OPTO-ELECTRONICS REVIEW **22**(1), 45–54

DOI: 10.2478/s11772-014-0177-z

A robust SVD-based image watermarking using a multi-objective particle swarm optimization

K. LOUKHAOUKHA[*1,2], M. NABTI[1,3], and K. ZEBBICHE[1,3]

[1]Centre de Recherche Développement, Bouchaoui, Algeria
[2]Department of Electrical and Computer Engineering, Laval University, 2325 Rue de l'Université, Québec, QC G1V 0A6, Canada
[3]School of Electronics, Electrical Engineering and Computer Science, Queen's University, Belfast, UK

The major objective in developing a robust digital watermarking algorithm is to obtain the highest possible robustness without losing the visual imperceptibility. To achieve this objective, we proposed in this paper an optimal image watermarking scheme using multi-objective particle swarm optimization (MOPSO) and singular value decomposition (SVD) in wavelet domain. Having decomposed the original image into ten sub-bands, singular value decomposition is applied to a chosen detail sub-band. Then, the singular values of the chosen sub-band are modified by multiple scaling factors (MSF) to embed the singular values of watermark image. Various combinations of multiple scaling factors are possible, and it is difficult to obtain optimal solutions. Thus, in order to achieve the highest possible robustness and imperceptibility, multi-objective optimization of the multiple scaling factors is necessary. This work employs particle swarm optimization to obtain optimum multiple scaling factors. Experimental results of the proposed approach show both the significant improvement in term of imperceptibility and robustness under various attacks.

Keywords: Digital watermarking, authentication, multi-objective, particle swarm optimization, multiple scaling factors.

1. Introduction

The advent of digital era at the end of the 20th century led to a widespread use of multimedia contents. This extraordinary revolution from analogue to digital technology has raised concern in terms of copyright issues and unauthorized modification and distribution of multimedia data. To achieve these issues, watermarking technology is used to solve these problems. It consists of hiding secret information, called watermark, into multimedia contents. Usually, embedding watermarks can degrade the images visual quality. Therefore, imperceptibility means this degradation must be invisible to human visual system. Moreover, watermarked image may suffer from distortions caused by intentional or unintentional attacks caused by common signal processing operations and the watermark must be robustly resistant to these attacks. Therefore, robustness denotes the idea that watermark should be effectively extracted after undergoing attacks. Watermarking schemes can be categorized into different classes according to domain, visibility and permanency.

According to domain in which watermark is embedded, existing watermarking techniques for images are divided into two categories, spatial and frequency domains. The spatial domain methods are the earliest watermarking techniques, it consist to embed watermark by modifying the value of image pixels directly. The most commonly in this domain are least significant bit (LSB) [1] and spread spectrum [2]. Watermarking schemes in this domain have advantages of low computational cost and are easy to implement. However, it still has relative low capacity and generally is not robust against attacks. On the other hand, the frequency domain transformed the host image using frequency transformations such as discrete cosine transform (DCT) [3,4], discrete wavelet transform (DWT) [5,6], discrete Fourier transform (DFT) [7,8], discrete Hadamard transform (DHT) [9,10] and Ridgelet transform (RT) [11,12]. Then, watermark is embedded by modifying these coefficients. Afterwards the watermarked image is obtained by inverse transformation. Although frequency watermarking schemes are more robust, more complex and more widely applied.

In terms of the visibility, digital watermarking schemes can be classified into two different groups visible and invisible. Invisible watermarking algorithm [13,14] is designed that the embedded watermarks on the unknown places in the multimedia content to be imperceptible. This is done by respecting that the watermarked images should be similar to the original ones. The schemes of this group are more complex than the visible one. Visible watermarking algorithm [15,16] is the one which watermark can easily be perceived and the owner of multimedia content can be easily identified. The main goal of this class is to provide an instant rec-

[*]e-mail: khaled.loukhaoukha.1@ulaval.ca

ognition of the owner multimedia document. A common weakness of visible watermarking is that it suffers from the fact that they can be easily removed or destroyed using image processing techniques. For that visible watermarking has received much less attention than invisible one. One can see that published articles discussing invisible watermarking schemes are in abundance, on the contrary of the visible watermarking schemes.

Depending to the permanency, invisible watermarking can be classified into three categories: robust, semi-fragile and fragile. Robust watermarking [11,17] is designed to be resistant against intentional or unintentional attacks that attempt to remove or destroy the watermark from the watermarked image. The most common attacks used are noise addition, filtering, compression, histogram equalization, geometric transformations, etc. The goal of this category is not the verification of the image authenticity, but rather the verification of their origins. The robust watermarking is typically employed for copyrights protection and ownership verification. Conversely, fragile watermarking [18,19] is designed to detect any unauthorized modification in such a way that slight modifications or tampering on the watermarked image will destroy the watermark. This category is employed to ensure the integrity and authenticity. Semi-fragile watermarking [20,21] combines the properties of fragile and robust watermarks, it is designed to be fragile against some attacks and being robust against other attacks.

In general, greater 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 imperceptibility. A trade-off between these two competing criteria, i.e., robustness and imperceptibility, is controlled by embedding strength which is generally determined empirically. To approach the upper performance limit of watermarking algorithms, we must determine their optimal embedding strength called scaling factor (SF). However, as stated above, it is usually difficult to empirically determine embedding strength. A popular way of solving the optimal watermarking problem is to regard it as an optimization problem. In this manner, artificial intelligence techniques such as genetic algorithm, ant colony optimization, particle swarm optimization can be applied to solve this optimization problem. Cox *et al.* [2] suggest the use of a multiple scaling factors (MSF) instead of single scaling factor (SSF). They state that a single scaling factor may not be applicable for altering all the pixel values of the original image.

Determining the optimal values of the multiple scaling factors can be viewed as optimization problem which is unfortunately a difficult problem. In this paper, we investigate the use of artificial intelligence in order to solve this optimization problem. A multi-objective particle swarm optimization is employed as a mean of finding the optimal values of the multiple scaling factors in order to improve the visual quality and at the same time, the robustness of the proposed watermarking algorithm. We propose an optimal image watermarking algorithm that uses a multi-objective particle swarm optimization (MOPSO) to find the optimal values of the multiple scaling factors, which guaranteed the highest possible robustness without losing the imperceptibility. This paper is organized as follows. Section 3.3, reviews the basic concepts of the particle swarm optimization (PSO). The proposed watermarking algorithm based on singular value decomposition and lifting wavelet transform (LWT) is presented in Sect. 4. SVD-watermarking algorithm using multi-objective particle swarm optimization is described in Sect. 5. The experimental results are provided in Sect. 6 and the conclusions are given in Sect. 7.

2. Previous works

In this section, an overview of the important existing SVD-based watermarking schemes and also watermarking algorithms using artificial intelligence will be explained briefly. Ganic and Eskicioglu [22] introduced a hybrid algorithm based on discrete wavelet transform and singular value decomposition. After decomposing the original image into four sub-bands (*LL*, *HL*, *LH* and *HH*), the SVD is applied to each band, the singular values of the original image are modified with the singular values of the watermark. Liu and Tan [23] proposed an SVD-watermarking in spatial domain. They suggested changing the singular values of the original image, based on SVD of a matrix made by addition of the original image matrix of singular values, and an attenuated version of watermark matrix. The singular values of the original image are then replaced by the resultant singular values of this decomposition. Mohan and Kumar [24] presented a robust image watermarking scheme for multimedia copyright protection. In their work, original image is partitioned into four sub-images and SVD are applied two chosen of them. After that, the watermark is embedded in both *U* and *S* matrices. Watermark image is embedded in the *S* matrix using dither quantization. In the proposed method, the largest singular values of the original image and the coefficients of the *U* matrix are modified to embed the watermark. Ramanjaneyulu and Rajarajeswari [25], presented a robust image watermarking scheme based on discrete wavelet transform (DWT). The discrete wavelet transform is applied to original image and the coefficients of LH_2 and LH_3 sub-bands are grouped into different blocks. In each block, the first minimum and the second minimum are identified and modified according to the watermark bit. Then, genetic algorithm (GA) is used to optimize algorithm parameters by maximizing the values of peak signal to noise ratio (PSNR) of the watermarked image and normalized correlation (NC) of the extracted watermark. Rohani and Avanaki [26] have presented a watermarking scheme on DCT domain. In this algorithm the PSO is used to determine the best DCT coefficients to which watermark will be embedded to guarantee the best imperceptibility.

Recently, Tsai *et al.* [27] proposed watermarking scheme for image copyright protection based on discrete wavelet transform (DWT), singular value decomposition and support vector regression (SVR). A watermark bit is embedded in the low-low sub-band of a target non-overlap block of the original image by modifying a coefficient of U component on SVD version of the block. A blind watermark extraction is designed using a trained SVR to estimate original coefficients. Subsequently, the watermark bit can be computed using the watermarked coefficient and its corresponding estimate coefficient. Additionally, the particle swarm optimization (PSO) is further utilized to optimize the proposed scheme. However, various SVD watermarking algorithms suffers from the vulnerability of false positive detection of watermark. The scheme proposed by Liu and Tan [23] suffers from this vulnerability as reported by Zhang and Li [28] and Rykaczewski [29]. Moreover, Loukhaoukha and Chouinard [30] have stated that watermarking algorithm proposed by Abdallah *et al.* [9] suffers from this vulnerability. Similarly, as stated by Loukhaoukha [45] the watermarking algorithm proposed by Lai [46] suffers from the vulnerability of false positive detection of the watermark. Ling *et al.* [31] showed that the hybrid watermarking algorithm based on singular value decomposition and Radon transform, proposed by Rastegar *et al.* [32] has a fundamental flaw and leads to false positive detection of watermark.

3. Background

3.1. Singular value decomposition

The theory of singular value decomposition (SVD) was established for real square matrices in the 1870's by Beltrami [33] and Jordan [34], for complex matrices by Autonne in 1902 [35] and has been extended to rectangular matrices by Eckart and Young [36] in 1939. Recently, singular value decomposition has been used in image processing applications, including image compression [37], image hiding [38] and noise reduction [39].

Let I be the image matrix of size $N \times N$. It can be represented using singular value decomposition as

$$I = U \cdot S \cdot V^T = \sum_{k=1}^{N} u_k \cdot s_k \cdot v_k^T \tag{1}$$

with $U = [u_1, u_2, \ldots, u_N], V = [v_1, v_2, \ldots, v_N]$ and

$$S = \begin{bmatrix} s_1 & 0 & \ldots & 0 \\ \ldots & s_2 & \ldots & 0 \\ \ldots & \ldots & \ddots & \ldots \\ 0 & 0 & \ldots & s_N \end{bmatrix}.$$

Here, U and V are the orthogonal matrices of size $N \times N$, whose column vectors are the left-singular and the right-singular vectors, respectively. S is the $N \times N$ diagonal matrix containing nonnegative terms. The diagonal elements $s_1, s_2, \ldots, s_N$ of matrix S are the singular values of matrix I, satisfying the ordering: $s_1 \geq s_2 \geq \ldots \geq s_N$.

It is important to note that:

- Singular values correspond to the luminance of the image (i.e, image brightness) and the corresponding singular vectors specifies the geometry of the image [40].
- Many singular values have small values compared to the first singular value s_1. If these small singular values are ignored in the reconstruction of the image, the quality of the reconstructed image will degrade only slightly [40].
- A slight variation of the singular values do not affect the visual perception of the image, i.e., singular values do have a good stability.

3.2. Lifting wavelet transform

Lifting wavelet transform (LWT), also termed second generation wavelet transform, was proposed by Sweldens in 1995 [41]. The lifting wavelet transform is widely used in signal processing because of its efficient implementation with low memory and computational complexity. The lifting scheme is described in Fig. 1.

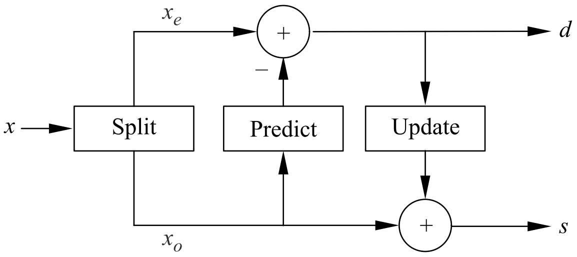


Fig. 1. Block diagram of lifting scheme [42].

A typical lifting stage consists of three operations, namely a split, a predict and an update operation. Let $X(m,n)$ be the image matrix. The two dimensional wavelet transform can be split into two one-dimensional wavelet transforms.

1) Split operation: all the samples are split into two subsets: the even sample set $X_e(m,n)$ and the odd sample set $X_o(m,n)$

$$\begin{cases} X_e(m,n) = X(m,2n) \\ X_o(m,n) = X(m,2n+1) \end{cases}. \tag{2}$$

2) Predict operation (also called dual lifting): in this step, the odd sample set $X_o(m,n)$ is predicted from the neighboring even coefficients. The high-pass coefficient $h(m,n)$ is calculated as the error in predicting the odd samples from the even ones using a prediction operator P, with

$$h(m,n) = X_o(m,n) - P[X_e(m,n)]. \tag{3}$$

From Eq. (3) one can recover the odd sample set as shown in Eq. (4)

$$X_o(m,n) = h(m,n) + P[X_e(m,n)]. \tag{4}$$

3) Update operation (also termed primal lifting): to produce the low-pass coefficient , the even sample is updated with the updating value

$$l(m,n) = X_e(m,n) + U_h(m,n). \tag{5}$$

3.3. Particle swarm optimization

Particle swarm optimization (PSO) is an evolutionary optimization technique devised by Kennedy and Eberhart [43], which mimics simplified social models such as fish schooling or bird flocking. A swarm is defined as a set of mobile agents that collectively carry out problem solving in a distributed manner. In a swarm each particle keeps track of its own attributes. Initially, the position $x_{i,j}(k)$ and the velocity $v_{i,j}(k)$ of each particle *p* are randomly created. Each particle represents a candidate solution to optimization problem. The fitness of each particle is evaluated against an objective function. At each iteration, the best location visited by each particle is kept as the local best position $P_{best_{i,j}}$ while the best location visited by all particles is kept as the global best position $G_{best_{i,j}}$. Therefore, a new population is created based on a preceding one and the particles are updated by the following equations

$$\begin{cases} v_{i,j}(k+1) = \omega \cdot v_{i,j}(k) + C_1 \cdot R_1 [P_{best_{i,j}} \\ \qquad\qquad {}_{i,j}(k)] + C_2 \cdot R_2 [G_{best_{i,j}} - x_{i,j}(k)] \\ x_{i,j}(k+1) = x_{i,j}(k) + v_{i,j}(k+1) \end{cases} \tag{6}$$

where:

- *i*: particle index;
- *j*: index of the position in the particle;
- *k*: iteration number;
- $v_{i,j}(k)$: velocity of the i^{th} particle in the swarm on the j^{th} index of the position in the particle;
- $x_{i,j}(k)$: position;
- R_1 and R_2: random numbers uniformly distributed between 0 and 1;
- C_1 and C_2: acceleration number, which control the influence of $P_{best_{i,j}}$ and $G_{best_{i,j}}$;
- ω: inertia weight, used to balance the search ability of the algorithm over global and local exploration and exploitation. Generally, inertia weight value is within $0.8 \le \omega \le 1.4$.

4. Proposed watermarking algorithm

In this section, a watermarking algorithm based on singular value decomposition (SVD) and lifting wavelet transform (LWT) is presented. Hence, this algorithm is formulated as follows:

4.1. Watermark embedding

Consider the original gray-scale image *I* of size $N \times N$ and let the watermark *W* be a binary image of size $M \times M$ pixels. The watermark embedding process is presented as follows:

1) The original image *I* is decomposed into wavelet domain using lifting wavelet transform (LWT) with *l* resolution levels. We obtain then $3l+1$ sub-bands.
2) Select one sub-band, denoted bellow by *SB*, of approximative detail of the level *l*.
3) Compute the inverse LWT of the selected sub-band (*SB*) and obtain the reference sub-band

$$A = LWT^{-1}(SB_l). \tag{7}$$

4) Perform singular value decomposition (SVD) on the reference sub-band *A*

$$A = U_A \cdot S_A \cdot V_A^T. \tag{8}$$

5) Encrypt the watermark *W* to get the encrypted watermark W_C.
6) Apply a singular value decomposition to encrypted watermark W_C

$$W = U_{W_C} \cdot S_{W_C} \cdot V_{W_C}^T. \tag{9}$$

7) Generate the digital signature of the matrices and using one-way hash functions[1]

$$\begin{cases} H_U = \text{hash}(U_{W_C}) \\ H_V = \text{hash}(V_{W_C}) \end{cases}. \tag{10}$$

8) Matrices U_{W_C} and V_{W_C}, and their signatures H_U and H_V are stored in the private key as embedding-extracting key.
9) Add singular values of the encrypted watermark to singular values of the reference sub-band to obtain matrix *S*

$$S = S_A + \alpha \cdot S_{W_C} \tag{11}$$

where α is the watermark strength factor that controls the trade-off between visual quality and robustness of the watermarking scheme.

10) Using the matrices U_A and V_A obtained from the step 6 and the matrix *S* obtained from step 9

$$X = U_A \cdot S \cdot V_A^T. \tag{12}$$

11) Compute the lifting wavelet transform of matrix *X*

$$SB_M = LWT(X). \tag{13}$$

12) Obtain the watermarked image I_W by applying the inverse *l*-level lifting wavelet transform to the modified sub-band SB_M and the 3*l* unmodified sub-bands.

4.2. Watermark extracting

The following steps summarize the extracting process:

1) The matching of the signature is verified[2]. The digital signature $H_{\tilde{U}}$ and $H_{\tilde{V}}$ of the matrices U_{W_C} and V_{W_C}, possibly altered by an attacker as $\tilde{U}_W$ and $\tilde{V}_W$, are compared to the signature stored in embedding-extracting key

$$\begin{cases} \text{if } H_U = H_{\tilde{U}} \text{ and } H_V = H_{\tilde{V}} \rightarrow \text{go to step 2} \\ \text{if } H_U \ne H_{\tilde{U}} \text{ and } H_V \ne H_{\tilde{V}} \rightarrow \text{Autentication failed} \end{cases}. \tag{14}$$

[1] 5 and 7 are only necessary to mitigate the false positive detection of watermark. This solution is proposed by Loukhaoukha and Chouinard in [30].

[2] This test is necessary to eliminate the problem of the false positive detection of watermark.

2) Decompose the original and watermarked images, I and I_W, by applying l-level lifting wavelet transform.
3) Select the same sub-band (SB) as selected in step 2 of watermark embedding process. Here, the subbands selected for the original and watermarked images are denoted by SB_I and SB_{I_W}, respectively.
4) Apply the inverse lifting wavelet transform of selected sub-bands as follows

$$\begin{cases} A = LWT^{-1}(SB_I) \\ A_W = LWT^{-1}(SB_{I_W}) \end{cases}. \tag{15}$$

5) Perform the singular value decomposition on matrices A and A_W

$$\begin{cases} A = U_A \cdot S_A \cdot V_A^T \\ A_W = U_{A_W} \cdot S_{A_W} \cdot V_{A_W}^T \end{cases}. \tag{16}$$

6) Compute matrix $\hat{S}$ as follows

$$\hat{S} = \frac{S_{A_W} - S_A}{\alpha}. \tag{17}$$

7) Get the possibly distorted encrypted watermark, $\hat{W}_C$, as

$$W_C = U_{W_C} \cdot \hat{S} \cdot V_{W_C}^T. \tag{18}$$

8) Decrypt $\hat{W}_C$ to get the possibly distorted extracted watermark $\hat{W}$.

5. Optimized multiple scaling factors using multi-objective particle swarm optimization

In general, watermarking schemes are either based on an additive or a multiplicative rule. The embedding rules themselves are usually of the form

$$\begin{cases} I_W = I + \alpha \cdot W \rightarrow \text{additive rule} \\ I_W = I(1 + \alpha \cdot W) \rightarrow \text{multiplicative rule} \end{cases}, \tag{19}$$

where I and I_W are respectively original and watermarked image[3]. α is used to control the trade-off between imperceptibility and robustness of an image, generally is used as scaling factor. Cox *et al.* [2] suggest the use of multiple scaling factors instead of single scaling factor. They state that a single scaling factor may not be applicable for altering all the values of the original image I. However, determining the optimal values of these multiple scaling factors is a difficult problem and can be viewed as an optimization problem. To solve it, we propose to use a multi-objective particle swarm optimization (MOPSO).

Figure 2 illustrates block diagram of multi-objective optimization which is a closed-loop control system. System input is multiple scaling factors and objective measure as system output, this measure is calculated from: the original image I, the watermarked image I_W, the watermark W and the $(T+1)$ extracted watermarks ($\hat{W}$ and $\hat{W}_j$, where $j = \{1,2, ...,T\}$) under attacks.

The steps for applying a multi-objective particle swarm optimization into the proposed watermarking scheme are enumerated below:

1) Define the swarm size, the acceleration coefficients C_1 and C_2, the random number R_1 and R_2, the objective function, and a generation number as the algorithm stopping criterion.
2) Generate randomly an initial swarm which constitutes a set of potential solutions.
3) For each particle p of the population:
   - Each particle is defined by it position x_p and the velocity v_p;
   - Produce the watermarking image I_W by embedding process previously described in Sect. 4.1 using the particle p as the watermark strength factor. Note that, Eq. (11) in embedding process is transformed into[4]

$$S_Y = S_X + diag(\alpha) \cdot S_{W_C} \tag{20}$$

   with $diag(\alpha)$ is diagonal matrix create from the vector p, which is the particle p.
   - Compute the objective measure between original and watermarked images I and I_{W_p}. Index p indicate that the watermarked image have been obtained using the particle p.
   - Apply a watermark attack out of a set of T selected attacks upon the watermarked image I_{W_p}. This leads to T attacked watermarked images $\{\hat{I}_{W_{p,j}}\}$, where $j = \{1, 2,...,T\}$.
   - Using extracting process as described in Section 4.2, extract the watermark $\hat{W}_p$ from the watermarked image I_{W_p}, while extracted watermark $\hat{W}_{p,j}$ is extracted from attacked watermarked image $\hat{I}_{W_{p,j}}$.
   - Compute the objective measure between the original watermark W and the extracted watermarks $\hat{W}_p$ and $\hat{W}_{p,j}$.
   - Construct the vector of objective values, $F_{\text{Obj}}(X)$, defined as

$$F(p) = \left(\frac{1}{NC(I, I_{W_p})} \frac{1}{NC(W, \hat{W})} \frac{1}{NC(W, \hat{W}_{p,1})} \right. \\ \left. \frac{1}{NC(W, \hat{W}_{p,2})} \cdots \frac{1}{NC(W, \hat{W}_{p,T})} \right)^T. \tag{21}$$

   - Evaluate the vector of objective values according to the *exponential weighted method* for multi-objective optimization [44]

$$F_{\text{Obj}}(p) = \sum_{i=1}^{T+2} (e^{pw} - 1) e^{p[F(p) - F_0]} \tag{22}$$

where: p, w and F_0 are the positive constants. In experiments, we take $p = 2,\ w = 5$ and $F_0 = 10$.

[3] Or theirs representation in other domains such as FFT, DCT, DWT, etc.

[4] α is changed into multiple scaling factors instead single scaling factor.

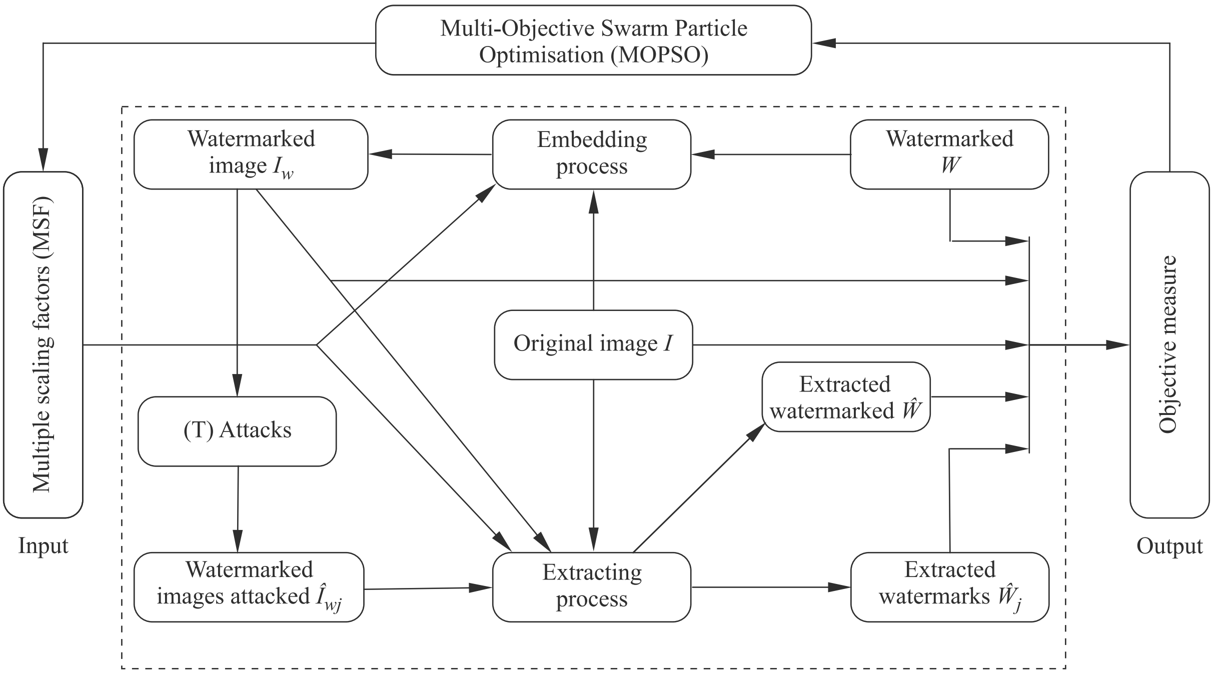

Multi-Objective Swarm Particle Optimisation (MOPSO)
Multiple scaling factors (MSF)
Input
Watermarked image I_w
Embedding process
Watermarked W
Original image I
Extracted watermarked $\hat{W}$
(T) Attacks
Watermarked images attacked $\hat{I}_{wj}$
Extracting process
Extracted watermarks $\hat{W}_j$
Objective measure
Output

Fig. 2. Block diagram of multi-objective optimization.

4) Find the best particle p_{Best} as the one having the smallest objective value F_{Obj}.
5) Update the position x_p and the velocity v_p of all swarm.
6) If the generation number is reached the optimization process is terminated, else go to step 3.

6. Experimental results

In this section, some experiments were carried out to demonstrate the performance of the proposed watermarking algorithm, denoted by MSF-MOSPO, based on lifting wavelet transform (LWT) and singular values decomposition (SVD) using multiple scaling factors (MSF) optimized by a multi-objective particle swarm optimization (MOPSO). Simulations were run using four 256×256 pixels gray-scale test images and a 32×32 pixels binary watermark depicted in Fig. 3. Note that, the embedding process is done in the LH_3 sub-band.

The performance of two algorithms is compared in order to evaluate the effectiveness of using multiple scaling factors (MSF) instead to single scaling factor (SSF). The first algorithm is the one presented in Sect. 4 using single scaling factor, denoted by SSF. The second one, is the same algorithm but using multiple scaling factors optimized by multi--objective particle swarm optimization, denoted by MSF--MOPSO. Table 1 shows the comparative in term of imperceptibility for these algorithms.

Table 1. Imperceptibility test results.

Image	Algorithm	PSNR(I, I_w)(dB)	NC(W, $\hat{W}$)
Baboon	MSF-MOPSO	52.857	1.000
	SSF	51.124	1
Boat	MSF-MOPSO	54.907	1.000
	SSF	53.716	1.000
Cameraman	MSF-MOPSO	49.696	1.000
	SSF	49.341	1.000
Lena	MSF-MOPSO	49.505	1.000
	SSF	48.899	1

From Table 1, one can see that the peak signal to noise ratios between original and watermarked images, *PSNR* (I, I_W) using either a single scaling factor or multiple scal-

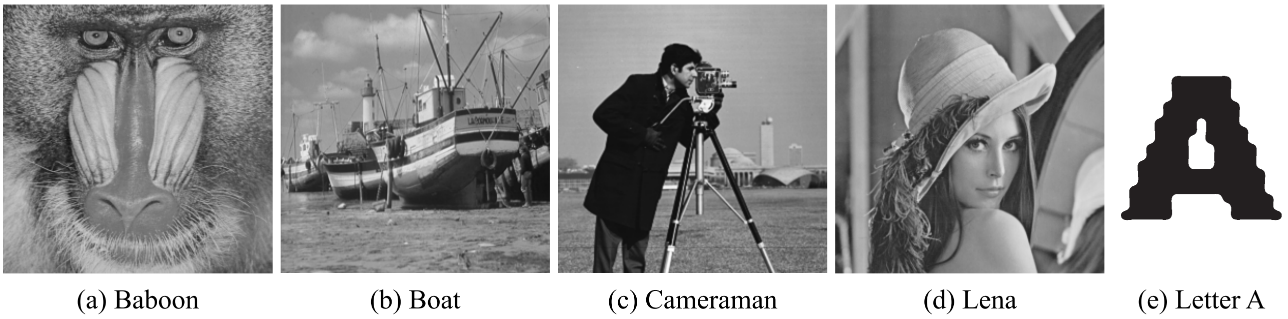

(a) Baboon (b) Boat (c) Cameraman (d) Lena (e) Letter A

Fig. 3. Original gray-scale images and binary watermark.

Table 2. Robustness tests (first series).

Image	Algorithm	SP	GF	CR	CM	SH	SC	HE	QN
Baboon	MSF-MOPSO	0.979	0.990	0.993	0.989	0.991	1	0.996	0.997
	SSF	0.885	0.936	0.998	0.930	0.950	1.000	0.977	0.965
Boat	MSF-MOPSO	0.989	0.984	0.988	0.994	0.995	0.999	0.992	0.995
	SSF	0.777	0.847	0.855	0.990	0.980	0.992	0.915	0.928
Cameraman	MSF-MOPSO	0.970	0.973	0.949	0.976	0.988	1	0.988	0.980
	SSF	0.726	0.907	0.894	0.729	0.976	1.000	0.959	0.958
Lena	MSF-MOPSO	0.980	0.994	0.951	0.980	0.992	0.999	0.994	0.987
	SSF	0.774	0.943	0.867	0.944	0.982	1.000	0.988	0.974

Table 3. Robustness tests (second series).

Image	GC	DI	RT	MB	MF	RW	CA	TR
Baboon	0.994	0.994	0.937	0.992	0.894	0.999	1.000	0.995
Boat	0.989	0.994	0.888	0.992	0.957	0.997	1.000	0.959
Cameraman	0.963	0.977	0.923	0.968	0.976	1.000	1.000	0.786
Lena	0.988	0.985	0.912	0.985	0.880	0.998	1.000	0.891

ing factors are close to each other. Furthermore, the PSNR values of the algorithms using multiple scaling factors (i.e., MSF-MOPSO) are greater than those obtained by the algorithm SSF. In addition, the normalized correlation values between watermark W and extracted watermark $\hat{W}$ for the two algorithms are very close to unity. For the robustness tests, eight different attacks were selected in conjunction to multi-objective particle swarm optimization (i.e., $T = 8$). These attacks are: salt & peppers noise (with a density of 0.05), Gaussian filtering (3×3), cropping (1/8 of the image centre), JPEG compression ($Q = 5$), sharpening, scaling (256 → 512 → 256), histogram equalization, and gray-scale quantization (1 bit): these attacks are identified respectively as **SP**, **GF**, **CR**, **CM**, **SH**, **SC**, **HE** and **QN**. The normalized correlation values between the embedded and the extracted watermarks, ($NC(W,\hat{W}_j)$, where $j = \{1, 2,...,8\}$), under different attacks for the algorithms are given in Table 2.

From Table 2, one can observe that the proposed algorithm (i.e., MSF-MOPSO) is robust against the following

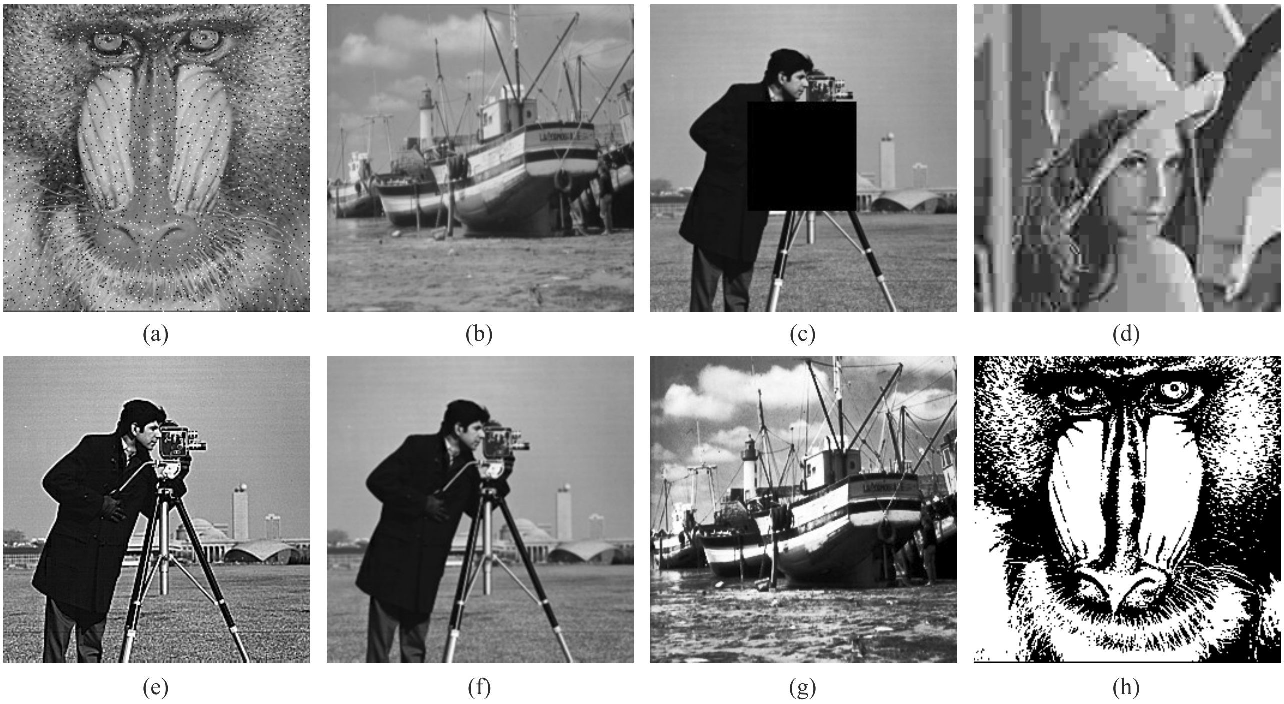
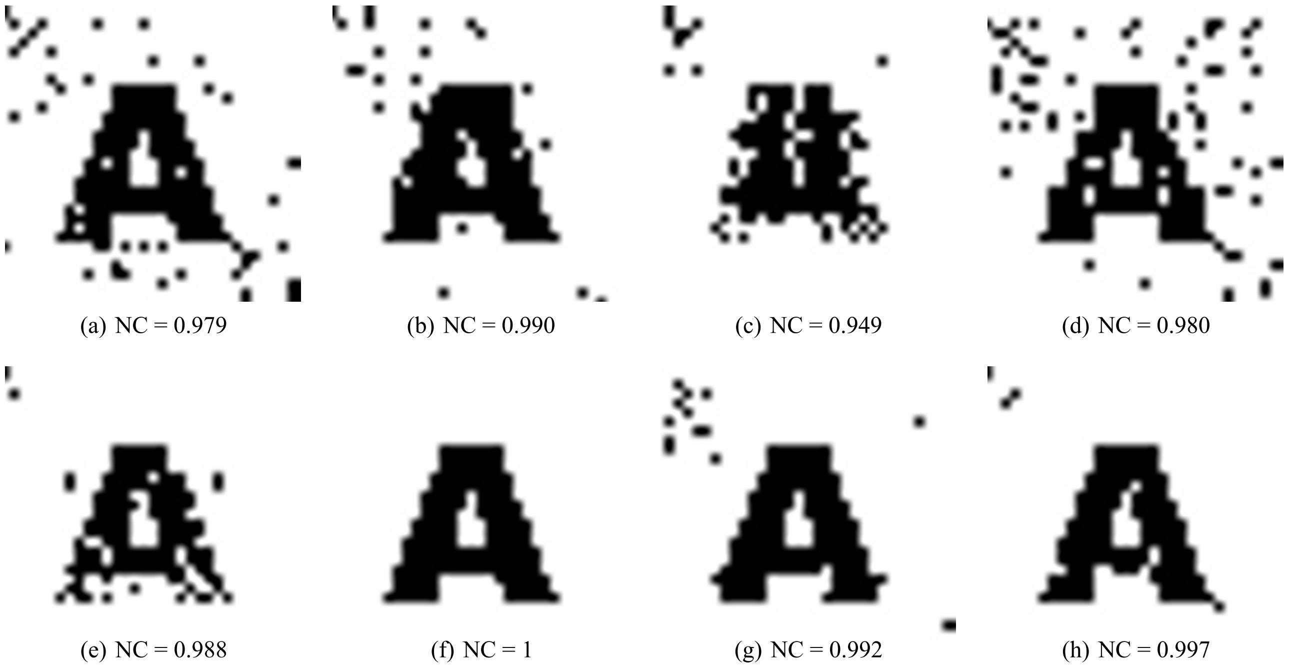


Fig. 4. Watermarked images under different attacks: (a) salt & peppers noise (5%), (b) Gaussian filter (3×3), (c) cropping (1/8 centre), (d) JPEG compression ($Q = 5$), (e) sharpening, (f) scaling (256→512→256), (g) histogram equalization and (h) gray-scale quantization (1 bit).

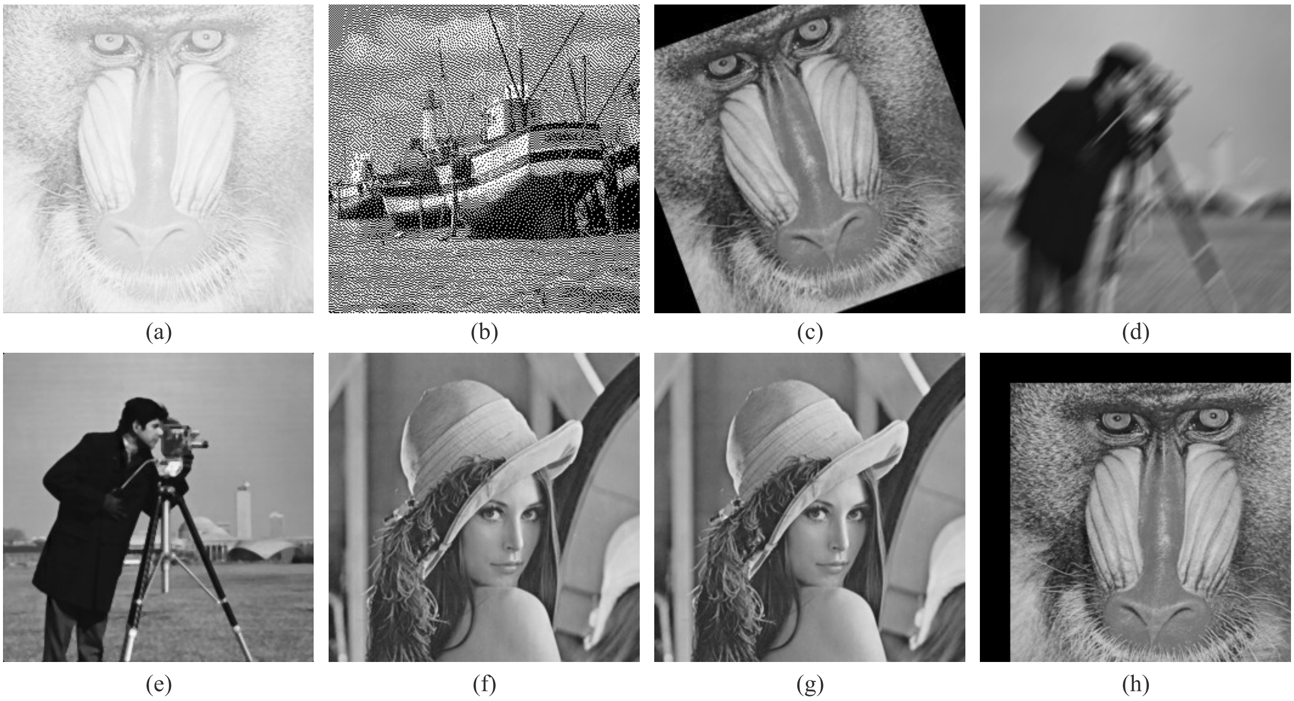

(a) NC = 0.979 (b) NC = 0.990 (c) NC = 0.949 (d) NC = 0.980

(e) NC = 0.988 (f) NC = 1 (g) NC = 0.992 (h) NC = 0.997

Fig. 5. Extracted watermarks under different attacks: (a) salt & peppers noise (5%), (b) Gaussian filter (3×3), (c) cropping (1/8 centre), (d) JPEG compression ($Q = 5$), (e) sharpening, (f) scaling (256→512→256), (g) histogram equalization and (h) gray-scale quantization (1 bit).

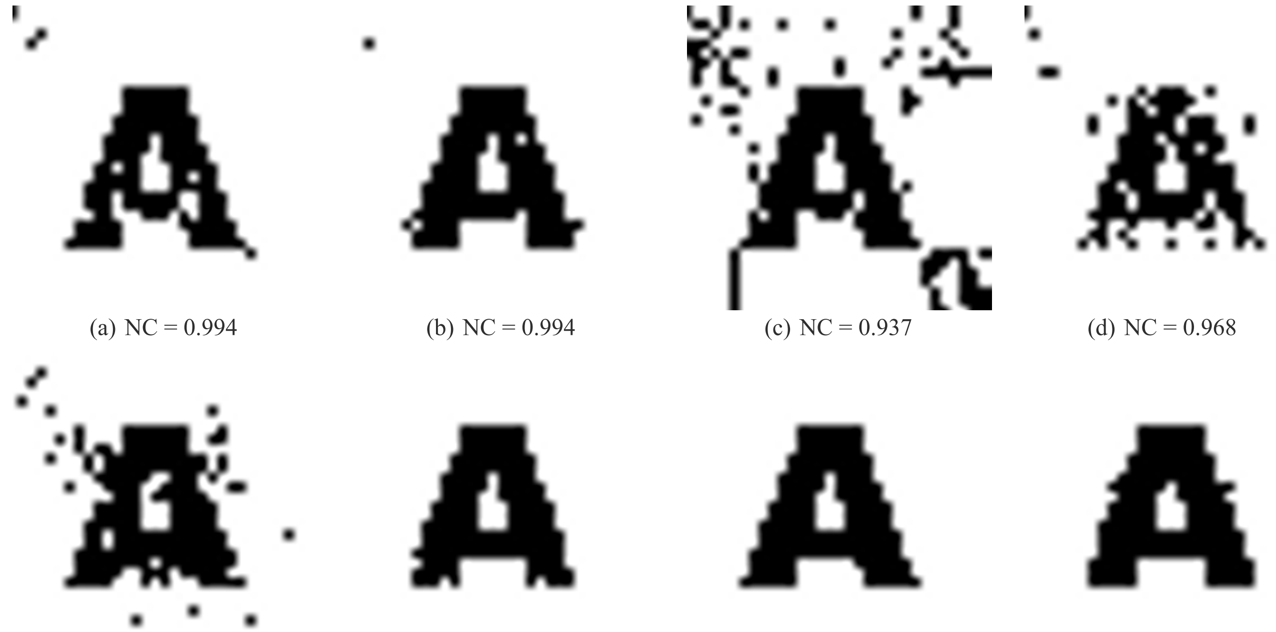
attacks: additive noise, Gaussian filter, cropping, JPEG compression, sharpening, scaling, histogram equalization and gray-scale quantization. Furthermore, the robustness results are improved with the use of multiple scaling factors optimized by multi-objective particle swarm optimization. Figure 4 shows different watermarked images under the eight different attacks, while Figure 5 depicts their corresponding extracted watermarks.

In addition to the eight attacks used in the multi-objective particle swarm optimization, the effectiveness of the proposed algorithm (i.e., MSF-MOPSO) was also tested against others attacks such as: gamma correction ($\gamma = 0.2$), dithering, rotation (25°), motion blur (45°), median filter (3×3), re-watermarked using other watermark, collusion attack using five watermarks and translation (25×25 pixels). Table 3 gives the normalized correlation values, $NC(W, \hat{W}_i)$,


(a) (b) (c) (d)

(e) (f) (g) (h)

Fig. 6. Watermarked images under different attacks: (a) gamma correction ($\gamma = 0{:}2$), (b) dithering, (c) rotation (25°), (d) motion blur (45°), (e) median filter (3×3), (f) rewatermarked, (g) collusion attack using five different watermarks and (h) translation (25×25 pixels).



(a) NC = 0.994 (b) NC = 0.994 (c) NC = 0.937 (d) NC = 0.968

(e) NC = 0.976 (f) NC = 0.998 (g) NC = 1 (h) NC = 0.995

Fig. 7. Extracted watermarks under different attacks: (a) gamma correction ($\gamma = 0{:}2$), (b) dithering, (c) rotation (25°), (d) motion blur (45°), (e) median filter (3×3), (f) re-watermarked, (g) collusion attack using five different watermarks and (h) translation (25×25 pixels).

under these attacks and which are respectively denoted by **GC**, **DI**, **RT**, **MB**, **MF**, **RW**, **CA** and **TR**. It is important to note here that these attacks were not used in multi-objective particle swarm optimization of the multiple scaling factors.

From Table 3, one can conclude that the proposed algorithm provides a good performance against these attacks. Figure 6 shows different watermarked images and attacked and Figure 7 depicting the extracted watermarks under these attacks.

7. Conclusions

In this paper, we present a new watermarking algorithm based on lifting wavelet transform (LWT) and singular value decomposition (SVD) using multiple scaling factors (MSF) optimized by multi-objective particle swarm optimization (MOPSO). The MSF are used instead to single scaling factor (SSF) to achieve a highest possible robustness without losing watermark imperceptibility. However, determining the optimal set of multiple scaling factors is a prohibitively complex problem. In order to solve this problem a multi-objective particle swarm optimization is used. Experimental results demonstrate that the MSF-MOPSO algorithm showed better imperceptibility and excellent resiliency against a wide range of watermarking attacks such as additive noise, compression, filtering and geometrical attacks.

References

1. K. Tanaka, Y. Nakamura, and K. Matsui, “Embedding secret information into a dithered multi-level image,” in *Proc. IEEE. Military Communications Conf.* **1**, 216–2201 (1990).
2. I.J. Cox, J. Kilian, F. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia,” *IEEE T. Image Process.* **6**, 1673–1687 (1997).
3. J.R. Hernandez, M. Amado, and F. Perez-Gonzalez, “DCT--domain watermarking techniques for still images: detector performance analysis and a new structure,” *IEEE T. Image Process.* **9**, 55–68, (2000).
4. C. Hsu and J. Wu, “Hidden digital watermarks in images,” *IEEE T. Image Process.* **8**, 58–68 (1999).
5. K. Loukhaoukha and J.-Y. Chouinard, “A new image watermarking algorithm based on wavelet transform,” in *IEEE Canadian Conf. Electrical and Computer Engineering*, 781–786, 2009.
6. W. Lu, W. Sun, and H. Lu, “Robust watermarking based on DWT and nonnegative matrix factorization,” *Comput. Electr. Eng.* **35**, 183–188 (2009).
7. V. Solachidis and I. Pitas, “Circularly symmetric watermark embedding in 2-D DFT domain,” *IEEE T. Image Process.* **10**, 1741–1753 (2001).
8. T.K. Tsui, X.-P. Zhang, and D. Androutsos, “Colour image watermarking using multidimensional fourier transforms,” *IEEE T. Information Forensics and Security* **3**, 16–28 (2008).
9. E. Abdallah, A.B. Hamza, and P. Bhattacharya, “Improved image watermarking scheme using fast Hadamard and discrete wavelet transforms,” *J. Electron. Imaging*. **16**, 1–9 (2007).
10. S.P. Maity and M.K. Kundu, “Perceptually adaptive spread transform image watermarking scheme using Hadamard transform,” *Inform. Sciences*. **181**, 450–465 (2011).
11. P. Campisi, D. Kundur, and A. Neri, “Robust digital watermarking in the Ridgelet domain,” *IEEE Signal Process. Lett.* **11**, 826–830 (2004).
12. H.-Y. Yu, J.-L. Fan, and X.-L. Zhang, “A robust watermark algorithm based on ridgelet transform and fuzzy c-means,” in

Int. Symp. Information Engineering and Electronic Commerce, 120–124 (2009).

13. S.P. Mohanty and B.K. Bhargava, "Invisible watermarking based on creation and robust insertion-extraction of image adaptive watermarks," *ACM T. Multimedia Computing, Communications and Applications* **5**, 12:1–12:22 (2008).
14. K. Loukhaoukha and J.-Y. Chouinard, "Hybrid watermarking algorithm based on SVD and lifting wavelet transform for ownership verification," in *Proc. Canadian Workshop on Information Theory*, pp. 177–182, 2009.
15. H.-M. Tsai and L.-W. Chang, "A high secure reversible visible watermarking scheme," in *Proc. IEEE Int. Conf. Multimedia and Expo*, pp. 2106–2109, 2007.
16. A. Verma and S. Tapaswi, "A novel reversible visible watermarking technique for images using noise sensitive region based watermark embedding (NSRBWE) approach," in *IEEE Eurocon*, pp. 1374–1377, 2009.
17. D. Simitopoulos, D. Koutsonanos, and M. Strintzis, "Robust image watermarking based on generalized radon transformations," *IEEE T. Circuits and Systems for Video Technology* **13**, 732–745 (2003).
18. V. Aslantas, S. Ozer, and S. Ozturk, "Improving the performance of DCT-based fragile watermarking using intelligent optimization algorithms," *Opt. Commun.* **282**, 2806–2817 (2009).
19. Y.-J. Chang, R.-Z. Wang, and J.-C. Lin, "A sharing-based fragile watermarking method for authentication and self-recovery of image tampering," Eurasip J. Advan. Sig. Pr., Article ID 846967, doi:10.1155/2008/846967, 17 pages (2008).
20. M.-J. Tsai and C.-C. Chien, "Authentication and recovery for wavelet-based semi fragile watermarking," *Opt. Eng.* **47**, 067005 (10 pages) (2008).
21. N. Ishihara and K. Abe, "A semi-fragile watermarking scheme using weighted vote with sieve and emphasis for image authentication," *IEICE T. Fund. Electr., Communications and Computer Sciences* **E90-A**, 1045–1054 (2007).
22. E. Ganic and A. M. Eskicioglu, "Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition," *J. Electron. Imaging* **14**, 043004 (2005).
23. R. Liu and T. Tan, "A SVD-based watermarking scheme for protecting rightful ownership," *IEEE T. Multimedia* **4**, 121–128 (2002).
24. B. Mohan and S. Kumar, "A robust image watermarking scheme using singular value decomposition," *Multimed. Tools Appl.* **3**, 7–15 (2008).
25. K. Ramanjaneyulu and K. Rajarajeswari, "Wavelet-based oblivious image watermarking scheme using genetic algorithm," *IET Image Process.* **6**, 364–373 (2012).
26. M. Rohani and A. Avanaki, "A watermarking method based on optimizing SSIM index by using PSO in DCT domain," in *Proc. IEEE Int. CSI Computer Conf.*, pp. 418–422, Tehran, 2009.
27. H.-H. Tsai, Y.-J. Jhuang, and Y.-S. Lai, "An SVD-based image watermarking in wavelet domain using SVR and PSO," *Appl. Soft Comput.* **12**, 2442–2453 (2012).
28. X. P. Zhang and K. Li, "Comments on "An SVD-based watermarking scheme for protecting rightful ownership"," *IEEE T. Multimedia* **7**, 593–594 (2005).
29. R. Rykaczewski, "Comments on an SVD-based watermarking scheme for protecting rightful ownership"," *IEEE T. Multimedia* **9**, 421–423 (2007).
30. K. Loukhaoukha and J.-Y. Chouinard, "On the security of ownership watermarking of digital images based on SVD decomposition," *J. Electron. Imaging* **19**, 013007 (2010).
31. H.-C. Ling, R. C.-W. Phan, and S.-H. Heng, "On the security of a hybrid watermarking algorithm based on singular value decomposition and Radon transform," *Int. J. Electron. Commun.* **65**, 958–960 (2011).
32. S. Rastegar, F. Namazi, K. Yaghmaie, and A. Aliabadian, "Hybrid watermarking algorithm based on singular value decomposition and radon transform," *Int. J. Electron. Commun.* **65**, 658–663 (2011).
33. E. Beltrami, "Sulle funzioni bilineari," *Giornale de Matematiche* **11**, 98–106 (1873) (in Italian).
34. C. Jordan, "Mémoire sur les formes trilinéaires," *J. Mathématiques Pures et Appliquées* **19**, 35–54 (1874) (in French).
35. L. Autonne, "Sur les groupes linéaires, réels et orthogonaux," *Bulletin de la société mathématique de France*, 1902 (in French).
36. C. Eckart and G. Young, "A principal axis transformation for Non-Hermitian matrices," *Bulletin of the American Mathematical Society* **45**, 118–121 (1939).
37. P. Waldemar and T. Ramstad, "Image compression using singular value decomposition with bit allocation and scalar quantization," in *Proc. Nordic Signal Process. Symp.*, 83–86, (1996).
38. K. Chung, C. Shen, and L. Chang, "A novel SVD and VQ--based image hiding scheme," *Pattern Recogn. Lett.* **22**, 1051–1058 (2001).
39. K. Konstantinides, B. Natarajan, and G. Yovanof, "Noise estimation and filtering using block-based singular value decomposition," *IEEE T. Image Process.* **6**, 479–483 (1997).
40. P. Bao and X. Ma, "Image adaptive watermarking using wavelet domain singular value decomposition," *IEEE T. Circuits and Systems for Video Technology* **15**, 96–102 (2005).
41. W. Sweldens, "The lifting scheme: A construction of second generation wavelets," *SIAM J. Mathematical Analysis* **29**, 511–546 (1997).
42. I. Daubechies and W. Sweldens, "Factoring wavelet transforms into lifting steps," *J. Fourier Analysis and Application* **4**, 247–269 (1998).
43. J. Kennedy and R. Eberhart, "Particle Swarm Optimization," in *IEEE Int. Conf. Neural Networks* **4**, 1942–1948 (1995).
44. R. Marler and J. Arora, "Survey of multi-objective optimization methods for engineering," *Structural and Multidisciplinary Optimization* **26**, 369–395 (2004).
45. K. Loukhaoukha, "Comments on "A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm"," *Digit. Signal Process.*, **23**, 1334, (2013).
46. C.-C. Lai, "A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm", *Digit. Signal Process.* **21**, 522–527 (2011).