irregular optimization. The performance of GA is empirical, requiring statistical verification [3].

The processes of the proposed watermarking scheme can be seen in Fig. 1; Fig. 1 consists of watermark embedding and watermark extraction processes.

3.1. Watermark embedding process

The first step of the watermark-embedding process is to apply DCT to the entire host image A: $A_d = dct(A)$, where A_d is the DCT-transformed host image of A, and A_d consists of r rows and c columns. In Step two, scan the DCT coefficients into 4 areas B1, B2, B3 and B4 respectively in the zigzag manner:

$$t = zigzag(A_d) \tag{6}$$

Let l be the length of DCT-transformed host image in each area: $l = \frac{(r \times c)}{4}$. Let A_d^j be an array to store all DCT coefficients of DCT-transformed host image in each area: $A_d^j = convert\_two(t(l(j-1)+1 : (j \times l)))$, where t is obtained from Eq. (6), *convert_two* is a function to convert the one-dimensional array t into a two-dimensional array of size $r' \times \frac{c'}{4}$, and j = 1, 2, 3, 4. For Step three, perform SVD operation on A_d^j for each area of B1, B2, B3 and B4, respectively:

$$A_d^j = U_d^j S_d^j V_d^{jT} \tag{7}$$

where $U_d^j S_d^j V_d^{jT} = svd(A_d^j)$ and j = 1, 2, 3, 4.

In Step four, perform SVD operation on W_d to obtain the DCT-transformed watermark image:

$$W_d = U_{w_d} S_{w_d} V_{w_d}^T \tag{8}$$

where $U_{w_d} S_{w_d} V_{w_d}^T = svd(W_d)$.

The following steps are to insert the watermark to each area. In Step five, modify the singular values of DCT-transformed host image on each area with the quantizing value [4,8]:

$$X_d^j = S_d^j(1,1) \bmod G \tag{9}$$

where $S_d^j(1,1)$ is the singular values of DCT-transformed host image on the first element of the maximum singular value of matrix in each area; G is the quantizing value obtained from Step six; $S_d^j(1,1)$ is quantized by G to get minimum changes in the image. The value of the obtained G must be accurately in line with the specification of an image both to obtain a maximum or minimum resistance towards a kind of attack and to obtain the minimum perceptibility.

The value of watermark W_d is a binary image; the process of watermark embedding involves two cases: embedding the pixel value '1' and embedding the pixel value '0'. When $W_d = 0$, it will be embedded as follows:

If $(X_d^j < 3G/4)$, then $S_d'^j(1,1) = S_d^j(1,1) + G/4 - X_d^j$else $S_d'^j(1,1) = S_d^j(1,1) + 5G/4 - X_d^j$.

When $W_{dct} = 1$, it will be embedded as follows:

If $(X_d^j < 3G/4)$, then $S_d'^j(1,1) = S_d^j(1,1) - G/4 + X_d^j$else $S_d'^j(1,1) = S_d^j(1,1) + 3G/4 + X_d^j$.

In Step six, decide the optimal of quantizing value G using Genetic Algorithm for each area. For Step seven, we obtain the modified DCT coefficients in each area.

$$A_d'^j = U_d^j S_d'^j V_d^{jT} \tag{10}$$

In Step eight, modify the coefficients back to their original positions, and then In Step nine, perform IDCT on AM_d^j calculated in Step 8 to obtain the watermarked image:

$$AM_d^j = dezigzag\left(A_{dct}'^j\right) \tag{11}$$

where *dezigzag* is an inverse operation of *zigzag*.

In summary, the process of watermark embedding takes 9 major steps. Step 1 is by applying DCT to the entire host image to obtain the DCT-transformed host image. In Step 2, the DCT-transformed host image is divided into four areas. Subsequently, Step 3 and Step 4 perform SVD operation on the DCT-transformed host image for each area and DCT-transformed watermark image, respectively. The remaining 5 steps are then used to insert watermark in each area. The combination of DCT and SVD (hybrid DCT-

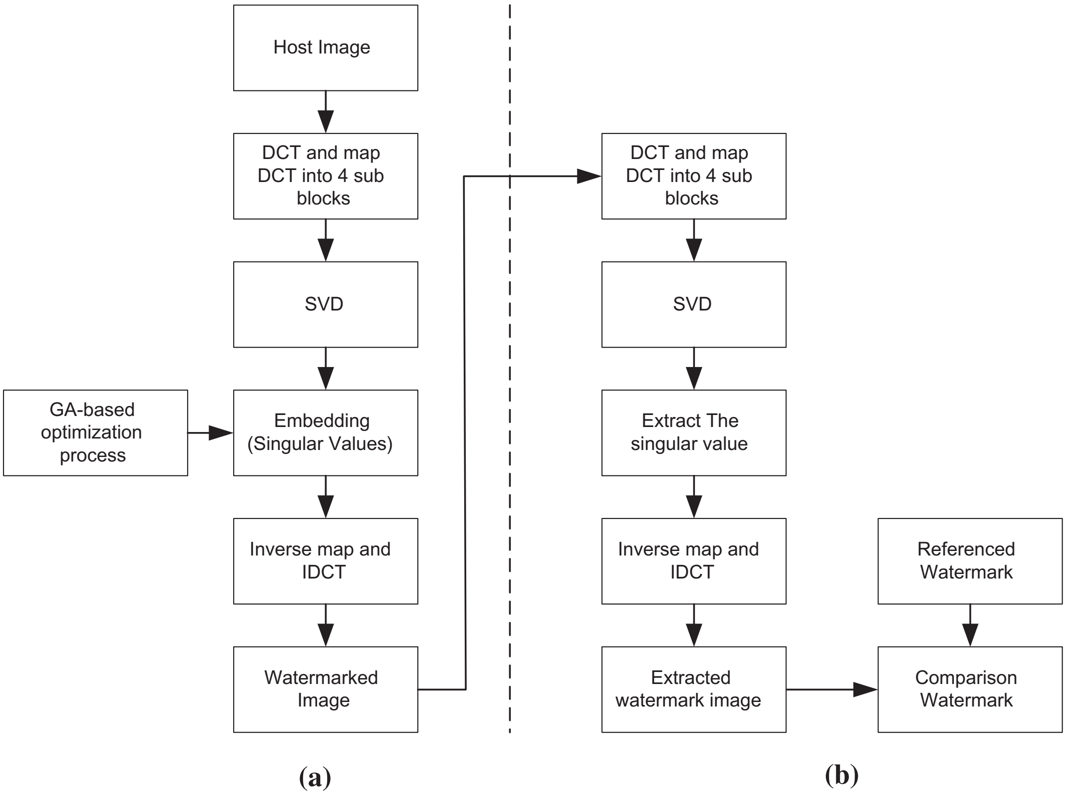
Host Image
DCT and map DCT into 4 sub blocks
SVD
GA-based optimization process
Embedding (Singular Values)
Inverse map and IDCT
Watermarked Image
DCT and map DCT into 4 sub blocks
SVD
Extract The singular value
Inverse map and IDCT
Referenced Watermark
Extracted watermark image
Comparison Watermark
(a)
(b)

Fig. 1. The watermarking processes: (a) Watermark embedding and (b) Watermark extraction.

SVD scheme) not only can make the watermarked image more resistant to various attacks but also can improve the performance, security and robustness of the watermarked image.

During Step 5, the singular value of DCT-transformed host image is modified on each area using the quantizing value G for determining the robustness of the proposed hybrid DCT-SVD scheme in which the watermark must be resistant towards the little change and any various attacks and unbreakable. To achieve these, the robustness of the proposed scheme must be minimized and maximized by changing the value of G. By doing so, the robustness of image will also change based on certain attacks. The relationship between the value of G and the robustness is not linear in that both of them rely on the different criteria such as the type of attacks and image block complexity. A certain value of G can result in a higher level of resistance for a certain block but it can also result in a lower level of resistance for other blocks. With the existence of the block condition that is more influenced and less influenced by the attacks, it makes the condition difficult and of course this condition will also be different depending on the specification of each image. Hence, one of the best solutions for this condition is by obtaining the accurate value of G for each specification of image to obtain the maximum and minimum resistance towards a type of attack and by obtaining the minimum perceptibility.

In the proposed scheme, in order to obtain the accurate value of G, it is done by optimizing the value of G using genetic algorithm that is obtained through Step 6. In Step 7, the modified DCT coefficient is obtained in each area. In Step 8, the coefficients are modified back to their original positions. Finally, in Step 9, IDCT on AM_d^j calculated in Step 8 is performed to obtain the watermarked image.

3.2. Watermark extraction process

The first step of the watermark-extraction process is to apply DCT to the watermarked image A: $A'_d = dct(A')$, where A'_d consists of r' rows and c' columns. In Step two, scan the DCT coefficients into 4 areas of B1, B2, B3 and B4, respectively in the zigzag manner:

$$t = zigzag(A'_d) \tag{12}$$

Let l' be the length of DCT- transformed host image in each area: $l' = \frac{(r' \times c')}{4}$. Let A'^j_d be an array to store all DCT coefficients of DCT-transformed host image in each area: $A'^j_d = t(l'(j-1)+1 : (j \times l'))$, where t is obtained from Eq. (12), and *convert_two* is a function to convert the one-dimensional array t into a two-dimensional array of size $r\prime \times \frac{c\prime}{4}$, and j = 1, 2, 3, 4.

In Step three, perform SVD operation on A'^j_d for each area:

$$A''^j_d = U'^j_d S''^j_d V'^{jT}_d \tag{13}$$

where $U'^j_d S''^j_d V'^{jT}_d = svd\left(A'^j_d\right)$ and j = 1,2,3,4.

In Step four, get the singular values from each area and extract the watermark:

$$X'^j = S'^j_d(1,1) \bmod G \tag{14}$$

If $\left\{X'^j \leqslant \frac{G}{2}\right\}$, $S^j_W = 0$, Else $S^j_W = 1$

In Step five, construct the DCT coefficients for 4-visual watermarks and apply IDCT to 4-visual watermark W'^j:

$$W'^j = A^j_w S^j_w V^{jT}_w \tag{15}$$

3.3. Optimization process based on genetic algorithm

Referring to [3,4,8], the optimal of quantizing value G is going to be found using GA as described in Step 6.

1. The genetic algorithm method is for the optimality of quantizing value G based on the mean of the value of watermark W_d, *li* as the minimum scaling factor and *ui* as the maximum one.

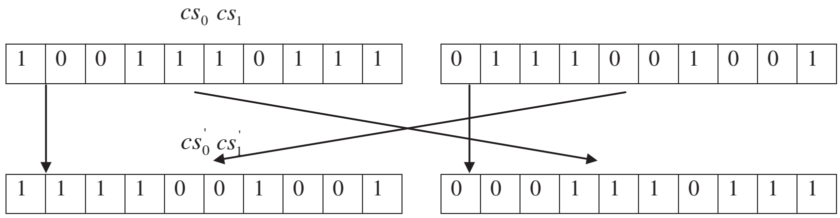

Fig. 2. The crossover process of chromosomes.

Here, the values of lower and upper interval of scaling factor for areas 1 to 4 are (−0.99, −0.01), (0.01, 0.99), (0.01, 0.99), and (0.01, 0.99) respectively.

2. The application of the initialization of population is to create a population of chromosomes and randomly initiate the vectors for chromosomes in each block. The population consists of a number of chromosomes in population (NcPop) and a number of genes in the chromosome (NumGen). Each of NcPop generates the value of G, multiplies NcPop and NumGen to get the G value, and inserts watermark with the calculated G in each block.
3. The application of the evaluation step is to evaluating each individual's fitness in which it will involve the roulette-wheel method to generate offspring. In this case, the highest fitness value of parent generation will produce one or more offspring.
4. This study also uses two genetic operators – crossover and mutation. The crossover stage is to mate two chromosomes for producing the next generation, for example by assuming two following chromosomes, namely cs_0 and cs_1 in Fig. 2.

From Fig. 2, suppose that the crossover point is randomly selected at the first gene before swapping the second parts of both chromosomes after the first gene. On the other hand, the mutation step is for preventing a premature convergence to local optimal by randomly sampling the number of genes. It can be done by altering one or more genes with the mutation probability.

4. Experiment results

The gray-scale image method is used in which the host images are the header of e-government document image, man, and Lena, whereas the watermark images are the logo image of Indonesian Institute of Sciences, peppers, and boat shown in Fig. 3(a) and (b) respectively. The corresponding sizes of those host and watermark images are 128 × 512 and 128 × 128, respectively.

The selection of tuning parameters includes population size, crossover rate, and mutation rate, the values of which are optimized to be 30, 0.8, and 0.01 respectively. Meanwhile, other tuning parameter, so-called the generation size, will be in a design ranging from 1 to 60 as the initial input and each number has a number of different evaluation function values.

Following that, several kinds of attacks on the watermarked image are performed to observe watermark robustness. In this case, the watermark from attacked image is subsequently extracted and compared to the original watermark. To measure the quality of the watermarked image, we have used the peak signal to noise ratio (PSNR) criteria as defined in Eq. (16).

To measure the objective function values, we, further, have used the minimum square error (MSE) as defined in Eq. (17):

$$PSNR = 10 \cdot \log_{10}(255^2/MSE) \tag{16}$$

$$MSE = \frac{1}{MN\sum_{x=1}^{M}\sum_{y=1}^{N}(A(x,y) - A'(x,y))^2} \tag{17}$$

where both $I(x,y)$ and $J(x,y)$ represent the gray-values of the host and the watermarked images and each of size $M \times N$.

For the verification of the watermark existence, a fitness value function as defined in Eq. (18) is used with a correlation coefficient between the host and the extracted watermark to obtain the normalized cross-correlation value (NC value):

$$f_k = \left(\frac{corr_I(A_w, A)}{\sum_{k=1}^{n}(1 - corr_w(W, W_k^*))}\right) \times n \tag{18}$$

where f_k is the fitness function of kth population element, A is the original image, and W is the watermark image. Furthermore, W_k^* represents the extracted watermark from A_w and n represents the number of attacks. The function of $corr$ is to represent a correlation between two input matrixes; consisting of $corr_I$ and $corr_w$. In this case, the lesser the $corr_I$, the lesser the perceptibility will be obtained; and the greater the $corr_w$, the more robustness will be obtained. Among the defined fitness functions, the third converges faster and results in the suitable G_s.

Finally, the fitness function of each population element (f_k) is sorted and the crossover and mutation operator will be executed then. Mutation operator is to produce a number of simple changes and reconstruct population. The procedure for other populations is repeated.

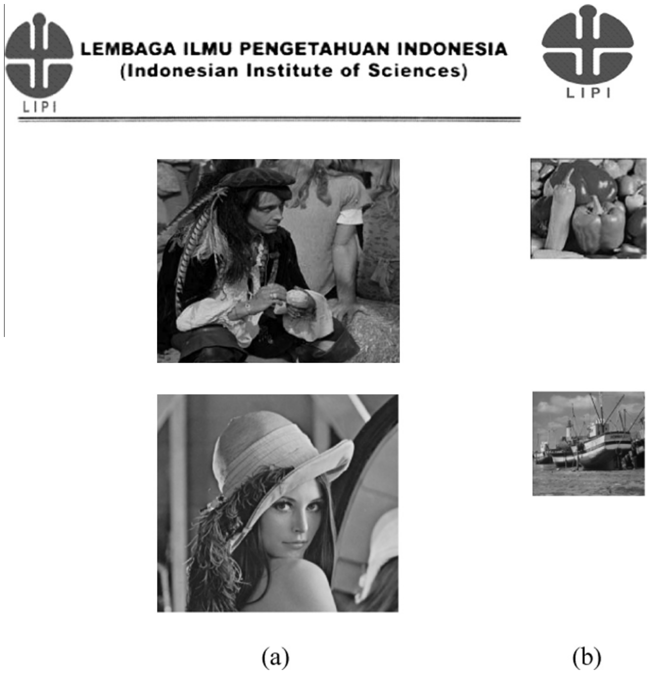
LEMBAGA ILMU PENGETAHUAN INDONESIA
(Indonesian Institute of Sciences)
LIPI
LIPI
(a)
(b)

Fig. 3. (a) Host images: The Indonesian Institute of Sciences; Man; Lena, (b) Watermark images: Logo of LIPI; Peppers; Boat.

4.1. The results of the proposed scheme

In this experiment, the use of several types of attacks, which include Gaussian noise, Rotation, Scaling, Cropping, Median filtering, Average filtering, JPEG compression and Salt and pepper noise is to verify the visual quality and the robustness of the proposed method. Under those attacks, it is found that the PSNR and the NC value of the extracted watermark from each area with different attacks (e.g. Gaussian noise attack) and various scales (1.5, 2.5, 3, 4.5, and 5) are the parameter values indicating the better visual quality and the robustness as tabulated in Table 2.

4.2. The proposed scheme in comparison to other related watermarking schemes

The experimental result that is the NC value, obtained from the proposed scheme is compared to other related blind watermarking schemes in order to emphasize the viability of the proposed scheme. By means of the comparison in NC value, all the related watermarking schemes are being evaluated and compared by the same types of attacks. In the following discussion, the NC value obtained by each scheme is compared based on the same types of

Table 2
Experiment results under various attacks.

Types of attacks	The host and watermark images	NC and PSNR values					
Gaussian noise		Variances	1.5	2.5	3	4.5	5
	IIS[a]	NC	0.5891	0.5931	0.5942	0.6007	0.6064
		PSNR	22.2400	19.1768	17.9199	15.1241	14.4094
	Man	NC	0.7630	0.7624	0.7507	0.7444	0.7197
		PSNR	27.1595	25.5937	22.1176	21.2573	18.4623
	Lena	NC	0.6990	0.6984	0.6980	0.6949	0.7282
		PSNR	12.6069	11.4914	13.3580	14.3326	15.4463
Rotation		Degree	−0.25	0.25	0.30	0.45	2.25
	IIS	NC	0.7621	0.7630	0.7624	0.7507	0.7505
		PSNR	27.1309	27.1595	25.5937	22.1176	12.2175
	Man	NC	0.7242	0.7505	0.7266	0.7349	0.7329
		PSNR	16.4937	12.2175	18.4558	16.4954	12.2194
	Lena	NC	0.7630	0.7185	0.7407	0.7130	0.7022
		PSNR	30.4355	31.9792	32.3599	27.4857	18.0816
Scaling		Scale	0.5	2	256–256	512–256	256–512
	IIS	NC	0.7863	0.7651	0.7449	0.7753	0.7076
		PSNR	19.2677	25.6074	20.6664	36.6070	26.1317
	Man	NC	0.7621	0.6064	0.5797	0.5891	0.5889
		PSNR	27.1309	14.4094	23.787	22.24	20.7072
	Lena	NC	0.7327	0.6981	0.7655	0.7023	0.7863
		PSNR	40.6394	35.0088	39.3277	28.5435	38.7886
Cropping		Size	1/2	1/3	1/4	1/5	1/8
	IIS	NC	0.7479	0.7426	0.7679	0.7909	0.8012
		PSNR	3.4831	2.2540	1.7602	1.4798	1.0832
	Man	NC	0.7863	0.7651	0.7449	0.7479	0.7426
		PSNR	19.2677	25.6074	26.1317	24.6664	24.6660
	Lena	NC	0.6962	0.7051	0.7364	0.7879	0.7590
		PSNR	7.8626	6.9829	6.6478	6.4764	6.3010
Median filtering		Size	(2 × 2)	(3 × 3)	(4 × 4)	(7 × 7)	(9 × 9)
	IIS	NC	0.7268	0.6788	0.7016	0.6931	0.7764
		PSNR	19.5268	21.1022	17.3960	15.7158	14.7561
	Man	NC	0.7679	0.7459	0.7449	0.6670	0.7909
		PSNR	1.7602	8.3192	4.6660	2.6604	1.4798
	Lena	NC	0.6698	0.6706	0.7172	0.7370	0.7764
		PSNR	33.0406	26.0592	26.3936	26.7044	24.8188
Average filtering		Size	(3 × 3)	(5 × 5)	(7 × 7)	(9 × 9)	(11 × 11)
	IIS	NC	0.7906	0.7600	0.7916	0.8000	0.8226
		PSNR	20.7285	17.1736	16.4224	15.7905	15.4435
	Man	NC	0.7459	0.7449	0.6670	0.8012	0.7268
		PSNR	11.0096	10.6600	8.4666	16.0832	19.5268
	Lena	NC	0.7571	0.7043	0.6092	0.5384	0.5165
		PSNR	30.8947	26.7990	24.8350	23.5334	22.5701
JPEG compression		Variances	10	20	30	35	50
	IIS	NC	0.6631	0.6680	0.6754	0.6801	0.6862
		PSNR	27.8061	30.8862	33.1465	34.0282	36.0124
	Man	NC	0.6788	0.7016	0.6931	0.7764	0.7906
		PSNR	21.1022	17.3960	15.7158	14.7561	20.7285
	Lena	NC	0.7240	0.7309	0.7215	0.7122	0.7041
		PSNR	28.4989	31.0385	32.4146	32.9435	34.2733
Salt and pepper and noise		Density parameter	0.01	0.02	0.08	0.18	0.2
	IIS	NC	0.5872	0.5678	0.5408	0.5297	0.5294
		PSNR	23.2051	20.4349	14.2333	10.7930	10.3109
	Man	NC	0.7600	0.7916	0.8000	0.8226	0.6631
		PSNR	17.1736	16.4224	15.7905	15.4435	27.8061
	Lena	NC	0.5674	0.5529	0.5369	0.5321	0.5306
		PSNR	25.2018	22.6194	16.4450	12.9105	12.4662

[a] IIS is Indonesian Institute of Sciences.

Table 3
The comparison of NC values for existing watermarking schemes.

JPEG compression						*Gaussian noise*				
[ps[a]]	[3]	[7]	[11]	[13]		[ps]	[3]	[7]		
0.7309	0.7403	0.5544	0.45	0.68		0.7282	0.6049	0.7209		
Rotation						*Scaling*				
[ps]	[3]	[7]	[11]	[13]	[17]	[ps]	[3]	[7]		
0.7630	0.7475	0.7209	0.13	0.67	0.76	0.7863	0.5721	0.6417		
Cropping						*Median filtering*				
[ps]	[3]	[7]	[13]	[17]		[ps]	[3]	[11]	[13]	[17]
0.7364	0.9090	0.5544	0.70	0.55		0.7764	0.6004	0.28	0.74	0.45
Average filtering						*Salt and pepper noise*				
[ps]	[3]	[7]	[11]	[13]		[ps]	[3]			
0.7571	0.5577	0.5595	0.5400	0.7500		0.5674	0.5496			

[a] ps is the proposed scheme.

attacks. In such comparison, the same attack types are applied to both the proposed scheme and the specific related one.

Table 3, for instance, discussed a comparison between the proposed scheme with those of Rosiyadi et al. [3], Makhloghi et al. [7], Zhao and Ho [11], Lin et al. [13], and You et al. [17], where the attack types applied are JPEG compression, Gaussian Noise, Rotation, Cropping, Scaling, Median Filtering, Average filtering and Salt and pepper noise respectively with the host image of Lena and the watermark of Boat.

As seen from Table 3, the most of NC values for the proposed scheme under several types of attacks are higher than those reported by Rosiyadi et al. [3], Makhloghi et al. [7], Zhao and Ho [11], Lin et al. [13], and You et al. [17], respectively. Hence, this indicates that the improved performance of the proposed scheme has more robust against several types of attacks.

Subsequently, the good visual quality of images against several types of attacks is obtained through PSNR values. In other words, the proposed scheme is able to provide better imperceptibility, meaning that the watermark should not be visible under several kinds of attacks, where human eyes cannot distinguish the watermarked image from the host image [6].

5. Conclusions

An efficient blind copyright protection for e-government document images is presented. The proposed scheme is combined by the discrete cosine transform (DCT) and the singular value decomposition (SVD) based on the genetic algorithm (GA) using the quantizing value. It finally has been observed that the fitness value can be chosen from optimization process by genetic algorithm using the quantizing value to increase the visual quality and the robustness of the proposed scheme from several types of attacks in all frequencies. The image visual quality and the robustness against several types of attacks of the proposed scheme are quite good.

At this point, the host image is not needed in the watermark extraction process and the blind scheme is not only more useful than another one but also suitable for internet applications where the original cover is not available to receivers. For the sake of fairness, all comparisons are under the same types of attacks. The experiment results show that the proposed scheme outperforms to other related existing schemes. Further research possibly deals with the fragile watermarking scheme based on genetic algorithm.

Acknowledgments

This paper was developed on the PhD research in National Taiwan University of Science and Technology, and the basis of LIPI's competitive research entitled *e-government Development Framework-Based Open Source in 2007-2008, no contract 11:04/SK/KPPI/II/2007.*

References

[1] Chih-Chin Lai, Hsiang-Cheh Huang, Cheng-Chih Tsai, Image watermarking scheme using singular value decomposition and micro-genetic algorithm, in: International Conference on Intelligent Information Hiding and Multimedia, Signal Processing, IEEE-978-0-7695-3278-3, 2008, pp. 469–472.

[2] Veysel Aslantas, An SVD Based Digital Image Watermarking Using Genetic Algorithm, International Journal of Electronics and Communications (2007) 1–4.

[3] Didi Rosiyadi, Shi-Jinn Horng, Pingzhi Fan, Xian Wang, Muhammad Khurram Khan, Pan Yi, An efficient copyright protection scheme for e-government document images, IEEE Multimedia 19 (3) (2012) 62–73.

[4] Feng Liu, Ke Han, Chang Zheng Wang, A novel blind watermark algorithm based on SVD and DCT, in: Proceeding of IEEE International Conference on Intelligent Computing and Intelligent Systems (ICIS), Shanghai, 2009, pp. 283–286.

[5] Kyung-Su Kim, Min-Jeong Lee, Heung-Kyu Lee, Blind image watermarking scheme in DWT-SVD domain, in: Proceeding of Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP), Kaohsiung, 2008, pp. 477–480.

[6] Xiaohu Ma, Xiaofeng Shen, A novel blind grayscale watermark algorithm based on SVD, in: Proceeding of International Conference on Audio, Language and Image Processing (ICALIP), Shanghai, 2008, pp. 1063-1068.

[7] M. Makhloghi, F. Akhlaghian, H. Danyali, Robust digital image watermarking using singular value decomposition, in: IEEE International Symposium on Signal Processing and Information Technology, 2010, pp. 219–224.

[8] H. Modaghegh, R.H. Khosravi, T. Akbarzadeh, A new adjustable blind watermarking based on GA and SVD, in: Proceeding of International Conference on Innovations in Information Technology (IIT'09), Al Ain, 2009, pp. 6–10.

[9] Hui-Qin Wang, Zhao Min, A blind watermarking algorithm for color image based on singular value quantization, digital content, in: Proceeding of 6th International Conference on Multimedia Technology and its Applications (IDC), Seoul, 2010, pp. 59–62.

[10] Ming Tong, Wei Feng, Hongbing Ji, A robust geometrical attack resistant digital image watermarking based on fast ICA algorithm, in: Congress on Image and Signal Processing (CISP), China, 2008, pp. 655–659.

[11] X. Zhao, A.T.S. Ho, An Introduction to Robust Transform Based Image Watermarking Techniques, Intelligent Multimedia Analysis for Security Applications, Springer, 2010. pp. 337–364.

[12] Wei-Hung Lin, Yuh-Rau Wang, Shi-Jinn Horng, Yi Pan, A blind watermarking method using maximum wavelet coefficient quantization, Expert Systems with Applications 36 (9) (2009) 11509–11516.

[13] W.H. Lin, S.J. Horng, T.W. Kao, P. Fan, C.L. Lee, Y. Pan, An efficient watermarking method based on significant difference of wavelet coefficient quantization, IEEE Transactions on Multimedia 10 (5) (2008) 746–757.

[14] W.H. Lin, S.J. Horng, T.W. Kao, R.J. Chen, Y.H. Chen, C.L. Lee, T. Terano, Image copyright protection with forward error correction, Expert Systems with Applications 36 (9) (2009) 11888–11894.

[15] Dilip Kumar Sharma, Vinay Kumar Pathak, G.P. Sahu, Digital Watermarking for Secure e-government Framework, Computer Society India, 2007. pp. 182–191.

[16] H.Y. Leung, L.M. Cheng, Robust blind watermarking scheme using wave atoms, Lecture Notes in Computer Science 6526 (2011) 148–158.

[17] Xinge You, Liang Du, Yiu-ming Cheung, Qiuhui Chen, A blind watermarking scheme using new nontensor product wavelet filter banks, IEEE Transaction on Image Processing 19 (12) (2010) 3271–3284.

[18] P. Agarwal, B. Prabhakaran, Robust blind watermarking of point-sampled geometry, IEEE Transaction on Information Forensics and Security 4 (1) (2009) 36–48.