A robust digital image watermarking scheme based on singular value decomposition (SVD) and a tiny genetic algorithm (Tiny-GA) is proposed in this paper. Previous works have shown that both one-way and non-symmetric properties of SVD make it desirable for watermarking techniques. The produced singular values are very stable and vary very little under various image processing operations or attacks. In the proposed scheme, the singular values of a cover image are modified by multiple scale factors to embed the watermark image. Since the values of scale factors determine the watermark strength; therefore, we use the Tiny-GA to search the proper values in order to improve the visual quality of the watermarked image and the robustness of the watermark. Experimental results demonstrate that our scheme is able to withstand a variety of image processing attacks.

© 2011 Elsevier Inc. All rights reserved.

1. Introduction

Owning to the rapid development of computer networks and Internet, the use of multimedia data has resulted in fast and convenient exchange of digital information. Consequently, such applications have also raised concern about copyright issues and unauthorized modification and distribution of digital data. To achieve these issues, watermarking technology is adopted to solve these problems. Watermarking [7] is the process of inserting data into a multimedia element such as an image, audio, or video file. The embedded data can later be detected or extracted from the multimedia for identifying the copyright owner.

A basic watermarking algorithm, an image for example, consists of a cover image, a watermark structure, an embedding algorithm, and an extraction or detection algorithm. Several techniques have been proposed for multimedia protection. Among the proposed methods, much interest has focused on digital images [1,7,12,22]. According to the domain in which the watermark is inserted, these techniques are divided into two broad categories: spatial-domain and frequency-domain methods. Embedding the watermark into the spatial-domain component of the original image is the straightforward method. It has the advantages of low complexity and easy implementation. However, the spatial domain watermarking algorithms are generally fragile to image processing operations or other attacks. On the other hand, the representative frequency-domain techniques embed the watermark by modulating the magnitude of coefficients in a transform domain, such as discrete cosine transform (DCT), discrete Fourier transform (DFT), and discrete wavelet transform (DWT) [3,5,21]. Although frequency-domain methods can yield more information embedding and more robustness against many common attacks, the computational cost is higher than spatial-domain watermarking methods.

In the last few years, a singular value decomposition (SVD)-based watermarking technique and its variations have been proposed [10,18]. SVD is a mathematical technique used to extract algebraic features from an image. The core idea behind SVD-based approaches is to apply the SVD to the whole cover image or, alternatively, to small blocks of it, and then modify the singular values to embed the watermark. There are three advantages to employ SVD method in digital watermarking scheme: (1) the size of the matrices from SVD transformation is not fixed; (2) when a small perturbation is added to an image, large variation of its singular values (SVs) does not occur; and (3) SVs represent intrinsic algebraic image properties [18]. The aforementioned properties of SVD are very much desirable for developing watermarking algorithms that are particular robust to geometric attacks.

In general, the strength (energy) of the embedded watermark can be controlled by a scaling factor. The performance of the watermarking process highly depends on choosing a proper scaling factor. Ganic et al. [10] found that the scaling factor is set to be constant in some SVD-based studies. However, Cox et al. [7] argued that considering a single and constant scaling factor may not be applicable in some cases, and they suggest users can use multiple scaling factors instead of one. In this paper, we proposed an innovative image watermarking scheme by integrating SVD technique and the tiny genetic algorithm (Tiny-GA) [13]. The proper scaling factors are determined by the Tiny-GA. Experimental results show that the proposed approach is resistant against common image-
processing attacks, while it preserves the quality of the original image.

The rest of this paper is organized as follows. Section 2 reviews some SVD-based watermarking schemes proposed in the literature. Section 3 illustrates the proposed watermarking scheme. Simulations of our method with respect to attacks are conducted in Section 4. Finally, conclusions are given in Section 5.

2. Related works

In this section, some SVD-based watermarking schemes proposed in the past years are briefly reviewed.

Ganic et al. [10] presented a double watermarking scheme based on SVD that embeds the watermark twice. In the first layer, the cover image is divided into smaller blocks and a piece of the watermark is embedded in each block. In the second layer, the cover image is used as a single block to embed the whole watermark. The purpose of considering two layers to embed watermark is that layer one allows flexibility in data capacity, and layer two provides additional robustness to attacks.

Lee et al. [16] proposed an SVD-based image content authentication method with improved security is proposed. By embedding watermark into randomly ordered block, adjusting and dithering the quantized largest singular value of an image block, the proposed method is robust against VQ attack and is safe from histogram analysis attack.

Galagna et al. [6] introduced an image watermarking scheme based on the SVD compression. They divided the cover image into blocks and applied the SVD to each block. The watermark is embedded in all the non-zero singular values according to the local features of the cover image so as to balance embedding capacity with distortion.

Mohan and Kumar [19] presented a robust image watermarking scheme for multimedia copyright protection. In their work, the proposed method uses SVD domain and dither quantization for embedding the watermark in both D and U matrices obtained from SVD. In the proposed method, the largest singular values of the cover image and the coefficients of the U matrix are modified to embed the watermark.

Mohammad et al. [20] presented an SVD-based watermarking technique. This technique is an improved version of the SVD-based technique proposed by Liu and Tan [18]. The proposed technique is non-invertible and its main application is in protecting rightful ownership.

Basso et al. [4] proposed a block-based watermarking scheme based on SVD. The watermark is inserted by modifying the angles formed by the right singular vectors of each block of the original image.

3. Proposed watermarking scheme

In this section, the powerful numerical analysis SVD transformation and the concept of SVD-based watermarking are first introduced. The proposed watermarking scheme which utilizes the Tiny-GA to determine proper multiple SVs and to embed the watermark is then described. The block diagram of the proposed approach is shown in Fig. 1.

3.1. SVD-based watermarking

From the perspective of image processing, an image can be viewed as a matrix with nonnegative scalar entries. The SVD of an image \( A \) with size \( m \times m \) is given by \( A = USV^T \), where \( U \) and \( V \) are orthogonal matrices, and \( S = \text{diag}(\lambda_i) \) is a diagonal matrix of singular values \( \lambda_i \), \( i = 1, \ldots, m \), arranged in decreasing order. The columns of \( U \) are the left singular vectors, whereas the columns of \( V \) are the right singular vectors of the image \( A \). This process is known as the Singular Value Decomposition (SVD) of \( A \), and can be written as

\[
A = USV^T = \sum_{i=1}^{r} \lambda_i u_i v_i^T,
\]

where \( r \) is the rank of \( A \) (\( r \leq m \)), \( u_i \) and \( v_i \) are the left and right singular vectors, respectively. It is important to note that each SV specifies the luminance of the image, whereas the respective pair of singular vectors specify the intrinsic geometry properties of images. It was discovered that slight variations of SVs do not affect the visual perception of the cover image, which motivates the watermarking embedding through slight modifications of SVs in the segmented images [2].

According to description in Liu and Tan's method [18], the watermark embedding and extraction procedures can be described as follows:

- **Watermark embedding**: First, the SVD is employed in a cover image \( A \) to obtain \( U \), \( V \), and \( S \) three matrices. Second, a watermark image \( W \) is inserted into the diagonal matrix \( S \) and then apply SVD on a new matrix \( S + aW \) to obtain three matrices \( U_W \), \( S_W \), and \( V_W \), where \( a \) is the scaling factor which controls the strength of the watermark to be inserted. Finally, the watermarked image \( A_W \) is obtained by multiplying the matrices \( U_W \), \( S_W \), and \( V_W \). The aforementioned three steps can be expressed by the following mathematical notions:

\[
A = USV^T.
\]

![Fig. 1. The proposed watermarking scheme.](image-url)
Watermark extraction: If \( U_W, S, V_W, \) and the possibly distorted image \( A_W^* \) are given, a possibly corrupted watermark \( W^* \) can be extracted by reversing the above three steps,

\[
A_W^* = U_W^* V_W^T.
\]

Genetic operators: The selection operator which is also called lightweight evolutionary algorithm, stands for an evolutionary procedure with small efforts. In other words, the Tiny-GA is characterized by the following features: (1) small population size (like ten chromosomes), (2) little number of generations, and (3) a simple fitness. In contrast to the conventional GA which requires a large number of chromosomes in each population, the Tiny-GA can reduce the amount of computational effort required to achieve the most-fit solution. However, the small population is unable to maintain diversity for many generation. In order to overcome this problem, whenever the diversity of the population is lost, the population should be restarted. This periodic infusion of new genetic material allows the Tiny-GA to search the function space using a very small population. It will also keep the population from being dominated by designs corresponding to a local minimum found early in the optimization process [9].

When we use the Tiny-GA to solve the problem, the following components must be considered: (1) a genetic representation of solutions to the problem, (2) one way to create the initial population of solutions, (3) an evaluation function that rates all candidate solutions to the problem, (4) genetic operators that alter genetic composition of children during reproduction.

3.2. Optimized scale factors

The pixel values or the transform domain coefficients of the cover image can be appropriately modified to embed a watermark invisibly. Before embedding process, the watermark can be scaled by a scaling factor to control the watermark strength [7]. However, determining the proper values of multiple scaling factors is a difficult problem, especially for different types of cover and watermark images. In some cases, the choice of them may be dependent on some general assumption. Therefore, a systematic mechanism is required for this purpose. Here we use the Tiny-GA to systematically determine these values without making any assumption.

The Tiny-GA, which is also called lightweight evolutionary algorithm, is the survival arbiter for chromosomes. The main objective of developing an image-watermarking technique is to satisfy both imperceptibility and robustness requirements. To achieve this objective, we define the fitness function as the function of imperceptibility and robustness,

\[
\text{fitness} = f(\text{imperceptibility}, \text{robustness}).
\]

The imperceptibility means a measure that the perceptual difference between the cover and watermarked images should be undistinguished by the human visual inspection. On the other hand, the robustness means a measure that an embedded watermark can be extractable even if common signal processing operations are applied to the watermarked image. The mathematical formulas for the aforementioned two measures are defined as follows:

\[
\text{imperceptibility} = NC(A, A_W^*),
\]

\[
\text{robustness} = \frac{N}{\sum_{i=1}^{N} NC(W, W_i^*)}.
\]

\[
NC(X, \hat{X}) = \frac{\sum_i \sum_j X(i, j) \hat{X}(i, j)}{\sqrt{\sum_i \sum_j X(i, j)^2} \sqrt{\sum_i \sum_j \hat{X}(i, j)^2}}.
\]

where \( A \) and \( A_W^* \) represent the cover and the watermarked images, respectively; \( W \) and \( W_i^* \) indicate the watermark and the extracted watermark image, respectively; \( NC \) denotes the two-dimensional normalized correlation value; \( X \) and \( \hat{X} \) stand for the original and the processed images; and \( N \) represents the number of attacking methods. Therefore, the fitness for the \( i \)-chromosome is given by

\[
\text{fitness} = \text{robustness} - \text{imperceptibility}.
\]

Since the proposed approach has to satisfy both requirements, the objective is to minimize the fitness function for achieving the optimal performance of a digital image watermarking scheme.

Genetic operators: The selection operator determines which chromosomes are chosen for mating and how many offspring each selected chromosome produces. We use the tournament selection scheme [8] in our approach because the time complexity of tournament selection is low. It does not require a global fitness comparison of all chromosomes in a population; therefore, it can accelerate the evolution process. Crossover operator aims at increasing the average quality of the population. We use the crossover operator proposed by Leung et al. [17] to swap genetic information and produce new chromosomes. Two chromosomes \( p_1 \) and \( p_2 \) are selected as parents and four chromosomes are generated according to the following mechanisms:

\[
\text{os}_1^1 = \frac{p_1 + p_2}{2}.
\]

\[
\text{os}_2^2 = (1 - w) \cdot p_{\text{max}} + w \cdot \text{min}(p_1, p_2),
\]

\[
\text{os}_3^3 = (1 - w) \cdot p_{\text{min}} + w \cdot \text{max}(p_1, p_2),
\]

\[
\text{os}_4^4 = \frac{1}{2}[(1 - w) \cdot (p_{\text{max}} + p_{\text{min}}) + w \cdot (p_1 + p_2)].
\]

\[
p_{\text{max}} = \left[\frac{\text{para}_{\text{max}}^I}{\text{para}_{\text{max}}^I} \cdots \frac{\text{para}_{\text{max}}^\text{vars}}{\text{para}_{\text{max}}^\text{vars}}\right],
\]

\[
p_{\text{min}} = \left[\frac{\text{para}_{\text{min}}^I}{\text{para}_{\text{min}}^I} \cdots \frac{\text{para}_{\text{min}}^\text{vars}}{\text{para}_{\text{min}}^\text{vars}}\right],
\]

where \( w \in [0, 1] \) denotes the weight to be determined by users (we set \( w = 0.5 \) in our approach), \( \text{max}(p_1, p_2) \) denotes the vector with each element obtained by taking the maximum among the corresponding element of \( p_1 \) and \( p_2 \). Similarly, \( \text{min}(p_1, p_2) \) gives a vector by taking the minimum value. Among the above four candidate offspring, the one with the smallest fitness value is used as the final offspring of the crossover operator.

Note that the mutation operator is not needed in the Tiny-GA, since enough diversity is introduced into the population every time the algorithm is restarted [14]. If more than half
of the chromosomes have the same fitness value, the restart strategy will be triggered. A few chromosomes are randomly generated to replace those chromosomes with the same fitness value. Also, the elitism strategy is required.

4. Experimental results

Several experiments were carried out to verify the validity of the proposed watermarking scheme. The image Lena with size $256 \times 256$ and a $64 \times 64$ gray-level image of Cameraman are used as the cover image and the watermark, respectively. These images are illustrated in Figs. 2(a) and (b). The related parameters used in the Tiny-GA about the experiments are as follows: the population size is 5, the maximum number of generation is 300, and the probability of crossover is 0.95.

4.1. Experiment I

In this experiment, we want to show that considering appropriate multiple scaling factors is necessary in order to obtain the highest possible imperceptibility and robustness of the watermarking scheme. To evaluate the robustness of the proposed approach, the watermarked image was tested against five kinds of image-processing attacks: (1) geometrical attack: cropping (CR) and rotation (RO), (2) noise attack: Gaussian noise (GN), (3) denoising attack: average filtering (AF), (4) format-compression attack: JPEG compression, and (5) image-processing attack: histogram equalization (HE) and darken (DK). The pure SVD-based watermarking scheme considering a single constant scaling factor [18] is also implemented for comparison.

Fig. 2(c) shows the watermarked version of the Lena image with PSNR 47.49 dB. The PSNR (peak signal-to-noise ratio), a measure of the quality of a watermarked image, is defined as follows,

$$\text{PSNR} = 10 \cdot \log_{10} \frac{255^2}{\text{MSE}},$$

$$\text{MSE} = \frac{1}{W \times H} \sum_{i}^{W} \sum_{j}^{H} (x_{ij} - x'_{ij})^2.$$  \hspace{1cm} (19) \hspace{1cm} (20)

Here, the notations $W$ and $H$ represent the width and height of an image, $x_{ij}$ is the pixel value of coordinate $(i, j)$ in an original image, and $x'_{ij}$ is the pixel value after the watermark embedding procedure. We can see that the watermarked image is not distinguishable from the cover image.

For comparing the similarities between the original and extracted watermarks, the two-dimensional normalized correlation (NC) value was employed. In the experiments, the values of the scaling factors are carried out with constant range from 0.02 to 0.08 with an interval of 0.02, and the results are illustrated in Table 1. The NC value can be anywhere between 0 and 1. In principle, if the NC value is closer to 1, the extracted watermark is getting more similar to the embedded one. From the results, it can be seen that the larger the scaling factor, the stronger the robustness of the applied watermarking scheme. Our approach can obtain higher NC value than [18], and this verifies that the proposed scheme achieves a good improvement on the robustness by considering multiple strength factors to embed the watermark.

In addition to quantitative analysis of the robustness of our approach, we also need the visual perceptions of the extracted watermarks. The distorted images after attacks and corresponding extracted watermarks are shown in Figs. 3(a)–(b), 4(a)–(b), 5(a)–(b), 6(a)–(b), 7(a)–(b), 8(a)–(b), and 9(a)–(b), respectively. From the experimental results, we find the even if the watermarked image has undergone severe physical distortions, the extracted watermark is still recognizable.

4.2. Experiment II

In this experiment, we compared the proposed scheme against the related SVD-based watermarking schemes [18,15] in their ability to withstand different types of attacks. The quality of the extracted watermark is determined by NC value. In [18], the authors apply the SVD to the entire cover image and embed the watermark in the diagonal matrix of the SVD transformation. The scaling factor which controls the watermark energy to be inserted is set to a single constant value in their method. In [15], the authors pro-

Table 1
NC values of extracted watermarks from different attacks.

<table>
<thead>
<tr>
<th>Method</th>
<th>CR</th>
<th>RO</th>
<th>GN</th>
<th>AF</th>
<th>JPEG</th>
<th>HE</th>
<th>DK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our approach</td>
<td>0.9948</td>
<td>0.9936</td>
<td>0.9735</td>
<td>0.9840</td>
<td>0.9951</td>
<td>0.9984</td>
<td>0.9995</td>
</tr>
<tr>
<td>Constant value</td>
<td>0.02</td>
<td>0.9858</td>
<td>0.9841</td>
<td>0.9609</td>
<td>0.9702</td>
<td>0.9830</td>
<td>0.9947</td>
</tr>
<tr>
<td>0.04</td>
<td>0.9856</td>
<td>0.9865</td>
<td>0.9634</td>
<td>0.9757</td>
<td>0.9865</td>
<td>0.9951</td>
<td>0.9963</td>
</tr>
<tr>
<td>0.06</td>
<td>0.9873</td>
<td>0.9868</td>
<td>0.9658</td>
<td>0.9733</td>
<td>0.9885</td>
<td>0.9953</td>
<td>0.9969</td>
</tr>
<tr>
<td>0.08</td>
<td>0.9896</td>
<td>0.9890</td>
<td>0.9677</td>
<td>0.9780</td>
<td>0.9900</td>
<td>0.9955</td>
<td>0.9971</td>
</tr>
</tbody>
</table>

Fig. 2. (a) The cover image, (b) watermark, and (c) the watermarked image.
posed a watermarking scheme based on SVD and the micro-genetic algorithm (μ-GA). In their method, the singular values of the cover image are modified by considering multiple scaling factors to embed the watermark. The μ-GA is used to efficiently search the proper values of scaling factors. In addition, we also implement a watermarking method which uses the simple genetic algorithm (SGA) [11] to find the appropriate multiple scaling factors. The NC values are listed in Table 2, and it is clear that the robustness performance of our proposed approach is superior to the other similar approaches.

5. Conclusions

In this paper, an image watermarking technique based on SVD and Tiny-GA has been proposed. The singular values of the cover image are modified to embed the watermark. The Tiny-GA offers a systematic way to consider the improvements of the scaling factors that are used to control the strength of the embedded watermark. With the proposed scheme, the embedded watermark can successfully survive after attacked by image-processing operations. Simulation results show that the proposed scheme outperforms the other similar works. Further work of extending the proposed approach with human visual systems and comparing the results with
Table 2
NC values obtained from different watermarking schemes under various attacks.

<table>
<thead>
<tr>
<th>Method</th>
<th>CR</th>
<th>RO</th>
<th>GN</th>
<th>AF</th>
<th>JPEG</th>
<th>HE</th>
<th>DK</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVD [18]</td>
<td>0.9896</td>
<td>0.9890</td>
<td>0.9677</td>
<td>0.9780</td>
<td>0.9900</td>
<td>0.9955</td>
<td>0.9971</td>
</tr>
<tr>
<td>SVD + SGA</td>
<td>0.9912</td>
<td>0.9903</td>
<td>0.9695</td>
<td>0.9806</td>
<td>0.9911</td>
<td>0.9963</td>
<td>0.9978</td>
</tr>
<tr>
<td>SVD + μ-GA [15]</td>
<td>0.9925</td>
<td>0.9917</td>
<td>0.9717</td>
<td>0.9819</td>
<td>0.9925</td>
<td>0.9971</td>
<td>0.9983</td>
</tr>
<tr>
<td>Our approach</td>
<td>0.9948</td>
<td>0.9936</td>
<td>0.9735</td>
<td>0.9840</td>
<td>0.9951</td>
<td>0.9984</td>
<td>0.9995</td>
</tr>
</tbody>
</table>

Fig. 9. (a) The darken image, and (b) watermark extracted from (a).

Acknowledgments

This work is supported by the National Science Council, Taiwan, under grant NSC 99-2221-E-390-035. The author would like to thank anonymous referees for their valuable comments and suggestions which led to substantial improvements of this paper.

References


Chih-Chin Lai received the B.S. degree in computer science and information engineering from the National Chiao Tung University, Hsinchu, Taiwan, in 1993, and the Ph.D. degree in computer science and information engineering from the National Central University, Jhongli, Taiwan, in 1999. He is currently an Associate Professor of the Department of Electrical Engineering, National University of Kaohsiung, Kaohsiung, Taiwan. His research interests include visual information computing, evolutionary computation, and information retrieval.