Optimal SVD based Robust Watermarking using Differential Evolution Algorithm

V. Aslantas

Abstract- **This paper presents a novel optimal watermarking scheme based on singular value decomposition (SVD) using differential evolution algorithm (DE). The singular values (SVs) of the host image are modified to embed the watermark image by employing multiple scaling factors (SFs). Modifications are optimised using DE to obtain the highest possible robustness without losing the transparency. Experimental results show both the significant improvement in transparency and the robustness under attacks.**

***Index Terms*— Differential evolution algorithm, image watermarking, optimization, singular value decomposition.**

I. Introduction

Two important requirements in watermarking are perceptual transparency and robustness [1]. Transparency means that watermark should neither be noticeable to the viewer nor should introduce a significant degree of distortion in the host image. Robustness refers to the ability of watermark to resist intentional or unintentional image modifications such as filtering, geometric transformations, noise addition, etc. Robustness can be achieved if significant modifications are made to the host image. However, such modifications are distinguishable and thus do not satisfy the requirement of transparency. The design of an optimal watermarking for a given application always involves a trade-off between these requirements. Therefore, image watermarking can be considered as an optimisation problem. Optimisation techniques have been employed to optimise these requirements [2-5].

In general, a watermarked image (I^*) can be obtained by adding the watermark (W) multiplied by a scaling factor (k) to the host image (I): $I^*=I+k.W$ where k is used to control the watermark strength. The larger the scaling factor (SF), the more the distortion of the quality of the host image (transparency) and the stronger the robustness. On the other hand, the smaller the SF, the better the image quality and the weaker the robustness. Different spectral components may exhibit different tolerance to modification so a single SF may not be applicable for modifying all the values of I. Therefore, multiple SFs should be employed for adapting to the different spectral components to reduce visual artifacts [6].

SVD is one of the most powerful numeric analysis techniques with numerous applications including watermarking [4-9]. This paper proposes an optimal watermarking scheme based on SVD for grey-scale images. The singular values of the host image are modified to embed the watermark image by employing multiple SFs that are optimally found using DE [10] to obtain the highest possible robustness without losing the transparency.

II. SVD-Based Watermarking

SVD decomposes an mxn real matrix A into a product of 3 matrices $A=USV^T$ where U and V^T are mxn and nxn orthogonal matrices, respectively. S is an nxn diagonal matrix. The elements of S are only nonzero on the diagonal and are called the SVs of A. The watermarking procedures are described as follows [7]:

Watermark embedding: Without loss of generality, let the size of the host image (I) and watermark (W) is NxN

1. Apply SVD to the host image:
$$I = USV^T \tag{1}$$
2. Modify the S with the W:
$$S_M = S + kW \tag{2}$$
3. Apply SVD to the S_M:
$$S_M = U_W S_W V_W^T \tag{3}$$
4. Compute watermarked image:
$$I_W = US_W V^T \tag{4}$$

Watermark Extracting: In general, the extraction process is the inverse of the embedding procedure. In watermark extraction, a possibly distorted watermark W^* is extracted from the possibly distorted watermarked image I_W^* by essentially reversing the above watermark embedding steps. The watermark extraction can be described as follows:

1. Apply SVD to the watermarked (possibly distorted) image:
$$I_W^* = U^* S_W^* V^{*T} \tag{5}$$
2. Compute possibly corrupted S_M^*:
$$S_M^* = U_W S_W^* V_W^T \tag{6}$$
3. Extract the watermark (possibly distorted) image:
$$W^* = (S_M^* - S)/k \tag{7}$$

III. Optimisation of SFs

An nxn host image can have n SVs that may reveal different tolerance to modification. Since we may have no idea of how sensitive the image is to various values of the SF, an algorithm is needed to achieve the optimum SFs that produce maximum

Manuscript received March 4, 2007. This work was supported in part by the Research Foundation of Erciyes University, Kayseri, Turkey under Grant FBA-05-04

V. A. is with the Computer Engineering Department, Engineering Faculty, Erciyes University, Kayseri, 38039, Turkey. (Phone: +90 352 4374901 Ex:32602;fax: +90 352 4375784; e-mail: aslantas@erciyes.edu.tr).

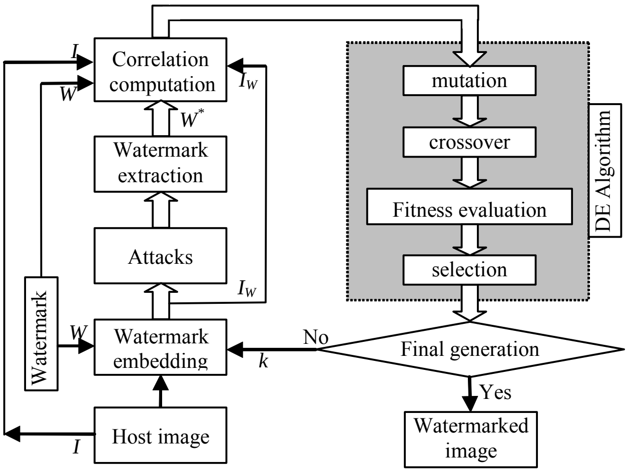


Fig. 1. Block diagram of DE-based watermark embedding scheme

transparency and robustness. Therefore, an efficient and powerful optimisation algorithm is required for this objective. For this purpose, DE [10] which is a novel stochastic nonlinear optimisation algorithm is employed in this work. Fig. 1 diagrammatically illustrates the flowchart of the watermark embedding technique based on DE algorithm developed in this study.

By applying DE, the SFs are obtained for watermarking to watch both the transparency and the robustness under certain attacks at each generation of optimisation process. Thus, DE optimally determines the SFs for watermarking process. Having modified the SVs of the host image at every generation, the watermarked image of the current generation is computed. After that, to evaluate the robustness of the watermark, four major attacks are employed including average filtering (AV), rotation (RT), resizing (RS) and sharpening (SH).

The watermarks are computed using the extraction procedure given above. The two dimensional correlations are measured between the original and watermarked images ($corr_I$) and between the original watermark and the extracted ones ($corr_W$). $corr_I$ and $corr_W$ are related to transparency and robustness measure, respectively The correlation values are then utilised to calculate the fitness value of a possible solution in the population of DE. These processes are repeated until predefined stopping criteria is satisfied, for example maximum generation number. In order to calculate fitness values, the following expression is used:

$$f_i = \left[1 \Big/ \left(\frac{1}{t} \sum_{i=1}^{t} corr_w(W, W_i^*) \right) - corr_I(I, I_W) \right]^{-1} \qquad (8)$$

where. f_i, and t are the fitness value of the i^{th} solution and the number of attacking methods, respectively.

IV. Results

To evaluate the performance of the proposed scheme, several experiments were conducted using the 256x256 Lena (host) and 32x32 watermark images that are illustrated in Fig.2(a) and (b). The attacks employed in the fitness evaluation process were: AV (3x3), SH (3x3), RS (bicubic: 256→128→256), and RT (30$^{\text{o}}$).

The control parameter values of DE were: the population size=150, weighting factor=0.6, crossover probability constant=0.8 and maximum generation=400. The crossover method used was DE/best/1/exp. In the representation scheme of solutions, each string consisted of 32 parameters. Every parameter represented a possible SF. Table 1 shows the SFs obtained by using DE.

The watermarked image is given in Fig.2(c). It is clear from Fig.2(c) that the watermarked image is not distinguishable from the original one. In addition to the attacks used in the optimisation process, the effectiveness of the algorithm was also tested to cope with the 30pixelx30pixel translation (TR), cropping (CR) on left half and JPEG compression (50:1) attacks. Distorted images after attacks and corresponding extracted watermarks are illustrated in Fig.3.

The results obtained are given in Table 2 by comparing the correlation values. The same experiments were also carried out with single SFs ranging from 0.1 to 0.9 with the interval of 0.2 [7]. The results are also given in Table 2. As can be seen from Table 2, the larger the SF, the more the distortion of the quality of the host image (transparency) and the stronger the robustness. In contrast, the smaller the SF, the better the image quality and the weaker the robustness. On the other hand, results of the multiple SFs obtained by DE show both the significant improvement in transparency and the robustness under attacks.

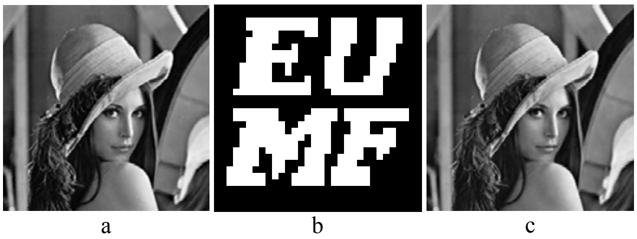


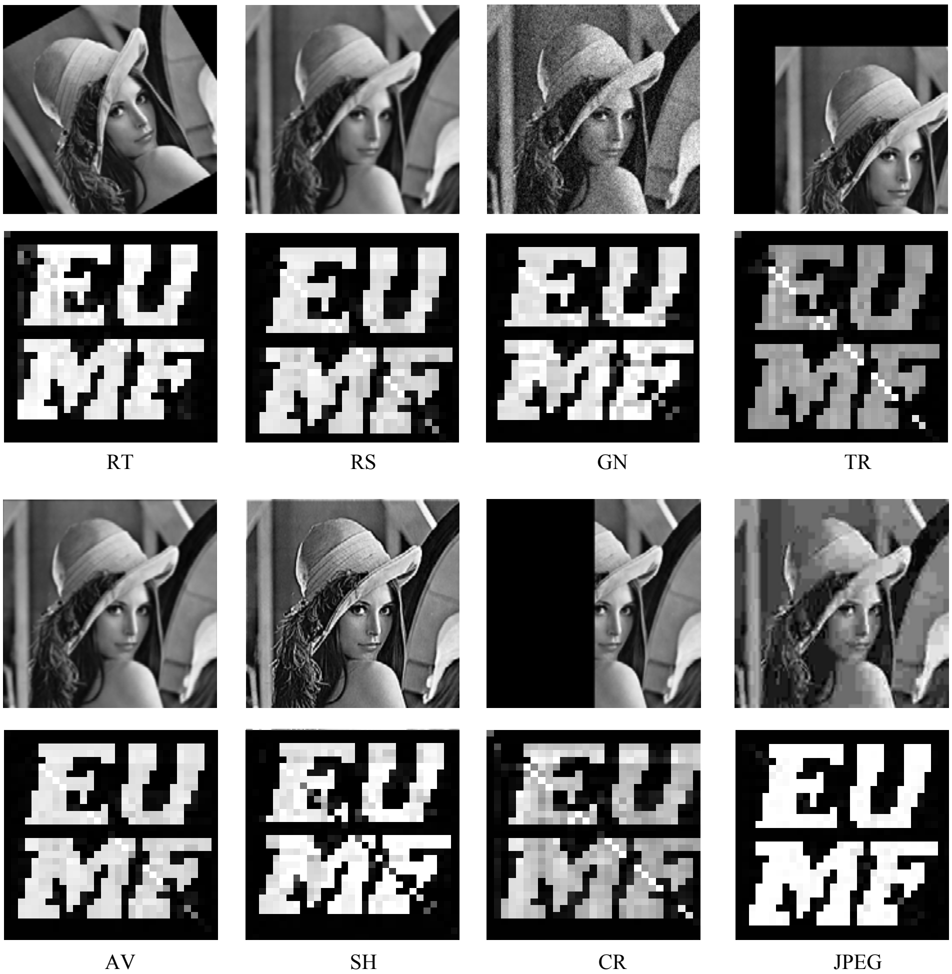
Fig. 2. (a) Host image, (b) watermark, (c) watermarked image

TABLE 1
SFs obtained by using DE

Number of Variables	1	2	3	4	5	6	7	8	9	10	11
SFs	-51.05	242.21	1.65	0.71	0.76	-1.14	-0.97	-2.30	-0.96	1.08	0.85
Number of Variables	12	13	14	15	16	17	18	19	20	21	22
SFs	0.95	-0.77	-0.63	7.90	-13.61	-1.13	-0.59	-1.22	0.77	-0.99	-1.10
Number of Variables	23	24	25	26	27	28	29	30	31	32	
SFs	-0.85	-1.22	0.62	1.07	-1.15	-1.24	-20.31	-19.48	27.54	-7.75	

TABLE 2
Correlation values ($corr_I(\boldsymbol{I}, \boldsymbol{I}^*)$ and $corr_W(\boldsymbol{W}, \boldsymbol{W}^*)$)

		DE	Single SF				
		SFs	0.1	0.3	0.5	0.7	0.9
$corr_I$		0.9995	1.0000	0.9996	0.9989	0.9986	0.9981
$corr_W$	RT	0.9965	0.9790	0.9799	0.9783	0.9703	0.9741
	RS	0.9947	0.9827	0.9820	0.9820	0.9838	0.9840
	AV	0.9963	0.9829	0.9829	0.9829	0.9846	0.9847
	SH	0.9843	0.9673	0.9728	0.9713	0.9710	0.9733
	GN	0.9944	0.9678	0.9744	0.9749	0.9774	0.9837
	TR	0.9809	0.9596	0.9708	0.9773	0.9776	0.9804
	CR	0.9815	0.9625	0.9708	0.9710	0.9751	0.9784
	JPEG	0.9996	0.9763	0.9922	0.9973	0.9975	0.9988



RT RS GN TR

AV SH CR JPEG

Fig. 3. Distorted images and corresponding extracted watermarks

V. Conclusions

In this paper, a novel optimal watermarking scheme based on SVD using DE is presented. DE is adopted in SVD-based watermarking to achieve the highest possible robustness without degrading image quality. Experimental results show the feasibility of multiple SFs estimated by DE and its superiority over the use of a single SF.

Acknowledgment

The author would like to thank Research Foundation of the Erciyes University, Kayseri, Turkey for supporting this work under the Grant No. FBA-05-04.

References

[1] F. Hartung, and M. Kutter, "*Multimedia watermarking techniques*", Proc. IEEE, vol. 87, no. 3, 1999, pp.1079–1107.

[2] C.S. Shieh, H.C. Huang, F.H. Wang, and J.S. Pan, "*Genetic watermarking based on transform-domain techniques*", Patttern Recognition, vol. 37, no. 3, 2004, pp. 555-565.

[3] F.Y. Shih, and Y.T. Wu, "*Enhancement of image watermark retrieval based on genetic algorithm*", J. Vis. Commun. and Image Repr., vol. 16, 2005, pp.115–133.

[4] V. Aslantas, "*A singular-value decomposition-based image watermarking using genetic algorithm*", Int J Electron Commun (AEU), 2007, doi: 10.1016/j.aeue.2007.02.010.

[5] V. Aslantas, S. Ozer and S. Ozturk, "*A Novel Clonal Selection Algorithm Based Fragile Watermarking Method*", LNCS, Vol.4628, 2007, pp. 358-369,

[6] E. Ganic, N. Zubair, and A.M. Eskicioglu, "*An optimal watermarking scheme based on singular value decomposition*", Int. Conf. on Comm., Net. and Inf. Security, December 2003, Uniondale, NY, p. 85.

[7] R. Liu, and T. Tan, "*An SVD-based watermarking scheme for protecting rightful ownership*", IEEE Trans. Multimedia, vol. 4, 2002, pp.121-128.

[8] S.C. Byun, S.K. Lee, A.H. Tewfik, and B.H. Ahn, "*An SVD-based fragile watermarking scheme for image authentication*", First Int. Workshop on Digital Watermarking, November 2002, Seoul, Korea, p. 170.

[9] F. Huang, and Z.H. Guan, "*A hybrid SVD-DCT watermarking method based on LPSNR*", Patt. Recog. Lett., vol. 25, 2004, pp. 1769-1775.

[10] R. Storn, and K. Price, "*Differential Evolution - A simple and efficient heuristic for global optimization over continuous spaces*", J. Global Optim., vol. 11, no. 4, 1997, pp. 341-359.