Journal of Information Security and Applications 41 (2018) 12–27

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

A robust HDR images watermarking method using artificial bee colony algorithm

F. Yazdan Bakhsh, Mohsen Ebrahimi Moghaddam*

Faculty of Computer Science and Engineering, Shahid Beheshti University, G.C., Tehran, Iran

ARTICLE INFO

Article history:

Keywords:
Artificial bee colony (ABC)
High dynamic range (HDR)
Tone mapping operator (TMO)
Watermarking
Discrete wavelet transform (DWT)

ABSTRACT

In this paper, a robust watermarking method for High Dynamic Range Images (HDRIs) is presented. In order to find the best block for watermark insertion, Artificial Bee Colony (ABC) is employed. After selection of the best block, the insertion procedure inserts binary marks in the selected first level approximation sub-band of Discrete Wavelet Transform (DWT) in each selected block. In the extraction process, an extraction method is applied to obtain and detect the hidden marks. Several experiments have been done to show imperceptibility and robustness of the proposed algorithm on a dataset of 12 HDR images. The results have shown the superiority of the proposed algorithm to some state of the art methods.

1. Introduction

The real world has much more brightness than what is captured by camera sensors. The limitation of these sensors and the desire of having images that are more similar to what the human eyes perceive have inspired many researchers to work on the problem. One of the methods presented to create high dynamic range images was the honored work of Debevec and Malik [1]. They produced an image by capturing multiple images from the same scene with different exposure time and combining them to create a high dynamic range image [2].

HDR images can offer a great range of intensity which makes them more natural images that cover a broader range of intensities visible to the human visual system. They can show more colors and cover greater intensity as they are based on floating points. These images use a full float of 32 for each channel, thus, they have the ability to show colors with 96 bits per pixel accuracy. Although HDR images have great quality, most of the displaying devices cannot show them due to devices limited dynamic range. As a result, tone mapping operators (TMOs) have been introduced as a solution. TMOs map HDR images dynamic range to a limited one; the process is called tone mapping attack. Thus, regular devices are able to display them. In HDR image watermarking, one of the most important challenges is extracting watermark after tone mapping attacks [3].

Because of the superiority of high dynamic range (HDR) images over low dynamic range images, they have drawn attention in the image industry. By increasing the popularity of HDR images, many concerns regarding authentication and copyright protection of them have been raised. The authentication is guaranteed by watermarking that is the process of embedding a watermark, tag or label into a cover multimedia in order to detect or extract the watermark later and make an assertion about the multimedia copyright licenses, tracking, and authorship. The multimedia can be audio, video, picture or text [4]. Watermarking methods should have several important factors; one of these factors is robustness that refers to the watermark ability to survive after employing processing operations and attacks. The other factor is imperceptibility that means the watermark should not be detectable by human eyes, and only the authorized agency can detect them through special processing. Another factor is capacity that is defined as the maximum amounts of information bits that can be embedded in a cover image [5].

Many types of research have been done in the watermarking of HDR images. The studies can be categorized based on their embedding domain, capacity, and HDR encodings. Some of the works are reviewed in Section 2.

In this paper, the HDR image is watermarked using the Artificial Bee Colony (ABC) algorithm. The idea of using evolutionary algorithms for watermarking HDR images is new and has not been studied before. Previous watermarking approaches have used evolutionary algorithms in the domain of RGB color images or gray scale ones. Therefore, those works never had issues related to HDR images such as robustness against tone-mapping operators and imperceptibility. The ABC is used to find the best insertion location (blocks). The proposed algorithm including the insertion and extraction of the watermark is robust against TMOs and common

* Corresponding author.
E-mail address: m_moghadam@sbu.ac.ir (M.E. Moghaddam).

https://doi.org/10.1016/j.jisa.2018.05.003
2214-2126/

watermarking attacks which are prevalent image manipulation techniques for low dynamic range (LDR) images.

The proposed insertion method is different from other works as it uses adaptive strength factor to insert the watermark in each block based on the blocks' properties to ensure a reasonable imperceptibility. In this conception, the block size is an important factor and should not be very large or very small. The proposed algorithm considers blocks of size 4×4 in the spatial domain; in other words, blocks of size 2×2 in the wavelet domain. The work uses non-overlapping blocks in order to remove limitation created by blocks' size. First, the original image is converted from RGB to LogLUV domain. Then LogL component is extracted and the wavelet transform is applied to the LogL component to obtain LH and HL sub-bands as the embedding domains for each block, the corresponding watermark bit is embedded once in the LH sub-band and once in the HL sub-band then the cost function is calculated and the sub-band with the better result based on cost function is selected as embedding sub-band. The embedding locations are selected randomly and improved using ABC algorithm. Since the embedding locations are selected randomly, the work is somewhat robust against different situations regarding the attacks that affect low frequency or high-frequency parts of images. Only one coefficient of each selected block in the investigated sub-band is changed in order to guarantee less distortion and as a result a better quality. Imperceptibility of the proposed algorithm is compared against the work proposed in [6] based on hdrvdp2 suggested in [7], and the robustness is evaluated against several tone mapping and regular watermarking attacks. Finally, results are reported in bit error rate (BER), and HDRVDP2 metrics.

The remainder of the paper is organized as follows: in Section 2, related works are explained, and in Section 3, the proposed method is explained thoroughly. The experimental results are illustrated in Section 4 and finally, the conclusion of the paper is brought in Section 5. There is also an Appendix part in which artificial bee colony is described.

2. Related works and backgrounds

2.1. Backgrounds

HDR images have three basic formats, RGBE, TIFF, and EXR. RGBE is known as Radiance format, introduced by Greg Ward Larson in [8]. The Format has three color channels including red, green, and blue mantissa values and a shared exponent channel. The format needs 32 bits to show an image instead of 24 bits that are typical for LDR images; in other words, it considers eight bits for each channel. The dynamic range for these encodings is quite large (over 76 orders of magnitude). The second format, TIFF, also introduced by Greg Ward Larson [8]. The format is also known as LOGLUV format. LOGLUV format is constituted of 32 bits, 16 bits for the logarithm of the luminance information and 16 bits for CIELUV (u', v') chromaticity coordinates. LogLUV allocates 8 bits for each of u' and v' coordinates. The dynamic range for these encodings is quite large (over 38 orders of magnitude). The third format is EXR and has the largest bit depth, 48 bits. It is based on a 16-bit half floating-point type. The half data type is also called S5E10 to identify the structure of each color channels; as it is obvious from this name, S5E10, one sign bit, five bits exponent and 10 bits mantissa constitute each channel. The dynamic range for these encodings is quite large (over 10.7 orders of magnitude).

2.2. Related works

Several studies have been done on HDR image watermarking. The studies have been classified based on their embedding domain. Most of the works presented so far are in the frequency domain and are divided into five groups: 1. approaches inserting watermark in LogLUV domain, 2. studies embedding a watermark in RGBE domain, 3. approaches using a bilateral filter to embed watermark, 4. studies using LDR representation of the HDR image to insert watermark and 5. those ones inserting watermark in the spatial domain.

The approaches in the first group embed watermark in LogLuv domain based on [9], LogLUV is one of the HDR images encoding. It is useful because of giving access to LogL channel that is the part of image manipulated by most of tone-mapping techniques, the other benefit of using this encoding as embedding domain is that the conversion to and from LogLUV to RGB is feasible and unlike tone-mapping, it is possible to retrieve HDR image; F. Guerrini [10] proposed a watermarking method in which watermark is inserted in the luminance component of the approximation layer of discrete wavelet transform. The luminance component is obtained by Logluv transform proposed in [9], and for the embedding, the watermark Quantization Index Modulation (QIM) has been used; the suggested method uses higher order statistics such as block kurtosis as a feature. The image is divided into different blocks with different shapes and the embedding process happens by modifying the coefficients of each block and set the block kurtosis equal to a quantized value determined by watermark bit that is intended to be embedded in the block. To meet imperceptibility requirements, a perceptual mask based on luminance, contrast, and texture is used to obtain the maximum amount of distortion for each coefficient in embedding domain without causing artifacts. 15 HDR image and 7 tone-mapping attacks are considered in this paper. The work is one of the comprehensive work in HDR image watermarking and takes into account several tone-mapping attacks and there are several experiments in different setting parameters, however, the work does not consider the regular watermarking attacks and the number of its parameters is too much. E. Maiorana et al. [11] introduced a high-capacity and multi-bit inserting method that uses LogLuv domain as embedding domain. The algorithm applies a LogLUV transform to the HDR image and separates luminance components to carry watermark message. First level DWT is applied to obtain HL, LH, and HH sub-band, then each sub-band is converted to 7*7 or 11*11 blocks. Radon discrete cosine transform (RDCT) is applied on each block. Once the RDCT of a given block is evaluated, the coefficients of the block with high energy that indicate edges regions are selected for embedding purpose. The embedding strategy is based on Quantization Index Modulation (QIM). The suggested work have high capacity for embedding watermark bits; however, in this work, no experiment is done on regular watermarking attacks and only the tone-mapping attacks are investigated. Also, the BER results are not ideal and they are deniable as the numbers of embedded bits are high.

The algorithms in the second group use RGBE domain as embedding domain. F. Autrusseau et al. [12] proposed a nonlinear hybrid watermarking method which is a combination of both additive and multiplicative watermarking insertion methods. Images with RGBE format having four channels for each image including three color channels, Red (R), Green (G) and Blue (B), and an Exponent (E) channel. Embedding is taken place in R, G, and B channels while the E channel is left untouched to prevent visible distortion. First, a one-level wavelet transform decomposes the image into four sub-bands (LL, LH, HL, and HH), then the watermark is inserted in LH sub-band of each red, green and blue channels using the proposed hybrid method. Finally, by combining watermarked sub-bands with untouched remaining sub-bands using inverse wavelet transform, the watermarked version of HDR image is produced. The work does not evaluate the algorithm's robustness against regular watermarking attacks and the embedding capacity is not announced clearly. Also, the work does not compare the results with other methods due to the different techniques that are

used. The robustness investigated using correlation and the imperceptibility is reported based on HDRVDP.

In the third group, bilateral filter based methods are studied. The filter divides an image to a detail and a large scale part image. In the work proposed by E. Maiorana et al. [6], a blind multi-bit watermarking method for HDR images is presented. The embedding method considers human visual system properties to ensure imperceptibility. The binary marks are inserted into DWT coefficients of Just Noticeable Difference domain. Embedding locations are determined based on the bilateral filter to indicate the detail parts of the image; besides, the strength factor in each sub-band is calculated by a contrast sensitivity function that considers scale and orientation of each sub-band. X. Xue et al. in [13] proposed a watermarking method based on the bilateral filter in which the bilateral filter is applied to an HDR image to obtain large scale parts of the image. The detail image in log domain is produced by subtracting HDR image in the log domain and large scale parts in the log domain. The watermark is embedded using three-level wavelet in detail parts of the image in the log domain. Finally, by summing the watermarked detail part and the large scales part in the log domain and using exponential transform, the watermarked HDR image is produced. This work also does not evaluate regular watermarking attacks, but in the concept of imperceptibility and robustness is superior in comparison with other works presented before it. The work uses BER criteria to evaluate the robustness and HDRVDP to evaluate imperceptibility. The work does not compare results with previous works because of different techniques and metrics used in other works. Another bilateral filter based work for HDR images was proposed in [14]. The approach is designed to ensure imperceptibility and robustness against tone mapping operators. To meet these goals, the embedding domain has been chosen to be the wavelet transforms of the Just Noticeable Difference (JND) scale space of the original HDR image. A visual mask is also employed to consider aspects of Human Visual System (HVS); moreover, the bilateral filter is used to indicate the places of insertion in the detail part of the image. Contrast Sensitivity Function (CSF) is applied to modulate the intensity of watermark in each wavelet sub-band based on its orientation and scale. This work likewise other works in HDR image watermarking field ignores regular watermarking attacks. Furthermore, it studies only three images in which 128 bits are embedded and no more results are reported for a message with different length. The robustness results are evaluated using BER and the imperceptibility is measured using HDRVDP metric.

The fourth group contains the methods that use a tone mapping method to produce the LDR version of the image and insert watermark in the LDR image. J.L Wu et al. in [15], proposed a work in which a tone mapping operator is applied on the original HDR image to produce its LDR counterpart; then a ratio image is obtained by dividing the original HDR image to its LDR counterpart. Then, the LDR image is divided into 8*8 blocks and the watermark is inserted using Discrete Cosines Transform (DCT). Two of the middle-frequency DCT coefficients are manipulated to embed zero and one bits in the LDR image. Finally, by multiplying the ratio image into the LDR watermarked image, the HDR watermarked image is retrieved. This work uses an LDR image watermarking method and there is no idea related to HDR images' features. It investigates both tone-mapping attacks and some of the regular attacks for embedding 4800 bits in the images. No references are stated for the images and there is no comparison with other related works. The imperceptibility is evaluated using PSNR (Peak Signal to Noise Ratio) and robustness is evaluated using Correlation.

The last group contains the studies employ embedding watermark in the spatial domain. The works in this group usually have very high capacity because they use pixel presentation and bits arrangement to embed more than one bit in each pixel. For example, the presented method in [16] uses RGBE encoding and least significant bits (LSB) to embed watermark bits. The HDR image is divided into the boundary and flat areas based on the exponents of pixels and neighbors' pixels. The number of bits to insert in each pixel is selected adaptively based on local contrast. The method embeds more bits in dark regions than bright regions. The capacity has been measured for seven HDR images and the measurement showed the capacity of 10 bit per pixel (bpp). Li et al. [17] is the first work using LogLUV, TIFF, encoding for data hiding. The method does embedding by changing LSB mantissa of both luminance and chromatic channels; It embeds up to 6 bits of a secret message in the luminance component with floating points representation and 10 bits in each chromatic channel with integer representation. The visual quality of the images is measured by PSNR and HDRVDP metrics for tone mapped version of the images. The method is blind and does not need to cover the image for the extracting process. Another work with high capacity was proposed by Yu et al. in [18] which considers RGBE encoding; first, it examines every pixel based on the secret key and determines the embedding order. For an examined pixel such as K, the algorithm provides the corresponding homogeneous representation group (HRG_K) and calculates the homogeneity value (HV_K) of the HRG_K. Then, the pixel capacity is calculated, and if the homogeneity value (HV_K) is less than or equal to one, the pixel cannot be selected to carry any watermark bits; otherwise, C_K bits of the secret message are read. Afterwards, the current cover pixel status is calculated considering the secret message and the stego pixel status is determined. Finally, the pixel that embedding is going to take place in it is altered to become the stego pixel. The capacity of about 0.12bpp is estimated over five HDR images. The works introduced in this paper uses pixel presentation to embed as much as bits that is possible. In this paper, no comparison with other works is explored. The paper use correlation to prove imperceptibility of the watermarked image. The tone-mapping operators are considered to compare the cover image and watermarked image quality and there is no analysis on the watermarking robustness against such attacks. The work also does not evaluate regular watermarking attacks.

Table 1 provides a summary of related works in order to make comparison of the works easier.

One of the works done for the LDR images is the approach proposed by M. Ebrahimi Moghadam et al. [19]. This work is a blind method for color LDR images using evolutionary algorithms. It proposed a novel robust watermarking technique using Imperialist Competitive Algorithm (ICA) [20] in the spatial domain. The method embedded a watermark in blocks which are selected by modified ICA and customized the algorithm for watermarking. Watermark bits are inserted in the color bands based on their color dynamic range in each block. The paper use PSNR metric to prove its imperceptibility and MAE to show the quality of the extracted message. The watermark message is 64 × 64 bits and the cover images are 512 × 512 pixels. The presented results show acceptable result for both imperceptibility and robustness against regular watermarking attacks.

Some of the other works in LDR images domain are based on Visual Cryptography (VC) suggested in [21-24]. In these works, the watermark is never hidden in the cover image; instead, they are hidden in the owner share. So these works are imperceptible due to not changing the original cover image. These works are also robust against some attackers who aim to detect, distort and remove the watermark. The problem with most of VC algorithms is pixel expansion. In other words, the generated shares are larger than the original watermark; however, the works in [21-24] consider this problem and use different techniques for reducing the size of shares. The usual procedure in such algorithm is as follows: given a cover image and a secret key, a feature vector (using different techniques) is computed and a threshold technique is

Table 1
The summary of the work in the field of HDR image watermarking.

Related work	Embedding domain	Embedding method	Data set	Capacity	Visibility	Robustness	Disadvantage
[10]	LogLUV	QIM	15 images were used	Depends on the size of blocks	Considers HDR-VDP criteria	Considers 7 tonemapping attack	Does not consider regular watermarking attacks
[11]	LogLUV-RDCT	QIM	6 images were used	High capacity 3000–21,000 bits	Considers HDR-VDP criteria	Considers 6 tonemapping attacks	Does not consider regular watermarking attacks
[12]	RGBE-wavelet	Hybrid(linear and nonlinear)	12 images were used	Same size as the number of the coefficients of LH subband	Considers HDR-VDP criteria	Considers 8 tonemapping attacks	Does not consider regular watermarking attacks
[6]	Wavelet-JND	Multiplicative	15 images were used	Embedding 128, 256, 512 bits is considered	Considers HDR-VDP criteria	Considers 7 tonemapping attacks	Does not consider regular watermarking attacks
[13]	Wavelet	Multiplicative	6 images were used	Same size as the number of the coefficients of LH3 subband	Considers HDR-VDP criteria	Considers 4 tonemapping attacks	Does not consider regular watermarking attacks
[14]	Wavelet	Additive	6 images were used	Not mentioned	Considers HDR-VDP criteria	Considers 6 tonemapping attacks	Does not consider regular watermarking attacks
[15]	DCT	Any embedding method for LDR images	4 images were used	4800 bits	Considers PSNR criteria	Considers 4 tonemapping attacks	Embedding takes place in LDR version of the Image not the HDR one
[16]	RGBE	LSB	7 images were used	10 bits per pixel	Considers PSNR criteria	Considers tonemapping attacks	Does not consider regular watermarking attacks
[17]	LogLUV- TIFF format	LSB	10 images were used	26 bits per pixel	Considers PSNR and HDR-VDP criteria	Considers tonemapping attacks	Does not consider regular watermarking attacks
[18]	RGBE	Homogeneous representation group	5 images were used	0.12 bits per pixel	Considers correlation criteia	Considers tonemapping attacks	Does not consider regular watermarking attacks

considered to produce a secret binary matrix (called master key) from the feature vector. The bits of master key and a (2,2) VC code table are used together to generate owner share key. In the extraction procedure, a public share is generated from the watermarked image using a similar process like the hiding procedure and the secret key. Combining owner share and public share will reveal the watermark.

3. Proposed method

The proposed method uses ABC to find the best insertion positions for watermark bits. The algorithm considers a host image, for each of the blocks in which a watermark is going to be embedded, two different sub-bands including HL and LH is considered and the watermark message's bits are inserted in these sub-bands considering cost function.

At the end of embedding procedure, there is a watermarked image as the output. The following sections describe the algorithm steps in more detail.

3.1. Watermark embedding

LogLuv transform proposed by [9] is used as embedding domain. The LogLUV domain is selected because of the tone mapping attacks features and their effects on the HDR images. The attacks are a combination of linear and nonlinear operations, and they will affect the embedded watermark message substantially; in other words, these attacks go beyond the robustness limit of the watermarking systems, and it is almost impossible to make the watermark robust against such attacks without creating artifacts. One of the possible solutions is to embed the watermark in the tone mapped version of the image. However, the drawback of the solution is that the TMOs are not invertible and the watermarked HDR image will never be available again. To fix the non-invertible problem, the LogLUV domain suggested in [9] is used. Since the LogLUV domain is a format of the HDR image where its inverse form exists, the LogLUV format is the best embedding domain to reproduce the situation in which the watermark message will encounter the tone mapping attacks. TMOs manipulate the luminance component of HDR Images in the same way as RGB-to-LogLUV transform manipulates it. In other words, the RGB-to-LogLUV transform can be considered as a pseudo-TMO because both of them manipulate the log luminance component [25].

For embedding purpose, the proposed method investigates a host image. To in order to make a decision about which sub-band to be used as embedding sub-band for each block. It is necessary to apply RGB-to-LogLUV [9] transform to the original image in order to gain log luminance image of the host image. Afterwards, one level wavelet transform is employed to acquire LH sub-band and HL sub-band as insertion domains. When the ABC procedure is completed, the best solution that is a one-dimensional array of best positions to insert watermark message is selected to insert the watermark message in the image. Now by considering the solution found by ABC we can test both LH and HL sub-bands separately to decide which one is better to insert watermark bit considering the cost function, a 2×2 block is created around each pixel of the solution in both LH and HL sub-bands separately while the first pixel of the block is the selected pixel. After embedding, to achieve the watermarked HDR image, the inverse wavelet transforms and LogLUV-to-RGB [9] transforms are applied. Finally, the watermarked version of the HDR image is ready.

Steps of the embedding procedure with more details are as follows:

1) The original HDR image is read as input to the proposed embedding algorithm.
2) The watermark message is also read as another input of the proposed embedding algorithm and considered in vector form as shown in Eq. (1) if it is not already a vector where w_x and w_y are indicators of length and width of the watermark message, respectively:

$$Wmessage = \left[w_1, w_2, \ldots, w_k, \ldots, w_{w_x \times w_y} \right] \quad (1)$$

where $1 \leq k \leq w_x \times w_y$

3) RGB-to-LogLUV transform is applied to the HDR image in order to obtain the LogL images.

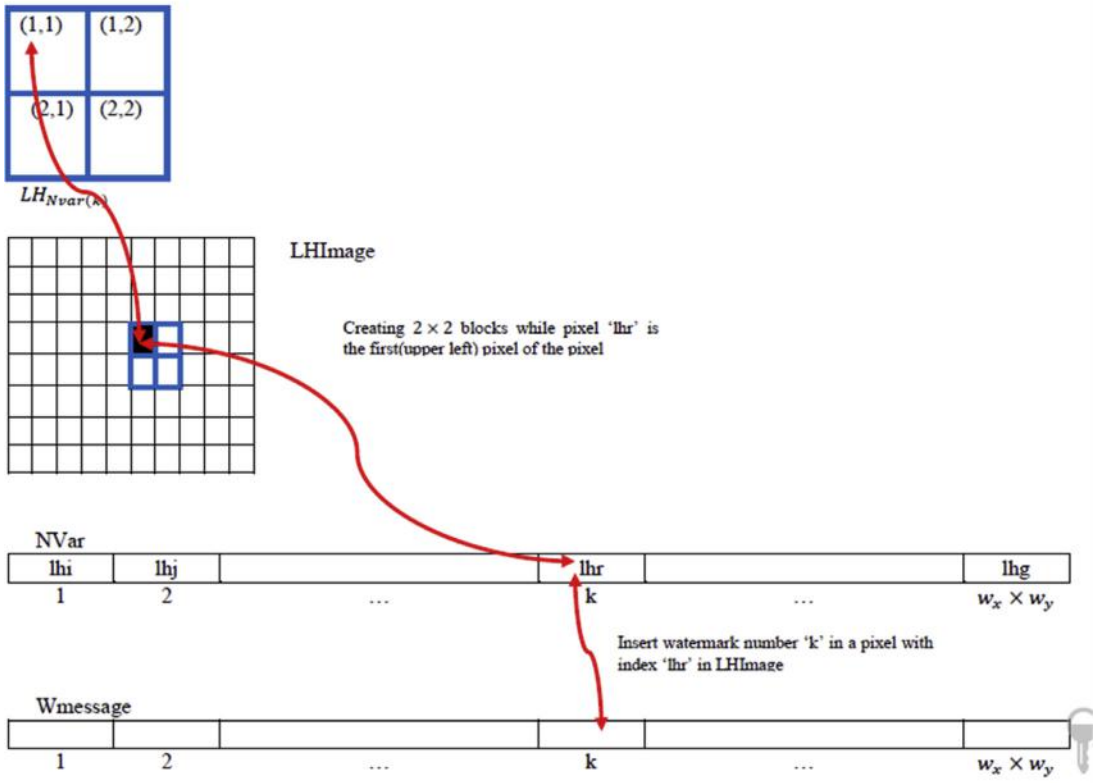

Fig. 1. Embedding formula illustration.

4) DWT is applied to the LogL version of the images and LH sub-band and HL sub-band are extracted as the embedding domains. LH and HL were selected because LL and HH sub-bands, cannot be very robust against high-pass and low-pass filters respectively. Embedding watermark bits in LL sub-bands is very visible; embedding in HH is more imperceptible but still less robust against attacks with low-pass filters effects. Therefore, to have a trade-off between imperceptibility and robustness LH or HL sub-bands have to be considered. Eq. (2) is defining the host image and variables such as x and y are the width and length of the host image. Eq. (3) is the LH sub-band of image and Eq. (4) presents the HL sub-band of the image.

$$Image = \left[h_{11}, h_{12}, \ldots, h_{ij}, \ldots h_{xy}\right] \quad (2)$$

where $1 \le i \le x$ *and* $1 \le j \le y$

$$LHImage = \left[lh_{11}, lh_{12}, \ldots, lh_{ij}, \ldots, lh_{x/2\,y/2}\right] \quad (3)$$

where $1 \le i \le x/2$ *and* $1 \le j \le y/2$

$$HLImage = \left[hl_{11}, hl_{12}, \ldots, hl_{ij}, \ldots, hl_{(x/2)(y/2)}\right] \quad (4)$$

where $1 \le i \le x/2$ *and* $1 \le j \le y/2$

5) ABC Algorithm is applied to find the best locations to insert watermark message bits. Inputs of this algorithm are the original HDR Image and Wmessage vector and the output of the algorithm contains information about the location in which the watermark message is going to be embedded and their corresponding sub-band. The comprehensive procedure is explained in the next sub-section (B).
6) The best solution found by ABC is selected and a 2×2 block is created around each pixel of the solution in LH or HL sub-band of the image considering the key.
7) Watermark bits are inserted in the first (upper left) pixel of the 2×2 blocks using Eq. (5) or (6). In this equation, k is a number between 1 and $w_x \times w_y$ that indicates watermark bit number that is going to be embedded in the block. For each embedding bit a 2×2 block in LH (or HL) sub-band around the pixel with index Nvar(k) is needed. This pixel is called $LH_{Nvar(k)}$ or $(HL_{Nvar(k)})$. Nvar is a one dimensional array with $w_x \times w_y$ elements that each element determines the indices of selected locations by ABC algorithm to embed k^{th} watermark bit. The k^{th} watermark bit is embedded in either LH using Eq. (5) or HL sub-band using Eq. (6) based on the information provided by the key obtained from ABC algorithm.

$$LH_{Nvar(k)}(1,1) = LH_{Nvar(k)}(1,1) + \propto \times \left(Max\left(LH_{Nvar(k)}(:)\right) - Min\left(LH_{Nvar(k)}(:)\right)\right) \quad (5)$$

where $length(Nvar) = w_x \times w_y$ *and* $1 \le Nvar(k) \le x/2 \times y/2$ *and* $1 \le k \le w_x \times w_y$

$$HL_{Nvar(k)}(1,1) = HL_{Nvar(k)}(1,1) + \propto \times \left(Max\left(HL_{Nvar(k)}(:)\right) - Min\left(HL_{Nvar(k)}(:)\right)\right) \quad (6)$$

where $length(Nvar) = w_x \times w_y$ *and* $1 \le Nvar(k) \le x/2 \times y/2$ *and* $1 \le k \le w_x \times w_y$

As it is obvious from the Eqs. (5) and (6), the watermark bits are inserted in the first pixel of the block (left upper pixel determined by (1,1)). After determining maximum and minimum pixels in the 2×2 block, maximum and minimum pixels have to be subtracted and multiplied by α in order to create an adaptive strength factor (α values is considered 2 in the experiments) . Fig. 1 illustrates the embedding of watermark bits in LH Image in which the k^{th} bits of the watermark is inserted in a location ('lhr' in the example image) indicated with Nvar[k]. The same process in Fig. 1 happens for HLImage as well.

8) The inverse wavelet transform is applied.
9) LogLUV-to-RGB transform is applied to obtain the watermarked version of the HDR host image.

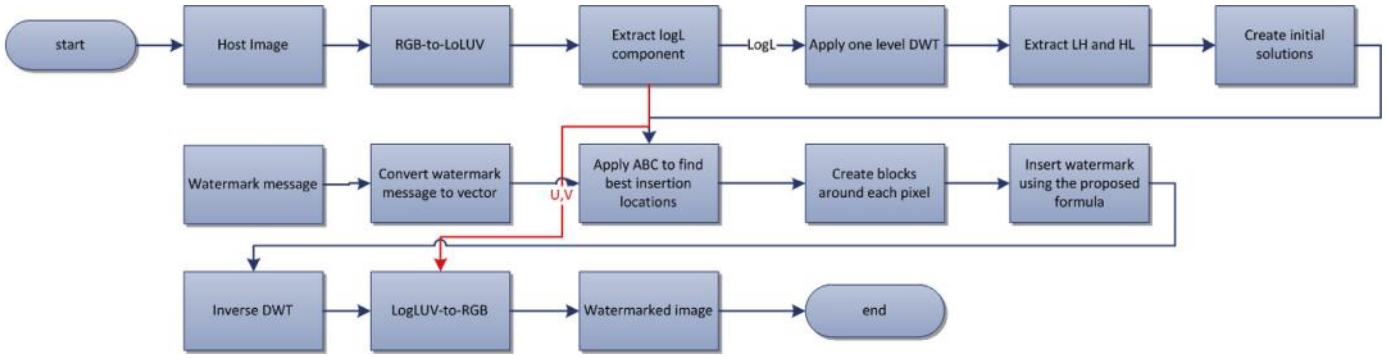

Fig. 2. Flowchart of embedding process.

The flowchart of embedding process is shown in Fig. 2.

3.2. ABC algorithm used for embedding watermark

The base idea of ABC algorithm that is used to implement the proposed algorithm is inferred from [26], however, some changes have been applied. These changes include using different cost function and adding extra steps to the ABC procedure in order to make it appropriate for manipulating pixels of an image. Details about regular ABC algorithm is described in the appendices part (Section VII). Flowchart of the modified ABC algorithm is drawn in Fig. 3 and definition of each step is explained completely as below.

The steps of the modified ABC in detail are as follows:

- Step1: Initialize the population of solutions

In this step, the solutions which show candidate places to embed watermark bits are created. To create initial solutions, some random vectors are created randomly. Each element of these solutions has to be an integer in the range of pixels of the input image. The initial number of the population size is SN and the number of bees is 2SN. It means for each food source, two bees are required, one employed bee and one onlooker bee. In this algorithm, the value of SN is chosen to be 30. The length of the solutions is the same as watermark message length, and each element of the solutions is a pixel location in the range of LH or HL wavelet domain of the LogL image ($\frac{x}{2} \times \frac{y}{2}$). In Eq. (7), FoodSource is an indicator of a solution which is a $1 \times w_x \times w_y$ array and the p variable shows the location of LogL image pixels in LH or HL sub-bands. The algorithm considers a binary vector called Information to indicate which ones of the watermark bits are embedded in LH and which ones are embedded in HL. If the value of a cell of the array is one it means the corresponding watermark message have to be embedded in HL sub-band; however, a value of zero means the corresponding watermark message have to be embedded in LH subband. In the Initialization process all the elements of the Information vector are initialized one or zero depending on the original image major direction (whether the lines are vertical or horizontal) if the image has more horizontal features the LH sub-band is considered as the initial values of the vector, otherwise the HL sub-band is considered as the initial values of the vector. The major direction of the image was calculated using Hough transform and considering the peaks. The initial solutions are embedded in the initial sub-bands. The contents of the Information vector can change in future steps based on the cost function.

$$FoodSource(NN) = [p\_1, p\_2, \ldots, p\_L, \ldots, p\_w_x \times w_y] \tag{7}$$

where $1 \le L \le w_x \times w_y$ *and* $1 \le p \le \frac{x}{2} \times \frac{y}{2}$ *and* $1 \le NN \le SN$

- Step2: Evaluate the population

For each solution, its cost has to be computed. The cost is calculated considering both of the LH and HL sub-bands. Since preserving the imperceptibility and quality of the watermarked image is the goal of the proposed algorithm, the HDR-VDP metric is an acceptable criterion to show the quality (details about this metric is presented in section VI (Experimental results), part A.1). The cost function is defined as the maximum probability for a person of detecting differences in at least 5% of the marked images, which is calculated as follow. The metric is defined as Eq. (8) in which 'I' is the original image and 'W_s' is the watermarked version of the original HDR image using solution 's' as embedding positions. Pixel_per_degree is visual resolution of the image and color_encoding is color representation for the input image, SN is the number of solutions and is equal to 30. By considering the Eq. (9), it can be concluded that by reducing the cost function, the result of the imperceptibility of the watermarked image will increase. **Prctile is** a MATLAB function that is defined as follow.

"$\underline{Y} = prctile(\underline{X,p})$ returns percentiles of the values in a data vector or matrix X for the percentages p in the interval [0,100]."

$$\text{METRIC}(W_s) = \text{hdrvdp}(W_s, \text{I}, \text{color\_encoding}, \text{pixels\_per\_degree}) \quad 1 \le s \le SN \tag{8}$$

$$Cost(W_s) = \text{Perceptibility}_{95} = \text{prctile}\left(\text{METRIC}(W_s).\text{P}_{\text{map}(:)}, 95\right); \quad 1 \le s \le SN \tag{9}$$

The cost function should be computed for all solutions. The solution 'f' is better than 'g' if the condition in Eq. (10) is met. The fitness function is the inverse of the cost function. It means when reducing the cost function, the fitness function increases.

$$cost\left(W_f\right) < cost\left(W_g\right) \tag{10}$$

where $1 \le f \le SN$ *and* $1 \le g \le SN$ *and* $f < > g$

- Step 3: cycle = 1

The cycle is initialized to 1. The cycle is a parameter that shows the number of cycles required for ABC algorithm to be iterated and produces reasonable answers.

- Step 4: start of the loop
- Step5: Producing New Solution for the Employed bee

For producing new solutions from previous ones, Eq. (11) is suggested. In this equation, 'X' is the selected food source or solution array and 'k' and 'j' are indices that selected randomly. Although the value of 'k' is selected randomly, it should not be equal to the value of 'i' . φ_{ij} is a random number between $[-1, 1]$ and its application is controlling the production of solutions in the neighborhood of x_{ij}. φ_{ij} is simulating the process of comparing two food

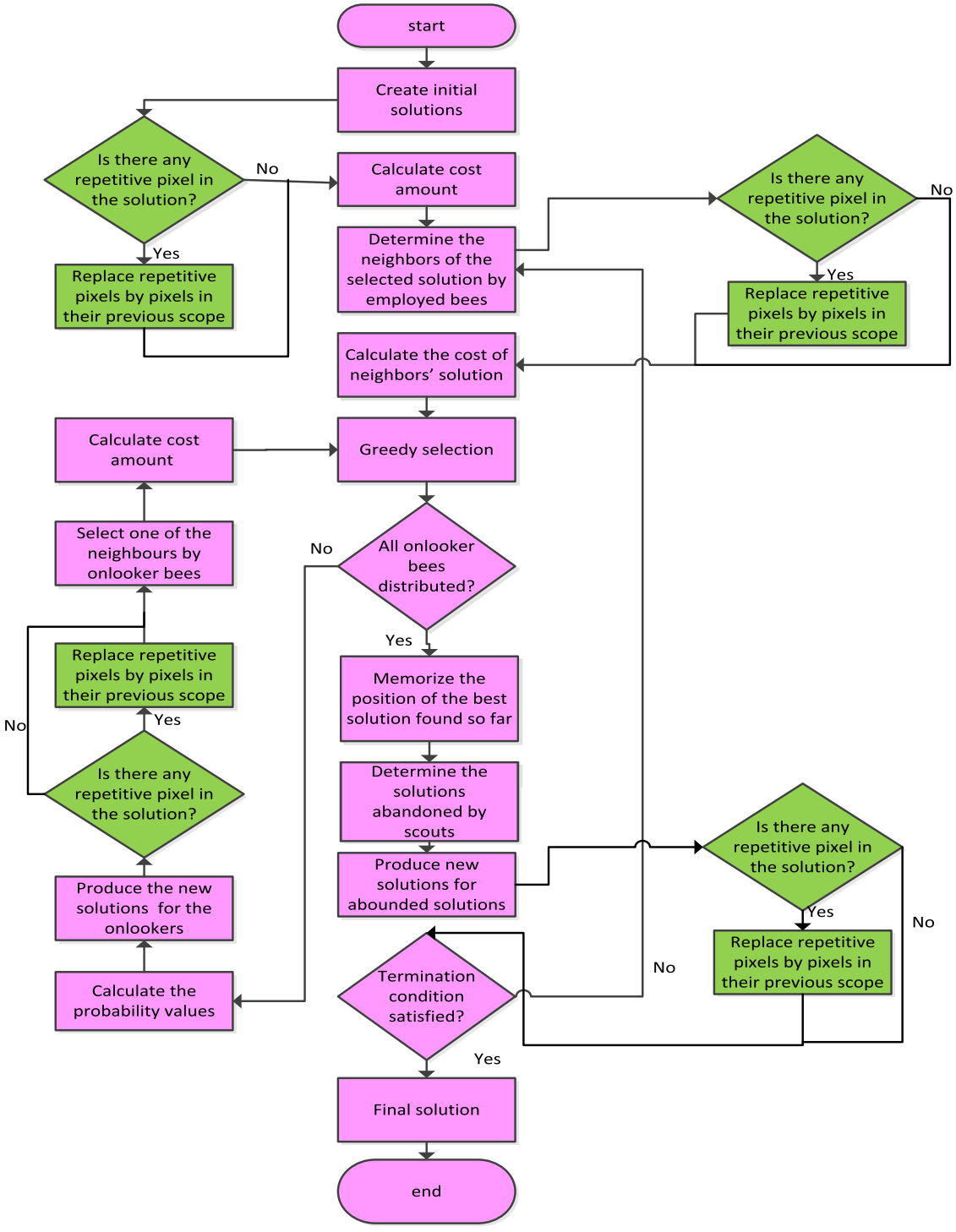

Fig. 3. Flowchart of the modified Artificial Bee Colony.

sources that are visible to a bee. SN is the size of the population or the number of food sources. The new position is evaluated in both the LH and HL sub-bands and the better result is selected and information vector is updated based on the selected sub-band.

$$X_{ij} = X_{ij} + \phi_{ij}\left(X_{ij} - X_{kj}\right) \tag{11}$$

where $i, k \in \{1, 2, \ldots, SN\}$ *and* $j \in (1, 2, \ldots, w_x \times w_y)$

- Step 6: Apply selection process

In ABC to show greedy selection, the employed bees compare the fitness function of the old solutions and the new ones. Then, it selects the solution with higher fitness. Fitness is the inverse of the Cost function that was defined beforehand in step 2.

- Step 7: Calculate the probability values P_i for the solutions x_{ij}

An onlooker bee chooses a solution based on the probability values associated with that solution (P_i) which is calculated by Eq. (12).

$$P_i = \left(\frac{0.9 \times fit_i}{\max\limits_{n=1} N(fit_n)}\right) + 0.1 \tag{12}$$

where fit_i is the fitness function of the i-th solution that was evaluated by the employed bee. This evaluated value is the inverse of 'cost' value which is an indicator of nectar amount of food source in the ABC algorithm. Eq. (13) shows the relation between the fitness function and the cost function. fit_i is the fitness function of the solution i and $cost_i$ is its cost function.

$$fit_i = \frac{1}{cost_i} \quad cost_i \geq 0 \qquad 1 \leq i \leq SN \tag{13}$$

- Step 8: Produce the new solutions u_{ij} for the onlookers from the solutions x_{ij} selected depending on P_i and evaluate them

This Step is same as step 5 with a little bit difference. The difference is that in step 5 all the solutions have an equal chance to be tested; however, here, the solutions with larger fitness have a higher probability and greater chance to be selected by onlooker bees. The probability is computed using Eq. (12).

- Step 9: Apply selection process

This step is same as the step 6. The onlooker bees do a greedy selection to choose their preference solution considering the probability of each solution.

- Step10: Determine the abandoned solution for the scout, if exists, and replace it with a new randomly produced solution

In ABC, if a solution cannot be improved further through a predefined number of cycles, then that solution can be supposed to be left. The predetermined number of cycles is a control parameter and it is called limit; the number of cycles is considered as 5 in the proposed algorithm. In Eq. (14), assuming that the abandoned solution is X_i^j, scouts bee will produce a new solution to be substituted with it. X_{max}^j is the maximum range of image pixels and X_{min}^j is the minimum range of the image pixels. SN is the number of solutions.

$$X_i^j = X_{min}^j + rand[0, 1]\left(X_{max}^j - X_{min}^j\right) \tag{14}$$

where $j \in (1, 2, \ldots, SN)$

- Step11: Memorize the best solution achieved so far.

The best solution found so far has to be saved. For this purpose, a variable is considered called GlobalMins which saves the index of the best solution found so far. The Eq. (15) compares the best solution between the two best solutions found in LH and HL sub-bands. And save the result in GlobalMins parameter.

$$GlobalMins = min\left(cost\left(W_{best_{LH}}\right), cost\left(W_{best_{HL}}\right)\right) \tag{15}$$

- Step12: cycle = cycle + 1

One unit is added to the number of cycles.

- Step13: until cycle = MCN

MCN is a predefined value for the number of cycles. The value of MCN is estimated through empirical experiments and its value is considered as 50 in this paper

- Step 14: create key

To make extraction process possible, what is required is a key that maintains the index of each pixel in either of LH or HL sub-band that holds a watermark bit. To satisfy this requirement, the final amount of GlobalMins is saved as Key. GlobalMins contains the index of the best solution found by ABC algorithm. The information regarding the sub-band in which insertion takes place is also added to the key as a new bit in which if the bit value is 0 it means insertion has taken place in LH sub-band and if the value is 1 it means the insertion has taken place in the HL sub-band. These information comes from Information vector corresponding to the considered solution.

- Extra Step: Find repetition

This step should be performed after steps 2, 5, 8 and 10. Because this is probable that during the watermarking process with each modification in the solutions, some similar locations are selected. For watermark insertion, the bits should not be embedded in repetitive locations because the information of the previous bit will be destroyed and consequently BER will be increased. To avoid such consequences, the extra step proposes a function to find same locations and replace them with a randomly selected location in their previous scope. This scope is a neighborhood in radius 10 of the selected location.

3.3. Extracting procedure

For the extracting procedure, some preprocessing same as what has been done in the embedding procedure has to be done again to acquire the image in the wavelet space of LogLUV domain. Then, extracting is performed on the LogL image in LH and HL sub-bands. Furthermore, by using the key created in the step 14th of the previous section, the exact place of the blocks in which watermark bits are hidden and their corresponding sub-band are revealed. To extract the watermark, the first pixel of the block is selected and compared to the mean value of the block. If the first pixel of the block is greater than the mean value of that block, the hidden message is one otherwise is zero. The flowchart of the extracting process is shown in Fig. 4.

The main steps of the extracting procedure are listed as follows:

1. Applying RGB-to-LogLUV transform, in order to gain log-luminance part of the image.
2. Extracting log-luminance part.
3. Applying wavelet transform and extracting LH and HL sub-bands.
4. Finding the pixel in which embedding has occurred based on the key and finding the sub-band in which the embedding has taken place based on the key and creating 2×2 blocks around each pixel in the way that the first pixel of the block is the considered pixel.
5. If the embedding of the considered bit has happened in LH domain, in another word the key has value of zero then Extract watermark from LH sub-band by using the following formula.
   if $LH(1, 1) > mean(LH(:))$.
   the hidden watermark is one
   else if $LH(1, 1) < mean(LH(:))$
   the hidden watermark is zero
6. If the embedding of the considered bit has happened in HL domain, in another word the key has value of one then Extract watermark from HL sub-band by using the following formula.
   if $HL(1, 1) > \text{mean}(HL(:))$.
   the hidden watermark is one
   else if $HL(1, 1) < mean(HL(:))$
   the hidden watermark is zero
7. Thus, the proposed algorithm has been successful to extract the embedded watermark without using the original HDR image.

To display the original HDR image and its watermarked version, Photosphere application [27] is used and the result for the Memorial image is shown in Fig. 5. The left picture is the original picture and the right one is the watermarked version of it in which a 512-bit message has been embedded.

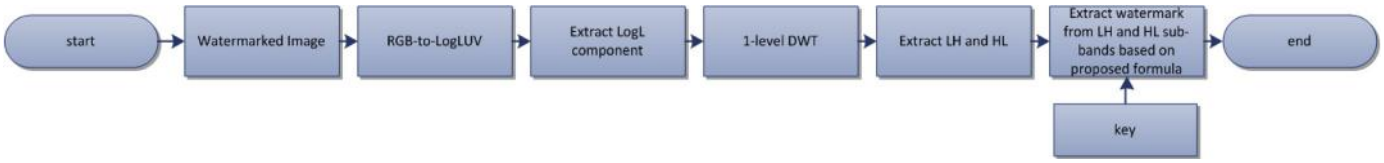

Fig. 4. Flowchart of extracting process.

Fig. 5. Original image vs. watermarked version using ABC algorithm.

4. Experimental results

For evaluating the proposed method and comparing its performance against the work presented in [6], 12 HDR images displayed in Fig. 6 are investigated. These images are converted to LDR ones using Photospher software [27] to be able to show them by regular displays or print by a regular printer. The images information such as dynamic range, size, and reference is listed in Table 2. The images have different size, amount of texture and dynamic range which prepare complete circumstances to evaluate the proposed watermarking method. The proposed approach is compared with the work suggested in [6] with the same images and TMOs with same references and implementations. The TMOs reference and implementation are listed in Table 3.

Table 2
Main properties of the high dynamic range images employed for the performed experimental tests.

Image_Name	Image_ID	Dynamic range	Size	Reference
AtriumMorning	1	1.99×2^{14}	1016×760	[28]
AtriumNight	2	1.62×2^{28}	1016×760	[28]
mpiAtrium	3	1.48×2^{14}	676×1024	[28]
NancyCathedral1	4	1.60×2^{14}	2048×1536	[28]
NancyCathedral2	5	1.94×2^{14}	2048×1536	[29]
Nave	6	1.64×2^{23}	480×720	[29]
Memorial	7	1.29×2^{18}	768×512	[29]
Rosette	8	1.83×2^{17}	480×720	[29]
Snow	9	1.02×2^{10}	1536×2048	[28]
Rend07	10	1.41×2^{28}	575×575	[29]
Rend10	11	1.20×2^{26}	1024×1024	[29]
Iwate	12	1.08×2^{19}	1396×3720	[28]

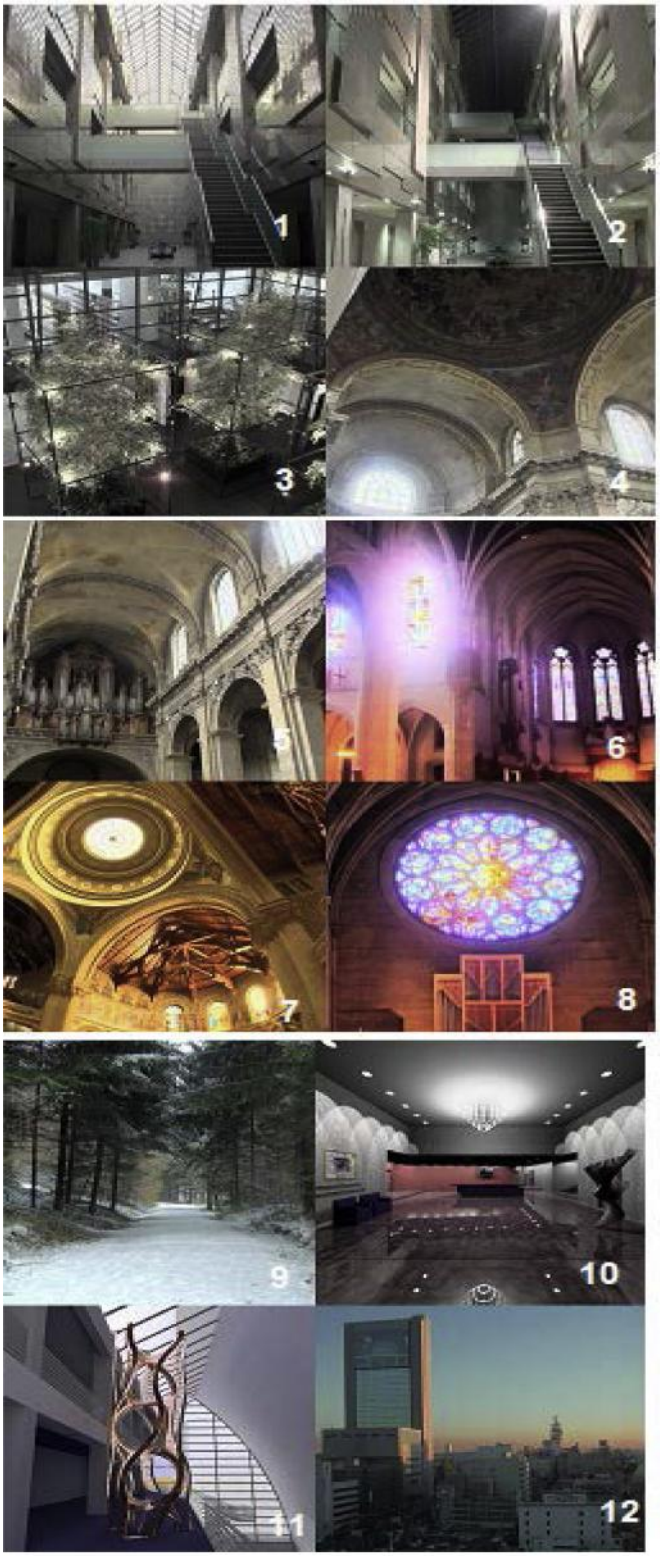

Fig. 6. The HDR images used in the experiments rendered by Photosphere.

4.1. Imperceptibility evaluation

4.1.1. HDRVDP2

To assess imperceptibility, the HDRVDP metric (version 2.2.1) [7] has been used in the experiments. This metric provides information for each modified pixel about the probability of being detected; it is a demonstrator of the probability of detecting a pixel as different for an average observer. The source code of this metric is available in [38].

Table 3
TMOs used in the performed experiments.

Tonemap_Attack	Reference	Implementation
Tonemap	[30]	[30]
iCam06	[31]	[31]
Drago	[32]	[33]
Reinhard	[34]	[33]
Tumblin	[35]	[33]
Chiu	[36]	[33]
Durand	[37]	[33]

Table 4
Imperceptibility performance of the proposed approach for high dynamic range image watermarking, the results are the maximum probability for a person of detecting differences in at least 5% of the marked images.

Image ID	512_5%	256_5%	128_5%	Other_5%
P1	3.82e-07	4.46e-08	3.82e-10	3.80e-03
P2	8.82e-08	2.42e-08	3.27e-07	3.00e-03
P3	1.39e-07	2.67e-08	3.2e-07	6.00e-03
P4	7.51e-10	2.26e-09	9.75e-07	3.30e-03
P5	5.73e-09	2.95e-06	9.35e-06	4.50e-03
P6	2.39e-09	6.33e-09	6.16e-09	7.00e-04
P7	8.95e-10	8.45e-09	6.16e-09	7.00e-04
P8	5.2e-08	6.82e-10	5.81e-10	8.00e-04
P9	4.67e-08	2.06e-08	1.57e-08	1.12e-02
P10	1.48e-07	8.26e-07	1.42e-06	7.00e-04
P11	8.78e-11	8.01e-11	7.97e-11	2.00e-04
P12	6.03e-06	1.65e-06	3.09e-05	3.80e-03

Table 5
Imperceptibility performance of the proposed approach for high dynamic range image watermarking, the results are the maximum probability for a person of detecting differences in at least 1% of the marked images.

Image ID	512_1%	256_1%	128_1%	Other_1%
P1	1.61e-05	3.28e-06	1.50e-08	1.06e-02
P2	1.22e-06	8.94e-08	7.45e-07	7.90e-03
P3	3.51e-06	1.14e-07	1.06e-06	1.54e-02
P4	2.78e-09	7.18e-09	3.01e-06	8.10e-03
P5	3.51e-08	1.75e-05	5.56e-05	1.16e-02
P6	8.45e-09	2.24e-08	2.17e-08	2.10e-03
P7	2.92e-08	6.47e-08	2.17e-08	2.10e-03
P8	8.04e-06	1.07e-07	2.72e-09	2.50e-03
P9	1.34e-06	9.29e-08	4.67e-08	2.60e-02
P10	2.2e-06	5.75e-06	9.77e-06	1.80e-03
P11	2.34e-10	2.04e-10	2.02e-10	6.00e-04
P12	1.34e-05	4.7e-06	8.69e-05	1.94e-02

Tables 4 and 5 report the obtained results regarding the imperceptibility of the embedded messages, in terms of the maximum probability for a person of detecting differences in at least 5% and 1% of the marked images respectively. As it can be seen from the results, the proposed method indicates better imperceptibility in all of the images and embedding circumstances. The overall average considering 5% of the marked images, in the case of embedding 512 bits, for the proposed approach is 5.75E-07 and for the other work is equal to 3.22E-03, in the case of embedding 256 bits, for the proposed approach is 4.63E-07 and for the other work is equal to 3.22E-03and in the case of embedding 128 bits, for the proposed approach is 3.61E-06 and for the other work is equal to 3.22E-03. The overall average considering 1% of the marked images in the case of embedding 512 bits, for the proposed approach is 3.82E-06 and for the other work is equal to 9.01E-03, in the case of embedding 256 bits, for the proposed approach is 2.64E-06 and for the other work is equal to 9.01E-03 in the case of embed-

Fig. 7. Results of embedding 64 × 64 watermark message in the Memorial Image.

ding 128 bits, for the proposed approach is 1.31E-05 and for the other work is equal to 9.01E-03. Because, the other work claims that its results are independent to the message length, therefore it has only one column each result table. However, the other work instead of depending on message length depends on attributes of the considered image such as smoothness. As a matter of fact, distinguishing modification is easier in images containing smooth and bright regions. Because in such images embedded messages may appear as noise. The proposed work performance depends on smoothness and brightness as well. This means the proposed work

Fig. 8. Presentation of image P12 through different tiles, obtained by means of the considered tone-mapping operators.

Table 6
MATLAB functions for regular image processing attacks.

Attacks	MATLAB_Function
Noise (0.01)	Noise1 = imnoise(Image,'speckle',0.01) ;
Noise (0.05)	Noise2 = imnoise(Image,'speckle',0.05) ;
Blur (once)	H = fspecial('disk',0.1)Blur1 = imfilter(Image,H,'replicate') ;
Blur (twice)	H = fspecial('disk',0.1)Blur2 = imfilter(Blur1,H,'replicate') ;
UnSharp (once)	H = fspecial('unsharp')Unsharp1 = imfilter(Image,H,'replicate')
UnSharp (twice)	H = fspecial('unsharp')Unsharp2 = imfilter(Unsharp1,H,'replicate')
Cropping (100*100)	Cropping attack created by cropping a 100*100 square in position (100, 100) of the watermarked image
Gaussian_Blur (r = 0.8)	H = fspecial('gaussian'[5,5],0.4)Blured = imfilter(Image,H,'replicate')

performance in images such as p12, p5, p10 is a little worse than other images with less smooth area. However, considering the result the proposed work has had more successful results regarding imperceptibility measuring with HDRVDP criterion.

4.2. Robustness evaluation

When a method is called robust, it has to resist predefined transformations (attacks). To prove the robustness of the proposed method, the Bit Error Rate metric is selected. This metric gives information about the percentage of bits that is detected differently from the original signature (watermark message). Eq. (16) expresses the BER relationship where S_t is the original signature and $\overline{S_t}$ is the extracted signature.

$$BER = \frac{1}{m}\sum_{t=0}^{m-1}\left|S_t - \overline{S_t}\right| \tag{16}$$

Fig. 7 presents the results of embedding a 64 × 64 watermark message in the Memorial Image. The first row of the figure shows the original image on the left and the watermarked one on the right side. These images are created using MATLAB software and Reinhard Tone-mapping attack. In the second row, parts of the first row's images are zoomed and finally, in the third row, the extracted watermark message in original size and zoomed version is displayed. Extracted watermark message's BER is equal to 2.78% and imperceptibility considering HDRVDP2 criterion is equal to HDRVDP(1%) = 5.22e-04 and HDRVDP(5%) = 4.25e-06.

4.2.1. Tone mapping attacks

There are several TMOs attacks that their function is limiting the dynamic range of HDR images, therefore, common displays are able to display them. In this paper, the effect of the same TMOs as the ones used in [6] has been studied. To illustrate the effect of each of TMOs, Fig. 8 is brought which shows the effect of each of the tone-mapping operators on the 'Iwate' (the image with ID 12) as tiles. From up to down the results refer to 'tonemap',' iCam06',' Drago',' Reinhad',' Tumblin',' Chiu' and ' Durand' attacks. In following sub-sections, the process of evaluation is explained. The results of the robustness experiment against TMOs for the proposed approach and the other related works are reported in Table 7 which shows the robustness for embedding 128, 256 and 512 bits watermark message in each image the indices 1 and 2 next to the name of each tone-mapping attacks demonstrate result of the proposed work and the other work respectively [6].

As this is obvious from the obtained results, the proposed method does not work properly in the case of Matlab tone map and iCAM06 attacks. The reason is that such TMOs try to leave the fine detail of an HDR image untouched while reducing their dynamic range. Therefore, the proposed work that selects the pixels randomly cannot demonstrate its ideal performance while the works such as the algorithm in [6] can perform stronger against such attacks since they are based on bilateral filter and embeds watermark bts in details part of the image [6].

As the length of watermark sequence is increasing, the BER performance of the proposed work improves while the other work is getting worse because the capacity of details parts of image for keeping watermarks bits in them reducee by increasing the number of watermark bits, in contrast, the proposed work's embedding strategy is not limited to a certain part of image and increasing the number of watermark bits is not a matter of being worry. As it can be seen, in the condition that 512-bit watermark is inserted, the proposed method works better. To prepare a condition to compare

Table 7
Measuring robustness for images against different tone mapping attack using BER, the results are in (%).

Attacks	M	Durand1	Durand2	Chiu1	Chiu2	Tumblin1	Tumblin2	Reinhard1	Reinhard2	Drago1	Drago2	ICAM1	ICAM2	Tone1	Tone2	HDR1	HDR2
12	128	**0.26**	10.79	**0.52**	5.71	**0**	1.13	**0.26**	2.32	**0**	7.99	2.34	**0.02**	8.59	**5.46**	**0**	3.82
	256	**0.26**	18.54	**0**	12.92	**0**	5.08	**0**	7.52	**0**	15.95	1.69	**0.63**	**5.99**	12.58	**0**	10.05
	512	**0.26**	26.09	**0.13**	20.88	**0**	11.7	**0**	15.49	**0**	23.14	**0.52**	3.71	**4.23**	20.45	**0**	18.02
11	128	14.06	**1.18**	17.03	**0.13**	37.66	**1.63**	13.44	**1.85**	14.22	**3.75**	21.88	**0.12**	32.81	**0.15**	13.59	**6.69**
	256	11.48	**4.85**	13.83	**1.71**	40	**5.74**	10.62	**6.62**	11.48	**9.78**	20.62	**1.78**	31.95	**2.2**	**10.55**	13.47
	512	**10.51**	11.52	14.06	**6.54**	36.37	**12.78**	**9.92**	14.05	**10.51**	17.63	20.51	**6.46**	32.15	**7.6**	**8.75**	21.8
10	128	4.22	**0.21**	10.78	**2.25**	5.31	**3.96**	3.28	**0.25**	**3.28**	8.27	8.13	**0**	18.44	**0.06**	**3.59**	16.32
	256	3.28	**2.29**	11.48	**7.81**	**4.45**	10.05	2.81	**2.61**	**2.5**	15.49	7.89	**0.17**	17.27	**0.83**	**3.05**	22.65
	512	**3.01**	7.56	**10.98**	15.4	**5.08**	17.16	**2.89**	8.14	**2.7**	21.92	7.66	**1.9**	17.27	**4.46**	**2.34**	27.48
9	128	**0.52**	8.05	**1.3**	7.57	**0.52**	9.84	**0.52**	4.7	**0.52**	7.93	1.3	**0.55**	3.12	**2.75**	**0.52**	2.41
	256	**0.26**	16.17	**0.26**	15.21	**0**	17.62	**0.13**	11.86	**0.13**	15.45	**0.78**	3.15	**2.47**	8.66	**0**	8.19
	512	**0.065**	24.04	**0.13**	23.7	**0**	25.76	**0**	20.26	**0**	23.79	**0.98**	9.63	**1.63**	16.91	**0**	16.49
8	128	0.78	**0**	4.37	**0**	**0.94**	0.48	0.47	**0**	**0.47**	4.27	9.06	**4.79**	6.72	**0**	**0.31**	23.16
	256	0.7	**0.02**	3.52	**0.03**	**0.23**	2.84	0.55	**0.02**	**0.16**	11.52	**9.22**	12.85	5.39	**0.02**	**0.078**	30.94
	512	0.66	**0.51**	3.52	**0.6**	**0.66**	8.96	1.02	**0.36**	**0.51**	19.97	**8.59**	21.53	4.73	**0.34**	**0.43**	36.47
7	128	2.97	**0**	1.25	**0**	1.41	**0.04**	0.16	**0**	**0.16**	0.2	5.63	**0.22**	4.37	**0**	**0**	4.02
	256	0.078	**0**	**0.86**	1.95	0.16	**0**	**0**	0	**0**	0	**3.91**	5.08	**2.5**	4.69	**0**	0
	512	**0.47**	0.65	1.25	**0.91**	**0.55**	3.47	**0.39**	1.04	**0.39**	6.9	**3.36**	6.68	1.8	**0.27**	**0.35**	17.79
6	128	2.97	**0**	1.25	**0**	1.41	**0.04**	**0**	0	**0**	0.2	5.63	**0.22**	4.37	**0**	**0**	4.02
	256	1.97	**0.02**	1.41	**0.08**	1.8	**0.74**	0.078	**0.03**	**0**	1.89	4.69	**1.95**	5.63	**0**	**0**	10.03
	512	1.99	**0.65**	2.27	**0.91**	**2.03**	3.47	**0.55**	1.04	**0.63**	6.9	**5.39**	6.68	5.55	**0.27**	**0.55**	17.79
5	128	**0**	0.66	**0.16**	1.1	**0.31**	0.9	**0**	0.71	0	**0.28**	2.81	**0.41**	5.63	**0.47**	**0**	2.17
	256	**0.55**	3.91	**1.02**	4.6	**0.63**	4.69	**0.23**	4.08	**0.16**	2.65	3.91	**3.46**	5.55	**3.66**	**0.078**	7.82
	512	**0.35**	10.39	**0.51**	11.49	**0.35**	12.03	**0.12**	10.74	**0.039**	8.28	**3.36**	9.63	**4.1**	9.73	**0.039**	15.36
4	128	0.16	**0**	0.16	**0.03**	**0**	0	**0**	0	**0**	0	5.78	**0.21**	5.47	**0**	**0**	0.7
	256	0.16	**0.15**	**0.39**	0.82	**0.47**	0.46	**0.078**	0.28	**0.078**	0.13	4.14	**2.24**	4.37	**0.09**	**0.078**	4.32
	512	**0.2**	2.12	**0.2**	4.8	**0.27**	3.67	**0.12**	3	**0.039**	1.75	**4.69**	7.8	4.41	**1.58**	**0.039**	11.11
3	128	**0.94**	5.33	**2.5**	12.67	**0.47**	10.03	**0.31**	7.15	**0.47**	4.79	**4.22**	5.31	3.28	**3**	**0.31**	9.14
	256	**0.55**	12.59	**2.03**	21.81	**0.39**	18.88	**0.16**	15.65	**0.16**	12.12	**3.36**	13.37	**2.97**	9.71	**0.078**	17.98
	512	**0.31**	21.07	**1.91**	28.17	**0.43**	26.25	**0.2**	23.53	**0.27**	20.53	**2.23**	21.08	**3.63**	17.82	**0.12**	25.42
2	128	**0.47**	2.09	**0.94**	6.81	**0.47**	3.62	**0.16**	2.79	**0.16**	3.13	1.25	**0.8**	6.25	**2.05**	**0.16**	4.22
	256	**0.23**	7.45	**1.02**	13.92	**0.16**	10.21	**0.16**	8.72	**0.16**	9.54	**1.41**	4.12	**4.06**	7.42	**0.16**	10.91
	512	**0.47**	15.03	**0.94**	21.81	**0.47**	17.76	**0.16**	16.61	**0.16**	17.3	**1.25**	11.1	**6.25**	14.92	**0.16**	18.79
1	128	**0.78**	11.76	**1.72**	14.93	**0.94**	19.28	**0.31**	13.69	**0.31**	6.94	**6.41**	9.01	**5.47**	6.5	**0.31**	15.03
	256	**0.16**	19.44	**1.8**	22.52	**0**	26.63	**0.078**	21.58	**0.078**	14.39	**5.00**	16.72	**4.61**	13.87	**0**	22.52
	512	**0.2**	27.15	**1.17**	29.7	**0.27**	32.8	**0.12**	28.44	**0.12**	22.31	**4.45**	24.84	**3.16**	21.8	**0.078**	29.28

Table 8
Average performance for robustness evaluation.

	proposed_128	[6]_128	proposed_256	[6]_256	proposed_512	[6]_512
durand	**2.34**	3.34	**1.63**	7.12	**1.54**	12.23
chiu	**3.49**	4.26	**3.15**	8.46	**3.08**	13.74
tumblin	**4.12**	4.25	**2.31**	4.02	**3.87**	14.65
reinhard	**1.57**	2.79	**0.31**	1.24	**1.29**	11.9
drago	**1.63**	3.98	**0.32**	1.24	**1.28**	15.84
ICAM	6.2	**1.8**	**4.02**	5.55	**5.24**	10.92
tone	8.7	**1.71**	**7.01**	7.73	**7.4**	9.68
HDR	**1.56**	7.64	**0.15**	1.17	**1.07**	21.32

Table 9
Robustness evaluation by BER (in %) for images with 512 or 256 or 128 bits message against regular attacks.

Attacks	M	Noise (0.01)	Noise (0.05)	Blur (once)	Blur (twice)	UnSharp (once)	UnSharp (twice)	Cropping (100*100)	Gaussian_Blur (r = 0.8)
12	128	20.91	36.72	0.78	0	1.56	14.84	0	0.78
	256	16.02	29.3	0	0	2.34	9.38	0	0
	512	12.89	29.49	0	0	2.34	13.87	0	0
11	128	36.72	37.5	15.62	15.62	19.53	23.44	12.5	15.62
	256	37.5	35.16	11.72	10.16	10.55	11.72	8.59	11.72
	512	30.66	40.23	10.74	12.7	13.28	15.23	8.79	10.74
10	128	25	32.81	3.91	5.66	6.84	14.84	4.3	3.91
	256	25	33.59	3.12	3.12	4.69	10.94	3.12	3.12
	512	26.56	35.74	3.91	5.66	6.84	14.84	4.3	3.91
9	128	10.16	22.66	1.56	1.56	5.47	25	0.78	1.56
	256	8.98	14.84	0	0.39	8.59	25	0	0
	512	6.64	14.06	0	0	8.01	33.4	0	0
8	128	12.5	24.22	0	0.78	10.94	24.22	0.78	0
	256	13.28	30.86	0	0	4.3	16.8	3.52	0
	512	14.26	22.85	0.98	1.17	8.59	26.56	2.93	0.98
7	128	5.47	20.31	0	0.78	7.81	17.19	0.78	0
	256	8.2	15.62	0	1.17	8.2	27.73	1.17	0
	512	8.4	15.04	0.2	0.59	7.23	23.24	0.59	0.2
6	128	16.41	31.25	0	0	1.56	10.16	3.91	0
	256	17.19	30.47	0	0.39	3.52	14.06	2.73	0
	512	16.02	26.37	0.59	1.17	4.3	11.52	2.15	0.59
5	128	25	28.91	0	0.78	1.56	10.94	0	0
	256	19.14	31.64	1.17	1.56	3.52	11.72	0	1.17
	512	20.31	31.25	0	0	4.49	10.74	0	0
4	128	18.75	28.71	0	0	1.95	13.48	0	0
	256	16.41	25	0	0	1.95	16.8	0.39	0
	512	18.95	28.71	0	0	1.95	13.48	0	0
3	128	15.62	22.66	2.34	2.34	7.81	21.09	2.34	2.34
	256	10.55	21.48	0.39	0.39	8.59	24.3	0.39	0.39
	512	9.18	14.26	0.39	1.37	9.77	27.54	0.2	0.39
2	128	14.06	30.47	0	1.56	7.81	17.97	1.56	0
	256	14.84	22.66	0.39	1.17	6.25	19.53	0.7	0.23
	512	16.02	23.63	0.2	0.78	7.23	19.34	0.98	0.2
1	128	21.09	32.03	0	1.56	8.59	12.5	0	0
	256	11.72	18.36	0	0	14.45	24.61	1.95	0
	512	15.23	25.98	0.2	0.39	9.77	20.31	0.98	0.2

related works easier, Table 8 provides the average of results on all the images. The average results show the strength of the proposed approach and introduce it as the unrivaled winner.

4.2.2. Regular attacks

Regular attacks are attacks such as cropping, filtering, adding noise, etc. These attacks are investigated on LDR images watermarking so far. Such attacks can happen to HDR images as well, thus, the proposed algorithm should be robust against these attacks as well. To evaluate the robustness against regular watermarking attacks, some Matlab filters have been used which are listed in Table 6.

The results of robustness tests against regular attacks are reported in Table 9. This table reports result for the condition in which 128, 256 and 512 bits are inserted. The BER amounts in Table 9 are in percent. The proposed work robustness against blurring, cropping and unsharp (once) is very desirable; however, the robustness against speckle noise and unsharp (twice) is not ideal but acceptable.

4.2.3. Security assessment

In order to evaluate the security of the proposed watermarking algorithm, having initial solutions (Foods) and watermark message. The proposed algorithm has to find a fake key equal to the final key based on which watermark embedding has been done. The watermark image and the original key also exist and the algorithm must test the fake key in order to distinguish the embedded watermark. To measure the efficiency of the watermark message extracted using fake key correlation and BER criteria are used to evaluate the similarity of the extracted watermark by the fake key and the original watermark message. To define False positive problem numerically, it is said that a false positive has occurred if the Normalized Correlation of extracted watermark and the original watermark message exceeds 0.7 [21]. NC is calculated for the tested images in this paper and none of them has produced NC more than 0.7. The average amount of NC is obtained as 0.041. That is a proof of security of the proposed method. Since the proposed work is based on random selections for modifying a solution. The intruders cannot produce the final Key even by having embedding

procedure and initial solutions (Foods). So it can be claimed that the proposed work is secure and revealing of the final key is not an easy work to do. NC formula is illustrated using Eq. (17) in which W is indicator of original watermark message and W' is indicator of extracted watermark using fake key. The parameters wx and wy are the dimension of the original watermark message and parameters i and j demonstrate the image indices. NC has values between 0 and 1. Higher NC means higher similarity between the two messages.

$$NC = \frac{\sum_{i=1}^{wy}\sum_{j=1}^{wx} W(i,j) \times W'(i,j)}{\left(\sqrt{\sum_{i=1}^{wy}\sum_{j=1}^{wx} W(i,j)^2}\right)\left(\sqrt{\sum_{i=1}^{wy}\sum_{j=1}^{wx} W'(i,j)^2}\right)} \quad (17)$$

5. Conclusion

In this paper, a new watermarking method for HDR images is proposed. This method is based on artificial bee colony (ABC) algorithm that seeks appropriate locations according to foraging behavior of honey bees. Then the insertion process considers a cover image and embeds watermark bits in the locations which are in LH sub-bands and HL sub-band of the wavelet transformed of the cover image in LogLUV domain. The strength factor is chosen based on each block intrinsic features which are different in each of blocks. The proposed extraction process has no need to have the original HDR image.

Several experiments are done on 12 HDR images. These images have different size and texture thus they can be a good test bench to evaluate the proposed watermarking method. Considering results obtained by BER criterion, it is obvious the proposed approach is robust against TMOs attacks and regular attacks except rotating and scaling. In another word, the proposed work is not robust against geometric attacks. Also, the proposed work is imperceptible considering HDRVDP2 criterion.

For future works, researchers can test other evolutionary algorithm and do insertion in different transform space or in the spatial domain. Also, they can improve the proposed work in order to be robust against geometric attacks.

6. Appendices

6.1. Artificial bee colony

Artificial Bee Colony (ABC) is an algorithm for optimization inspired by the intelligent foraging behavior of honey bees. The algorithm proposed by Karaboga in 2005 [39]. The algorithm is as simple as other evolutionary algorithms such as Particle Swarm Optimization (PSO) and Differential Evolution (DE) algorithms. Furthermore, its control parameters are fewer than others and it only uses limit, colony size and maximum cycle number as control parameters. ABC creates a population-based search in which each food source position is modified by artificial bees [40]. A food source position represents a possible solution to the problem to be optimized. The amount of nectar of a food source corresponds to the quality of the solution represented by that food source. The bee's purpose is to detect places with a high amount of nectar and finally, find the best place having the highest amount of nectar. The whole procedure is based on some artificial bees (employed and onlooker) who fly around the search space to select food sources based on their experience and the information received from their nest mates. Onlookers are placed on the food sources by using a probability-based selection process. As the nectar amount of a food source increases, the probability of considering the food source by onlookers increases [39]. Some bees (such as scouts) fly and choose food sources randomly. The scouts do not save previous experience; each time, if the new place has a higher amount of nectar, it will be chosen. Thus, the ABC algorithm is a combination of local search and global search methods. The local search is performed by employed and onlooker bees, while the global search is accomplished by onlookers and scouts. The ABC algorithm is explained as follows:

- Initial food sources are produced for all employed bees
- REPEAT
  - Each employed bee goes to a food source which is in her memory and determines a neighbor source, then evaluates the nectar amount of the food source and dances in the hive.
  - Each onlooker watches the dance of the employed bees and chooses one of their sources depending on the dances, and then goes to that source. After choosing a neighbor around that source, she evaluates its nectar amount.
  - Abandoned food sources are determined and are replaced with the new food sources discovered by scouts.
  - The best food source found so far is registered.
  - UNTIL (requirements are met) [41].

References

[1] Debevec PE, Malik J. Recovering high dynamic range radiance maps from photographs. In: ACM SIGGRAPH 2008 classes; 2008. p. 31.
[2] Kang SB, Uyttendaele M, Winder S, Szeliski R. High dynamic range video. In: ACM Transactions on Graphics (TOG); 2003. p. 319–25.
[3] Reinhard E, Heidrich W, Debevec P, Pattanaik S, Ward G, Myszkowski K. High dynamic range imaging: acquisition, display, and image-based lighting. Morgan Kaufmann; 2010.
[4] Mohanty SP. Digital watermarking: A tutorial review http://www.csee.usf.edu/~smohanty/research/Reports/WMSurvey1999Mohanty.pdf.
[5] Singh P, Chadha R. A survey of digital watermarking techniques, applications and attacks. Int J Eng Innovative Technol (IJEIT) 2013;2:165–75.
[6] Maiorana E, Campisi P. Multi-bit watermarking of high dynamic range images based on perceptual models. Secur Comm Networks 2015.
[7] Mantiuk R, Kim KJ, Rempel AG, Heidrich W. HDR-VDP-2: a calibrated visual metric for visibility and quality predictions in all luminance conditions. ACM Trans. Graphics (TOG) 2011;30:40.
[8] Ward G. Real pixels. Graphics Gems II 1991:80–3.
[9] Larson GW. LogLuv encoding for full-gamut, high-dynamic range images. J Graphics Tools 1998;3:15–31.
[10] Guerrini F, Okuda M, Adami N, Leonardi R. High dynamic range image watermarking robust against tone-mapping operators. IEEE Trans Inf Forensics Secur 2011;6:283–95.
[11] Maiorana E, Solachidis V, Campisi P. Robust multi-bit watermarking for HDR images in the Radon-DCT domain. In: 2013 8th International Symposium on Image and Signal Processing and Analysis (ISPA); 2013. p. 284–9.
[12] Autrusseau F, Goudia D. Non linear hybrid watermarking for high dynamic range images. In: 2013 IEEE International Conference on Image Processing; 2013. p. 4527–31.
[13] Xue X, Okuda M, Goto S. Bilateral filtering based watermarking for high dynamic range image. In: Intelligent Signal Processing and Communications Systems (ISPACS), 2011 International Symposium on; 2011. p. 1–5.
[14] Solachidis V, Maiorana E, Campisi P. HDR image multi-bit watermarking using bilateral-filtering-based masking. IS&T/SPIE Electronic Imaging; 2013. 865505–865505-12.
[15] Wu J-L. Robust watermarking framework for high dynamic range images against tone-mapping attacks. INTECH Open Access Publisher; 2012.
[16] Cheng Y-M, Wang C-M. A novel approach to steganography in high-dynamic-range images. IEEE Multimedia 2009;16:70–80.
[17] M.-T. Li, N.-C. Huang, and C.-M. Wang, A data hiding scheme for high dynamic range images, 2011.
[18] Yu C-M, Wu K-C, Wang C-M. A distortion-free data hiding scheme for high dynamic range images. Displays 2011;32:225–36.
[19] Moghaddam ME, Nemati N. A robust color image watermarking technique using modified imperialist competitive algorithm. Forensic Sci Int 2013;233:193–200.
[20] Atashpaz-Gargari E, Lucas C. Imperialist competitive algorithm: an algorithm for optimization inspired by imperialistic competition. In: 2007 IEEE Congress on Evolutionary Computation; 2007. p. 4661–7.
[21] Gavini NS, Borra S. Lossless watermarking technique for copyright protection of high resolution images. In: Region 10 Symposium, 2014 IEEE; 2014. p. 73–8.
[22] Surekha B, Swamy G. Digital image ownership verification based on spatial correlation of colors, 2012.
[23] Surekha B, Swamy G. Sensitive digital image watermarking for copyright protection. IJ Network Secur 2013;15:113–21.
[24] Surekha B, Swamy G. Security analysis of A novel copyright protection scheme using Visual Cryptography. In: Computer and Communications Technologies (ICCCT), 2014 International Conference on; 2014. p. 1–5.

[25] Guerrini F, Okuda M, Adami N, Leonardi R. High dynamic range image watermarking. In: The 23rd Intl Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC 2008); 2008. p. 949–52.
[26] Karaboga D, Basturk B. Artificial bee colony (ABC) optimization algorithm for solving constrained optimization problems. In: International Fuzzy Systems Association World Congress; 2007. p. 789–98.
[27] AnyhereSoftware, Photospheresoftware download link.
[28] m. p. i. informatik. Image Gallery Dec 14 Available: http://resources.mpi-inf.mpg.de/hdr/gallery.html.
[29] Greg Ward AS. High Dynamic Range Image Examples Dec 14 Available: http://www.anyhere.com/gward/hdrenc/pages/originals.html.
[30] T.M.I.N. MATLAB (r2012b), MA, USA, 2012.
[31] Kuang J, Johnson GM, Fairchild MD. iCAM06: A refined image appearance model for HDR image rendering. J Visual Commun Image Represent 2007;18:406–14.
[32] Drago F, Myszkowski K, Annen T, Chiba N. Adaptive logarithmic mapping for displaying high contrast scenes. In: Computer Graphics Forum; 2003. p. 419–26.
[33] Banterle F, Artusi A, Debattista K, Chalmers A. Advanced high dynamic range imaging: theory and practice. CRC Press; 2011.
[34] Reinhard E, Stark M, Shirley P, Ferwerda J. Photographic tone reproduction for digital images. ACM Transactions on Graphics (TOG) 2002;21:267–76.
[35] Tumblin J, Rushmeier H. Tone reproduction for realistic images. IEEE Comput Graph Appl 1993;13:42–8.
[36] Chiu K, Herf M, Shirley P, Swamy S, Wang C, Zimmerman K. Spatially nonuniform scaling functions for high contrast images. Graphics Interface; 1993. pp. 245-245.
[37] Durand F, Dorsey J. Fast bilateral filtering for the display of high-dynamic-range images. In: ACM transactions on graphics (TOG); 2002. p. 257–66.
[38] Mantiuk R. *Download page for HDRVDP*. Available: http://sourceforge.net/projects/hdrvdp/files/hdrvdp/.
[39] Karaboga D. An idea based on honey bee swarm for numerical optimization.
[40] Karaboga D, Akay B. A comparative study of artificial bee colony algorithm. Appl Math Comput 2009;214:108–32.
[41] Teodorović D. Bee Colony Optimization (BCO). Innovations in swarm Intelligence Studies in computational intelligence, 248 eds. Berlin, Heidelberg: Springer; 2009.