Forensic-Based Investigation approach for an enhanced robust and secure image watermarking schemes

Najia Trache, Mohammed Salem, Mohamed Fayçel Khelfi

Abstract

In recent years, image watermarking has become the most active research in the information hiding field. This paper presents an application of a computational intelligence technique to obtain robust and secure image-watermarking schemes for data image transmission. The optimization goal is achieved via a new robust method based on the hybridization (in the digital domain) of the image-watermarking scheme using Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD). The Forensic-Based Investigation (FBI) optimization algorithm is considered to search for the best scaling factor and the appropriate location for the watermark insertion. The Arnold Transform (AT) encryption is also introduced to enhance the watermark image process security. To show the efficiency of the proposed schemes, several watermarked images are subjected to several attacks, and their imperceptibility and robustness are checked via structural similarity index measure (SSIM) and Normalized Correlation Coefficient (NCC) where the proposed schemes provide competitive simulation results. Statistical analysis is also carried out to prove the performance of the used optimization algorithm.

Keywords: Forensic-Based Investigation (FBI), Robustness and Imperceptibility, Image Watermarking, Singular Value Decomposition, Normalized Correlation Coefficient, Discrete Wavelet Transformation.

MSC 2020: 94A08, 68U10, 92C55, 90C27.

ACM CCS 2020: Computing methodologies

doi:10.56415/csjm.v32.13

1 Introduction

Watermarking is a technology developed to secure digital images from illegal alteration or manipulations during image transmissions [1]. The imperceptibility, robustness, capacity, and security of watermarking are important properties that characterize this technique used to ensure copyright protection without visible degradation to the host image. Imperceptibility means that the quality of the watermarked image cannot be strongly influenced. Robustness characterizes how the watermark in a watermarked image can be integrally extracted even when the watermarked image has been distorted by attacks. However, a stronger watermark can be used to enhance robustness but, in this case, the watermark becomes noticeable [20].

On the other hand, increasing the capacity decreases robustness. Consequently, a tradeoff between these requirements should be taken into account according to the application [2]. To satisfy these requirements for the embedded watermark, many techniques have been proposed in the literature and can be classified, based on the information required for the extraction/detection process, into blind, semi-blind, and non-blind categories. These methods can also be categorized as spatial or frequency domain techniques according to the embedding domain of the watermark.

Spatial domain techniques have high data hiding capacity but are less robust against various image processing attacks [12] since the embedding of the watermark is performed into the pixel values without any transformation. In contrast, the frequency domain methods such as Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Singular Value Decomposition (SVD), in which the watermark is embedded by modulating the magnitude of transform coefficients, offer enhanced robustness and imperceptibility.

On the other hand, watermarking embedding procedures involve single or multiple scaling factors used to determine the strength of the watermark. The selection of these scaling factors is generally cast as an optimization problem that can be solved to find the optimum factors that achieve robustness and improve the image quality of the water-

marked image. Examples of the optimization algorithms used for this purpose are Genetic Algorithm (GA) [13], Particle Swarm Optimization (PSO) [7], [14], Ant Colony Optimization (ACO) [9], Differential Evolution (DE) [6], Artificial Neural Network (ANN) [10], and Artificial Bee Colony [4]. These algorithms are aimed to reach two main goals, namely, searching for optimum parameters of watermarking (e.g., embedding strengths and threshold), and finding the most appropriate embedding positions [11].

In [13], for instance, a GA is combined with DWT and SVD to obtain optimum scaling factors to meet high robustness under a class of attacks. Similarly, the authors in [15] proposed a watermarking optimization using a GA to find the optimal frequency bands for embedding the watermarks. In [6], the Differential Evolution (DE) algorithm is used to find the scaling factors achieving the best balance between invisibility and robustness. In [19], the PSO has been applied to search for the embedding location of the integer DCT coefficients in a block, optimizing hence the requirement of imperceptibility and robustness in watermarking. The same method (PSO) has been used in [17] for the energy optimization of the embedding watermark to balance the quality and robustness of the watermarked image while the artificial immune system technique has been applied in the frequency domain presenting many advantages as compared to its spatial domain application [16].

Motivated by the above approaches, we present in this paper an enhanced computational watermarking approach leading to the best balance between invisibility and robustness. The optimum scaling factor is obtained by the Forensic-Based Investigation (FBI) optimization algorithm [5]. The latter is an intelligent computational algorithm inspired by the suspect investigation–location–pursuit operations of police agents with the important properties of parallelism, learning, adaptation, and robustness [5]. FBI has been developed in two steps corresponding to the investigation and pursuit of suspects by police officers; it has been applied in several domains [18], and in [3], an enhanced version is used to tackle optimization problems with frequency constraints.

The proposed approach is based on the DWT-SVD methods to embed the watermark in the singular value of the 3rd-level DWT approxi-

mation matrix of the host image. The proposed algorithm is secure due to applying Arnold Transform (see [13] and [11]) on the watermark image before the embedding progress. The obtained results in this study, which considers both gray and color host images, show further its efficiency in this topic as compared to the above-mentioned methods using other optimization algorithms in terms of structural similarity index measure (SSIM) [18] and Normalized Correlation Coefficient (NCC).

Generally, Peak Signal to Noise Ratio (PSNR) and Mean square Error (MSE) metrics are often used in watermarking because they are mathematically simple to implement and easy to compute but do not meet the criterion of perceived visual quality. We chose the SSIM metric because it provides a better assessment of the visual quality of the image compared to PSNR and MSE. It is based on the structure of the image and allows us to calculate the errors of perception and salience. It gives the average value of the structural similarity between the manipulated image and the reference image. Statistical analysis is also carried out to check the performance of the used optimization algorithm against other known optimization techniques.

This paper is organized as follows: Section 2 presents important preliminaries on the image watermarking procedures 'DWT', 'SVD', and 'AT', as well as the computational intelligence approach used in this paper, namely, the 'FBI'. Section 3 is devoted to the proposed approach consisting of a secure and imperceptible image watermarking process. In Section 4, we present the results of the simulation tests, and concluding remarks are given in Section 5.

2 Preliminaries

This section presents an overview of the main techniques used in the proposed approaches to obtain an imperceptible and robust image watermarking for the transmission data.

2.1 DWT, SVD, and Arnold Transform Techniques

Digital watermarking schemes consist of two processes: the embedding process and the extracting or detecting process after attacks (see

Figure 1). The first process aims to obtain a good imperceptibility that is evaluated from the obtained SSIM. The second process, which is the inverse of the first evaluated by the appropriate NCC, achieves robustness against different attacks.

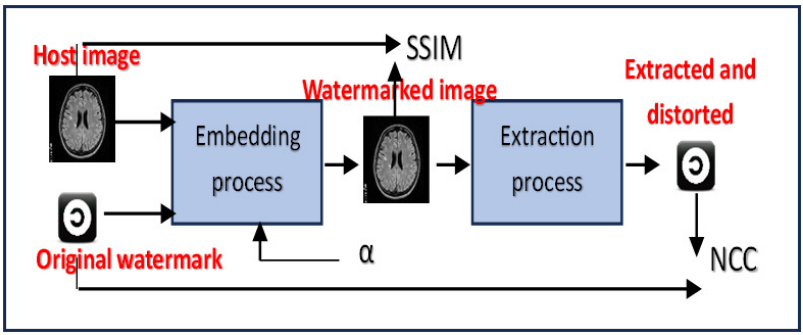


Figure 1. Digital watermarking flowchart

In general, digital watermarking is combined with the DWT and SVD techniques to enhance robustness and imperceptibility. The scheme inserts a watermark and modulates the coefficients of the magnitude of the DWT after the decomposition of the image into several sub-bands (depending on the level of decomposition). This ensures greater robustness against both image processing attacks (e.g., compression) and malicious attacks (e.g., rotation, cropping, scaling ...). The low-frequency sub-band is referred to as the approximate image LLn with n being the level of decomposition. The SVD decomposes an image I with size (M, N) as follows:

$$I = U * S * V', \tag{1}$$

where, U and V are two orthogonal unitary matrices (respectively $m \times m$ and $n \times n$) and S is a rectangular diagonal matrix with non-negative real numbers on the diagonal and has singular values. The singular values in a digital image exhibit good stability; a small perturbation in the image does not change significantly its singular values. Under the latter condition, the singular values of an image in an SVD-based watermarking scheme are modified to embed the watermark such that

[8]:

$$S_{new} = S_{old} + \alpha w, \tag{2}$$

where w is the watermark. The scaling factor ($0 < \alpha < 1$) controls the strength of the watermark to be inserted, hence, controlling the compromise between imperceptibility and robustness. The fact that the parameter α used in the embedding phase, as given in (2), is generally empirically computed doesn't allow for achieving fixed aims in terms of imperceptible and robust watermarking. To solve this issue, some heuristic methods have been used to optimize this scaling parameter α, as done in [13] and [14], for example. Instead, we consider in this work a novel technique named FBI for scaling factor optimization to establish improved efficiency as compared to the existing literature. In addition, to achieve a secure image transmission and to overcome the problem of false-positive detection, we adopt the Arnold Transform technique, discussed in [13] and [11]. This technique not only improves the security of the watermark but also reduces the visual difference between the watermarked image and the original one. The applied Arnold Transform technique is given by:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} * \begin{pmatrix} x \\ y \end{pmatrix} * mod(M), \tag{3}$$

where $mod(.)$ denotes 'modulo' and (x, y) are the original coordinates of the image pixel; (x', y') are the scrambled coordinates, and M denotes the width of the image. To restore the original watermark, the corresponding inverse transformation formula can be defined as follows:

$$\begin{pmatrix} x \\ y \end{pmatrix} = (\begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} * \begin{pmatrix} x' \\ y' \end{pmatrix} + \begin{pmatrix} M \\ M \end{pmatrix}) * mod(M). \tag{4}$$

Generally, a secret key K (in our case, the number of iterations is adopted) is used before the watermark decryption process during authentication. If the K value is matched, the watermark decrypting procedure is continued, and the embedded watermark is obtained. Otherwise, the process is stopped.

2.2 Forensic-based investigation algorithm

The Forensic-based investigation algorithm (FBI) is an optimization method inspired by the forensic criminal investigation process done by police officers [5]. When a crime is reported, an investigation process is started to gather information, collect evidence, interview witnesses, and identify potential suspects which are equivalent to the suspect locations inside the search space of an optimization problem. This information is sent to the pursuit team to arrest the suspects (optimal solution) or update the investigation data with new suspects.

The original algorithm [5] considers a population of NP investigators and NP police agents, where X_{A_i} is the i^{th} suspected location to be investigated and X_{B_i} is the location of police agent i, who is pursuing the suspect, each possible solution X_{B_i} is a D-dimensional parameter vector. The investigation process stops when it reaches the maximum number of the iteration ($gmax$). The FBI algorithm uses the probability calculated by Equation 5 to compare candidates' solutions:

$$Prob(X_i) = ((f_{worst} - f_i))/((f_{worst} - f_{best})), \tag{5}$$

where f is the objective function to be minimized, f_{worst} and f_{best} are the worst and the best objective function values, respectively. It proceeds in two main steps as depicted in the flowchart in Figure 2:

Step A1: The interpretation of findings [5] The investigation team assesses the information and identifies possible suspect locations. Each location is investigated with the others. First, a new solution $XA1_i$ is deduced based on XA_i and information relevant to the other two random suspected locations k and h as follows:

$$X_{A1_{ij}} = X_{A_{ij}} + \beta(X_{A_{ij}} - (X_{A_{kj}} - X_{A_{hj}})/2), \tag{6}$$

where $\beta = (rand - 0.5) * 2$, $rand$ is a random number in the range $[0, 1]$; k, h, and i are three suspected locations: $k, h, i \in 1, 2, \ldots, NP$, k, and h are chosen randomly; $j = 1, 2, \ldots, D$; NP is the number of suspected locations; D is the number of dimensions. The solution with a better objective function value is retained between X_{A1_i} and X_{A_i}.

Step A2: Direction of inquiry In this step, randomly chosen directions in a certain location are changed to increase the diversity of

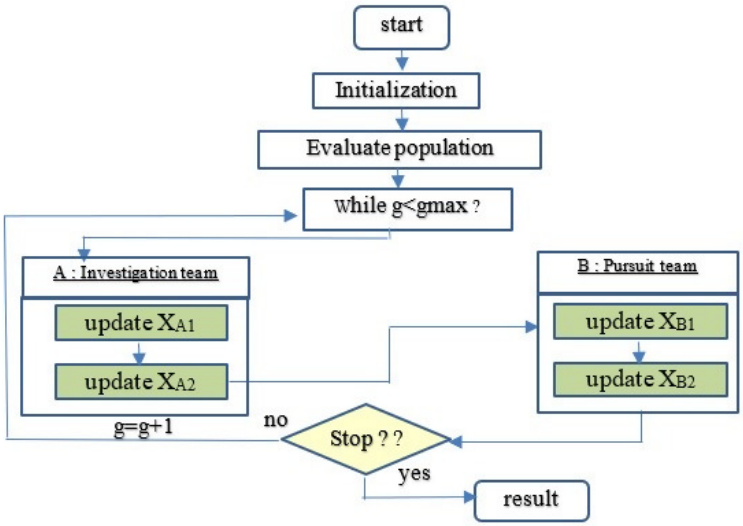


Figure 2. FBI Flowchart

search areas. The move of X_{A_i} is simply affected by the best-suspected location and two other random individuals. The general formula for the move is presented in Equation 7, where a new location X_{A2_i} is obtained.

$$X_{A2_{ij}} = X_{best} + X_{A_{ij}} + rand * (X_{A_{ej}} + X_{A_{fj}}, \tag{7}$$

X_{best} is the best location obtained from Step A1, $rand$ is the random number in the range $[0, 1]$; and d, e, f, and i are four suspected locations: $d, e, f, i \in 1, 2, \ldots, NP$, d, e, and f are chosen randomly; $j = 1, 2 \ldots, D$.

This modification is computed only if $f_{worst} \neq X_{best}$. However, not all directions are changed; the location X_{A_i} is updated only if its probability is lower than a random number. We keep only the best X_{A2_i} locations.

Step B1: Actions step The pursuit team members go together toward the target suspect when they receive the report of the best locations from the first team. Each agent B_i approaches the location that has the best objective value according to Equation 8. This new

location is maintained if it yields a better objective value than that of the old location

$$X_{B1_{ij}} = rand * X_{B_{ij}} + rand * (X_{best} - X_{B_{ij}}), \tag{8}$$

where X_{best} is the best location that the investigation team has provided; $rand$ is a random number in the range $[0, 1]$; $j = 1, 2, ..., D$.

Step B2: Extended Action step Along with their movement, the police agents transfer the objective values of the new locations to headquarters which updates the location and orders the pursuit team to bring near that position. Each agent B_i moves toward the best location, and it is influenced by other team members B_r. X_{B2_i}, the new location of agent B_i is calculated by Equation 9. The newly found location is updated when it attains a better objective value than that of the old location

$$X_{B2_{ij}} = \begin{cases} X_{B_{rj}} + rand * (X_{B_{rj}} - X_{B_{ij}}) + rand * (X_{best} - X_{B_{rj}} \\ \quad \text{if } Prob(X_{B_i}) > Prob(X_{B_r}) \\ X_{B_{ij}} + rand * (X_{B_{ij}} - X_{B_{rj}}) + rand * (X_{best} - X_{B_{ij}}) \\ \quad \text{otherwise} \end{cases}, \tag{9}$$

where X_{best} is the best location provided in Step B1, $rand$ is a random number in the range $[0, 1]$; r and i are two police agents: $r, i \in 1, 2, \ldots, NP$, and r is chosen randomly; $j = 1, 2, \ldots, D$.

Pursuit teams report suspects best locations to investigative teams to help them improve the accuracy of their assessments.

3 Proposed Image watermarking based DWT-SVD optimized by FBI Technique

In this section, we present our proposed approach used to overcome the disadvantages of the arbitrary choice of the scaling factor α of the DWT-SVD watermarking approach proposed in this section. The

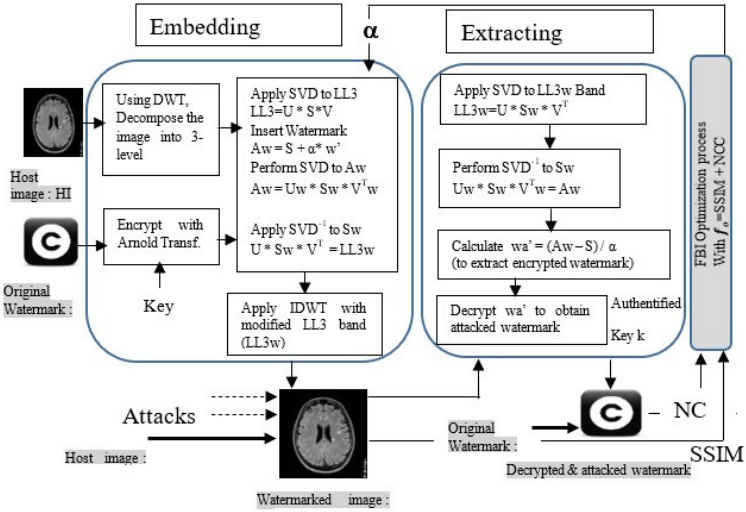


Figure 3. Flowchart of the proposed approach

flowchart in Figure 3 illustrates the main steps in the proposed approach. As shown in Figure 3, the SSIM and NCC values are used in the optimization process to relate the imperceptibility and robustness of a watermarked image; we consider the objective function as the sum of structural similarity index measure (SSIM) and Normalized Correlation Coefficient (NCC) as reported in Equation 10:

$$f_o = \frac{1}{SSIM + NCC}. \tag{10}$$

The SSIM and NCC values are the sum of five types of attacks on the watermarked images as JPEG compression, Median Filter, Mean Filter, Gaussian noise, and Rotation in addition to the results of the image without attacks as given by Equation 11

$$SSIM = \frac{\sum_{i=1}^{6} a_i SSIM_i}{\sum_{i=1}^{6} a_i}; \tag{11a}$$

$$NCC = \frac{\sum_{i=1}^{6} b_i NCC_i}{\sum_{i=1}^{6} b_i}, \tag{11b}$$

where a_i and b_i are weighting coefficients. Note that the goal of the proposed techniques is to maximize the $SSIM$ and NCC values between the original image $I(i,j)$ and a distorted image $I*(i,j)$, they are given by Equations 12 and 13:

$$SSIM(I, I^*) = \frac{(2\mu_I\mu_{I^*} + c_1)(2\sigma_{II^*} + c_2)}{(\mu_I^2 + \mu_{I^*}^2 + c_1)(\sigma_I^2 + \sigma_{I^*}^2 + c_2)}, \tag{12}$$

where μ_I is the average of I, μ_{I^*} is the average of I^*, σ_I is the variance of I, σ_{I^*} is the variance of I^*, σ_{II^*} is the covariance of I and I^*, and c_1, c_2 are two variables to stabilize the division with weak denominator:

$$NCC = \frac{\sum_{i=1}^{N} w_i * \bar{w}_i}{\sqrt{\sum_{i=1}^{N} w_i}\sqrt{\sum_{i=1}^{N} \bar{w}_i}}. \tag{13}$$

We start by coding the decision variables where each value of α represents a suspect location whose values are between 0 and 1. After setting the algorithm parameters and initialization of the initial population, the objective function in Equation 10, referred to as the probability in the FBI technique, is used to evaluate the locations. To achieve the optimal solution, this optimization process is depicted in Figure 4.

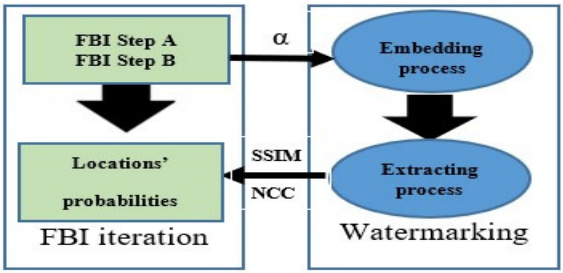
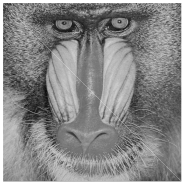


Figure 4. Proposed optimization approach using FBI

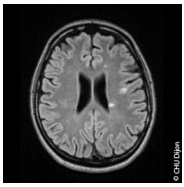


(a) Baboon.

(b) barbara.

(c) Boats.

(d) Lena color.



(e) Brain MRI.

(f) cameraman.

(g) Copyright.

Figure 5. Experimental images used in the simulation.

4 Simulation results

The simulation experiments have been conducted using MATLAB. Six popular images have been used as host images (See Figure 5): Lena color (256x256), Brain MRI (256x256), Barbara (512x512), Baboon (512x512), Cameraman (512x512), and Boats (512x512). The watermark image Copyright of size 256x256 has been used. To study the robustness of the proposed schemes, we have applied many types of attacks on the watermarked images as JPEG compression, Median Filter, Mean Filter, Gaussian noise, and Rotation.

To carry out the optimization process in the proposed approach, the parameters of the FBI are depicted in Table 1.

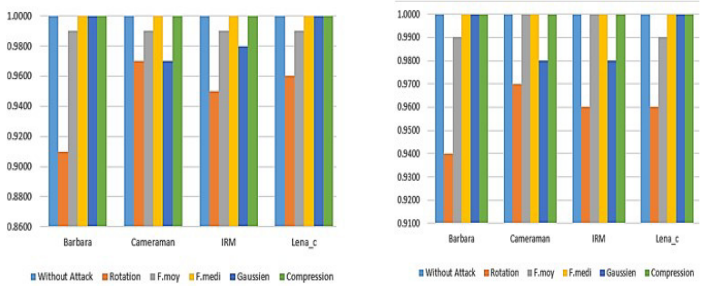
Table 1. FBI parameters

Parameters	Values
Population size (Np)	50 and 100
Generation number gmax	50

4.1 Proposed approach evaluation

For the progression of our simulations, we have adopted two options for each algorithm to illustrate the performances. FBI, as reported in Table 1, has been conducted for a determined choice of 50 and 100 populations and 50 generations. For the objective function weights, we have chosen the same values for the NCC and SSIM weights $a_i = b_i$.

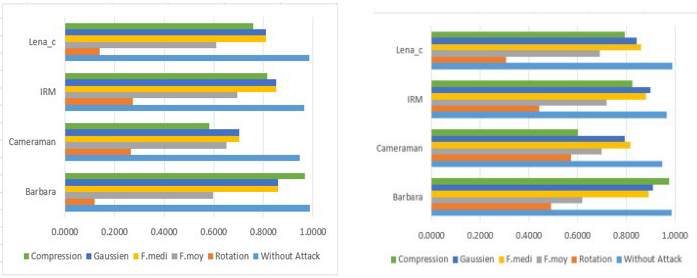
We have also set $a_1 = a_2 = a_3 = 1$ for the first three attacks and $a_4 = 20, a_5 = 100$ for the Gaussian filter and the rotation attacks, respectively. This choice is motivated by the sensitivity of the image to these two attacks and the big changes they make to the image structure. The obtained results with the proposed approach are shown in Figures 6-7. From these figures, the good efficiency of the proposed method can be easily deduced from the obtained values of parameters SSIM and NCC, which correspond to the imperceptibility and robustness, respectively. The obtained NCC parameters close to 1 for most of the considered attacks indicate that the image is extracted without distortion.



(a) Population size=50. (b) Population size=100.

Figure 6. Histogram of SSIM values for the four Images (Lena color, MRI, Cameraman, and Barbara)

The evolution of the objective function (Equation 10) using the FBI approach for the Barbara image is shown in Figure 8 for 50 and 100 iterations, respectively. It is clear that when increasing the iterations number, the optimization goes faster and reaches the global minimum in less time but one has to keep in mind that is very expensive in time to use a higher number, so a compromise has to be found.



(a) Population size=50. (b) Population size=100.

Figure 7. Histogram of NCC values for the four Images (Barbara, Cameraman, MRI, and Lena color

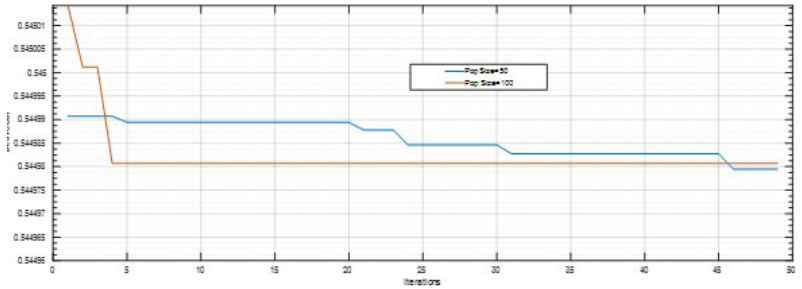


Figure 8. Cost function of Barbara with number of 50 and 100 iterations

Figures 11 and 12 present the performances of the FBI in terms of $SSIM$ and NCC according to the population size for the Barbara image for different attacks. We conducted two experiments with population sizes of 50 and 100 and a fixed iteration number of 100. We can notice that the performance of the proposed approach increases with the increase in the population size. The increase of this parameter offers a better exploration searching for the optimal value of α. These results are validated by Figure 10 where a grayscale SSIM map between the original Barbara image and the watermarked Barbara resulted from our FBI-based approach which provides a spatial understanding of how

(a) Original Barbara. (b) Watermarked Barbara.

Figure 9. Original and watermarked Barbara using our approach

Figure 10. SSIM Map for Barbara image.
In this heatmap, white pixels represent high SSIM values, indicating high similarity between the corresponding pixels in the original and processed images. Black pixels represent low SSIM values, indicating significant differences. Grayscale shades represent intermediate levels of similarity

the SSIM measure varies across different regions of the Barbara image. This allows for a more nuanced analysis compared to a single SSIM value of the two images being compared.

4.2 Comparison with other techniques

In addition to the above results, we compare in the following the proposed method with the last similar optimization-based watermarking techniques DWT-GA [13],IWT-PSO [13], DWT-AIS [16], DWT-SVD, and DWT-CMAES. We take the Lena image as an example to show the comparison results. Tables 2 and 3 list the SSIM and NCC values, respectively.

Table 4 presents the results of the objective function values for six images with the considered algorithms. The best values are shown in

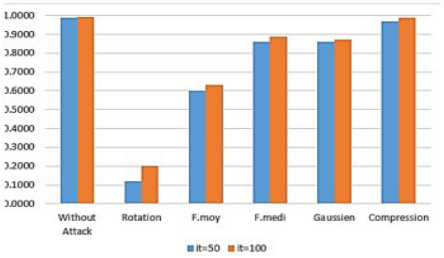


Figure 11. SSIM values for Barbara image with population size: 50 and 100

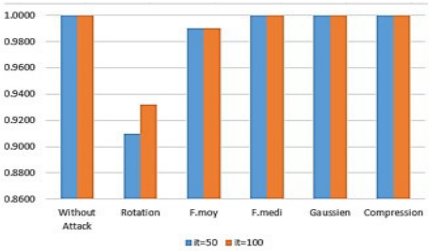


Figure 12. NCC values for Barbara image with population size: 50 and 100

Table 2. SSIM performance comparison for host image Lena

	DWT-GA	IWT-PSO	DWT-AIS	DWT-CMAES	DWT-FBI
Rotation	0.9352	0.9320	0.9299	0.9251	**0.9416**
Gaussian noise	0.9044	0.9052	0.8957	0.8920	**0.9122**
Mean Filter	0.9455	0.9478	0.9362	0.9488	**0.9522**
Compression	0.8029	0.8157	0.8147	0.8001	**0.8255**

bold. From the comparative study of our results with those existing in the literature and referenced in Tables 2, 3, and 4, we can easily state that our proposed scheme is competitive. The NCC metric used shows that the scheme is resistant to several attacks since it is in many cases equal to or very close to 1. Robustness is therefore guaranteed. For the imperceptibility requirement, the SSIM metric is superior to all

Table 3. NCC performance comparison for host image Lena

	DWT-GA	IWT-PSO	DWT-AIS	DWT-CMAES	DWT-FBI
Rotation	0.98	0.97	0.98	0.98	**0.99**
Gaussian noise	0.99	0.99	0.99	0.99	**1.00**
Mean Filter	**0.98**	0.97	**0.98**	0.97	**0.98**
Compression	**0.99**	0.98	0.97	0.98	**0.99**

Table 4. Objective function values comparison for the optimization algorithms

	DWT-GA	IWT-SO	DWT-AIS	DWT-CMAES	DWT-FBI	DWT-SVD
Baboon	**0.5109**	0.5725	0.5522	0.5681	0.5583	0.5831
Barbara	**0.5250**	0.5487	0.6534	0.5475	0.5453	0.6004
cameraman	**0.5293**	0.5698	0.5811	0.5605	0.5578	0.5769
Boats	**0.5486**	0.5910	0.6048	0.5879	0.5764	0.5998
IRM	0.5897	0.6637	**0.5359**	0.6574	0.6414	0.7051
Lena_Color	0.5443	0.5831	**0.5321**	0.5687	0.5631	0.5889
mean	**0.5413**	0.5766	0.5881	0.6090	0.5817	0.5737
Std	**0.0273**	0.0468	0.0397	0.0480	0.0393	0.0346

those used in the referenced works. We can also remark that the FBI approach has given the lower mean and Std values which represents an index about the dispersion of the samples and the exploration power of the FBI algorithm. From the randomized experiments and Table 4, we can see that the FBI algorithm leads to performances that are largely competitive with those existing in the literature.

5 Conclusion

We presented an approach that exploits computational intelligence techniques in the application of image watermarking schemes. The expected goal is achieved by improving the robustness and reinforcing the security of the image content during the transfer process. FBI is applied for the first time in the image watermarking context. In the proposed approach, secure and imperceptible image watermarking is guaranteed. This approach is attractive for transmission data

purposes, which is supported by the obtained simulation results (using several images) showing increased robustness and imperceptibility performance parameters NCC and SSIM.

In the future works, this approach could be applied to watermark the patient's data into the MRI images so to encrypt and protect them.

References

[1] S. Sameerunnisa and J. Jabez, "Efficient memory handling model with consistent video frame duplication removal with precise compression," *Revue d'Intelligence Artificielle*, vol. 37, no. 2, pp. 387–395, 2023. doi:10.18280/ria.370215.

[2] L. Laouamer, "Toward a robust image watermarking method: Exploiting human visual system properties in the spatial domain," *Traitement du Signal*, vol. 40, no. 3, pp. 1119–1126, 2023. doi:10.18280/ts.400327.

[3] Ali Kaveh, Kiarash Biabani Hamedani, and Mohammad Kamalinejad, "An enhanced Forensic-Based Investigation algorithm and its application to optimal design of frequency-constrained dome structures," *Computers & Structures*, vol. 256, Article ID. 106643, 2021. doi:10.1016/j.compstruc.2021.106643.

[4] Assem Mahmoud Abdelhakim, Hassan Ibrahim Saleh, and Amin Mohamed Nassar, "A quality guaranteed robust image watermarking optimization with artificial bee colony," *Expert Systems with Applications*, vol. 72, pp. 317–326, 2017. doi:10.1016/j.eswa.2016.10.056.

[5] Jui-Sheng Chou and Ngoc-Mai Nguyen, "Fbi inspired meta-optimization," *Applied Soft Computing Journal*, vol. 93, Article ID. 106339, 2020. doi:10.1016/j.asoc.2020.106339.

[6] Xinchun Cui, Yuying Niu, Xiangwei Zheng, and Yingshuai Han, "An optimized digital watermarking algorithm in wavelet domain based on differential evolution for color image," *PLoS ONE*, vol. 13, no. 5, 2018. doi:10.1371/journal.pone.0196306.

[7] K. Kuppusamy and K. Thamodara, "Optimized image watermarking scheme based on PSO," *Procedia Engineering*, vol. 38, pp. 493–503, 2012. doi:10.1016/j.proeng.2012.06.061.

[8] Chih-Chin Lai and Cheng-Chih Tsai, "Digital image watermarking using discrete wavelet transform and singular value decomposition," *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 11, pp. 3060–3063, 2010. doi:10.1109/TIM.2010.2066770.

[9] K. Loukhaoukha, "Image watermarking algorithm based on multiobjective ant colony optimization and singular value decomposition in wavelet domain," *Journal of Optimization*, vol. 2013, pp. 1–10, 2013. doi:10.1155/2013/921270.

[10] Raheleh Khorsand Movaghar and Hossein Khaleghi, "A new approach for digital image watermarking to predict optimal blocks using artificial neural networks," *Turkish Journal of Electrical Engineering and Computer Sciences*, vol. 25, no. 1, pp. 644–654, 2017. doi:10.3906/elk-1507-232.

[11] Sarthak Nandi and V. Santhi, "DWT-SVD-based watermarking scheme using optimization technique," *Advances in Intelligent Systems and Computing*, vol. 394, pp. 69–77, 2016. doi:10.1007/978-81-322-2656-7_7.

[12] V. M. Potdar, S. Han, and E. Chang, "A survey of digital image watermarking techniques," in *3rd IEEE International Conference on Industrial Informatics INDIN'05*, pp. 709–716, 2005. doi:10.1109/INDIN.2005.1560462.

[13] R. Surya Prakasa Rao and P. Rajesh Kumar, "Ga-based digital image watermarking for enhanced robustness and imperceptibility," *Journal of Computer Engineering*, vol. 19, no. 3, pp. 26–33, 2017. doi:10.9790/0661-1903012633.

[14] R. Surya Prakasa Rao and P. Rajesh Kumar, (2017b) "PSO- based lossless and robust image watermarking using integer wavelet transform," *Global Journal of Computer Science and Technology: F Graphics & Vision*, vol. 17, no. 1, pp. 29–39.

[15] Chin-Shiuh Shieh, Hsiang-Cheh Huang, Feng-Hsing Wang, and Jeng-Shyang Pan, "Genetic watermarking based on transform domain techniques," *Pattern Recognition*, vol. 37, no. 3, pp. 555–565, 2004. doi:10.1016/j.patcog.2003.07.003.

[16] N. Trache, Z. A. Foitih, and N. Benamrane, "Artificial lmmune system optimization technique for robust and secure lmage water-

marking," *lnternational Journal of lmaging and Robotics*, vol. 19, no. 1, pp. 1–16, 2019.

[17] Ehsan Vahedi, Caro Lucas, Reza Aghaeizadeh Zoroofi, and Mohsen Shiva, "A new approach for image watermarking by using particle swarm optimization," in *ICSPC 2007 Proceedings – 2007 IEEE International Conference on Signal Processing and Communications*, (Dubai UAE), pp. 1383–1386, 2007. doi:10.1109/ICSPC.2007.4728586.

[18] Zhou Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600–612, 2004. doi:10.1109/TIP.2003.819861.

[19] Yun Zheng, C. H. Wu, Zhe-Ming Lu, and W. H. Ip, "Optimal robust image watermarking based on PSO and HVS in integer DCT domain," *International Journal of Computer Sciences and Engineering System*, vol. 9, no. 2, pp. 281–287, 2008.

[20] S. Patsariya and M. Dixit, "Entropy based secure and robust image watermarking using lifting wavelet transform and multi-level-multiple image scrambling technique," *Traitement du Signal*, vol. 39, no. 5, pp. 1751–1759, 2022. doi:10.18280/ts.390533.

Najia Trache, Mohammed Salem,
Mohamed Fayçel Khelfi

Received February 10, 2024
Accepted February 29, 2024

Najia Trache
ORCID: https://orcid.org/0000-0003-0833-3179
Université Oran1
Oran, Algeria
E–mail: n_khelfi@yahoo.fr

Mohammed Salem
ORCID: https://orcid.org/0000-0001-7052-5978
University of Mascara
Mascara, Algeria
E–mail: salem@univ-mascara.dz

Mohamed Fayçel Khelfi
ORCID: https://orcid.org/0000-0001-7060-1547
ESGEE Oran
Oran, Algeria
E–mail: mf_khelfi@yahoo.fr