

Quality assured and optimized image watermarking using artificial bee colony

Irshad Ahmad Ansari¹ · Millie Pant¹

Received: 11 April 2016/Revised: 17 December 2016/Published online: 28 December 2016

© The Society for Reliability Engineering, Quality and Operations Management (SREQOM), India and The Division of Operation and Maintenance, Lulea University of Technology, Sweden 2016

Abstract Watermarking is a process of secret information (watermark) insertion in the digital image, which later on helps in finding out the correct owner of that image. The insertion of watermark's singular values into the host image provide a high value of capacity, robustness and imperceptibility but the scheme remain vulnerable towards false positive attacks. Alternatively, insertion of watermark's principle components into the host image make the scheme secured towards security errors but it also reduces the robustness and imperceptibility of the scheme. The exact recovery of this information becomes even more difficult after attacks because attacks change the information even further. This eventually leads to low imperceptibility and robustness of scheme. In general, the optimization of embedding strengths for image watermarking focuses on the maximization of both imperceptibility and robustness equally. In doing so, often, imperceptibility suffers as it gets degraded beyond a certain limit (<35 dB). This degradation becomes unacceptable in many fields because important information of host image might get lost. In this study, the optimization is performed with a quality assurance so that imperceptibility of scheme does not fall below a user specific threshold. The proposed scheme shows a very decent performance after optimization.

Keywords False positive free watermarking · Quality assured watermarking · Robust watermarking · Discrete wavelet transform · Artificial bee colony

1 Introduction

In the current era, the ease of sharing digital data brings people close to each other. The development of information technology and digital media make the communication remarkably easy between individuals (File and Ryan 2014). Now, one can easily share his/her photograph to the remotely located friend or family with just a simple click. Though, the sharing become easy but the software development also produces new security threats to one's privacy as the manipulation of images also become common and very easy with the help of advance tools (Zhu et al. 2016; Potdar et al. 2005). False ownership claim and unauthorised use of personal images are one of the biggest concerns for any individual or company. Digital image processing provides a powerful solution to this issue within its subdomain known by the name of digital image watermarking (Potdar et al. 2005; Lin et al. 2011).

Image watermarking is performed in order to protect the digital image from being misused. The principal behind image watermarking is very simple and it utilizes the concept of pre-embedding of ownership information (Potdar et al. 2005; Lin et al. 2011). In this approach, some information (known as ownership data) is embedded into the original image (that needs to be protected). When someone claims the ownership of this image or make an unlawful use of this image, the ownership can be verified on the basis of this pre-embedded ownership information. The image watermark can be visible (Kankanhalli and

✉ Irshad Ahmad Ansari
01.irshad@gmail.com

Millie Pant
millifpt@iitr.ac.in

¹ Department of ASE, Indian Institute of Technology Roorkee, Roorkee, India

Ramakrishnan 1999) (like a television logo) or invisible (Yeung and Mintzer 1997) (not visible to naked eye). In practice, invisible watermarking is more famous as it is hard to remove from the image without the knowledge of embedding algorithm itself. The simplest example of watermarking is the change of LSB (least significant bit) of the image. This sort of watermarking is known as fragile watermarking (Ansari et al. 2015) as they did not provide very robust nature towards attack and so they are not very useful for copyright protection. Though, such watermarking can be used for tamper localization and recovery of tampered region (Ansari et al. 2015). As time domain insertion did not provide good protection towards false ownership claim so researchers try to embed the watermark in the transform domain such as DCT (discrete cosine transform), DWT (discrete wavelet transform), IWT (integer wavelet transform), DFT (discrete fourier transform), SVD (singular value decomposition) etc. This sort of insertion result into much better robustness and very decent imperceptibility (Mobasserri 2002; Ansari et al. 2016; Urvoy et al. 2014; Ansari and Pant 2015). Security of watermarking scheme is also an important issue and many watermarking scheme suffer with poor security implementation of watermarking algorithm, which finally make the scheme unusable for its said purpose (Ali and Ahn 2015; Ling et al. 2013).

As discussed above, a good robust watermarking scheme must not have a security flaw and it must be able to provide good robustness towards attack with decent capacity and imperceptibility so this study is dedicated to achieve the said task. The PC (principal components) based insertion is used in this work to make the scheme free from security error and DWT is used to tackle the robustness, imperceptibility and capacity issue within a good limit. The quality assured trade-off is also achieved in this study to obtain the maximum robustness for the given value of imperceptibility.

The organization of rest of the paper is done in following manner: Sect. 2 provides an overview of work related to image watermarking domain. Section 3 provides a discussion on the preliminaries theories and concepts used in this study. Section 4 elaborates the proposed watermarking model and its optimization. Section 5 provides a detailed discussion on the obtained results from the study and Sect. 6 provides a conclusive remark on the study.

2 Related work

Different researchers proposed many watermarking methods in spatial (Ansari et al. 2015) and transformed domain (Mobasserri 2002; Ansari et al. 2016; Urvoy et al. 2014;

Ansari and Pant 2015) in past and transformed domain approach is proven to be better for robust watermarking as compared to the time domain approach because of its invariable nature. SVD based approach remains a preferred choice of developers in the recent past due to its robust behaviors towards attacks. The hybridization of SVD with other transform performed even better. Ganic and Eskicioglu (2005) proposed the hybridization of DWT with the SVD, this lead to better robustness and imperceptibility. Rastegar et al. (2011) introduce the host image pixel shift approach to enhance the security of algorithm. Dugad et al. (1998) suggested the use of LL band of DWT transformed image over the other bands to increase the robustness but this reduced the capacity of scheme. A multi resolution watermarking approach is proposed by the Hsieh et al. (2001). It utilized the significant wavelet tree in order to do so. A blind watermarking approach is proposed by the Shao-Zhang et al. (2004) by the help of DCT and LU decomposition. Jane and Elbaşı (2014) goes further ahead and incorporate SVD along with LU to improve the robustness. The use of binary watermark make the scheme (Jane and Elbaşı 2014) free from security error but it also reduced the capacity of scheme. Lagzian et al. (2011) proposed the SVD and RDWT based approach to improve the capacity of scheme but this again lead to false positive error. A solution of this false positive error is proposed by Guo and Prasetyo (2014) by using the principal components for insertion instead of singular values.

Guo and Prasetyo (2014) suggested the use of principal components based insertion to make the watermarking secure towards false positive error. Doing so; secured the scheme (Guo and Prasetyo 2014) but reduced the capacity, imperceptibility and robustness. The scheme of Guo and Prasetyo (2014) was further improved by incorporating scaling factors optimization by Ansari et al. (2016) but capacity still remains low.

Ali and Ahn (2014) suggested the use of all the bands of DWT for principal components insertion using optimal scaling factors to attain an improved robustness and imperceptibility simultaneously. This scheme (Ali and Ahn 2014) also improved the watermark capacity as compared to Guo and Prasetyo (2014). Though, the scheme of Ali and Ahn (2014) performs quite well but with different host images, the imperceptibility fall below an acceptable level many a times. This reason of the same was the scaling factor optimization without assuring the quality of watermarked image.

The objective of this study is to develop a quality assured, efficient and secured watermarking approach, which provides robust nature to the scheme. The proposed work is an effort to extend the scheme of Ali and Ahn (2014) in an efficient way so that maximum value of robustness can be obtained with an assured image quality

(imperceptibility level). To achieve the said task, this study makes use of ABC for quality assured scaling factors optimization.

3 Preliminaries

3.1 Discrete wavelet transform

DWT based image watermarking has shown more robust nature as compared to other (DCT, DFT etc.) domains because of its excellent time-frequency representation of image (Ma and Wang 2003; Shensa 1992). The feature of exceptional time-frequency localization is a very useful tool for image data hiding/watermarking because it provides good value of both imperceptibility as well as robustness. Many researches make use of this feature of DWT to design image watermarking algorithms in recent past (Potdar et al. 2005; Ganic and Eskicioglu 2005). On the contrary to this advantage, DWT provides poor capacity (low space for data hiding) because of its shift variance feature. Shift variance happens due to the down sampling for each level filtering. Even a small alteration in the sampling, make a perceptible deviations in the wavelet coefficients. This led to inaccurate reconstruction of cover image as well as watermark image. The hybridization of SVD along with the DWT solves this issue to a fair level and so same hybridization is also used in this work.

3.2 False positive solution using principal components

SVD is a decomposition method of linear algebra, which is used to decompose any given symmetric matrix into three separate matrices namely: right singular matrix, left singular matrix and singular matrix (Henry and Hofrichter 1992). These matrices, when multiplied in an ordered manner result into the original matrix/image. The singular matrix contains the singular value of the original matrix in a descending order and they are also used to determine the rank of matrix as all the singular values turns out to be zero after a certain element, if the rank is lesser than the order. Equation 1 is showing the mathematical representation of SVD decomposition. Here, I is the original image/matrix, U is left singular matrix, V is right singular matrix and S is singular matrix.

$$I = USV^T \quad (1)$$

The singular values contained by S shows a very robust nature and get very less affected by the original matrix I . Though, it only contained the information about the participation level of different rows of U and V matrices. The left and right singular matrices contains the detailed

information about the original matrices I . This is the main reason of security error (false positive) in the watermarking scheme, which uses the SVD based insertion. If the attacker changes the singular matrices (as it is supplied by the user only) then the regenerated matrix will be totally different than the original matrix I . A detailed of false positive error can be read from the references (Ali and Ahn 2015; Ling et al. 2013).

A solution of this issue can be insertion of complete watermark in the host image but this reduces the capacity as well as imperceptibility so a more optimal solution is the insertion of the principal components in the host. This will provide a good trade-off between capacity and imperceptibility. Equation 2 shows the principal components calculation.

$$PC = U * S \quad (2)$$

These principal components contain the unique features of any matrix and duplication (false matrix generation) not remains possible. Even if the wrong/false V matrix is used in the extraction process, the false positive issue can be avoided with the help of original PC values. So the same is utilized in this work for ownership checking.

3.3 Artificial bee colony (ABC)

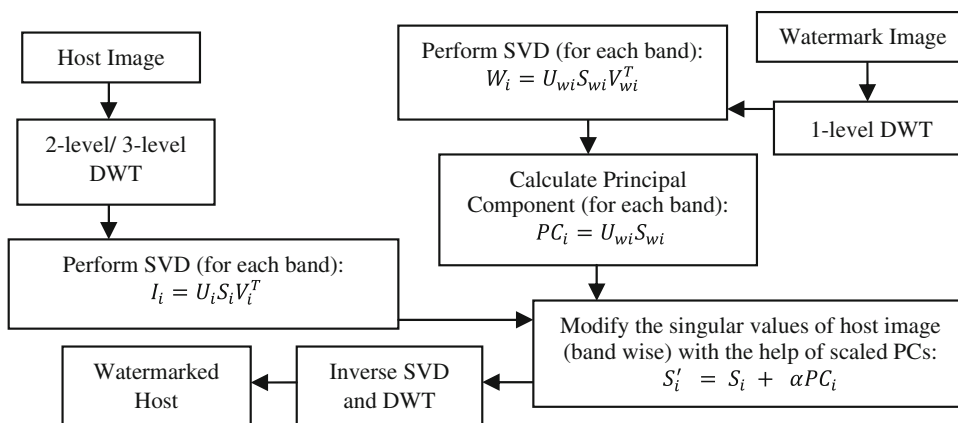
Artificial bee colony is very efficient and fast evolutionary optimization method proposed by the Karaboga (2005). This method is inspired by the bee's behavior and popular for its robust and simple performance (Karaboga and Akay 2009). ABC is used by many researchers in past for the optimal values search in complex and multidimensional space and it provides quite good results (Akay and Karaboga 2015). The additional advantage of ABC over other similar metaheuristics is the use of less control parameters and faster convergence as shown by Ref. Karaboga and Akay (2009). The application of ABC ranges from financial optimization to medical optimization. Some application of ABC in context to imaging optimization is as follows (Akay and Karaboga 2015): image compression, image enhancement, image segmentation etc.

ABC tries to minimize/maximize the given cost function by initializing the random bees food locations throughout the search space. The steps of ABC and its application in the image watermarking optimization can be seen from Ref. Ansari et al. (2016).

4 Quality assured robust watermarking scheme

The insertion of watermark's principle components into the host image make the scheme secured towards both type of security errors (false positive and false negative) but it also reduces the robustness and imperceptibility of the

Fig. 1 Watermark’s principal components embedding into the host image



scheme because the change in the singular values of host using the principal components, changes a large amount of information contained by host. The exact recovery of this information become even more difficult after attacks, as attack changes the information even further. This eventually leads to low imperceptibility and robustness of scheme. In general, the optimization of embedding strengths for image watermarking focuses on the maximization of both imperceptibility and robustness equally. In doing so, often, imperceptibility suffers as it gets degraded beyond a certain limit (<35 dB). This degradation becomes unacceptable in many fields because important information of host image might get lost. In this study, the optimization is performed with a quality assurance so that imperceptibility of scheme does not fall below a user specific threshold.

The quality assured watermarking is designed based on the watermark’s principal components insertion and the ABC optimization of scaling factors. The scheme’s detail is as follows:

4.1 Embedding scheme of watermark

Figure 1 shows the principal component based insertion of watermark data and the required steps are as follows:

1. Apply DWT (1-level) on the watermark image and then, decompose (SVD) the bands using Eq. 3.

$$W_i = U_{wi} S_{wi} V_{wi}^T \tag{3}$$

2. Apply DWT (2-level/3-level) on the host image and then, decompose (SVD) the bands using Eq. 4.

$$I_i = U_i S_i V_i^T \tag{4}$$

3. After the SVD decomposition of watermark image, calculate the principal components of the same with the help of Eq. 5.

$$PC_i = U_{wi} S_{wi} \tag{5}$$

4. Perform the band wise modification of singular values with scaled principal components with the help of Eq. 6. Here α represents the scaling factor.

$$S'_i = S_i + \alpha PC_i \tag{6}$$

5. Perform the inverse SVD with the watermarked singular values and calculate the watermarked sub-bands I_{wi} as shown in Eq. 7.

$$I_{wi} = U_i S'_i V_i^T \tag{7}$$

6. Now, apply the inverse DWT on these watermarked bands to calculate the watermarked image H_w .

4.2 Extraction scheme of watermark

The attackers may try to remove the watermark from the watermarked image by using the various signal processing operations on the watermarked image. Let’s assume that the attacked watermarked image is represented by H_w^* . Figure 2 shows the extraction procedure of the hidden

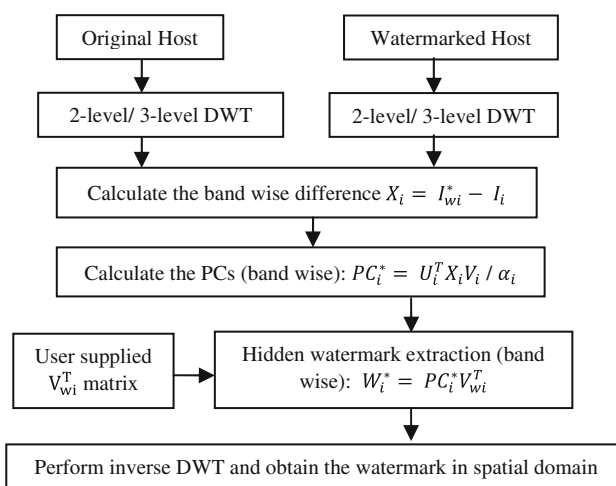


Fig. 2 Watermark extraction from the watermarked image

Fig. 3 Block diagram of optimization process

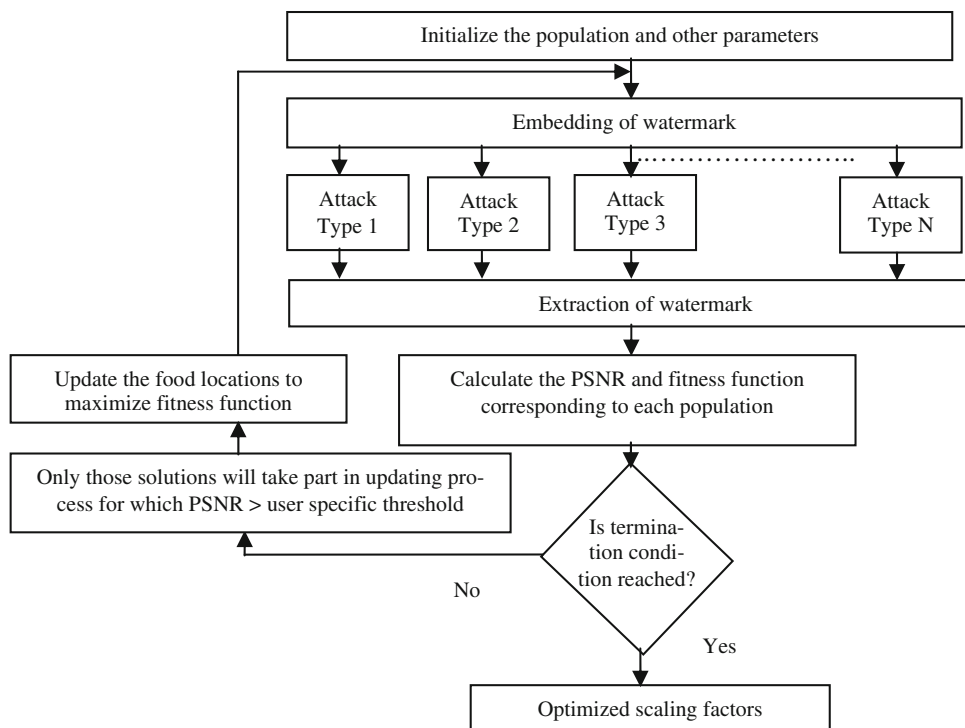
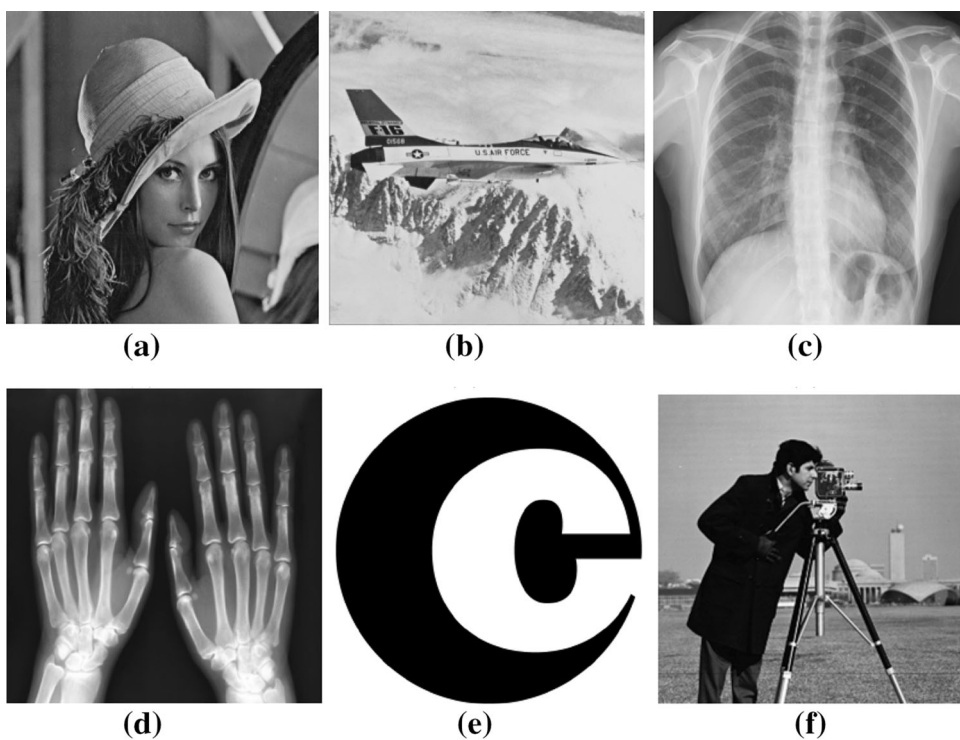


Fig. 4 Host images **a** lena, **b** plane, **c** chest, **d** hand and watermarks, **e** copyright, **f** man



watermark from the attacked watermarked image H_w^* . The corresponding steps of extraction are as follows:

1. Perform 2-level/3-level DWT on the attacked watermarked image and original host image to obtain the equivalent transform domain I_{wi}^* and I_i respectively.

2. Perform band wise subtraction between I_{wi}^* and I_i in accordance with Eq. 8.

$$X_i = I_{wi}^* - I_i \tag{8}$$

3. With the help of Eq. 9, find out the possibly corrupted PC_i^* .

$$PC_i^* = U_i^T X_i V_i / \alpha_i \tag{9}$$

4. Extract the possibly corrupted watermark W_i^* using PC_i^* and user provided right singular matrix V_{wi}^T as shown in Eq. 10.

$$W_i^* = PC_i^* V_{wi}^T \tag{10}$$

5. Perform inverse DWT and obtain the watermark in spatial domain.

4.3 Quality assured optimization of watermarking scheme

The embedding of robust watermark is done by varying the singular values of host image using an appropriate embedding strength. The embedding strength of watermark decides the imperceptibility as well as robustness of scheme. A high value of embedding strength ensures a better robustness but poor imperceptibility; whereas a low

Table 1 Variation in the imperceptibility of watermarked images with different scaling factors (SF) and watermarks (copyright and man)

Host image	PSNR (dB)					
	Copyright			Man		
	SF = 0.01	SF = 0.05	SF = 0.25	SF = 0.01	SF = 0.05	SF = 0.25
Lena	48.5880	35.0630	21.3303	50.9627	37.6336	23.7768
Plane	48.6041	35.0616	21.2662	50.9746	37.6375	23.7005
Chest	48.6323	35.0641	21.3754	50.9125	37.6340	23.7328
Hand	48.7516	35.1264	21.6364	51.1838	37.6628	23.9222

Table 2 Variation of NCC quality of extracted watermark (copyright) and watermarked image with different scaling factors

Host image	Robustness (NCC)					
	SF = 0.01		SF = 0.05		SF = 0.25	
	Watermarked host	Watermark	Watermarked host	Watermark	Watermarked host	Watermark
Lena	0.9998	0.3131	0.9964	0.7998	0.9229	0.9677
Plane	0.9998	0.3048	0.9954	0.7724	0.9083	0.9620
Chest	0.9999	0.4802	0.9968	0.8899	0.9314	0.9650
Hand	0.9999	0.4307	0.9980	0.8623	0.9560	0.9480

Table 3 Variation of NCC quality of extracted watermark (man) and watermarked image with different scaling factors

Host image	Robustness (NCC)					
	SF = 0.01		SF = 0.05		SF = 0.25	
	Watermarked host	Watermark	Watermarked host	Watermark	Watermarked host	Watermark
Lena	0.9999	0.1732	0.9980	0.5537	0.9543	0.8988
Plane	0.9999	0.1716	0.9975	0.5323	0.9441	0.8914
Chest	0.9999	0.2862	0.9982	0.7123	0.9576	0.9320
Hand	0.9999	0.2480	0.9989	0.6569	0.9743	0.8806

Table 4 Imperceptibility and Average robustness of proposed scheme after the scaling factor optimization for threshold > 35 dB

Host image	PSNR of watermarked image		Average NCC of extracted watermark	
	Copyright	Man	Copyright	Man
	Lena	35.3879	35.0567	0.8932
Plane	35.8038	35.0029	0.8491	0.7334
Chest	35.5008	35.2361	0.9159	0.8509
Hand	35.5854	35.3787	0.9041	0.8048

Fig. 5 Watermarked images **a** lena, **b** plane, **c** chest and **d** hand

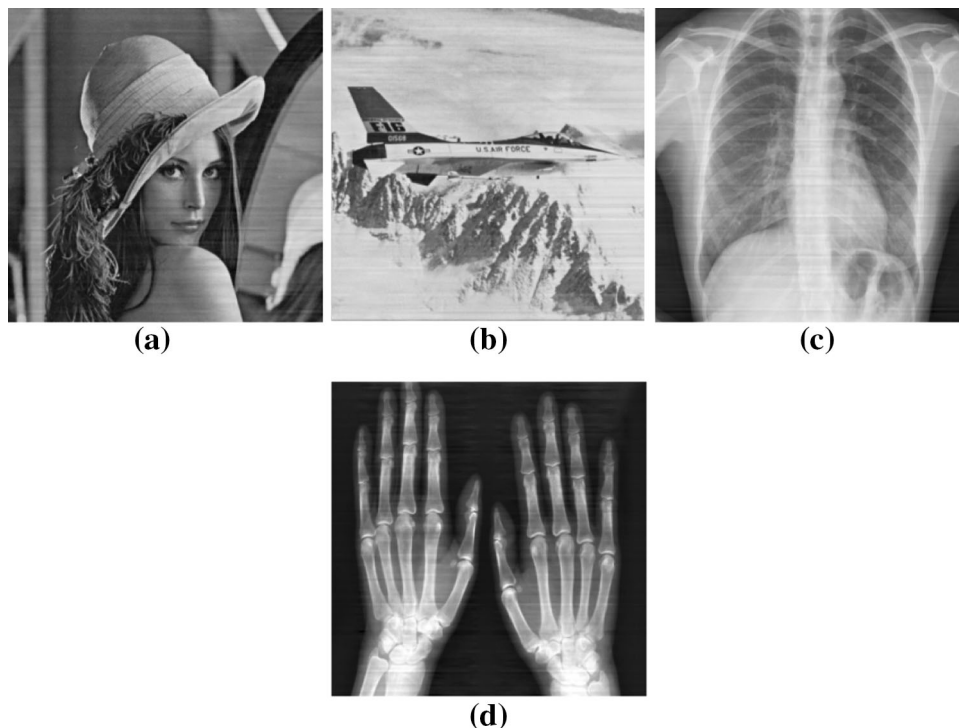


Table 5 NCC of extracted watermarks under different attacks with respect to original watermark (W-1) for threshold > 35 dB

Attack	NCC of extracted watermarks			
	Lena	Plane	Chest	Hand
No attack	0.9994	0.9993	0.9991	0.9957
Average filter (3 × 3)	0.7525	0.6794	0.7707	0.8046
Downscale (512 → 256 → 512)	0.9482	0.9326	0.9807	0.9547
Upscale (512 → 1024 → 512)	0.9961	0.9954	0.9970	0.9923
Gamma correction (0.8)	0.8229	0.7003	0.8365	0.8235
Median filter (3 × 3)	0.8874	0.8624	0.9735	0.9532
Speckle noise (0.001)	0.9724	0.9129	0.9202	0.9570
Gaussian noise (M = 0, V = 0.001)	0.8364	0.8192	0.7678	0.7921
Compression with JPEG (QF = 50)	0.9590	0.9559	0.9505	0.9521
Compression with JPEG 2000 (ratio = 12)	0.9018	0.9154	0.9719	0.9683
Low-pass Gaussian filter (3 × 3)	0.9848	0.9813	0.9947	0.9851
Sharpening (0.8)	0.9148	0.8871	0.9847	0.9395
Contrast adjustment 20%	0.7154	0.3889	0.6920	0.6541
Wiener filter (3 × 3)	0.9320	0.9123	0.9600	0.9510
Motion blur (theta = 4, len = 7)	0.7748	0.7935	0.9393	0.8383

value ensures a better imperceptibility but poor robustness. As these both terms are inversely proportional to each other so an optimal choice of embedding strength is necessary for the scheme to provide satisfactory value of both imperceptibility and robustness. As the value of imperceptibility and robustness both remains low in PC based watermarking, the search of optimal scaling factors often lead to unacceptable reduction in imperceptibility. The proposed optimization scheme is designed in such a way

that the imperceptibility level can be controlled by the user and the optimization also provides maximum robustness corresponding to that imperceptibility. The block diagram of optimization process is shown in Fig. 3. The basic idea of this type of optimization lies with the fact that the PSNR of each population is checked against the user defined threshold and only those populations take part in the solution update process, which have PSNR > user defined threshold.

Table 6 NCC of extracted watermarks under different attacks with respect to original watermark (W-2) for threshold > 35 dB

Attack	NCC of extracted watermarks			
	Lena	Plane	Chest	Hand
No attack	0.9962	0.9963	0.9965	0.9866
Average filter (3 × 3)	0.5849	0.5496	0.6691	0.6874
Downscale (512 → 256 → 512)	0.8239	0.8167	0.9516	0.8962
Upscale (512 → 1024 → 512)	0.9819	0.9814	0.9916	0.9792
Gamma correction (0.8)	0.6501	0.5200	0.7376	0.6066
Median filter (3 × 3)	0.7346	0.7084	0.9303	0.8711
Speckle noise (0.001)	0.8887	0.7507	0.8112	0.8750
Gaussian noise (M = 0, V = 0.001)	0.6337	0.6277	0.6378	0.6360
Compression with JPEG (QF = 50)	0.8386	0.8473	0.8701	0.8628
Compression with JPEG 2000 (ratio = 12)	0.7558	0.7852	0.9191	0.8991
Low-pass Gaussian filter (3 × 3)	0.9366	0.9334	0.9842	0.9546
Sharpening (0.8)	0.7541	0.7348	0.9302	0.8314
Contrast adjustment 20%	0.5615	0.3268	0.5718	0.4080
Wiener filter (3 × 3)	0.8124	0.7985	0.9103	0.8825
Motion blur (theta = 4, len = 7)	0.5981	0.6240	0.8522	0.6960

In this study, the robustness and imperceptibility is defined in terms of correlation between (W, W^*) and (H, H_w) respectively. Where (W, W^*) represents the actual and extracted watermark images and (H, H_w) represents the actual and watermarked host images.

The correlation is used to measure the similarity between two images/matrices of same size and it is defined mathematically as shown in Eq. 11. In Eq. 11, $n \times n$ represents the size of the each image.

$$NCC(W, W^*) = \frac{\sum_{i=1}^n \sum_{j=1}^n \overline{W_{(i,j)} XOR W_{(i,j)}^*}}{n \times n} \tag{11}$$

A higher value of NCC is sought after for better similarity between host and watermarked images as well as embedded and extracted watermarks.

To calculate the optimal value of scaling factor, N types of attacks are considered during optimization process, which lead to the formulation of following objective function (as shown in Eq. 12). The objective function is created in such a way that maximization of this function; eventually, maximize the robustness and imperceptibility both.

$$objective\ function = correlation(H, H_w) + \frac{\sum_{i=1}^N correlation(W, W_i^*)}{N} \tag{12}$$

The objective function (shown by Eq. 12) is a multi-dimensional search and that’s why ABC is used to find out an optimal solution of the same. An initial population of 50 swarms is taken. Then onlookers and employed bees are divided 50% each from the population. A limit of 10

iterations is used to replace the abended food location. The initialization of population is done in the range of 0.001–0.5 (scaling factors).

One more parameter PSNR (peak signal to noise ratio) is calculated to show the similarity of host and watermarked host as the same is needed to ensure the quality assured optimization. The PSNR is defined in the Eq. 13, where, (H, H_w) represents the host and watermarked host respectively and $n \times n$ is the size of both the images.

$$PSNR(H, H_w) = 10 \log_{10} \left(\frac{n \times n \times (H_{max})^2}{\sum_{i=1}^n \sum_{j=1}^n (H(i,j) - H_w(i,j))^2} \right) \tag{13}$$

5 Results and discussions

In the experimental phase, four gray scaled images (general-2, medical-2) are used as shown in Fig. 4. The size of all the hosts images are 512×512 . Two different gray scaled images of size 256×256 are used as the watermark images, which are also shown in the Fig. 4. PSNR and Normalized cross correlation are used to compare the similarity of watermarked images with host images and extracted watermarks with original watermarks respectively.

5.1 Variation of imperceptibility and robustness with different scaling factors

This section provides the variation in the PNSR and NCC values with the change in the scaling factors. The PSNR variation of watermarked image with respect to host image





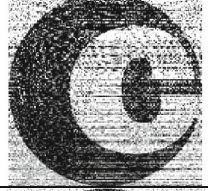























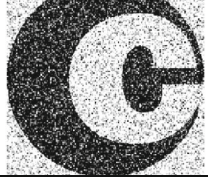



Attack	Extracted Watermarks			
	G-1		M-1	
	W-1	W-2	W-1	W-2
No Attack				
Average Filter (3×3)				
Downscale (512-256-512)				
Upscale (512-4024-512)				
Gamma Correction (0.8)				
Median Filter (3×3)				
Speckle Noise (0.001)				
Gaussian Noise (M=0, V=0.001)				

Fig. 6 Extracted watermarks from Hosts after different attacks

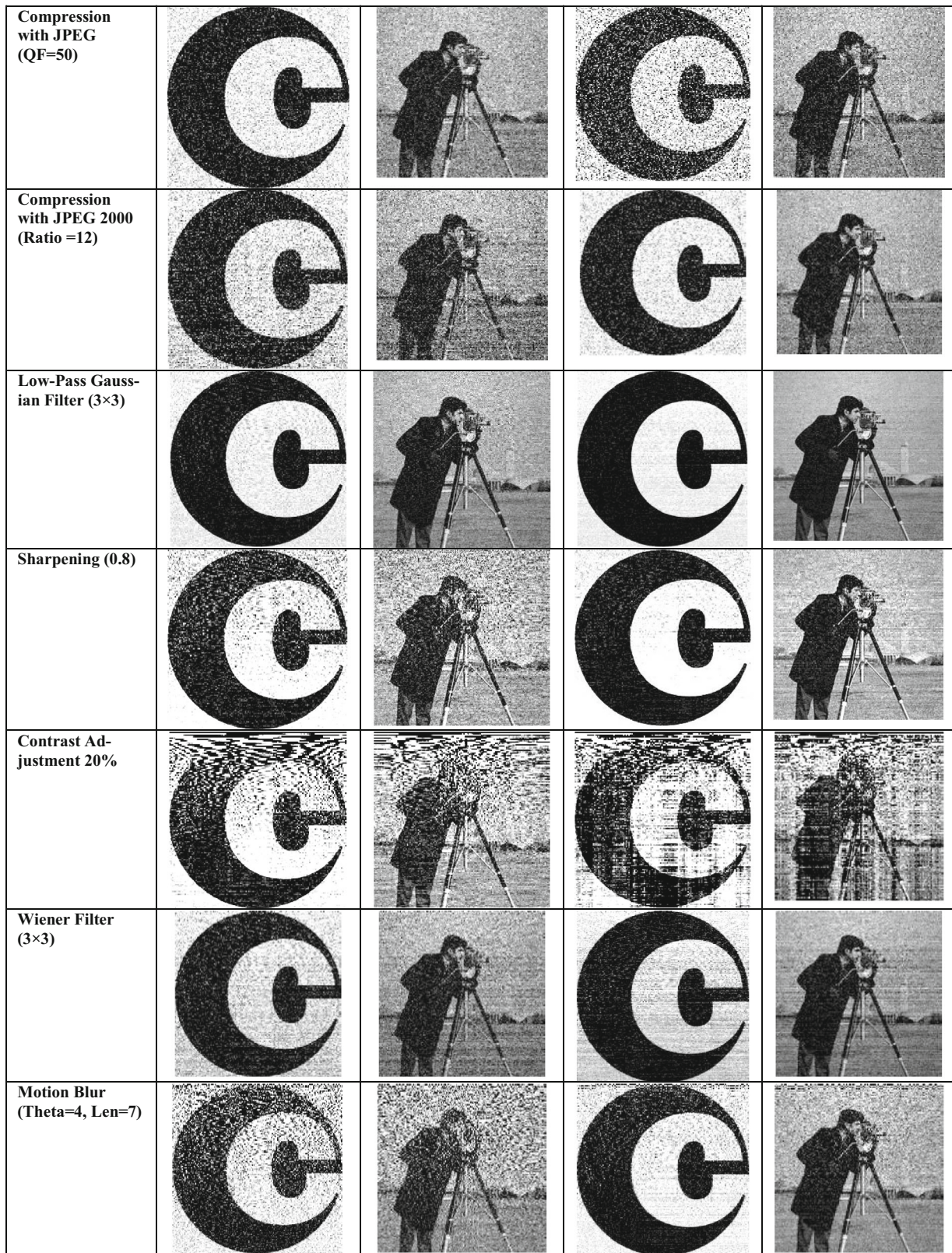


Fig. 6 continued

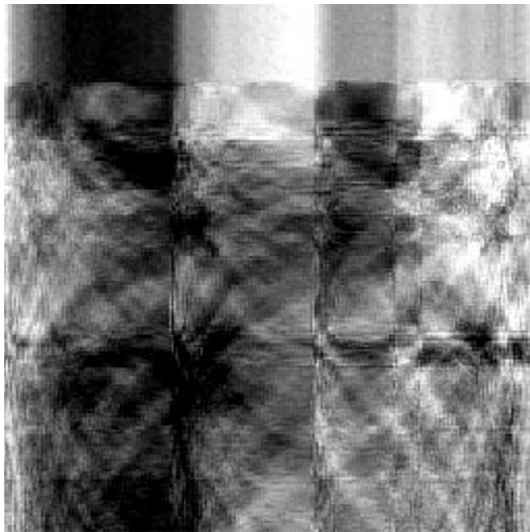


Fig. 7 Extracted watermark from watermarked ‘lena’ when matrix V_w^T is replaced with wrong matrix

is shown in Table 1, which clearly indicates that the low scaling factor provides a better imperceptibility. Tables 2 and 3 shows the variation of the NCC (for both watermarked image and watermark), which also clearly indicates that the high value of scaling factor provides a better robustness.

5.2 Optimization of scaling factors

As both the parameters (imperceptibility and robustness) are inversely proportional (see Tables 1, 2, 3) so optimization of scaling factor is needed. In order to achieve the

Table 7 Average robustness of proposed scheme after the scaling factor optimization for threshold > 36, 37 and 38 dB

Host image	Average NCC of extracted watermark					
	36 dB		37 dB		38 dB	
	Copyright	Man	Copyright	Man	Copyright	Man
Lena	0.8365	0.7269	0.8201	0.6885	0.8107	0.6702
Plane	0.8273	0.7066	0.8046	0.6326	0.7830	0.6267
Chest	0.9081	0.8346	0.8915	0.8035	0.8797	0.7638
Hand	0.8874	0.7796	0.8709	0.7652	0.8428	0.7443

Table 8 Average robustness of proposed scheme after the scaling factor optimization for threshold > 36, 37 and 38 dB

Host image	Average NCC of extracted watermark					
	36 dB		37 dB		38 dB	
	Copyright	Man	Copyright	Man	Copyright	Man
Lena	0.9310	0.8586	0.9107	0.8301	0.9084	0.8121
Plane	0.9057	0.8067	0.8819	0.7964	0.8694	0.7868
Chest	0.9467	0.8910	0.9363	0.8739	0.9265	0.8590
Hand	0.9253	0.8481	0.9209	0.8376	0.8787	0.8200

said task, ABC based quality assured optimization is used in this work; as already explained in Sect. 4.3. Table 4 shows the robustness (without any attack) and imperceptibility of the scheme after the ABC optimization is performed with a quality assurance (imperceptibility threshold > 35 dB). Figure 5 shows the generated watermarked images after this optimization.

Tables 5 and 6 is showing the proposed watermarking scheme’s performance under different attacks for four host images using imperceptibility threshold > 35 dB. The threshold can easily be changed and so any imperceptibility quality can be set with corresponding maximum robustness.

Figure 6 shows the extracted watermark ‘W1’ and ‘W2’ from host ‘G-1’ and ‘M-1’, after different attacks are performed on them.

5.3 False positive error checking

False positive error is known as the wrong extraction of watermark or in other words, extraction of watermark, which is never been inserted into the host image. Figure 7 is showing the extracted watermark, if we change the original V_w^T by a wrong V_w^T . As we can see in the Fig. 7 that the extracted watermark become unrecognizable, if someone changes the original V_w^T by a wrong V_w^T . So this proves that the scheme is secured towards false positive error.

5.4 Robustness variation with user specific threshold

The proposed scheme provides imperceptibility > user threshold. Table 7 shows the average robustness of

proposed scheme after the threshold PSNR is set as: PSNR > 36 dB, PSNR > 37 dB and PSNR > 38 dB.

5.5 Robustness variation with Capacity

It is quite visible from the Table 7 that the robustness of proposed scheme degrades if imperceptibility threshold gets increased. This robustness can further be controlled by the capacity (watermark data size). The reduction in capacity improves the robustness of scheme. The proposed scheme is redesigned with the watermark size of 128×128 using 3-level of DWT transform. Table 8 is showing the average robustness of proposed scheme (watermark size of 128×128) for PSNR > 36 dB, PSNR > 37 dB and PSNR > 38 dB.

From Tables 7 and 8, it can be concluded that reduction in capacity improves the robustness performance.

6 Conclusion

Image watermarking is a very powerful method to figure out the rightful ownership of digital images. Though, the insertion of watermark should be done in such a way that it can provide secured, invisible, robust and good capacity watermarking. The present study tried to do that in an optimal manner with the help of ABC. The proposed work provided an improved robustness while maintaining the imperceptibility of watermarked image above the given threshold level. The proposed scheme was again tested for different capacities of watermark and it performed get further enhanced with reduction in capacity. A number of host images (from different domains) were used during the testing phase of algorithm and scheme performed quite well with all of them. In future, the scheme will be further extended to provide the multipurpose nature (tamper localization/and self-recovery too).

Acknowledgement This work was supported by Ministry of Human Resource Development, India.

References

- Akay B, Karaboga D (2015) A survey on the applications of artificial bee colony in signal, image, and video processing. *Signal Image Video Process* 9(4):967–990
- Ali M, Ahn CW (2014) An optimized watermarking technique based on self-adaptive DE in DWT–SVD transform domain. *Signal Process* 94:545–556
- Ali Musrrat, Ahn Chang Wook (2015) Optimized gray-scale image watermarking using DWT-SVD and Firefly Algorithm. *Expert Syst Appl* 42(5):2392–2394
- Ansari IA, Pant M (2015) SVD watermarking: particle swarm optimization of scaling factors to increase the quality of watermark. In: *Proceedings of fourth international conference on soft computing for problem solving*. Springer, pp 205–214
- Ansari IA, Pant M, Ahn CW (2016) Artificial bee colony optimized robust-reversible image watermarking. *Multimed Tools Appl*. doi:10.1007/s11042-016-3680-z
- Ansari IA, Pant M, Ahn CW (2015) SVD based fragile watermarking scheme for tamper localization and self-recovery. *Int J Mach Learn Cybern*. doi:10.1007/s13042-015-0455-1
- Ansari IA, Pant A, Ahn CW (2016b) Robust and false positive free watermarking in IWT domain using SVD and ABC. *Eng Appl Artif Intell* 49:114–125
- Ansari IA, Pant M, Ahn CW (2016c) ABC optimized secured image watermarking scheme to find out the rightful ownership. *Opt-Int J Light Electron Opt* 127(14):5711–5721
- Dugad R, Ratakonda K, Ahuja N (1998) A new wavelet-based scheme for watermarking images. In: *Proceedings of the international conference on image processing, ICIP 98, vol 2*. IEEE, pp 419–423
- File T, Ryan C (2014) *Computer and internet use in the United States: 2013*. American Community Survey Reports
- Ganic E, Eskicioglu AM (2005) Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition. *J Electron Imaging* 14(4):043004
- Guo JM, Prasetyo H (2014) False-positive-free SVD-based image watermarking. *J Vis Commun Image Represent* 25(5):1149–1163
- Henry ER, Hofrichter J (1992) [8] Singular value decomposition: application to analysis of experimental data. *Methods Enzymol* 210:129–192
- Hsieh MS, Tseng DC, Huang YH (2001) Hiding digital watermarks using multiresolution wavelet transform. *IEEE Trans Ind Electron* 48(5):875–882
- Jane O, Elbaşı E (2014) A new approach of nonblind watermarking methods based on DWT and SVD via LU decomposition. *Turk J Electr Eng Comput Sci* 22(5):1354–1366
- Kankanhalli MS, Ramakrishnan KR (1999) Adaptive visible watermarking of images. In: *IEEE international conference on multimedia computing and systems, vol 1*. IEEE, pp 568–573
- Karaboga D (2005) An idea based on honey bee swarm for numerical optimization. Technical report-tr06, Erciyes University, Engineering faculty, Computer Engineering Department, vol 200
- Karaboga D, Akay B (2009) A comparative study of artificial bee colony algorithm. *Appl Math Comput* 214(1):108–132
- Lagzian S, Soryani M, Fathy M (2011) A new robust watermarking scheme based on RDWT-SVD. *Int J Intell Inf Process* 2(1):22–29
- Lin W, Tao D, Kacprzyk J, Li Z, Izquierdo E, Wang H (eds) (2011) *Multimedia analysis, processing and communications, vol 346*. Springer, Berlin
- Ling HC, Phan RCW, Heng SH (2013) Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition. *AEU-Int J Electron Commun* 67(10):894–897
- Ma J, Wang H (2003) Discrete wavelet transform (DWT). In: *Proceedings of the third international conference on wavelet analysis and its applications*. World Scientific, p 63
- Mobasser BG (2002) Digital watermarking in joint time-frequency domain. In: *Proceedings of the international conference on image processing, vol 3*. IEEE, pp III–481
- Potdar VM, Han S, Chang E (2005) A survey of digital image watermarking techniques. In: *3rd IEEE international conference on industrial informatics INDIN'05*. pp 709–716
- Rastegar S, Namazi F, Yaghmaie K, Aliabadian A (2011) Hybrid watermarking algorithm based on singular value decomposition and radon transform. *AEU-Int J Electron Commun* 65(7):658–663
- Shao-Zhang N, Xin-Xin N, Yi-Xian Y (2004) Digital watermarking algorithm based on LU decomposition. *J Electron Inf Technol* 26(10):1620–1625

- Shensa MJ (1992) The discrete wavelet transform: wedding the a trous and Mallat algorithms. *IEEE Trans Signal Process* 40(10):2464–2482
- Urvoy M, Goudia D, Autrusseau F (2014) Perceptual DFT watermarking with improved detection and robustness to geometrical distortions. *IEEE Trans Inf Forensics Secur* 9(7):1108–1119
- Yeung MM, Mintzer F (1997). An invisible watermarking technique for image verification. In: *Proceedings of the international conference on image processing*, vol 2. IEEE, pp 680–683
- Zhu JY, Krähenbühl P, Shechtman E, Efros AA (2016) Generative visual manipulation on the natural image manifold. In: *European conference on computer vision*. Springer, pp 597–613