



TÜBİTAK

An improved digital image watermarking scheme using the discrete Fourier transform and singular value decomposition

Justin VARGHESE^{1,*}, Saudia SUBASH², Omer BIN HUSSAIN¹,
Krishnan NALLAPERUMAL², Mohammed RAMADAN SAADY³,
Mohamed SAMIULLA KHAN⁴

¹College of Computer Science, King Khalid University, Abha, Kingdom of Saudi Arabia

²Centre for Information Tech. & Eng., Manonmaniam Sundaranar University, India

³College of Science, South Valley University, Qena, Egypt

⁴Department of Computer Science & Engineering, Manonmaniam Sundaranar University, India

Received: 02.09.2014

Accepted/Published Online: 27.04.2015

Final Version: 20.06.2016

Abstract: The paper presents an improved digital image watermarking algorithm by incorporating the discrete Fourier transform (DFT) and singular value decomposition (SVD). The Fourier transformed carrier image is decomposed into four different frequency subbands by the proposed onion peel decomposition (OPD) algorithm and the SVD-based watermarking scheme is applied to attach the transformed watermark in all four carrier subbands. The proposed inverse OPD algorithm together with inverse DFT is utilized to reconstruct the watermarked image from the frequency blocks. The watermark extraction algorithm is simple and it performs the inverse of watermarking process. The experimental analysis on different images shows that the proposed algorithm produces good quality watermarked images. The watermarks extracted from watermarked images inflicted with potential attacks are also of better perception quality than those produced by other prominent algorithms in terms of subjective and objective metrics.

Key words: Watermarking, singular value decomposition, Fourier transform, copyright protection

1. Introduction

Digital watermarking is the process of embedding digital documents, audio, images, text, and video in digital multimedia documents and it became significant with the advancement of information technology to guard against digital flaws like illegal copying, forgery, and copyright violations [1]. The watermarking algorithms are broadly classified in accordance with the domain in which the digital watermarking is performed. The spatial domain-based watermarking algorithms attach watermarks directly to the whole/portion of the carrier image by replacing selected bits of the carrier image with less computational complexity, but are easy targets for external potential attacks [2] since these algorithms fail to mix frequency components of the watermark with carrier images. Moreover, the watermarked images produced by spatial domain techniques are easy candidates for intruders to perform watermark inversion and copying. These drawbacks of spatial domain-based techniques motivated later algorithms to work in the transform domain to attach digital watermarks in the frequency domain by performing the discrete cosine transform (DCT), discrete wavelet transform (DWT), singular value decomposition (SVD), or discrete Fourier transform (DFT). When a watermark is embedded in the frequency domain, its energy is spread throughout the carrier image by strong embedding with less distortion in the

*Correspondence: justin_var@yahoo.com

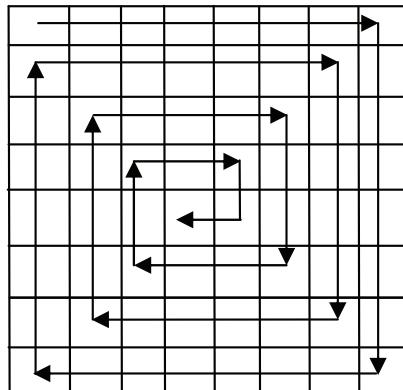
watermarked image and hence these algorithms are robust in preserving watermarks even from grave damage due to potential attacks [2]. The SVD-based algorithms dominate other algorithms due to their simplicity and compactness [2]. Ganic and Eskicioglu proposed an efficient watermarking scheme [3] by embedding the singular values of the watermark with the singular values of all the four subbands of the Haar DWT. Since the algorithm does not perform any transformation on the watermark image before determining the singular values, the extracted watermarks are not robust against most of the potential external attacks. Sverdlov et al. proposed a DCT-SVD-based image watermarking algorithm [4] by addressing the limitations of Ganic and Eskicioglu's algorithm, but it could not meet the requirements of digital watermarking due to the limitations associated with DCT. Run et al. proposed two algorithms [5] by addressing the limitations of the algorithms proposed by Sverdlov et al. and Ganic and Eskicioglu, respectively. Unlike the algorithms proposed by Sverdlov et al. and Ganic and Eskicioglu, Run et al. attached the principal component of the watermark image to the singular values of the transformed carrier image. However, such algorithms are found to be very sensitive to potential attacks. Bhatnagar et al. [6] proposed a logo watermarking scheme in the wavelet domain, which limits its performance to embed only small watermark images. Lai et al. [7] proposed a watermarking scheme by embedding equally divided watermark to carrier HL and LH subbands of the Haar wavelet. The same authors have published a DCT-SVD-based watermarking algorithm [8] by considering human perception characteristics. Makbol et al. [9] proposed a blind image watermarking scheme by incorporating the redundant discrete wavelet transform (RDWT) and SVD. Rawat et al. [10] proposed a two-level watermarking scheme by incorporating DWT packets in its embedding stage. However, the complexity involved in performing two levels of watermarking remained the major drawback of the algorithm. Naskar et al. [11] proposed a dual watermarking scheme by incorporating the DWT, wavelet packet transform (WPT) with best tree, and SVD. The algorithm is computationally complex due to the dual levels of watermark embedding. Wu et al. proposed a watermarking scheme [12] that decomposes the carrier image into overlapping blocks wherein the DCT is then applied. From each DCT block, the direct current (DC) coefficients are extracted and the watermark is embedded in the SVD domain. Das et al. proposed a blind image watermarking scheme [13] by exploiting the interblock correlation of DCT coefficients. Ali and Chang proposed a watermarking scheme based on self-adaptive differential evolution (DE) and DWT-SVD transforms [14]. However, the algorithm is computationally complex due to the numerous iterations performed by the DE genetic algorithm. Numerous other algorithms are also found in the literature [15–22] by introducing different spatial and frequency domain techniques to embed watermark images by satisfying some requirements of image watermarking but they could not meet all vital aspects [23,24] of image watermarking simultaneously, like image quality, robustness, and protection against attacks.

By making an overall assessment of transform-based algorithms in the literature, it can be noted that the DWT-based watermarking algorithms provide better spatial localization with multiresolution analysis that is similar to the human visual system but it does not provide robustness towards geometric potential attacks. The DCT-based algorithms provide better robustness towards JPEG compression but do not provide better resistance towards geometrical distortions. While comparing DCT and DWT, DFT has the advantage of strong energy spreading, translation, and rotation invariance and hence DFT-based algorithms provide better resistance towards geometric and nonlinear transformation-based potential attacks [25]. The singular value component of SVD has strong resistance towards the added perturbation by external potential attacks and is strongly unaffected by transpose, flip, rotation, scaling, and translation-based attacks [26]. The OPD algorithm proposed in this paper helps the watermarking scheme to separate the frequency components into different frequency bands so that multiple copies of watermarks can be attached to different frequency bands. This multiple attachment

of watermark copies to different frequency bands protects the watermark from external potential attacks since the majority of potential attacks will affect only some specific frequency bands. Considering the collective advantages of the DFT, SVD, and OPD, this paper presents an effective watermarking scheme by incorporating the DFT, SVD, and OPD. The paper is organized in five sections. Section 2 illustrates the proposed OPD algorithm. Section 3 details the watermarking and extraction schemes, while section 4 demarcates the improved performance of the proposed algorithm in terms of objective and subjective metrics. Conclusions are finally made in section 5.

2. Forward and inverse onion peel decomposition algorithm

The proposed forward onion peel decomposition is a circular traversal through the pixels; it starts from the upper left corner and ends at the center of the image. A pictorial illustration together with an example for performing traversal using the OPD algorithm is shown in Figure 1. Same as the zigzag ordering of the DCT, OPD is applied to an origin shifted Fourier transformed image; **it decomposes the two-dimensional image into a one-dimensional array where the spectrum of frequencies fall off with decreasing order.** This means the one-dimensional array produced by the algorithm starts from the higher frequency (top left corner of the origin shifted Fourier transformed image) and ends at the lower frequency component of the transformed image (center of the origin shifted Fourier transformed image). The pseudo code of this algorithm is given in Figure 2(a). The proposed watermarking algorithm uses OPD for decomposing the origin shifted Fourier transformed image into four frequency subbands so that the watermarking algorithm can attach multiple copies of watermark to these different subbands.



(a)

13	20	15	2	4	1	12	11
12	13	12	11	4	3	3	2
11	16	14	16	17	14	24	15
19	20	21	15	17	12	11	1
3	7	6	24	23	24	26	24
12	35	31	27	3	7	8	9
21	14	18	15	21	12	11	24
15	36	23	65	45	24	25	29

(b)

[13 20 15 2 4 1 12 11 2 15 1 24 9 24 29 25 24 45
..... 24 7 3 27 31 6 21 15 17 23 24]

Figure 1. Example of traversing using onion peel decomposition: (a) Illustration of traversal, (b) An example of traversal.

The inverse onion peel decomposition (IOPD) performs the inverse operation of the forward traversal wherein it converts the one-dimensional array into a two-dimensional image by placing the elements of the one-dimensional array in a circular fashion. The pseudo code of this algorithm is given in Figure 2(b). The proposed watermarking algorithm uses IOPD for reconstructing the origin shifted Fourier transformed image from the four watermarked subbands.

Procedure for Onion Peel Algorithm	Procedure for Inverse Onion Peel Algorithm
<pre> // Inputs // Input image, O; //m , n : Size of the Input image O ; // Outputs // 1 Dimensional array, I Initialization : i = 1 ; j = 1 ; I = [] ; while (i ≤ m) S = O (i , j : n) ; I = [I , S] ; S = O (i + 1 : m , n)' ; I = [I , S] ; S = O (m , n - 1 : - 1 : j) ; I = [I , S] ; S = O (m - 1 : - 1 : i + 1 , j)' ; I = [I , S] ; m = m - 1 ; n = n - 1 ; i = i + 1 ; j = j + 1 ; end </pre>	<pre> // Inputs // 1 Dimensional array, I //m , n : Size of the output image, O ; // Outputs // Output image, O ; Initialization : i = 1 ; j = 1 ; O = zeros (m , n) ; co = 1 ; while (i ≤ m) O (i , j : n) = I (1 , co : co + (n - j)) ; co = co + (n - j) + 1 ; O (i + 1 : m , n) = I (1 , co : co + (m - i - 1))' ; co = co + (m - i) ; O (m , n - 1 : - 1 : j) = I (1 , co : co + n - j - 1) ; co = co + n - j ; O (m - 1 : - 1 : i + 1 , j) = I (1 , co : co + m - i - 2)' ; co = co + m - i - 1 ; m = m - 1 ; n = n - 1 ; i = i + 1 ; j = j + 1 ; end </pre>
(a)	(b)

Figure 2. Onion peel and inverse onion peel decomposition algorithms.

3. DFT-SVD-based watermarking scheme

The proposed DF T-SVD-based watermarking algorithm incorporates two distinct stages of embedding and extracting watermarks and these stages are explained in the following subsections.

3.1. DFT-SVD-based watermark embedding

The proposed DFT-SVD-based watermark embedding algorithm attaches the watermark image in the DFT and SVD domains. The Fourier transformed carrier image is decomposed into four different frequency blocks by the OPD algorithm to attach the Fourier transformed watermark. Figure 3 is an example of the decomposition operation performed on a Fourier transformed Man image to four subbands using the OPD algorithm. We use the terminologies ultrahigh, very high, high, and low frequency subband to differentiate various subbands. The

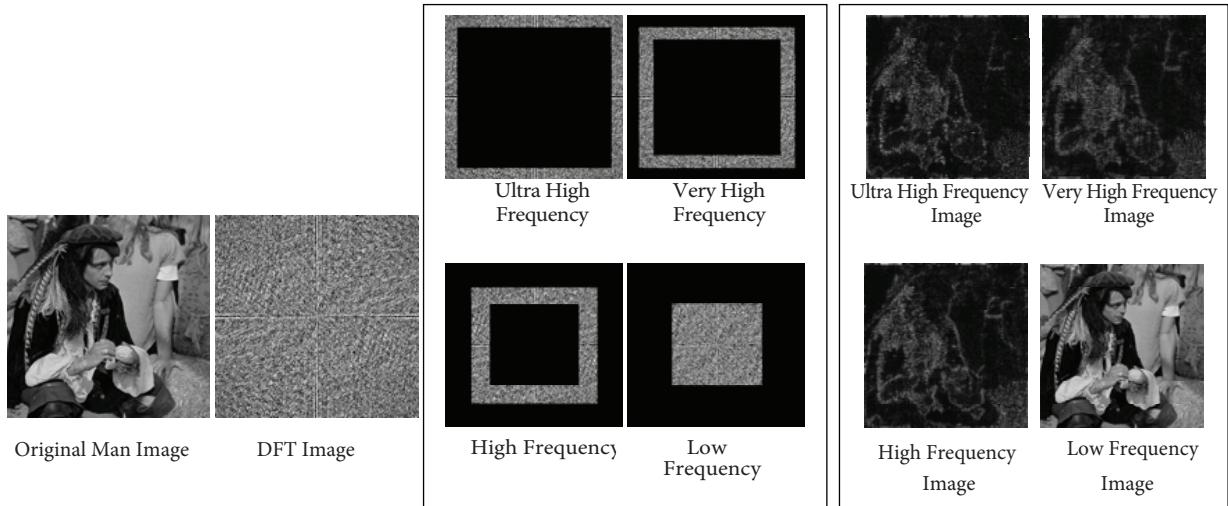


Figure 3. Frequency-based image decomposition example for Fourier transformed images using onion peel decomposition.

proposed algorithm uses SVD for attaching the Fourier transformed watermark in all the four carrier frequency subbands. The algorithm constructs the watermarked image by performing the inverses of SVD, OPD, and DFT. The block diagram of the proposed scheme is outlined in Figure 4. If A and W are the carrier and watermark images, respectively, of sizes $M \times N$ and $\frac{M}{2} \times \frac{N}{2}$, the proposed watermark embedding algorithm is tracked through the following steps:

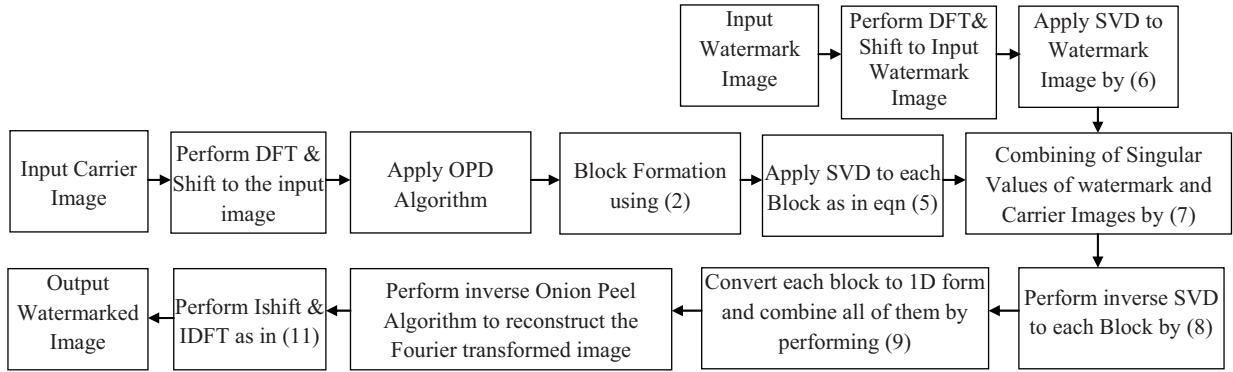


Figure 4. Block diagram of the proposed watermark embedding scheme.

Step 1: The DFT is applied to the carrier image A and the origin of frequency image is shifted to the center to form the frequency domain image \tilde{F} as

$$\tilde{F}(u, v) = \frac{1}{M \times N} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} (-1)^{x+y} A(x, y) e^{-j2\pi(\frac{ux}{M} + \frac{vy}{N})} \quad (1)$$

Step 2: The Fourier transformed image \tilde{F} is decomposed into one-dimensional array \tilde{F}^1 of size $1 \times M \cdot N$ by using the proposed OPD algorithm. This step is performed to reform the two-dimensional \tilde{F} to one-dimensional form without altering the frequency order.

Step 3: The one-dimensional array \tilde{F}^1 is decomposed into four nonoverlapping blocks $Bl^i \quad \forall 0 \leq i \leq 3$ of size $\frac{M}{2} \times \frac{N}{2}$ in such a way that

$$Bl^{c_1} = \left\{ F_{k,l} = \tilde{F}_j^1 : 0 \leq k < \frac{M}{2}, 0 \leq l < \frac{N}{2} \text{ and } j_1 \leq j < (j_1 + n_1) \right\}, \quad (2)$$

where

$$j_1 \in \{(c_1 \cdot n_1) : 0 \leq c_1 < 4\} \quad (3)$$

Here $n_1 = \frac{M \times N}{4}$ and each block Bl^i is the different frequency subband of the image.

Step 4: The DFT is applied to the watermark image W and the origin of the transformed image is shifted to the center for getting the origin shifted image \tilde{W} as

$$\tilde{W}(u, v) = \frac{4}{M \times N} \sum_{x=0}^{\frac{M}{2}-1} \sum_{y=0}^{\frac{N}{2}-1} (-1)^{x+y} W(x, y) e^{-j2\pi(\frac{2ux}{M} + \frac{2vy}{N})} \quad (4)$$

Step 5: SVD is applied to all the four Fourier transformed carrier blocks Bl^i and watermark image \tilde{W} as

$$Bl^i = U_i \sum_i V_i' \quad \forall 0 \leq i \leq 3 \quad (5)$$

$$\tilde{W} = U^w \sum^w V^w' \quad (6)$$

where \sum_i and \sum^w respectively represent the singular values of Fourier transformed carrier block Bl^i and the Fourier transformed watermark image \tilde{W} .

Step 6: The singular value component \sum^w of the watermark image \tilde{W} is attached to each of the singular value components of Fourier transformed carrier blocks \sum_i as

$$\sum_i^* = \sum_i + \left(\alpha_i \times \sum^w \right) \forall 0 \leq i \leq 3 \quad (7)$$

Here α_i is the scaling factor for the i th block that determines the strength of watermarking

Step 7: The watermarked blocks \tilde{Bl}_i are reconstructed using U_i and V_i components of Bl^i as

$$\tilde{Bl}^i = U_i \sum_i^* V_i' \quad \forall 0 \leq i \leq 3 \quad (8)$$

Step 8: Once the singular values of the watermark image are embedded in all frequencies and the watermarked blocks \tilde{Bl}^i are created, they are decomposed into one-dimensional form in \tilde{F}_1^* as

$$\tilde{F}_1^* = \left\{ \begin{array}{l} \tilde{F}_j^1 = \tilde{Bl}_{k,l}^i : 0 \leq k < \frac{M}{2}, 0 \leq l < \frac{N}{2}, \\ j_1 \leq j < (j_1 + n_1) \text{ and } \forall 0 \leq i \leq 3 \end{array} \right\}, \quad (9)$$

where

$$j_1 \in \{(c_1 \cdot n_1) : 0 \leq c_1 < 4\} \quad (10)$$

Step 9: Inverse OPD is performed to reconstruct the Fourier transformed watermarked image \tilde{F}^* from the one-dimensional array \tilde{F}_1^* of size $1 \times M \cdot N$.

Step 10: The inverse DFT is applied to the transformed watermarked image \tilde{F}^* after shifting the origin of frequency from the center to create the watermarked image \tilde{A} as

$$\tilde{A}(x, y) = \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} (-1)^{u+v} \tilde{F}^*(x, y) e^{j2\pi(\frac{ux}{M} + \frac{vy}{N})} \quad (11)$$

The watermarked image produced by the proposed algorithm is of better quality due to the frequency spreading/translation and rotation invariance properties of the Fourier transform even if the scaling factor α for embedding the watermark is very high.

3.2. OPD-SVD-based watermark extraction algorithm

The watermark extraction algorithm performs the inverse of the embedding process and it extracts the attached watermark from the watermarked image. Like the embedding process, the extraction algorithm starts by decomposing the Fourier transformed carrier image into four different frequency blocks by the OPD algorithm and creates the Fourier subbands. SVD is applied to all the four frequency subbands and the singular value components of the subbands are determined. The final watermark copies are reconstructed by performing inverse SVD and DFT operations. The scheme is outlined through the following steps.

Step 1: The DFT is applied to the received watermarked image \tilde{A} and its origin is shifted to the center for determining the frequency domain image \tilde{F}' as in (1).

Step 2: The Fourier transformed image \tilde{F}' is now decomposed into one-dimensional array \tilde{F}'^1 of size $1 \times M \cdot N$ by using the OPD algorithm.

Step 3: The one-dimensional array \tilde{F}'^1 is decomposed into four nonoverlapping blocks \tilde{Bl}_i ($1 \leq i \leq 4$) of size $\frac{M}{2} \times \frac{N}{2}$ in such a way that

$$\tilde{Bl}_{c_1} = \left\{ \tilde{F}_{k,l}' : 0 \leq k < \frac{M}{2}, 0 \leq l < \frac{N}{2} \text{ and } j_1 \leq j < (j_1 + n_1) \right\}, \quad (12)$$

where

$$\bigcup_{l=0}^3 \tilde{Bl}_i = \tilde{F}' \quad (13)$$

and

$$j_1 \in \{(c_1 \cdot n_1) : 0 \leq c_1 \leq 3\} \quad (14)$$

Here $n_1 = \frac{M \times N}{4}$

Step 4: Apply SVD to all the four Fourier transformed watermarked blocks \tilde{Bl}_i as

$$\tilde{Bl}_i = \tilde{U}_i \sum_i^* \tilde{V}_i' \quad (15)$$

Step 5: The copies of singular value component \sum_i^{*w} of the watermark image \tilde{W} are extracted from each singular value component of Fourier transformed carrier blocks \sum_i^* as

$$\sum_i^{*w} = \frac{\left(\sum_i^* - \sum_i \right)}{\alpha_i} \forall 0 \leq i \leq 3 \quad (16)$$

Step 6: The Fourier transformed watermark copies attached to four blocks \tilde{W}_i are reconstructed from $\sum_i^{*w} \forall 0 \leq i \leq 3$ as

$$\tilde{W}_i = U^W \sum_i^{*w} V^W' \quad (17)$$

Step 7: Apply the inverse DFT to the Fourier transformed individual watermark image copies \tilde{W}_i after shifting its origin from the center to get the watermarked image copies \tilde{W}_i^* as

$$\tilde{W}_i^*(x, y) = \sum_{u=0}^{\frac{M}{2}-1} \sum_{v=0}^{\frac{N}{2}-1} (-1)^{x+y} \tilde{W}_i(u, v) e^{j2\pi(\frac{2ux}{M} + \frac{2vy}{N})} \quad (1 \leq i \leq 4) \quad (18)$$

The proposed algorithm is capable of producing better extracted watermark images even in cases where the watermarked image undergoes potential attack because of the collective advantages of the DFT, SVD, and OPD over other transformations.

4. Experimental results and analysis

The effectiveness of the proposed algorithm is compared with the Run et al. 1, Run et al. 2 [5], Sverdlov et al., and Ganic and Eskicioglu algorithms that attach copies of watermark singular values in all frequency components similar to the proposed algorithm. The experimental analysis is performed by analyzing 20 sets of different images with varying characteristics. From among these images, for demonstration in this paper, we use 512×512 sized Man, Bridge, and Baboon images as carrier images, while 256×256 sized Peppers, Lena, and Cameraman are used as watermark images. The concept-wise watermarking comparison of these algorithms is presented in Table 1. We used peak signal to noise ratio (PSNR) and mean absolute error (MAE) for analyzing the objective quality of the watermarked images. The PSNR of the watermarked image \tilde{A} against the true uncorrupted image A is defined by

Table 1. Concept-wise comparative analysis of different algorithms.

Notes	Run et al. 1	Run et al. 2	Sverdlov et al.	Ganic and Eskicioglu	Proposed algorithm
Transforms	DCT-SVD	DWT-SVD	DCT-SVD	DWT-SVD	FT-SVD
Subband embedding	All	All	All	All	All
Watermark transform	DCT-SVD	SVD	DCT-SVD	SVD	FT- SVD
Carrier image size	512×512	512×512	512×512	512×512	512×512
Watermark size	256×256	256×256	256×256	256×256	256×256
Type of watermark	Gray	Gray	Gray	Gray	Gray

$$PSNR = 10 \log_{10} \left(\frac{(255)^2}{MSE} \right) (dB), \quad (19)$$

where the mean square error (MSE) is the average squared error between watermarked image \tilde{A} and the original carrier image A of size $M \times N$,

$$MSE = \frac{1}{M \times N} \sum_{i_1=0}^{M-1} \sum_{i_2=0}^{N-1} (\tilde{A}(i_1, i_2) - A(i_1, i_2))^2 \quad (20)$$

The MAE between watermarked image \tilde{A} and the original image A is given by

$$MAE = \frac{1}{M \times N} \sum_{i_1=0}^{M-1} \sum_{i_2=0}^{N-1} |\tilde{A}(i_1, i_2) - A(i_1, i_2)| \quad (21)$$

The subjective visual quality of the watermarked images produced by various algorithms is assessed by structural similarity index measure (SSIM) [27]. SSIM conducts a visual quality assessment that is similar to the human visual system and is mathematically expressed as

$$SSIM = \frac{(2\mu_A\mu_{A^*} + c_1)(2\sigma_{AA^*} + c_2)}{(\mu_{A^2} + \mu_{A^*}^2 + c_1)(\sigma_{A^2} + \sigma_{A^*}^2 + c_2)}, \quad (22)$$

where μ_A , μ_{A^*} , σ_A , σ_{A^*} , and σ_{AA^*} respectively are the mean of the original carrier image, mean of the original watermarked image, standard deviation (SD) of the original carrier image, SD of the watermarked image, and joint SD of the carrier and watermarked images. Here c_1 and c_2 are the constants to avoid zero denominators. Mean structural similarity index measure (MSSIM) is determined by averaging all the SSIMs. MSSIM value is equal to one when both the images are identical. An ideal watermarking algorithm should produce high PSNR and MSSIM values with low MSE and MAE values. The PSNR, MAE, and MSSIM values produced by different algorithms of its respective watermarked images are experimentally obtained and are shown in Table 2. It is to be noted from Table 2 that the PSNR, MAE, and MSSIM values produced by the proposed algorithm are better when compared to other algorithms. Table 2 also shows the computation time of different algorithms in seconds. For testing the performance of different algorithms we used MATLAB software in an Intel Core 2 Duo system of 2.6 GHz with 4 GB RAM. The scaling factor α is set uniformly for all algorithms to ensure that the watermark content attached by all algorithms is the same. For experimental purposes, we set α to 0.1 for high frequency bands and 0.05 for low frequency bands. The cropped watermarked Man images produced by different algorithms are shown in Figure 5. From Figure 5, it is very clear that the watermarked images produced by the proposed algorithm are of better visual quality when compared to other algorithms. The robustness of the proposed algorithm is tested against various potential attacks that affect the watermarked images from which Gaussian noise, Gaussian filtering, histogram equalization, JPEG compression, rescaling, image unsharpening, gamma correction, salt & pepper impulse noise, pixelate, rotation, and crop operations are used in the analysis. The cropped watermarked Man images affected by Gaussian noise, Gaussian filtering, rescaling, image unsharpening, salt & pepper impulse noise, and pixelate attacks are shown in Figure 6. We use Pearson's correlation coefficient (PCC) as the objective metric for numerically analyzing the robustness of the

Table 2. PSNR and MAE values of watermarked images produced by different algorithms by setting scaling parameter $\alpha = 0.1$ for high frequency bands and $\alpha = 0.05$ for low frequency bands.

Carrier image	Watermark image	Criteria	Run et al. 1	Run et al. 2	Sverdlov et al.	Ganic and Eskicioglu	Proposed algorithm
Baboon	Cameraman	MAE	5.3125	5.1017	7.4527	6.6782	4.9820
		PSNR	28.981	29.182	26.484	29.178	38.941
		MSSIM	0.9901	0.9941	0.9862	0.9952	0.9986
		CT (S)	2.4837	2.5381	2.6839	2.7921	2.5999
Man	Peppers	MAE	5.2947	6.1753	6.2784	6.1273	4.5301
		PSNR	29.172	30.267	27.574	30.265	39.721
		MSSIM	0.9923	0.9950	0.9956	0.9963	0.9992
		CT(S)	2.4842	2.5461	2.7399	2.7869	2.5998
Bridge	Lena	MAE	5.4762	6.9175	7.7182	6.9015	5.2215
		PSNR	29.291	29.286	26.60	29.296	40.124
		MSSIM	0.9931	0.9959	0.9962	0.9964	0.9994
		CT(S)	2.5375	2.5461	2.7246	2.7728	2.6011

extracted watermarks from watermarked images affected by the potential attacks. PCC determines the degree of linear similarity of attached watermark singular values \sum^w against the extracted watermark singular values \sum^{*w} and is mathematically defined by

$$PCC_i = \frac{\sum (\sum^w - \bar{\sum}) (\sum^{*w} - \bar{\sum}^{*w})}{\sqrt{\sum (\sum^w - \bar{\sum})^2} \sqrt{\sum (\sum^{*w} - \bar{\sum}^{*w})^2}} \quad (23)$$

Here $\bar{\sum}^w$ and $\bar{\sum}^{*w}$ respectively represent the mean of \sum^w and \sum^{*w} . The PCC values obtained for the extracted watermark singular values \sum^w produced by different algorithms from watermarked Man, Bridge, and Baboon images affected by potential attack are respectively shown in Table 3, Table 4, and Table 5. For the two algorithms proposed by Run et al., we used principal components instead of \sum^w and \sum^{*w} . For all algorithms, we selected the best PCC values among all PCC_i values produced by various frequency subbands. In order to ensure uniformity in all algorithms, we set the PSNR of the watermarked image to around 31 db by varying the scaling factor α , which produced better results for all algorithms.



Figure 5. Cropped watermarked Man image produced by different algorithms against original crop image.



Figure 6. Cropped watermarked Man images affected by various potential attacks.

Table 3. PCC values obtained for Pepper watermark image extracted from watermarked Man image affected with various potential attacks by different algorithms.

	Run et al. 1	Run et al. 2	Sverdlov et al.	Ganic and Eskicioğlu	Proposed algorithm
PSNR of watermarked image	30.6126	30.5439	30.4892	30.6936	30.7372
Potential attacks					
Gaussian noise 0.001	0.8069	0.7609	0.9983	0.9927	0.9991
Gaussian filtering 5 × 5	0.9317	0.9520	0.9942	0.9762	0.9961
Histogram equalization	0.9161	0.8682	0.9776	0.9913	0.9787
JPEG (50% quality)	0.0924	0.1433	0.5128	0.8118	0.9812
Rescaling 512 -> 256 -> 512	0.6442	0.8502	0.9726	0.9380	0.9253
Rescaling 512 -> 1024 -> 512	0.9657	0.9871	0.9988	0.9976	0.9991
Image unsharpening	0.7587	0.7825	0.8801	0.9025	0.9007
Gamma correction 0.8	0.9867	0.9658	0.9994	0.9997	0.9889
Salt & pepper noise 5%	0.2922	0.2268	0.8585	0.6794	0.8789
Pixelate with 4 × 4 window	0.3443	0.4198	0.9316	0.6948	0.8778
Rotate 20°	0.5849	0.6107	0.9463	0.9771	0.9826
Crop (20 columns on both sides)	0.4986	0.7523	0.9641	0.9788	0.9873

Table 4. PCC values obtained for Lena watermark image extracted from watermarked Bridge image affected by various potential attacks by different algorithms.

	Run et al. 1	Run et al. 2	Sverdlov et al.	Ganic and Eskicioglu	Proposed algorithm
PSNR of watermarked image	30.3251	30.4752	30.3785	30.4871	30.5694
Potential attacks					
Gaussian noise 0.001	0.8537	0.8551	0.9983	0.9958	0.9987
Gaussian filtering 5 × 5	0.9460	0.9412	0.9960	0.9698	0.9946
Histogram equalization	0.6733	0.8041	0.8679	0.9341	0.9575
JPEG (50% quality)	0.1842	0.2185	0.6191	0.8692	0.9941
Rescaling 512 -> 256 -> 512	0.7260	0.8123	0.9844	0.9168	0.9886
Rescaling 512 -> 1024 -> 512	0.9687	0.9804	0.9982	0.9960	0.9989
Image unsharpening	0.4396	0.5831	0.7847	0.7896	0.7970
Gamma correction 0.8	0.9783	0.9867	0.9998	0.9979	0.9914
Salt & pepper noise 5%	0.3821	0.3751	0.8601	0.7277	0.8975
Pixelate with 4 × 4 window	0.4643	0.4216	0.9659	0.6609	0.9562
Rotate 20°	0.6493	0.7386	0.9582	0.9791	0.9894
Crop (20 columns on both sides)	0.5271	0.8027	0.9783	0.9882	0.9961

Table 5. PCC values obtained for Cameraman watermark image extracted from watermarked Baboon image affected by various potential attacks by different algorithms.

	Run et al. 1	Run et al. 2	Sverdlov et al.	Ganic and Eskicioglu	Proposed algorithm
PSNR of watermarked image	30.1542	30.7251	30.6459	30.9122	30.9122
Potential attacks					
Gaussian noise 0.001	0.8572	0.8565	0.9991	0.9974	0.9995
Gaussian filtering 5 × 5	0.9072	0.9112	0.9865	0.9461	0.9863
Histogram equalization	0.4913	0.6242	0.8382	0.8385	0.8820
JPEG (50% quality)	0.1990	0.2880	0.4722	0.8242	0.9780
Rescaling 512 -> 256 -> 512	0.5883	0.7277	0.9388	0.8509	0.9546
Rescaling 512 -> 1024 -> 512	0.9508	0.9654	0.9967	0.9913	0.9982
Image unsharpening	0.3301	0.4549	0.6569	0.7584	0.7898
Gamma correction 0.8	0.9664	0.9846	0.9684	0.9902	0.9970
Salt & pepper noise 5%	0.3959	0.4006	0.9420	0.8031	0.9335
Pixelate with 4 × 4 window	0.3786	0.3965	0.8589	0.5580	0.8680
Rotate 20°	0.4855	0.6849	0.9461	0.9632	0.9864
Crop (20 columns on both sides)	0.4729	0.7843	0.9618	0.9854	0.9928

It is to be noted from Table 3, Table 4, and Table 5 that the PCC values produced by the proposed algorithm are better than those of other competing algorithms for the majority of potential attacks. This is because of the collective advantages of the DFT, SVD, and OPD algorithms. **The proposed algorithm performs exceptionally well for geometric-based rescaling, rotation, and cropping. This is because of the advantage of DFT in resisting geometrical attacks.** For Gaussian noise, Gaussian filtering, salt & pepper, and pixelate type of potential attacks, the proposed algorithm works equally well as the Sverdlov et al. [4] algorithm, while for histogram equalization, image unsharpening, and gamma correction-based potential attacks, the proposed algorithm performs reasonably well in comparison with the Ganic and Eskicioglu [3] algorithm. The majority of these potential attacks affect only specific frequencies of the carrier image. The proposed algorithm achieves

these advantages because of the ability of the DFT to separate different frequencies and it attaches multiple copies of the watermark to different frequencies of the carrier image. Hence the proposed algorithm has the advantage of effective frequency separable capability of the DFT when compared to other algorithms although other algorithms are also similar to the proposed algorithm in attaching multiple copies of the watermark to different frequencies of the carrier image. The visual analysis on the extracted watermark images produced by different algorithms from the watermarked images affected by various potential attacks is shown in Figures 7 and 8. The extracted watermark images produced by the proposed algorithm are found to be better when compared with other algorithms in most of the cases as seen from Figures 7 and 8.



Figure 7. Extracted watermarked images produced by Sverdlov et al., Ganic and Eskicioglu, and the proposed algorithms respectively in the 1st, 2nd, and 3rd column from the watermarked Man image affected by potential attacks Gaussian noise 0.001, Gaussian filter 3×3 , and rescaling 512 -> 1024 -> 512 respectively in each row.

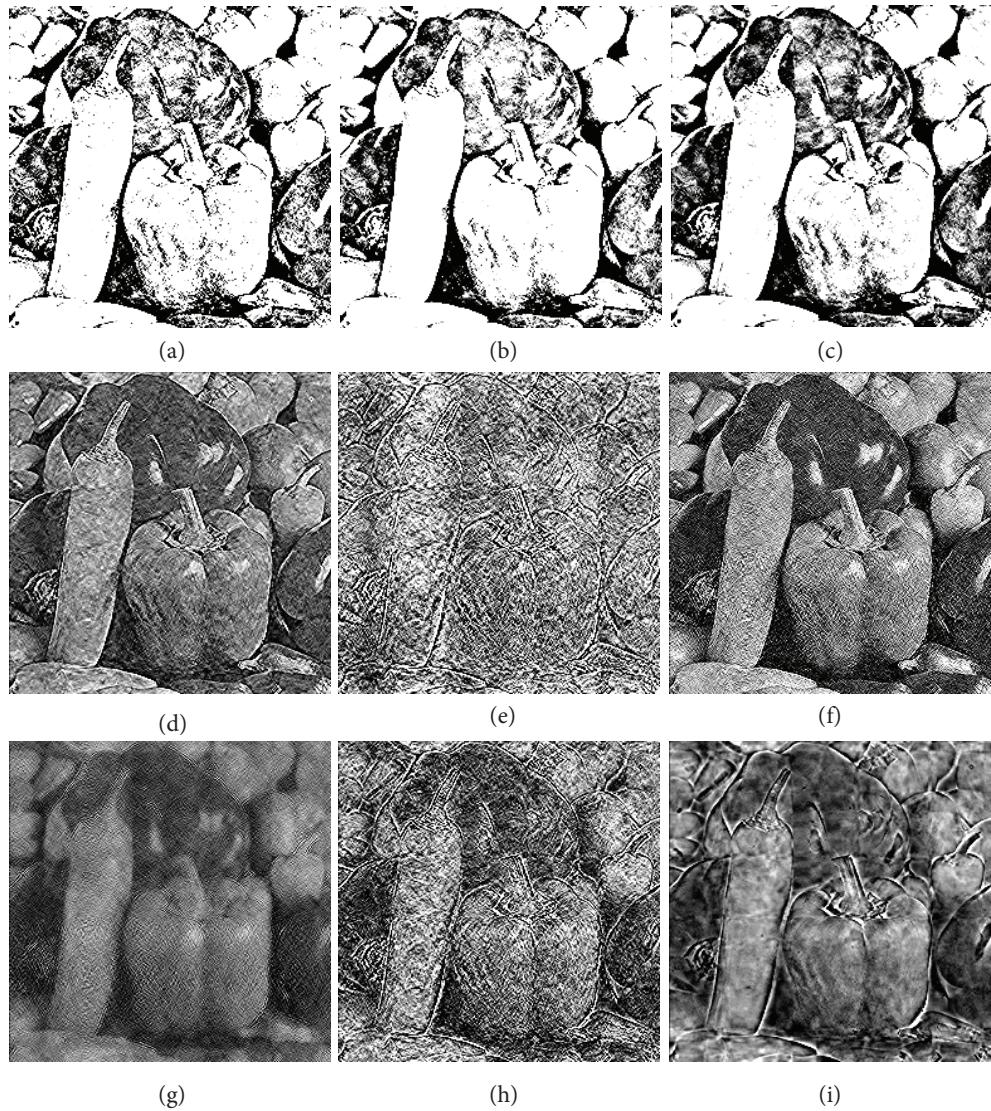


Figure 8. Watermarked images extracted by Sverdlov et al., Ganic and Eskicioglu, and the proposed algorithms respectively in the 1st, 2nd, and 3rd column from the watermarked Man image affected by potential attacks unsharpening, salt & pepper impulse noise 5%, and pixelate 4×4 respectively in each row.

5. Conclusion

The proposed image watermarking algorithm incorporates the DFT and SVD. The algorithm applies the onion peel decomposition algorithm to decompose the Fourier transformed carrier image into four different frequency blocks. The inverse OPD algorithm together with the inverse DFT is utilized to reconstruct the watermarked image from four watermarked frequency blocks. The embedded watermarks are extracted by performing the reverse process of watermarking. The experimental analysis on different images showed that the proposed algorithm is capable of producing high quality watermarked images and the extracted watermarks even from watermarked images affected by potential attacks are of good perception quality compared to other prominent algorithms.

References

- [1] Ingemar JC, Miller ML, Bloom JA, Honsinger C, Kalker K. Digital Watermarking and Steganography. 2nd ed. Burlington, MA, USA: Morgan Kaufmann, 2008.
- [2] Juergen S. Digital Watermarking for Digital Media. Hershey, PA, USA: Information Science Publishing, 2005.
- [3] Ganic E, Eskicioglu AM. Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition. *J Electron Imaging* 2005; 14: 043004-043007.
- [4] Sverdlov A, Dexter S, Eskicioglu AM. Secure DCT-SVD domain image watermarking: embedding data in all frequencies. In: Image Processing Seminar; 23– 26 October 2006; New York, NY, USA. New York, NY, USA: Particle Revelation. pp. 121-124.
- [5] Run RS, Horng SJ, Lai JL, Kao TW, Chen RJ. An improved SVD-based watermarking technique for copyright protection. *Expert Syst Appl* 2012; 39: 673-689.
- [6] Bhatnagar G, Wu JQM, Raman B. Robust gray-scale logo watermarking in wavelet domain. *Comput Electr Eng* 2012; 38: 1164-1176.
- [7] Lai CC, Cheng CT. Digital image watermarking using discrete wavelet transform and singular value decomposition. *IEEE T Instrum Meas* 2010; 59: 3060-3063.
- [8] Lai CC. An improved SVD-based watermarking scheme using human visual characteristics. *Opt Commun* 2011; 284: 938-944.
- [9] Makbol NM, Bee EK. Robust blind image watermarking scheme based on Redundant Discrete Wavelet Transform and Singular Value Decomposition. *AEU-Int J Electron C* 2013; 2: 102-112.
- [10] Rawat S, Balasubramanian R. Best tree wavelet packet transform based copyright protection scheme for digital images. *Opt Commun* 2012; 285: 2563-2574.
- [11] Naskar R, Chakraborty RS. Reversible watermarking utilising weighted median-based prediction. *IET Image Process* 2012; 6: 507-520.
- [12] Wu X, Wei S. Robust copyright protection scheme for digital images using overlapping DCT and SVD. *Appl Soft Comput* 2013; 2: 1170-1182.
- [13] Das C, Swetalina P, Vijay KS, Mahapatra KK. A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation. *AEU-Int J Electron C* 2014; 3: 244-253.
- [14] Ali M, Chang WA. An optimized watermarking technique based on self-adaptive DE in DWT-SVD transform domain. *Signal Process* 2013; 94: 545-556.
- [15] Elbaşı E. Robust multimedia watermarking: hidden Markov model approach for video sequences. *Turk J Electr Eng & Comp Sci* 2010; 18: 159-170.
- [16] Laouamer L, Tayan O. A semi-blind robust DCT watermarking approach for sensitive text images. *Arab J Sci Eng* 2015; 40: 1-13.
- [17] Walia E, Anu S. A robust watermark authentication technique based on Weber's descriptor. *Signal Image Video P* 2014; 8: 859-872.
- [18] Lee MS. Image compression and watermarking by wavelet localization. *Int J Comput Math* 2013; 80: 401-412.
- [19] Vargas L, Vera E. An implementation of reversible watermarking for still images. *IEEE Lat Am T* 2013; 11: 54-59.
- [20] Wang C, Ni J, Huang J. An informed watermarking scheme using hidden Markov model in the wavelet domain. *IEEE T Inf Foren Sec* 2012; 7: 853-867.
- [21] Wu Y. On the security of an SVD-based ownership watermarking. *IEEE T Multimedia* 2005; 7: 624-627.
- [22] Leung HY, Lee MC, Fang L. Robust digital image watermarking scheme using wave atoms with multiple description coding. *EURASIP J Adv Sig Pr* 2012; 2012: 1-14.

- [23] Craver S, Memon N, Yeo BL, Yeung MM. Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks, and implications. *IEEE J Sel Area Comm* 1998; 16: 573-586.
- [24] Ting GCW, Bok MG, Swee HH. Attacks on a robust watermarking scheme based on self-reference image. *Comput Stand Inter* 2008; 30: 32-35.
- [25] Poljicak A, Lidija M, Darko A. Discrete Fourier transform-based watermarking method with an optimal implementation radius. *J Electron Imaging* 2001; 20: 33008-33016.
- [26] Haouzia A, Noumeir R. Methods for image authentication: a survey. *Multimed Tools Appl* 2008; 39: 1-46.
- [27] Wang Z, Bovik AC, Sheikh HR, Simoncelli EP. Image quality assessment: from error visibility to structural similarity. *IEEE T Image Process* 2004; 13: 600-612.