Optics and Lasers in Engineering 107 (2018) 325–334

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

journal homepage: www.elsevier.com/locate/optlaseng

Ownership protection of plenoptic images by robust and reversible watermarking

A. Ansari [a,*], S. Hong [a], G. Saavedra [a], B. Javidi [b], M. Martinez-Corral [a]

[a] Department of Optics, University of Valencia, E-46100 Burjassot, Spain
[b] Department of Electrical and Computer Engineering, University of Connecticut, Storrs, CT 06269, USA

ARTICLE INFO

Keywords:
Plenoptic images
Logo extraction
Robust watermarking
Reversible watermarking
DCT
SVD
Gaussian noise
JPEG Compression
Median filtering

ABSTRACT

Plenoptic images are highly demanded for 3D representation of broad scenes. Contrary to the images captured by conventional cameras, plenoptic images carry a considerable amount of angular information, which is very appealing for 3D reconstruction and display of the scene. Plenoptic images are gaining increasing importance in areas like medical imaging, manufacturing control, metrology, or even entertainment business. Thus, the adaptation and refinement of watermarking techniques to plenoptic images is a matter of raising interest. In this paper a new method for plenoptic image watermarking is proposed. A secret key is used to specify the location of logo insertion. Employing discrete cosine transform (DCT) and singular value decomposition (SVD), a robust feature is extracted to carry the watermark. The Peak Signal to Noise Ratio (PSNR) of the watermarked image is always higher than 54.75 dB which is by far more than enough for Human Visual System (HVS) to discriminate the watermarked image. The proposed method is fully reversible and, if no attack occurs, the embedded logo can be extracted perfectly even with the lowest figures of watermark strength. Even if enormous attacks occur, such as Gaussian noise, JPEG compression and median filtering, our method exhibits significant robustness, demonstrated by promising bit error rate (BER) performance.

1. Introduction

Swift development of information technology has facilitated sharing digital images. Consequently, it seems necessary to have some tool to preserve the authors undergoing illegal duplication of digital content [1]. Digital watermarking is to embed the logo, the desired information, into the host image in a way that the watermarked image seems identical to the host one [2]. The basic premise of image watermarking lies on the hypothesis that HVS is unable to identify small modification of the pixels of the host image. In this way, the logo can be embedded into the host image such that it will be very difficult for the HVS to discriminate between the host image and the watermarked one [3]. Importantly, the embedded logo should be as robust as possible against various attacks applied to the watermarked image. In other words, despite how sever is the attack, it should be possible to extract the embedded logo perfectly with minimum or (if feasible) zero error. Other important characteristic is imperceptibility, which implies that the watermarked image should seem identical to the host one such that it is impossible to discriminate between them. Finally, the higher the capacity, the higher amount of information can be embedded via watermarking algorithm. There is always a compromise between the robustness, imperceptibility and capacity [4]. Hence, incorporating all the three aforementioned characteristics in the same watermarking method remains a daunting challenge.

A comprehensive review of watermarking literature can be found in [5] in which the watermarking techniques have been categorized from many aspects. Regarding the domain which the watermarking techniques have been implemented in, they can be divided into the methods of the spatial domain [6], the transform domain [3], and hybrid methods using both domains for digital watermarking [7,8]. A wide range of transformations and factorizations may be employed to embed the logo such as DCT [9–11], wavelet [12–14], Contourlet [3], PCA [15], SVD [16], or other transforms [17]. The spatial-domain methods usually alter the pixels of the host image in spatial domain to embed the logo, while the transform-domain methods embed the watermark information in the transform coefficients [18]. Conversely the hybrid methods may use both, pixels in spatial domain and transform coefficients, to embed the logo [8]. The logo may be embedded by additive methods [5,14,19–21] or multiplicative methods [3,22]. Based on the embedding mechanism, the watermark may be fragile or robust. The fragile watermarking is very sensitive, even to the smallest tampering of the image, while the robust image watermarking is quite resistant against different attacks. The robust watermarking methods are usually used in

* Corresponding author.
E-mail addresses: Amir.Ansari@uv.es (A. Ansari), Seokmin.Hong@uv.es (S. Hong), Genaro.Saavedra@uv.es (G. Saavedra), bahram.javidi@uconn.edu (B. Javidi), Manuel.Martinez@uv.es (M. Martinez-Corral).

https://doi.org/10.1016/j.optlaseng.2018.03.028
Received 12 December 2017; Received in revised form 1 March 2018; Accepted 22 March 2018

ownership protection whereas the fragile watermarking is often used in authentication of the image content [11,23,24]. In the recent years, another category is added to this branch, which is known as semifragile in the literature. The semifragile watermark may resist against some benign attacks but easily gets collapsed if exposed to some malignant ones, e.g. robust against Gaussian noise and JPEG compression but fragile to tampering [25]. If the original image or the original watermark are not required in the extraction process, the watermarking scheme is referred to as blind and otherwise it will be non-blind [26,27].

Another categorization of watermarking techniques is based on the possibility of recovering the host image after watermark extraction and in this way, the watermarking techniques can be split into reversible and irreversible ones. The former delivers a replica of the host image after watermark extraction while the latter lacks such possibility [28,29].

Conventional cameras fail to capture a proper description of 3D scenes in the real world. In fact, conventional cameras record the summation of all the rays passing through a point and therefore, lose an enormous amount of the angular information [31]. In contrast, plenoptic cameras get samples from different rays passing through each point in the space. To do that, a microlens array is placed at the image plane of a conventional camera, and the CCD is displaced up to the focal plane of the microlenses [30,32]. In this way, any microlens provides a microimage, which has the information of all the rays passing through the center of the microlens but with different inclination. From the microimages it is possible to compute a collection of perspective images (also known as elemental images) and also to calculate the integral image, that is, the image that is displayed in the plenoptic monitor [33].

While a countless number of digital watermarking methods have been proposed for conventional 2D images, to the best of our knowledge these methods rarely concern plenoptic images and there are only a few works in digital watermarking of multi-perspective images [34–38], 3D object watermarking [39] and some general optical techniques for security [40,41]. For this reason, in this paper we propose a new algorithm for plenoptic-image watermarking and keep a trade-off between watermark characteristics outlined earlier. The remainder of this paper is organized as follows: The proposed method is elaborated in Section 2, while the experimental results are discussed in Section 3. Finally, the conclusions are drawn in the last section.

2. The proposed method

2.1. The embedding procedure

The proposed method for digital watermarking has two inputs: the host image and the secret key. Suppose the dimensions of the embedded binary logo are $N_b \times N_b$. The assumption of equal length and width of the logo is merely for the notation convenience, but the proposed method can be used for any arbitrary dimension. The secret key is utilized to determine which pixel from which microimage (μI) should be selected. As the first step of hijacking the embedded logo would be locating the selected pixels, it is very important to keep the pixel location secret. In Fig. 1a possible permutation of pixels of μIs is shown. Each μI is drawn in a different color and the selected pixel of each μI is checked. As shown in Fig. 2, the chosen pixel from each μI is arranged as a component of the selected image block: $img\_blk\_sel_{ij}$, which corresponds to the arranged block for embedding the w_{ij}, the watermark bit in the ith row and jth column. Without any loss of the generality, in this paper we select pixel (i, j) from the $\mu I(i, j)$ to arrange the first block for embedding the watermark bit (1, 1). A similar trend is followed to arrange all the other blocks. The arrangement shown in Figs. 1 and 2 is just an example and one may use any arbitrary pixel from any μI. Although it is possible to use the pixels of the same μI to arrange $img\_blk\_sel_{ij}$, it is highly preferred to insert the logo bit in the pixels of different μIs. This strategy has three main advantages. The first one is to reinforce the robustness of the proposed method; this is due to the high correlation of the adjacent pixels of the same μI. If e.g. a single μI is exposed to Gaussian noise, then the embedded bit in this block may be lost.

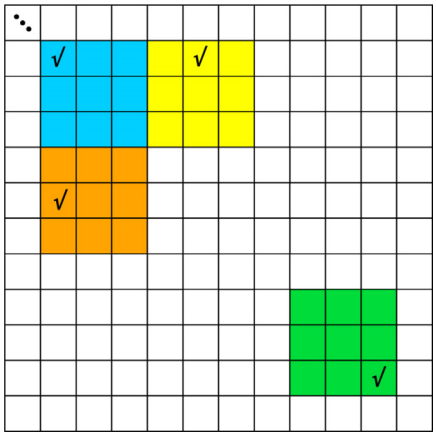

Fig. 1. A possible pixel selection from the different μIs. In this scheme, for simplicity, mI are comprised of 3×3 pixels. Of course in a real case there is no limitation in their dimension.

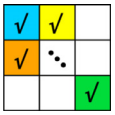

Fig. 2. Arrangement of the selected pixels as a matrix.

Conversely, if the $img\_blk\_sel_{ij}$ is comprised of different μIs and one of them is prone to an attack, the information from all other μIs can be utilized to extract the embedded bit and it will be very likely to extract the logo bit correctly. The second advantage lies on the fact that each μI carries the angular information of a point in the 3D scene in real world. If all the pixels of the same μI are exploited to embed the watermark bit, then the angular (and also the spatial) information of a point is adversely affected. Finally, the third benefit is that even if the third party finds out the mathematical mechanism of the proposed method and makes a wild guess about the embedding location, he/she will not be able to extract the watermark accidentally. Note that hijacking a single bit of the embedded watermark, the third party should make $n_{El,\,h} \times n_{El,\,v}$ wild guesses correctly, where $n_{El,\,h}$ and $n_{El,\,v}$ are the number of the rows and the columns of the μI. Regarding the practical values of $n_{El,\,h}$, $n_{El,\,v}$, the third party would have empirical problems to pinpoint the location of chosen μIs for watermark insertion. It is emphasized again that the proposed method is not biased to any specific permutation of the μIs nor any order of selecting the pixels of the μIs.

It is well-known that the HVS has the least sensitivity to the blue channel of an RGB image and hence the proposed method is applied to this channel [42]. Before preceding the remainder of this paper, we would like to point out briefly that the energy is distributed according to a zigzag order among DCT coefficients [11]. As an example, the energy distribution of an 8×8 matrix is shown in Fig. 3. The coefficient in the top left corner has the lowest frequency (the DC component) and the highest energy while the coefficient in the right bottom has the highest frequency and the lowest level of energy.

In Fig. 4 the block diagram of the embedding procedure is shown. The $img\_blk\_sel_{ij}$ is transformed to the DCT domain. Suppose $A_{M\times N}$ is a matrix and its DCT coefficients are defined as

$$B_{uv} = \sum_{i=0}^{M-1}\sum_{j=0}^{N-1} \alpha_u \alpha_v \cos\left[\frac{\pi u}{2M}(2i+1)\right] \cos\left[\frac{\pi v}{2N}(2j+1)\right] A_{ij} \qquad (1)$$

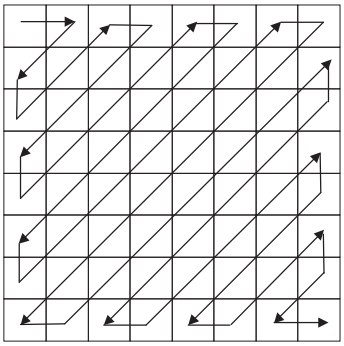

Fig. 3. The zigzag order of the energy distribution between the DCT coefficients.

where $0 \le u \le M-1$, $0 \le v \le N-1$, and

$$\alpha_u = \begin{cases} 1/\sqrt{2} & u = 0 \\ 1 & u \neq 0 \end{cases} \quad 0 \le u \le M-1$$
$$\alpha_v = \begin{cases} 1/\sqrt{2} & v = 0 \\ 1 & v \neq 0 \end{cases} \quad 0 \le v \le N-1 \tag{2}$$

The SVD factorization of an arbitrary matrix $M_{m\times n}$ is defined as

$$M = U\Sigma V' \tag{3}$$

where Σ is a diagonal matrix, often known as the matrix of the singular values. The components of Σ are arranged in descending order, i.e. Σ(1, 1) is the largest component while others decrease monotonously. The columns of U are the left singular vectors and V' has rows that are the right singular vectors.

As mentioned earlier, the energy level of the DCT coefficients is arranged in zigzag order, i.e. the components at the location of the (1,1) has the highest energy level, then (1,2), (2,1), and so on (trace the arrow in Fig. 3). The first *n_dct* components of the DCT transform are selected and the other components are discarded and in this way $img\_blk\_sel\_dct_{ij}$ is obtained by DCT (Eq. (1)). Afterwards, an SVD factorization is applied into $img\_blk\_sel\_dct_{ij}$. The component (1,1) of Σ is used for embedding the watermark bit:

$$\sigma_w = \begin{cases} \sigma_1 + gf & \text{if } w_{ij} = 1 \\ \sigma_1 - gf & \text{if } w_{ij} = 0 \end{cases} \tag{4}$$

Here σ_1 stands for the component (1,1) of the matrix of the singular values, *gf* is the watermark strength, and w_{ij} is the desired watermark bit to embed. Besides, σ_w is the new singular value of the watermarked block. The DCT coefficients of the watermarked block is yielded by

$$wm\_img\_blk\_sel\_dct_{ij} = U\Sigma_w V', \tag{5}$$

where U and V' are obtained from Eq. (3). To calculate Σ_w, Σ(1,1) is replaced by $\Sigma_w(1, 1)$. The value of σ_1 is later required in extraction process and will be stored in ref_img_{ij}. The reference image *ref_img* has the same dimensions of the watermark and each component of the reference image corresponds to the largest singular value of $wm\_img\_blk\_sel\_dct_{ij}$. In other words $ref\_img_{ij} = \sigma_1$, where σ_1 is the largest singular value of the $img\_blk\_sel\_dct_{ij}$. Using the largest singular value of low frequency DCT coefficients and discarding the noise-prone ones, substantially fortifies the robustness of the proposed method against common attacks.

The inverse DCT of matrix $B_{M\times N}$ is defined as

$$A_{ij} = \sum_{u=0}^{M-1}\sum_{v=0}^{N-1} \alpha_u\alpha_v \cos\left[\frac{\pi u}{2M}(2i+1)\right]\cos\left[\frac{\pi v}{2N}(2j+1)\right]F(u,\ v) \tag{6}$$

where α_λ is defined according to Eq. (2). After obtaining the watermarked pixels in the spatial domain, they are replaced in the selected locations (look at Figs. 1 and 2).

2.2. The extraction procedure

To extract the embedded watermark, it is necessary to have the key used in the embedding procedure. Fig. 5 shows the extraction procedure. The three inputs of the extraction procedure are the watermarked image, the key, and the reference image. The block selection, the DCT, and the SVD are carried out exactly in the same way as elaborated in Section 2.1. We avoid prolonging this section by repeating the same flow. To extract the embedded watermark bit, $\hat{w}_{ij}$, the Σ of the relevant $wm\_img\_blk\_sel\_dct_{ij}$ is calculated and is compared to the ref_img_{ij}:

$$\hat{w}_{ij} = \begin{cases} 1 & ref\_img_{ij} > \sigma_{1w} \\ 0 & ref\_img_{ij} \le \sigma_{1w} \end{cases} \tag{7}$$

After extracting the watermark bit, it's possible to remove the watermark from the watermarked image. To do so

$$\sigma_{1,rec} = \begin{cases} \sigma_{1w} - gf & \hat{w}_{ij} = 1 \\ \sigma_{1w} + gf & \hat{w}_{ij} = 0 \end{cases} \tag{8}$$

where $\sigma_{1,\ rec}$ refers to the largest singular value of the relevant block of the recovered image.

The DCT coefficients of the relevant block is obtained by

$$rec\_blk\_sel\_dct_{ij} = U\Sigma_{rec}V' \tag{9}$$

where Σ_{rec} is obtained according to Eq. (8). As stated previously in Section 2.1, the inverse DCT is applied into $rec\_blk\_sel\_dct_{ij}$ to obtain the pixels of the recovered image in the spatial domain.

3. Experimental results

3.1. Assessment criteria

Compared to the host image, the watermarked image is expected to be as imperceptible as possible. A classical metric to measure the coincidence between the host image and the degraded one, is PSNR and is defined as

$$PSNR = 10\log_{10}\left(\frac{MAX^2 n_{El,h}n_{El,v}n_{\mu I,h}n_{\mu I,v}}{\sum_{i=1}^{n_{El,h}}\sum_{j=1}^{El,v}\sum_{k=1}^{\mu I,h}\sum_{l}^{\mu I,v}\left(I(i,j,k,l) - I_w(i,j,k,l)\right)^2}\right) \tag{10}$$

Here $n_{\mu I,\ h}n_{\mu I,\ v}$ are the number of horizontal and vertical views used to capture the elemental images, while I and I_w stand for the host and the watermarked image, respectively.

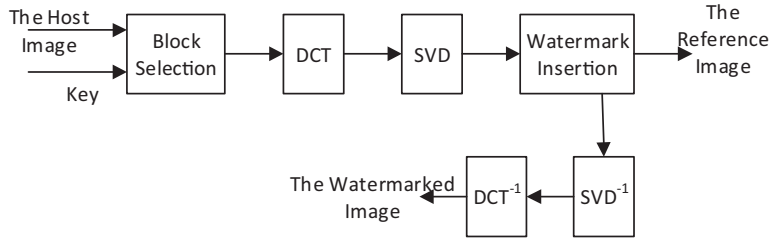

Fig. 4. The embedding procedure.

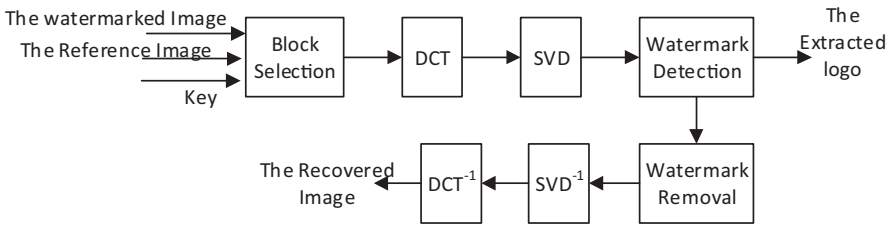

Fig. 5. The extraction procedure.

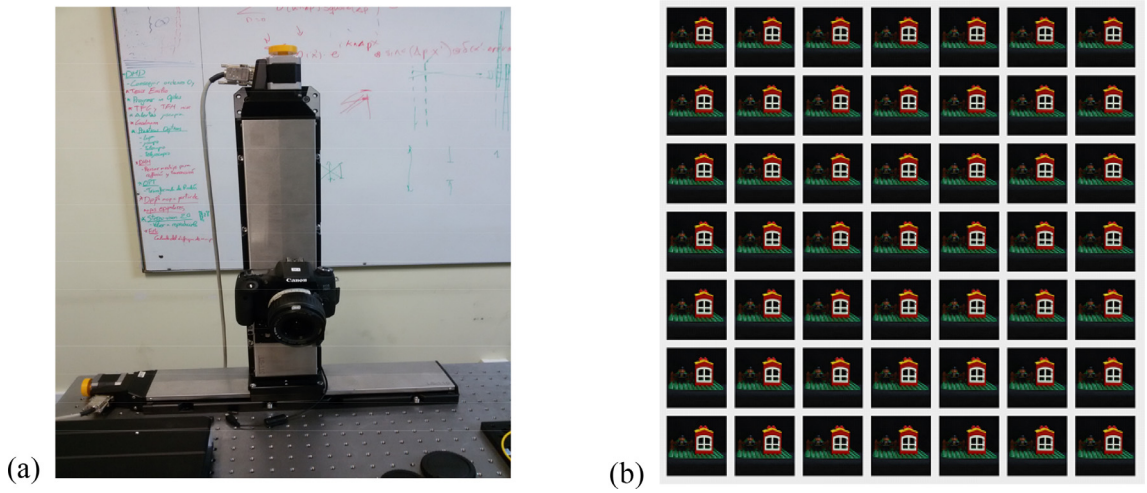

Fig. 6. (a) The experimental setup; (b) Central 7×7 elemental images of the 3D scene.

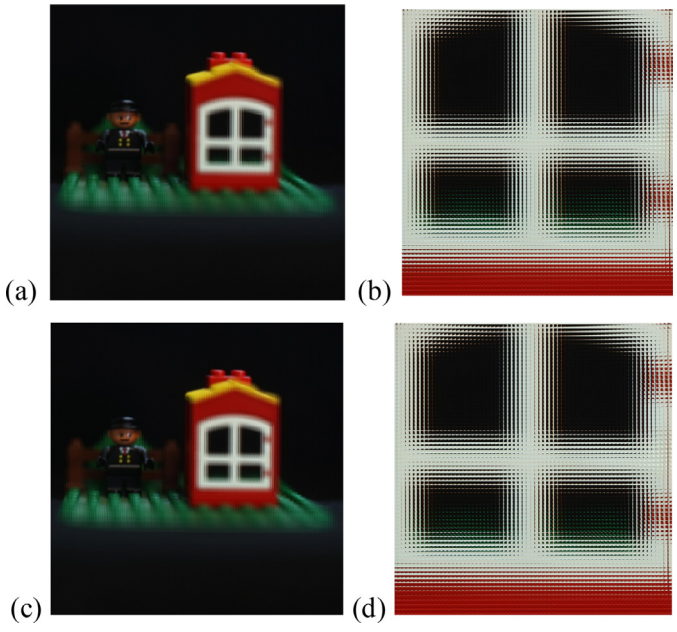

Fig. 7. (a) The host plenoptic image; (b) Zoomed area of it; (c) The watermarked image; and (d) Zoomed area of it. The watermark strength $gf = 90$, $n_{dct} = 3$, $SNR = 63.360\ dB$.

The higher the PSNR, the better the quality of the watermarked image. Ideally, the *PSNR* of two identical images is infinite, as the denominator of the Eq. (10) will be equal to zero. Similarly, the *PSNR* of recovered image is expected to be infinite. This hypothesis doesn't hold practically, due to the finite number of bits used to represent the float point figures, e.g. $\sqrt{2}$, in Eqs. (1) and (2). However, the *PSNR* of recovered images is high enough for making it identical to the host image for HVS.

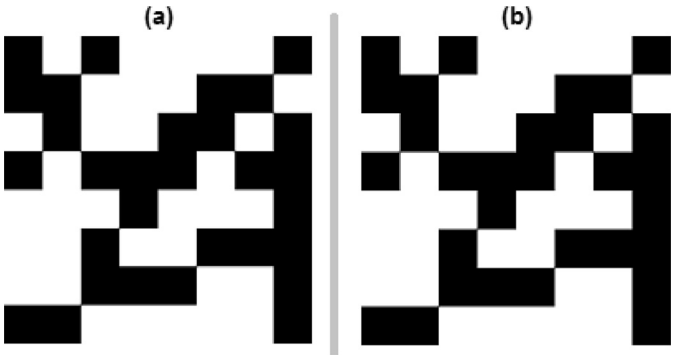

Fig. 8. (a) The embedded logo.; (b) The extracted logo. Watermark Strength = 90, $BER = 0$.

To verify the accuracy of the extracted logo, *BER* is used and is defined as

$$BER = \frac{\sum_{i=1}^{N_b} \sum_{j=1}^{N_b} \left(w_{i,j} \oplus \hat{w}_{ij}\right)}{N_b \times N_b}, \tag{11}$$

where $\oplus$ is the exclusive OR operator. The perfect extraction of the embedded logo will lead to $BER = 0$. In that case, all the bits of the extracted logo would be equal to those of the embedded logo. On the other hand, if all the bits are extracted incorrectly, $BER = 1$.

PSNR and *BER* are classical metrics and are widely used in the literature. These metrics merely consider the numerical values and do not incorporate the HVS. In [43] the authors highlight the vision mechanism resulting in perceiving the world visually. They suggest that HVS is mainly sensitive to the mean structural similarity (MSSIM), which is used to measure the structural degradation of the image content and is

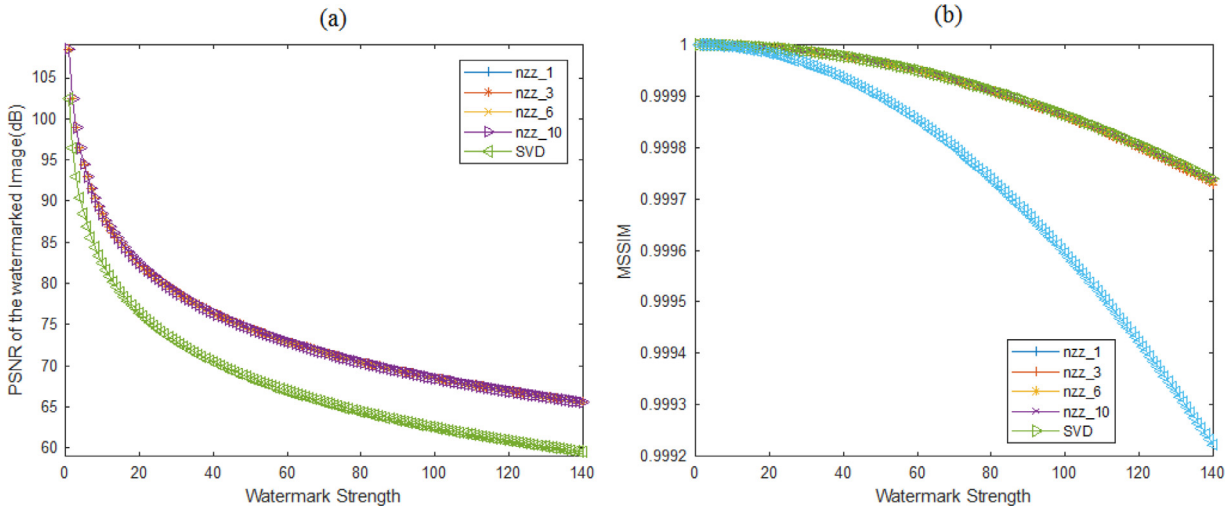

Fig. 9. (a) The PSNR of the watermarked images vs. watermark strength; (b) the MSSIM. Note that both metrics are calculated for four different number of DCT coefficients, and also for the SVD method.

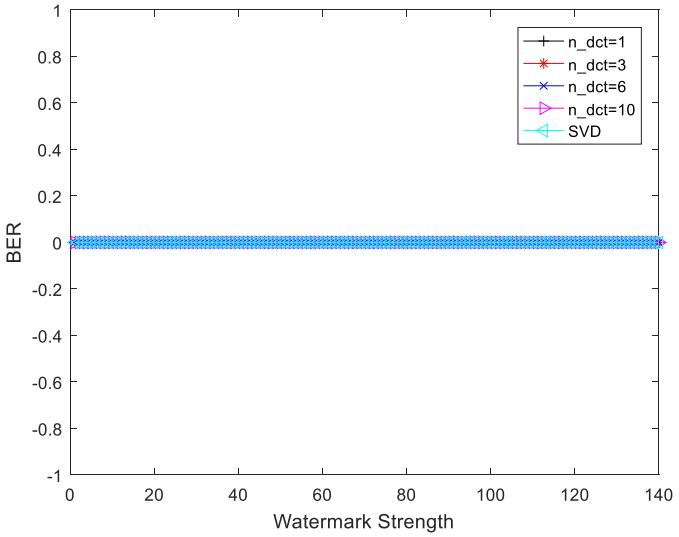

Fig. 10. The BER of the watermarked images vs. watermark strength.

stated as

$$MSSIM(I,\ I_w) = \frac{(2\mu_I\mu_w + C_1)(2\sigma_{I,I_w} + C_2)}{(\mu_I^2 + \mu_{I_w}^2 + C_1)(\sigma_I^2 + \sigma_{I_w}^2 + C_2)} \tag{12}$$

Here μ_I *and* μ_{I_w} are the mean intensities. Besides, σ_I *and* σ_{I_w} are the variances of the host and the watermarked image, respectively. Constants C_1 and C_2 are selected depending on the image content. If C_1 and C_2 are set equal to zero, then MSSIM turns to universal quality index (UQI). According to [43], the HVS is extremely non-linear and it may happen that two images with very different amount of degradation have exactly the same *PSNR* but having different *MSSIM*. The MSSIM compares the luminance, contrast and structure of the two images. The minimum and the maximum value of the MSSIM are −1 and + 1. The figure + 1 can be obtained only in the case of comparing two identical images (i.e. PSNR = ∞). It is noticeable that the MSSIM drops below its maximum value rapidly and therefore, there's a significant degradation at MSSIM = 0.9.

3.2. Performance analysis

In order to verify the performance of the proposed method, some experiments are conducted. The experimental setup used for the acquisition of the original image, is shown in Fig. 6(a) In this setup a digital camera (Canon 450D) was mounted in a rail, so that a computer could control its lateral position accurately. The scene was placed at an axial depth of about 73 cm from the digital camera. With this setup we captured 16 × 16 elemental images, each resized to 300 × 300 pixels. The camera displacement between adjacent images was of 5.00 mm. This collection of elemental images (or view images) composes an integral image with 4800 × 4800 pixels (See Fig. 6(b), where only the 7 × 7 central elemental images are shown).

After applying a light-field transposition algorithm [44], the plenoptic image is calculated from the integral image. Such image is composed of 300 × 300 microimages with 16 × 16 pixels each. The importance of such plenoptic image is essential, since it is the one that is projected onto the plenoptic monitor. Fig. 7(a) shows the host plenoptic image, while Fig. 7(b) shows a zoomed area of it, in which the structure of the microimages is more apparent.

Our next step in this experimental Section is to embed the logo into the host plenoptic image. The embedded logo is shown in Fig. 8(a). The randomness of the logo ensures us that the proposed method is not biased toward any specific logo and can be used with any arbitrary logo. This logo consists of 8 × 8 bits, whose values were generated on a random basis.

Following the procedure described above, the logo is embedded into the host plenoptic image and the watermarked image is obtained. The watermarked plenoptic image is shown in Fig. 7(c) and (d). To make sure of the accuracy of the proposed method, two evaluations should be carried out: First, the indistinguishability between the host plenoptic image and the watermarked one. The second item to evaluate is the similarity between the embedded and the extracted logo.

In order to compare the imperceptibility of any possible difference between the host and the watermarked images, the PSNR and the MSSIM are employed. The results are shown in Fig. 9. It can be deduced from these results that neither PSNR nor MSSIM are affected by the number of the DCT coefficients. More important is the fact that even for the largest values of the watermark strength, the PSNR is still higher than 59.5 *dB*. For example, in case of $gf = 90$, and $n_{dct} = 3$, the $PSNR = 69.38\ dB$. These values are definitely much more than enough for HVS to avoid distinguishing between the host image and the watermarked one. It is interesting, as well, that for all the values of watermark strength *SSIM*

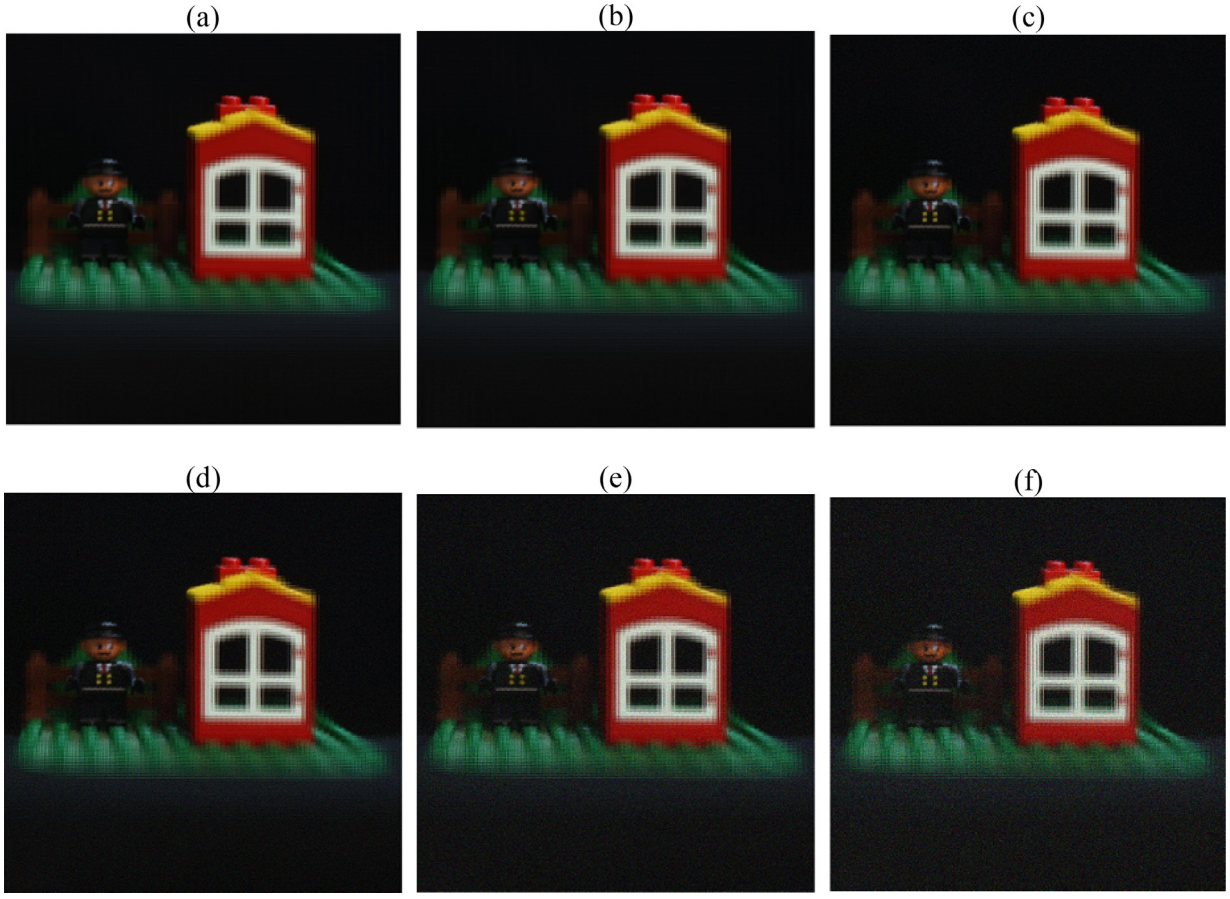

Fig. 11. The noisy watermark image. (a) The host plenoptic image; (b) The watermarked image (gf = 90 and n_dct = 3); (c) The watermarked image exposed to Gaussian noise of $\sigma^2 = 100$; (d) $\sigma^2 = 225$; (e) $\sigma^2 = 625$; and (f) $\sigma^2 = 1225$.

remains higher than 0.997 and therefore the structural similarity of the watermarked image is highly preserved by the proposed method.

A question of interest is whether one could eliminate the DCT and DCT^{-1} stages from the building blocks of the embedding and the extraction subsystems (Figs. 4 and 5). Hereafter, we will refer to this approach as the SVD method. What we can say here is that in terms of the PSNR and the MSSIM, SVD method is superior. Although the obtained results of other methods, are by far beyond HVS power to recognize even the most infinitesimal differences between the host image and the watermarked one. Also for median filtering and low-bit-rate JPEG compression ($qf = 5\%,\ 50\%$), SVD method yields better results. It is noticeable that JPEG compression at very low-bit-rate is not very common and causes a drastic fall in image quality. While the imperceptibility is a promise of image watermarking, even the host image (without any watermark) is immensely degraded and it does not make any sense to preserve neither the content nor the ownership of such degraded image. As an example, the reader may pay attention to the two vertical stakes of Fig. 5(b) which are appeared as some ugly spots in the image. On the other hand, when it comes to $qf = 100\%$, the SVD method and the proposed method converge to the same results and it is safe to say that for $93 < gf$, the SVD method is identical to the proposed method. While the *qf* of JPEG compression is often controlled by human, the noise usually has a random nature and it's impossible to predict the noise power in practical applications. A popular example may be the wireless communication channels which are inevitable part of communication systems nowadays, from mobile data networks to bluetooth and wifi, all of them are subject to noise and the proposed method exhibits a promising robustness against noise and our finding show that the DCT decreases the vulnerability of the proposed method against Gaussian noise dramatically.

To evaluate the similarity between the embedded and the extracted logo the BER is calculated according to Eq. (11). The results are shown in Fig. 10. We found that even for the smallest values of the watermark strength, the embedded logo can be extracted perfectly. Indeed, this result is absolutely consistent with the aforementioned fact that the extraction process is error-free regardless of the watermark strength. It is very interesting to note that this remark also holds for different values of n_{dct}. Again, there is no difference between the BER of the both methods.

The last step in this Section is to compare the recovered image and the host image. Again, the comparison was made in terms of the PSNR. Our simulations show that the *PSNR* of the recovered image is always higher than 67 dB and makes it impossible for the HVS to distinguish between the host and the recovered images. The minimum difference between the PSNR of the recovered image and the watermarked one, is always 6 dB or higher. In the specific case of $gf = 90$, the PSNR of the recovered image is 293.96 dB better than the watermarked one. As mentioned earlier, in Section 3.1, the finite number of bits used in any software to represent floating-point values, hinders reaching infinite *PSNR* for the recovered image. Anyway, *PSNR* is a logarithmic parameter and even an increment of one unit, can improve the quality substantially. It is noticeable that the *PSNR* of the recovered images are considerably higher than that of the watermarked images.

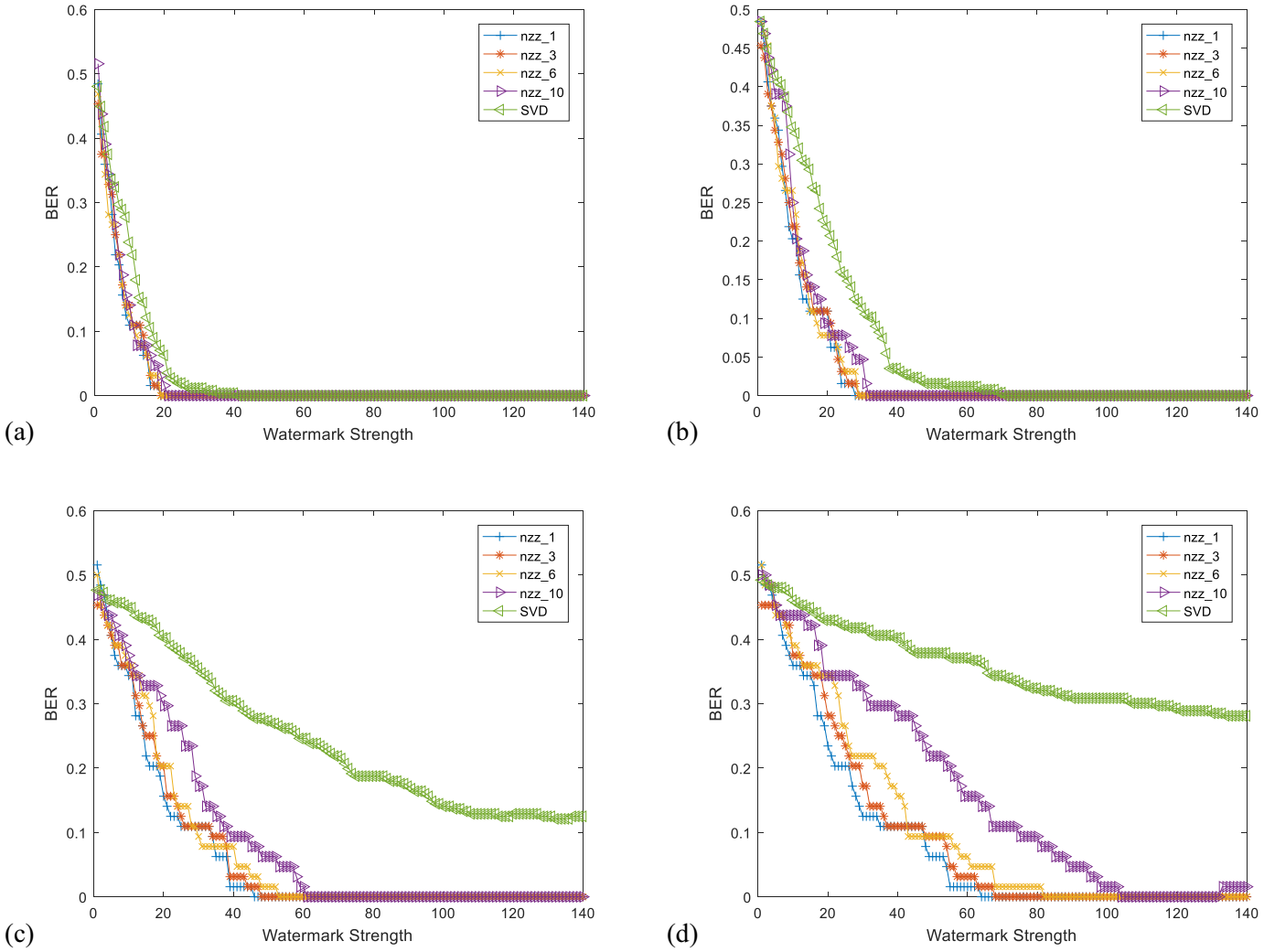

Fig. 12. The BER of watermarked image exposed to Gaussian noise of: (a) $\sigma^2 = 100$; (b) $\sigma^2 = 225$; (c) $\sigma^2 = 625$; (d) $\sigma^2 = 1225$.

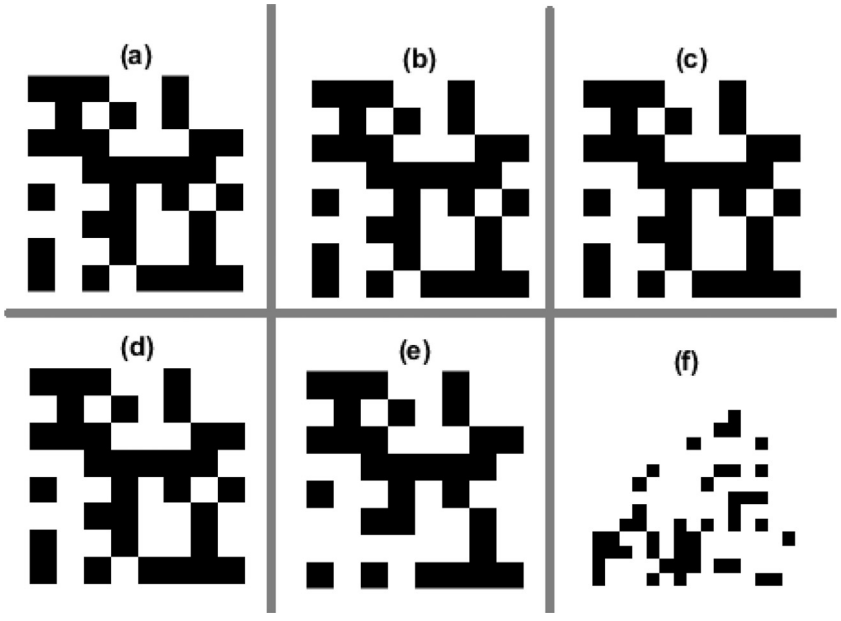

Fig. 13. The extracted logo from the noisy watermarked image for watermark image for $gf = 90$ and $\sigma^2 = 1225$. (a) The extracted logo from noise-free watermarked image, $gf = 90$ and $n_{dct} = 3$ $(BER = 0)$; (b) $\sigma^2 = 1225, gf = 90$ *and* $n_{dct} = 1(BER = 0)$; (c) $\sigma^2 = 1225, gf = 90$ *and* $n_{dct} = 3(BER = 0)$; (d) $\sigma^2 = 1225, gf = 90$ *and* $n_{dct} = 6(BER = 0)$; (e) $\sigma^2 = 1225, gf = 90$ *and* $n_{dct} = 10(BER = 0.047)$; and (f) SVD method with $\sigma^2 = 1225, gf = 90(BER = 0.309)$.

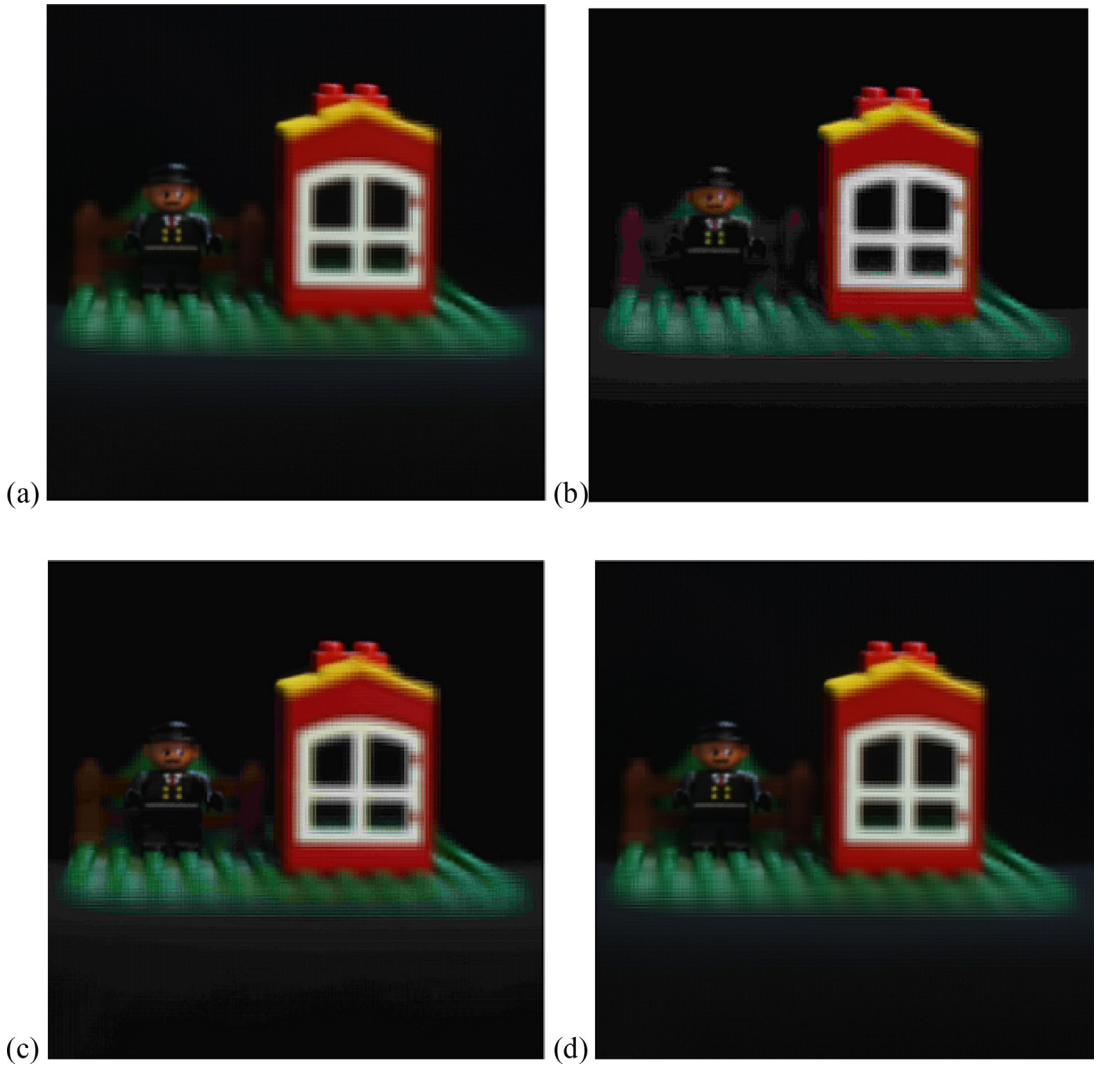

Fig. 14. The impact of JPEG compression on watermarked images. (a) The watermarked image (calculated for gf = 90 and n_dct = 3) (b) The watermarked image after JPEG compression ($qf = 5\%$); (c) $qf = 50\%$; and (d) $qf = 100\%$.

3.3. Robustness analysis

As demonstrated in the previous section, our proposed technique provides indistinguishable watermarked and recovered images. In addition, the extracted logo is identical to the embedded logo. However, as it is common in the literature, the performance analysis has been done under the assumption of no attack. As well known, a good watermarking technique should deliver a great robustness against any potential attack. Specifically, the robustness of the proposed method is verified against the most common attacks, i.e., Gaussian noise, JPEG compression and median filtering.

3.3.1. Gaussian noise

First, the watermarked plenoptic image was contaminated with additive Gaussian noise of different noise powers. Fig. 11 shows the host image, the watermarked image (corresponding to the specific case of n_dct = 3 and gf = 90) and the noisy images. These particular images are shown to illustrate that high values of Gaussian noise are very overwhelming and have heavy adverse effect on the visual quality of the image. As it is evident from Fig. 11, the noise power of 625 (Fig. 5(e)) has a significant affect on the watermarked image and the impact is even more noticeable for noise power of 1225..

Aimed at evaluating the robustness of the method, the BER is computed not only for the specific case shown in Fig. 11, but also for the watermarked images obtained for $n\_dct = 1, 3, 6$ and 10, and for gf from 1 to 140. The results of this calculation are shown in Fig. 12. Provided that the *gf* is over a certain threshold, it is evident from Fig. 12 that the proposed method is capable of achieving very low BER figure regardless of the noise extremity. This also holds even for the severest noise attacks and is independent from the value of n_dct. However, when the watermarked image is exposed to the extreme noise, the SVD method leads to unacceptable BER results vastly inferior to the proposed method. It can be inferred that even if heavy noise attacks occur the proposed method exhibits outstanding robustness. Fig. 13 shows the extracted logo from the watermarked image exposed to Gaussian noise. It conveys a criterion of the importance of n_dct as well as the inability of the SVD method to extract the embedded logo in extreme noise conditions.

Before going to the next Section we would like to make a deeper analysis of these results and explain the physical reason behind the fact that lower values of n_dct provide better results, and also why SVD method provides such unacceptable results.

As stated in Section 2, the high-frequency coefficients of DCT are highly sensitive to noise and can be easily modified if attacked by Gaussian noise. Hence, using such coefficients degrades the robustness of the proposed method. This hypothesis is in complete agreement with our

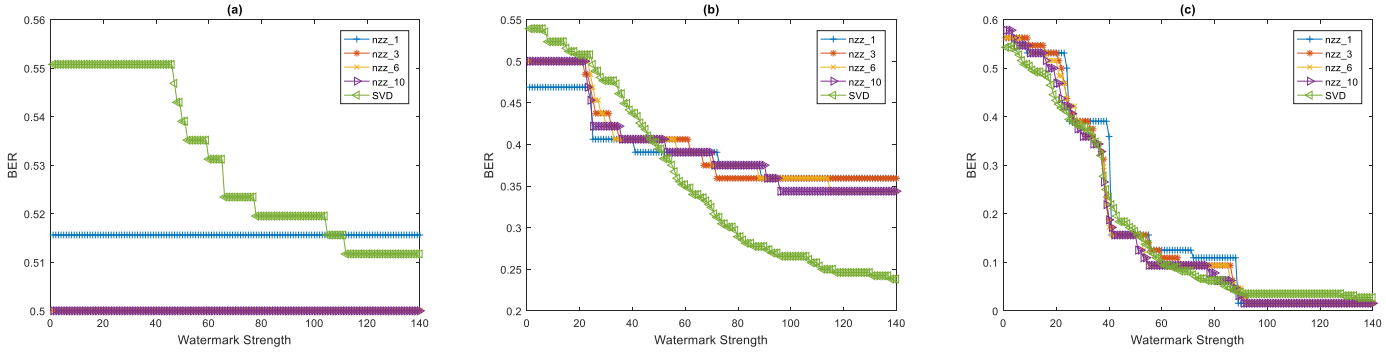

Fig. 15. The BER of watermarked image under JPEG Compression with (a) $qf = 5\%$; (b) $qf = 50\%$; and (c) $qf = 100\%$.

findings and it seems that using more than three DCT coefficients, will not improve the robustness of the method against noise any further. The first three coefficients ($n_{dct} = 3$) are very unlikely to be affected by noise and hence it is a brilliant idea to use these coefficients in the watermarking process. As other DCT coefficients may be affected by noise, using these coefficients makes the proposed method more vulnerable to the Gaussian noise.

Another noticeable point is removal of the DCT subblock. Although the proposed method can be implemented without DCT, it will be highly susceptible to the Gaussian noise. Discarding DCT subblock implies involving *all* DCT coefficients for watermark insertion (including the ones that are easily affected by noise) and results in exacerbation of the method performance against noise. It is apparent from Fig. that this hypothesis is fully consistent with our outcomes. The more powerful the noise imposed to the watermarked image, the higher error rate is yielded from excluding DCT subblock. If the power of the Gaussian noise is set 1225, the ramp of the SVD method roughly approaches zero and can be estimated by a few horizontal lines in a few intervals which are approximately independent of the watermark strength in respective intervals. In other words, excluding the DCT subblock has such fatal affect that even increasing the watermark strength will no longer cause any significant improvement of the BER. Such coefficients are also quantized more roughly by image compression standards and involving such coefficients in the watermarking process would decay the robustness of the method. The experimental results have further strengthened our confidence in eliminating most DCT coefficients. Consequently, it doesn't make any sense to remove the DCT sub-block.

3.3.2. JPEG compression

Another common attack is JPEG compression, which is frequently used by various commercial systems. The robustness of the proposed method is verified against JPEG compression with quality factors (qf) of 5%, 50%, 100% [45] and for $n_{dct} = 1,\ 3,\ 6$ and 10. Fig. 14 shows the impact of JPEG compression on the watermarked images. The extreme severity of JPEG compression with qf of 5% (Fig. 14(b)) is easily detectable, e.g. the artifacts behind the doll. If the severity of the compression attack is moderated in the rate of 50% (Fig. 14(c)), some distortions are still observable, such as the artifacts in the bottom of the image. The qf = 100% (Fig. (d)) works quite well and the compressed image looks like the watermarked image and the artifacts are more visible only after zooming in the compressed image. This is just an example demonstrating the adverse affects of extremely low-rate JPEG compression on the quality of the watermarked image and typically, the compression ratio of the 5% and 50% are not expected to occur. If the JPEG compression with qf of 5%, 50% and 100% is used for an image watermarked with the gf = 90 and the $n_{dct} = 3$, the *BER* will be 0.500, 0.359 and 0.031.

Fig. 15 shows the numerical results for *BER* against JPEG compression. The simulations have been carried out for $qf = 5\%,\ 50\%,\ 100\%$ and $n_{dct} = 1,\ 3,\ 6,\ 10$. The main philosophy of JPEG compression is to reduce the file size, which causes an irreversible detrimental effect when *qf* falls down drastically.

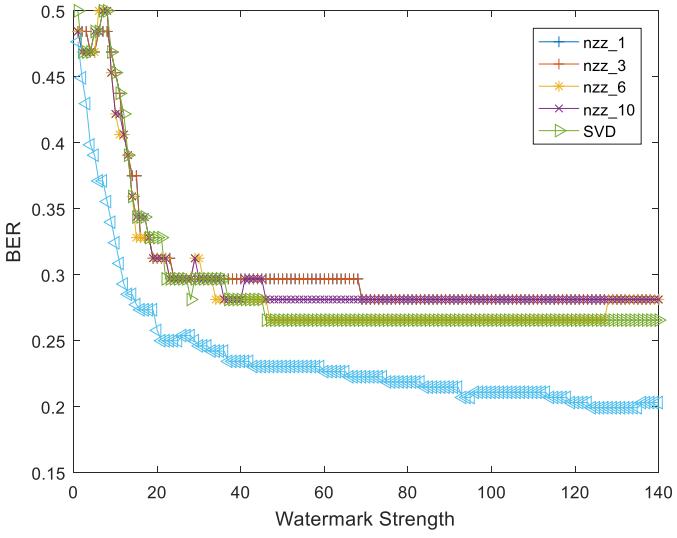

Fig. 16. The BER of watermarked image after median filtering.

3.3.3. Median filtering

Another typical attack is median filtering. For median filtering, a 3×3 window is used. Fig. 16 shows the results of the extracting logo after passing the watermarked image through median filter. The used values for n_dct are 1, 3, 6 and 10. From Fig. 16, it can be deduced that if the values of gain factor and n_{dct} are set 90 and 3 respectively, then the *BER* will be 0.266 after passing the watermarked image through the median filter.

4. Conclusions

In this paper we proposed a novel watermarking method for the plenoptic images. The essential notion and the mathematical details of the proposed method are elaborated and the role of each building block in the embedding and the extraction procedure is addressed. The assessment metrics are introduced briefly and the numerical results of the simulations are represented. The importance of the DCT is highlighted and the experimental results also confirm the lucid advantage of employing DCT. Even with the lowest figures of the watermark strength, the embedded logo can be extracted perfectly on assumption that no attack will affect the watermarked image. The robustness of the proposed method has been verified against Gaussian noise, JPEG compression and median filtering. The authors express their highest gratitude for the potential readers who give any feedback about this research.

Acknowledgments

This work was supported in by the Plan Nacional I + D + I, under the grant DPI2015-66458-C2-1R, Ministerio de Economía y Competitividad (MINECO), Spain. We also acknowledge the support from the Generalitat Valenciana (GVA), Spain, (grant PROMETEOII/2014/072). S. Hong acknowledges a predoctoral contract from University of Valencia. A. Ansari acknowledges a predoctoral contract from EU H2020 program under MSCA grant 676401.

References

[1] Rial A, Deng M, Bianchi T, Piva A, Preneel B. A provably secure anonymous buyer–seller watermarking protocol. IEEE Trans Inf Forensics Secur 2010;5:920–31.
[2] Panah AS, Van Schyndel R, Sellis T, Bertino E. On the properties of non-media digital watermarking: a review of state of the art techniques. IEEE Access 2016;4:2670–704.
[3] Sadreazami H, Ahmad MO, Swamy M. Multiplicative watermark decoder in contourlet domain using the normal inverse Gaussian distribution. IEEE Trans Multimed 2016;18:196–207.
[4] Subramanyam A, Emmanuel S, Kankanhalli MS. Robust watermarking of compressed and encrypted JPEG2000 images. IEEE Trans Multimed 2012;14:703–16.
[5] Sadreazami H, Ahmad MO, Swamy MS. A study of multiplicative watermark detection in the contourlet domain using alpha-stable distributions. IEEE Trans Image Process 2014;23:4348–60.
[6] Karybali IG, Berberidis K. Efficient spatial image watermarking via new perceptual masking and blind detection schemes. IEEE Trans Inf Forensics Secur 2006;1:256–74.
[7] Wang J, Lian S. On the hybrid multi-watermarking. Signal Process 2012;92:893–904.
[8] Song C, Sudirman S, Merabti M. A robust region-adaptive dual image watermarking technique. J Vis Commun Image Represent 2012;23:549–68.
[9] Parah SA, Sheikh JA, Loan NA, Bhat GM. Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing. Digit Signal Process 2016;53:11–24.
[10] Kishk S, Javidi B. Watermarking of three-dimensional objects by digital holography. Opt Lett 2003;28:167–9.
[11] Cheng C-J, Hwang W-J, Zeng H-Y, Lin Y-C. A fragile watermarking algorithm for hologram authentication. IEEE J Disp Technol 2014;10:263–71.
[12] Huang H-Y, Yang C-H, Hsu W-H. A video watermarking technique based on pseudo-3-D DCT and quantization index modulation. IEEE Trans Inf Forensics Secur 2010;5:625–37.
[13] Lin W-H, Horng S-J, Kao T-W, Fan P, Lee C-L, Pan Y. An efficient watermarking method based on significant difference of wavelet coefficient quantization. IEEE Trans Multimed 2008;10:746–57.
[14] Rahman SM, Ahmad MO, Swamy M. A new statistical detector for DWT-based additive image watermarking using the Gauss–Hermite expansion. IEEE Trans Image Process 2009;18:1782–96.
[15] Khalilian H, Bajic IV. Video watermarking with empirical PCA-based decoding. IEEE Trans Image Process 2013;22:4825–40.
[16] Wu Y. On the security of an SVD-based ownership watermarking. IEEE Trans Multimed 2005;7:624–7.
[17] Kim H-D, Lee J-W, Oh T-W, Lee H-K. Robust DT-CWT watermarking for DIBR 3D images. IEEE Trans Broadcast 2012;58:533–43.
[18] Ansari A, Dorado A, Saavedra Tortosa G, Martínez Corral M. Plenoptic image watermarking to preserve copyright. In: Proceedings of the SPIE, 10219; 2017 *0A-1-0A-6*.
[19] Mairgiotis AK, Galatsanos NP, Yang Y. New additive watermark detectors based on a hierarchical spatially adaptive image model. IEEE Trans Inf Forensics Secur 2008;3:29–37.
[20] Kwitt R, Meerwald P, Uhl A. Lightweight detection of additive watermarking in the DWT-domain. IEEE Trans Image Process 2011;20:474–84.
[21] Ansari A, Danyali H, Helfroush M. Spread-spectrum robust image watermarking for ownership protection. In: Proceedings of the twenty second Iranian conference on electrical engineering (ICEE); 2014. p. 1427–31.
[22] Sadreazami H, Ahmad MO, Swamy MS. A robust multiplicative watermark detector for color images in sparse domain. IEEE Trans Circuits and Syst II: Express Br 2015;62:1159–63.
[23] Li X, Sun X, Liu Q. Image integrity authentication scheme based on fixed point theory. IEEE Trans Image Process 2015;24:632–45.
[24] Roldan LR, Hernandez MC, Chao J, Miyatake MN, Meana HP. Watermarking-based color image authentication with detection and recovery capability. IEEE Lat Am Trans 2016;14:1050–7.
[25] Boyer J-P, Duhamel P, Blanc-Talon J. Scalar DC–QIM for semifragile authentication. IEEE Trans Inf Forensics Secur 2008;3:776–82.
[26] Chang C-S, Shen J-J. Features classification forest: a novel development that is adaptable to robust blind watermarking techniques. IEEE Trans Image Process 2017;26.
[27] Stütz T, Autrusseau F, Uhl A. Non-blind structure-preserving substitution watermarking of H. 264/CAVLC inter-frames. IEEE Trans Multimed 2014;16:1337–49.
[28] Bao F, Deng RH, Ooi BC, Yang Y. Tailored reversible watermarking schemes for authentication of electronic clinical atlas. IEEE Trans Inf Technol Biomed 2005;9:554–63.
[29] Jiang R, Zhou H, Zhang W, Yu N-H. Reversible Data Hiding in Encrypted 3D Mesh Models. IEEE Trans Multimed 2017.
[30] Adelson EH, Bergen JR. The plenoptic function and the elements of early vision. In: Computational models of visual processing. Cambridge, MA: MIT Press; 1991. p. 3–20.
[31] Navarro H, Dorado A, Saavedra G, Corral MM. Three-dimensional imaging and display through integral photography. J Inf Commun Converg Eng 2014;12:89–96.
[32] Lippmann G. Epreuves reversibles donnant la sensation du relief. J Phys Theor Appl 1908;7:821–5.
[33] Javidi B, Shen X, Markman AS, Latorre-Carmona P, Martínez-Uso A, Sotoca JM, et al. Multidimensional optical sensing and imaging system (MOSIS): from macroscales to microscales. Proc IEEE 2017;105:850–75.
[34] Koz A, Cigla C, Alatan AA. Watermarking of free-view video. IEEE Trans Image Process 2010;19:1785–97.
[35] Paudyal P, Battisti F, Neri A, Carli M. A study of the impact of light fields watermarking on the perceived quality of the refocused data. In: Proceedings of the 3DTV-conference: the true vision-capture, transmission and display of 3D video (3DTV-CON); 2015. p. 1–4.
[36] Koz A, Cigla C, Alatan AA. Free-view watermarking for free-view television. In: Proceedings of the IEEE international conference on image processing; 2006. p. 1405–8.
[37] Koz A, Çığla C, Alatan AA. Watermarking for light field rendering. In: Proceedings of the Fifteenth European signal processing conference; 2007. p. 2296–300.
[38] He M, Cai L, Liu Q, Wang X, Meng X. Multiple image encryption and watermarking by random phase matching. Opt Commun 2005;247:29–37.
[39] Kishk S, Javidi B. 3D object watermarking by a 3D hidden object. Opt Express 2003;11:874–88.
[40] Javidi B. Optical and digital techniques for information security vol. 1. Springer Science & Business Media; 2006.
[41] Cho M, Javidi B. Three-dimensional photon counting double-random-phase encryption. Opt Lett 2013;38:3198–201.
[42] Wang Y, Ostermann J, Zhang Y-Q. Digital video processing and communications. New Jersy: Prentice Hall; 2001.
[43] Wang Z, Bovik AC, Sheikh HR, Simoncelli EP. Image quality assessment: from error visibility to structural similarity. IEEE Trans Image Process 2004;13:600–12.
[44] Martínez-Corral M, Dorado A, Navarro H, Saavedra G, Javidi B. Three-dimensional display by smart pseudoscopic-to-orthoscopic conversion with tunable focus. Appl Opt 2014;53:E19–25.
[45] Luo W, Huang J, Qiu G. JPEG error analysis and its applications to digital image forensics. IEEE Trans Inf Forensics Secur 2010;5:480–91.