Expert Systems With Applications 62 (2016) 177–189

Contents lists available at ScienceDirect

Expert Systems With Applications

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

Improving digital image watermarking by means of optimal channel selection☆

Thien Huynh-The[a], Oresti Banos[b], Sungyoung Lee[a,*], Yongik Yoon[c], Thuong Le-Tien[d]

[a] Department of Computer Science and Engineering, Kyung Hee University (Global Campus), 1732 Deokyoungdae-ro, Giheung-gu, Yongin-si, Gyeonggi-do, 446-701, Korea
[b] Telemedicine Group, University of Twente, Drienerlolaan 5, 7500 AE Enschede, Netherlands
[c] Department of Multimedia Science, Sookmyung Women's University, Cheongpa-ro 47-gil 100, Youngsan-gu, Seoul, 140-742, Korea
[d] Faculty of Electrical and Electronics Engineering, Hochiminh City University of Technology HCM B2015-20-02, 268 Ly Thuong Kiet Street, District 10, Ho Chi Minh City 700000, Vietnam

ARTICLE INFO

Article history:
Received 20 April 2015
Revised 5 April 2016
Accepted 9 June 2016
Available online 11 June 2016

Keywords:
Digital image watermarking
Discrete wavelet transform
Coefficients quantization
Optimal color-channel selection
Adaptive Otsu thresholding

ABSTRACT

Supporting safe and resilient authentication and integrity of digital images is of critical importance in a time of enormous creation and sharing of these contents. This paper presents an improved digital image watermarking model based on a coefficient quantization technique that intelligently encodes the owner's information for each color channel to improve imperceptibility and robustness of the hidden information. Concretely, a novel color channel selection mechanism automatically selects the optimal HL4 and LH4 wavelet coefficient blocks for embedding binary bits by adjusting block differences, calculated between LH and HL coefficients of the host image. The channel selection aims to minimize the visual difference between the original image and the embedded image. On the other hand, the strength of the watermark is controlled by a factor to achieve an acceptable tradeoff between robustness and imperceptibility. The arrangement of the watermark pixels before shuffling and the channel into which each pixel is embedded is ciphered in an associated key. This key is utterly required to recover the original watermark, which is extracted through an adaptive clustering thresholding mechanism based on the Otsu's algorithm. Benchmark results prove the model to support imperceptible watermarking as well as high robustness against common attacks in image processing, including geometric, non-geometric transformations, and lossy JPEG compression. The proposed method enhances more than 4 dB in the watermarked image quality and significantly reduces Bit Error Rate in the comparison of state-of-the-art approaches.

1. Introduction

Millions of multimedia contents are daily generated and distributed among diverse social networks, websites, and applications fostered by the rapid growth of mobile devices and the Internet. Particularly noticeable is the current pace of creation and sharing of digital images, which are ubiquitously captured to record and show diverse aspects of our personal and social life. This poses important challenges in terms of transmission, storage, and especially the usage of these data, in which the copyright protection plays a crucial role. Unprotected images can be accessed, downloaded and reused by others illegitimately. As a consequence, personal images might be subject to commercial or other purposes by third parties without legally requiring the user consent. To avoid this kind of situations, efficient and robust techniques are especially required for digital image copyright protection and authentication.

Digital watermarking is one of the most widely used approaches to univocally authenticate the owner of a given image. This technique allows embedding the owner's information, a.k.a, watermark, into the host image so that it is ideally unobserved by the human eye. In an inverse process, the watermark is recovered from the embedded image to obtain the hidden information to determine its originality. Most of the research in the digital image watermarking domain revolve around two main concepts, namely, perceptibility and robustness. First, embedding a watermark into a given image implies an alteration of the latter one, which normally translates into an effective degradation of the quality of the host image (Chou & Liu, 2010; Xiang-yang, Chun-peng, Hong-ying, &

☆ This work was supported by a grant from the Kyung Hee University in 2013[KHU-20130438].

* Corresponding author. Fax: +82312012514.
E-mail addresses: thienht@oslab.khu.ac.kr (T. Huynh-The), o.banoslegran@utwente.nl (O. Banos), sylee@oslab.khu.ac.kr (S. Lee), yiyoon@sookmyung.ac.kr (Y. Yoon), thuongle@hcmut.edu.vn (T. Le-Tien).

http://dx.doi.org/10.1016/j.eswa.2016.06.015
0957-4174/

Table 1
Theoretical comparison of highlight digital image watermarking approaches.

Method	Transform domain	Side information	Host image	Watermark	Key
Tsai [2007]	None	Embedding position	Color	BinImg	Support vector machine
Tsui [2008]	Fourier	Real component	Color	BinBitSeq	Spatiochromatic discrete Fourier transform
Fu [2008]	None	Reference watermark	Color	BinImg	Linear discriminant analysis
Chou [2010]	Wavelet	Block location	Color	BinImg	Just noticeable color difference
Niu [2011]	Contourlet	Block location	Color	BinImg	Nonsubsampled contourlet transform
Dejey [2011]	Wavelet	Original host image	Grayscale	BinBitSeq	Fan beam transform
Bhatnagar [2012]	Wavelet-SVD	Transform order	Grayscale	GrayImg	Fractional wavelet packet transform
Wang [2012]	Wavelet	Bit ordering key	Grayscale	BinBitSeq	Hidden Markov model
Xiang-yang [2013]	Fourier	Number of scambling	Color	BinImg	Least squares support vector machine
Tsougenis [2014]	Fourier	Frequency number	Color	BinImg	Quaternion image moments
Proposed	Wavelet	Block location	Color	BinImg	Optimal channel selection

BinImg: binary image BinBitSeq: binary bit sequence GrayImg: grayscale image

Pan-pan, 2013). Thus, reducing the perceptibility of the watermark is the objective of most proposed models, which mainly apply to grayscale images, with very less recognized attempts in watermarking color images. Second, the watermark must be as robust as possible to resist common image processing operations (Su, Chang, & Wu, 2013; Tsai, Huang, & Kuo, 2011), so the owner information can be entirely extracted from the watermarked image. In addition to these, another important property typically sought in watermarking techniques is blindness. Fundamentally, the blind watermarking technique (Dejey & Rajesh, 2011; Nasir, Khelifi, Jiang, & Ipson, 2012; Nezhadarya, Wang, & Ward, 2011; Yamato, Hasegawa, Tanaka, , & Kato, 2012) is the most challenging type since they do not require the original image, the watermark, and reference image for the recovery process, conversely to semi-blind schemes (Bhatnagar, Raman, & Wu, 2012; Dadkhah, Manaf, Yoshiaki, Hassanien, & Sadeghi, 2014; Ganic & Eskicioglu, 2005; Song, Yu, Yang, Song, & Wang, 2008), which require the watermark and reference image, and non-blind models that require all of them (Song, Sudirman, & Merabti, 2012; Tsui, Zhang, & Androutsos, 2008). However, in most watermarking techniques, a secret key is required for the extraction process. This key may be presented in different forms and encode diverse kind of information, e.g., a permutation of the watermark image, locations of the watermarked blocks, color profiles of the host image, and among others.

In this work, the authors develop a color watermark method using the wavelet quantization technique from the existing grayscale watermarking approach (Huynh-The, Banos, Lee, Yoon, & Le-Tien, 2015; Huynh-The, Lee, Pham-Chi, & Le-Tien, 2014). In order to enhance imperceptibility and robustness, an optimal channel selection mechanism for color images is proposed. During the embedding process, both LH and HL wavelet coefficients of the host image are grouped into wavelet blocks for each color channel. The bits of the binary watermark image are securely shuffled and then encoded into the optimal channel wavelet blocks by modifying the value of their coefficients. To that end, an innovative color channel selection scheme is proposed here, which aims at minimizing the visual difference between the original image and the watermarked image. The robustness is controlled by a factor that weights the watermark strength in the host image. In the extraction process, an adaptive threshold calculated by the Otsu method is for classification of the detected bits to recover the watermark. Compared to existing approaches, the proposed research method has strengths of: (1) a color channel selection mechanism for the embedding process to obtain the impressive imperceptibility, (2) a factor describing the strength of the watermark to flexibly balance robustness and imperceptibility, (3) an adaptive Otsu threshold in the extraction process to accurately recovery watermark. Nevertheless, the proposed method is fragile with rotation variances due to the use of Wavelet transform in the image decomposition process and the payload capacity is constrained by the decomposition level. Providing a theoretical comparison between the proposed research with highlight approaches in the removal-attack resistance watermarking field is necessary and further summarized in Table 1.

The remaining of this paper is organized as follows. Section 2 introduces the state-of-the-art in the digital image watermarking domain. Section 3 describes the proposed watermarking scheme. Experimental results and their evaluation are presented in Section 4. Finally, conclusions are outlined in Section 5.

2. Related work

Watermarking techniques can be categorized into two classes based on the processing domain: spatial domain and transformed domain. In spatial domain techniques, the watermark is embedded by directly modifying pixel values or the histogram of the host image. Here, most studies focus on the relationship between the visual quality of the watermarked image and the payload capacity of the host image. For example, Reversible Data Hiding (RDH) is considered by Tian (2003) together with Difference Expansion (DE) (Tian, 2002) to discover extra storage space in images by searching redundancy in their content. In this line, Li, Zhang, Gui, and Yang (2013) proposed Difference-Pair-Mapping (DPM) for the RDH scheme to increase the payload capacity of the embedded watermark. This is performed by modifying the histogram of the host image, so high-frequency bins are expanded to carry new data. However, the embedded capacity of this method is not as high as expected, since only one pixel in a pixel-pair can be modified for the embedment process. A general scheme for RDH based on Histogram Shifting (HS) has been reported by Li, Li, Yang, and Zeng (2013) to increase the payload capacity and visual quality. In recent years, Prediction-Error Expansion (PEE) (Thodi & Rodriguez, 2007) has been used in watermarking schemes as an improvement of DE. Li, Yang, and Zeng (2011) presented an adaptive embedding mechanism for increment in capacity and a pixel selection technique for visual quality enhancement based on PEE. The efficiency of PEE is further improved by leveraging the spatial correlation among color channels, as shown by Li, Li, and Yang (2012). Concretely, it is shown that more data can be hidden in the host image by using gradient information to enhance the prediction accuracy.

Due to the shortcomings of watermarking in the spatial domain, i.e., perceptible changes in the original image or fragility to image processing operations, most image watermarking techniques operate on a more robust transformed domain. Commonly used transformations are the Cosine transform (Lin & Chen, 2000), Fourier transform (Tsui et al., 2008; Wang, Han, & J.-C. Huang, 2007; Xiang-yang et al., 2013), Contourlet transform (Luo, Wei, & Liu, 2013; Niu, Wang, Yang, & Lu, 2011; Song et al., 2008), Curvelet

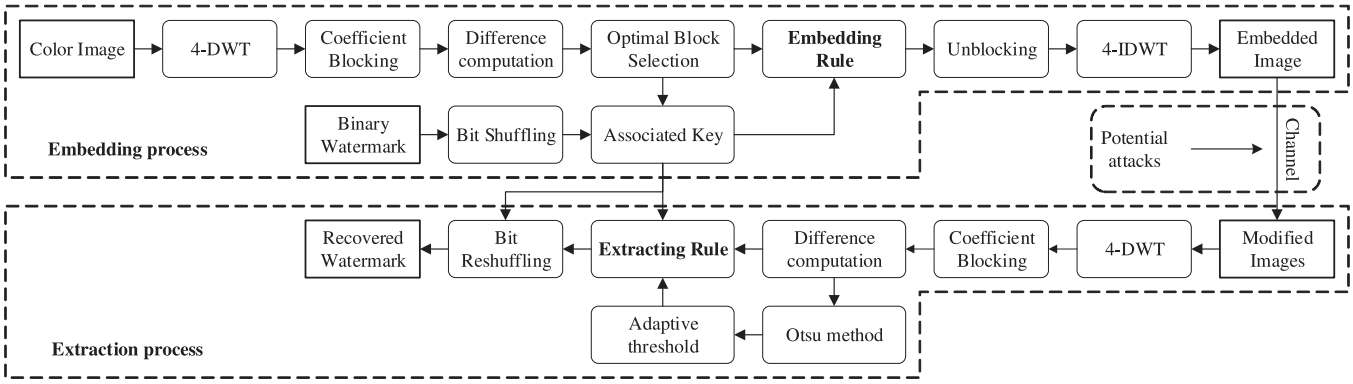

Fig. 1. Proposed watermarking model flowchart.

transform (Zhang, Cheng, Qiu, & Cheng, 2008) and Wavelet transform (Bhatnagar et al., 2012; Dejey & Rajesh, 2011; Lin et al., 2008; Meerwald, Koidl, & Uhl, 2009; Nezhadarya et al., 2011; Run et al., 2011; Wang, Ni, & Huang, 2012). In the study of Lin and Chen (2000), the host image is divided into spatial blocks for applying a Discrete Cosine Transform (DCT) to embed a binary watermark. This technique stands out for its simplicity; however, the existing correlations among pixels of neighboring blocks are shown to affect the results of this approach. A combination of Fast Fourier Transform (FFT) and Log-Polar mapping (Araujo & Dias, 1996) was suggested by Wang et al. (2007) and Ridzon and Levicky (2008) to embed a watermark into the amplitude spectrum of the host image. Nevertheless, this method turns to be quite fragile to geometric distortions. In the non-blind model proposed by Tsui et al. (2008), two approaches based on Quaternion Fourier Transform (QFT) (Bas, Bihan, & Chassery, 2003) and Spatiochromatic DFT (SCDFT) (McCabe, Caelli, West, & Reeves, 2000) were used to convert the host image from the spatial domain to the frequency domain. Although both of them are robust against many digital signal processing operations, the perceptibility of the watermark is an important limitation. Xiang-yang et al. (2013) recently described a robust blind color image watermarking based on the combination of Discrete Fourier Transform (DFT) and Least Squares Support Vector Machine (LS-SVM) to counteract the effects of color-based attacks and geometric distortions. Main drawbacks of this scheme are the computational time required for the LS-SVM training model as well as the assessment of the pseudo-Zernike moments (Khotanzad & Hong, 1990) in the decoding stage. Contourlet transform (Do & Vetterli, 2005), typically used to efficiently represent contour and textures, has been also adopted to decompose the host image for data hiding. Song et al. (2008) spread a watermark into the four largest detail sub-bands by adjusting the coefficient strength. To resist geometric distortions, Nonsubsampled Contourlet Transform (NSCT) and Support Vector Regression (SVR) were combined by Niu et al. (2011). However, the quality of the watermarked images is quite poorer than in other approaches. NSCT was further merged with Particle Swarm Optimization (PSO) (Luo et al., 2013) to upgrade the performance of the watermarking procedure. Zhang et al. (2008) exploited the Curvelet transform to decompose the original image and encode the watermark bits into the middle-frequency sub-bands. However, the high computational cost of this approach represents a limitation for its use in real-time applications.

Particularly popular has become the use of the Wavelet transform due to its multiple uses in image processing. Lin et al. (2008) quantized the significant differences of grayscale image wavelet coefficients to embed a binary watermark. Although the method was shown to be robust to various signal processing operations, its security is severely compromised because of the simplicity of the embedding process. Also using a binary image as watermark, Run et al. (2011) developed a blind watermarking scheme using a quantization technique based on Wavelet Tree Analysis (WTA). However, this scheme cannot deal with some type of attacks as a consequence of using a constant threshold for the extraction process. Based on the combination of DWT and Fan Beam Transform (FBT) (Nagy & Kuba, 2006), Dejey and Rajesh (2011) proposed two non-blind watermarking schemes for color images using the luminance and chrominance channel. Both of them significantly improved imperceptibility; however, they actually needed to be developed as blind models to make them storage compliant. Nezhadarya et al. (2011) introduced an angle quantization watermarking scheme, called the Gradient Direction Watermarking (GDWM). The watermark bits are embedded into the direction gradient of DWT coefficients through the Absolute Angle Quantization Index Modulation technique (AAQIM). The method obtains superior robustness to various types of attacking operations when compared with other state-of-the-art approaches. Bhatnagar et al. (2012) suggested a robust watermarking method using the Fractional Wavelet Packet Transform (FWPT) for decomposition. The embedding algorithm is implemented based on the modification of singular values of non-overlapping blocks of host images in the wavelet domain. The sensitivity evaluation and analysis of the moment-based watermarking approaches were comprehensively summarized (Tsougenis, Papakostas, Koulouriotis, & Tourassis, 2012) based on the investigation of robustness, imperceptibility, and capacity to achieve the acceptable tradeoff.

3. New watermarking scheme for image authentication

The proposed watermarking scheme consists of a set of steps for the watermark embedding and extraction processes (Fig. 1). These steps are described next.

3.1. Watermark embedding process

The embedding process consists in encoding the watermark information in a transformed version of the host image, which is then recovered back to its original domain. Given a color host image, the first step of the watermark embedding process consists in transforming this image into a more robust domain, here the wavelet domain. To that end, a DWT is applied to each channel of the host image, i.e., red (R), green (G) and blue (B). The choice of the level of decomposition strictly relates to the robustness and amount of information that can be actually embedded into the image. In fact, the higher the decomposition level is, the more robust the hidden information will be, but also, the less information can be hidden. Moreover, the amount of information that can be embedded into a particular host image also depends on its size. It can

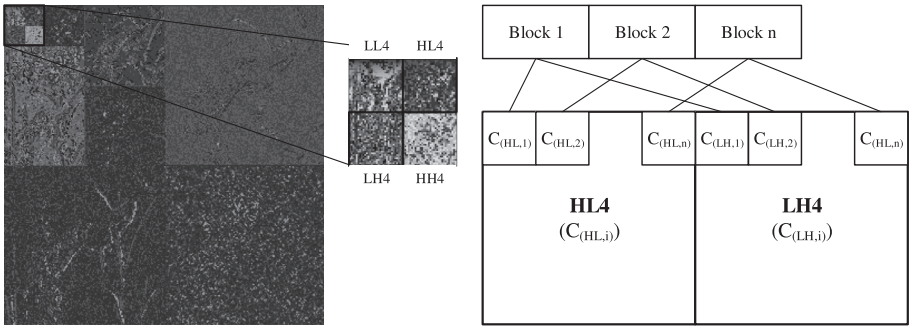

Fig. 2. Extraction and grouping of the 4-DWT LH and HL coefficients.

be simply derived that for a n-DWT decomposition, given a host image of $P \times R$ pixels, the watermark payload, i.e., the maximum number of binary bits that can be hidden in the host image, would be $N = \frac{P \times R}{2^{2n}}$. Accordingly, in this work we use a 4-DWT decomposition as a default setting, which is devised to provide a reasonable trade-off between robustness and payload. For this case, if an 512×512 host image is for example used, the watermark payload would be 1024 bits. However, it is important to note that the maximum number of embedded bits can be extended by degrading the decomposition level.

For each level of decomposition, four sub-bands are generated, respectively containing the approximation coefficients, LL, and detail coefficients, LH, HL and HH (horizontal, vertical, and diagonal). From these, only the two middle-frequency components, i.e., LH and HL, are used to effectively embed the watermark information, since LL coefficients are too much sensitive to noise and HH coefficients are easily eliminated during some image processing such as JPEG compression. Once both HL and LH coefficients are obtained, these are grouped as shown in Fig. 2. From here, the difference between LH and HL coefficients is computed for each channel as follows:

$$\Delta_{i,k} = \left| C_{LH_{i,k}} - C_{HL_{i,k}} \right| \tag{1}$$

where $C_{LH_{i,k}}$ and $C_{HL_{i,k}}$ represent the LH and HL coefficients of the ith wavelet block from the kth color channel.

In order to encode the information of the watermark into the LH and HL coefficients, a quantization technique is employed. Two quantization thresholds, δ_1 and δ_2 ($\delta_1 < \delta_2$), are respectively used to quantize the watermark bits w_i. The quantization technique seeks to set $\Delta_{i,k}$ to δ_1 if w_i is a 0-bit ($w_i = 0$), and to δ_2 or higher if w_i is a 1-bit ($w_i = 1$). To improve the quality of the eventual watermarked image, $C_{LH_{i,k}}$ and $C_{HL_{i,k}}$ coefficients are first sorted in ascending order of difference. We note in advance the sorted coefficient differences as $\Delta^S_{i,k}$. Accordingly, the coefficients with the smallest difference ($\Delta_{i,k}\downarrow$) will be used to code the 0-bits, while those with the greatest difference ($\Delta_{i,k}\uparrow$) will be used to code the 1-bits. Then, given N_0 the number of 0-bits in the watermark, δ_1 can be determined through averaging $\Delta^S_{i,k}$ across all channels and the first N_0 blocks:

$$\delta_1 = \frac{1}{N_0} \sum_{k=1}^{3} \sum_{i=1}^{N_0} \Delta^S_{i,k} \tag{2}$$

Being N_1 the number of 1-bits in the watermark, the value of δ_2 can be calculated as follows:

$$\delta_2 = \frac{1}{3} \sum_{k=1}^{3} \Delta^S_{i=\lambda N_1,k} \tag{3}$$

where λ is the robustness factor representing the strength of the watermark on the host image. The higher the λ value, the higher the δ_2 and vice versa. From these equations it can be clearly seen that the first N_0 sorted blocks are used for encoding the watermark 0-bits, while the remaining N_1 blocks are used for encoding the 1-bits (with $N = N_0 + N_1$). In order to increase the robustness of the embedding process, as well as to enrich the quality of the watermarked image, the quantization is not applied to all channels for all blocks. Rather than that, one specific channel is selected for each block during the codifications of the watermark bits. The selected channel, k^*, is simply the one which minimizes the difference between $\Delta^S_{i,k}$ and δ_1 for $w_i = 0$ and δ_2 for $w_i = 1$:

$$k^* = \begin{cases} \arg\min_k \left(\left| \Delta^S_{i,k} - \delta_1 \right| \right) & \forall\, w_i = 0 \\ \arg\min_k \left(\left| \Delta^S_{i,k} - \delta_2 \right| \right) & \forall\, w_i = 1 \end{cases} \tag{4}$$

This process is part of the so-called optimal block selection.

Now that the quantization thresholds are computed and also the optimal blocks are selected, the embedding rule to encode the watermark 0-bits and 1-bits can be simply described as follows:

- For $w_i = 0$:

$$\begin{aligned} C_{LH_{i,k^*}} \geq C_{HL_{i,k^*}} &\rightarrow C_{LH_{i,k^*}} = C_{LH_{i,k^*}} + \nabla^0_i \\ C_{LH_{i,k^*}} < C_{HL_{i,k^*}} &\rightarrow C_{HL_{i,k^*}} = C_{HL_{i,k^*}} + \nabla^0_i \end{aligned} \tag{5}$$

where $C_{LH_{i,k^*}}$ and $C_{HL_{i,k^*}}$ are the LH and HL coefficients of the ith wavelet block ($\forall i = 1, \ldots, N_0$) after sorting from the k^* channel. $\nabla^0_i = \delta_1 - \Delta^S_{i,k^*}$ represents the actual modification of the original coefficients required to encode the 0-bits.

- For $w_i = 1$:

If $\Delta^S_{i,k^*} < \delta_2$

$$\begin{aligned} C_{LH_{i,k^*}} \geq C_{HL_{i,k^*}} \rightarrow & \begin{cases} C_{LH_{i,k^*}} = C_{LH_{i,k^*}} + \nabla^1_i \\ C_{HL_{i,k^*}} = C_{HL_{i,k^*}} - \nabla^1_i \end{cases} \\ C_{LH_{i,k^*}} < C_{HL_{i,k^*}} \rightarrow & \begin{cases} C_{LH_{i,k^*}} = C_{LH_{i,k^*}} - \nabla^1_i \\ C_{HL_{i,k^*}} = C_{HL_{i,k^*}} + \nabla^1_i \end{cases} \end{aligned} \tag{6}$$

$\nabla^1_i = \delta_2 - \Delta^S_{i,k^*}$ the change that needs to be introduced in the original coefficients when encoding the 1-bits for the ith block ($\forall i = N_0 + 1, \ldots, N$) after sorting and N is the total of bits in the watermark.

If $\Delta^S_{i,k^*} \geq \delta_2$

$$\begin{aligned} C_{LH_{i,k^*}} &= C_{LH_{i,k^*}} \\ C_{HL_{i,k^*}} &= C_{HL_{i,k^*}} \end{aligned} \tag{7}$$

This quantization procedure could be applied to the watermark directly. However, for the sake of security, the watermark bits are initially shuffled as an example in Fig. 3 to encrypt the information by using a pseudorandom function with a seed. An associated key containing the information about the position of the watermark bits before shuffling and the corresponding channel blocks used for the codification of each pixel is generated. This key is used to recover the original watermark during the extraction process.

(a) (b)

Fig. 3. Watermark used for evaluation. (a) Original. (b) After shuffling.

After encoding the watermark into the image, the modified coefficients are reconstructed into the LH and HL sub-bands. Then, each color channel is recovered by using Inverse Discrete Wavelet Transform (IDWT). At this point, the watermarked image is ready.

The detailed embedding process is listed as follows:

- Input: A 512 × 512 color image and a 32 × 32 watermarking image.
- Output: A watermarked image.
- Step 1: A binary watermark is randomly shuffled firstly using a seed.
- Step 2: Three color channels of an original image are decomposed by the 4-level DWT.
- Step 3: The wavelet coefficients are grouped into blocks to compute the differences between LH and LH coefficients for each color channel by Eq. (1).
- Step 4: Calculate two quantization thresholds by Eq. (2) and (3).
- Step 5: Determine the optimal blocks at three channels through Eq. (4). Store the information of block information and the seed into the associated key.
- Step 6: Embed watermark bits into optimal wavelet blocks by the embedding algorithm using Eq. (5–7).
- Step 7: Transform the modified wavelet coefficients by using IDWT technique and obtain the watermarked image.

3.2. Watermark extraction process

A process very similar to the watermark embedding is used for extracting the watermark from the authenticated image. The watermarked image is 4-DWT decomposed to obtain its wavelet coefficients. Then, both LH and HL coefficients are grouped in blocks and the coefficient differences computed. From here, the blocks containing watermark information are simply identified by using the associated key. Although there are totally 3072 blocks generated from three color channels, only the 1024 optimal ones are selected for embedding. Clearly the extraction process cannot successfully be done without using the key because attackers do not know which blocks were used to the watermark. As described in the previous section, for $\Delta_{i,k} = \delta_1$ a 0-bit would be found, and a 1-bit for $\Delta_{i,k} \geq \delta_2$. Exploration of two peaks δ_1 and δ_2 through investigating the difference histogram of the embedded image is difficult (see Fig. 4). At worst, two quantization thresholds are interpolated, identification of embedded blocks cannot be completed based on the statistic approach. For example, for some blocks, the difference values may be greater than δ_2, even for all channels, are not used for 1-bit embedding.

Basically, δ_1 and δ_2 are unknown to the extraction model. Therefore, an empirical threshold, δ, must be determined based on the available information. This threshold, that must satisfy $\delta_1 < \delta < \delta_2$, may potentially vary from image to image, and also under the effects of image transformations. Thus, the authors propose the use of an adaptive threshold based on the Otsu method (Gonzalez & Woods, 2007) (see Appendix). This method, regularly used in the image segmentation, calculates the optimum threshold to separate an intensity distribution into two classes so that the intra-class variance is minimal. However, conversely to the segmentation case in which the pixel intensities are distributed in the fixed range [0,255], the coefficient differences may pertain a larger range. Moreover, the coefficient differences may be distributed across high values, with large zero bins that may potentially lead to an incorrect determination of the threshold (see Fig. 5). To solve this problem, the range of the original coefficient differences is compressed and the values adjusted before computing the threshold:

$$\bar{\Delta}_{i,k^*} = \begin{cases} \Delta_{i,k^*} & \forall\ \Delta_{i,k^*} \leq T \\ T & \forall\ \Delta_{i,k^*} > T \end{cases} \tag{8}$$

where T, the mean of the coefficient difference, is calculated as follows:

$$T = \frac{1}{N}\sum_{i=1}^{N} \Delta_{i,k^*} \tag{9}$$

Fig. 5 shows the scattered range in distribution and the computed thresholds in two cases of adjusting and non-adjusting the

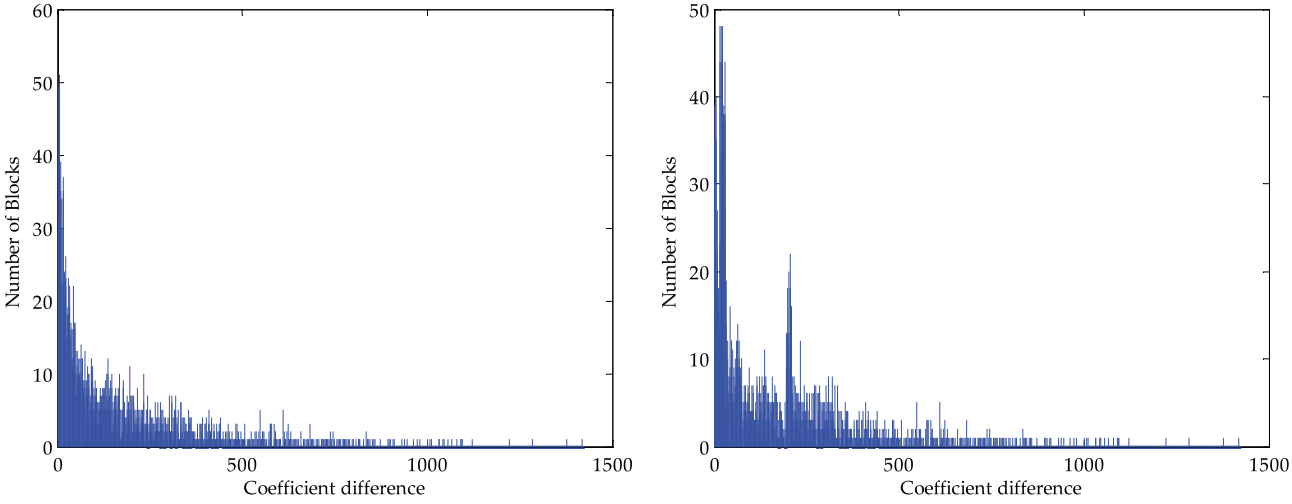

Fig. 4. Block distribution in difference value of: (a) the original image and (b) the embedded image.

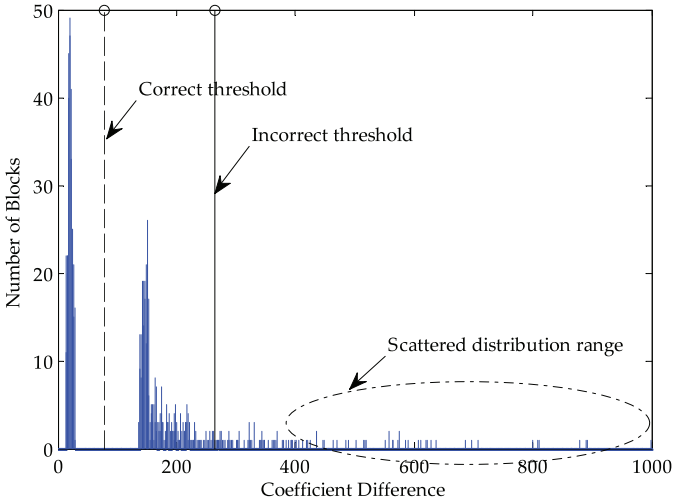

Fig. 5. Example of a large scattered distribution of the coefficients difference for selected blocks which is identified by the associated key. Determined threshold in case of using adjustment (dash line) or not (dot line).

coefficient difference by using (8). Finally, the Otsu-based threshold would be computed as follows:

$$\delta = \arg\min_{\bar{\Delta}} \left(\sigma_{\omega}^{2}\left(\bar{\Delta}_{i,k^*}\right)\right) \tag{10}$$

where $\sigma_{\omega}^{2}\left(\bar{\Delta}_{i,k^*}\right)$ represents the variance of the coefficients differences.

The watermark bits can be then simply extracted from the coefficient differences by comparing them to δ:

$$w_i = \begin{cases} 1 & \forall\ \Delta_{i,k^*} \geq \delta \\ 0 & otherwise \end{cases} \tag{11}$$

Finally, the recovered bit series need to be reshuffled to obtain the original binary watermark image, for which the key is used.

The detailed extraction process is listed as follows:

- Input: An embedded image.
- Output: A binary watermark image.
- Step 1: Three color channels of an embedded image are decomposed by the 4-level DWT.
- Step 2: The wavelet coefficients are grouped into blocks to compute the differences between LH and LH coefficients for each color channel.
- Step 3: Calculate the Otsu-based threshold by Eq. (8–10).
- Step 4: Identify the embedded blocks at three channels from the associated key.
- Step 5: Extract the watermark bits by using Eq. (11).
- Step 6: The extracted watermark is reshuffled with a seed stored in the associated key to obtain the binary watermark image.

4. Experimental results and discussion

The capabilities of digital watermarking schemes are commonly assessed by the imperceptibility of the inserted mark to human observers and the robustness of the mark to manipulations of the embedded image. Imperceptibility and robustness are coupled goals because increasing robustness normally translates into more alteration of the original image, the distortion which at some level may become perceptible. In this section, both imperceptibility after the embedment process and robustness after the extraction process are neatly evaluated.

4.1. Experimental setup

Several well-known color images from USC-SIPI-Database (1977), a widely used dataset in the image watermarking domain, are used to benchmark the proposed watermarking method. A total of eight color samples (512 × 512 pixels, 8 bits/pixel/channel) are used in the experimentation (see Fig. 6). The watermark used for evaluation is a 32 × 32 binary image containing information for authentication (see Fig. 3). This image fulfills the maximum watermark payload for the considered host images (1024 bits) at 4-level wavelet decomposition. The simplest wavelet family, Haar wavelet, is used for decomposition in the embedding and extraction processes. All experiments were performed on a desktop PC with 2.67 GHz Intel Core i5 CPU and 4GB RAM, running Windows 7. The software for simulation was MATLAB R2013a.

4.2. Evaluation metrics

For the watermark embedding process, the Color Peak Signal-To-Noise Ratio (CPSNR) is used to measure the quality of the watermarked image, i.e., the perceptibility of the watermark in the host image. The CPSNR is calculated as follows:

$$CPSNR = 10\log_{10}\left(\frac{255^2}{\frac{\sum_{k=1}^{3}\sum_{x=1}^{P}\sum_{y=1}^{R}\left(Q_k(x,y)-W_k(x,y)\right)^2}{3\times P\times R}}\right) \tag{12}$$

where P and R are the height and width of the original (O) and watermarked (W) image, and $O_k(x, y)$ and $W_k(x, y)$ the values of the pixel at the coordinate (x, y) for each channel k. Typically, the higher the CPSNR value the lower the perception of the watermark in the host image.

For the extraction process, the quantitative metric commonly used to estimate the performance of the extraction process is the Bit Error Rate (BER), which is calculated as follows:

$$BER = \frac{b}{p \times r} \tag{13}$$

where b is the number of erroneously detected bits and $p \times r$ is the size of the watermark The value of BER should converge to zero in case the original watermark is completely recovered.

4.3. Watermark perceptibility after embedment

This section analyzes the perceptibility of the watermark after embedment, otherwise, the visual quality of the watermarked image. To that end, the effect of the robustness factor λ is considered. As it was described in Section 3.2, λ represents the strength of the watermark into the host image. Concretely, this factor disturbs the second quantization threshold δ_2 calculation and further the 1-bits embedding performance. In theory, for low λ values, the robustness of the watermarked image decreases while its overall quality increases. The opposite is seen for high λ values. Table 2 shows this effect in a quantitative manner. In here, the CPSNR values obtained after embedment using various values of λ are displayed. Diverse textual images deliver different results, however, through analyzing the tendencies of CPSNR for all samples, it is confirmed that the quality of the output image degrades as λ increases. Therefore, the value of λ should be chosen to keep a pleasing tradeoff between the imperceptibility of watermarked images and the robustness of extracted watermarks. Based on the experimental evaluation, $\lambda = 0.5$ is selected hereafter.

A key asset of the proposed method consists of the selective embedding of the watermark information into the three host image channels. As shown in Table 3, this mechanism yields better

Fig. 6. Test images used for evaluation. (a) Airplane, (b) Girl, (c) House, (d) Lena, (e) Mandrill, (f) Peppers, (g) Sailboat, (h) Splash.

Table 2
Quality of the watermarked image - CPSNR (dB) in terms of robustness factor λ.

Image	Robustness factor				
	0.3	0.4	0.5	0.6	0.7
Airplane	55.26	50.95	45.81	41.33	36.68
Girl	58.97	57.01	53.13	49.12	44.87
House	50.51	46.75	43.41	39.74	36.22
Lena	57.68	52.88	48.17	43.07	39.56
Mandrill	52.04	49.98	46.75	43.64	40.21
Peppers	53.28	49.34	44.57	40.51	36.66
Sailboat	52.59	48.45	43.73	39.54	35.12
Barbara	48.91	45.34	42.84	39.11	35.42
Average	53.66	50.09	46.05	42.01	38.09

Table 3
Quality of the watermarked image - CPSNR (dB) in terms of embedding channel.

Image	Embedding channel ($\lambda = 0.5$)				
	3-channel	Luminance	Red	Green	Blue
Airplane	45.81	38.59	43.27	42.28	47.97
Girl	53.13	43.38	50.32	45.82	47.47
House	43.41	39.27	42.01	43.79	41.54
Lena	48.17	39.24	44.79	43.74	47.32
Mandrill	46.75	40.34	45.85	45.16	44.25
Peppers	44.57	38.08	45.91	40.55	42.80
Sailboat	43.73	35.69	45.12	38.59	40.54
Barbara	42.84	39.76	41.45	47.23	52.87
Average	46.05	39.29	44.84	43.39	45.60

results in overall than directly embedding the watermark into a single channel, either R-G-B or Y, the luminance channel in the YCbCr color space. This is motivated by the minimization of the distance between the coefficient values of each channel and the quantization thresholds, which allows us to reduce the modification of the host image.

The relationship between the quality of watermarked images and the embedding rate (ER) is extra investigated. In the proposed method, the embedding rate represents the payload capacity and depends on the wavelet decomposition level (described in Section 3.1). This parameter is identified as the ratio between the number of watermarked bits and the number of pixels in the host image. In theory, the more watermark bits are embedded, the lower imperceptibility of the watermark in the host image is produced because the host image has to be analyzed at a DWT lower-level. The quantitative results of CPSNR are reported in Table 4 for three cases of embedding rate ($ER = \frac{1}{256}$, $\frac{1}{64}$, and $\frac{1}{16}$ bpp) corresponding to three different sizes of the watermark (32 × 32, 64 × 64, 128 × 128) using 4, 3, and 2-level wavelet decomposition due to the maximum number of bits (see Section 3.1), respectively. After all, one of the most remarkable advantages of our method is the quality improvement for embedded images through an effective watermark bit spreading mechanism, in which the visual sensitivity and the payload capacity are compliantly managed.

Table 4
Quality of the watermarked image - CPSNR (dB) in terms of embedding rate.

Image	Embedding rate (*ER*)		
	$\frac{1}{256}$	$\frac{1}{64}$	$\frac{1}{16}$
Airplane	45.81	43.09	39.98
Girl	53.13	49.88	44.20
House	43.41	42.13	40.09
Lena	48.17	45.85	44.93
Mandrill	46.75	41.98	36.75
Peppers	44.57	41.54	40.02
Sailboat	43.73	41.81	38.85
Barbara	42.84	41.81	39.70
Average	46.05	43.51	40.57

4.4. Watermark robustness after extraction

This section explores the capability of the proposed model to recover the hidden information, as well as its resistance to a designated class of transformations or attacks. For the latter, popular digital image transformations are considered, here categorized into three types of attacks (see Fig. 7) with the illustration of Lena):

Geometric attacks:

- *Scaling*: resize the watermarked image from 512 × 512 to 64 × 64 and then restore it to its original size for the first test. The second test is from 512 × 512 to 1024 × 1024 and then restore again to the original size.
- *Cropping*: replace the top left 25% of the watermarked image with zeros.
- *Rotation*: rotate the embedded image by $\theta = 0.5^0$ and $\theta = 2^0$ in the counterclockwise.

Non-geometric attacks:

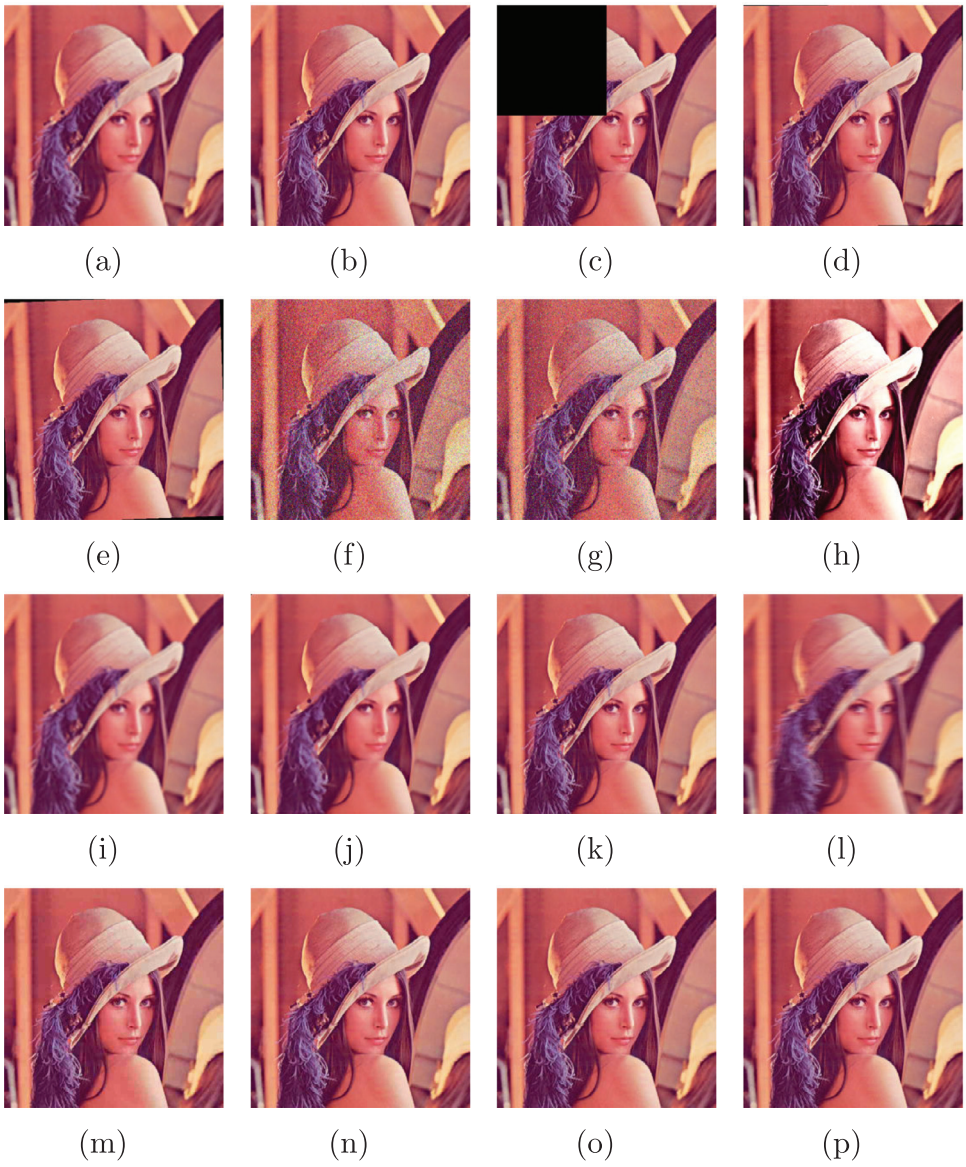

Fig. 7. Watermarked image subject to: (a) Scaling 64 × 64, (b) Scaling 1024 × 1024, (c) Cropping, (d) Rotation 0.5^0, (e) Rotation 2^0, (f) Gaussian noise, (g) Salt & pepper noise, (h) Histogram equalization, (i) Average filter, (j) Median filter, (k) Gaussian filter, (l) Motion blur, (m) JPEG Compression QF=30%, (n) QF=40%, (o) QF=50%, and (p) QF=70%.

- *Gaussian noise*: add Gaussian white noise to the embedded image with $\mu = 0$ and variance $\sigma^2 = 0.01$.
- *Salt & pepper noise*: add salt and pepper noise to the embedded image with a noise density $den = 0.01$, which approximately affects $den \times P \times R$ pixels.
- *Histogram equalization*: enhance the overall contrast of the image, only applied to the luminance channel.
- *Average filter*: 2-D average filtering by using a 7 × 7 pixel mask.
- *Median filter*: 2-D median filtering by using a 7 × 7 pixel mask.
- *Gaussian filter*: 2-D Gaussian low-pass filtering by using a 7 × 7 pixel mask with mean $\mu = 0$ and standard deviation $\sigma = 0.5$.
- *Motion blur*: 2-D linear filtering by using a 1 × 9 pixel mask.

Lossy JPEG compression: The last common operation used to evaluate the robustness is the lossy JPEG compression. The compression level is controlled through the parameter QF, which ranges from 0 to 100, where 0 refers to highest compression and lowest quality, and 100 to the opposite.

The BER values measured after extraction of the watermark for the aforementioned attacks are reported inTables 5–7. As it can be observed, in the absence of attacks the original watermark is perfectly recovered in all cases. Likewise, a very high robustness is shown for most types of attacks, with values close to absolute. Compared to scaling image resolution up 2 times, scaling resolution down 8 times from 512 × 512 to 64 × 64 brings the stronger attenuation of robustness. In the rotation attack, the number of correctly recovered bits will be reduced if the degree is increased. For the cases of Gaussian noise and Salt & Pepper noise, the variance factor and noise density mainly affect the extraction accuracy, for instance, a heavier intensity modification is emitted with a larger variance and more pixels are touched with a higher density. Average, Median and Gaussian filters are smoothing filters in image processing for the high-frequency noise elimination, therefore, the embedded information is insignificantly affected by them because the information hiding is performed on middle sub-bands. However, it is important to note that BER will be unexpectedly boosted whenever using a larger size of the mask. In Table 6, it can be seen that the extraction accuracy is improved following the increment of parameter QF in the lossy JPEG compression.

Table 5
BER values computed for the extracted watermark under geometric attacks.

Image	Non-attack	Scaling 64×64	Scaling 1024×1024	Cropping 25%	Rotation $\theta = 0.5^0$	Rotation $\theta = 2^0$
Airplane	0.000	0.053	0.006	0.130	0.094	0.242
Girl	0.000	0.024	0.001	0.104	0.075	0.236
House	0.000	0.042	0.002	0.150	0.085	0.246
Lena	0.000	0.041	0.000	0.119	0.054	0.232
Mandrill	0.000	0.083	0.000	0.147	0.133	0.279
Peppers	0.000	0.033	0.001	0.130	0.062	0.236
Sailboat	0.000	0.059	0.002	0.139	0.081	0.248
Barbara	0.000	0.077	0.000	0.117	0.077	0.246
Average	0.000	0.051	0.002	0.129	0.082	0.246

Table 6
BER values computed for the extracted watermark under non-geometric attacks.

Image	Gaussian noise	Salt& pepper	Histogram equalization	Average filter	Median filter	Gaussian filter	Motion blur
Airplane	0.027	0.005	0.190	0.022	0.039	0.000	0.020
Girl	0.086	0.016	0.126	0.010	0.038	0.000	0.011
House	0.004	0.000	0.127	0.006	0.020	0.000	0.011
Lena	0.023	0.003	0.069	0.011	0.016	0.000	0.017
Mandrill	0.032	0.006	0.107	0.030	0.056	0.000	0.021
Peppers	0.021	0.002	0.101	0.007	0.010	0.000	0.115
Sailboat	0.007	0.002	0.058	0.024	0.021	0.000	0.033
Barbara	0.033	0.016	0.133	0.027	0.021	0.000	0.020
Average	0.029	0.006	0.114	0.017	0.027	0.000	0.031

Table 7
BER values computed for the extracted watermark under lossy JPEG compression attacks.

Image	JPEG $QF = 30\%$	JPEG $QF = 40\%$	JPEG $QF = 50\%$	JPEG $QF = 70\%$
Airplane	0.023	0.008	0.004	0.000
Girl	0.040	0.019	0.012	0.004
House	0.006	0.001	0.000	0.000
Lena	0.010	0.003	0.002	0.000
Mandrill	0.037	0.022	0.002	0.000
Peppers	0.006	0.000	0.002	0.000
Sailboat	0.008	0.002	0.000	0.000
Barbara	0.043	0.017	0.002	0.000
Average	0.022	0.009	0.003	0.001

Nevertheless, the proposed model shows particular fragility to some operations such as cropping, rotation, and histogram equalization.

In the proposed method, the watermark bits are randomly encoded all over the host image from a spatial perspective. Accordingly, when part of the image is removed, as it happens to occur for the cropping attack, also part of the watermark information is potentially and inevitably lost. However, it is necessary to note that some 0-bits which are hidden in blocks belonging to cropped region can be correctly recovered because the modified coefficient differences are less than the Otsu threshold as Eq. (11). As a result, the BER values of cropping attack are mostly smaller the amount of removed area in the watermarked images. This is a well-known artifact of most watermarking techniques.

The proposed method cannot effectively cope with rotations because of the nature of the wavelet decomposition. This transformation operates in the horizontal and vertical dimensions of the image, thus, during the detection of the watermark, some of the encoded pixels are incorrectly determined, especially those embedded in areas close to the edges of the host image. Contourlet transform, a potential diagonal decomposition technique, is certainly applied to solve the problem of the rotation attack. However, an expensive computation is required because of its more complexity compared to Wavelet transform. The histogram equalization introduces modifications into the luminance channel, which in turn varies each color channel and correspondingly the embedded information. The influence of the equalization depends on the global contrast of the watermarked image. Therefore, low and high contrast images are particularly subject to important alteration, which translates into less resilience.

Moreover, different results are obtained for each image, thus confirming that the structure of the image also influences the robustness to some extent. For example, poor contrast images, such as airplane, are more strongly affected by the histogram equalization, which translates into low robustness values. Similarly, the effects of the Gaussian noise are more prominent in the latter image, which is observed to be quite homogeneous in terms of texture and color. Finally, as it could be expected, the effect of lossy JPEG compression becomes more harmful for decreasing the value of the quality factor, although a notable robustness is achieved for most cases.

The impact of the proposed optimal channel selection model is further investigated and compared with typical single channel schemes in terms of robustness. Table 8 shows the BER values obtained during the watermark extraction process for Lena sample, under various types of attacks and for different embedding channels. No significant differences are observed among the diverse embedding models, although the luminance channel appears to be slightly more robust than the others. In digital image watermarking, high robustness normally translates into low imperceptibility and vice versa. However, the noteworthy fact here is that the proposed approach attains a very high degree of imperceptibility (Table 3) while keeping a prominent level of robustness. Through the detailed experimental outcomes of the robustness validation, it can be seen that the color channel selection mechanism is capable not only in the imperceptibility improvement but also in the

Table 8
BER values of the extracted watermark for different embedding channels (results for the Lena sample).

Attacks	3-channel	Luminance	Red	Green	Blue
Scaling 64 × 64	0.041	0.040	0.053	0.050	0.040
Scaling 1024 × 1024	0.000	0.001	0.002	0.010	0.008
Cropping 25%	0.119	0.123	0.121	0.124	0.122
Rotation $\theta = 0.5^0$	0.054	0.055	0.065	0.047	0.059
Rotation $\theta = 2^0$	0.246	0.256	0.250	0.248	0.236
Gaussian noise $\sigma^2 = 0.01$	0.023	0.002	0.036	0.010	0.057
Salt & pepper $den = 0.01$	0.003	0.000	0.004	0.000	0.008
Histogram equalization	0.068	0.037	0.067	0.058	0.053
Average filter 7 × 7	0.011	0.011	0.012	0.009	0.012
Median filter 7 × 7	0.016	0.006	0.010	0.008	0.014
Gaussian filter 7 × 7	0.000	0.000	0.000	0.000	0.000
Motion blur $len = 9$	0.017	0.013	0.016	0.016	0.014
JPEG $QF = 30\%$	0.010	0.000	0.013	0.000	0.089
JPEG $QF = 40\%$	0.003	0.000	0.006	0.000	0.053
JPEG $QF = 50\%$	0.002	0.000	0.000	0.000	0.020
JPEG $QF = 70\%$	0.000	0.000	0.000	0.000	0.002

robustness enhancement against to most image processing operations.

4.5. Comparison with state-of-the-art methods

In this section, the authors compare the proposed method with some existing state-of-the-art methods, concretely, Chou and Liu (2010), Xiang-yang et al. (2013), Niu et al. (2011), Tsai and Sun (2007), Fu and Shen (2008), and Tsougenis, papakostas, Koulouriotis, and Karakasis (2014). These methods describe the watermarking schemes for color images using a binary watermark image without the requirement of the original image in the extraction process, so they can be essentially seen as blind watermarking techniques. However, a key containing side information generated in the embedding process is required for the extraction process. For example, an associated key comprising the coefficient block locations, full-band JND/MND profiles of three color channels, and permutation of the watermark image is required in Chou and Liu (2010). A single secret key is considered in the Arnold transform (Xiang-yang et al., 2013), the quantization process (Tsougenis et al., 2014), and the coefficient block selection (Niu et al., 2011) to enhance the security. A mixture key containing the copyright owner's privacy is also expressed in studies of Tsai and Sun (2007) and Fu and Shen (2008). Although presented under different manners, a secret key is firstly used to protect the watermark out of attackers and secondly support for the extraction process. The methods are compared in term of visual quality of the embedded images (Fig. 8) and robustness of the extracted watermarks under common attacks (Tables 9–11). As for Section 4.3, the CPSNR is used for comparing the imperceptibility of the watermark while the BER factor is particularly considered for the robustness assessment in average. The specification of some operations has been changed in order to fit with the characteristics of the attacks used in the related works, such as cropping 1%, rotation 5^0 - 15^0, Gaussian noise ($\sigma = 0.05$), and mask filters of dimension 3 × 3.

Three color images, Lena, Mandrill and Barbara, common in these works, are used for evaluation. Some previous works incurred in unfairness when comparing their approaches with other models, mainly because they used a more advantageous payload capacity (Niu et al., 2011; Tsougenis et al., 2014). In order to avoid so, this work categorizes the considered approaches in three groups, based on the embedding rate (ER), i.e., group 1, with $ER = \frac{1}{256}$ bpp (bits per pixel) including the studies of Fu and Niu; group 2, with $ER = \frac{1}{64}$ bpp including the approaches of Tsai and Tsougenis; and group3 with $ER = \frac{1}{16}$ bpp comprising the works of Chou and Wang. The scheme proposed here is compared with each group by using different sizes of the watermark to fit with each group requirements (32 × 32, 64 × 64, 128 × 128). For the proposed method, the embedding and extraction process have been modified to support more payload capacity. First, the wavelet decomposition is kept to 4-level for $ER = \frac{1}{256}$ bpp and changed to 3-level and 2-level for $ER = \frac{1}{64}$ and $ER = \frac{1}{16}$ bpp, respectively.

Table 9
Comparison between the proposed model and similar approaches (group 1) in terms of robustness.

Method	Fu	Niu	Proposed
Non-attack	0.0010	0.0120	0.0000
Scaling 1024 × 1024	0.5020	0.0240	0.0000
Cropping 1%	0.1040	0.0900	0.0010
Cropping 4%	0.1110	0.1120	0.0072
Rotation 5^0	0.5310	0.0230	0.3825
Gaussian N. $\sigma^2 = 0.006$	0.0730	0.0240	0.0078
Salt & pepper ($den = 0.003$)	0.0730	0.0200	0.0007
Median 3 × 3	0.0840	0.0200	0.0020
Gaussian 3 × 3	0.0650	0.0220	0.0000
Sharpening	0.0830	0.0320	0.0000
JPEG 30%	0.2830	0.0340	0.0163
JPEG 50%	0.2530	0.0290	0.0013
JPEG 70%	0.1930	0.0260	0.0000

Table 10
Comparison between the proposed model and similar approaches (group 2) in terms of robustness.

Method	Tsai	Tsougenis	Proposed
Non-attack	0.0038	0.0000	0.0000
Scaling 256 × 256	N/A	0.0937	0.0008
Scaling 1024 × 1024	0.5098	0.0033	0.0000
Cropping 1%	0.0667	0.0104	0.0008
Cropping 4%	0.0693	0.0778	0.0059
Rotation 5^0	0.5071	0.0036	0.4120
Rotation 15^0	N/A	0.0084	0.4577
Gaussian N. $\sigma^2 = 0.006$	0.1104	N/A	0.0918
Gaussian N. ($\sigma = 0.05$)	N/A	0.0729	0.0291
Salt & pepper ($den = 0.003$)	0.0554	N/A	0.0186
Salt & pepper ($den = 0.01$)	N/A	0.0003	0.0577
Average 3 × 3	N/A	0.0120	0.0050
Median 3 × 3	0.1530	0.0137	0.0098
Gaussian 3 × 3	0.1048	0.0000	0.0016
Blurring ($len = 6$)	N/A	0.0322	0.0314
Sharpening	0.0475	N/A	0.0042
JPEG 30%	0.3892	0.0765	0.0942
JPEG 40%	N/A	0.0667	0.0719
JPEG 50%	0.3167	0.0619	0.0583
JPEG 70%	0.2259	0.0238	0.0294

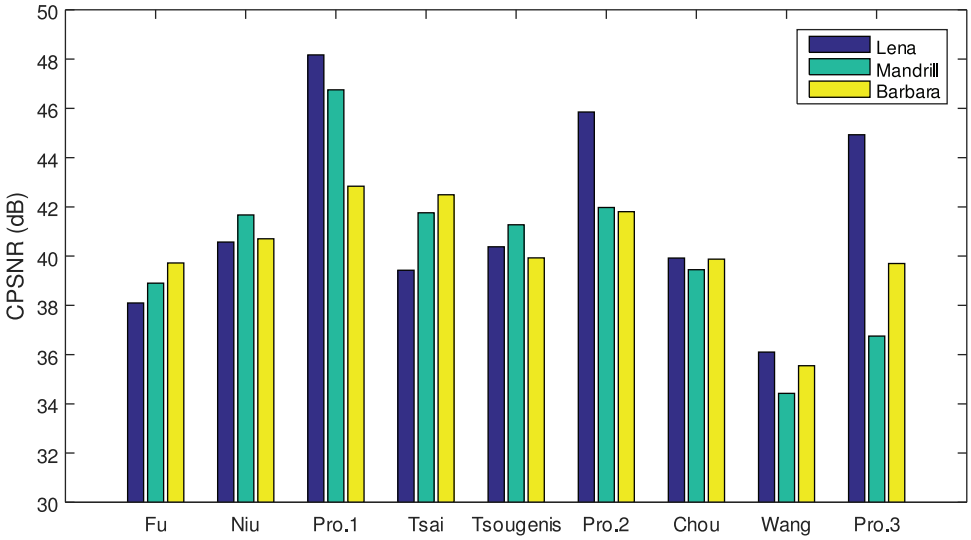

Fig. 8. Comparison between the proposed model and similar approaches in terms of perceptibility (CPSNR in dB). Fu, Niu, and proposed method (pro.1) are in the group 1 with $ER = \frac{1}{256}$ bpp. Tsai, Tsougenis, and proposed method (pro.2) are in the group 2 with $ER = \frac{1}{64}$ bpp. Chou, Wang, and proposed method (pro.3) are in the group 3 with $ER = \frac{1}{64}$ bpp.

Table 11
Comparison between the proposed model and similar approaches (group 3) in terms of robustness.

Method	Chou	Wang	Proposed
Non-attack	0.0117	0.0000	0.0000
Scaling 256 × 256	0.0563	0.1461	0.0240
Scaling 1024 × 1024	0.0262	0.4080	0.0000
Cropping 1%	0.0245	0.0000	0.0010
Cropping 4%	0.0622	0.0000	0.0058
Cropping 25%	N/A	0.0000	0.0435
Rotation 5^0	N/A	0.0243	0.3971
Rotation 15^0	N/A	0.0387	0.4425
Gaussian N. ($\sigma = 0.05$)	0.2252	0.0569	0.1324
Salt & pepper ($den = 0.01$)	0.0771	0.0220	0.0411
Histogram equalization	N/A	0.0039	0.0869
Average 3 × 3	0.0587	0.0772	0.0560
Median 3 × 3	0.0561	0.0708	0.0616
Gaussian 3 × 3	N/A	0.0044	0.0053
Blurring ($len = 6$)	0.0443	0.0267	0.1936
Sharpening	N/A	0.1131	0.0130
JPEG 30%	0.1085	0.1160	0.1776
JPEG 40%	0.0947	0.0605	0.1546
JPEG 50%	0.0772	0.0333	0.1367
JPEG 70%	0.0594	0.0038	0.1088

Second, λ is increased to compensate the degradation in robustness experienced as a consequence of embedding the watermark into a lower level of decomposition. Accordingly, λ is set to 0.5, 0.6 and 0.7 for each group respectively to keep the balance between imperceptibility and robustness for the increasing watermark payloads.

In the term of imperceptibility, it can be said that the proposed method generally outperforms the other approaches. Results from group 1 show that the NSTC-based watermarking scheme presented by Niu provides a greater watermarked image quality than Fu's spatial technique, but both are largely exceeded by the method proposed here, with CPNSR values up to 10 dB higher. This is also observed for the group 2, with improvements greater than 5 dB for the Lena sample, although no important differences are observed for the other two images. In fact, Tsai's approach subtly overcomes the others for the Barbara sample. In the group 3, Wang's method proves to provide the poorest imperceptibility for the three testing images. The perceptually tuned color image watermarking scheme proposed by Chou obtains the highest performance for Mandrill and Barbara while the proposed method significantly surpasses the others for the Lena case.

With respect to robustness, the LDA approach used in Fu's method to watermark images in the spatial domain proves to be particularly fragile to geometric attacks such as scaling, cropping and rotation, as well as to lossy JPEG compression. The watermarking scheme of Niu offers better robustness for most operations, but nevertheless, it also shows important limitations when dealing with cropping. In addition, this scheme presents special computational cost for the SVR training for the extraction process. This limitation is also shared by the method of Tsai, which further shows important fragility to scaling, rotation, filtering, and lossy JPEG compression operations, since it builds on the spatial domain like Fu's approach. Geometric transformations such as scaling and rotation can be counteracted through the *Theta* angle and *Alpha* factor of Tsougenis's approach, thus increasing the resilience to these attacks. However, this method seems to be weak to cropping, filtering and compression processes, the limitation shared with other methods that also operate in the Fourier transform domain. Chou's method provides low robustness to geometric distortions and Gaussian noise addition operations. In the study of Wang, the pseudo-Zernike moments obtained through LS-SVM geometric correction is utilized to maximize the imperceptibility. The enhancement is observed for most geometric operations, but for the scaling attack, for which this approach appears to be particularly fragile. Although the scheme proves to be robust to most common signal processing operations, the expensive computation required for the training of the SVM classifier turns to be a practical drawback. In broad strokes, the proposed model outperforms the others, especially those of groups 1 and 2 under most attacks. For group 3, the model shows better results than Chou's approach, although it is surpassed by Wang's technique, which nevertheless was shown to provide low imperceptibility capabilities. In fact, the most important characteristic of the proposed method is the flexible balance provided in terms of both imperceptibility and robustness, which is observed to outperform the rest of compared approaches.

4.6. Computational assessment

Digital image watermarking approaches are seldom evaluated in terms of computation cost. This is particularly important when

Table 12
Average computation time (in second) of the proposed method.

Host image	watermark	Embedding time	Extraction time
512 × 512	32 × 32	0.441	0.318
1024 × 1024	64 × 64	1.291	0.644
2048 × 2048	128 × 128	5.509	2.239
4096 × 4096	256 × 256	24.707	8.580

dealing with applications devised to operate on a real-time basis. Hence, this section analyzes the time required for both embedding and extraction processes of the proposed model. To that end, ER is set to $\frac{1}{256}$ bpp and host images and watermarks scaled with respect to the original size used in previous evaluations of this work (512 × 512 and 32 × 32, respectively). The invested time is computed through a profiling tool included in Matlab 2013a. Results are shown in Table 12. As it can be observed, for regular sizes such as 512 × 512, the time requested for both embedding and extraction is inferior to half a second. This corresponds to typical sizes used in most social network platforms, thus confirming the potential use of the proposed approach even for commonly used apps. As the size of both host image and watermark increases also, the computation time does. Reasonable times are obtained for host images of 1024 × 1024, while highly superior sizes, rarely used in this applications, require more intensive computation. Those cases can, in either case, benefit from parallel computing and distributed platforms, such as Cloud Computing, in order to highly expedite watermarking processes. Finally, it is worth noting that the embedding time is always greater than the extraction time. This is motivated by the fact that during the embedding both direct and inverse discrete wavelet transformations are used while the only direct transformation is utilized in the extraction process. Moreover, during the evaluation of both embedding and extraction processes, it was determined that more than 80% of the computation time falls on the wavelet transform.

5. Conclusions

An improved digital color image watermarking technique has been presented in this work. The embedding process consists of encoding a binary image containing the watermark information into the DWT coefficients of middle sub-bands of the host image. An optimal color channel selection procedure is defined to quantize the wavelet coefficients based on the value of a binary watermark. This color channel selection mechanism is proved to be a key advantage of this model since it improves the quality of the watermarked images. The watermark is automatically extracted by using an adaptive threshold approach based on the Otsu method, which is shown to be applicable in different cases of image attacks. The experimental results from the simulation demonstrate that the proposed method generates embedded images which are imperceptible to the human vision. Likewise, the embedding mechanism allows for a very robust recovery of the watermark even when the embedded image is subject to harsh image attacks. The proposed approach also generally outperforms other similar watermarking approaches after an equitable comparison for different embedding rates and settings. The proposed model can be perfectly integrated as part of regular applications used for creation, curation and sharing of digital images, although next steps need to seek computational refinement to deal with more demanding problems.

In the future, Contourlet transform becomes a good candidate to replace the Wavelet transform in the image decomposition. Moreover, the balance between robustness and imperceptibility should be managed better with Ant Colony Optimization (ACO) or Particle Swarm Optimization (PSO) algorithms that can be effectively operated in calculating a robustness factor. In recent years, Deep Learning (DL) is considered as a strong solution for many image processing applications even image watermarking, however, big computing for big data is a practical challenge, especially with multidimensional data likes images.

Appendix A. The Otsu algorithm

This appendix briefly describes the utilization of the Otsu algorithm (Gonzalez & Woods, 2007) to determine the optimal threshold in the watermark extraction process. Coefficient differences are encoded into two classes, respectively corresponding to 0-bit and 1-bit of the watermark, and distributionally separated by this threshold. In the Otsu algorithm, the threshold is calculated by exhaustively seeking to minimize the intra-class variance, which is defined as the weighted sum of variances of the two classes:

$$\sigma_\omega^2\left(\bar{\Delta}_{i,k^*}\right) = \omega_0\left(\bar{\Delta}_{i,k^*}\right)\sigma_0^2\left(\bar{\Delta}_{i,k^*}\right) + \omega_1\left(\bar{\Delta}_{i,k^*}\right)\sigma_1^2\left(\bar{\Delta}_{i,k^*}\right) \tag{A.1}$$

where 0-bit and 1-bit class probabilities ω_0 and ω_1 at value $\bar{\Delta}_{i,k^*}$ are:

$$\begin{aligned} \omega_0\left(\bar{\Delta}_{i,k^*}\right) &= \sum_{d=1}^{\bar{\Delta}_{i,k^*}} p(d) \\ \omega_1\left(\bar{\Delta}_{i,k^*}\right) &= \sum_{d=\bar{\Delta}_{i,k^*}+1}^{\max\left(\bar{\Delta}_{i,k^*}\right)} p(d) \end{aligned} \tag{A.2}$$

with $p(d)$ the probability density function of coefficient block at the coefficient difference d. The individual class variances are calculated as follows:

$$\begin{aligned} \sigma_0^2\left(\bar{\Delta}_{i,k^*}\right) &= \sum_{d=1}^{\bar{\Delta}_{i,k^*}} \left(\left(d-\mu_0\left(\bar{\Delta}_{i,k^*}\right)\right)^2 \frac{p(d)}{\omega_0\left(\bar{\Delta}_{i,k^*}\right)}\right) \\ \sigma_1^2\left(\bar{\Delta}_{i,k^*}\right) &= \sum_{d=\bar{\Delta}_{i,k^*}+1}^{\max\left(\bar{\Delta}_{i,k^*}\right)} \left(\left(d-\mu_1\left(\bar{\Delta}_{i,k^*}\right)\right)^2 \frac{p(d)}{\omega_1\left(\bar{\Delta}_{i,k^*}\right)}\right) \end{aligned} \tag{A.3}$$

where the means of 0-bit and 1-bit classes are given by:

$$\begin{aligned} \mu_0\left(\bar{\Delta}_{i,k^*}\right) &= \sum_{d=1}^{\bar{\Delta}_{i,k^*}} \frac{d\times p(d)}{\omega_0\left(\bar{\Delta}_{i,k^*}\right)} \\ \mu_1\left(\bar{\Delta}_{i,k^*}\right) &= \sum_{d=\bar{\Delta}_{i,k^*}+1}^{\max\left(\bar{\Delta}_{i,k^*}\right)} \frac{d\times p(d)}{\omega_1\left(\bar{\Delta}_{i,k^*}\right)} \end{aligned} \tag{A.4}$$

The Otsu threshold can be calculated then as follows:

$$\delta = \arg\min_{\bar{\Delta}} \left(\sigma_\omega^2\left(\bar{\Delta}_{i,k^*}\right)\right) \tag{A.5}$$

References

Araujo, H., & Dias, F. M. (1996). An introduction to the log-polar mapping. In *Proceedings of IEEE international workshop on cybernetic vision* (pp. 139–144).

Bas, P., Bihan, N. L., & Chassery, J.-M. (2003). Color watermarking using quaternion fourier transform. In *Proceedings of international conference on acoustics, speech, and signal processing* (pp. 521–525).

Bhatnagar, G., Raman, B., & Wu, Q. (2012). Robust watermarking using fractional wavelet packet transform. *IET Image Processing, 6*(4), 386–397.

Chou, C.-H., & Liu, K.-C. (2010). A perceptually tuned watermarking scheme for color images. *IEEE Transactions on Image Processing, 19*(11), 2966–2982.

Dadkhah, S., Manaf, A. A., Yoshiaki, Hassanien, A. E., & Sadeghi, S. (2014). An effective svd-based image tampering detection and self-recovery using active watermarking. *Signal Process - Image, 29*, 1197–1210.

Dejey, D., & Rajesh, R. (2011). Robust discrete wavelet-fan beam transforms-based colour image watermarking. *IET Image Processing, 5*(4), 315–322.

Do, M., & Vetterli, M. (2005). The contourlet transform: an efficient directional multiresolution image representation. *IEEE Transactions on Image Processing, 14*(12), 2091–2106.

Fu, Y.-G., & Shen, R.-M. (2008). Color image watermarking scheme based on linear discriminant analysis. *Computer Standards Interfaces, 30*, 115–120.

Ganic, E., & Eskicioglu, A. M. (2005). Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition. *Journal of Electronic Imaging, 14*, 043004–1–043004–10.

Gonzalez, R. C., & Woods, R. E. (2007). *Digital image processing*. Upper Saddle River, New Jersey: Prentice Hall.

Huynh-The, T., Banos, O., Lee, S., Yoon, Y., & Le-Tien, T. (2015). A novel watermarking scheme for image authentication in social networks. In *Proceedings of the 9th international conference on ubiquitous information management and communication*. In *IMCOM '15* (pp. 48:1–48:8).

Huynh-The, T., Lee, S., Pham-Chi, H., & Le-Tien, T. (2014). A dwt-based image watermarking approach using quantization on filtered blocks. In *Proceedings of international conference on advanced technologies for communication (ATC)* (pp. 280–285).

Khotanzad, A., & Hong, Y. H. (1990). Invariant image recognition by zernike moments. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 12*(5), 489–497.

Li, J., Li, X., & Yang, B. (2012). A new pee-based reversible watermarking algorithm for color image. In *Proceedings of IEEE international conference on image processing (ICIP)* (pp. 2181–2184).

Li, X., Li, B., Yang, B., & Zeng, T. (2013). General framework to histogram-shifting-based reversible data hiding. *IEEE Transactions on Image Processing, 22*(6), 2181–2191.

Li, X., Yang, B., & Zeng, T. (2011). Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection. *IEEE Transactions on Image Processing, 20*(12), 3524–3533.

Li, X., Zhang, W., Gui, X., & Yang, B. (2013). A novel reversible data hiding scheme based on two-dimensional difference-histogram modification. *IEEE Transactions on Information Forensics and Security, 8*(7), 1091–1100.

Lin, S., & Chen, C.-F. (2000). A robust dct-based watermarking for copyright protection. *IEEE Transactions on Consumer Electronics, 46*(3), 415–421.

Lin, W.-H., Horng, S.-J., Kao, T.-W., Fan, P., Lee, C.-L., & Pan, Y. (2008). An efficient watermarking method based on significant difference of wavelet coefficient quantization. *IEEE Transactions on Multimedia, 10*(5), 746–757.

Luo, P., Wei, P., & Liu, Y.-Q. (2013). A color digital watermarking in nonsampled contourlet domain using generic algorithm. In *Proceedings of IEEE international conference on intelligent networking and collaborative systems (INCoS)* (pp. 673–676).

McCabe, A., Caelli, T., West, G., & Reeves, A. (2000). Theory of spatiochromatic image coding and feature extraction. *Journal of the Optical Society of America A- Optics Image Science and Vision, 17*(10), 1744–1754.

Meerwald, P., Koidl, C., & Uhl, A. (2009). Attack on watermarking method based on significant difference of wavelet coefficient quantization. *IEEE Transactions on Multimedia, 11*(5), 1037–1041.

Nagy, A., & Kuba, A. (2006). Parameter settings for reconstructing binary matrices from fan-beam projections. *Journal of Computing and Information Technology, 14*(2), 101–110.

Nasir, I., Khelifi, F., Jiang, J., & Ipson, S. (2012). Robust image watermarking via geometrically invariant feature points and image normalisation. *IET Image Processing, 6*(4), 354–363.

Nezhadarya, E., Wang, Z., & Ward, R. (2011). Robust image watermarking based on multiscale gradient direction quantization. *IEEE Transactions on Information Forensics and Security, 6*(4), 1200–1213.

Niu, P.-P., Wang, X.-Y., Yang, Y.-P., & Lu, M.-Y. (2011). A novel color image watermarking scheme in nonsampled contourlet-domain. *Expert Systems with Applications, 38*(3), 2081–2098.

Ridzon, R., & Levicky, D. (2008). Robust digital watermarking in dft and lpm domain. In *Proceedings of IEEE 50th international symposium on ELMAR* (pp. 651–654).

Run, R.-S., Horng, S.-J., Lin, W.-H., Kao, T.-W., Fan, P., & Khan, M. K. (2011). An efficient wavelet-tree-based watermarking method. *Expert Systems Applications, 38*(12), 14357–14366.

Song, C., Sudirman, S., & Merabti, M. (2012). A robust region-adaptive dual image watermarking technique. *Journal of Visual Communication and Image Representation, 23*(4), 549–568.

Song, H., Yu, S., Yang, X., Song, L., & Wang, C. (2008). Contourlet-based image adaptive watermarking. *Signal Process-Image, 23*(3), 162–178.

Su, P.-C., Chang, Y.-C., & Wu, C.-Y. (2013). Geometrically resilient digital image watermarking by using interest point extraction and extended pilot signals. *IEEE Transactions on Information Forensics and Security, 8*(12), 1897–1908.

Thodi, D. M., & Rodriguez, J. (2007). Expansion embedding techniques for reversible watermarking. *IEEE Transactions on Image Processing, 16*(3), 721–730.

Tian, J. (2002). Reversible watermarking by difference expansion. In *Proceedings of international workshop on multimedia and security* (pp. 19–22).

Tian, J. (2003). Reversible data embedding using a difference expansion. *IEEE Transactions on Circuits and Systems for Video Technology, 13*(8), 890–896.

Tsai, H.-H., & Sun, D.-W. (2007). Color image watermark extraction based on support vector machine. *Information Sciences, 177*, 550–569.

Tsai, J.-S., Huang, W.-B., & Kuo, Y.-H. (2011). On the selection of optimal feature region set for robust digital image watermarking. *IEEE Transactions on Image Processing, 20*(3), 735–743.

Tsougenis, E., papakostas, G., Koulouriotis, D., & Karakasis, E. (2014). Adaptive color image watermarking by the use of quaternion image moments. *Expert Systems with Applications, 41*, 6408–6418.

Tsougenis, E., Papakostas, G., Koulouriotis, D., & Tourassis, V. (2012). Performance evaluation of moment-based watermarking methods: A review. *Journal of Systems and Software, 85*(8), 1864–1884.

Tsui, T. K., Zhang, X.-P., & Androutsos, D. (2008). Color image watermarking using multidimensional fourier transforms. *IEEE Transactions on Information Forensics and Security, 3*(1), 16–28.

USC-SIPI-Database (1977). Image database. [online]. available: http://sipi.usc.edu/database/.

Wang, B., Han, G.-Q., Huang, J.-C., Hou, A.-M., & Chao, Q. (2007). A robust blind algorithm for color image watermarking. In *Proceedings of IEEE international conference on control and automation (ICCA)* (pp. 142–146).

Wang, C., Ni, J., & Huang, J. (2012). An informed watermarking scheme using hidden Markov model in the wavelet domain. *IEEE Transactions on Information Forensics and Security, 7*(3), 853–867.

Xiang-yang, W., Chun-peng, W., Hong-ying, Y., & Pan-pan, N. (2013). A robust blind color image watermarking in quaternion fourier transform domain. *Journal of Systems and Software, 86*(2), 255–277.

Yamato, K., Hasegawa, M., Tanaka, Y., & Kato, S. (2012). Digital image watermarking method using between-class variance. In *Proceedings of IEEE international conference on image processing (ICIP)* (pp. 2185–2188).

Zhang, C., Cheng, L., Qiu, Z., & Cheng, L. (2008). Multipurpose watermarking based on multiscale curvelet transform. *IEEE Transactions on Information Forensics and Security, 3*(4), 611–619.