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
Available online 25 April 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.

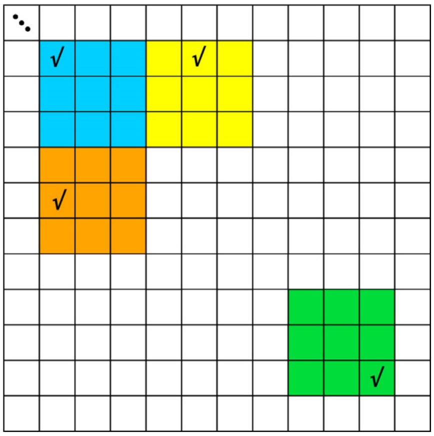

Fig. 1. A possible pixel selection from the different μIs. In this scheme, for simplicity, mI are comprised of 3 × 3 pixels. Of course in a real case there is no limitation in their dimension.

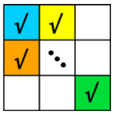

Fig. 2. Arrangement of the selected pixels as a matrix.

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

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