An Intelligent Watermarking Approach Based Particle Swarm Optimization in Discrete Wavelet Domain

Abdelaziz I. Hammouri[1], Basem Alrifai[2] and Heba Al-Hiary[1]

[1] Computer Information System Department, Prince Abdullah Bin Ghazi Faculty of Information Technology Al-Salt, 19117, Jordan

[2] Software Engineering Department, Prince Abdullah Bin Ghazi Faculty of Information Technology Al-Salt, 19117, Jordan

Abstract

A watermarking scheme for digital images based on Particle Swarm Optimization (PSO) in the Discrete Wavelet Transform (DWT) is proposed. The watermark is inserted into the DWT subbands which have the most important coefficients. The robustness of proposed scheme is empowered by applying the PSO. PSO optimizes the imperceptibleness of the watermark and the quality of the watermarked image which results in identifying the optimal / nearly optimal embedding positions. A series of experiments were carried out using different host images with different watermarks under different attacks. It has been shown that the approach is robust against several watermarking attacks that may meet the watermarked image. The efficacy of the proposed scheme is verified by using two basic criteria; the peak signal to noise ratio and the cross-correlation function which are used to measure the quality and strength of the watermark. In conclusion, the experimental results substantiate that PSO in the DWT can improve the quality of the watermarked image effectively, as well as it can yield a watermark that is invisible to human eyes, and robust against common image processing attacks.

Keywords: *Intelligent* Watermarking, Particle Swarm Optimization, Discrete Wavelet Transform, Cross-Correlation, Peak Signal to Noise Ratio.

1. Introduction

The progression in Internet technologies enabled the multimedia data in distributed environments; audio, video, and digital images, to be easily transferred, downloaded, shared and unlimitedly modified by anyone browsing the Internet [2]. Apart from this progress, the digital multimedia contents suffer from copyright infringement [3], [4] that may be caused through duplication and unauthorized sharing sites. Those risks may have implications in the area of document security and computer forensics. Therefore, data piracy has become a major concern over copyright protection of digital multimedia contents [1], [5]. Currently, encryption and control access techniques were employed to protect the proprietorship of digital multimedia contents. These techniques, however, do not protect the media contents against unauthorized access. Digital watermarking has been growing as means of protecting content rather than merely controlling access to documents. Digital watermarking techniques share common features of operating in transform domain and not on raw data. These techniques minimize the perceptible distortions and make the optimization to different requirements more practical. The relationship between different transform domains and the performance of digital watermarking has been extensively investigated during the last decade [6], [7]. Artificial intelligence techniques have been already introduced to improve the performance of watermarking schemes [8]. Some researchers utilize the evolutionary computation strategies to acquire nearly optimal solution [8], [9]. For example, some researchers explored the optimal watermark embedding positions using Genetic Algorithms (GAs), they utilized GA to examine the correlation between the robustness and the quality of the digital image [8], [10]. Others presented a new approach to find nearly optimal positions for embedding an authentication message by GAs [11]. In this paper, Particle Swarm Optimization (PSO) [12] has been used to design a feasible watermarking scheme. The watermark embedding was performed to the coefficients produced by the Discrete Wavelet Transform (DWT). The embedded positions of the watermark in the original image must be decided precisely in order to resist the most common image processing attacks, therefore, the watermarked image quality is assured, and the extracted watermark must match the embedded watermark to a high degree. The PSO parameters are formalized to select the best positions for the embedding process so that the robustness and imperceptible requirements are still preserved. The embedding process can be viewed as a selection process of feasible embedding points within acceptable positions in the host image. Then, the nearly optimal embedding positions are attained, moreover, the PSO evolution can efficiently achieve high quality watermarked image and secure watermark against different

attacks. At last, the feasibility of the proposed approach is examined and evaluated using the Peak Signal-to-Noise Ratio (PSNR) and cross-correlation function.

2. Overview of Digital Watermarking

Digital watermarking can be described as a way of embedding secret information (the watermark), into the original image itself to protect the ownership of the original sources [4], [13]. In this manner, watermarking provides copyright protection by hiding appropriate information into the original cover data. Digital watermarking can be represented in spatial domain, or frequency domain. The watermarking schemes can be categorized as:

1) Visible watermarking: the visible watermarks, for instance, are those company logos on one corner of the TV screen. They are easily identified and can be easily removed from original images [14].

2) Invisible watermarking: the invisible watermarks are more secure and robust than the visible watermarks. Here, the embedding locations are secret and must be done in a such way that the embedded data is hidden, and only the authorized persons with the secret keys can extract the watermark [3].

A. Types and Components of Digital Watermarking

There are two main types of watermarks:

- Blind (or public) watermark: the watermark is extracted "blindly" without knowledge of the original host image or the watermark itself, hence it is invisible.
- Non-blind (or private): the watermark is embedded into the original host image, and it is intentionally visible to the human observer. The original data is essential for the watermark extraction [15].

Generally, watermarking system consists of two main components: watermark embedder and watermark extractor as shown in Figure 1. The embedder combines the digital data (X) with the hidden watermark (W). The output of the embedder is the watermarked data (Xw), which is perceptually identical to the data (X) but with the embedded watermark W. The attacker (y) represents the malicious attacks that are intended to change the watermarked data.

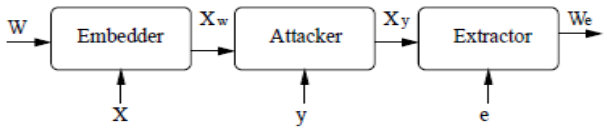

Fig 1: General structure of watermarking.

The goal of the attacker is to modify (Xw) with (y) to make the detection of the watermark complex, or to covertly corrupt some sensitive contents in the watermarked data (Xy) for violating its integrity. The embedding process usually leads to unwanted visible objects, especially in regions, which are more sensitive to noise. In doing so, robustness is lost. The role of the extractor (e) is to recover the watermark We from the corrupted watermarked data (Xy) or to detect the integrity violation action [16].

3. The Proposed Intelligent Watermarking Scheme

The proposed watermarking scheme is based on both of swarm intelligence and the 2-dimensional wavelet transform [17], in this way, embedding the watermark takes full merits of both PSO and DWT2 to select the best embedding regions adaptively. PSO and DWT2 can assure to guarantee the perceptual invisibility of the embedded watermark and high quality of the watermarked image. Some preparation steps should be adapted, they are:

1) The host image is transformed to the discrete wavelet domain with two levels DWT.

2) The embedding positions were selected with the help of a private embedding key (secret key).

The host image has a size of (H x V). H indicates the number of rows in the horizontal direction, and V indicates the number of columns in the vertical direction. The watermark image (W) with size of N x M is transformed to a binary-valued image. N and M are the number of pixels in the horizontal and vertical directions, respectively. The embedding and extracting processes are precisely summarized by the block diagram as described in Figure 2.

In Figure 2 the host image is transformed to the wavelet domain using a two level DWT, at the same time, the watermark is perturbed using a secret key. Next, the embedding process is carried out by an optimal search block based on PSO. After all, the extraction process can be performed, in order to obtain the original watermark and the host image. A detailed explanation of the proposed technique is coming in the following subsections.

A. *Watermark Embedding*

The embedding part is an inevitable part of any watermarking technique, in this research it consists of two main phases: the perturbation and the embedding algorithm.

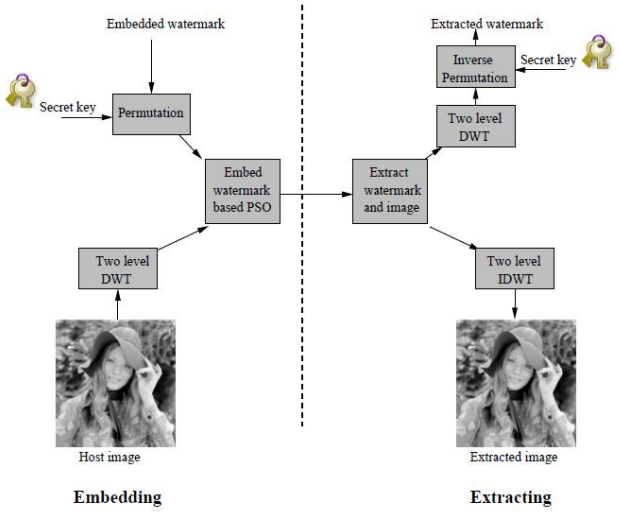

Fig 2: The watermark embedding and detection processes.

1) Perturbation the Watermark: Perturbation is generally employed to increase the security against scrambled or unauthorized access, such that the watermark is perceptually encrypted, and the human observer could not easily notice the watermark. Accordingly, permutation has been performed in a robust fashion to ensure imperceptibility of the embedding algorithm, while not perceivably degrading the watermark strength. On doing perturbation, with a pre-determined key, (*key0*), is used to permute the watermark (*W*); $Wp = permute(W; key_0)$. Thus, *W* is encrypted by means of key_0 based on permutation the *N* rows and *M* columns.

2) Embedding Algorithm: The perturbed watermark (*Wp*) is embedded into the selected DWT frequency bands by adjusting small changes in the pixel values of the host image based PSO. Therefore, the pixels in each selected block are adaptively modified to satisfy two requirements; maximize the robustness and guarantee the invisibility. As a matter of fact, PSO accomplishes the embedding algorithm in two level-DWT by follow-up the next steps:

- **Step 1:** All the wavelet coefficients in the frequency bands are divided into *k* blocks. $k = (H \times V)/9$, and each block has size of 3 × 3. Next, the maximum, minimum, and average intensities of each block are computed and stored in an array.
- **Step 2:** All the blocks of the wavelet coefficients are sorted descending based on the contrast, and then the embedding blocks will be selected using PSO based on subsequent criterion.
- **Step 3:** Once the embedded Block (B) is chosen, PSO proceeds by modifying the intensities of the block's pixels, such that, each bit of the watermark data is embedded by altering the coefficient values in the selected block (*B*) according to the following scenario:

– ***for*** $Wp_i = 1$:

$$\bar{g}(x,y) = \begin{cases} g_{max} & if\ g(x,y) > g_{mean} \\ g(x,y) + \delta_j & if\ g(x,y) \le g_{mean} \end{cases}$$

– ***for*** $Wp_i = 0$:

$$\bar{g}(x,y) = \begin{cases} g_{min} & if\ g(x,y) < g_{min} \\ g(x,y) + \delta_k & if\ g(x,y) \ge g_{mean} \end{cases}$$

Where *Wpi* is the *ith* bit of the perturbed watermark, and $(x; y)$, $g(x; y)$, $g(x; y)$ respectively are the coefficients position in the block, the original coefficients, the watermarked coefficients. g_{max}, g_{min}, g_{mean} respectively represent the maximum, minimum, and average intensities of the block (*B*) which are computed in the neighbourhood centered at location $(x; y)$.

g_{max}, g_{min} and g_{mean} were computed as given in the following formulas:

- $g_{\max} = \max(b_{xy} \ ; 0 < x, y < 3)$
- $g_{\min} = \min(b_{xy} \ ; 0 < x, y < 3)$
- $\text{gmean} = \frac{1}{9}\sum_{x=0}^{3} \sum_{y=0}^{3} b_{xy}$

Where b_{xy} represents the intensity value of the $(x, y)^{th}$ pixel in the block B.

δ_j and δ_k are the embedding strength for each embedded pixel, they are used to tune the pixels intensities, and their values imply the watermark power. For each block, δ_j and δ_k are picked as follows:

$$\delta_j = \frac{g_{max}}{g_{min}}$$

$$\delta_k = \frac{g_{max} - g_{min}}{g_{mean}} + g_{mean}$$

- **Step 4:** Finally, an inverse two level DWT is performed to the modified wavelet coefficients to return back the watermarked image to its spatial domain.

The same embedding procedure based PSO is repeatedly applied to the remaining blocks. It can be observed from the above steps that the embedding algorithm modifies the contents of the wavelet coefficients slightly. This increases the robustness of the algorithm whilst reduces the effects of the attacks. That is, if the block has a high contrast, then, the intensities of the pixels will be modified greatly. On the other hand, if the block has a low contrast, then, the intensities will be tuned slightly.

B. Watermark Extraction

Watermark extraction consists of two main phases: the extraction algorithm and the inverse permutation.

1) *Extraction Algorithm*: The extraction strategy was applied to the optimized blocks of the embedded watermark. The optimized watermark image (X_o) might be subjected to some attacks, the image after attack (A) can

be represented by (X_{oa}). Firstly, the attacked two level DWT of the watermarked image (X_o) was extracted using the secret key (key_0). Then, all the watermarked blocks and host blocks are returned back to the time domain.

The following strategy has been applied for the extraction algorithm: For each selected position, assume B and B' respectively are the corresponding blocks of the cover and watermarked images. The sum of pixel intensities of B is indicated by S_0, while the sum of pixel intensities of B' is indicated by S_w. It can be inferred that S_w will be larger than S_0 if the inserted watermark bit W_p is 1. On the contrary, if the inserted watermark bit W_p is 0, then, S_0 will be larger than or equal to S_w. Next, the sums of pixel intensities of each two corresponding blocks are computed. In conclusion, the bits of the extracted permuted watermark are determined using the following relation:

$$W_{ep} \begin{cases} 1 & if\ S_w > S_0 \\ 0 & if\ S_w \leq S_0 \end{cases}$$

2) *Inverse Permutation*: After that, the extracted watermark (W_{ep}) must be decrypted using the same secret key (key_0) in the reverse order.

$W_e = inverse\_permute\ (W_{ep};\ key_0)$, where W_e and W_{ep} are the extracted and the permuted extracted watermarks, respectively. This detection step should be repeated until all the embedded bits are detected.

4. Problem Implementation

The proposed discrete wavelet-based PSO algorithm has been implemented in Matlab withWindows XP environment. MATLAB supports built in numerous wavelets, MATLAB's Haar wavelet was adopted in the presented approach. An illustrative diagram for the implemented watermarking scheme based on PSO is shown in Figure 3.

A. PSO Based Intelligent Watermarking Scheme

The major tasks of using PSO in the watermarking approach are: preventing any image degradation, improving the image quality of the watermarked image, and securing the watermark strength after an attacking procedure. PSO has been used extensively as a multi-objective function to find the most suitable bands in the two level DWT coefficients. At first, it searches for the best blocks for the embedding positions; next, it modifies the contrast of the selected blocks using the embedding algorithm. In the evolution process of PSO, the embedding positions within the host image are simulated as swarms, and then they are obtained by particle's positions and speeds that employ both of PSO operators and cross-correlation function.

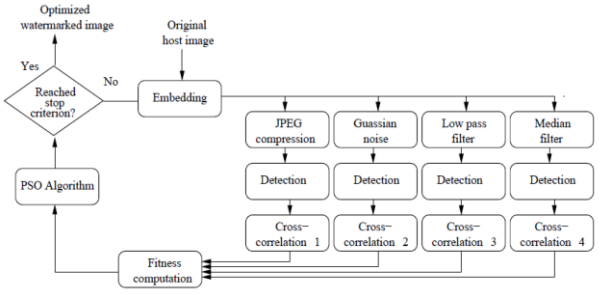

Fig 3: An illustrative diagram for the proposed watermarking system

B. Swarm Encoding

PSO's swarms are represented by a sequence of numbers equal to (N X M) that are initialized randomly; each swarm represents an embedding position that holds only one bit of the binary watermark. So, only one bit of the watermark is embedded into the selected block, and the coefficients chosen for embedding the watermark bits are indexed by swarms. The number of the embedding blocks are equal to (N X M), and $log2(N$ X $M)$ bits stand for the positions of the watermark bits. The watermark used in this work has N = 32 and M = 32. Thus, there are 1024 bits in the watermark, and, 10-bit number is needed to represent the position of one bit. In this aspect, the PSO swarms are used to adjust the position values, and the PSO operations are applied iteratively to optimize the watermarked image, where the optimal or near optimal embedding positions should be achieved.

C. Fitness Function

The Normalized Cross-correlation (NC) [17] has been evaluated as a measure of profit during the evolution of PSO. The watermark (W_e) is extracted from (X_{oa}), and then the NC value between the embedded watermark and the corresponding extracted watermark is calculated. The (NC) between the embedded watermark $W(i, j)$ and the extracted watermark $W_e(i, j)$ was defined as given in Equation 1 [17].

$$NC = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M} W(i,j)W_e(i,j)}{\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{M} W(i,j)^2}\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{M} W_e(i,j)^2}} \quad (1)$$

Where i and j are the indexes of the binary watermark image. NC is normalized by the energy of the watermark to give a unity value as the peak correlation. The watermark is detected exactly if NC approaches to 1. The fitness function can be defined by combining both of the robustness and the image quality into one relation. Though, the image quality is not included in the fitness criterion. The fitness function of PSO was defined as given in Equation 2.

$$Fitness = \sum_{i=1}^{4}(NC_i) \quad (2)$$

The counter from 1 to 4 indicates the number of attacking procedures.

5. Experimental Results and Discussion

In order to exploit the proposed technique, six host images of size 256 X 256 were conducted. Moreover, the watermark presented in the experimental results has the size of 32 X 32. Four major attacking schemes were employed in this work for the purpose of valuation the robustness and performance of the wavelet intelligent scheme; Low Pass Filter (LPF) attack with different normalized radiuses, Median Filter (MF) attack with different windows sizes, Gaussian noise attack with different strengths, and JPEG compression attack with quality factor of 70%. The original girl image and it's watermarked version without adding any attacking procedure, as well as the embedded and the extracted watermarks are shown in Figure 4. It's obvious from Figure 4 that the visual results of the watermarked image and the extracted watermark are very similar to the host image and the embedded watermark, respectively. A more conceptual illustration of the image quality can be educed by exposing the watermarked image to the four major attacks as shown in Figure 5. It's intelligible from Figure 5 that the watermarked images are perceptually equal to the originals in terms of visuality that is, the proposed scheme is robust to the susceptible attacks. Moreover, this result may figure out that the proposed scheme approaches to the optimal embedding configuration. The corresponding extracted watermarks from the girl image using 25 generations under the effect of the above mentioned attacks are shown in Figure 6.

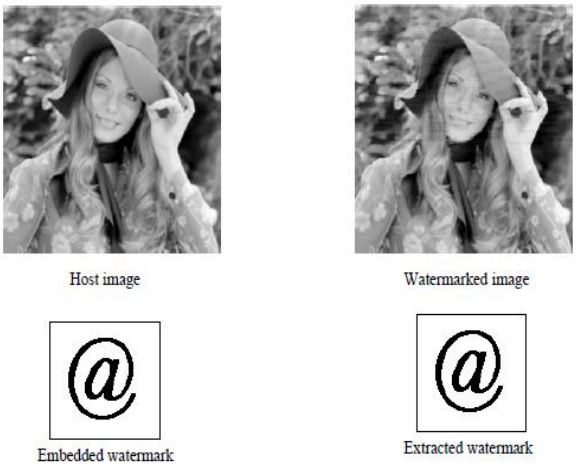

Fig 5: The results of the proposed approach without adding any attack

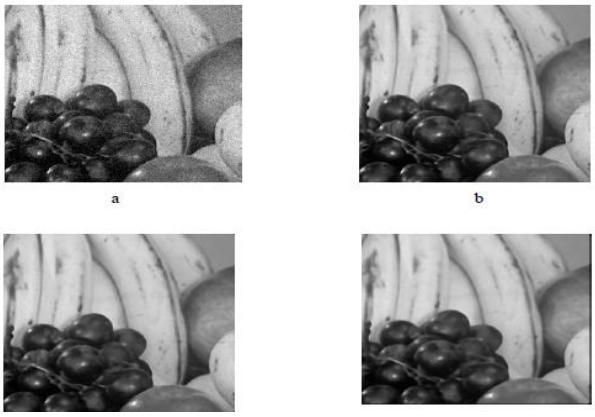

Fig 4: The extracted watermarked images after applying the major attacks: a) 3 X 3 low pass filtered b) 3 X 3 median filtered c) 5% Gaussian noise added d) JPEG compressed image with compression ratio of 70%

Figure 4 assures that the watermarks are still detectable with distinct similarity values even after exposing the watermarked images to some image processing attacks. Also, the NC values between the embedded and extracted watermarks are satisfied and convinced. Thus, Figures 5 and 6 affirm the invisibility and the robustness of the proposed approach. Figure 7 shows the watermarked images when they are subjected to Gaussian attack with different ratios. Furthermore, the extracted watermarks under the effect of Gaussian noise with different ratios are shown in Figure 8. Figure 8 reveals the fact that the watermark could still be well revealed even after the watermarked image was attacked by the Gaussian noise using high Gaussian rate. Utilizing PSO distinctly can be inferred from Figure 9. This figure approves that the selection of the optimal cover blocks boost the visuality of the extracted watermark and the cross-correlation value, which in turn increases the robustness of the proposed scheme. The performance of the PSO-based wavelet watermarking scheme is verified through several experiments with different number of generations under various attacks. As an example, Figure 10 shows the extracted watermarks from the optimized girl image using different number of generations, considering that the watermarked image has been affected by Gaussian attack.

Fig 6: Extracted watermarks from the girl image: a) Low pass filter b) Median filter c) Gaussian noise d) JPEG compression

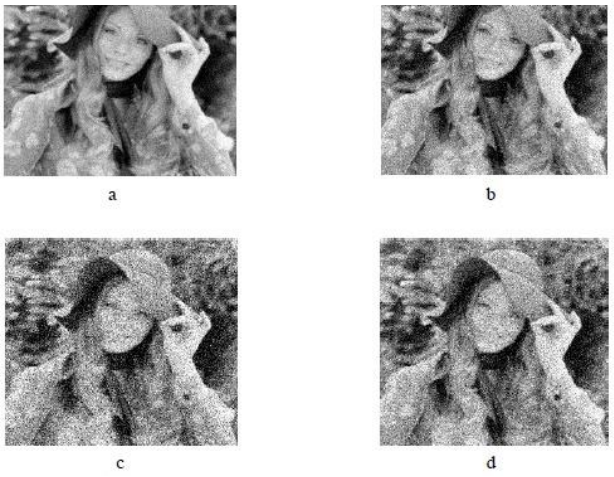

Fig 7: Extracted watermarked images after they are exposed to Gaussian noise: a) 5% Gaussian noise added b) 4% Gaussian noise added c) 3% Gaussian noise added d) 1% Gaussian noise added

It can be perceived from Figure 10 that, as the number of generations increases, the watermarks are extracted more meticulously, though, more execution time is needed. Another example as shown in Figure 11 evinces the extracted watermarks from different host images which are influenced by JPEG attack, with quality factor of 80%. The efficacy of the proposed watermarking approach is evaluated mathematically by measuring three criteria: PSNR, NC values, and the average fitness.

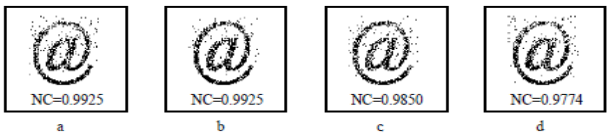

Fig 8: Extracted watermarks under Gaussian attack: a) 5% Gaussian noise added b) 4% Gaussian noise added c)3% Gaussian noise added d) 1% Gaussian noise added

Fig 9: a) Extracted watermark without PSO, b) Extracted watermark with PSO-based scheme using 25 generations

Fig 10: Extracted watermarks under Gaussian noise, (a) generations = 25, (b) generations = 50, (c) generations = 100, (d) generations = 150

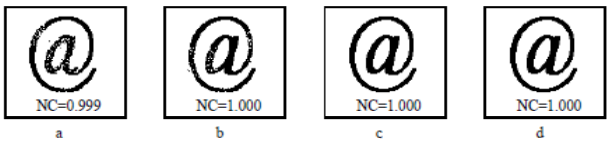

Fig 11: Extracted watermarks under JPEG attack from different host images using 100 generations, (a) Lena image, (b) Fruit image, (c) Baboon image, (d) Boat image

Table 1: THE PSNR FOR SOME IMAGES UNDER VARIOUS ATTACKS

Host image	*Low pass filter*	*Median filter*	*Gaussian noise*	*JPEG compression*
Girl	*39.89*	*40.97*	*43.00*	*48.30*
Boat	*40.01*	*42.90*	*46.40*	*49.51*
Baboon	*41.88*	*43.91*	*46.09*	*49.08*
Lady	*42.42*	*44.13*	*48.00*	*50.17*
Fruit	*42.93*	*43.70*	*43.99*	*44.59*
Lena	*41.98*	*43.96*	*45.34*	*47.95*

A. Visibility Measure Using PSNR Criterion

The watermarked image quality is represented by (PSNR) between X and $X_{(e)i}$. PSNR relies on the fact that the original and the watermarked images are almost nearly similar. PSNR is formulated as given in Equation 3 [17].

$$PSNR_i = 10 \text{ X } \log_{10} \text{X } \left(\frac{255^2}{MSE_i}\right) [dB] \qquad (3)$$

Whereas, (MSE) is the Mean Square Error between the original and the watermarked images, and is defined as given in Equation 4.

$$MSE_i = \frac{1}{H \text{ X } V} \sum_{i=1}^{H} \sum_{j=1}^{V} [X(i,j) - X_{(e)i}]^2 \qquad (4)$$

Where X(i, j) and $X_{(e)i}$(i, j) denote the intensity values of the same pixel position at (i, j) of X and X_e of the current iteration *i*. The higher the PSNR value is, the less perceptible the embedded watermark will be to the human eye. As well, the higher the PSNR is for the recovered watermark, the easier is to identify. The corresponding PSNR values between the original and watermarked images under the associated attacks are illustrated in Table 1. As a consequence, it can be observed from Table 1 that the intelligent scheme is efficient, and provides high image quality values, while still offers effective resistance against the associated attacks. The best evolved PSNR value is 50.17, and is recorded in the Lady image under JPEG compression attack.

Table 2. The NC values against the evolved attacks

Host image	Low pass filter	Median filter	Gaussian noise	JPEG compression
Girl	0.8912	0.9761	0.9860	1.000
Boat	0.9210	0.9521	0.9620	1.000
Baboon	0.8248	0.9841	0.9844	1.000
Lady	0.9142	0.9132	0.9230	1.000
Fruit	0.9378	0.9700	0.9723	1.000
Lena	0.9248	0.9601	0.9630	0.9999

Table 3. The PSNR values under Gaussian attack with different number of generations

Host image	0	25	50	75	100	150
Girl	35.42	43.00	42.10	44.91	47.9	50.78
Boat	38.90	46.40	43.10	45.06	48.57	53.17
Baboon	36.24	46.09	44.99	46.00	47.60	49.23
Lady	37.23	44.13	48.00	48.96	50.05	50.86
Fruit	35.23	43.99	46.93	47.19	49.38	50.91
Lena	34.56	45.34	46.12	48.23	50.04	51.70

B. Robustness Measure Using Cross-Correlation

The NC function as defined in Equation 1 is used to evaluate the robustness of the proposed scheme. The NC values of all the retrieved watermarks for each type of attacks of the tested images are demonstrated in Table 2. Actually, if the NC value approaches to 1, then, the hidden watermark can be detected correctly. As shown in Table 2, the NC values for all the extracted watermarks are approximated to 1. In this way, robustness is improved for all possible attacks, and this fact can be observed absolutely. The PSNR values under the Gaussian attack with different number of PSO's generations are stated in Table 3. It can be seen from Table 3 that the PSNR value is improved as the number of PSO's iterations is increased. Also, the quality of the watermarked image can be significantly improved when the generation number is large enough. The NC values for the extracted watermarks which are attacked by Gaussian noise using different number of generations are displayed in Table 4. It can be established from Table 4 that as the number of generations increases, the NC values approach to unity. This concludes that the optimization performance of the PSO-based wavelet scheme converges to an optimal value after approximately 100 generations. At last, the PSNR was computed for different windows of LPF and MF as shown in Tables 5 and 6.

Table 4. The NC values under Gaussian attack with different number of generations

Host image	0	25	50	75	100	150
Girl	0.88001	0.9860	0.9915	0.9989	1.000	1.000
Boat	0.9010	0.9620	0.9706	0.9757	0.9867	0.9977
Baboon	0.9224	0.9844	0.9860	1.000	1.000	1.000
Lady	0.8604	0.9230	0.9626	0.9905	1.000	1.000
Fruit	0.8937	0.9723	0.9809	0.9898	0.9989	1.000
Lena	0.9012	0.9630	0.9723	1.000	1.000	1.000

Table 5. Extracted watermarked images under LPF attack with 25 generations

Low pass filter	Image	PSNR
5 x 5	Girl	40.01
	Boat	40.09
	Baboon	41.98
	Lady	42.49
	Fruit	42.93
	Lena	42.07
7 x 7	Girl	40.03
	Boat	41.13
	Baboon	41.98
	Lady	42.49
	Fruit	42.94
	Lena	42.08

Table 6. Extracted watermarked images under MF attack with 25 generations

Median filter	Image	PSNR
5 x 5	Girl	41.00
	Boat	42.94
	Baboon	43.98
	Lady	45.00
	Fruit	43.70
	Lena	43.97
7 x 7	Girl	41.02
	Boat	43.01
	Baboon	43.98
	Lady	45.01
	Fruit	43.70
	Lena	43.99

As a conclusion, the PSO-based discrete wavelet scheme successfully optimizes the watermark embedding, and nearly finds the optimal embedding positions, this yields to improving the image quality and watermark strength, though more computation time is still needed. This reveals the fact that PSO could be very efficient for use in watermarking whereas it can survive LPF, MF, Gaussian noise, and JPEG compression.

C. Average Fitness Criterion

The employed PSO's fitness has been used as an evaluation criterion to rate the watermarking scheme. The average fitness can be defined as given in Equation 5.

$$Averagefitness = \frac{1}{4}\sum_{i=1}^{4}(\mathrm{NC}_i) \qquad (5)$$

Table 7 shows the average fitness against all the applied attacks when the number of PSO's iterations is 25. The presented results in Table 7 corroborate the appropriateness of the intelligent watermarking scheme against the image processing attacks.

Table 7. The average fitness against the attacking schemes

Host image	Average fitness
Girl	0.966825
Boat	0.968275
Baboon	0.952225
Lady	0.956850
Fruit	0.976925
Lena	0.971175

D. Comparison Between PSO and GA Based Scheme

The proposed two levels DWT watermarking scheme based on PSO is compared with the GA-based the same scheme. The NC values for each type of attack that are impacted upon on the watermarked images optimized by the GA-based scheme are presented in Table 8. Verily, the entire NC values in Table 8 approach to 1, this fact shows the complete watermark extraction. Furthermore, the obtained result based on GA-scheme is almost similar to the PSO-based scheme. Notwithstanding, more computation time is needed for the GA-based scheme. All the experiments are done on a desktop computer with Genuine Intel(R) CPU 4 T2400 @ 1.83 GHz and 1.00 GB of RAM.

Table 8. The NC values against the evolved attacks using GA-based scheme

Host image	Low pass filter	Median filter	Gaussian noise	JPEG compression
Girl	0.8900	0.9789	0.9999	0.9998
Boat	0.9189	0.9545	1.000	0.9999
Baboon	0.8198	0.9901	0.9989	1.000
Lady	0.9139	0.9134	1.000	1.000
Fruit	0.9365	0.9719	0.9999	1.000
Lena	0.9199	0.9698	0.9999	0.9996

E. PSO and GA Parameters Settings

The values of PSO's and GA's parameters should be chosen carefully to get the optimized watermarked image within a reasonable period of time. In the PSO based approach, the number of generations is chosen to be 100, on the other hand, in the GA based approach, the population, the mutation and the crossover probabilities are 100, 0.03 and 0.93, respectively. Tables 9 and 10 sum up the parameters settings for the PSO and GA-based watermarking experiments, respectively.

Table 9. Parameters setting for the PSO-based experiments

Parameter description	Value
Number of particles	7225
Generations	100
Acceleration constants	1.2
Dimension	1
Momentum weight	0.9

Table 10. Parameters setting for the GA-based experiments

Parameter description	Value
Number of chromosomes	7225
Population	100
Mutation probability	0.03
Crossover probability	0.93

6. Conclusions and Future Works

An intelligent watermarking scheme in discrete wavelet transform is proposed in this paper. Particle Swarm Optimization (PSO) proceeds to find the optimal embedding blocks based on the contrast of the host image. The hidden binary watermark was extracted correctly in all kinds of the four attacks identified in this work. The experimental results clarified that PSO can provide an intelligent approach to the digital watermarking schemes. Further works will be performed in many directions: supporting parallel PSO with multi-objectives in digital watermarking, updating the embedding algorithm such that is can resist scaling and cropping attacks, and finally, a combination of the peak signal to noise ratio and the cross-correlation function will be into the fitness function.

References

[1] I.-K. Yeo and H. J. Kim, "Modified patchwork algorithm: a novel audio watermarking scheme.," IEEE Transactions on Speech and Audio Processing, vol. 11, no. 4, pp. 381–386, 2003.

[2] P. Meerwald and A. Uhl, "Watermarking of raw digital images in camera firmware: embedding and detection," in Proceedings of the 3rd Pacific Rim Symposium on Image and Video Technology, PSIVT '09, vol. 5414 of Lecture Notes in Computer Science, (Tokyo, Japan), pp. 340–348, Springer, Jan. 2009.

[3] E. Brannock, M. Weeks, and V. Rehder, "Detecting filopodia with wavelets," in in Proceedings of the 2004 International Symposium on Circuits and Systems, 2006.

[4] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding - a survey," in Proceeding of IEEE, pp. 1062–1078, 1999.

[5] G. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data," IEEE Signal Processing Magazine, vol. 17, p. 2043, 2000.

[6] J. M. Kim, "A digital image watermarking scheme based on vector quantisation," in IEICE Trans. Inf.&Syst, vol. E85-D., pp. 305–303, IEEE Press, 2002.

[7] A. Khan and A. M. Mirza, "Genetic perceptual shaping: Utilizing cover image and conceivable attack information during watermark embedding," Information Fusion, vol. 8, pp. 354–365, October 2007.

[8] W. Zhicheng, H. Li, J. Dai, and S. Wang, "Image watermarking based on genetic algorithm," in ICME IEEE, p. 11171120, 2006.

[9] W. C. Chu, "Dct-based image watermarking using subsampling," IEEE Trans. Multimedia, vol. 1, no. 5, pp. 34–38, 2003.

[10] C.-S. Shieh, H.-C. Huang, F.-H. Wang, and J.-S. Pan, "Genetic watermarking based on transform-domain techniques," The journal of the Pattern Recognition Society, no. 37, p. 555 565, 2004.

[11] C.-C. Chen and C.-S. Lin, "A ga-based nearly optimal image authenticationapproach," International Journal of Innovative Computing,Information and Control ICIC International, vol. 3, no. 3, p. 631640, 2006.

[12] M. Braik, A. Sheta, and A. Ayesh, "Particle swarm optimisation enhancement approach for improving image quality," Int. J. InnovativeComputing and Applications, vol. 1, no. 2, pp. 138–145, 2007.

[13] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," IBM Systems Journal, vol. 35, no. 3&4, 1996. MIT Media Lab.

[14] N. F. Johnson, Z. Duric, and S. Jajodia, Information Hiding: Steganography and Watermarking - Attacks and Countermeasures (Advances in Information Security, Volume 1), vol. 1. Kluwer Academic Publishers, Norwell, MA, 2006.

[15] G. W. Braudaway, "Protecting publicly-available images with an invisible image watermark," in ICIP (1), pp. 524–527, 1997.

[16] R. Tachibana, "Audio watermarking for live performance," in Proc. of SPIE Int. Conf. on Security and Watermarking of Multimedia Contents V, vol. 5020, (Santa Clara, USA), pp. 32–43, January 2003.

[17] M. Ketcham and S. Vongpradhip, "Intelligent audio watermarking using genetic algorithm in dwt domain," World Academy of Science, Engineering and Technology, pp. 336–341, Jan. 2007.