Research Journal of Applied Sciences, Engineering and Technology 5(12): 3312-3319, 2013
DOI:10.19026/rjaset.5.4573
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: June 09, 2012 Accepted: July 18, 2012 Published: April 10, 2013

Research Article

Watermark Extraction Optimization Using PSO Algorithm

[1]Mohammad Dehghani Soltani, [2]Ali Seyedjafari and [2]Hamid Dehghani
[1]Amirkabir University of Technology, Tehran, Iran
[2]Islamic Azad University of Bushehr, Bushehr, Iran

Abstract: In this study we propose an improved method for watermarking based on ML detector that in comparison with similar methods this scheme has more robustness against attacks, with the same embedded length of logo. Embedding the watermark will perform in the low frequency coefficients of wavelet transform of high entropy blocks (blocks which have more information). Then in the watermark extraction step by using PSO algorithm in a way that maximum quality in comparison with previous methods obtain, by optimizing the Lagrange factor in the Neyman-Peyrson test, we extract the watermark. Finally, performance of proposed scheme has been investigated and accuracy of results are shown by simulation.

Keywords: ML receiver, PSO algorithm and Neyman-Peyrson test, watermarking, wavelet transform

INTRODUCTION

Digital watermark is a process in which some information is embedded within a digital media, so that the inserted data becomes part of the media (Akhaee *et al*., 2009). Watermark is classified in two categories. First category uses the watermark as a transmission code. In this case the decoder should detect the whole transmitted information correctly (Cox *et al*., 1999; Ramkumar and Akansu, 2001). In the second category, the watermark is used for authorizing the originality of the medium. In this system, detector should recognize the existence of certain pattern (Kutter, 1998).

There are some ways to embed watermark data in a host image such as additive or multiplicative methods (Bi *et al*., 2007). For additive methods optimum detection has been investigated in some literatures (Wang *et al*., 2002; Donoho and Johnsone, 1994). Since multiplicative methods depend on the content of image, these methods are more robust against attacks so they are preferred to additive methods (Akhaee *et al*., 2010). The correlation detector for multiplicative watermarking has been utilized in Bi *et al*. (2007). A robust detector for multiplicative method in DCT, DWT and DFT domain was proposed in Akhaee *et al*. (2010). Distribution of high frequency coefficients of DCT and DWT are generalized Gaussian however, the distribution of amplitude of DFT coefficients are weibull (Kalantari *et al*., 2010). In (Ramkumar and Akansu, 2001), a method based on selection of optimum region for watermarking has been proposed. Based on the distribution of watermarked image coefficients, varieties of optimal and locally optimal detectors have been proposed (Akhaee *et al*., 2010; Kalantari *et al*., 2010). In Akhaee *et al*. (2009) a multiplicative and semi-blind method for watermarking was proposed. It utilized the low frequency wavelet coefficients in order to increase the robustness of the algorithm. Then it designed an optimum ML detector with consideration of Gaussian distribution for coefficients and it used a multi-objective optimization technique in order to have a balance between robustness and accuracy of watermarked image.

Ng and Garg (2005) detect digital watermark in the transform domain by using maximum-likelihood, the threshold value is obtained by means of Neyman-Pearson criterion. Maximum-Likelihood (ML) detection schemes based on Bayes' decision theory have been considered for image watermarking in transform domain (Barni *et al*., 2001; Kwon *et al*., 2002; Ng and Garg, 2004). The Neyman–Pearson criterion is used to derive a decision threshold to minimize the probability of missed detection subject to a given probability of false alarm. To achieve optimum behavior of the ML detector, a Probability Distribution Function (PDF) that correctly models the distribution of the transform coefficients is required.

The Particle Swarm Optimizer (PSO) (Eberhart and Kennedy, 1995; Kennedy and Eberhart, 1995) is a relatively new technique. Although PSO shares many similarities with evolutionary computation techniques, the standard PSO does not use evolution operators such as crossover and mutation. PSO emulates the swarm behavior of insects, animals herding, birds flocking and fish schooling where these swarms search for food in a collaborative manner. Each member in the swarm adapts its search patterns by learning from its own experience and other members' experiences. These

Corresponding Author: Mohammad Dehghani Soltani, Amirkabir University of Technology, Tehran, Iran

phenomena are studied and mathematical models are constructed. In PSO, a member in the swarm, called a *particle,* represents a potential solution which is a point in the search space. The global optimum is regarded as the location of food. Each particle has a fitness value and a velocity to adjust its flying direction according to the best experiences of the swarm to search for the global optimum in the D-dimensional solution space. The PSO algorithm is easy to implement and has been empirically shown to perform well on many optimization problems.

A brief review of PSO algorithm: In the bird community algorithm, particles' position will be change according to the history of particle motion and their neighbors. Each particle has a position that we show it with $\vec{x}_i(t)$. It represents position of P_i^{th} particle in the time t. In addition to have a position, each particle needs a velocity (Bird and Li, 2006):

$$\vec{v}_i(t) = \vec{x}_i(t) - \vec{x}_i(t-1)$$

The stages of this algorithm are as follow:

- First we form an initial population randomly
- Determining eligibility of particles using their current position
- Comparison of the particle's current competence and their best experience and required replacement

  if $F(P_i) > pbest_i$ then:

  - $pbest_i = F(P_i)$
  - $\vec{x}_{pbest_i} = \vec{x}_i(t)$
- Comparing the current competence of each particle with the best previous result of all particles and required replacement as follow

  if $F(P_i) > gbest$ then:

  - $gbest = F(P_i)$
  - $\vec{x}_{gbest} = \vec{x}_i(t)$
- Set the velocity vector for each particle:

$$v_{id}(t+1) = w.v_{id}(t) + C_1.rand(pbest_{id} - xid + C2.randgbestd - xid$$

where in the above equation, w is the inertia weight, C_1 and C_2 are learning factors and $rand$ is a random number in the interval (0,1). To avoid divergence of algorithm, the final velocity of each particle is limited.

- Move particles to their new position:
  - $\vec{x}_i(t) = \vec{x}_i(t-1) + \vec{v}_i(t)$
  - $t = t + 1$
- Go to step 2 and repeat the algorithm to reach convergence

In this study with PSO algorithm for optimizing the threshold value in the obtained detecting equation, output error rate reduces much.

PROPOSED METHOD

The method proposed in this study is a semi-blind technique which is obtained from modifying the detector of Akhaee *et al*. (2009). In this model we design the detector based on PSO algorithm that in addition to have high quality it has more robustness against attacks in comparison with (Akhaee *et al*., 2009) and previous methods.

Embedding method: For embedding information such as a logo or a series of bits in an original image we use the following approach. First we divide image into non-overlapped blocks of size $2^n \times 2^n$ $(n = 2,3,4)$ and then we choose high entropy blocks (i.e., blocks with high information) according to a threshold which determine the bit rate. Then, two dimensional discrete wavelet transform applies to these determined blocks. Now assume in one block, w_i's are considered as wavelet coefficients with mean μ and variance σ^2. For embedding the watermark, we multiply coefficients by α to insert bit "1" or we multiply them by $1/\alpha$ to insert bit "0", i.e., watermarking will be done via scaling the coefficients according to the following process:

$$w_i' = w_i \times \alpha : \text{embedding "1"} \quad (1)$$

$$w_i' = w_i \times \frac{1}{\alpha} : \text{embedding "0"} \quad (2)$$

In the above equation, α is a factor with the value greater than one and named as strength factor. Also i is the block index.

Watermark decoding: As mentioned because of the Gaussian coefficients we can use ML detector in the detecting process. In this process we assume position, mean and variance of watermarked blocks are available in the receiver. Thus, we optimize the receiver according to this information (Akhaee *et al*., 2009).

In the receiver after noise or other attacks, we receive y_i's which are wavelet coefficients of received image. These coefficients are a mixture of wavelet coefficients w_i and zero mean additive white Gaussian noise. Since wavelet coefficients and noise are both Gaussian and are uncorrelated with each other and themselves, the distribution of y_i is as follow:

$$y_{i|1} = \alpha.w_i + n_i \rightarrow y_{i|1} \sim N(\alpha\mu, \sigma_{y|1}^2) \quad (3)$$

and similarly for bit "0" we have:

$$y_{i|0} = \alpha^{-1}.w_i + n_i \rightarrow y_{i|0} \sim N(\alpha^{-1}\mu, \sigma_{y|0}^2) \quad (4)$$

where,

$$\sigma_{y|0}^2=\alpha^{-2}\sigma^2+\sigma_n^2 \text{، } \sigma_{y|1}^2=\alpha^2\sigma^2+\sigma_n^2 \quad (5)$$

and in these equation σ_n^2 is the variance of noise. Because wavelet coefficients are decimated in each level of decomposition, we assumed that they are i.i.d in our proposed method. Let Y be the vector of received wavelet coefficients and we want to determine whether Y belongs to w_0 or w_1.

where,

w_0 : Wavelet coefficients distribution if bit "0" embedded

w_1 : Wavelet coefficients distribution if bit "1" embedded

A decision rule based on the probabilities may be written as:

$$q(w_0|Y) \underset{w_1}{\overset{w_0}{\gtrless}} q(w_1|Y) \quad (6)$$

By using the Bayes theorem, we can calculate the a posteriori probability $q(w_i|Y)$ from the a priori probability P_i and the conditional density function $P_i(Y) = P(Y|w_i)$ as:

$$q(w_i|Y) = \frac{P(w_i)P(Y|w_i)}{P(Y)} \quad (7)$$

We can eliminate P(Y) from the both side of the decision rule. So:

$$P(w_0)P(Y|w_0) \underset{w_1}{\overset{w_0}{\gtrless}} P(w_1)P(Y|w_1) \quad (8)$$

We take the minus logarithm of both sides:

$$-\mathrm{Ln}(P(Y|w_0)) + \mathrm{Ln}(P(Y|w_1)) \underset{w_0}{\overset{w_1}{\gtrless}} \mathrm{Ln}\left(\frac{P(w_0)}{P(w_1)}\right) \quad (9)$$

Because the $P(Y|w_i)$s' have Gaussian distribution with expected values μ_{y_i} and σ_{y_i} and by using the definition of Gaussian distribution and distance function, Eq. (13) simplifies as:

$$\frac{1}{2}(Y-M_0)^T\Sigma_0^{-1}(Y-M_0)-\frac{1}{2}(Y-M_1)^T\Sigma_1^{-1}(Y-M_1)$$

$$+\frac{1}{2}Ln(\frac{|\Sigma_0|}{|\Sigma_1|}) \underset{w_0}{\overset{w_1}{\gtrless}} Ln(\frac{P(w_0)}{P(w_1)}) \quad (10)$$

where,

$$M_0 = \mu_{y|0} \times Ones(N,1) \quad (11)$$

$$M_1 = \mu_{y|1} \times Ones(N,1) \quad (12)$$

$\Sigma_0 = \sigma^2{}_{y|0} \times I_{N\times N}$: Covariance matrix for received coefficients if "0" has been embedded.

$\Sigma_1 = \sigma^2{}_{y|1} \times I_{N\times N}$: Covariance matrix for received coefficients if "1" has been embedded.

Substituting the covariance matrices, after some simplifications, Eq. (10) converted to:

$$\frac{1}{2\sigma^2{}_{y|0}}\sum_{i=1}^N (y_i-\mu_{y|0})^2 - \frac{1}{2\sigma^2{}_{y|1}}\sum_{i=1}^N \left(y_i-\mu_{y|1}\right)^2 +$$

$$\frac{N}{2}\mathrm{Ln}(\frac{\sigma^2{}_{y|0}}{\sigma^2{}_{y|1}}) \underset{w_0}{\overset{w_1}{\gtrless}} \mathrm{Ln}(\frac{P(w_0)}{P(w_1)}) \quad (13)$$

Then after some simplification we have:

$$\left(\frac{1}{\sigma^2{}_{y|0}}-\frac{1}{\sigma^2{}_{y|1}}\right)\sum_{i=1}^N y_i^2 - 2\mu\left(\frac{\alpha^{-1}}{\sigma^2{}_{y|0}}-\frac{\alpha}{\sigma^2{}_{y|1}}\right)\sum_{i=1}^N y_i \underset{w_0}{\overset{w_1}{\gtrless}}$$

$$2\ln\left(\frac{\sigma_{y|1}}{\sigma_{y|0}}\right) + 2\ln\left(\frac{P(w_0)}{P(w_1)}\right) - N\mu^2\left(\frac{\alpha^{-2}}{\sigma^2{}_{y|0}}-\frac{\alpha^2}{\sigma^2{}_{y|1}}\right) \quad (14)$$

Through (5) and (14), the best decision depends on estimation of the noise variance σ^2.

Consider the detector at the limiting values for high SNR, that is $\sigma_n \to 0$. So, we can simplify Eq. (14) as:

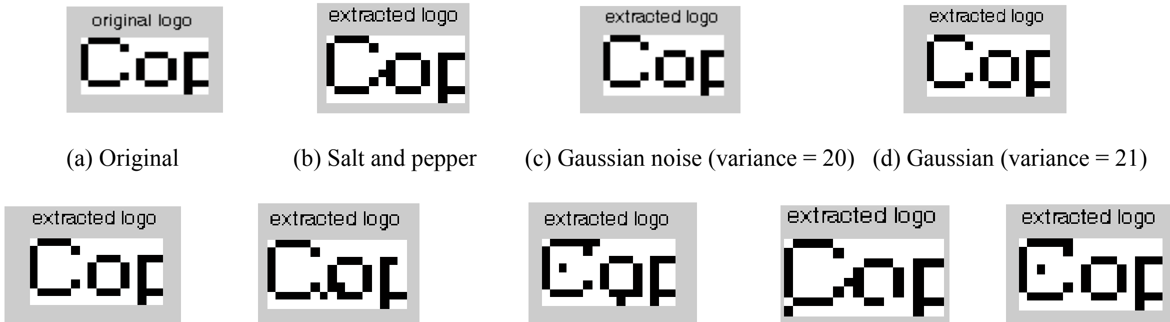
$$(\alpha^4-1)\sum_{i=1}^N y_i^2 - 2\alpha\mu(\alpha^2-1)\sum_{i=1}^N y_i \underset{w_0}{\overset{w_1}{\gtrless}}$$

$$4N\alpha^2\sigma^2\mathrm{Ln}(\alpha)+2\alpha^2\sigma^2\mathrm{Ln}(\frac{P(w_0)}{P(w_1)}) \quad (15)$$

The threshold value of (15) can be optimized based on the minimum detection error. In practice, the optimum value obtained empirically with numerical algorithm. In this study, we multiply k_0 named detection factor by the right side of Eq. (15) and use PSO optimization algorithm to set the optimum k_0 . In the other words, the threshold value of discriminant function can be modeled as Lagrange multiplier (λ) in the Neyman-Pearson test:

$$\lambda = k_0(4N\alpha^2\sigma^2 ln(\alpha) + 2\alpha^2\sigma^2 ln\left(\frac{P(w_0)}{P(w_1)}\right) \quad (16)$$

From this point of view, we use PSO algorithm to optimize Lagrange multiplier in our discriminant function:



(a) Original (b) Salt and pepper (c) Gaussian noise (variance = 20) (d) Gaussian (variance = 21)

(e) Blurring (f) Rotate with angle = 2° (g) Resize (scale = 0.5) (h) Medfilt2 (3 3) (i) JPEG (QP = 20)

Fig. 1: Robustness of our proposed method against attacks

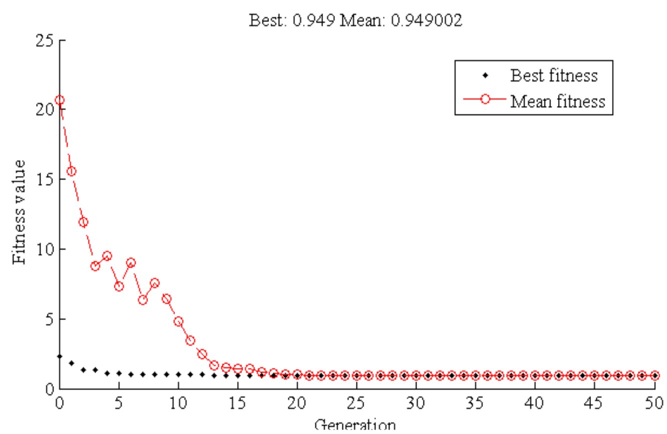


Fig. 2: Finding K_0 using PSO algorithm for salt and pepper attack (optimum value is $K_0 = 0.949$)

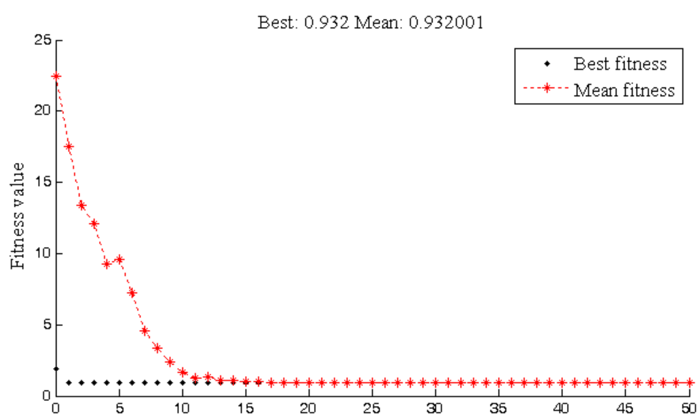


Fig. 3: Finding K_0 using PSO algorithm for blurring attack (optimum value is $K_0 = 0.932$)

$$(\alpha^4-1)\sum_{i=1}^{N} y_i^2 - 2\alpha\mu(\alpha^2-1)\sum_{i=1}^{N} y_i \underset{w_0}{\overset{w_1}{\gtrless}} \left(4N\alpha^2\sigma^2 Ln(\alpha)+2\alpha^2\sigma^2 Ln\left(\frac{P(w_0)}{P(w_1)}\right)\right) K_0 \qquad (17)$$

Priori probabilities in Eq. (17) depend on white and black pixel ratio in watermark data. These parameters with other side information should be available to the receiver.

SIMULATION RESULTS

Simulation results show performance of our proposed method against various kinds of attacks, such as resize, lossy compression, i.e., JPEG, rotation, median filter and additive white Gaussian noise

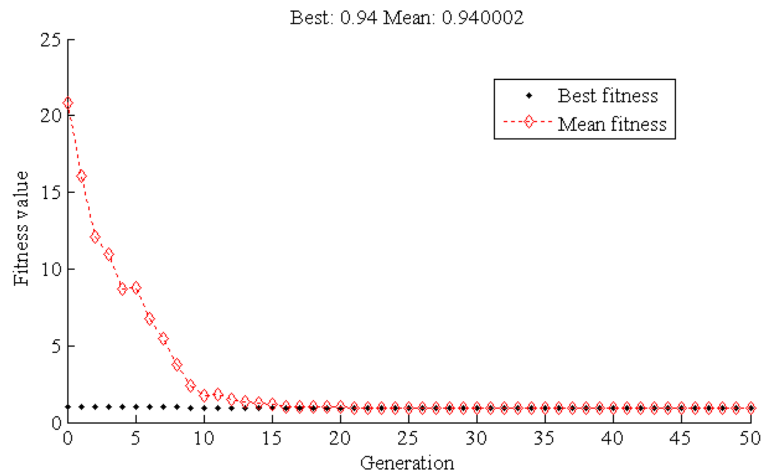


Fig. 4: Finding K_0 using PSO algorithm for median filter attack (optimum value is $K_0 = 0.94$)

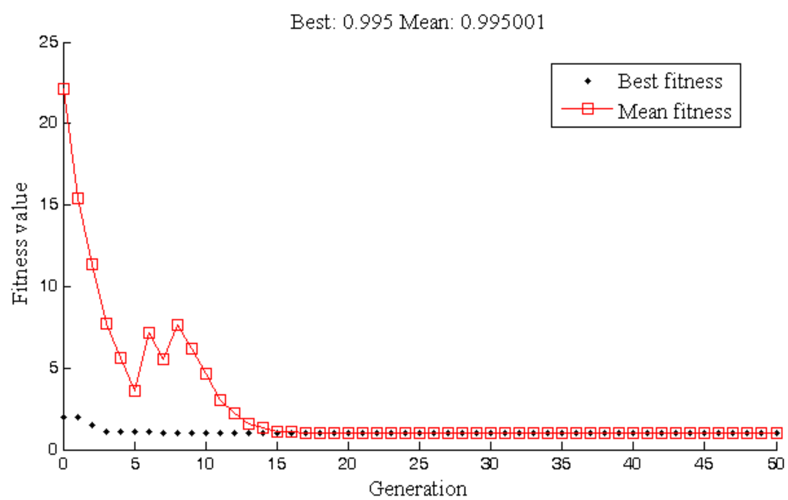


Fig. 5: Finding K_0 using PSO algorithm for additive white Gaussian noise with $\sigma_n^2 = 20$ (optimum value is $K_0 = 0.995$)

(AWGN) on the standard watermark images. Throughout our simulations, we use the Daubechies length-8 Symlet filters with one level of decomposition to compute the 2-D DWT. Although embedding in wavelet coefficients of high levels can enhance the quality of watermarked image, but due to diffuse error from low to higher levels after attacks, the sensitivity of error to attacks increases.

The parameters of PSO algorithm in simulations to obtain optimum detection factor K_0 are as follows:

$N = 100$; Number of particles
$Iter = 200$; Number of iterations
$X_{min} = 0$; $X_{max} = 2$; Range of search for K_0
$V_{max} = 0.4 \times X_{max}$; $V_{min} = -V_{max}$; Range of velocity
$W_{min} = 0.1$; $W_{max} = 0.6$; Range of inertia weight

Fitness function is equal to the difference between BER of extracted logo and embedded logo where C_1 and C_2 are learning factors.

The following results obtained via averaging through 100 runs for each test that are represented by error percentage for different attacks. Figure 1 shows extracted logo after popular attacks. As one can see this approach is a robust method against attacks and the extracted logo can be recognized easily. Among these attacks, watermarked image shows a weak performance against median filter that we could reduce detected errors from 13 bits to just 3 bits by means of PSO algorithm and adjusting K_0.

Figure 2 to 8 shows optimum Lagrange coefficient for different attacks. As we can see from these figures, PSO algorithm converges in low repetitions.

To show the improvement of our approach we present Table 1 as a comparison between our method and method proposed in Akhaee *et al*. (2009). To have a fair comparison we set the parameters of our method similar to Akhaee *et al*. (2009) as α = 1.0238, block size of 16×16 and code length (the length of

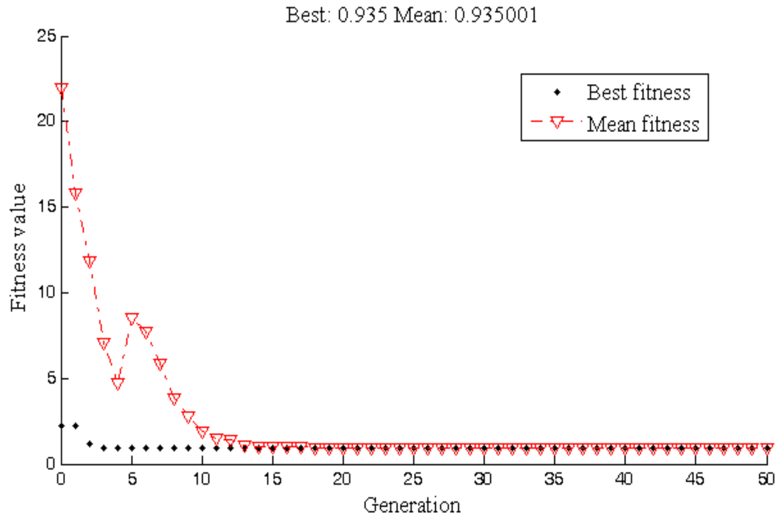


Fig. 6: Finding K_0 using PSO algorithm for rotation attack equal to 2° (optimum value is $K_0 = 0.935$)

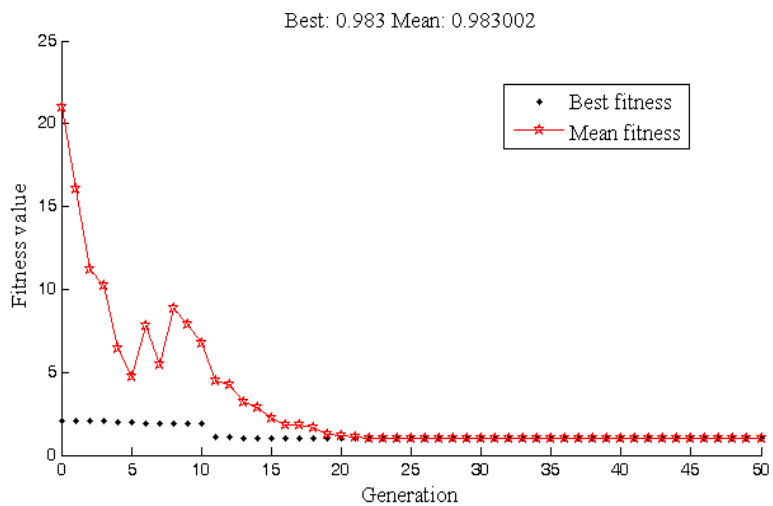


Fig. 7: Finding K_0 using PSO algorithm for scaling attack equal to 0.5 (optimum value is $K_0 = 0.983$)

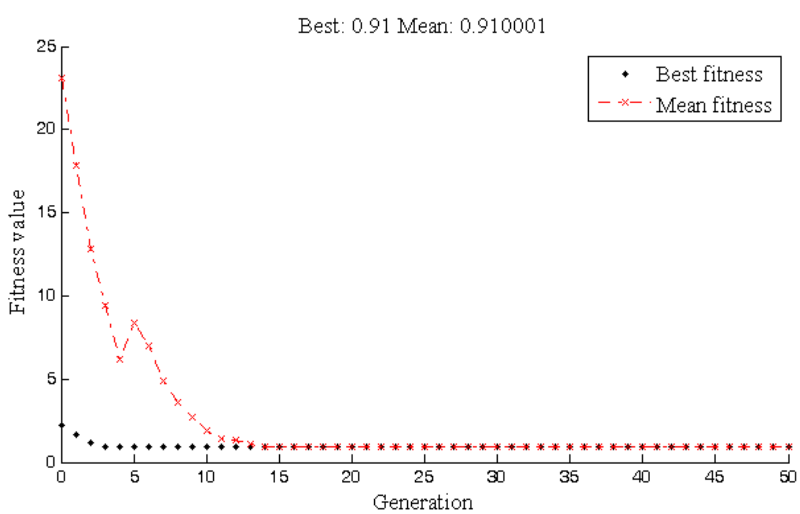


Fig. 8: Finding K_0 using PSO algorithm for JPEG (QP = 20)attack (optimum value is $K_0 = 0.91$)

Table 1: Comparison between proposed method by optimizing K_0 using PSO algorithm and Akhaee's method

	PSNR	BER	α	Size block	K_0
Salt and pepper	46.665	3	1.0238	16	1
Salt and pepper	**46.665**	**1**	**1.0238**	**16**	**0.949**
Gaussian variance = 21	46.665	6	1.0238	16	1
Gaussian variance = 21	**46.665**	**0**	**1.0238**	**16**	**0.995**
Gaussian variance = 20	46.665	0	1.0238	16	1
Gaussian variance = 20	**46.665**	**0**	**1.0238**	**16**	**0.995**
Blurring LEN = 3 θ = 5	46.665	2	1.0238	16	1
Blurring LEN = 3 θ = 5	**46.665**	**0**	**1.0238**	**16**	**0.932**
Rotate (angle = 2°)	46.665	4	1.0238	16	1
Rotate (angle = 2°)	**46.665**	**2**	**1.0238**	**16**	**0.935**
Resize (scale = 0.5)	46.665	7	1.0238	16	1
Resize (scale = 0.5)	**46.665**	**4**	**1.0238**	**16**	**0.983**
Medfilt2 (3 3)	46.665	23	1.0238	16	1
Medfilt2 (3 3)	**46.665**	**3**	**1.0238**	**16**	**0.94**
JPEG (QP = 20)	46.665	3	1.0238	16	1
JPEG (QP = 20)	**46.665**	**1**	**1.0238**	**16**	**0.91**

White rows and highlighted rows are related to Akhaee's method and our approach, respectively

information which is embedded in an image as logo) of 128 bits. As this table shows in all these attacks we reduced BER using this new approach by means of PSO algorithm.

CONCLUSION

As the simulation results show:

- Embedding data in the low frequency wavelet coefficients
- Using detector based on the bays theorem
- Optimizing threshold value by means of PSO algorithm, decrease detection error rate significantly in comparison with similar methods. Also imposing Arnold transform both on the host image and logo with specified iteration number, increase security of watermarking.

So, in the proposed method embedding data within a selected image by using priori known parameters according to the optimum condition, not only enhances robustness against attacks but also makes our method more secure.

REFERENCES

Akhaee, M.A., S.M.E. Saheaeian, F. Marvasti and B. Sankur, 2009. Robust scaling-based image multiplicative watermark technique using maximum likelihood decoder with optimum strength factor. IEEE T. Multimedia, 11: 822-833.

Akhaee, M.A., S.M.E. Saheaeian and F. Marvasti, 2010. Contourlet-based image watermarking using optimum detector in a noisy environment. IEEE T. Image Process., 19: 967-980.

Barni, M., F. Bartolini, A. De Rosa and A. Piva, 2001. A new decoder for the optimum recovery of nonadditive watermarks. IEEE T. Image Process., 10: 755-766.

Bi, N., Q. Sun, D. Huang, Z. Yang and J. Huang, 2007. Robust image watermarking based on multiband wavelets and empirical mode decomposition. IEEE T. Image Process., 16: 1956-1996.

Bird, S. and X. Li, 2006. Enhancing the robustness of a speciation-based PSO. Proceeding of Congress of Evolutionary Computation (CEC'06), IEEE Service Center, Piscataway, NJ 08855-1331, pp: 3185-3192.

Cox, I.J., M.L. Miller and A.L. McKellips, 1999. Watermarking as communications with side information. Proc. IEEE, 87(7): 1127-1141.

Donoho, D.L. and I.M. Johnstone, 1994. Ideal spatial adaptation via wavelet shrinkage. Biometrika, 81: 425-455.

Eberhart, R.C. and J. Kennedy, 1995. A new optimizer using particle swarm theory. Proceeding of 6th International Symp. Micromachine Human Sci., Nagoya, Japan, pp: 39-43.

Kalantari, N.K., S.M. Ahadi and M. Vafadust, 2010. A robust image watermarking in the ridgelet domain using universally optimum decoder. IEEE T. Circuits Syst. Video Technol., 20: 396-406.

Kennedy, J. and R.C. Eberhart, 1995. Particle swarm optimization. Proceeding of IEEE International Conference on Neural Networks, pp: 1942-1948.

Kutter, M., 1998. Watermarking resisting to translation, rotation and scaling. Proc. SPIE, 3528: 423-431.

Kwon, S.G., S.H. Lee, K.K. Kwon, K.R. Kwon and K.I. Lee, 2002. Watermark detection algorithm using statistical decision theory. Proceeding of IEEE International Conference on Multimedia Expo, 1: 561-564.

Ng, T.M. and H.K. Garg, 2004. Wavelet domain watermarking using maximum-likelihood detection. Proceeding of SPIE Conference Security, Steganography, Watermarking Multimedia Contents, 6: 5306.

Ng, T.M. and H.K. Garg, 2005. Maximum-likelihood detection in DWT domain image watermarking using Laplacian modeling. IEEE Signal Process. Lett., 12: 345-348.

Ramkumar, M. and A.N. Akansu, 2001. Capacity estimates for data hiding in compressed images. IEEE T. Image Process., 10: 1252-1263.

Wang, Y., J.F. Doherty and R.E. Van Dyck, 2002. A wavelet-based watermarking algorithm for ownership verification of digital images. IEEE T. Image Process., 11: 77-88.