International Journal of Mechatronics, Electrical and Computer Technology

Vol. 4(10), Jan, 2014, pp. 98-110, **ISSN**: 2305-0543
Available online at: http://www.aeuso.org
© Austrian E-Journals of Universal Scientific Organization

- -

Providing a digital watermarking algorithm using genetic algorithm and SVD

H. Motameni and Zahra Ebrahimi
Islamic Azad University, Sari, Iran
*Corresponding Author's E-mail: *zahra.ebrahimi@chmail.ir*

Abstract

In this paper, a scheme suggested for watermarking of digital images that used a singular value decomposition (SVD) and genetic algorithm. The singular values derived from the SVD are resistant towards image processing attacks such as cutting, noise, rotation and... And have resistant capability. Using SVD, the eigenvalues of the original image extracted and changed using genetic algorithms. Then the process of watermark embedding is carried out. SVD is the ability to be reversed after watermarking, the watermark image from the original image be removed again. The experimental results show that this scheme is resistant against image processing included a montage of previous methods.

Keywords- watermarking, singular value decomposition, genetic algorithm.

1. Introduction

Nowadays, image processing refers to image processing subject that is a branch of computer science that represents pictures taken digital signal processing involved in a digital camera or scanned by the scanner from. Nowadays, the use of multimedia data and exchange of digital information are growing rapidly. As a result, many applications in relation to ideas such as copying and distributing unauthorized changes have been posed digital data [1]. To reach these goals watermarking and the problems they raised. In order to maintain security and privacy of data before transmission, or distribution, they must be protected. Access rights are controlled by user's entity.

Vol. 4(10), Jan, 2014, pp. 98-110, **ISSN**: 2305-0543
Available online at: http://www.aeuso.org
© Austrian E-Journals of Universal Scientific Organization

1.1. What is watermarking?

Watermarking is data insertion process in a multi-media element such as image, audio or video and embedded data can then be extracted from the original image.

Basic watermarking algorithm in a picture consisted of the following:

- The original image
- A watermarking structure
- An integrated algorithm is implemented
- An algorithm identifying or extracting

In general, a multimedia watermarking system is consisted of different components. The original image using watermarking algorithm and by its key is converted to latent image. So image watermarking by using the algorithm and key extracted is obtained from the original image. Furthermore, it is possible to break the system and obtain the components of multimedia attacks to be carried out. Many research projects have focused on the extraction efficiency of the watermarking algorithms and the algorithms are secure against attacks [2].

1.2. Objectives and requirements of watermarking

There are several watermarking applications, some of which including:

a. owner identification or preserving publication patent
b. transactional watermarks (fingerprinting) of different data of possibility of radar
c. Control copy operation
d. Broadcast Monitoring
e. Data Authentication
f. Indexing on pictures
g. Secret telecommunication and Data hiding

International Journal of Mechatronics, Electrical and Computer Technology

Vol. 4(10), Jan, 2014, pp. 98-110, **ISSN**: 2305-0543
Available online at: http://www.aeuso.org
© Austrian E-Journals of Universal Scientific Organization

1.3. The literature review

Lai in [1] proposed a scheme which used genetic algorithms and SVD to find the intensity of watermarking. Then using the watermarking or extracting formulas, values of the original image and the watermark is changing to carried out watermarking process and mining. Ganic et al [11] proposed a SVD-based two-level watermarking schemes that image watermark that is hidden again. In the first layer, the original image is divided into smaller blocks and each block is a piece of watermark image. In the second layer, the whole embedded watermark image is used as a block. In the dual approach, the first layer has more capacity and a second layer will create more resistance against attacks [1].

Lee et al [17] proposed a SVD-based image content authentication with improved security. With watermarking watermark in random blocks, with the largest amount of quantized by setting vague image of a block, the proposed method is resistant against attacks and against VQ histogram analysis is also safe[1]. Calagna et al [7] Introduced watermarking scheme based on SVD and compression. In this method, the original image is divided into blocks and each block is applied to the SVD. Watermark image of the local characteristics of original image embedded in all the non-zero values [1]. Mahan and Kumar in [20] offered the watermarking scheme for protection of multimedia copyright. In this method, the SVD and quantization range used for embedding watermark in obtained U and D from SVD. In this way, the largest single amount of watermark embedding the original image and the coefficient matrix U to be corrected [1].

Mohammad et al [21] proposed a SVD-based watermarking technique. This technique is an improved version of the SVD-based technique proposed by Liu and Tan was proposed at figure [19]. This method is not reversed and its main use is protection of legal property. Basso et al [5] have proposed scheme based on block scheduling. By changed angle of the watermark image inserted using the eigenvectors of each image block on SVD of watermark image [1]. Among various

Vol. 4(10), Jan, 2014, pp. 98-110, ISSN: 2305-0543
Available online at: http://www.aeuso.org
© Austrian E-Journals of Universal Scientific Organization

methods in this field, the proposed method applied in this study was based Lai. In this way, Intensity watermarking using the genetic algorithm is obtained. Then the original image and the watermark can be improved by using SVD and the watermarking is carried out. In our proposed method, unlike the method of Lai, in order to establish the integrity of all states in the algorithm, the convex combination is used to generate new offspring. Optimality conditions are studied rather than Lai.

2. Watermarking Algorithm

The watermarking algorithm structure is shown in Figure 1.

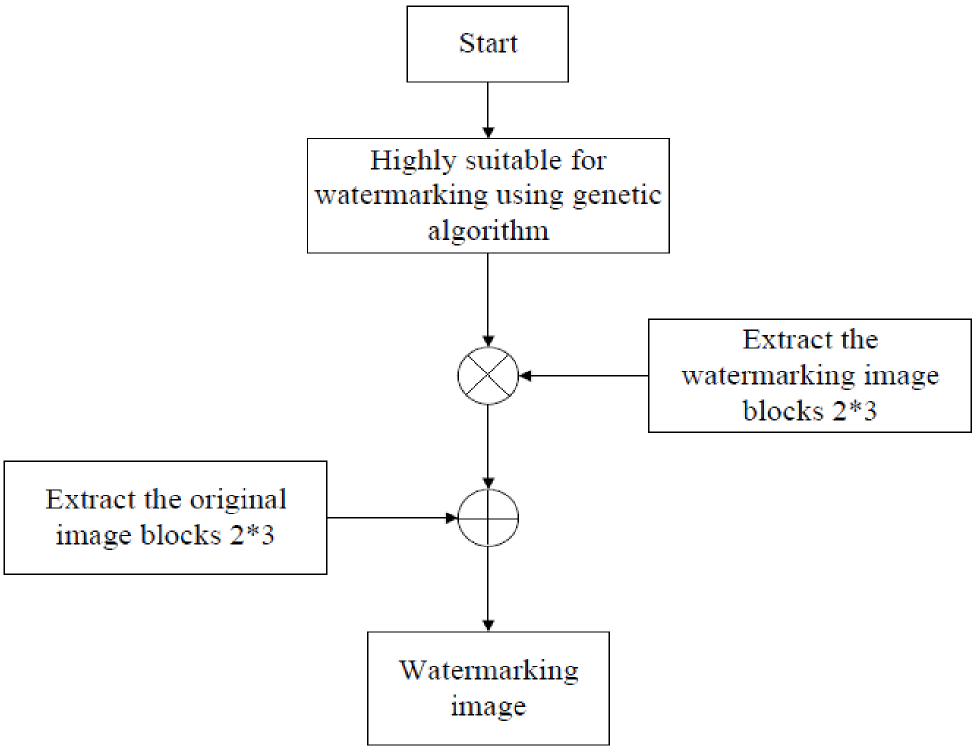

Figure 1: The watermarking algorithm structure

Vol. 4(10), Jan, 2014, pp. 98-110, **ISSN**: 2305-0543
Available online at: http://www.aeuso.org
© **Austrian E-Journals of Universal Scientific Organization**

- -

2.1. Embed watermark

First, SVD is applied to the original image into three matrices U, S and V is reached. SVD on image A with size m * m is shown in the form A = USVT. Where U and V are orthogonal matrices and S= diag (λi) is a diagonal matrix with λi values and i =1,2,..,m that are arranged in decreasing order. This process as single value decomposition (SVD) of A is known and can be written as follows:

$$A=USV^T=\sum_{i=1}^{r} \Lambda\text{I}\ \text{UI}\ \ V_I^T \quad (1)$$

r is degrees of picture A and is defined as r <=m. Ui and Vi are the left and right eigenvectors, respectively. Then intensity of watermarking is a diagonal matrix and shown with "a" (One factor to control the intensity of watermarking), multiplying in the image watermark and the result by the diagonal matrix S is collected. In the next step, SVD is applied on the new matrix s to obtain three matrix s_w,v_w,u_w. In the end, the image watermarking A_w is derived by multiplication U, S_w and Vt that vt is the transpose of matrix v. the three steps can be expressed as the following mathematical concepts:

$$A = U\,SV^{\,T} \quad (2)$$

$$S+AW= U_W\,S_W\,V_W^{\ T} \quad (3)$$

$$AW=U\,S_W\,V^T \quad (4)$$

2.2. Extracted watermark

To extract the watermark, the watermarking process is performed in reverse order. The main reason for using SVD is its reversibility. It means that the algorithm is efficient and convenient. The extracting process is as follows:

If we have s, v_w, u_w and the watermarked and flexible image Aw, Biodegradable watermark image W* is obtained by applying the above steps again:

Vol. 4(10), Jan, 2014, pp. 98-110, **ISSN**: 2305-0543
Available online at: http://www.aeuso.org
© Austrian E-Journals of Universal Scientific Organization

$$A_w^* = U^* S_W^* V^{*T} \quad (5)$$

$$D^* = U_W S_W^* V_W^T \quad (6)$$

$$W^* = \frac{1}{A}(D^* - S) \quad (7)$$

2.3. Optimal Factor of intensity watermarking

Before watermarking process, we need to obtain an intensity value. However, determining an appropriate value for this factor is difficult to measure. Especially if there is a variety of original and watermark image. In some cases, the choice of these factors is entirely independent of previous assumptions. So, systematic mechanism is needed to calculate the proper intensity factor. Regardless of any default, in these cases, we use the Tiny-GA for systematically determining these values.

"a" variable in the formula (3) must be a diagonal matrix. In this method, different quantity of the intensity factors are on a diagonal matrix called V= {V1, V2,…, Vn}. Viϵ [0.1] and 1<=i<=n and n is diagonal matrix dimension. Initial population: Usually at the beginning of this process, a set of values will be selected randomly. These values must be in the range [0,1]. It is obvious that the population values are closer to 1, the latent image is clearer. And if the random value is zero, the latent image is not recognizable.

Genetic operators: Selected operators determine how to combine chromosomes and its offspring are produced. Tournament selection was used in the method of Lai. Because, it has less time complexity and no need to compare the fitness of all the chromosomes in the population. Two chromosomes P1 and P2 are selected as parents and four chromosomes are generated according to the following formulas:

International Journal of Mechatronics, Electrical and Computer Technology

Vol. 4(10), Jan, 2014, pp. 98-110, **ISSN**: 2305-0543
Available online at: http://www.aeuso.org
© Austrian E-Journals of Universal Scientific Organization

$$OS_C^1 = W * P1 + (1 - W) * P2 \quad (8)$$

$$OS_C^2 = \frac{1}{2}(P_{MAX} + MAX(P1, P2)) \quad (9)$$

$$OS_C^3 = \frac{1}{2}(P_{MIN} + MIN(P1, P2)) \quad (10)$$

$$OS_C^4 = \frac{1}{4}(P_{MAX} + P_{MIN} + P1 + P2) \quad (11)$$

$$P_{MAX} = [PARA_{MAX}^1 \dots PARA_{MAX}^{NO\_VARS} \quad (12)$$

$$P_{MIN} = [PARA_{MIN}^1 \dots PARA_{MIN}^{NO_{VARS}} \quad (13)$$

Fitness function: In methods based on genetic algorithm, Fitness function is the criteria to judge the sustainability of chromosomes. The main feature of watermarking technique is maintaining both the features of robustness and imperceptibility. For this purpose, fitness function is defined as follows:

$$\text{FITNESS}=f(imperceptibility, robustness)$$

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 [1]. The mathematical formulas for the aforementioned two measures are defined as follows[1]:

$$\text{IMPERCEPTIBILITY}= NC\,(A, AW) \quad (14)$$

$$\text{ROBUSTNESS}=\frac{N}{\sum_{I=1}^{N} NC(W,W_I^*)} \quad (15)$$

$$NC(X, X^\wedge) = \frac{\sum_I \sum_J X(I,J) X^\wedge(I,J)}{\sqrt{\sum_I \sum_J X(I,J)^2}\sqrt{\sum_I \sum_J X^\wedge(I,J)^2}} \quad (16)$$

International Journal of Mechatronics, Electrical and Computer Technology

Vol. 4(10), Jan, 2014, pp. 98-110, **ISSN**: 2305-0543
Available online at: http://www.aeuso.org
© Austrian E-Journals of Universal Scientific Organization

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 $X^{\hat{}}$ stand for the original and the processed images; and N represents the number of sentence methods [1].

3. The results of these study

Different trials have been conducted to ensure the accuracy of the proposed watermarking scheme. Hydrangeas gray image with size 255 * 255 and 255 * 255 Image Lighthouse size has been used as the original image and the watermark image. These images shown in figure 2 and figure 3.

Figure 2: original image

Figure 3: watermark image

Vol. 4(10), Jan, 2014, pp. 98-110, **ISSN**: 2305-0543
Available online at: http://www.aeuso.org
© Austrian E-Journals of Universal Scientific Organization

Maximum number of generations has been considered equal to 300. In the beginning, the generation is considered as one empty matrix. W and the range of random numbers intended for watermarking intensity factor, any time can be set by the user. In this experiment, w = 0.5 and the same amount of watermarking is a random in the range 0 to 0.5 is considered. For the result number is closer to 0.5, each random number in the range [0.52, 0.58] to multiply have incrementally. Thus, the initial population is obtained as follows:

$$P1 = [\,\mathrm{rand}() * 0.52 \quad \mathrm{rand}() * 0.54 \quad 0]; \tag{18}$$

$$P2 = [\,\mathrm{rand}() * 0.56 \quad \mathrm{rand}() * 0.58 \quad 0]; \tag{19}$$

Due to the rest of the algorithm, the image is broken up into blocks 3 x 2 and each block is individually watermarking; for the watermarking intensity factor, the basic chromosome 3*1 used and the last element is considered zero.

$$P1 = [\,0.3288 \quad 0.0527 \quad 0] \tag{20}$$

$$P2 = [\,0.1560 \quad 0.3172 \quad 0] \tag{21}$$

Figure 4 shows the result of watermarking on the images 2 and 3 and Fig 5 shows the result of extracting watermarking image.

Figure 4: watermarked image

International Journal of Mechatronics, Electrical and Computer Technology

Vol. 4(10), Jan, 2014, pp. 98-110, **ISSN**: 2305-0543
Available online at: http://www.aeuso.org
© Austrian E-Journals of Universal Scientific Organization

Figure 5: extracted watermark

4. The Measurement

When compressing an image for example (A) watermarked with different types of watermarking method or (B) or extracted from another image, Image obtained (C) with the original image are not the same, it means that A and C are not equal.

A: Original image

B: a version of the compressed or watermarking image A

C: image taken from B (extracted watermark)

Now, if we have scale for measuring the similarity between A and C, it will be effective to optimize watermarking and improve the compression. PSNR or SNR is the difference between image A and C. Difference is considered as noise ratio be entered upon the Picture on effect Compress or Watermarking. This value is much larger than (The denominator is zero) the final image is closer to the original image and Quality is better. And whatever may be close to zero, indicating that the final image has a lot of information is lost and is very similar to the original image.

International Journal of Mechatronics, Electrical and Computer Technology

Vol. 4(10), Jan, 2014, pp. 98-110, **ISSN**: 2305-0543
Available online at: http://www.aeuso.org
© Austrian E-Journals of Universal Scientific Organization

- -

5. PSNR and SNR are also two different methods to calculate the differences are

The PSNR (peak signal-to-noise ratio), a measure of the quality of a watermarked image, is defined as follows[1]:

$$\mathrm{PSNR}=10\ \mathrm{LOG}\frac{255^2}{MSE} \quad (22)$$

$$\mathrm{MSE}=\frac{1}{W*H}\sum_i^W\sum_j^H(Xij-X'ij)^2 \quad (23)$$

SNR is a general formula for all signal types (image, sound ...) and PSNR are mostly used for Grayscale images. Since the logarithm is the PSNR, its value is expressed in terms of decibels db. PSNR is less than 30 images are usually of low quality images that watermarking it reduces the quality of data in the form of tangible and easily seen by the human eye. In fact Images can be desirable that The PSNR values are greater than 40 db. If PSNR are applied of the image watermarking images 2 and 3, Table 1 can be obtained. W is the initial weight for watermarking process that it can be a value surrounding [0, 1].

Conclusions

In this paper, a watermarking scheme is presented for digital images and a number of important principles for the design and evaluation of the project was cited. Results of the algorithm were tested in two ways:

- Comparison in small blocked matrix from image
- Comparison of the original image and the final version of the image watermarking.

To conclude that both of the proposed method is convenient and efficient method and the results will be good. it can be used in different applications and Included in future research at universities and research institutes and even on TV and radio as a

Vol. 4(10), Jan, 2014, pp. 98-110, **ISSN**: 2305-0543
Available online at: http://www.aeuso.org
© Austrian E-Journals of Universal Scientific Organization

method for watermarking images and hide or reveal the hidden form is used. In fact, one of the tricks to promote best practices, used watermarking and encryption of multimedia information such as images and video applications.

Table 1: Comparison of our method with the previous method

	W=0.1	W=0.2	W=0.5	W=0.8	W=0.9
The proposed method	66.3805	66.9951	66.6084	67.9627	67.1354
	66.2961	67.5998	66.8035	66.6092	68.1999
The previous method	66.4100	66.5467	66.1164	66.5116	66.1999
	66.8093	66.2530	66.9090	66.9090	66.6972

References

[1] C.C. Lai, A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm, Digital Signal Processing 21, 2011,pp. 522–527

[2] K. Zebbiche, F. Khelifi, and A. Bouridane, Robust Multibit Decoding and Detection of Multiplicative Watermarks for Fingerprint, JOURNAL OF MULTIMEDIA , 5(2) , APRIL 2010,pp. 167-180

[3] M. Shirvanian and F. Torkamani Azar, Adaptive SVD-Based Digital Image Watermarking, Springer-Verlag Berlin Heidelberg, 2009,pp. 113-123

[4] C.C. Chang,Y.S. Hu, and C.C. Lin, A Digital Watermarking Scheme Based on Singular Value Decomposition, Springer-Verlag Berlin Heidelberg, 2007,pp. 82-93

[5] B.F. Bergadano, D. Cavagnino, V. Pomponiu and A. Vernone, A Novel Block-based Watermarking Scheme Using the SVD Transform, Algorithms, 2, 2009, pp. 46-75

[6] A.M. Ahmed, D.D. Day, Applications of the naturalness preserving transform to image watermarking and data hiding, Digital Signal Process. 14 (2004) 531–549.

[7] P. Bao, X. Ma, Image adaptive watermarking using wavelet domain singular value decomposition, IEEE Trans. Circ. Syst. Video Technol. 15 (1) (2005) 96–102.

[8] M. Barni, F. Bartolini, A. De Rosa, A. Piva, Optimal decoding and detection of multiplicative watermarks, IEEE Trans. Signal Process. 51 (4) (2003) 1118–1123.

[9] B.F. Bergadano, D. Cavagnino, V. Pomponiu, A. Vernone, A novel blockbased watermarking scheme using the SVD transform, Algorithms 2 (2009) 46–75.

Vol. 4(10), Jan, 2014, pp. 98-110, **ISSN**: 2305-0543
Available online at: http://www.aeuso.org
© **Austrian E-Journals of Universal Scientific Organization**

[10] M. Calagna, H. Guo, L.V. Mancini, S. Jajodia, A robust watermarking system based on SVD compression, in: Proc. 2006 ACM Symposium on Applied Computing, 2006, pp. 1341–1347.

[11] K. Deb, Multi-Objective Optimization Using Evolutionary Algorithms, Wiley, 2001.

[12] B.H. Dennis, G.S. Dulikravich, Optimization of magneto-hydrodynamic control of diffuser flows using micro-genetic algorithms and least-squares finite element method, Finite Elem. Anal. Des. 37 (5) (2001) 349–363.

[13] E. Ganic, N. Zubair, A.M. Eskicioglu, An optimal watermarking scheme based on singular value decomposition, in: Proc. IASTED Int'l Conf. on Communication, Network, and Information Security, 2003, pp. 85–90.

[14] C.C. Lai, H.-C. Huang, C.-C. Tsai, Image watermarking scheme using singular value decomposition and micro-genetic algorithm, in: Proc. of the Fourth International Conference on Intelligent Information Hiding and Multimedia, Signal Processing, 2008, pp. 239–242.

[15] S. Lee, D. Jang, C.D. Yoo, AN SVD-based watermarking method for image content authentication with improved security, in: Proc. ICASSP05, 2005, pp. 525–528.

[16] F.H.F. Leung, H.K. Lam, S.H. Ling, P.K.S. Tam, Tuning of the structure and parameters of a neural network using an improved genetic algorithm, IEEE Trans. Neural Netw. 14 (1) (2003) 79–88.

[17] B.C. Mohan, S.S. Kumar, A robust image watermarking scheme using singular value decomposition, J. Multimedia 3 (1) (2008) 7–15.

[18] R. Liu, T. Tan, An SVD-based watermarking scheme for protecting rightful ownership, IEEE Trans. Multimedia 40 (1) (2002) 121–128.

[19] B.C. Mohan, S.S. Kumar, A robust image watermarking scheme using singular value decomposition, J. Multimedia 3 (1) (2008) 7–15.

[20] A.A. Mohammad, A. Alhaj, S. Shaltaf, An improved SVD-based watermarking scheme for protecting rightful ownership, Signal Process. 88 (9) (2008) 2158–2180.

[21] A. Nikolaidis, I. Pitas, Asymptotically optimal detection for additive watermarking in the DCT and DWT domains, IEEE Trans. Image Process. 12 (5) (2003) 563–571.

[22] T.V. Nguyen, J.C. Patra, A simple ICA-based digital image watermarking scheme, Digital Signal Process. 18 (2008) 762–776.

[23] Creative Commons Attribution-ShareAlike License, (2013), Singular value decomposition, Available:http://en.wikipedia.org/wiki/Singular_value_decomposition.

[24] F. edrisi,L. ehsan, Spread spectrum digital image watermarking method in DCT domain, Telecommunication MSc thesis, summer 2002 (in Persian).

[25] Z. ebrahimi, Providing a digital watermarking algorithm using SVD and Genetic algorithm, M.Sc THESIS, Faculty of Engineering- Department of Computer, Islamic Azad University Sari Branch, summer 2013 (in Persian).