Adaptive HDR Image Blind Watermarking Approach Based on Redundant Discrete Wavelet Transform

https://doi.org/10.3991/ijim.v17i10.38795

Roa'a M. Al_airaji[1(✉)], Ibtisam A. Aljazaery[2], Haider TH. Salim ALRikabi[3]
[1] Information Technology College, Babylon University, Babylon, Iraq
[2] Engineering College, Babylon University, Babylon, Iraq
[3] Electrical Engineering Department, Wasit University, Wasit, Iraq
roaaalairaji90@gmail.com

Abstract—Remarkable success has been recorded in the usage of digital watermarking which is aimed at protecting the intellectual property of multimedia content. In this paper, a new tone mapping attack-resistant high dynamic range (HDR) image zero-watermarking algorithm is proposed. In this algorithm extraction of stable and invariant features are extracted for efficient zero-watermarking through the application of the redundant discrete wavelet transform (RDWT) to the HDR image. The first step involves transforming the HDR image to HVS color space, and RDWT is implemented using the V-channel so that the LL sub-band which contains the strong structure contents of the image is obtained. The second step involves dividing the LL sub-band into non-overlapping blocks, which are afterwards subjected to the process of transformation through the use of the singular value decomposition (SVD) so that the U matrix can be extracted. Third, the use of an Auto-Regressive (AR) prediction technique was employed in generating a local relationship model and comparison is done to facilitate the production of a binary feature mask. In the fourth process, hybrid chaotic mapping (HCM) is used to generate blended watermark so that the security of the watermark can be fortified. Lastly, the computation of an effective zero-watermark is achieved through the implementation of an exclusive-or operation on the blended watermark and the binary feature mask. Based on the results, the approach presented in this study demonstrated superior performance in terms of withstanding TM attacks and other attacks associated with image processing.

Keywords—HDR, singular value decomposition, LDR, DWT, RDWT, AR

1 Introduction

Today, humans have higher expectations in terms of the quality of mages and visual perception. There is a huge constraint on the ability to capture the wide dynamic range in conventional low dynamic range (LDR) images, which in turn makes the dark areas underexposed and the light areas overexposed in the actual scene[1-4]. The low dynamic range (LDR) imaging is replaced with the high dynamic range (HDR) imaging technology so that actual scenes can be described accurately, while more details in both light and dark areas can be well captured [5-7]. The attentions of both professionals and

academics have been drawn to the protection of HDR images ownership due to their constant practical use [8-11]. The usage of watermarking technology is critical to information security as it facilitates the effective protection of multimedia data's copyright [12-17]. The dynamic range constraint that accompanies the present LDR display device makes it necessary perform tone mapping (TM) when HDR images are displayed on LDR display [18, 19]. Unlike in LDR image, TM operation is a kind of attack that cannot be avoided when the protection of HDR image ownership is taken into consideration. Despite the importance of watermarking of HDR images, only little attention has been given to it, with few techniques of watermarking for HDR image presented [20-30]. The watermarking algorithms presented by some authors majorly focuses on the ability of the watermark to blend in and be concealed within the image, and these algorithms have only been implemented within the image's spatial domain. In the work of Wang et al. [20] and Yu et al. [21], the exponential channel of HDR image stored in RGBE format was used to achieve direct guidance of the lossless watermark embedding. In another study, the authors, Li et al. [22] and Cheng et al. [23], embedded watermark within the image using least significant bit (LSB) method with RGBE and LogLuv (TIFF) storage formats. The use of 10-digit mantissa in OpenEXR format was employed in the sudy carried out by Lin et al. to convey secret data [24]. Apart from the aforementioned cases of embedded watermarking, there are other works where other forms of HDR watermark algorithms have been employed within the domain of transformation, paying attention to the structural properties of the HDR images. In the study carried out by Guerrini et al. watermarking was embedded through the use of quantization index modulation (QIM) in the discrete wavelet transformation (DWT) domain's low-frequency band [25]. Despite the fact that good imperceptibility was demonstrated by their algorithm, significant bit error rate was observed for the extraction of watermark. The use of bracketing process was employed by Solachidis et al. for the decomposing of the HDR image into a range LDR images that were exposed in different ways, with the watermark embedded image sequence's DWT domain [26, 31]. Nevertheless, the process did not demonstrate the needed imperceptibility. Based on the extraction of feature map, an approach for the watermarking of a HDR image was introduced by Luo et al. in study [27]. The approach which they presented has the ability to resist different kinds of TM attacks as well as several other traditional attacks associated with image processing so that the robust relationships among the three colour components of an HDR image can be maintained. Through the deployment of the above-mentioned techniques of watermarking, the strength of watermarking can be enhanced, thereby increasing the robustness of the watermarking method and deforming the image. Consequently, the struggle to achieve, watermarking, robustness, and imperceptibility becomes a challenge for professionals. In addition, it is sometimes not necessary to make modifications to certain HDR remote sensing and HDR medical images, and it is also important to create a technique that does not distort those images. In an attempt to solve this problem, a lossless zero-watermarking approach was proposed in the work done by Wen et al.; their result shows that the performance of their proposed method was better than those of traditionally-used watermarking algorithms in terms of the quality of the image [32-34]. Typically, when the zero-watermarking technique is

used, the in-built characteristics of the HDR images are retrieved to enable the computation of the robust zero-watermark while the quality of the image is maintained, and a balance between the invisibility and robustness of the watermark are balanced. Similar to zero-watermarking, is the process of image hashing which involves the extraction of the characteristics from the HDR images and converting it into a brief numerical format. Nevertheless, it is majorly used for the verification of image integrity [35, 36]. More so, the process of image hashing is that which supports, effectively, the content of the image and can be deployed to facilitate zero-watermarking [37-39].

There are two broad categories of zero-watermarking algorithms, which include, transform domain-based and spatial domain-based. The later involves the direct extraction of the characteristics from the spatial domain to enable the creation of the feature matrix. In the study carried out by Xiong et al. a reliable zero-watermarking based on the spatial domain was presented, and the feature matrices were constructed through a comparison of the size of block mean and the whole mean of the image [40]. In comparison with the spatial domain-based technique, the transform domain-based algorithms are more reliable as a wide variety of such algorithms are used in creating robust zero-watermarking. A technique for zero-watermarking was presented in the research work carried out by Cui et al.; the technique was based on DWT that creates watermarking through the selection of image wavelet coefficients [41], which is resistant to a wide range of image attacks. A number of multiscale transforms like Shearlet and Contourlet are regarded as extensions of the wavelet transform, and have been applied in zero-watermarking to enable the realization of high watermarking robustness. A zero-watermarking techniques which is based on Schur decomposition and contour-let transform was presented by Zhu et al. [42]; the proposed technique demonstrated high efficiency in resisting compression and rotation attacks. In the study by Maiorana et al. [43], a blind multi-bit watermarking method that is based on the characteristics of the Radon-discrete cosine transform (RDCT) and the QIM nonuniform quantizer was presented, but the experimental results revealed that a high BER of 22% was recorded for the technique. Regardless of the challenges and disadvantages of using the redundant discrete wavelet transform (RDWT), it is also accompanied by some advantages including, optimal spatial localization and it is a transform that is compactly supported. The decomposition of multiscale, results in the efficient extraction of stable information from images by RDWT, without engaging in a procedure of downsampling. In this paper, the RDWT has been used for the extraction of stable and invariant structure features from the HDR image so that a dependable zero-watermark can be created for the protection of copyright.

In this work, an algorithm for HDR image zero-watermarking based on SVD and RDWT was proposed.

RDWT was applied on HDR so that the LL sub-band can be computed, while its invariant geometrical structures are extracted. The decomposition of the LL sub-band is done consecutively through the use of the SVD so that the stability of the feature matrix can be achieved. In the study carried out by the authors [44] an Auto-Regressive (AR) prediction approach was used to generate a local correlation model. Subsequently, a comparison was done to enable the construction of a binary feature mask, and this in

turn increases the robustness of zero-watermarking. Meanwhile, a hybrid chaotic mapping (HCM) method of security is used to create scrambled watermark, while the zero-watermark is created through the implementation of an exclusive or operation on the scrambled watermark and binary feature mask. The contributions of this article are listed as follows:

1. It proposes a robust approach for zero-marking of HDR images.
2. The transformation of HDR image is performed using the RDWT to enable the extraction of stable and invariant characteristics.
3. Based on the results obtained in this study, the HDR image zero-watermarking approach presented in this work demonstrates higher reliability than some of the existing HDR image zero-watermarking approaches.

The remaining of this article is organized as follows: Section 2 contains a brief introduction of the RDWT, SVD, AR prediction approach and HCM method. Section 3 presents the process through which the embedding and extraction of watermarking is carried out. Section 4 presents the discussion of results and the analysis performed. Section 5 report presents the study conclusions.

2 Background

In this part of the paper, redundant discrete wavelet transforms (RDWT), singular value decomposition (SVD), Auto-Regressive (AR) prediction method and hybrid chaotic mapping (HCM) which were used in the presented approach are presented and described subsequently.

2.1 RDWT and SVD property

The use of the RDWT in this work is due to the resolution properties which it possesses as well as the frequency spread, and optimal spatial localization which are almost the same as those of the HVS theoretical models. All these characteristics enable the extraction of the invariant and stable structure features from the HDR image so that a trusted zero-watermark can be produced for copyright protection of HDR images. The Eq 1. below explains the analysis and synthesis of RDWT [45].

$$\begin{cases} b_j[k] = b_{j+1}[k] * l_j[-k] \\ c_j[k] = c_{j+1}[k] * h_j[-k] \end{cases} \tag{1}$$

$$b[k] = \frac{1}{2}\left(b_j[k] * l_j[k] + c_j[k] * h_j[k]\right) \tag{2}$$

Where l[k], l[-k] represent the lower-pass synthesis filter and corresponding lower-pass analysis filter, respectively. h[k], h[-k] denotes the high-pass synthesis filter and the corresponding high-pass analysis filter. bj and cj are the coefficients of the output for lower-band and higher-band at level j. The symbol $*$ denotes convolution.

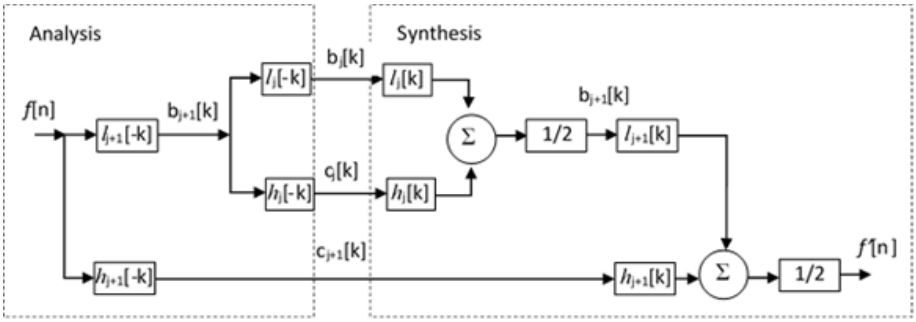

Fig. 1. 1D RDWT analysis and synthesis filters

2.2 SVD

An image's basic algebraic characteristics are effectually represented by the singular value decomposition (SVD), where the image geometry is reflected by the singular vectors and singular values match with image brightness. SVD of a matrix is a term used to describe the decomposition of the matrix into a product of three matrices. The following defines the SVD representation of matrix A [46].

$$A = U\Sigma V^T = [U_1, U_2, \dots U_N] \begin{bmatrix} \lambda_1 & 0 & 0 & 0 \\ 0 & \lambda_2 & 0 & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & \lambda_N \end{bmatrix} [V_1, V_2, \dots V_N]^T \tag{3}$$

$$= \lambda_1 U_1 V_1^{\mathrm{T}} + \lambda_2 U_2 V_2^{\mathrm{T}} + \dots + \lambda_N U_N V_N^{\mathrm{T}}$$

Where U and V denote the orthogonal matrices, the columns that are represented as left and right vectors, respectively. Σ denotes a diagonal matrix, the diagonal items whose arrangement is done in a descending manner and represent non-negative singular values.

2.3 Arnold transform

The method through images are scrambled is referred to as Arnold transform, and is also regarded as a 2D chaotic mapping [47]. This method of watermarking is used frequently with the aim of increasing the security of images with embedded watermark while enhancing the robustness of the algorithm [48]. Subsequent to subjecting an image to the process of Arnold transform, different positions of pixels can be altered. The illustration of the 2D transform is given as follows:

$$\binom{a'}{b'} = \left[\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \binom{a}{b}\right] mod\ P \tag{4}$$

Where P is the size of the watermark, (a, b) represents the position coordinates of the original pixels of the image, and (a′, b′) denotes the locus coordinates of the image's blended pixels. Subsequent to the transformation of all the pixels of the image, the

blended image is derived. The process of Arnold blending is initiated occasionally. Once T iterations is completed, where T is regarded as the period of transformation, the image can return to its original state [49]. The secret key could be the number of images blending iterations and T. It is not possible to achieve the recreation of the authentic image in the absence of the keys. The technique presented in this work uses the Arnold transform method to distort the initial watermark image.

2.4 Hybrid chaotic mapping (HCM)

Basically, there are two kinds of chaotic approaches that constitute the HCM: the first is referred to as the logistic map (LM) [50] and it is represented as follows:

$$x_{m+1} = \mu x_m(1 - x_m) \tag{5}$$

Where $x_0 \notin \{0, 0.25, 0.5, 0.75\}$, x_m denotes chaotic map sequence, and $\mu \in [0, 4]$ is representative of the control variable. The second one is the piecewise linear chaotic map (PWLCM)[51], and is also employed in watermark encryption due to the characteristics it possess. These characteristics include diffusion, confusion, distribution uniformity, and good ergodicity. Piecewise linear chaotic map is represented in the following manner:

$$x_{m+1} = F(x_m, p) = \begin{cases} \frac{x_m}{p}, & x_m \in [0, p] \\ \frac{(x_m - p)}{(0.5 - p)}, & x_m \in [p, 0.5] \\ F(1 - x_m, p), & x_m \in [0.5,1] \end{cases} \tag{6}$$

Where $p \in (0, 0.5)$ and $x_m \in (0, 1)$ $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. The above mentioned PWLCM technique has a control variable p which is converted to a control variable p_m so that the security of the presented approach can be achieved; p_m is depends on the random sequence that emerges from x_m. The condition p (0, 0.5) can be satisfied by making p_m to be one-third of x_m. The definition of the mixed chaotic map method can be as follows:

$$\begin{cases} x_{m+1} = \mu x_m(1 - x_m, p_m = x_m/3) \\ \frac{y_m}{p_m}, & y_m \in [0, p] \\ y_{m+1} = \frac{(y_m - p_m)}{(0.5 - p_m)}, & y_m \in [p_m, 0.5] \\ F(1 - yy_m, p_m), & y_m \in [0.5,1] \end{cases} \tag{7}$$

The watermark image encryption of the proposed watermarking technique can be realized by using equation (5) to produce hybrid sequences.

2.5 Auto-regressive (AR) prediction method and Feature matrix construction

AR prediction is defined as a time-series statistical method with extensive application in the areas of signal processing, state estimation, recognition of patterns, and related areas of prediction. In AR, the probability of a Bayesian condition between the

values of input value and its surrounding values is maximized so that the objective of error ε minimization can be realized. In addition, it has demonstrated superior performance as compared with the conventional four or eight adjacent forecasting techniques in terms of accuracy [52]. In this article, optimal representation of image and the prevention of a wide range of image attacks are realized by denoting AR coefficients as the image's local correlation model. The use of AR prediction is employed in determining the local correlation between the center value $A_{i,j}$ of a block and its neighbors values $A_{i+h,j+k}$ of the orthogonal matrix U matrix of SVD. The feature matrix is constructed using the predicted center value with the local correlation model by comparing it with the initial center value of the block. The definition of the AR model is given as follows:

$$A_{i.j} = \sum_{h=-t}^{t} \sum_{k=-t}^{t} A_{\mathrm{i+h,j+k}} \times \alpha_{m,n} + \varepsilon \tag{8}$$

where h,k denotes the AR coefficients of the corresponding position and reflects the relationship between $A_{i,j}$ and its neighbor values $A_{i+h,j+k}$, where m , n are both not zero at the simultaneously, $A_{i,j}$ denotes the pixel value of the position (i, j) in the U matrix, t is representative of the neighbor range deployed in the prediction of $A_{i;j}$ and it is equal to 2 in this paper; Ɛ is the error term.

3 Proposed zero-watermarking algorithm

In this section of the article, a blind-watermark is introduced. The introduced watermark is a blind-watermark which uses RDWT and SVD. Also, the section touches on the creation of zero watermark and the process of extracting the watermark; the characterization of extraction process is done in details as follows:

3.1 Zero-watermark creation

Assuming W is the authentic binary watermark, and possesses a size of N×N, and I denotes the original HDR image with the size of M×M, where N=M÷ n. Figure 2 shows the process through which zero-watermark is produced, and details of the basic steps in this process are described below:

Step 1. HDR image should be converted into HSV color space.

Step 2. RDWT should be applied on V channel of the HDR image, and the LL subband is divide into n × n non-overlapping blocks.

Step 3. Apply SVD on each block in order to obtain the orthogonal matrix U.

Step 4. Compute the predicted center value with the local correlation technique through the use of Eq. (8) for all blocks.

Step 5. The authentic center values of all blocks should be arranged in a matrix R1, and the predicted center values are arranged in a matrix R_2.

Step 6. The feature matrix T should be constructed through a comparison of the real value with the predicted value of the center pixel as follows:

$$T(a,b) = \begin{cases} 1, |R_1(a,b)| \geq |R_2(a,b)| \\ 0, |R_1(a,b)| < |R_2(a,b)| \end{cases} \tag{9}$$

Step 7. Scramble the authentic watermark W by using the Arnold transform to get W1, with the secret key k_1:

$$W_1 = Arnold(W) \tag{11}$$

Step 8. Use equation (9) to generate random series S_1. S_1 is transformed into a binary image represented by G. The encrypted watermark, W_2, is obtained by applying X-OR operator between W_1 and G_1:

$$W_2 = XOR(W_1, G_1) \tag{12}$$

Step 9. Generate zero-watermark W^* by using X-OR operator between the encrypted watermark W_2 and T.

$$W^* = XOR(W_2, T) \tag{13}$$

Step 10. The protection of copyright was achieved by using an intellectual rights property (IPR) of a third-party dataset to register the acquired zero-watermark W^* and secret key k1 for security purposes.

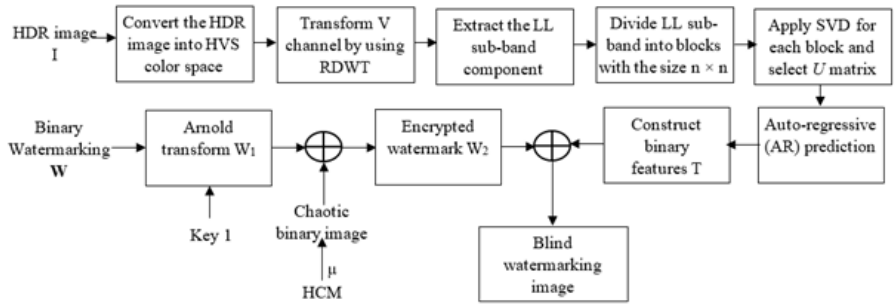

Fig. 2. Zero-watermarking generation

3.2 Zero-watermark extraction

Where I^* represents the image to be verified, Figure 3 shows the process through which the blind-watermark is extracted for the verification of ownership, and the basic steps are described in details as follows:

Step 1. HDR image I^* is converted into HSV color space.

Step 2. Apply RDWT on V channel of the HDR image, and the LL sub-band is divide into n × n non-overlapping blocks.

Step 3. Application of SVD is made on each block to get the orthogonal matrix U.

Step 4. Compute the predicted center value with the local correlation method through the use of Eq. (8) for all blocks.

Step 5. The original center value of all blocks should be arranged in a matrix R_1^*, and the predicted values are arranged in a matrix R_2^*.

Step 6. Feature matrix T* should be constructed through a comparison of the authentic value and predicted center value as follow:

$$T^*(a,b) = \begin{cases} 1, |R_1^*(a,b)| \geq |R_2^*(a,b)| \\ 0, |R_1^*(a,b)| < |R_2^*(a,b)| \end{cases} \quad (14)$$

Step 7. Chaotic binary mage G1 is also generated by the saved private keys. Afterwards, an exclusive-or operations is carried out as seen in equation (10) below.

$$W_0 = XOR(XOR(W^*, T^*), G_1) \quad (15)$$

Step 8. The use of Arnold transform is employed in the extraction of the final watermark W_1.

$$W_1 = Arnold^{-1}(W_0) \quad (16)$$

A comparison is done between the initial binary watermark W and the extracted W_1, and if any similarity is found between the two watermarks, then successful certification has been achieved are similar, the certification is successful.

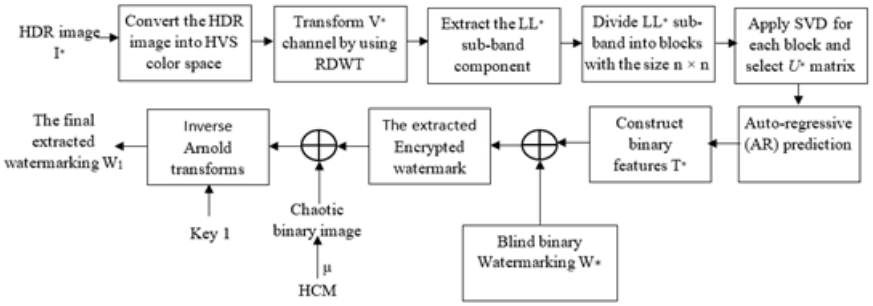

Fig. 3. Zero-watermarking extraction

4 Experimental results and analysis

Based on Figure 5 below, it can be observed that the 10 HDR images used for testing were obtained from TMQI database[53] and Gred Ward database[54]. The binary watermark image can be seen in Figure 4. Also, the robustness of the watermarking method was evaluated through the use of 18 conventional TM attacks, and these are presented in Table which also shows other conventional attacks launched on image processing. The Arnold scrambling secret key k1 =27.

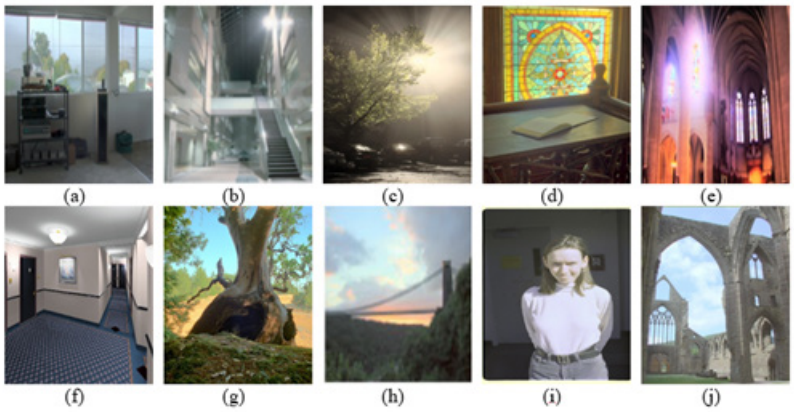

Fig. 4. Original HDR images. (a) Apartment. (b) AtriumNight. (c) bigFogMap. (d) desk. (e) nave. (f) rend02. (g) tree. (h) 2. (i) 3. (j) 15

Fig. 5. Watermark image

Table 1. List of the used different TM Attacks [55]

TM NO	TM Name	TM NO	TM Name	TM NO	TM Name
TM_1	Banterle	TM_7	Mertens	TM_{13}	Kuang
TM_2	Ashikhmin	TM_8	WardHistAdj	TM_{14}	Lischinski
TM_3	TumblinRushmeier	TM_9	WardGlobal	TM_{15}	Logarithmic
TM_4	Gamma	TM_{10}	Raman	TM_{16}	Exponential
TM_5	Drago	TM_{11}	Reinhard	TM_{17}	Durand
TM_6	Normalize	TM_{12}	Krawczyk	TM_{18}	Fattal

Watermarking robustness is described as the ability of the watermarking which has been generated through a given method to demonstrate resilience towards a wide range of unintended attacks like the conventional image processing attacks and TM attacks. The watermarking's robustness is evaluated using the normalized cross-correlation (NC) [14] and bit error rate (BER)[50] between the extracted and authentic watermarks. The definitions of the normalized cross-correlation (NC) and bit error rate (BER) are provided in equations (12) and (13), respectively:

Where $W_1(a, b)$ and W (a, b) represent the original watermark as well as the extracted watermark, respectively.

$$NC = \frac{\sum_a \sum_b W(a,b) \times W_1(a,b)}{\sqrt{\sum_a \sum_b W^2(a,b)} \sqrt{\sum_i \sum_j W_1^2(a,b)}} \tag{12}$$

Where N_t represents the number of total bits within a watermark and Ne is the number of error bits in a watermark.

$$BER = \frac{N_e}{N_t} \tag{13}$$

4.1 Verification of zero-watermarking uniqueness

It is crucial for a zero-watermark generated from a wide range of original images to demonstrate uniqueness. This means that, the zero-watermark generated from an image should only be peculiar to the given image. The normalized cross-correlation (NC) of zero-watermark images, which is derived by calculating the similarities between the binary zero-watermark images created from the ten original HDR images can be seen in Table 1. Based on the results presented in Table 1, the maximum and minimum NCs are both well below, Table 2.

Table 2. Maximum and Minimum NCs

Image	Apart-ment	Atrium Night	bigFog Map	desk	nave	rend02	Tree	2	3	15
Apart-ment	100.00	66.72	65.28	59.27	64.02	65.21	68.24	61.54	52.16	64.21
Atri-umNight	66.72	100.00	63.76	60.89	68.09	61.38	65.36	63.46	50.10	64.59
bigFog-Map	65.28	63.76	100.00	62.73	63.38	60.72	70.14	64.17	54.04	64.32
desk	59.27	60.89	62.73	100.00	62.38	61.05	61.17	64.38	54.04	69.56
nave	64.02	68.09	63.38	62.38	100.00	65.69	64.78	65.05	53.89	65.02
rend02	65.21	61.38	60.72	61.05	65.69	100.00	59.58	65.47	54.30	62.41
Tree	68.24	65.36	70.14	61.17	64.78	59.58	100.00	59.03	63.02	60.22
2	61.54	63.46	64.17	64.38	65.05	65.47	59.03	100.00	65.15	60.25
3	62.16	60.10	64.04	64.04	63.89	64.30	63.02	65.15	100.00	63.52
15	64.21	64.59	64.32	69.56	65.02	62.41	60.22	60.25	63.52	100.00

It can conclude, based on the results, that the zero-watermarking produced by the method proposed in this study is unique and shares low similarity with numerous original HDR images.

4.2 Robustness evaluation

To evaluate the robustness of the watermarking method, 18 TM attacks were targeted at the original HDR images so that the resilience of the proposed watermarking method

to the given attacks can be determined. Table 3 presents BERs of the proposed algorithm for ten attacked images.

Table 3. BERs of HDR TM-attacked images [. %]

Attack	Apart-ment	Atrium Night	bigFog Map	desk	Nave	rend02	Tree	2	3	15
TM1	1.98	7.96	1.61	6.98	3.59	1.95	5.03	8.62	6.63	9.56
TM3	1.42	6.98	2.08	2.91	3.93	2.20	4.74	6.98	2.90	8.11
TM4	4.17	8.50	5.27	7.37	4.57	7.13	4.96	7.18	5.48	9.72
TM5	0.85	3.03	0.78	2.05	1.15	1.15	0.78	2.32	3.27	5.01
TM7	7.30	10.40	7.96	9.08	8.23	8.62	7.32	13.09	7.07	8.62
TM8	1.12	0.59	0.42	0.81	0.27	0.59	0.49	2.03	5.50	10.47
TM9	2.54	7.28	3.83	2.91	6.10	3.56	4.39	4.57	8.14	2. 78
TM10	0.32	7.18	1.20	2.69	2.44	2.17	8.62	5.86	5.06	7.75
TM12	1.46	5.69	3.49	3.17	3.42	3.25	2.71	5.22	4.51	4.79
TM14	3.37	10.06	6.32	6.88	3.44	6.08	5.27	8.57	7.91	4.78
TM17	16.61	16.27	12.32	12.78	13.56	8.17	13.00	14.20	4.39	16.34
TM18	10.88	11.90	11.00	11.32	10.76	9.10	11.56	2.25	16.23	7.40
Average	4.34	7.99	4.69	5.75	5.12	4.50	5.74	6.74	6.42	8.21

It can be clearly seen from Table 3 that effective copyright protection was achieved as BERs of less than 0.76 were achieved for most of the TM-attacked images. As compared to other TMs, the BERs for TM17 and TM18 attacks were quite higher, but they can be of importance in copyright protection. More so, all TMs demonstrated an average BER of less than 0.08, indicating that the proposed algorithm is robust against TM attacks. The method proposed in this paper has demonstrated resistance to both TM attacks and conventional image processing attacks. The original HDR images were exposed to ten traditional image processing attacks including, cropping, noise addition, scaling, rotation, filtering, rotation, and so on. Table 4 shows the BERs of the proposed algorithm.

Table 4. BERs of HDR images while under traditional image processing attacks [.%]

Attack	Apart ment	Atrium Night	bigFog Map	desk	nave	rend02	Tree	2	3	15
Pepper & salt (0.001)	4.00	4.79	1.32	2.98	3.76	1.49	3.74	7.76	4.63	5.52
Poisson	0.17	4.61	0.81	1.37	2.47	1.07	2.88	4.61	3.80	1.20
Median filter (3 × 3)	1.68	0.44	0.49	0.76	1.48	0.93	0.72	0.98	0.17	0.24
Median filter (5 × 5)	5.10	0.98	1.07	1.51	3.27	2.00	0.42	5.01	0.32	2.15
Scaling (4)	0.27	1.15	0.07	3.44	0.07	0.20	0	0.15	0.12	0.62
Scaling (1/4)	0.46	4.37	0.29	4.91	0.47	0.46	0	0.42	0.50	0.27

Attack	Apartment	Atrium Night	bigFog Map	desk	nave	rend02	Tree	2	3	15
Gaussian low-pass filter (3 × 3)	0.81	1.78	0.32	1.37	0.37	0.46	0.09	0.42	0.14	0.46
Image sharpen (0.5)	0.73	5.44	1.42	7.75	3.05	2.59	2.95	5.42	5.06	2.49
Average filter (4 × 4)	2.73	0.83	0.73	3.00	1.05	1.22	0.42	0.83	0.51	0.79
Imrotate (10º)	5.61	1.22	5.23	2.021	4.65	4.02	5.06	1.22	2.91	3.78
Average	2.16	2.56	1.18	2.91	2.06	1.44	1.63	2.68	1.82	1.75

Figure 6 shows the BERs obtained by the proposed algorithm when the HDR images are subjected to conventional image processing attacks. It can be seen from Table 5 that the ten HDR images demonstrated an average BER of less than 5% with a minimum value of 2.18%, implying that the proposed method is resistant to traditional attacks on image processing. Figure 6 shows the extraction of watermark from image under different attacks so that the process of watermark extraction can be demonstrated. It can be observed that the recreated watermark is more obvious, implying that it is possible to extract the watermark for protection of ownership. Similar results can be produced by other HDR images, and this shows that the proposed method is capable of resisting TM attacks as well as other conventional image processing attacks.

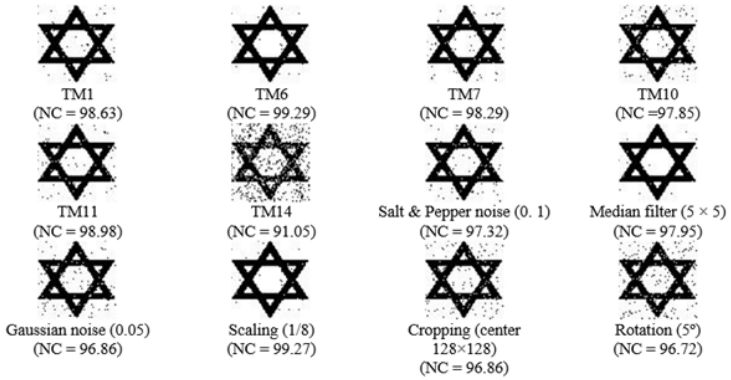

Fig. 6. It shows the BERs obtained by the proposed algorithm when the HDR images are subjected to conventional image processing attacks

4.3 Robustness comparison

A comparison is done between the proposed algorithm and Bai's [56] and Wang's [57] in terms of robustness against various TM attacks so as to validate the results of the comparative experiment. The results of the comparison are presented in Table 5 with the best results presented in bold fonts. From the table, it is clear that majority of

the BERs achieved by the proposed algorithm are lower than those of the two other algorithms. More so, it can be seen from Table 5 that a much lower average BER is achieved by the proposed algorithm, implying that the robustness of the proposed algorithm has been confirmed by the comparative experiments.

Table 5. Comparison between the proposed algorithm with Bai's and Wang's of robustness against various TM attacks

Attack type	Proposed	Bai's [56]	Wang's [57]
TM1	**4.17**	6.97	7.23
TM3	**0.88**	8.09	3.64
TM4	**1.42**	12.34	3.87
TM5	**1.61**	6.85	4.13
TM7	7.30	**6.15**	10.10
TM8	**2.54**	7.07	4.31
TM9	**1.12**	5.60	2.54
TM10	**3.37**	9.64	9.40
TM11	**1.46**	11.99	4.88
TM12	**1.98**	11.04	4.56
TM14	**0.32**	5.38	3.91
TM15	**0.85**	6.87	2.37
TM17	19.56	**6.66**	20.44
TM18	16.63	**13.89**	14.10
Average	**4.51**	8.47	6.82

5 Conclusion

In this article, a new HDR image zero-watermarking algorithm based on redundant discrete wavelet transform and singular value decomposition (SVD) has been presented. The use of RDWT method has been employed in transforming the V channel of HVS color space to facilitate the extraction of the invariant information of the HDR image. The successive decomposition of the LL sub-band image is carried out through the use of the SVD so that the characteristic matrix can be stabilized. A binary feature image is created using an Auto-Regressive technique with the aim of enhancing the robustness of the zero-watermarking. A zero-watermarking was created by applying an exclusive-or operation to the binary feature image as well as the watermarked image. Furthermore, the use of a hybrid chaotic mapping (HCM) was employed in obtaining the scrambled watermark so that the security of the watermarking is ensured. It is concluded, based on the experimental results, that the proposed algorithm is able to resist numerous TM attacks and the majority of traditional image processing attacks.

6 References

[1] Y. Huang, S. Qiu, C. Wang, and C. Li, "Learning representations for high-dynamic-range image color transfer in a self-supervised way," *IEEE Transactions on Multimedia,* vol. 23, pp. 176-188, 2020. https://doi.org/10.1109/TMM.2020.2981994

[2] A. Rana, P. Singh, G. Valenzise, F. Dufaux, N. Komodakis, and A. Smolic, "Deep tone mapping operator for high dynamic range images," *IEEE Transactions on Image Processing,* vol. 29, pp. 1285-1298, 2019. https://doi.org/10.1109/TIP.2019.2936649

[3] H. T. Hazim, "Secure Chaos of 5G Wireless Communication System Based on IOT Applications," *International Journal of Online & Biomedical Engineering,* vol. 18, no. 12, 2022. https://doi.org/10.3991/ijoe.v18i12.33817

[4] J. Q. Kadhim, "Enhancement of Online Education in Engineering College Based on Mobile Wireless Communication Networks and IOT," *International Journal of Emerging Technologies in Learning (iJET),* vol. 18, no. 02, 2023. https://doi.org/10.3991/ijet.v18i01.35987

[5] Z. Pan, M. Yu, G. Jiang, H. Xu, Z. Peng, and F. Chen, "Multi-exposure high dynamic range imaging with informative content enhanced network," *Neurocomputing,* vol. 386, pp. 147-164, 2020. https://doi.org/10.1016/j.neucom.2019.12.093

[6] S. Xie, W. Wu, R. Chen, and H.-Z. Tan, "Reduced-dimensional capture of high-dynamic range images with compressive sensing," *Discrete Dynamics in Nature and Society,* vol. 2020, 2020. https://doi.org/10.1155/2020/6703528

[7] H. T. S. A. Ibtisam A. Aljazaery, "Encryption of Color Image Based on DNA Strand and Exponential Factor," *International Journal of Interactive Mobile Technologies (iJIM),* 2021.

[8] V. Hulusic, K. Debattista, G. Valenzise, and F. Dufaux, "A model of perceived dynamic range for HDR images," *Signal Processing: Image Communication,* vol. 51, pp. 26-39, 2017. https://doi.org/10.1016/j.image.2016.11.005

[9] Y. Song, G. Jiang, H. Jiang, M. Yu, F. Shao, and Z. Peng, "A new tone-mapped image quality assessment approach for high dynamic range imaging system," in *2017 IEEE International Conference on Image Processing (ICIP)*, 2017: IEEE, pp. 1012-1016. https://doi.org/10.1109/ICIP.2017.8296434

[10] M. A. Khalifa, A. M. Ali, S. A. Alsadai, N. F. Alwan, and G. S. Mahdi, "A Novel Arabic Words Recognition System Using Hyperplane Classifier," *Wasit Journal of Computer and Mathematics Sciences,* vol. 1, no. 2, pp. 12-20, 2022.

[11] H. Ibrahim, "A Review on the Mechanism Mitigating and Eliminating Internet Crimes using Modern Technologies: Mitigating Internet crimes using modern technologies," *Wasit Journal of Computer and Mathematics Sciences,* vol. 1, no. 3, pp. 76-108, 2022.

[12] G. Bhatnagar, Q. J. Wu, and P. K. Atrey, "Secure randomized image watermarking based on singular value decomposition," *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM),* vol. 10, no. 1, pp. 1-21, 2013. https://doi.org/10.1145/2542205.2542207

[13] H.-Y. Yang, X.-Y. Wang, P.-P. Niu, and A.-L. Wang, "Robust color image watermarking using geometric invariant quaternion polar harmonic transform," *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM),* vol. 11, no. 3, pp. 1-26, 2015. https://doi.org/10.1145/2700299

[14] Z. Shao, Y. Shang, Y. Zhang, X. Liu, and G. Guo, "Robust watermarking using orthogonal Fourier–Mellin moments and chaotic map for double images," *Signal Processing,* vol. 120, pp. 522-531, 2016. https://doi.org/10.1016/j.sigpro.2015.10.005

[15] M. Amirmazlaghani, "Additive watermark detection in the wavelet domain using 2D-GARCH model," *Information Sciences,* vol. 370, pp. 1-17, 2016. https://doi.org/10.1016/j.ins.2016.06.037

[16] N. Alseelawi, and H. T. Hazim, "A Novel Method of Multimodal Medical Image Fusion Based on Hybrid Approach of NSCT and DTCWT," *International Journal of Online & Biomedical Engineering,* vol. 18, no. 3, 2022. https://doi.org/10.3991/ijoe.v18i03.28011

[17] B. K. Mohammed, S. A. A. A. Alsaidi, and R. F. Chisab, "Efficient RTS and CTS mechanism which save time," *International Journal of Interactive Mobile Technologies,* Article vol. 14, no. 4, pp. 204-211, 2020. https://doi.org/10.3991/ijim.v14i04.13243

[18] D. Kundu, D. Ghadiyaram, A. C. Bovik, and B. L. Evans, "Large-scale crowdsourced study for tone-mapped HDR pictures," *IEEE Transactions on Image Processing,* vol. 26, no. 10, pp. 4725-4740, 2017. https://doi.org/10.1109/TIP.2017.2713945

[19] M. A. a. Roa'a, I. A. Aljazaery, and S. K. Al_Dulaimi, "Generation of high dynamic range for enhancing the panorama environment," *Bulletin of Electrical Engineering and informatics,* vol. 10, no. 1, pp. 138-147, 2021. https://doi.org/10.11591/eei.v10i1.2362

[20] C.-M. Yu, K.-C. Wu, and C.-M. Wang, "A distortion-free data hiding scheme for high dynamic range images," *Displays,* vol. 32, no. 5, pp. 225-236, 2011. https://doi.org/10.1016/j.displa.2011.02.004

[21] Y.-M. Cheng and C.-M. Wang, "A novel approach to steganography in high-dynamic-range images," *IEEE MultiMedia,* vol. 16, no. 03, pp. 70-80, 2009. https://doi.org/10.1109/MMUL.2009.43

[22] Z.-H. Wang, T.-Y. Lin, C.-C. Chang, and C.-C. Lin, "A novel distortion-free data hiding scheme for high dynamic range images," in *2012 Fourth International Conference on Digital Home*, 2012: IEEE, pp. 33-38. https://doi.org/10.1109/ICDH.2012.49

[23] M.-T. Li, N.-C. Huang, and C.-M. Wang, "A data hiding scheme for high dynamic range images," *International Journal of Innovative Computing Information and Control (IJICIC),* vol. 7, no. 5A, pp. 2021-2035, 2011.

[24] Y.-T. Lin, C.-M. Wang, W.-S. Chen, F.-P. Lin, and W. Lin, "A novel data hiding algorithm for high dynamic range images," *IEEE Transactions on Multimedia,* vol. 19, no. 1, pp. 196-211, 2016. https://doi.org/10.1109/TMM.2016.2605499

[25] F. Guerrini, M. Okuda, N. Adami, and R. Leonardi, "High dynamic range image watermarking robust against tone-mapping operators," *IEEE Transactions on Information Forensics and Security,* vol. 6, no. 2, pp. 283-295, 2011. https://doi.org/10.1109/TIFS.2011.2109383

[26] V. Solachidis, E. Maiorana, and P. Campisi, "HDR image multi-bit watermarking using bilateral-filtering-based masking," in *Image Processing: Algorithms and Systems XI*, 2013, vol. 8655: SPIE, pp. 29-40. https://doi.org/10.1117/12.2005240

[27] T. Luo, G. Jiang, M. Yu, H. Xu, and W. Gao, "Robust high dynamic range color image watermarking method based on feature map extraction," *Signal Processing,* vol. 155, pp. 83-95, 2019. https://doi.org/10.1016/j.sigpro.2018.09.024

[28] R. a. M. Al_airaji, I. A. Aljazaery, and A. H. M. Alaidi, "Automated Cheating Detection based on Video Surveillance in the Examination Classes," *International Journal of Interactive Mobile Technologies,* vol. 16, no. 8, 2022. https://doi.org/10.3991/ijim.v16i08.30157

[29] N. Alseelawi, and H. T. Hazim, "A Novel Method of Multimodal Medical Image Fusion Based on Hybrid Approach of NSCT and DTCWT," *iJOE,* vol. 18, no. 03, p. 115, 2022. https://doi.org/10.3991/ijoe.v18i03.28011

[30] R. Mohamad, "Data hiding by using AES Algorithm: Data hiding by using AES Algorithm," *Wasit Journal of Computer and Mathematics Sciences,* vol. 1, no. 4, pp. 112-119, 2022.

[31] A. H. M. Alaidi, R. a. M. Al_airaji, H. T. ALRikabi, I. A. Aljazaery, and S. H. Abbood, "Dark Web Illegal Activities Crawling and Classifying Using Data Mining Techniques," *International Journal of Interactive Mobile Technologies,* vol. 16, no. 10, 2022. https://doi.org/10.3991/ijim.v16i10.30209

[32] Q. Wen, T.-f. SUN, and S.-x. Wang, "Concept and application of zero-watermark," *ACTA ELECTONICA SINICA,* vol. 31, no. 2, p. 214, 2003. https://www.ejournal.org.cn/EN/Y2003/V31/I2/214

[33] A. S. Mohamad, "Data encryption for bank management system: Data encryption for bank management system," *Wasit Journal of Computer and Mathematics Sciences,* vol. 1, no. 4, pp. 14-20, 2022.

[34] I. A. Aljazaery, H. T. S. Alrikabi, and M. R. Aziz, "Combination of Hiding and Encryption for Data Security," *International Journal of Interactive Mobile Technologies,* vol. 14, no. 9, pp. 34-47, 2020. https://doi.org/10.3991/ijim.v14i09.14173

[35] I. Bashir, F. Ahmed, J. Ahmad, W. Boulila, and N. Alharbi, "A secure and robust image hashing scheme using Gaussian pyramids," *Entropy,* vol. 21, no. 11, p. 1132, 2019. https://doi.org/10.3390/e21111132

[36] S. Q. Abbas, F. Ahmed, and Y.-P. P. Chen, "Perceptual image hashing using transform domain noise resistant local binary pattern," *Multimedia Tools and Applications,* vol. 80, no. 7, pp. 9849-9875, 2021. https://doi.org/10.1007/s11042-020-10135-w

[37] B. Han, J. Li, and Y. Li, "Zero-watermarking algorithm for medical volume data based on difference hashing," *International Journal of Computers Communications & Control,* vol. 10, no. 2, pp. 188-199, 2015. https://doi.org/10.15837/ijccc.2015.2.1752

[38] X. Wang and Y. Zhan, "A zero-watermarking scheme for three-dimensional mesh models based on multi-features," *Multimedia Tools and Applications,* vol. 78, no. 19, pp. 27001-27028, 2019. https://doi.org/10.1007/s11042-017-4666-1

[39] R. A. Azeez, M. K. Abdul-Hussein, M. S. Mahdi, and H. T. S. ALRikabi, "Design a system for an approved video copyright over cloud based on biometric iris and random walk generator using watermark technique," *Periodicals of Engineering Natural Sciences,* vol. 10, no. 1, pp. 178-187, 2021. https://doi.org/10.21533/pen.v10i1.2577

[40] J. Zhao, W. Xu, S. Zhang, S. Fan, and W. Zhang, "A strong robust zero-watermarking scheme based on shearlets' high ability for capturing directional features," *Mathematical Problems in Engineering,* vol. 2016, 2016. https://doi.org/10.1155/2016/2643263

[41] D. Cui, "Zero-watermarking technology for digital image based on DWT," *Journal of Chengdu Institute of Information Engineering,* vol. 3, pp. 306–308, 2007.

[42] C. Zhu, Y. Li, W. Chi, S. Gao, and D. Fan, "Zero-watermarking algorithm for color image in contourlet domain based on Schur decomposition," *Inf. Technol. Inf. Technol,* vol. 227, pp. 94-98, 2019.

[43] E. Maiorana, V. Solachidis, and P. Campisi, "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: IEEE, pp. 284-289. https://doi.org/10.1109/ISPA.2013.6703754

[44] X. Zhang, X. Li, Y. Feng, H. Zhao, and Z. Liu, "Image fusion with internal generative mechanism," *Expert Systems with Applications,* vol. 42, no. 5, pp. 2382-2391, 2015. https://doi.org/10.1016/j.eswa.2014.10.050

[45] T. D. Hien, Z. Nakao, and Y.-W. Chen, "Robust multi-logo watermarking by RDWT and ICA," (in), *Signal Processing,* vol. 86, no. 10, pp. 2981-2993, 2006. https://doi.org/10.1016/j.sigpro.2005.12.003

[46] C.-C. Chang, C.-C. Lin, and Y.-S. Hu, "An SVD oriented watermark embedding scheme with high qualities for the restored images," *International Journal of Innovative Computing, Information and Control,* vol. 3, no. 3, pp. 609-620, 2007.

[47] M. Khalili, "DCT-Arnold chaotic based watermarking using JPEG-YCbCr," *Optik,* vol. 126, no. 23, pp. 4367-4371, 2015. https://doi.org/10.1016/j.ijleo.2015.08.042

[48] S. Roy and A. K. Pal, "A robust blind hybrid image watermarking scheme in RDWT-DCT domain using Arnold scrambling," *Multimedia Tools and Applications,* vol. 76, no. 3, pp. 3577-3616, 2017. https://doi.org/10.1007/s11042-016-3902-4

[49] R. Keshavarzian and A. Aghagolzadeh, "ROI based robust and secure image watermarking using DWT and Arnold map," *AEU-International Journal of Electronics and Communications,* vol. 70, no. 3, pp. 278-288, 2016. https://doi.org/10.1016/j.aeue.2015.12.003

[50] C.-p. Wang, X.-y. Wang, X.-j. Chen, and C. Zhang, "Robust zero-watermarking algorithm based on polar complex exponential transform and logistic mapping," *Multimedia Tools and Applications,* vol. 76, no. 24, pp. 26355-26376, 2017. https://doi.org/10.1007/s11042-016-4130-7

[51] Y. Hu, C. Zhu, and Z. Wang, "An improved piecewise linear chaotic map based image encryption algorithm," *The Scientific World Journal,* vol. 2014, 2014. https://doi.org/10.1155/2014/275818

[52] J. Yang, X. Ye, K. Li, C. Hou, and Y. Wang, "Color-guided depth recovery from RGB-D data using an adaptive autoregressive model," *IEEE transactions on image processing,* vol. 23, no. 8, pp. 3443-3458, 2014. https://doi.org/10.1109/TIP.2014.2329776

[53] Subject-Rated Image Database of Tone-Mapped Images. https://ece.uwaterloo.ca/~z70wang/research/tmqi (accessed.

[54] Anyhere Software Database. http://www.anyhere.com/gward/hdrenc/pages/originals.html (accessed.

[55] V. O. F. Banterle. (2016). HDR Toolbox for MATLAB. https://github.com/banterle/HDR_Toolbox (accessed.

[56] Y. Bai, G. Jiang, M. Yu, Z. Peng, and F. Chen, "Towards a tone mapping-robust watermarking algorithm for high dynamic range image based on spatial activity," *Signal Processing: Image Communication,* vol. 65, pp. 187-200, 2018. https://doi.org/10.1016/j.image.2018.04.005

[57] R. Wang, H. Shaocheng, P. Zhang, M. Yue, Z. Cheng, and Y. Zhang, "A novel zero-watermarking scheme based on variable parameter chaotic mapping in NSPD-DCT domain," *IEEE Access,* vol. 8, pp. 182391-182411, 2020. https://doi.org/10.1109/ACCESS.2020.3004841

7 Authors

Roa'a M. Al_airaji received the Bachelor degree from Department of Computer, College of Science, University of Babylon, in 2012. Received the Master degre from Department of software, College of Information Technology, University of Babylon, in 2018. Currently work as assistant teacher in College of Science, University of Babylon.

Ibtisam A. Aljazaery is presently Asst. Prof. and on the faculty of Electrical Engineering Department, College of Engineering, University of Babylon. Babylon, Iraq. E-mail: sci.ibtisam.abdulwahid@uobabylon.edu.iq. The number of articles in national databases – 20, The number of articles in international databases – 5.

Haider Th. Salim ALRikabi is presently Asst. Prof. and one of the Faculty College of Engineering, Electrical Engineering Department, Wasit University in Al Kut, Wasit, Iraq. He received his B.Sc. degree in Electrical Engineering in 2006 from the Al Mustansiriya University in Baghdad, Iraq. His M.Sc. degree in Electrical Engineer-ing focusing on Communications Systems from California State University/Fullerton/USA

in 2014. His current research interests include Communications systems with the mobile generation, Control systems, intelligent technologies, smart cities, and the Inter-net of Things (IoT). Al Kut City-Hay ALRabee, Wasit, Iraq. E-mail: hdhiyab@uowasit.edu.iq. The number of articles in national databases – 15, The number of articles in international databases – 60.

Article submitted 2023-02-12. Resubmitted 2023-03-28. Final acceptance 2023-03-29. Final version published as submitted by the authors.