This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2016.2556723, IEEE Access

Rank-Based Image Watermarking Method with High Embedding Capacity and Robustness

Tianrui Zong, Yong Xiang, *Senior Member, IEEE,* Song Guo, *Senior Member, IEEE,* and Yue Rong, *Senior Member, IEEE*

***Abstract*— This paper presents a novel rank-based method for image watermarking. In the watermark embedding process, the host image is divided into blocks, followed by 2-D discrete cosine transform (DCT). For each image block, a secret key is employed to randomly select a set of DCT coefficients suitable for watermark embedding. Watermark bits are inserted into an image block by modifying the set of DCT coefficients using a rank-based embedding rule. In the watermark detection process, the corresponding detection matrices are formed from the received image using the secret key. Afterwards, the watermark bits are extracted by checking the ranks of the detection matrices. Since the proposed watermarking method only uses two DCT coefficients to hide one watermark bit, it can achieve very high embedding capacity. Moreover, our method is free of host signal interference. This desired feature and the usage of an error buffer in watermark embedding result in high robustness against attacks. Theoretical analysis and experimental results demonstrate the effectiveness of the proposed method.**

***Index Terms*— Image watermarking, host signal interference, discrete cosine transform, high embedding capacity.**

I. Introduction

With the fast growth of communication networks and advances in multimedia processing technologies, multimedia piracy has become a serious problem. In an open network environment, digital watermarking is a promising technology to tackle multimedia data piracy. In digital watermarking, the watermark data (such as publisher information, user identity, file transaction/downloading records, etc.) are hidden into the actual multimedia object without affecting its normal usage. When necessary, the owners or law enforcement agencies can extract the watermark data, by using a secret key, to trace the source of illegal distribution. While digital watermarking can be applied to various multimedia data such as audio, image and video, this paper focuses on image watermarking.

In the context of image watermarking, imperceptibility, robustness, embedding capacity and security are of primary concerns. So far, various image watermarking schemes have been reported in the literature and many of them were built upon techniques related to histogram [1], [2], moment [3], [4], spatial feature regions [5], [6], spread spectrum (SS) [7]-[14] and quantization [15]-[21]. In many applications, such as covert communication, high embedding capacity is desired, while robustness against geometric attacks is not mainly concerned. Compared to the watermarking methods in [1]-[6], the methods based on SS and quantization can normally achieve higher embedding capacity under given imperceptibility and robustness.

The SS-based watermarking methods usually insert watermark bits into the host image as pseudo-random noise either additively or multiplicatively. The idea of SS-based watermarking originated from Cox's pioneer work [7]. The SS-based watermarking approach has simple watermark embedding and detection structure but it suffers from the problem of host signal interference (HSI). It is known that HSI can greatly degrade the performance of watermark detection, especially in the presence of attacks, and thus lower robustness. Cannons and Moulin used the hash information of the host image in both embedding and detection phases of SS-based watermarking to reject HSI [8] but the method in [8] is not blind. Many efforts have been made to develop blind SS-based methods to cope with HSI. Under the additive SS structure, the method in [9] reduced HSI by modulating the watermark energy based on the correlation between the host image and the watermark sequence. Its detection performance was further enhanced in [10] by utilizing the probability distribution function leakage of the detector. In [11] and [12], two types of new watermark detectors were proposed to tackle HSI, which exploit the hierarchical spatially adaptive image model and the multi-carrier concept, respectively. Under the multiplicative SS structure, some SS-based methods have also been developed to combat HSI [13], [14]. Whilst the methods in [9]-[14] can reduce HSI to certain extents, their performance deteriorates dramatically with the rise of embedding rate.

In quantization based watermarking methods, features are extracted from the host image and quantized to the lattice points to embed watermark sequences [15]-[17]. Compared to the SS-based methods, the methods in [15]-[17] do not have the HSI problem. However, they are vulnerable to the amplitude scaling attack. Pilot signals were used in [18] to tackle the amplitude scaling attack but pilot signals can be easily detected and thus removed. In [19], the modified Watson's perceptual model, which scales linearly with the amplitude scaling attack, was utilized to adaptively select the quantization amount. Nezhadarya *et al.* proposed a gradient direction watermarking method in [20] by uniformly quantizing the direction of gradient vectors. In [21], the host signal is divided into two parts and quantization is implemented in both parts, respectively. However, similar to the SS-based

T. Zong and Y. Xiang are with the School of Information Technology, Deakin University, Victoria 3125, Australia (e-mail: {tzong, yxiang}@deakin.edu.au).

S. Guo is with the Department of Computer Science and Engineering, The University of Aizu, Japan (e-mail: sguo@u-aizu.ac.jp).

Y. Rong is with the Department of Electrical and Computer Engineering, Curtin University, Bentley, WA 6102, Australia (e-mail: y.rong@curtin.edu.au).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2016.2556723, IEEE Access

watermarking methods, the quantization based watermarking methods do not perform well under high embedding rates.

In [22], Koch and Zhao proposed a method by modifying the relationship between three coefficients to embed one watermark bit. However, this method can only embed one watermark bit in each image block, which significantly limits its embedding capacity. In addition, since the watermark detection in [22] depends on a fixed detection threshold, it cannot work under the amplitude scaling attack with a factor smaller than 1 and is vulnerable to some other common attacks like noise addition.

In this paper, we present a novel rank-based image watermarking method to significantly increase embedding capacity while maintaining satisfactory imperceptibility and robustness against common attacks. In the proposed method, the 2-D discrete cosine transform (DCT) is applied to each image block to obtain the corresponding DCT coefficients. A secret key is utilized to randomly choose a set of DCT coefficients suitable for embedding watermarks. The embedding of watermark bits is carried out by altering the set of DCT coefficients using a rank-based embedding rule, where an error buffer is also utilized to deal with the errors caused by attacks. At the watermark detection end, we compute the DCT coefficients from the received image and then construct the detection matrices using the same secret key. The embedded watermark bits can be extracted by checking the ranks of the detection matrices. Compared with the existing image watermarking methods, the proposed method has much higher embedding capacity. At the same time, it has high perceptual quality and is robust against common attacks. The superior performance of our method is analyzed in theory and demonstrated by simulation results.

The remainder of the paper is organized as follows. Section II introduces the proposed image watermarking method. The robustness of the proposed method is analyzed in Section III. The simulation results are shown in Section IV. Section V concludes the paper.

II. Proposed method

The proposed image watermarking method is composed of two parts: watermark embedding and watermark detection. Figs. 1 and 2 show the watermark embedding process and detection process, respectively.

A. Watermark embedding

Consider a gray level host image $\mathbf{I}$ of size $R \times C$. Without loss of generality, $\mathbf{I}$ is partitioned into N non-overlapping blocks $\mathbf{I}_1, \mathbf{I}_2, \ldots, \mathbf{I}_N$, where the size of each block is $M \times M$ and M is a positive integer power of 2. The 2-D DCT is applied to each block to obtain the DCT counterparts $F\{\mathbf{I}_1\},\ F\{\mathbf{I}_2\},\ \ldots,\ F\{\mathbf{I}_N\}$ of dimension $M \times M$. Since low frequency components carry perceptually important information and high frequency components are vulnerable to image compression attack, it is appropriate and common to use the DCT coefficients corresponding to the middle frequency range for watermark embedding [23], [24]. In each block, we use a secret key to randomly select $2K$ suitable DCT coefficients to form a DCT coefficient set, where the purpose of using a secret key is to introduce security. Denote the length-$2K$ coefficient set in the nth block by

$$\mathbf{x}_n = [x_n(1), x_n(2), \ldots, x_n(2K)] \tag{1}$$

where $n = 1, 2, \ldots, N$. From $\mathbf{x}_n$, we can obtain K pairs of DCT coefficients $\mathbf{x}_{n,1}, \mathbf{x}_{n,2}, \ldots, \mathbf{x}_{n,K}$ with

$$\mathbf{x}_{n,k} = [x_n(2k-1), x_n(2k)] \tag{2}$$

where $k = 1, 2, \ldots, K$. Based on (1) and (2), it follows

$$\mathbf{x}_n = [\mathbf{x}_{n,1}, \mathbf{x}_{n,2}, \ldots, \mathbf{x}_{n,K}] \tag{3}$$

where $n = 1, 2, \ldots, N$. Each pair of DCT coefficients will be used to hide one watermark bit.

Let

$$\mathbf{w}_n = [w_n(1), w_n(2), \ldots, w_n(K)] \tag{4}$$

be the sequence of K watermark bits to be embedded into the nth image block, where the watermark bits $w_n(k),\ k = 1, 2, \ldots, K$ take values from $\{0, 1\}$. The total length of the watermark sequence is $N \times K$. Define the $2K \times 2K$ matrix

$$\mathbf{A}_n \triangleq \{A_n(i,j)\}_{1 \le i,j \le 2K} \tag{5}$$

and initiate it as a zero matrix. Let

$$\mathbf{E}_0 = \begin{bmatrix} 0.5 & 0.5 \\ 0.5 & 0.5 \end{bmatrix} \text{ and } \mathbf{E}_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{6}$$

Based on the values of the watermark bits, we update some entry values of $\mathbf{A}_n$ as follows:

$$\begin{bmatrix} A_n(2k-1, 2k-1) & A_n(2k-1, 2k) \\ A_n(2k, 2k-1) & A_n(2k, 2k) \end{bmatrix} = \begin{cases} \mathbf{E}_0, & \text{if } w_n(k) = 0 \\ \mathbf{E}_1, & \text{if } w_n(k) = 1 \end{cases} \tag{7}$$

for $k = 1, 2, \ldots, K$.

Also, define the $1 \times 2K$ vector

$$\mathbf{b}_n \triangleq \{b_n(i)\}_{1 \le i \le 2K} \tag{8}$$

and let

$$T_n(k) = T - |x_n(2k-1) - x_n(2k)| \tag{9}$$

where T is a threshold and $|\cdot|$ denotes the absolute function. For $k = 1, 2, \ldots, K$, the element values of $\mathbf{b}_n$ are set as follows:

- If $w_n(k) = 0$ or $T_n(k) \le 0$, then
$$[b_n(2k-1),\ b_n(2k)] = [0,\ 0]. \tag{10}$$
- If $w_n(k) = 1$ and $T_n(k) > 0$, then
$$[b_n(2k-1),\ b_n(2k)] = \begin{cases} [\alpha T_n(k),\ -\beta T_n(k)], & \text{if } x_n(2k-1) \ge x_n(2k) \\ [-\alpha T_n(k),\ \beta T_n(k)], & \text{if } x_n(2k-1) < x_n(2k) \end{cases} \tag{11}$$

where α and β are weighting parameters satisfying $\alpha \ge 0$, $\beta \ge 0$ and $\alpha + \beta = 1$.

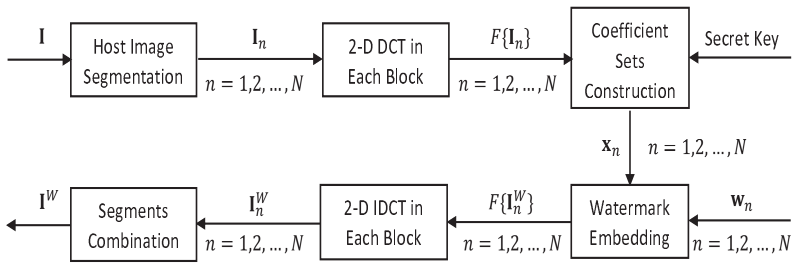

Fig. 1. Block diagram of watermark embedding process.

Let

$$\mathbf{x}_n^W = [x_n^W(1), x_n^W(2), \dots, x_n^W(2K)] \tag{12}$$

be the watermarked counterpart of $\mathbf{x}_n$. Given $\mathbf{A}_n$ and $\mathbf{b}_n$, the sequence of watermark bits $\mathbf{w}_n$ are embedded into $\mathbf{x}_n$ using the following embedding rule:

$$\mathbf{x}_n^W = \mathbf{x}_n \mathbf{A}_n + \mathbf{b}_n \tag{13}$$

where $n = 1, 2, \dots, N$. Here, $\mathbf{b}_n$ acts as an error buffer in the embedding of watermark bits. By replacing $\mathbf{x}_n$ in $F\{\mathbf{I}_n\}$ with $\mathbf{x}_n^W$, one can get the watermarked counterpart of $F\{\mathbf{I}_n\}$, denoted as $F\{\mathbf{I}_n^W\}$. After that, we apply the 2-D inverse discrete cosine transform (IDCT) to $F\{\mathbf{I}_n^W\}$ to obtain the watermarked image block $\mathbf{I}_n^W$. Finally, the watermarked image $\mathbf{I}^W$ can be constructed by combining all of the watermarked image blocks together.

Remark 1: The proposed watermark embedding scheme uses only two DCT coefficients to hide one watermark bit. As a result, high embedding capacity can be achieved. In contrast, those image watermarking methods reported in the literature like [12], [19] and [21] require more coefficients to embed one watermark bit; Otherwise, poor watermark detection performance is expected.

B. Watermark detection

Denote the received image as $\mathbf{I}'$. Similar to the embedding process, $\mathbf{I}'$ is divided into N non-overlapping blocks $\mathbf{I}'_1, \mathbf{I}'_2, \dots, \mathbf{I}'_N$ of dimension $M \times M$. Applying 2-D DCT to the received image blocks yields the corresponding DCT components $F\{\mathbf{I}'_1\}, F\{\mathbf{I}'_2\}, \dots, F\{\mathbf{I}'_N\}$ of dimension $M \times M$. In the nth block $F\{\mathbf{I}'_n\}$, the secret key can be used to find the length-$2K$ DCT coefficient set $\mathbf{x}'_n$ containing K watermark bits. Denoting

$$\mathbf{x}'_n = [x'_n(1), x'_n(2), \dots, x'_n(2K)] \tag{14}$$

one can sequentially compute

$$\bar{x}'_n(k) = |x'_n(2k-1) - x'_n(2k)| \tag{15}$$

and

$$T'_n(k) = \max\{\bar{x}'_n(k),\ T/2\}. \tag{16}$$

Based on $T'_n(k)$, we construct the following detection matrix for the extraction of the kth watermark bit in the nth block:

$$\mathbf{X}_{n,k} = \begin{bmatrix} T/2 & T'_n(k) \\ T'_n(k) & T/2 \end{bmatrix} \tag{17}$$

where $k = 1, 2, \dots, K$ and $n = 1, 2, \dots, N$.

In order to use $\mathbf{X}_{n,k}$ to extract the kth watermark bit in the nth block, let us analyze the property of $\mathbf{X}_{n,k}$ in the absence of attacks. Since attacks are absent, it is obvious that $\mathbf{I}' = \mathbf{I}^W$, which results in $\mathbf{x}'_n = \mathbf{x}_n^W$ or $x'_n(k) = x_n^W(k)$ with $k = 1, 2, \dots, K$ and $n = 1, 2, \dots, N$. The analysis is conducted under two scenarios: the watermark bit is “0” and the watermark bit is “1”.

1) The case of $w_n(k) = 0$: If $w_n(k) = 0$, it follows from (6), (7), (10) and (13) that

$$\begin{aligned} & [x_n^W(2k-1),\ x_n^W(2k)] \\ = & [x_n(2k-1),\ x_n(2k)] \cdot \mathbf{E}_0 + [b_n(2k-1),\ b_n(2k)] \\ = & \left[\frac{x_n(2k-1) + x_n(2k)}{2},\ \frac{x_n(2k-1) + x_n(2k)}{2}\right] \end{aligned} \tag{18}$$

which means

$$\left|x_n^W(2k-1) - x_n^W(2k)\right| = 0. \tag{19}$$

Since $x'_n(k) = x_n^W(k)$, it yields from (15) and (19) that

$$\bar{x}'_n(k) = 0. \tag{20}$$

Based on (16) and (20), it follows

$$\begin{aligned} T'_n(k) &= \max\{0,\ T/2\} \\ &= T/2. \end{aligned} \tag{21}$$

Substituting (21) into (17), we can see that the detection matrix $\mathbf{X}_{n,k}$ is rank deficient as its entries have the same value $T/2$.

2) The case of $w_n(k) = 1$: Without loss of generality, we first consider the situation of $w_n(k) = 1$, $T_n(k) > 0$ and $x_n(2k-1) \geq x_n(2k)$. From (6), (7), (11) and (13), we have

$$\begin{aligned} & [x'_n(2k-1),\ x'_n(2k)] \\ = & [x_n^W(2k-1),\ x_n^W(2k)] \\ = & [x_n(2k-1),\ x_n(2k)] \cdot \mathbf{E}_1 + [\alpha T_n(k),\ -\beta T_n(k)] \\ = & [x_n(2k-1) + \alpha T_n(k),\ x_n(2k) - \beta T_n(k)]. \end{aligned} \tag{22}$$

Recall that $\alpha + \beta = 1$. From (9), (15) and (22), it holds that

$$\begin{aligned} \bar{x}'_n(k) &= |(x_n(2k-1) + \alpha T_n(k)) - (x_n(2k) - \beta T_n(k))| \\ &= |(x_n(2k-1) - x_n(2k)) + (\alpha T_n(k) + \beta T_n(k))| \\ &= |T - T_n(k) + T_n(k)| \\ &= T. \end{aligned} \tag{23}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2016.2556723, IEEE Access

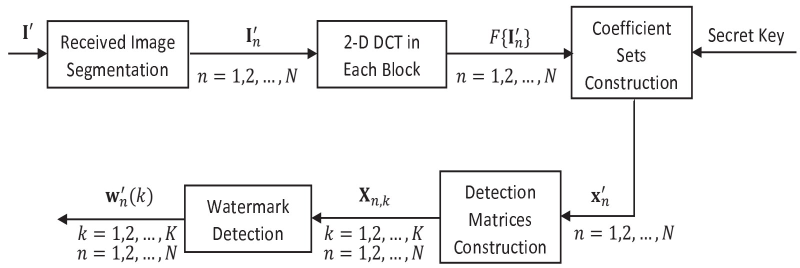

Fig. 2. Block diagram of watermark detection.

Combing (16) and (23), we obtain

$$\begin{aligned} T'_n(k) &= \max\{T,\ T/2\} \\ &= T. \end{aligned} \tag{24}$$

By substituting (24) into (17), one can see that the detection matrix $\mathbf{X}_{n,k}$ is of full rank.

Also, it can be verified that $\mathbf{X}_{n,k}$ has full rank in the situation of $w_n(k) = 1$, $T_n(k) > 0$ and $x_n(2k-1) < x_n(2k)$. Furthermore, it can be shown in a similar way that $\mathbf{X}_{n,k}$ has full rank when $w_n(k) = 1$ and $T_n(k) \le 0$. In summary, the detection matrix $\mathbf{X}_{n,k}$ is of full rank when $w_n(k) = 1$, regardless of the values of $T_n(k)$, $x_n(2k-1)$ and $x_n(2k)$.

Based on the property of $\mathbf{X}_{n,k}$, the kth watermark bit in the nth block can be extracted using the following detection rule:

$$w'_n(k) = \begin{cases} 1, & \text{if } \mathbf{X}_{n,k} \text{ is of full rank.} \\ 0, & \text{otherwise} \end{cases} \tag{25}$$

where $k = 1, 2, \ldots, K$ and $n = 1, 2, \ldots, N$. Finally, the extracted watermark sequences $\mathbf{w}'_1, \mathbf{w}'_2, \ldots, \mathbf{w}'_N$ can be obtained by combining all of the detected watermark bits.

Remark 2: In the proposed watermarking method, watermark detection is implemented by checking the ranks of the detection matrices, which makes our method free of HSI. This feature is important for achieving high detection rate. Moreover, the error buffer employed in the embedding process further enhances the detection performance as it can, to a large extent, tolerate the errors imposed by attacks.

C. Selection of watermarking parameters

In the proposed watermarking method, α, β and T are three important watermarking parameters and their values need to be properly chosen. The parameter T is the threshold of the error buffer, which is primarily introduced to resist Gaussian noise addition attack. The selection of T will be discussed in the analysis of robustness against Gaussian noise addition in Subsection III-A. So, we only discuss how to select α and β in this subsection.

The parameters α and β were introduced in (11) under the condition of $w_n(k) = 1$ and $T_n(k) > 0$. We first investigate the impact of α and β on perceptual quality. We assume, without loss of generality, that $x_n(2k-1) > x_n(2k)$. According to (11) and (13), embedding a watermark bit into the kth pair of DCT coefficients in the nth block under the above condition results in

$$x_n^W(2k-1) = x_n(2k-1) + \alpha T_n(k) \tag{26}$$

and

$$x_n^W(2k) = x_n(2k) - \beta T_n(k). \tag{27}$$

Alternatively, (26) and (27) can be expressed as

$$\begin{aligned} &F\left\{\mathbf{I}_n^W\left(p_n(2k-1), q_n(2k-1)\right)\right\} \\ =&F\left\{\mathbf{I}_n\left(p_n(2k-1), q_n(2k-1)\right)\right\} + \alpha T_n(k) \end{aligned} \tag{28}$$

and

$$\begin{aligned} &F\left\{\mathbf{I}_n^W\left(p_n(2k), q_n(2k)\right)\right\} \\ =&F\left\{\mathbf{I}_n\left(p_n(2k), q_n(2k)\right)\right\} - \beta T_n(k) \end{aligned} \tag{29}$$

where $(p_n(2k-1), q_n(2k-1))$ and $(p_n(2k), q_n(2k))$ are the indices of the DCT coefficients $x_n(2k-1)$ and $x_n(2k)$, respectively, and $(p_n(2k-1), q_n(2k-1)) \neq (p_n(2k), q_n(2k))$. Obviously, $p_n(2k-1)$, $p_n(2k)$, $q_n(2k-1)$ and $q_n(2k)$ are all nonnegative integers.

Applying the 2-D IDCT to $F\left\{\mathbf{I}_n^W\right\}$, which represents the DCT coefficients in the nth block, the corresponding watermarked image block in the spatial domain can be expressed as

$$\begin{aligned} \mathbf{I}_n^W(i,j) &= \sum_{u=0}^{M-1}\sum_{v=0}^{M-1} \vartheta_u \vartheta_v F\left\{\mathbf{I}_n^W(u,v)\right\} \cdot \\ &\quad \cos\frac{(2i+1)u\pi}{2M} \cos\frac{(2j+1)v\pi}{2M} \end{aligned} \tag{30}$$

where $0 \le i \le M-1$, $0 \le j \le M-1$ and

$$\vartheta_u = \begin{cases} \sqrt{1/M}, & u = 0 \\ \sqrt{2/M}, & u \neq 0 \end{cases}, \quad \vartheta_v = \begin{cases} \sqrt{1/M}, & v = 0 \\ \sqrt{2/M}, & v \neq 0 \end{cases}. \tag{31}$$

From (28)-(30), it follows:

$$\begin{aligned} \mathbf{I}_n^W(i,j) &= \mathbf{I}_n(i,j) + \alpha T_n(k) \vartheta_{p_n(2k-1)} \vartheta_{q_n(2k-1)} \cdot \\ &\quad \cos\frac{(2i+1)p_n(2k-1)\pi}{2M} \cdot \\ &\quad \cos\frac{(2j+1)q_n(2k-1)\pi}{2M} - \\ &\quad \beta T_n(k) \vartheta_{p_n(2k)} \vartheta_{q_n(2k)} \cos\frac{(2i+1)p_n(2k)\pi}{2M} \cdot \\ &\quad \cos\frac{(2j+1)q_n(2k)\pi}{2M} \\ &= \mathbf{I}_n(i,j) + \alpha T_n(k) S_{n,i,j}(2k-1) - \\ &\quad \beta T_n(k) S_{n,i,j}(2k). \end{aligned} \tag{32}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2016.2556723, IEEE Access

Here, the definitions of $S_{n,i,j}(2k-1)$ and $S_{n,i,j}(2k)$ can be easily seen from the second equation in (32).

Given the nth host image block $\mathbf{I}_n$ and its watermarked counterpart $\mathbf{I}_n^W$, we define the distortion caused by watermark embedding as

$$\boldsymbol{\Delta}_n = \sum_{i=0}^{M-1}\sum_{j=0}^{M-1}\left[\mathbf{I}_n^W(i,j) - \mathbf{I}_n(i,j)\right]^2. \tag{33}$$

By substituting (32) into (33), it yields

$$\begin{aligned}\boldsymbol{\Delta}_n &= \sum_{i=0}^{M-1}\sum_{j=0}^{M-1}[\alpha T_n(k)S_{n,i,j}(2k-1) - \\ &\quad \beta T_n(k)S_{n,i,j}(2k)]^2 \\ &= \alpha^2 T_n^2(k)\sum_{i=0}^{M-1}\sum_{j=0}^{M-1}S_{n,i,j}^2(2k-1) - \\ &\quad 2\alpha\beta T_n^2(k)\sum_{i=0}^{M-1}\sum_{j=0}^{M-1}S_{n,i,j}(2k-1)S_{n,i,j}(2k) + \\ &\quad \beta^2 T_n^2(k)\sum_{i=0}^{M-1}\sum_{j=0}^{M-1}S_{n,i,j}^2(2k).\end{aligned} \tag{34}$$

From the definition of $S_{n,i,j}(2k-1)$, we have

$$\begin{aligned}&\sum_{i=0}^{M-1}\sum_{j=0}^{M-1}S_{n,i,j}^2(2k-1) \\ &= \vartheta^2_{p_n(2k-1)}\vartheta^2_{q_n(2k-1)}\left(\sum_{i=0}^{M-1}\cos^2\frac{(2i+1)p_n(2k-1)\pi}{2M}\right)\cdot \\ &\quad \left(\sum_{j=0}^{M-1}\cos^2\frac{(2j+1)q_n(2k-1)\pi}{2M}\right) \\ &= \frac{\vartheta^2_{p_n(2k-1)}\vartheta^2_{q_n(2k-1)}}{4}\cdot \\ &\quad \left(\sum_{i=0}^{M-1}\cos\frac{(2i+1)\left(p_n(2k-1)+p_n(2k-1)\right)\pi}{2M} + \right. \\ &\quad \left.\sum_{i=0}^{M-1}\cos\frac{(2i+1)\left(p_n(2k-1)-p_n(2k-1)\right)\pi}{2M}\right)\cdot \\ &\quad \left(\sum_{j=0}^{M-1}\cos\frac{(2j+1)\left(q_n(2k-1)+q_n(2k-1)\right)\pi}{2M} + \right. \\ &\quad \left.\sum_{j=0}^{M-1}\cos\frac{(2j+1)\left(q_n(2k-1)-q_n(2k-1)\right)\pi}{2M}\right)\cdot \\ &= \frac{\vartheta^2_{p_n(2k-1)}\vartheta^2_{q_n(2k-1)}}{4}\cdot \\ &\quad \left(\sum_{i=0}^{M-1}\cos\frac{(2i+1)(2p_n(2k-1))\pi}{2M} + M\right)\cdot \\ &\quad \left(\sum_{j=0}^{M-1}\cos\frac{(2j+1)(2q_n(2k-1))\pi}{2M} + M\right).\end{aligned} \tag{35}$$

As will be shown in (63) and (64), $\sum_{i=0}^{M-1}\cos\frac{(2i+1)u\pi}{2M} = 0$ when $u \neq 0$ and $\sum_{j=0}^{M-1}\cos\frac{(2j+1)v\pi}{2M} = 0$ when $v \neq 0$. Based on (31), (35), (63) and (64), when $(p_n(2k-1), q_n(2k-1)) \neq (0,0)$, one has

$$\begin{aligned}\sum_{i=0}^{M-1}\sum_{j=0}^{M-1}S_{n,i,j}^2(2k-1) &= \frac{1}{M^2}\cdot(0+M)\cdot(0+M) \\ &= 1.\end{aligned} \tag{36}$$

Similarly, when $p_n(2k-1) \neq q_n(2k-1) = 0$ or $q_n(2k-1) \neq p_n(2k-1) = 0$, we obtain

$$\begin{aligned}\sum_{i=0}^{M-1}\sum_{j=0}^{M-1}S_{n,i,j}^2(2k-1) &= \frac{1}{2M^2}\cdot(M+M)\cdot(0+M) \\ &= 1.\end{aligned} \tag{37}$$

And when $p_n(2k-1) = q_n(2k-1) = 0$, it results in

$$\begin{aligned}\sum_{i=0}^{M-1}\sum_{j=0}^{M-1}S_{n,i,j}^2(2k-1) &= \frac{1}{4M^2}\cdot(2M)\cdot(2M) \\ &= 1.\end{aligned} \tag{38}$$

From (36)-(38), the first term on the right hand side of (34) can be written as

$$\alpha^2 T_n^2(k)\sum_{i=0}^{M-1}\sum_{j=0}^{M-1}S_{n,i,j}^2(2k-1) = \alpha^2 T_n^2(k). \tag{39}$$

Following the same way, the second term and third term on the right hand side of (34) can be respectively derived to be

$$2\alpha\beta T_n^2(k)\sum_{i=0}^{M-1}\sum_{j=0}^{M-1}S_{n,i,j}(2k-1)S_{n,i,j}(2k) = 0 \tag{40}$$

and

$$\beta^2 T_n^2(k)\sum_{i=0}^{M-1}\sum_{j=0}^{M-1}S_{n,i,j}^2(2k) = \beta^2 T_n^2(k). \tag{41}$$

Substituting (39)-(41) into (34), it follows:

$$\boldsymbol{\Delta}_n = T_n^2(k)\left(\alpha^2+\beta^2\right). \tag{42}$$

In order to ensure that the perceptual quality degradation caused by α and β is minimum, $\boldsymbol{\Delta}_n$ should be minimized. Recalling that $\alpha \geq 0$, $\beta \geq 0$ and $\alpha + \beta = 1$, (42) can be expanded as

$$\begin{aligned}\boldsymbol{\Delta}_n &= T_n^2(k)\cdot\left(\alpha^2+(1-\alpha)^2\right) \\ &= T_n^2(k)\cdot\left(2\alpha^2-2\alpha+1\right).\end{aligned} \tag{43}$$

Minimizing the above $\boldsymbol{\Delta}_n$ yields $\alpha = 0.5$, which leads to $\beta = 1-\alpha = 0.5$. Therefore, the desired α and β values are $\alpha = \beta = 0.5$ as they cause the minimum perceptual quality degradation on the image.

III. Analysis of robustness against attacks

The types of attacks considered in [19] include Gaussian noise addition, amplitude scaling, constant luminance change and compression. In this section, we analyze the robustness of the proposed method against these attacks.

A. Robustness against Gaussian noise addition

The robustness of the proposed method against Gaussian noise addition is facilitated by the error buffer term $\mathbf{b}_n$ in (13). This can be explained by showing the relationship between the error probability caused by Gaussian noise addition and the buffer threshold T. We assume that in the DCT domain, the Gaussian noise follows the normal distribution $Norm(0, \sigma^2)$ whose mean and variance are 0 and σ^2, respectively. Under a Gaussian noise addition attack, the kth pair of DCT coefficients in the nth block of the received image can be expressed as

$$\begin{cases} x'_n(2k-1) = x_n^W(2k-1) + \chi_n(2k-1) \\ x'_n(2k) = x_n^W(2k) + \chi_n(2k) \end{cases} \tag{44}$$

where $\chi_n(2k-1)$ and $\chi_n(2k)$ are the corresponding noise components.

Now, we inspect how noise affects the watermark detection result. When $w_n(k) = 0$, one has from (15), (19) and (44) that

$$\bar{x}'_n(k) = |\chi_n(2k-1) - \chi_n(2k)| . \tag{45}$$

According to (16), the detection error will occur when $|\chi_n(2k-1) - \chi_n(2k)| > T/2$, which means $\chi_n(2k-1) - \chi_n(2k) > T/2$ or $\chi_n(2k-1) - \chi_n(2k) < -T/2$. Since $\chi_n(2k-1) \sim Norm(0, \sigma^2)$ and $\chi_n(2k) \sim Norm(0, \sigma^2)$, then $\chi_n(2k-1) - \chi_n(2k) \sim Norm(0, 2\sigma^2)$. Hence, when $w_n(k) = 0$, the detection error probability can be calculated as

$$\begin{aligned} \Phi_0 &= \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{-\frac{T}{2\sqrt{2}\sigma}} e^{-t^2/2} dt + \frac{1}{\sqrt{2\pi}} \int_{\frac{T}{2\sqrt{2}\sigma}}^{\infty} e^{-t^2/2} dt \\ &= \frac{2}{\sqrt{2\pi}} \int_{-\infty}^{-\frac{T}{2\sqrt{2}\sigma}} e^{-t^2/2} dt. \end{aligned} \tag{46}$$

In a similar manner, we can show that when $w_n(k) = 1$ and $T_n(k) \leq 0$, the detection error probability is

$$\Phi_1 = \frac{1}{\sqrt{2\pi}} \int_{\frac{-3T+2T_n(k)}{2\sqrt{2}\sigma}}^{\frac{-T+2T_n(k)}{2\sqrt{2}\sigma}} e^{-t^2/2} dt. \tag{47}$$

And when $w_n(k) = 1$ and $T_n(k) > 0$, the detection error probability is

$$\Phi_2 = \frac{1}{\sqrt{2\pi}} \int_{\frac{-3T}{2\sqrt{2}\sigma}}^{\frac{-T}{2\sqrt{2}\sigma}} e^{-t^2/2} dt. \tag{48}$$

From (46)-(48), it is obvious that the buffer threshold T has a big impact on the detection error probability caused by Gaussian noise addition. In (46), the larger T is, the smaller Φ_0 is, which leads to higher robustness against Gaussian noise addition attack. In (47) and (48), when T is relatively small, Φ_1 and Φ_2 will increase with the rise of T. However, after certain T values, Φ_1 and Φ_2 will fall with the growth of T. For illustration purpose, Fig. 3 shows the plots of Φ_0, Φ_1 and Φ_2 versus T, where $\sigma = 1$ and $T_n(k) = -0.5$. It can be seen that good resistance against Gaussian noise addition can be obtained by setting T to a value much greater than $T = 1.5$. Therefore, by choosing a fairly large T value, the error buffer term $\mathbf{b}_n$ in (13) makes the proposed method robust to Gaussian noise addition attack. On the other hand, it can be seen from (9), (11) and (13) that increasing T will lower perceptual quality. A suitable T value can be chosen experimentally.

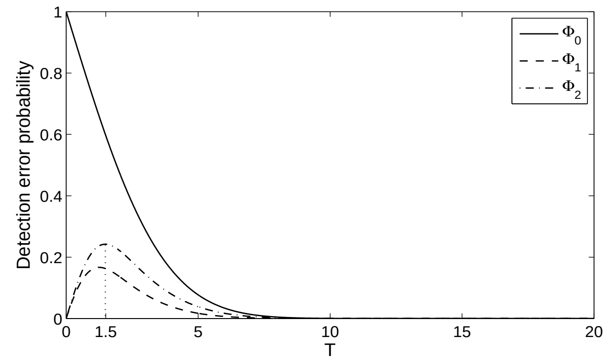

Fig. 3. The plots of Φ_0, Φ_1 and Φ_2 versus T, where $\sigma = 1$ and $T_n(k) = -0.5$.

B. Robustness against amplitude scaling

Assume that the watermarked image block $\mathbf{I}_n^W$ is scaled by a scaling factor η ($\eta > 0$). Under an amplitude scaling attack, one can express the kth pair of DCT coefficients in the nth block of the received image as

$$\begin{cases} x'_n(2k-1) = \eta \cdot x_n^W(2k-1) \\ x'_n(2k) = \eta \cdot x_n^W(2k) \end{cases} . \tag{49}$$

From (15), it follows

$$\bar{x}'_n(k) = \eta \cdot \left| x_n^W(2k-1) - x_n^W(2k) \right| . \tag{50}$$

When the embedded watermark bit $w_n(k) = 0$, it holds from (19) and (50) that $\bar{x}'_n(k) = 0$. Further, from (16) and (17), we obtain $T'_n(k) = \max\{0, T/2\} = T/2$ and $\mathbf{X}_{n,k} = \begin{bmatrix} T/2 & T/2 \\ T/2 & T/2 \end{bmatrix}$, respectively. Obviously, $\mathbf{X}_{n,k}$ is rank deficient. According to (25), the extracted watermark bit is "0", which is the expected result.

When the embedded watermark bit $w_n(k) = 1$, we can similarly show that $\bar{x}'_n(k) \geq T$. If $\eta > 0.5$, then $\eta \cdot \bar{x}'_n(k) > T/2$. From (16) and (17), it gives $T'_n(k) = \max\{\eta \cdot \bar{x}'_n(k), T/2\} = \eta \cdot \bar{x}'_n(k)$ and $\mathbf{X}_{n,k} = \begin{bmatrix} T/2 & \eta \cdot \bar{x}'_n(k) \\ \eta \cdot \bar{x}'_n(k) & T/2 \end{bmatrix}$. Since $\mathbf{X}_{n,k}$ is of full rank, the extracted watermark bit is "1", which is the desired result. On the other hand, if $\eta \leq 0.5$, there is the possibility that $\eta \cdot \bar{x}'_n(k) \leq \frac{T}{2}$. Since $T'_n(k) = T/2$ in this case, $\mathbf{X}_{n,k}$ will be rank deficient, which leads to incorrect watermark detection result. However, a scaling factor of 0.5 or even smaller can degrade the perceptual quality of the watermarked image significantly. Thus, such level of severe amplitude scaling attack is not desirable for the attackers. Therefore, in general, the proposed watermarking method has good resistance against amplitude scaling attacks.

C. Robustness against constant luminance change

Given the nth host image block $\mathbf{I}_n^W$ of size $M \times M$, the (u,v)th entry of the corresponding DCT counterpart $F\left\{\mathbf{I}_n^W\right\}$ can be computed by

$$F\left\{\mathbf{I}_n^W(u,v)\right\} = \sum_{i=0}^{M-1}\sum_{j=0}^{M-1} \vartheta_u \vartheta_v \mathbf{I}_n^W(i,j) \cdot \cos\frac{(2i+1)u\pi}{2M} \cos\frac{(2j+1)v\pi}{2M} \quad (51)$$

where i and j are the indices of pixels, u and v are the indices of the DCT coefficients, $0 \leq u \leq M-1$, $0 \leq v \leq M-1$, and ϑ_u and ϑ_v are defined in (31). Assume that $\mathbf{I}_n^W$ has undergone a constant luminance change of $+\delta$. Then, the (u,v)th pixel of the nth received image block $\mathbf{I}'_n$ can be expressed as

$$\mathbf{I}'_n(u,v) = \mathbf{I}_n^W(u,v) + \delta. \quad (52)$$

Applying 2-D DCT to the two sides of (52), one has

$$F\left\{\mathbf{I}'_n(u,v)\right\} = F\left\{\mathbf{I}_n^W(u,v)\right\} + \vartheta_u \vartheta_v \delta \cdot \sum_{i=0}^{M-1} \cos\frac{(2i+1)u\pi}{2M} \sum_{j=0}^{M-1} \cos\frac{(2j+1)v\pi}{2M}. \quad (53)$$

Now, let us have a closer look at the first cosine term in (53). Since M is a positive integer power of 2, $M/2$ is a positive integer. If u is a nonzero positive odd integer (i.e., $u = 1,3,5,\ldots$), it can be verified that

$$\left.\cos\frac{(2i+1)u\pi}{2M}\right|_{i=0,1,\ldots,M/2-1} = \left.-\cos\frac{(2i+1)u\pi}{2M}\right|_{i=M-1,M-2,\ldots,M/2}. \quad (54)$$

The verification of the equations in (54) is straightforward, as shown in the following two examples:

$$\begin{aligned}\left.\cos\frac{(2i+1)u\pi}{2M}\right|_{i=0} &= \cos\frac{u\pi}{2M} \\ &= -\cos\left(u\pi - \frac{u\pi}{2M}\right) \\ &= -\cos\frac{(2\cdot(M-1)+1)u\pi}{2M} \\ &= \left.-\cos\frac{(2i+1)u\pi}{2M}\right|_{i=M-1}\end{aligned}$$

and

$$\begin{aligned}\left.\cos\frac{(2i+1)u\pi}{2M}\right|_{i=M/2-1} &= \cos\frac{(M-1)u\pi}{2M} \\ &= -\cos\left(u\pi - \frac{(M-1)u\pi}{2M}\right) \\ &= -\cos\frac{(M+1)u\pi}{2M} \\ &= -\cos\frac{(2\cdot M/2+1)u\pi}{2M} \\ &= \left.-\cos\frac{(2i+1)u\pi}{2M}\right|_{i=M/2}.\end{aligned}$$

From (54), it follows

$$\sum_{i=0}^{M-1} \cos\frac{(2i+1)u\pi}{2M} = 0, \quad u = 1,3,5,\ldots. \quad (55)$$

On the other hand, if u is a nonzero positive even integer (i.e., $u = 2,4,6,\ldots$), similar to (54), it can be shown that

$$\left.\cos\frac{(2i+1)u\pi}{2M}\right|_{i=0,1,\ldots,M/2-1} = \left.\cos\frac{(2i+1)u\pi}{2M}\right|_{i=M-1,M-2,\ldots,M/2} \quad (56)$$

which leads to

$$\sum_{i=0}^{M-1} \cos\frac{(2i+1)u\pi}{2M} = 2\cdot\left(\sum_{i=0}^{M/2-1} \cos\frac{(2i+1)u\pi}{2M}\right). \quad (57)$$

Since u is a nonzero positive even integer, we can decompose it as $u = 2\cdot(u/2)$. If $u/2$ is also an even integer, we can further decompose u as $u = 2^2\cdot(u/2^2)$. In this way, we can eventually obtain

$$u = 2^m \cdot u' \quad (58)$$

where m is a nonzero positive integer and

$$u' = u/2^m \quad (59)$$

is a nonzero positive odd integer. For example, if $u = 56$, then the corresponding m and u' are 3 and 7, respectively. Now, we consider the decomposition of $\sum_{i=0}^{M-1}\cos\frac{(2i+1)u\pi}{2M}$. By repeatedly using (57), it results in

$$\begin{aligned}&\sum_{i=0}^{M-1} \cos\frac{(2i+1)u\pi}{2M} \\ =\ & 2\cdot\left(2\cdot\left(\sum_{i=0}^{(M/2)/2-1}\cos\frac{(2i+1)u\pi}{2M}\right)\right) \\ =\ & 2^2\cdot\left(\sum_{i=0}^{M/2^2-1}\cos\frac{(2i+1)u\pi}{2M}\right) \\ &\vdots \qquad \vdots \qquad \vdots \\ =\ & 2^m\cdot\left(\sum_{i=0}^{M/2^m-1}\cos\frac{(2i+1)u\pi}{2M}\right) \\ =\ & 2^m\cdot\left(\sum_{i=0}^{M/2^m-1}\cos\frac{(2i+1)\left(u/2^m\right)\pi}{2\cdot\left(M/2^m\right)}\right) \\ =\ & 2^m\cdot\left(\sum_{i=0}^{M'-1}\cos\frac{(2i+1)u'\pi}{2M'}\right) \end{aligned} \quad (60)$$

where

$$M' = M/2^m. \quad (61)$$

Recall that M is a positive integer power of 2 and $0 \leq u \leq M-1$. Since $u = 2^m \cdot u'$ and u' is a nonzero positive odd integer, it is clear that $u \geq 2^m$, which leads to $2^m \leq u \leq M-1$ or $2^m \leq u < M$. Based on the properties of M and u,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2016.2556723, IEEE Access

it is easy to verify that M' is also a positive power of 2 and $0 \leq u' \leq M'-1$. Moreover, since u' is a nonzero positive odd integer, from (55), it holds that $\sum_{i=0}^{M'-1} \cos \frac{(2i+1)u'\pi}{2M'} = 0$. In combination with (60), we obtain

$$\sum_{i=0}^{M-1} \cos \frac{(2i+1)u\pi}{2M} = 0, \quad u = 2, 4, 6, \ldots. \tag{62}$$

Based on (55) and (62), we can conclude that

$$\sum_{i=0}^{M-1} \cos \frac{(2i+1)u\pi}{2M} = 0 \;\text{ if } u \neq 0. \tag{63}$$

Similarly, it can be shown that

$$\sum_{j=0}^{M-1} \cos \frac{(2j+1)v\pi}{2M} = 0 \;\text{ if } v \neq 0. \tag{64}$$

Based on (53), (63) and (64), when $(u, v) \neq (0, 0)$,

$$F\left\{\mathbf{I}'_n(u, v)\right\} = F\left\{\mathbf{I}_n^W(u, v)\right\}. \tag{65}$$

This means that constant luminance change does not alter the DCT coefficients of the watermarked image block, except for the DCT coefficient at $(u, v) = (0, 0)$. As mentioned in Subsection II-A, only the DCT coefficients corresponding to the middle frequency range will be used to embed watermark bits, i.e., the DCT coefficient at $(u, v) = (0, 0)$ will not be utilized for watermark embedding. Therefore, the proposed method is robust against constant luminance change attack.

D. Robustness against compression

It is shown in [23] that image compression attack has more impact on the DCT coefficients relating to the region of high frequency. Moreover, the DCT coefficients associated with the middle frequency range are considered to be more robust against image compression attack [24]. In the proposed method, the resistance towards image compression attack results from using the DCT coefficients corresponding to the middle frequency region for watermark embedding. It is expected that increasing embedding rate will decrease the robustness to compression attacks. The reason is that in this scenario, some DCT coefficients outside the middle frequency region might have to be employed to embed watermarks.

IV. Simulation results

In this section, we evaluate the performance of the proposed image watermarking method by simulations, in comparison with the methods in [12], [19] and [21]. Eight standard 512 × 512 8-bit gray scale images *Bee*, *Elaine*, *Goldhill*, *Hill*, *Lena*, *Lighthouse*, *Truck*, and *Zelda* are used as host images, which are shown in the top two rows of Fig. 4. The peak signal-to-noise ratio (PSNR) index and the bit error rate (BER) index are used to measure perceptual quality and robustness, respectively. The performance indices PSNR and BER are calculated by averaging the results obtained from the eight images. Regarding imperceptibility, the larger PSNR value, the better perceptual quality. It is mentioned in [25] that the PSNR value of 40dB indicates good perceptual quality. For example, the bottom two rows of Fig. 4 show the watermarked counterparts of the afore-mentioned eight images by our method, where PSNR=40.32 dB. Clearly, there is no visual difference between the original images and their watermarked versions. With regard to robustness, a smaller BER value indicates better robustness, and vice versa.

Fig. 4. Upper two rows: original images *Bee*, *Elaine*, *Goldhill*, *Hill*, *Lena*, *Lighthouse*, *Truck*, and *Zelda*. Lower two rows: watermarked counterparts of these images, where PSNR=40.32 dB.

In the simulations, we choose $N = 4096$ for all images. Two embedding rates: 12288 and 20480 watermark bits per image are considered, which correspond to $K = 3$ and 5, respectively. As for T, in order to experimentally choose a suitable value, we embed 20480 watermark bits into each host image and then apply Gaussian noise addition to the watermarked images. Four different noise variances are considered, which are $\sigma^2 = 1, 4, 7$ and 10, respectively. The simulation results about robustness and perceptual quality are shown in Fig. 5. As expected, as T rises, BER decreases (or the resistance against Gaussian noise addition increases). Meanwhile, the perceptual quality, measured by PSNR, degrades with the escalation of T. To achieve satisfactory robustness while maintaining good perceptual quality, we choose $T = 15$ for our method.

TABLE I

PSNRs under different K values

Watermarking method	PSNR (dB)	
	$K = 3$	$K = 5$
Proposed method	42.51	40.32
Method in [12]	41.76	39.57
Method in [19]	39.93	39.80
Method in [21]	41.73	39.53

The robustness of our method and those in [12], [19] and [21] is compared under different K values. The comparison is conducted both in the absence and in the presence of attacks.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2016.2556723, IEEE Access

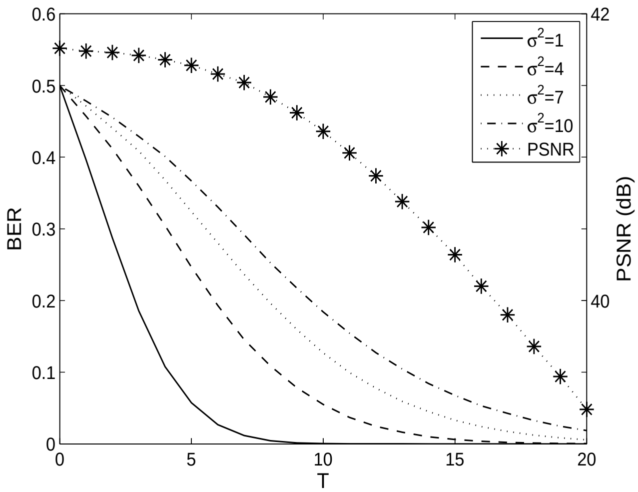

Fig. 5. BER (under Gaussian noise addition attack) and PSNR of the proposed method versus T, where the embedding rate is 20480 watermark bits per image.

Same as [19], the Gaussian noise addition, amplitude scaling, constant luminance change, and JPEG compression attacks are considered in the simulations. In order to have a fair comparison of robustness, we ensure that the watermarked images produced by our method have higher perceptual quality than those produced by the methods in [12], [19] and [21]. The PSNRs of the four watermarking methods under different K values are shown in Table I.

Tables II-VI show the BERs of the concerned watermarking methods. Specifically, Table II shows the results when attack is absent. For a watermarking method, its BER value obtained in the absence of attacks indicates the impact of HSI. Since HSI does not exist in the proposed method, perfect watermark detection can be achieved, regardless of the K values or equivalently the embedding rates. The quantization based methods [19] and [21] also show nearly perfect and perfect detection results, respectively. In contrast, the SS-based method [12] cannot reach zero BER due to the impact of HSI. Besides, its BER increases with the rise of K.

TABLE II

BERs UNDER DIFFERENT K VALUES, IN THE ABSENCE OF ATTACK

Value of K	Proposed method	Method in [12]	Method in [19]	Method in [21]
$K = 3$	0	0.0746	0.0001	0
$K = 5$	0	0.2435	0.0001	0

Table III shows the results when Gaussian noise addition attack is present. We can see that the proposed method performs much better than the methods in [12], [19] and [21] in all situations. Moreover, as K increases, the performance gap between our method and the other methods widens. The reason is that in the presence of Gaussian noise addition attack, the detection performance of the proposed method is determined by the threshold T used in the error buffer, which is irrelevant to embedding rates. On the contrary, the detection performance of the methods in [12], [19] and [21] degrades with the increase of embedding rates.

TABLE III

BERs UNDER DIFFERENT K VALUES, IN THE PRESENCE OF GAUSSIAN NOISE ADDITION ATTACK

Value of K	Noise variance σ^2	Proposed method	Method in [12]	Method in [19]	Method in [21]
$K = 3$	1	0.0001	0.0995	0.0306	0.0097
	4	0.0061	0.1438	0.1484	0.0495
	7	0.0329	0.1953	0.2119	0.0887
	10	0.0676	0.2348	0.2508	0.1250
$K = 5$	1	0.0001	0.2609	0.0607	0.0547
	4	0.0062	0.2798	0.2075	0.1412
	7	0.0329	0.3138	0.2737	0.1989
	10	0.0676	0.3388	0.3124	0.2425

The BERs of the four methods against amplitude scaling attack and constant luminance change attack are shown in Tables IV and V, respectively. It can be seen that the proposed method achieves zero BER under both attacks. This result is not surprising. As we have analyzed theoretically in Section III, our method can correctly extract watermarks in the presence of amplitude scaling attack so long as the scaling factor is greater than 0.5 and in the presence of constant luminance change attack if the DCT coefficient at $(u, v) = (0, 0)$ is not used for watermark embedding. The methods in [19] and [21], which are specifically designed to tackle amplitude scaling attack, also achieve almost perfect and perfect detection results, respectively, in the presence of amplitude scaling attack. However, they are not robust against constant luminance change attack. Regarding the method in [12], it is not robust against either of the two attacks.

TABLE IV

BERs UNDER DIFFERENT K VALUES, IN THE PRESENCE OF AMPLITUDE SCALING ATTACK

Value of K	Scaling factor	Proposed method	Method in [12]	Method in [19]	Method in [21]
$K = 3$	60%	0	0.0924	0.0001	0
	80%	0	0.0822	0.0001	0
	120%	0	0.0851	0.0001	0
	140%	0	0.0891	0.0001	0
$K = 5$	60%	0	0.2542	0.0001	0
	80%	0	0.2525	0.0001	0
	120%	0	0.2443	0.0001	0
	140%	0	0.2487	0.0001	0

TABLE V

BERs UNDER DIFFERENT K VALUES, IN THE PRESENCE OF CONSTANT LUMINANCE CHANGE ATTACK

Value of K	Luminance change	Proposed method	Method in [12]	Method in [19]	Method in [21]
$K = 3$	+10	0	0.0746	0.0024	0.2878
	-10	0	0.0770	0.0057	0.3329
	+30	0	0.0770	0.0213	0.4790
	-30	0	0.0910	0.1077	0.4989
$K = 5$	+10	0	0.2446	0.0051	0.3971
	-10	0	0.2494	0.0096	0.4398
	+30	0	0.2470	0.0395	0.4791
	-30	0	0.2529	0.1343	0.5000

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2016.2556723, IEEE Access

The impact of JPEG compression attack on the proposed method and the methods in [12], [19] and [21] is shown in Table VI. One can see that the proposed method and the method in [21] performs much better than the other two methods. Between the proposed method and the method in [21] themselves, they have comparable BERs when $K = 3$. However, in the case of $K = 5$, our method outperforms the latter by large margins.

TABLE VI
BERS UNDER DIFFERENT K VALUES, IN THE PRESENCE OF JPEG COMPRESSION ATTACK

Value of K	Quality factor	Proposed method	Method in [12]	Method in [19]	Method in [21]
$K = 3$	50	0.2644	0.4789	0.4553	0.2593
	70	0.1120	0.4738	0.4070	0.1513
	90	0.0007	0.3157	0.1946	0.0345
$K = 5$	50	0.2698	0.4829	0.4730	0.3577
	70	0.1191	0.4799	0.4380	0.2655
	90	0.0018	0.3785	0.2585	0.1138

V. CONCLUSION

In this paper, we proposed a novel method for image watermarking in the DCT domain. Thanks to the rank-based watermark embedding and detection rules, the proposed watermarking method possesses some desirable features. Firstly, our method can use as little as two DCT coefficients to embed one watermark bit. Secondly, it is free of HSI. Thirdly, it can considerably tolerate the errors caused by attacks. The first feature leads to high embedding capacity. The second and third features make the proposed method robust against common attacks. The superior performance of the new method was analyzed theoretically in detail and demonstrated by simulation results.

REFERENCES

[1] S. Xiang, H. J. Kim, and J. Huang, "Invariant image watermarking based on statistical features in the low-frequency domain," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 18, no. 6, pp. 777–790, Jun. 2008.

[2] T. Zong, Y. Xiang, I. Natgunanathan, S. Guo, W. Zhou, and G. Beliakov, "Robust histogram shape based method for image watermarking," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 25, no. 5, pp. 717-729, May 2015.

[3] M. Alghoniemy and A. H. Tewfik, "Geometric invariance in image watermarking," *IEEE Trans. Image Process.*, vol. 13, no. 2, pp. 145–153, Feb. 2004.

[4] P. Dong, J. G. Brankov, N. P. Galatsanos, Y. Yang, and F. Davoine, "Digital watermarking robust to geometric distortions," *IEEE Trans. Image Process.*, vol. 14, no. 12, pp. 2140–2150, Dec. 2005.

[5] J. S. Seo and C. D. Yoo, "Image watermarking based on invariant regions of scale-space representation," *IEEE Trans. Signal Process.*, vol. 54, no. 4, pp. 1537–1549, Apr. 2006.

[6] X. Gao, C. Deng, X. Li, and D. Tao, "Geometric distortion insensitive image watermarking in affine covariant regions," *IEEE Trans. Syst., Man, and Cybernetics, Part C: Applications and Reviews.*, vol. 40, no. 3, pp. 278–286, May 2010.

[7] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shanon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, no. 12, pp. 1673–1687, Dec. 1997.

[8] J. Cannons and P. Moulin, "Design and statistical analysis of a hash-aided image watermarking system," *IEEE Trans. Image Process.*, vol. 13, no. 10, pp. 1393–1408, Oct. 2004.

[9] H. S. Malvar and D. A. Florencio, "Improved spread spectrum: A new modulation technique for robust watermarking," *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 898–905, Apr. 2003.

[10] A. Valizadeh and Z. J. Wang, "Correlation-and-bit-aware spread spectrum embedding for data hiding," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 267–282, Jun. 2011.

[11] A. K. Mairgiotis, N. P. Galatsanos, and Y. Yang, "New additive watermark detectors based on a hierarchical spatially adaptive image model," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 1, pp. 29–37, Mar. 2008.

[12] M. Li, M. K. Kulhandjian, D. A. Pados, S. N. Batalama, and M. J. Medley, "Extracting spread-spectrum hidden data from digital media," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 7, pp. 1201–1210, Jul. 2013.

[13] Q. Cheng, "Generalized embedding of multiplicative watermarks," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 7, pp. 978–988, Jul. 2009.

[14] A. Valizadeh and Z. J. Wang, "An improved multiplicative spread spectrum embedding scheme for data hiding," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 4, pp. 1127–1143, Aug. 2012.

[15] B. Chen and G. W. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1423–1443, May 2001.

[16] S.-H. Wang and Y.-P. Lin, "Wavelet tree quantization for copyright protection watermarking," *IEEE Trans. Image Process.*, vol. 13, no. 2, pp. 154–165, Feb. 2004.

[17] N. K. Kalantari and S. M. Ahadi, "A logarithmic quantization index modulation for perceptually better data hiding," *IEEE Trans. Image Process.*, vol. 19, no. 6, pp. 1504–1517, Jun. 2010.

[18] I. D. Shterev and R. L. Lagendijk, "Amplitude scale estimation for quantization-based watermarking," *IEEE Trans. Signal Process.*, vol. 54, no. 11, pp. 4146–4155, Nov. 2006.

[19] Q. Li and I. J. Cox, "Using perceptual models to improve fidelity and provide resistance to valumetric scaling for quantization index modulation watermarking," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 2, pp. 127–139, Jun. 2007.

[20] E. Nezhadarya, Z. Wang, and R. Ward, "Robust image watermarking based on multiscale gradient direction quantization," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 4, pp. 1200–1213, Dec. 2011.

[21] M. Zareian and H. R. Tohidypour, "A novel gain invariant quantization-based watermarking approach," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 11, pp. 1804–1813, Nov. 2014.

[22] E. Koch and J. Zhao, "Towards robust and hidden image copyright labeling," in *Proc. IEEE Workshop Nonlinear Signal Image Process.*, 1995, pp. 452–455.

[23] A. K. Parthasarathy and S. Kak, "An improved method of content based image watermarking," *IEEE Trans. Broadcasting*, vol. 53, no. 2, pp. 468–479, Jun. 2007.

[24] P.-C. Su, Y.-C. Chang, and C.-Y. Wu, "Geometrically resilient digital image watermarking by using interest point extraction and extended pilot signals," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 1897–1908, Dec. 2013.

[25] H. Zhang, H. Z. Shu, G. Coatrieux, J. Zhu, Q. M. J. Wu, Y. Zhang, H. Q. Zhu, and L. M. Luo, "Affine legendre moment invariants for image watermarking robust to geometric distortions," *IEEE Trans. Image Process.*, vol. 20, no. 8, pp. 2189–2199, Aug. 2011.