A Highly Robust Reversible Watermarking Scheme Using Embedding Optimization and Rounded Error Compensation

Yichao Tang, Shuai Wang, Chuntao Wang, *Member, IEEE*, Shijun Xiang, *Member, IEEE*, and Yiu-Ming Cheung, *Fellow, IEEE*

***Abstract*— The robust reversible watermarking (RRW) requires high robustness and capacity on the condition of reversibility and imperceptibility, which still remains a big challenge nowadays. In this paper, we propose a two-stage RRW scheme that improves robustness and capacity through embedding optimization and rounded error compensation. The first stage inserts a robust watermark into the selected Pseudo-Zernike moments (PZMs) by using an adaptive normalization method and an optimized embedding strategy. Specifically, the adaptive normalization method achieves both an invariance to pixel amplitude variation and a balance between robustness and imperceptibility, and the optimized embedding strategy reduces embedding distortions remarkably. The watermarked PZMs are inversely transformed to generate the robustly watermarked image, in which rounded errors caused in the inverse transformation is compensated elaborately and thus a larger capacity can be obtained at the same embedding distortion. The second stage embeds a reversible watermark consisting of errors between the robust watermark embedded image and the original one, aiming at achieving the reversibility in case of no attacks. Extensive experimental simulations show that the proposed scheme provides strong robustness against common signal processing, including AWGN, salt-and-pepper noise, JPEG, JPEG2000, median filtering, mean filtering, geometrical transformations involving rotation and scaling, and a compressive sensing attack exemplified by two-dimensional compressive sensing, which outperforms the state-of-the-art schemes. Our code is available at https://github.com/yichao-tang/PZMs-RRW.**

***Index Terms*— Robust reversible watermarking, compensation information, Pseudo-Zernike moments, geometric deformations.**

I. Introduction

NOWADAYS the demand for high-fidelity digital images such as high-resolution photography products, computer graphics, satellite remote sensing images has been increasing gradually. As these digital images have outstanding commercial or application values, their copyrights need to be protected while their contents require to be recovered perfectly. Although the technique of robust watermarking [1] can well protect copyrights, it leads to permanent distortions to the original image. Though the reversible watermarking [2] can ensure perfect recovery of the original image after the inserted watermark has been extracted, it cannot resist against even weak attacks to fulfill the copyright protection. Thus, either the robust or reversible watermarking cannot satisfy the requirements of copyright protection and reversibility. To achieve these requirements simultaneously, the techniques of robust reversible watermarking (RRW) have been developed in the literature [3].

RRW achieves both the robustness and reversibility. Specifically, if the watermarked image is not attacked with common signal processing (CSP) such as noise pollution, compression, and filtering or with geometrical deformations such as rotation and scaling, both the watermark and the original image can be recovered perfectly. Otherwise, the embedded watermark can be extracted to demonstrate the copyright of the original image whereas the original image cannot be reconstructed perfectly. Besides the robustness and invertibility, invisibility and high capacity are also required in general, where the invisibility indicates that the embedded watermark is invisible and the high capacity implies that a large number of watermark bits for copyright protection are inserted in the original image.

The first RRW proposed by Honsinger et al. [4] can successfully detect tampered regions, but generally lead to salt-and-pepper noises. Since then, many RRW methods have been developed in the literature. According to the watermark robustness, the existing RRW methods can be roughly divided

Manuscript received 20 March 2022; revised 9 August 2022; accepted 19 October 2022. Date of publication 25 October 2022; date of current version 5 April 2023. This work was supported in part by the National Natural Science Foundation of China under Contract 62172165 and Contract 62272197, in part by the Guangdong Major Project of Basic and Applied Basic Research under Grant 2019B030302008, in part by the Natural Science Foundation of Guangdong Province under Grant 2022A1515010325, in part by the Science and Technology Program of Guangzhou under Grant 201902010081, in part by the Guangzhou Basic and Applied Basic Research Project under Contract 202201010742, in part by the NSFC/Research Grants Council (RGC) Joint Research Scheme under Grant N_HKBU214/21, in part by the General Research Fund of RGC under Grant 12201321, and in part by the Hong Kong Baptist University (HKBU) under Grant RC-FNRA-IG/18-19/SCI/03. This article was recommended by Associate Editor Y. Zhao. *(Corresponding author: Chuntao Wang.)*

Yichao Tang, Shuai Wang, and Chuntao Wang are with the College of Mathematics and Informatics, South China Agricultural University, Guangzhou 510642, China, also with the Key Laboratory of Smart Agricultural Technology in Tropical South China, Ministry of Agriculture and Rural Affairs, Guangzhou 510642, China, and also with the Guangzhou Key Laboratory of Intelligent Agri culture, Guangzhou 510642, China (e-mail: yichao_tang@foxmail.com; frank_wangshuai@qq.com; wangct@scau.edu.cn).

Shijun Xiang is with the College of Information Science and Technology, Jinan University, Guangzhou 510632, China (e-mail: shijun_xiang@qq.com).

Yiu-Ming Cheung is with the Department of Computer Science, Hong Kong Baptist University, Hong Kong, SAR, China (e-mail: ymc@comp.hkbu.edu.hk).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TCSVT.2022.3216849.

Digital Object Identifier 10.1109/TCSVT.2022.3216849

into two categories, i.e., RRW with semi-fragileness [5], [6], [7], [8], [9] and RRW with robustness [10], [11], [12], [13], [14]. RRW with semi-fragileness has a certain robustness to unintentional attacks such as slight JPEG compression, JPEG2000 compression, and salt-and-peppers noises; while RRW with robustness can treat intentional attacks including CSP and geometrical deformations.

According to the robustness degree, RRW with robustness can be further classified as RRW resisting against CSP (RRW-CSP) [15], [16], [17], [18], [19] and RRW counteracting both CSP and geometric deformations (RRW-CG) [20], [21], [22], [23], [24]. RRW-CSP mainly resists against CSP such as additive white gaussian noises (AWGNs), salt-and-pepper noises, median filtering, and JPEG compression; while RRW-CG counteracts both CSP and geometric deformations.

As high-fidelity images generally require the feasible robustness to achieve copyright protection, RRW with robustness is more preferable and has been explored extensively. For RRW-CSP that belongs to the category of RRW with robustness, it can be traced back to the work by Coltuc et al. [15], [16], which develops a reversible contrast mapping to achieve the reversibility and embeds the bitmap via a distributed manner in the neighborhood of a pair of pixels for contrast mapping to fulfill the robustness against cropping. Later, researchers proposed dozens of RRW-CSP methods in the spatial [25], [26], transformed [27], [28], and miscellaneous domains [29], [30]. These methods well resist against JPEG compression, AWGN, salt-and-pepper noise, median filtering, Gaussian filtering, Wiener filtering, cropping, etc, but they cannot deal with geometrical deformations including rotation and scaling.

As another type in the category of RRW with robustness, RRW-CG can well counteract geometrical deformations as well as CSP. The first work pertaining to this type was developed by Chrysochos et al. [20], which selects two bins at a distance from the generated image histogram and modifies relative height of these two bins to embed one bit watermark. Simulation results show that this method can resist against mirror transformation, cropping, rotation, scaling, and aspect ratio changing. Later, Chang et al. [21] constructed a novel RRW by exploiting pair-difference correlations upon subsampling and the technique of just noticeable noise difference (JND), which achieves desirable invisibility and high robustness against blurring, brightness modification, contrast variation, cropping, equalization, Gaussian noising, JPEG compression, rotation, scaling, and sharpening. By deploying α-trimmed mean algorithm and support vector machine, Tsai et al. [31] proposed an RRW scheme that well counteracts JPEG compression, AWGN, salt-and-pepper noise, blurring, brightening, darkening, sharpening, equalization, cropping, and scaling. Recently, Hu and Xiang [23] have developed a novel two-stage RRW method with high robustness, in which the first stage embeds 128 watermark bits by quantizing the integer parts of selected low-order Zernike moments and the second stage inserts the auxiliary information for lossless recovery of the original image via the histogram shifting. Experimental simulation results show that this method achieves high robustness to AWGN, JPEG, JPEG2000, rotation, and scaling.

To sum up, one can find that RRW with robustness is preferable to that with semi-fragileness. For the two classes, i.e., RRW-CSP and RRW-CG, of RRW with robustness, dozens of RRW-CSP approaches have been developed in the literature, while only several RRW-CG methods are proposed. As high robustness to both CSP and geometrical deformations is generally required in practical applications, RRW-CG deserves further investigation. Although the RRW-CG method by Hu and Xiang [23] has achieved high robustness to CSP and geometrical transformations, high-robustness and high-capacity on the condition of invisibility and reversibility still remains a challenge.

To satisfy the constraints of high robustness, high capacity, invisibility, and reversibility, the two-stage strategy may be exploited. Specifically, at the first stage, the robust watermark for copyright protection is embedded in a given image, achieving robustness and invisibility by adjusting the embedding strength. At the second stage, differences between the original and watermarked images are taken as the reversible watermark for the lossless recovery of the original image and inserted in the watermarked image, leading to the reversibility. As enhancing the robustness and embedding capacity at the first stage would yield larger differences and thus more reversible watermark bits, the robust watermarking capacity depends on the embedding method at the first stage. Thus, the embedding approach is highly related to the robust watermarking capacity, invisibility, and reversibility. From this view of point, RRW is not a naive combination of robust watermarking and reversible watermarking. In essence, these two stages affect each other significantly, and a favorable design for two-stage watermark embedding is therefore desired.

In this paper, we design a two-stage RRW-CG scheme using an optimized embedding strategy and a rounded error compensation for robustness and capacity. Specifically, as Pseudo-Zernike moments (PZMs) of the original image is more robust to noises than the conventional Zernike moments [32], we take PZMs as carriers for watermarking. For each to-be-watermarked PZM, we designed an optimized embedding strategy, aiming to reduce embedding distortions. To further enhance the robustness at the same distortion, we introduce a normalization method using an adaptive normalized weight to implement the watermark insertion. To decrease the amount of auxiliary information that is used as the reversible watermark to achieve large embedding capacity, we modify the conventional quantization index modulation with distortion compensation (DC-QIM) by forcing quantization errors to be integers and develop a rounded error compensation according to characteristics in image reconstruction from watermarked PZMs. Afterwards, we embed the generated auxiliary information through the technique of prediction error expanding and histogram shifting (PEE-HS) [33]. By operating in an inverse process, we can extract the watermark and recover the original image. Extensive simulation results show that the proposed scheme achieves high robustness to both CSP and geometrical transformations including rotation and scaling at the embedding rate of 256 bits per image. Also, it outperforms remarkably the state-of-the-art RRW-CSP and RRW-CG methods.

The contributions of the proposed scheme are three-fold below:

1) Design an optimized embedding strategy, reducing embedding distortions remarkably. And introduce a normalization method using an adaptive normalized weight for different to-be-watermarked PZM, enhancing the robustness at the same embedding distortion.
2) Develop an enhanced reversible watermark generation method, decreasing significantly the amount of auxiliary information for reversible watermarking.
3) Propose an RRW-CG scheme, achieving high robustness and large embedding capacity on the condition of invisibility and reversibility and outperforming the state-of-the-arts.

The rest of this paper is organized as following. In Section II, we make an overview of the RRW methods using the two-stage strategy and PZMs. The proposed scheme is presented in Section III. Section IV shows the effects of the developed embedding strategy, adaptive normalization, and enhanced reversible watermark generation. In addition, this section also gives experimental results against CSP, geometrical transformations, and compressive sensing attack as well as performance comparison with the state-of-the-arts. Finally, we draw a conclusion in Section V.

II. Overview of Related Work

In this section, we briefly introduce RRW using the two-stage strategy, and PZMs and its calculation method.

A. RRW Methods Using the Two-Stage Strategy

The first two-stage RRW method was proposed by Coltuc et al. in [16]. At the first stage, it embeds the robust watermark for copyright protection in a given image; and at the second stage, it inserts differences between the original and watermarked images into the watermarked image, where differences are taken as the reversible watermark and embedded in a reversible way. As this method embeds both the robust and reversible watermarks in the same domain, the robust watermark would probably be weakened by the reversible watermark. To alleviate this problem, Wang et al. [13] proposed an independent domain based RRW method, which first transforms a cover image into two independent embedded domains such as low- and high-frequency bands, one for robust watermarking and the other for reversible watermarking. Experimental simulations show that it achieves remarkable improvement against AWGN and JPEG compression. These two-stage RRW methods mainly counteract CSP (common signal processing) attacks, but they cannot resist geometric deformations such as rotation and scaling. To tackle this problem, Hu and Xiang [23] developed a Zernike moment based two-stage RRW approach, which embeds the robust watermark into the normalized low-order Zernike moments by quantizing the integer part of a to-be-watermarked moment followed by inserting the reversible watermark into the robustly watermarked image. Experimental results demonstrate that this method is robust to AWGN, JPEG, JPEG2000, rotation, and scaling. By applying the embedding strategy to polar harmonic transform, they further improved the robustness [24].

B. PZM and Its Calculation Method

PZMs are orthogonal moments obtained by the inner product of an image and Pseudo-Zernike polynomials, where Pseudo-Zernike polynomials are variants of Zernike polynomials. Apart from being rotation and scaling invariant, PZMs are more robust and less sensitive to image noise than Zernike moments [32]. It is noted that the number of PZMs is twice that of Zernike moments for the same moment order. Because of these desirable characteristics, PZMs are widely used in numerous image processing and pattern recognition applications [34], [35].

Suppose that $V_{nm}(x, y)$ denotes Pseudo-Zernike polynomials that are a set of complete and orthogonal functions and $f(x, y)$ $(x, y \in [1, N])$ is an image function. Then $f(x, y)$ defined over a unit circle can be decomposed to a linear combination of $V_{nm}(x, y)$, i.e.,

$$f(x, y) = \sum_{n} \sum_{m} Z_{nm} V_{nm}(x, y) \tag{1}$$

where Z_{nm} represents the PZM of order n with repetition m. The PZM, Z_{nm}, is calculated from the inner product of $f(x, y)$ and $V_{nm}(x, y)$, i.e.,

$$Z_{nm} = \frac{n+1}{\pi} \iint\limits_{x^2+y^2 \le 1} f(x, y) V_{nm}^{*}(x, y) \mathrm{d}x \mathrm{d}y \tag{2}$$

where $V_{nm}^{*}(x, y)$ denotes the conjugation of $V_{nm}(x, y)$, i.e.,

$$V_{nm}(x, y) = R_{nm}(r) e^{im\theta} \tag{3}$$

where n is a non-negative integer, m is an integer satisfying $0 \le |m| \le n$, $r = \sqrt{x^2 + y^2}$, $i = \sqrt{-1}$, and $\theta = \tan^{-1}(y/x)$. The radial Pseudo-Zernike polynomial $R_{nm}(r)$ is defined as

$$R_{nm}(r) = \sum_{k=0}^{n-|m|} (-1)^k \frac{(2n+1-k)! r^{n-k}}{k!(n+|m|+1-k)!(n-|m|-k)!} \tag{4}$$

Eq. (2) is applicable to a continuous function, and its discrete version is defined as

$$Z_{nm} = \frac{n+1}{\pi} \sum_{s}^{N-1} \sum_{t}^{N-1} f(x_s, y_t) V_{nm}^{*}(x_s, y_t) \Delta x_s \Delta y_t \tag{5}$$

where $x_s^2 + y_t^2 \le 1$, $(x_s, y_t) = (\frac{2s+1-N}{N}, \frac{2t+1-N}{N})$, $\Delta x_s = \Delta y_t = \frac{2}{N}$, $s, t \in \{0, 1, \ldots, N-1\}$.

Pseudo-moments Z_{nm} can be used to reconstruct the original function, i.e.,

$$\hat{f}(x_s, y_t) = \sum_{n=0}^{M} \sum_{m=-n}^{n} Z_{nm} V_{nm}(x_s, y_t) \tag{6}$$

where $V_{nm}(x, y)$ is a set of complete and orthogonal functions, in theory $\hat{f}(x_s, y_t)$ would approach to $f(x, y)$ when $M \to \infty$ holds. In practice, $\hat{f}(x_s, y_t)$ does not approximate to $f(x, y)$ because both Z_{nm} and $V_{nm}(x_s, y_t)$ become numerically unstable and inaccurate for high-order moments.

III. Proposed RRW Scheme

In this section, we present the proposed two-stage RRW (robust reversible watermarking) scheme that exploits an optimized embedding strategy, an adaptive normalization method on PZMs, and an enhanced reversible watermark generation method. It consists of three parts, i.e., watermark embedding, integrity authentication, and recovery of watermark and the original image. First, the watermark embedding part inserts both robust and reversible watermarks in a given image. Then the integrity authentication part checks whether the received watermarked image has been attacked or not. Finally, the part for recovery of watermark and the original image performs the watermark extraction and the original image reconstruction in case of no attacks while conducting the watermark extraction in situation of CSP and/or geometrical transformations. Details for these parts are described in Section III-A, III-B, and III-C, respectively.

A. Watermark Embedding

The watermark embedding part inserts both the robust and reversible watermarks in a given image. The robust watermark is a specially designed message for copyright protection, and the reversible watermark aims for reversibility of the original image and generally consists of differences between the original and watermarked images. The robust watermark is embedded at the first stage, while the reversible watermark is inserted at the second stage.

Fig. 1 illustrates the two-stage embedding process, where the first and second stages are denoted the robust and reversible embedding stages, respectively. In the robust embedding stage, PZMs are first computed from an image, eligible PZMs are then selected and watermarked via an adaptive normalization method and an optimized embedding strategy, a watermarked image is subsequently reconstructed from watermarked PZMs, rounded errors in the watermarked image reconstruction are compensated to yield the robustly watermarked image. In the reversible embedding stage, the reversible watermark is generated and then embedded in the robustly watermarked image. Details for these steps are presented below.

1) Robust Embedding Stage:

a) PZM calculation: Suppose that I_{cover} of size $N \times N$ is a given image and Z_{nm} is a PZM with order n $(0 \leq n \leq M)$ and repetition number m $(0 \leq |m| \leq n)$, where M denotes the maximum order. Then radial Pseudo-Zernike polynomials, R_{nm}, of the inscribed circle of image I_{cover} are calculated by Eq. (4), and the corresponding PZMs, Z_{nm}, are calculated according to Eqs. (3) and (5).

b) PZM selection and normalization: Although Eq. (5) can be applied to calculate PZMs for discrete digital images, there exist geometric and integral approximation errors [36], [37]. Due to these errors, Xin et al. [38] proved that PZMs of $m = 4j$ $(j \in \mathbb{Z})$ deviate from the orthogonality and thus cannot be computed accurately. Therefore, PZMs of $m = 4j$ cannot be used for watermark embedding. In other words, the eligible PZMs are selected as $C = \{Z_{nm}, 0 < n \leq M, 0 < m \leq n, m \neq 4j\}$.

Assume that one selected PZM is embedded with one watermark bit and totally there are L $(L < length(C))$ watermark bits w_i^{ro} $(w_i^{ro} \in \{0, 1\}, i = 1, 2, \ldots, L)$, where $length(\cdot)$ counts the number of elements in a set. Then L PZMs are randomly chosen from set C via a secret key, *KEY*, which yields $Z = \{Z_{n1,m1}, Z_{n2,m2}, \ldots, Z_{nL,mL}\}$.

As the scaling operation would change the magnitude of a PZM significantly, a normalization strategy is generally applied to solve this problem [23], [39], which is expressed as

$$Z_{ni,mi}^{R} = \frac{Z_{ni,mi}}{Z_{00}} \tag{7}$$

Via the normalization, $Z_{ni,mi}^{R}$ is invariant to scaling. As the low-order PZMs are generally more robust to CSP (common signal processing) attacks than the high-order ones, the high-order PZMs should be imposed with larger embedding strength than the low-order ones, aiming to maximize the robustness on subject to the same embedding distortion. In view of this, we develop an adaptive normalization method, i.e.,

$$Z_{ni,mi}^{R} = \frac{Z_{ni,mi}}{Z_{00}} \times T_{ni} \tag{8}$$

where T_{ni} is an adaptive normalized weight that is larger than 0 and varies with respect to the PZM order. Thus, $Z_{ni,mi}^{R}$ is in the range of $[0, T_{ni}]$.

As it is hard to derive an optimal T_{ni} theoretically, in our work we set T_{ni} as

$$T_{ni} = T_{start} - \gamma \times n_i \tag{9}$$

where T_{start} represents a starting value for the adaptive normalized weight, γ $(\gamma > 0)$ is a global parameter adjusting the strength of embedded watermark, and n_i is the PZM order for watermark bit w_i^{ro}. Parameters T_{start} and γ are used to control the invisibility of the robustly watermarked image and can be practically determined via experimental simulations.

c) Robust watermark embedding: As aforementioned, the normalized PZMs $Z_{ni,mi}^{R}$ is invariant to scaling. To further achieve the rotation invariance, by exploiting characteristics of Zernike moments, we take the magnitude of a PZM, i.e., $\left|Z_{ni,mi}^{R}\right|$, as the carrier for watermarking. In this way, we can achieve rotation and scaling invariance.

With $\left|Z_{ni,mi}^{R}\right|$ as the carrier for watermarking, the technique of quantization index modulation with dither compensation (DC-QIM) may be employed to insert watermark bit w_i, which is expressed as

$$\left|Z_{ni,mi}^{Rj}\right| = \left\lfloor \frac{\left|Z_{ni,mi}^{R}\right|}{\Delta} \right\rfloor \times \Delta + \beta_i(j), \quad i = 1, 2, \ldots, L, \quad j \in \{0, 1\} \tag{10}$$

where $\beta_i(j)$ is a dither value with constraint $\beta_i(1) = \beta_i(0) + \Delta/2$, $\lfloor \cdot \rfloor$ is a floor function, and Δ is a quantization step. Via DC-QIM, $\left|Z_{ni,mi}^{R0}\right|$ and $\left|Z_{ni,mi}^{R1}\right|$ represent the watermarked versions of carrier $\left|Z_{ni,mi}^{R}\right|$ for bits 0 and 1, respectively.

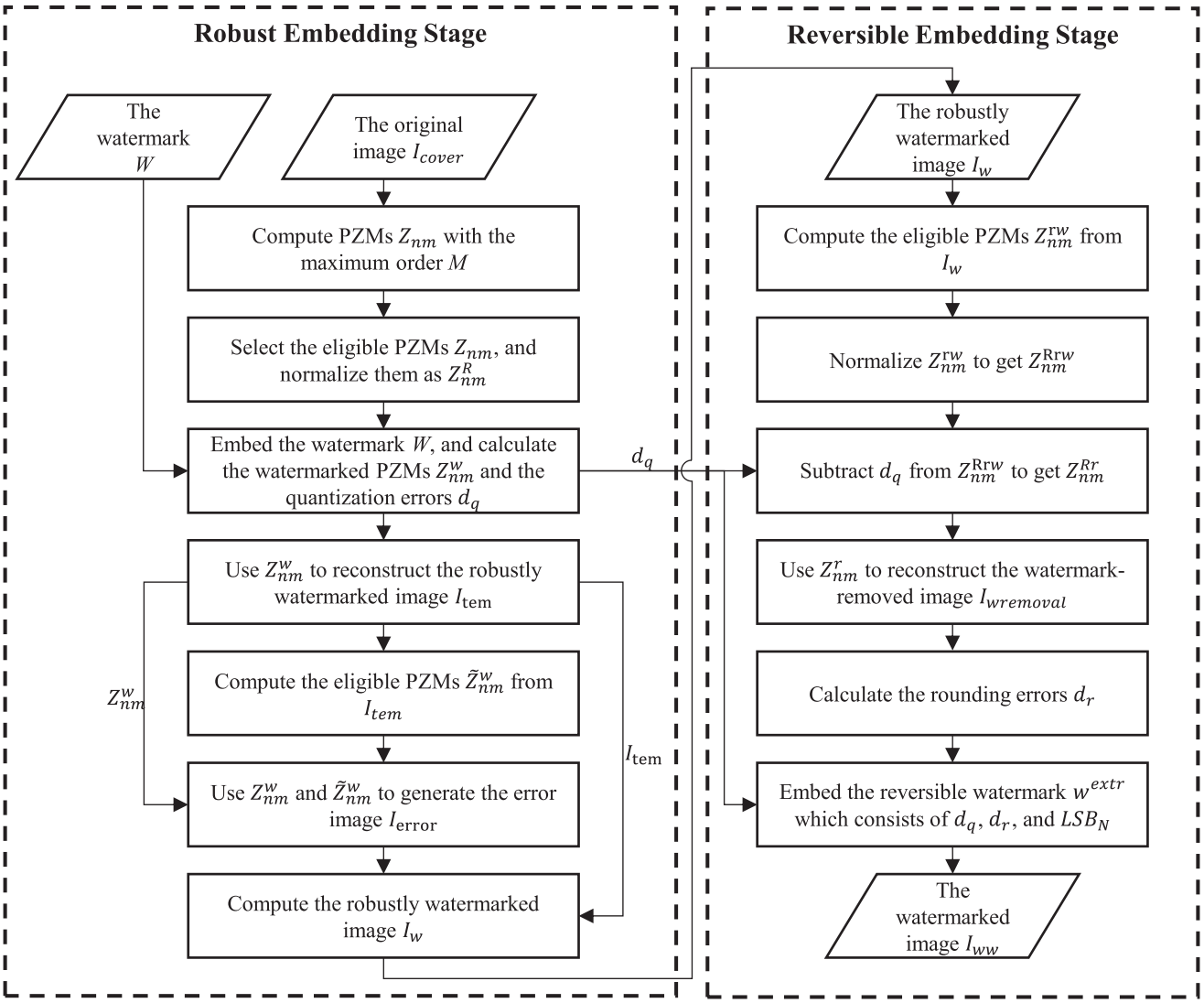


Fig. 1. Flowchart of the proposed RRW scheme.

Without loss of generality, we set $\beta_i(0) = 0$ and $\beta_i(1) = \Delta/2$ and illustrate the DC-QIM based embedding in Fig. 2(a).

As illustrated in Fig. 2(a), the quantization error for $\left|Z^R_{ni,mi}\right|$ is

$$d_{qi} = \left|Z^{Rj}_{ni,mi}\right| - \left|Z^R_{ni,mi}\right|, \quad i = 1, 2, \ldots, L, \ \ j \in \{0, 1\} \tag{11}$$

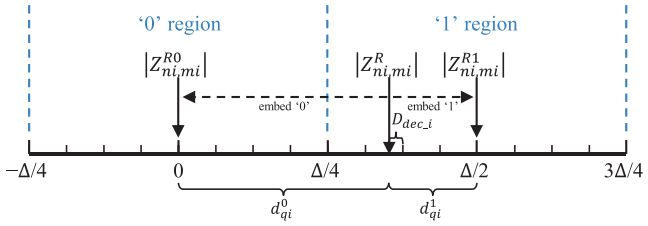
As the normalized PZM is a real number, d_{qi} is a real number, too. To save these real numbers, d_{qi}s, for reversibility of the original image, a large number of bits are required to represent them. In return, this would lead to lots of to-be-embedded bits for the reversible embedding stage and thus make the second stage intractable. To alleviate this problem, we optimize the conventional DC-QIM by forcing quantization errors to be integers. Specifically, we first round $\left|Z^R_{ni,mi}\right|$ to the nearest integer, i.e., $\left|Z^R_{ni,mi}\right|_{rnd} = \left[|Z^R_{ni,mi}|\right]$, and then compute $D_{dec\_i} = \left|\left|Z^R_{ni,mi}\right| - \left|Z^R_{ni,mi}\right|_{rnd}\right|$. Next, we improve the conventional DC-QIM to yield the watermarked normalized PZM, i.e.,

$$\left|Z^{Rj}_{ni,mi}\right| = \left[\frac{\left|Z^R_{ni,mi}\right| - \beta_i(j)}{\Delta}\right] \times \Delta + \beta_i(j) - D_{dec\_i} \tag{12}$$

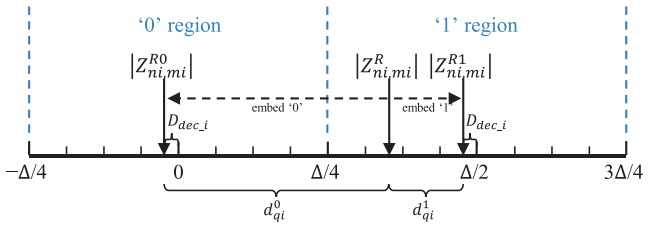
where $[\cdot]$ denotes a rounding function. Via Eq. (12), the quantization error calculated through Eq. (10) would be an integer, and thus less bits are required to represent them. It is noted that in Eq. (12) we adopt the rounding function to replace the floor function in Eq. (10), aiming to further reduce quantization errors. Fig. 2(b) illustrates the optimized DC-QIM-based embedding strategy, and its effectiveness will be demonstrated in Section IV-C.

After the watermarked normalized PZM is generated, the inverse normalization is conducted to yield the watermarked PZM, i.e.,

$$Z^w_{ni,mi} = \frac{\left|Z^{Rj}_{ni,mi}\right|}{\left|Z^R_{ni,mi}\right|} \times \ Z^R_{ni,mi} \tag{13}$$



(a) Conventional DC-QIM



(b) Optimized DC-QIM

Fig. 2. Illustration of DC-QIM based watermarking method. (a) The conventional DC-QIM with $\beta_i(0) = 0$ and $\beta_i(1) = \Delta/2$, where $\Delta = 16$; (b) The optimized DC-QIM that forces the quantization error d^j_{qi} to be an integer.

d) Robustly watermarked image reconstruction: After obtaining the watermarked PZM $Z^{w}_{ni,mi}$,we proceed to reconstruct the robustly watermarked image from $Z^{w}_{ni,mi}$. Specifically, to guarantee pixel values of the reconstructed image to be real values, we first apply the same embedding operations on the conjugate of $Z_{ni,mi}$, i.e., $Z_{ni,-mi}$, as those on $Z_{ni,mi}$. By deploying the selected and watermarked PZMs, $Z^{w}_{ni,mi}$, we then reconstruct the robustly watermarked image, I_{tem}, as follows:

$$I_{tem} = I_{cover} + \left[\sum_{i=1}^{L}((Z^{w}_{ni,mi} - Z_{ni,mi})V_{ni,mi} + (Z^{w}_{ni,-mi} - Z_{ni,-mi})V_{ni,-mi})\right] \tag{14}$$

In reconstruction via Eq. (14), rounding operations occur inevitably because of discretization of PZM calculation, and thus rounding errors are caused accordingly. To further reduce possible rounding errors, we propose to compensate these rounding errors. In more detail, I_{tem} is used to compute watermarked PZMs, say $\tilde{Z}^{w}_{ni,mi}$. As there exist rounding errors, $\tilde{Z}^{w}_{ni,mi}$ actually deviates from $Z^{w}_{ni,mi}$. In other words, the differences between $\tilde{Z}^{w}_{ni,mi}$ and $Z^{w}_{ni,mi}$ essentially represent rounding errors and thus can be exploited to compensate rounding errors. That is, these differences are first deployed to reconstruct an error image, I_{error}, in the following way,

$$I_{error} = \left[\sum_{i=1}^{L}((Z^{w}_{ni,mi} - \tilde{Z}_{ni,mi})V_{ni,mi} + (Z^{w}_{ni,-mi} - \tilde{Z}_{ni,-mi})V_{ni,-mi})\right] \tag{15}$$

I_{error} is then added to I_{tem} to compensate rounding errors, i.e.,

$$I_{w} = I_{tem} + I_{error} \tag{16}$$

which generates the robustly watermarked image I_w.

2) Reversible Embedding Stage: After the robust watermark has been inserted into the original image, distortions due to robust watermark embedding have been caused. To ensure the reversibility in case of no attacks, the caused distortions are required to save in the robustly watermarked image I_w. To this end, the technique of reversible watermarking is generally employed [13], [15], [16], which forms the reversible embedding stage.

In the reversible embedding stage, we first use I_w to calculate PZMs according to Eqs. (3) and (5), then generate a watermark-removed image approximating to the original one, next construct the reversible watermark and embed it in I_w to yield the image watermarked with both robust and reversible watermarks, I_{ww}, and finally insert integrity-authentication-oriented hash values of I_{ww} in least significant bits (LSBs). Details are given below.

a) Watermark-removed image generation: Intuitively, differences between the robustly watermarked image I_w and the original one I_{cover} need to be taken as the reversible watermark. These references are somewhat large and lots of reversible watermark bits are required to represent them. As the robust watermark in I_w can be removed exactly with the help of quantization errors $d_q = \{d_{qi}, i = 1, 2, \ldots, L\}$, we first generate the watermark-removed image, says $I_{wremoval}$, that approximates closely to the original one and then take differences between $I_{wremoval}$ and I_{cover} as the reversible watermark, which in turn reduces the number of reversible watermark bits significantly.

Suppose that $Z^{rw}_{ni,mi}$ are selected PZMs from I_w. Then normalize $Z^{rw}_{ni,mi}$ according to Eq. (8) to form $Z^{Rrw}_{ni,mi}$, and subtract the quantization error d_{qi} from $Z^{Rrw}_{ni,mi}$, i.e.,

$$\left|Z^{Rr}_{ni,mi}\right| = \left|Z^{Rrw}_{ni,mi}\right| - d_{qi} \tag{17}$$

Due to rounding errors, $\left|Z^{Rr}_{ni,mi}\right|$ only approximates to the original normalized version $\left|Z^{R}_{ni,mi}\right|$ in Eq. (8). It is further de-normalized to obtain the corresponding PZM of $I_{wremoval}$, i.e.,

$$Z^{r}_{ni,mi} = \frac{\left|Z^{Rr}_{ni,mi}\right|}{\left|Z^{Rrw}_{ni,mi}\right|} \times Z^{rw}_{ni,mi} \tag{18}$$

Via $Z^{r}_{ni,mi}$, the watermark-removed image $I_{wremoval}$ is reconstructed as

$$I_{wremoval} = I_{w} + \left[\sum_{i=1}^{L}((Z^{r}_{ni,mi} - Z^{rw}_{ni,mi})V_{ni,mi} + (Z^{r}_{ni,-mi} - Z^{rw}_{ni,-mi})V_{ni,-mi})\right] \tag{19}$$

b) Reversible watermark embedding: As aforementioned, the modified DC-QIM is developed to embed the robust watermark. Due to the quantization by DC-QIM, permanent distortions are caused. To ensure the reversibility, quantization errors d_q are needed to save. In the two-stage based RRW, d_q is taken as part of the reversible watermark and saved into the robustly watermarked image I_w.

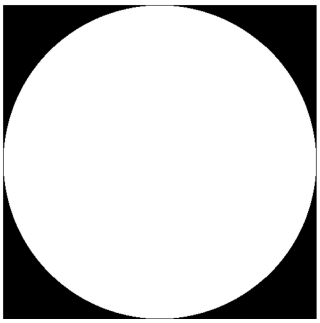


Fig. 3. Illustration of embedding regions for reversible watermarking, where the black and white regions represent those for reversible and robust watermarking, respectively.

Due to rounding errors existed in image reconstruction from PZMs, $I_{wremoval}$ actually deviates from the original image I_{cover}. To achieve the reversibility, differences between $I_{wremoval}$ and I_{cover}, says $d_r = I_{cover} - I_{wremoval}$, are required to save. Thus, d_r also forms part of the reversible watermark.

For attack authentication, we further consider the other part of the reversible watermark. For RRW methods, both the robust watermark and the original image are required to recover in case of no attacks, while in scenario of attacks only the robust watermark is extracted. Thus, when a watermarked image is received, we need to check whether the received image is attacked or not. To this end, we employ the hashing technique. That is, we impose a hashing operation on the image inserted with both the robust and reversible watermarks and yield a sequence with N (e.g., $N = 256$) hash bits, namely H. As H can only be embedded after the robust and reversible watermarks have been inserted, we preserve N least significant bits (LSBs) by extracting N LSBs from the first N non-watermarked image pixels of the robustly watermarked image I_w and place these N hash bits in the preserved LSBs after reversible watermark embedding. To meet this requirement, we thus take the extracted N LSB bits, says LSB_N, as another part of the reversible watermark.

In summary, the reversible watermark in our scheme consists of d_q, d_r, and LSB_N, i.e., $w^{re} = \{d_q, d_r, LSB_N\}$. After constructing w^{re}, we embed it in the robustly watermarked image I_w. Specifically, as image pixels in the inscribed circle of I_w has been robustly watermarked, we first choose image pixels located outside the inscribed circle for reversible watermarking, as illustrated in Fig. 3. We then set LSBs of the first N pixels as 0. Subsequently, we deploy the excellent reversible watermarking technique in [33] to insert w^{re} in image pixels other than the first N ones, yielding the image watermarked with both the robust and reversible watermarks, namely I_{ww}. For space limitation, embedding details are recommended to refer to [33].

After I_{ww} is generated, it is imposed with a hashing operation such as MD5, SHA-224, or SHA-256 to obtain a sequence of N hash bits, H. Next, H is placed in N preserved LSBs of the first N chosen image pixels. This thus leads to the finally watermarked image I_{final}.

It is worth pointing out that if image pixels outside the inscribed circle of I_w cannot accommodate w^{re}, part of image pixels inside the inscribed circle are used to embed the remained reversible watermark bits. In this case, although the inserted reversible watermark possibly degrades robustness of the embedded robust watermark, the degradation would be rather limited due to small strength of the inserted reversible watermark.

B. Integrity Authentication

After receiving an image I_{recv}, the receiver first conducts the integrity authentication by checking whether I_{recv} has been attacked or not. In more detail, image pixels outside the inscribed circle of I_{recv} are first chosen; and LSBs of the first N image pixels are extracted as the sequence for integrity authentication, which is denoted H_{extr}.

After the LSB extraction, these N LSBs are substituted with 0s, which results in the image for hashing calculation, I'_{ww}, and the same hashing operation as the embedder is then imposed on I'_{ww} to generate a hash sequence H_{cmpt}. If H_{cmpt} is exactly equal to H_{extr}, we then claim that the received image I_{recv} has not been attacked; otherwise, it has undergone unintentional or intentional attacks.

C. Watermark Extraction and Image Recovery

After the integrity authentication, the receiver can determine whether the received image has been attacked or not. If the received image does not suffer any attack, i.e., $I_{recv} = I_{final}$, the robust watermark can then be correctly extracted and the original image can be recovered perfectly. Fig. 4 illustrates the procedure for watermark extraction and image recovery in case of no attacks, and details are described below.

We first extract the reversible watermark from I'_{ww} that has removed the N hashing bits H_{extr}. By applying the extraction method in [33], the reversible watermark w^{extr} is obtained, which is essentially equivalent to the original reversible watermark $w^{re} = \{d_q, d_r, LSB_N\}$ in situation of no attacks, and the image removing the reversible watermark is recovered. By replacing LSBs of the first N image pixels for reversible watermarking with the extracted LSB_N the robustly watermark I'_w is thus obtained, which is actually equivalent to the robustly watermarked image I_w at the embedder in case of no attacks.

We then detect the robust watermark from I'_w. First, PZMs are calculated from I'_w. By adopting the same secret key, *KEY*, that is sent from the embedder through a secret channel, the same PZMs are chosen from all PZMs and normalized via Eq. (8) as $Z^{Rrw} = \left\{Z^{Rrw}_{n1,m1}, Z^{Rrw}_{n2,m2}, \ldots, Z^{Rrw}_{nL,mL}\right\}$. From Z^{Rrw}, the robust watermark is detected as

$$\left|Z^{Rrj}_{ni,mi}\right| = \left\lfloor \frac{\left|Z^{Rrw}_{ni,mi}\right| - \beta_i(j)}{\Delta} \right\rfloor \times \Delta + \beta_i(j), \quad i = 1, 2, \ldots, L, \;\; j \in \{0, 1\} \tag{20}$$

$$w_i^{ro\prime} = \begin{cases} 0, \text{if } \left|Z^{Rrw}_{ni,mi}\right| - \left|Z^{Rr0}_{ni,mi}\right| \le \left|Z^{Rrw}_{ni,mi}\right| - \left|Z^{Rr1}_{ni,mi}\right| \\ 1, \text{if } \left|Z^{Rrw}_{ni,mi}\right| - \left|Z^{Rr0}_{ni,mi}\right| > \left|Z^{Rrw}_{ni,mi}\right| - \left|Z^{Rr1}_{ni,mi}\right| \end{cases} \tag{21}$$

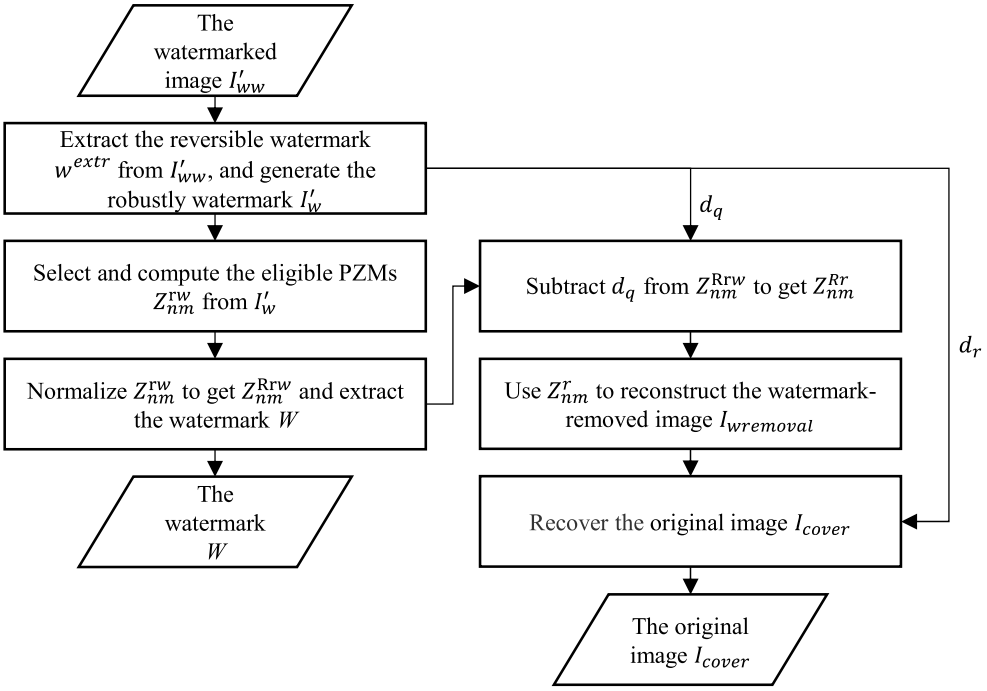


Fig. 4. Extraction process in case of no attacks.

By exploiting the extracted quantization errors d_q, the watermark removed image $I_{wremoval}$ can be obtained at the receiver through Eqs. (17)–(19). Thus, by further adding the extracted rounded errors d_r, the original image can be recovered as

$$I_{cover} = I_{wremoval} + d_r \tag{22}$$

When I_{recv} has been attacked with CSP and geometrical transformations, we can no longer recover the original image. In this situation, we directly use I_{recv} rather than I'_w to generate PZMs and extract the robust watermark $w^{ro\prime} = \{w_i^{ro\prime}, i = 1, 2, \ldots, L\}$.

IV. Experimental Results and Analysis

In this section, we investigate the proposed RRW (reversible robust watermarking) scheme using the adaptive normalization, optimized embedding strategy, and rounded error compensation. The preferable parameter setting is first sought via experimental simulations, the effectiveness of adaptive normalization, optimized embedding strategy, and rounded error compensation is then demonstrated, the performance in terms of visual quality of watermarked images are illustrated, and the robustness is finally evaluated by comparing the proposed scheme to the state-of-the-art RRWs such as Zeng et al. [11], Thabit et al. [40], Liu et al. [19], Wang et al. [13], and Hu and Xiang [23]. For notational convenience, these compared methods are denoted ZENG, THABIT, LIU, WANG, and HU, respectively. These are presented in Sections from IV-A to IV-G, respectively.

A. Parameter Setting

In the simulation, we tested 200 512×512 gray images of different edges and textures from the USC-SIPI image database [41] and took four gray images shown in Fig. 5 for the optimal parameter seeking and effectiveness illustration.

Fig. 5. Four typical images. (a) Lena, (b) Gold hill, (c) Peppers, and (d) Barbara.

As described in Section III, the proposed scheme involves six parameters, i.e., 1) a starting value for the adaptive normalized weight, T_{start}; 2) a global parameter adjusting the strength of embedded watermark, γ ($\gamma > 0$); 3) the maximum order of PZMs, M; 4) the number of robust watermark bits, L; 5) the quantization step for robust watermark embedding, Δ; and 6) the length of a hash sequence, N. For T_{start} and γ, we set them as $T_{start} \in [1500, 3000]$ and $\gamma \in [5, 25]$, then embed a watermark message consisted of $L = 256$ random bits on the test 200 images using different combinations of T_{start} and γ, and finally take $T_{start} = 2400$ and $\gamma = 10$ that result in an average PSNR of about 40 dB as practically feasible parameters. For convenience of capacity illustration and performance comparison, we use two settings for L, i.e., $L = 128$ and $L = 256$. By trading off the PZM number and the computational complexity, we set $M = 26$ and $M = 18$ for $L = 256$ and $L = 128$, respectively. To balance robustness and imperceptibility, $\Delta = 32$ is employed in our simulation. To probably decrease the extra information, $N = 256$ is deployed in practice.

For the compared state-of-the-art RRWs by ZENG, THABIT, LIU, WANG, and HU, the optimal settings given in

TABLE I

KEY PARAMETERS OF THE COMPARED STATE-OF-THE-ARTS AND THE PROPOSED SCHEME IN CASE OF 128-BIT

Methods	Parameters settings
ZENG	blocks size 64×32; $T = 2000$; $G = 4000$
THABIT	blocks size 32×32; $T = 4$
LIU	blocks size 8×8; $\Delta = 100$
WANG	blocks size 64×16; $\zeta = 2.4$
HU	$N = 31$; $\Delta = 18$; $T = 1000$
Proposed	$M = 18$; $\Delta = 32$; $T_{start} = 2000$; $\gamma = 10$

TABLE II

KEY PARAMETERS OF THE COMPARED STATE-OF-THE-ARTS AND THE PROPOSED SCHEME IN CASE OF 256-BIT

Methods	Parameters settings
ZENG	blocks size 32×32; $T = 1000$; $G = 2000$
THABIT	blocks size 32×32; $T = 8$
LIU	blocks size 8×8; $\Delta = 80$
WANG	blocks size 32×16; $\zeta = 2.9$
HU	$N = 36$; $\Delta = 14$; $T = 1000$
Proposed	$M = 26$; $\Delta = 32$; $T_{start} = 2400$; $\gamma = 10$

the corresponding paper are used. Tables I and II summarize key parameters for the compared state-of-the-art as well as the proposed scheme for 128- and 256-bit cases, respectively.

B. Effectiveness of Adaptive Normalization

As described in Section III-A.1.b, the proposed scheme develops the adaptive normalization, which imposes large embedding strength for high-order PZMs while adopting small embedding strength for low-order PZMs. This in turn would result in a good trade-off between robustness and invisibility. To demonstrate this, we adopt two normalization strategies using a fixed normalized weight, namely T_{ni}^{f}, and an adaptive normalized weight, says T_{ni}^{a}, and compare their robustness performance against AWGN (additive white Gaussian noise) and JPEG on the condition of close PSNRs. In the simulation, T_{ni}^{a} is determined via Eq. (9) with $T_{start} = 2400$ and $\gamma = 10$ and T_{ni}^{f} is adjusted image by image to make the generated PSNR close to that by T_{ni}^{a}; the standard deviation, σ, of AWGN is set as 0.005, 0.009, 0.013, 0.017, 0.021, 0.025, and 0.029; and quality factors (QFs) for JPEG are 10, 30, 50, 70, and 90.

Table III summarizes the bit error rate (BER) for the typical image of Lena and that averaged all 200 test images. It is found that on the condition of nearly identical PSNRs, BERs (%) for the adaptive normalization are smaller than those for the fixed normalization, which thus demonstrates the effectiveness of the adaptive normalization.

C. Effectiveness of the Optimized Embedding Strategy

In Section III-A.1.c, we optimize the conventional DC-QIM for robust watermark embedding by forcing quantization errors to be integers and adopting the rounding instead of flooring operation. Via this optimization, the number of bits for saving quantization errors, d_q, decreases remarkably. To demonstrate this, we examine two cases: 1) robust watermark embedding via the conventional DC-QIM, and 2) the optimized DC-QIM. For case 1, the integral part is converted to a bit sequence and the decimal part is coded via the arithmetic codec and then compare the bit number for saving the corresponding d_q. For case 2, quantization errors are directly converted to a bit sequence. For evaluation convenience, both cases use the flooring operation. Table IV summarizes bit numbers for two cases, where each bit number is averaged over 200 test images. It is observed that case 2 using the optimized DC-QIM requires much less bits than case 1, in which the bit number in case 2 is about 14% of that in case 1. This well demonstrates the effectiveness of the strategy forcing quantization errors to be integers.

To further illustrate the effectiveness of the rounding operation, we first fix the embedding strategy forcing quantization errors to be integers and then compare numbers of bits for saving d_q in cases with flooring and rounding operations, respectively. Table V presents results for these two cases. It is shown that using the rounding operation needs remarkably less bits 70% less than the flooring operation. This implies that the rounding operation leads to smaller quantization distortions and thus is more preferable than the flooring operation.

D. Effectiveness of Rounded Error Compensation

As described in Section III-A.1.d, there exist rounded errors in reconstructing an image from PZMs. To alleviate this problem, the proposed scheme compensates rounded errors via Eqs. (15) and (16). To illustrate the effectiveness of this strategy, we evaluate the number of all reversible watermark bits in scenarios with and without the rounded error compensation. In the simulation, the same robust watermark of $L = 256$ bits are embedded in each test image, the same parameters of $T_{start} = 2400$ and $\gamma = 10$ are used to generate nearly identical PSNRs for these two scenarios, and the reversible watermark is finally constructed via the method in Section III-A.2.b.

Table VI presents the number of all reversible watermark bits for scenarios with and without rounded error compensation. It is found that on the condition of nearly identical PSNRs, the bit number in case with the proposed rounded error compensation is 33% less than that in case without the rounded error compensation. This well indicates the effectiveness of rounded error compensation.

E. Evaluation on Quality of Watermarked Images

In this subsection, we illustrate the visual quality of a watermarked image and examine their PSNRs. In the simulation, we embed a robust watermark message with $L = 256$ random bits in each test image using parameters in Section IV-A, and compute PSNRs for the robustly watermarked image, I_w, and the final image inserted with both the robust and reversible watermarks, I_{final}.

Fig. 6 illustrates the original image of Boat I_{cover}, the finally watermarked image I_{final}, the difference between I_{cover} and I_{final}, and the difference between I_{cover} and the recovered original image from I_{final}. It is shown that the finally watermarked image I_{final} has desirable visual quality, which is hard to distinguish via naked eyes from the original image. Similar results can be observed for the other test images. Also, Fig. 6(d) shows that the original image can be exactly recovered by the proposed scheme in case of no attacks.

TABLE III

ROBUSTNESS PERFORMANCE IN TERMS OF BER (%) AGAINST AWGN AND JPEG FOR THE FIXED AND ADAPTIVE NORMALIZATION, WHERE ATK., PARAM., AND AVG. STAND FOR ATTACK, PARAMETER, AND AVERAGE, RESPECTIVELY

Atk		AWGN							JPEG					PSNR
Param.		0.005	0.009	0.013	0.017	0.021	0.025	0.029	10	30	50	70	90	
T_{ni}^{f}	Lena	0.00	1.95	4.30	6.25	8.20	14.84	17.58	3.91	0.00	0.00	0.00	0.00	39.84
	Avg.	0.88	3.36	7.52	12.17	13.63	19.79	22.68	3.67	0.02	0.00	0.00	0.00	40.26
$\boldsymbol{T_{ni}^{a}}$	Lena	0.00	1.56	3.13	7.03	7.81	13.28	13.67	3.52	0.00	0.00	0.00	0.00	39.87
	Avg.	**0.71**	**2.80**	**6.49**	**10.67**	**12.17**	**17.30**	**20.39**	**2.92**	**0.02**	**0.00**	**0.00**	**0.00**	**40.31**

TABLE IV

THE BIT NUMBER FOR SAVING QUANTIZATION ERRORS d_q IN CASES 1 AND 2, RESPECTIVELY, WHERE THE AVERAGE BIT NUMBER IS AVERAGED OVER ALL 200 TEST IMAGES

Case	Case 1	**Case2**
Bit number for Lena	1257831	**186360**
Average bit number	1182463.42	**168912.39**

TABLE V

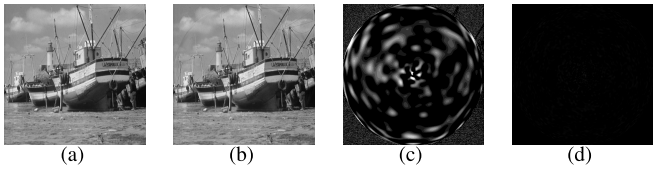
THE BIT NUMBER FOR SAVING d_q IN CASES WITH FLOORING AND ROUNDING OPERATIONS, RESPECTIVELY, WHERE THE AVERAGE BIT NUMBER IS AVERAGED OVER ALL 200 TEST IMAGES

Case	Flooring	**Rounding**
Bit number for Lena	186360	**56696**
Average bit number	168912.39	**50967.54**

TABLE VI

THE NUMBER OF ALL REVERSIBLE WATERMARK BITS FOR SCENARIOS WITH AND WITHOUT ROUNDED ERROR COMPENSATION (REC), WHERE AVERAGE VALUES ARE RESULTS AVERAGED OVER 200 TEST IMAGES

Scenario	Without REC		**With REC**	
	PSNR	Bitnumber	PSNR	**Bitnumber**
Lena	39.90	56696	39.84	**40712**
Average	40.35	50967.54	40.31	**34113.9**



(a) (b) (c) (d)

Fig. 6. Illustration of visual quality of the watermarked image, Boat, by the proposed scheme. (a) The original image; (b) The finally watermarked image (PSNR = 39.7 dB); (c) Differences between (a) and (b), where the amplitude is scaled for visual convenience; and (d) Differences between the (a) and the recovered original image from (b), in which all pixel values are 0.

In addition, Table VII summarizes these two types of PSNRs for four typical images as well as average PSNRs over all 200 test images. It is found that the proposed scheme achieves average PSNRs of 40.04 and 39.02 dB for I_w and I_{final}, which is desirable in practice. The embedding of reversible watermark degrades PSNR of I_w remarkably, which varies image by image and decreases on average about one dB.

F. Comparative Studies Under CSP and Geometrical Attacks

In this subsection, we further evaluate the proposed scheme by comparing it with the state-of-the-arts including ZENG, THABIT, LIU, WANG, and HU. For comprehensive

TABLE VII

PSNRS OF THE ROBUSTLY WATERMARKED IMAGE I_w AND THE FINAL IMAGE INSERTED WITH BOTH THE ROBUST AND REVERSIBLE WATERMARKS I_{final}

Image (dB)	Lena	Goldhill	Peppers	Barbara	Average
I_w	39.84	40.23	40.32	39.59	40.04
I_{final}	39.14	39.86	38.53	39.05	39.02

TABLE VIII

PSNRS (DB) OF IMAGES WATERMARKED BY SIX INVOLVED RRW APPROACHES IN CASE OF 128-BIT ROBUST WATERMARK

Methods	Lena	Goldhill	Peppers	Barbara
ZENG	38.52	38.53	38.52	38.57
THABIT	38.24	38.27	38.39	38.01
LIU	38.47	38.89	38.08	37.85
WANG	38.85	38.59	38.23	39.00
HU	39.21	39.04	39.57	39.41
Proposed	39.75	40.71	39.82	40.14

comparison, we embed both 128- and 256-bit robust watermarks for the compared methods and the proposed scheme. Specifically, we insert the same robust watermark of 128 and 256 random bits in each test image, respectively, using the five compared methods and the proposed scheme, in which PSNRs of watermarked images are motified to be nearly identical by adjusting the embedding strength of each concerned RRW approach, and then evaluate the robustness against CSP (common signal processing) and geometrical transformations. The robust watermark embedding and performance examination can be conducted in a similar way. Results for 128- and 256-bit cases are given as follows.

1) Performance Evaluation in Case of 128-bit Robust Watermark: In the simulation, we take four typical images including Lena, Goldhill, Peppers, and Barbara for illustration. For fair comparison, PSNRs of watermarked images corresponding to the same original test image are adjusted to be rougly the same, in which PSNRs by the proposed scheme are generally larger than those by the compared methods. Table VIII summarizes PSNRs of watermarked images for all test images. Under this PSNR setting, robustness performance against CSP and geometrical transformations can be evaluated in a reasonable way.

a) Robustness against CSP: We first assess the performance of six involved RRW approaches against CSP. In the simulation, we impose AWGN, salt-and-pepper noise, JPEG, JPEG2000, median filtering, and mean filtering on each watermarked image and check the bit error rate (BER) for each attacked image, in which the standard deviation of AWGN is set as $\sigma \in [0.005, 0.029]$ with step 0.002, the noise density

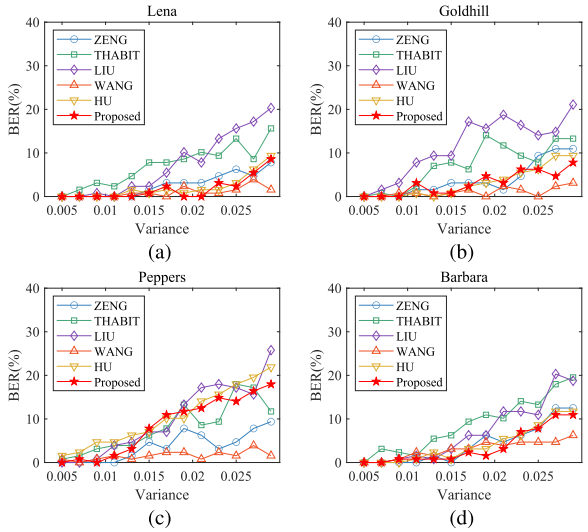


Fig. 7. Robustness to AWGN in case of 128-bit robust watermark.

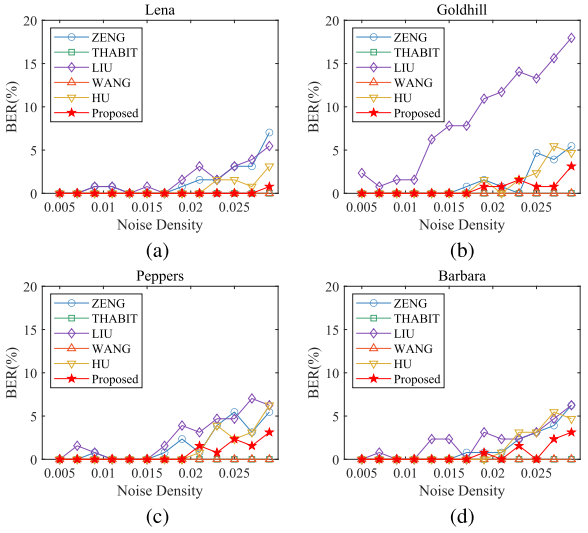


Fig. 8. Robustness to salt-and-pepper noise in case of 128-bit robust watermark.

of salt-and-pepper noise is selected as $D \in [0.005, 0.029]$ with step 0.002, the quality factor (QF) of JPEG is set to be $Q \in [10, 100]$ with step 10, the compression ratios of JPEG2000 are configured as $R \in [10, 100]$ with step 10, and window sizes of median filtering and mean filtering are 3×3, 5×5, and 7×7. Figs. 7–10 present robustness curves against AWGN, salt-and-pepper noise, JPEG and JPEG2000 for all six RRW approaches on different test images, respectively. Table IX shows the experiment results for resisting median filtering and mean filtering.

As shown in Fig. 7, for test images except Peppers, it can be seen the proposed scheme and HU outperform ZENG, THABIT, and LIU. This is because the proposed scheme and HU embed the robust watermark in low-order PZMs and Zernike moments that are highly robust to AWGN, respectively. In contrast, ZENG, THABIT, and LIU insert the robust watermark in the spatial domain, middle-frequency subbands (i.e., LH and HL) from Slantlet transform (SLT), and low-frequency subband of SLT, respectively, which leads to weaker robustness against AWGN than PZMs and Zernike moments. It is also observed that the proposed scheme and HU are somewhat inferior to WANG, which is because WANG embeds the robust watermark in low-frequency band of Harr transform that have higher robustness than low-order PZMs and Zernike moments. In addition, the proposed scheme is slightly better than HU, which attributes to the fact that PZMs are less sensitive to image noise than Zernike moments [32]. By the way, as Image Peppers has more bright regions, it suffers more AWGNs than the other test images.

As illustrated in Fig. 8, it can be seen that all approaches achieve promising performance. Note that LIU performs poorly on Image Goldhill because it uses small embedded blocks that cannot resist salt-and-pepper noise. The proposed scheme outperforms HU and achieves BERs below 5% under all noise densities. This implies that PZMs have higher robustness than Zernike moments.

From Fig. 9, it is observed that all approaches except ZENG perform well against JPEG compression with quality

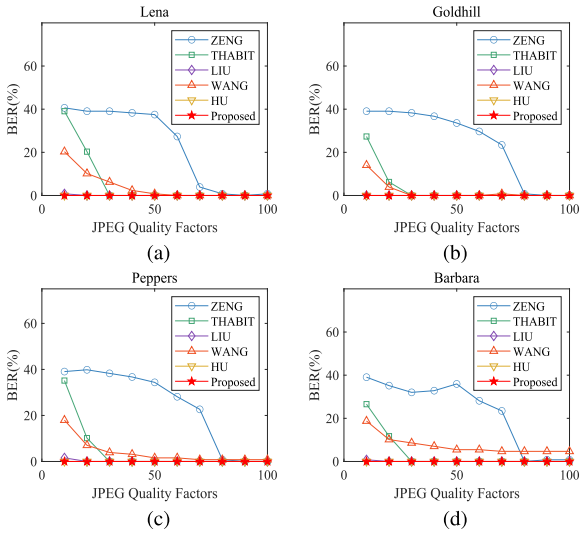


Fig. 9. Robustness to JPEG compression in case of 128-bit robust watermark.

factors greater than 30. For quality factors smaller than 30, the proposed scheme and HU achieve zero BERs while the other methods lead to BERs far larger than zero, which implies the strong robustness of the proposed scheme and HU.

Fig. 10 presents the robustness performance against JPEG2000 compression. It is demonstrated that the proposed scheme provides better performance than HU by developing the adaptive normalization and optimized embedding strategy. The proposed scheme is highly competitive in terms of BER even when the compression ratio is 100.

The average BERs (%) of four typical images for the six approaches under median and mean filters with different window sizes are given in Table IX. It is shown that the proposed scheme effectively resists mean filtering, and achieves zero BER under the filter of size 7×7. In addition, it is found that the performance of ZENG, THABIT, and WANG is unsatisfactory. A plausible reason is that the median and mean filters may replace pixels in one block with the same value and thus reduce their robustness. The PZMs and Zernike

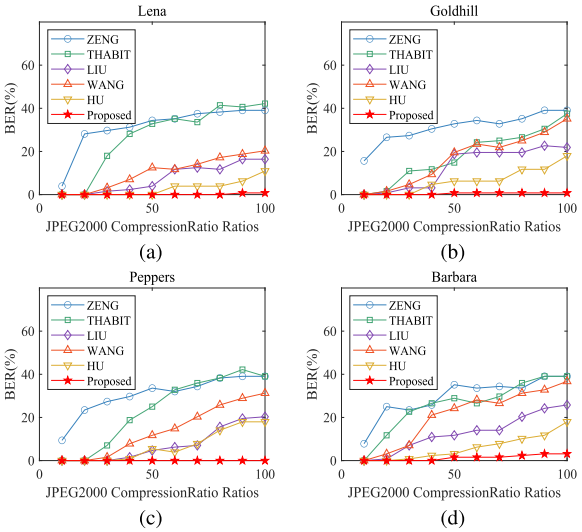


Fig. 10. Robustness to JPEG2000 compression in case of 128-bit robust watermark.

TABLE IX

ROBUSTNESS TO MEDIAN FILTERING AND MEAN FILTERING IN CASE OF 128-BIT ROBUST WATERMARKING

Methods	median filtering			mean filtering		
	3×3	5×5	7×7	3×3	5×5	7×7
ZENG	22.07	26.76	28.52	22.46	30.86	33.01
THABIT	0.78	9.18	19.34	0.39	8.40	16.21
LIU	1.56	4.30	6.84	1.17	3.32	7.03
WANG	7.03	19.14	26.17	7.03	18.16	29.30
HU	0.00	0.78	4.88	0.00	0.98	2.54
Proposed	**0.00**	**0.20**	**1.56**	**0.00**	**0.00**	**0.00**

moments used by the proposed scheme and HU represent the global features of an image, which therefore gives them a better performance.

b) Robustness against geometric deformations: We proceed to evaluate the robustness performance against geometric deformations including rotation and scaling. As the RRW methods of ZENG, THABIT, LIU, and WANG cannot resist geometrical deformations, we mainly compare the proposed scheme with HU. In the simulation, rotation angles range from 0 to 360 degrees with an interval of 20, and scaling factors are from 0.5 to 2.0 with an interval of 0.1. Figs. 11 and 12 summarize the performance of the proposed scheme and HU against rotation and scaling attacks, respectively.

It can be seen from Fig. 11 that BER values are zero for both the proposed scheme and HU under any rotation angles. This indicates that both PZMs and Zernike moments are able to resist in nature rotation operations.

As illustrated in Fig. 12, both the proposed scheme and HU have similar performance against scaling, which is because both of them adopt the scaling-invariant normalization technique. Compared with HU, however, the proposed scheme is somewhat better, which comes from the fact that the proposed scheme develops the adaptive normalization and the optimized embedding strategy.

2) Performance Evaluation in Case of 256-bit Robust Watermark: In the simulation, we embed the same 256-bit watermark in test images including Lena, Goldhill, Peppers, and Barbara. Table X lists PSNRs of watermarked images by the concerned six RRW approaches involving ZENG, THATBIT, LIU, WANG, HU, and the proposed scheme. It is shown that PSNRs by the proposed scheme are somewhat larger than those by the compared methods. In this case, achieving better performance shall well indicate the superiority of the proposed scheme.

a) Robustness against CSP: Similar to the case of 128-bit robust watermark, we also conduct AWGN, salt-and-pepper

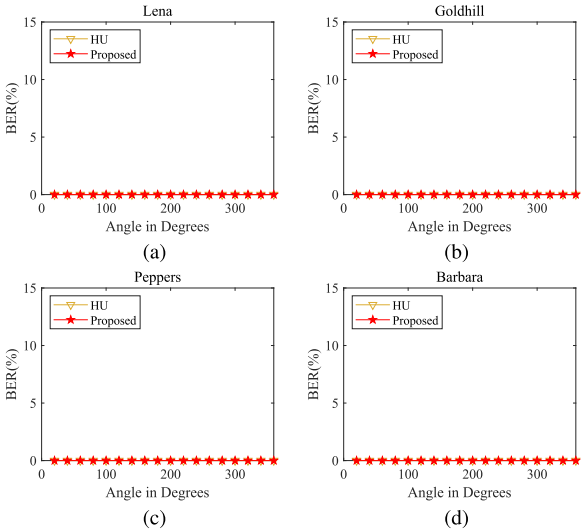


Fig. 11. Robustness to the rotation operations in case of 128-bit robust watermarking.

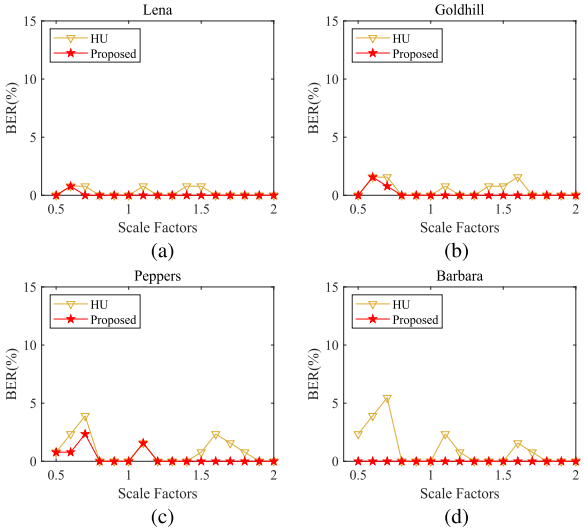


Fig. 12. Robustness to the scaling operations in case of 128-bit robust watermarking.

TABLE X

PSNRS (DB) OF IMAGES WATERMARKED BY SIX INVOLVED RRW APPROACHES IN CASE OF 256-BIT ROBUST WATERMARK

Methods	Lena	Goldhill	Peppers	Barbara
ZENG	38.87	38.49	38.59	38.73
THABIT	39.00	39.01	38.98	38.92
LIU	38.10	39.67	38.04	38.77
WANG	38.51	39.14	38.40	38.74
HU	38.92	38.93	37.50	39.29
Proposed	39.14	39.86	39.03	39.35

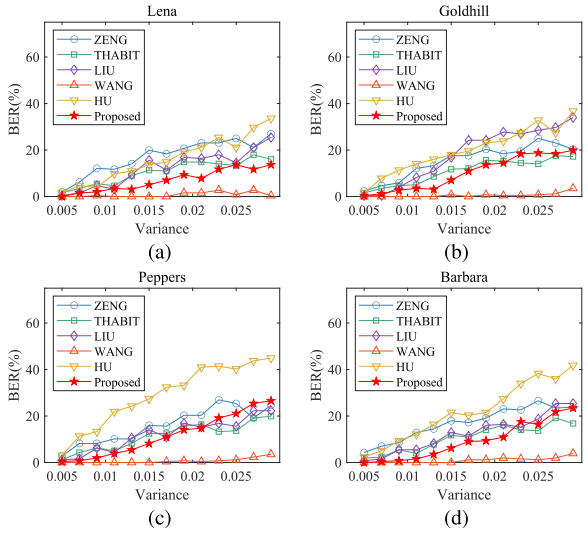


Fig. 13. Robustness to AWGN in case of 256-bit robust watermark.

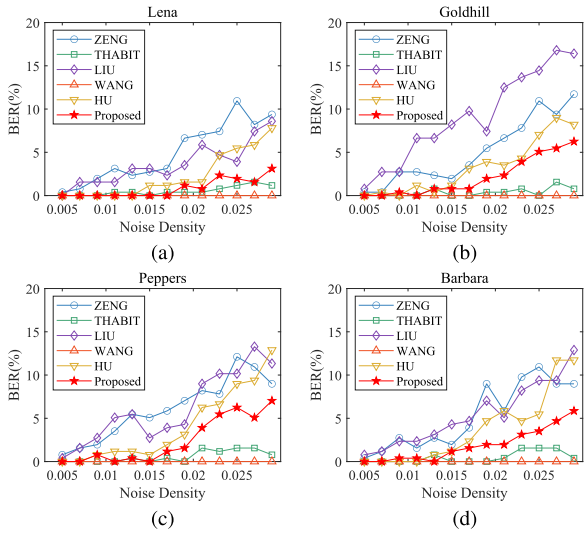


Fig. 14. Robustness to salt-and-pepper noise in case of 256-bit robust watermark.

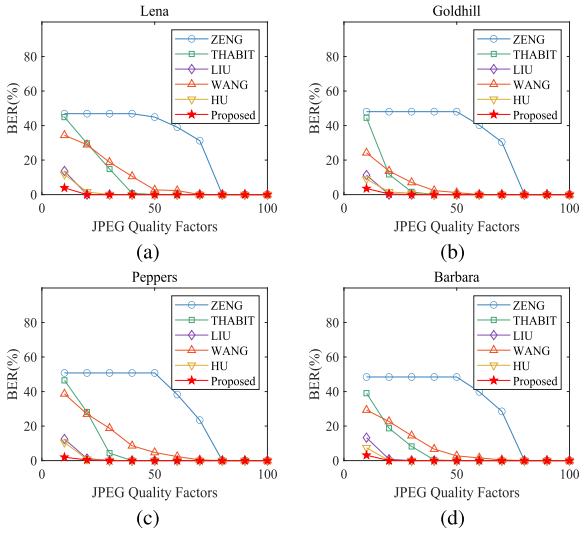


Fig. 15. Robustness to JPEG compression in case of 256-bit robust watermark.

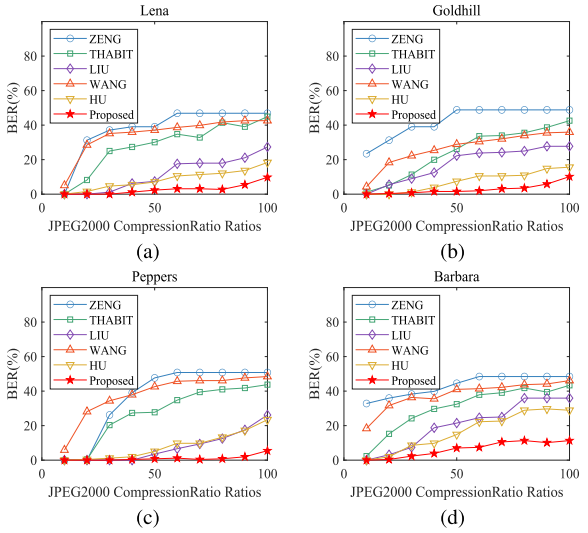


Fig. 16. Robustness to JPEG2000 compression in case of 256-bit robust watermark.

noise, JPEG, JPEG2000, median filtering, and mean filtering attacks on the watermarked images with a 256-bit watermark and assess BERs of the extracted robust watermarks. Figs. 13–16 and Table XI present the resulted performance against AWGN, salt-and-pepper noise, JPEG, JPEG2000, median filtering, and mean filtering, respectively.

By comparing Fig. 13 with Fig. 7, it is found that the performance comparison in the 256-bit case is similar to that in the 128-bit case. A main difference between Figs. 13 and 7 is that compared with the proposed scheme, robustness performance of HU degrades remarkably in the 256-bit case. This attributes to the fact that as the number of PZMs is more than that of Zernike moments on the condition of the same order, HU needs Zernike moments with higher order to accommodate the same robust watermark of larger capacity and consequently degrades the robustness considerably. In addition, the larger the capacity of robust watermark is, the more the number of auxiliary information for reversibility would be, and the higher the probability that inserts the auxiliary information inside the inscribed circle of the robustly watermarked image could be, which in turn weakens the robustness of the robust watermark.

Figs. 14 and 8 show that the performance of all approaches except WANG degrades to some extent. It is noted that the increase in BERs of HU is greater than that of the proposed scheme. This implies that the adaptive normalization and optimized embedding strategy developed in the proposed scheme provide higher robustness.

From Fig. 15 for comparison of performance against JPEG, one can find that both the proposed scheme and HU show outstanding robustness to JPEG compression, which is comparable to LIU but achieves significant improvement over the others. It is also observed that the proposed scheme obtains remarkable gains over LIU and HU for quality factor 10, which implies that the adaptive normalization and the optimized embedding strategy developed in our work leads to higher robustness. Compared with Fig. 9 for 128-bit case, BERs of the proposed scheme and HU at quality factor 10 increase

TABLE XI

ROBUSTNESS TO MEDIAN FILTERING AND MEAN FILTERING IN CASE OF 256-BIT ROBUST WATERMARKING

Methods	median filtering			mean filtering		
	3×3	5×5	7×7	3×3	5×5	7×7
ZENG	25.20	28.03	29.59	24.71	33.40	35.16
THABIT	0.88	10.84	18.85	0.68	8.98	16.02
LIU	1.76	4.79	8.59	1.56	3.81	7.52
WANG	11.62	26.56	32.42	11.62	25.78	32.71
HU	0.00	0.98	8.40	0.00	1.76	7.62
Proposed	**0.00**	**0.59**	**4.30**	**0.00**	**0.29**	**3.71**

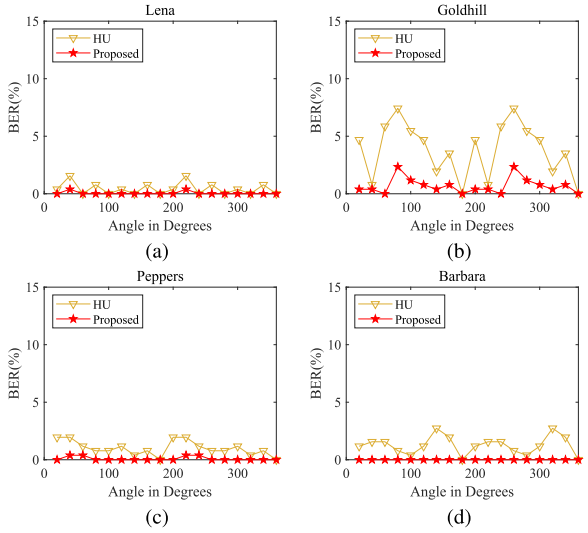


Fig. 17. Robustness to the rotation operations in case of 256-bit robust watermarking.

slightly on the condition that the number of embedded robust watermark bits doubles.

The experimental results in Fig. 16 are similar to those in Fig. 10, where the proposed scheme still achieves significant performance improvement over the other approaches although its robustness degrades to some extent. This demonstrates the effectiveness of the adaptive normalization and optimized embedding strategy implemented in the proposed scheme once again.

The results in Table XI are also similar to those in Table IX. It is shown that the proposed scheme leads to higher robustness than the other approaches. It is also noted that LIU provides better performance than ZENG, THABIT, and WANG. This is because LIU embeds the watermark into smaller image blocks and can therefore use larger embedding strength at the same PSNR. As a result, LIU achieves stronger robustness against both median and mean filtering.

b) Robustness against geometric deformations: As described in the evaluation for the case of 128-bit robust watermark, we mainly examine the proposed scheme on the robustness against geometric deformations such as rotation and scaling by comparing it with HU. Figs. 17 and 18 summarize the performance resilient to rotation and scaling, respectively.

As shown in Fig. 17, both the proposed scheme and HU are sufficiently robust against rotation operations, but their BERs increase in comparison with those in Fig. 11. This comes

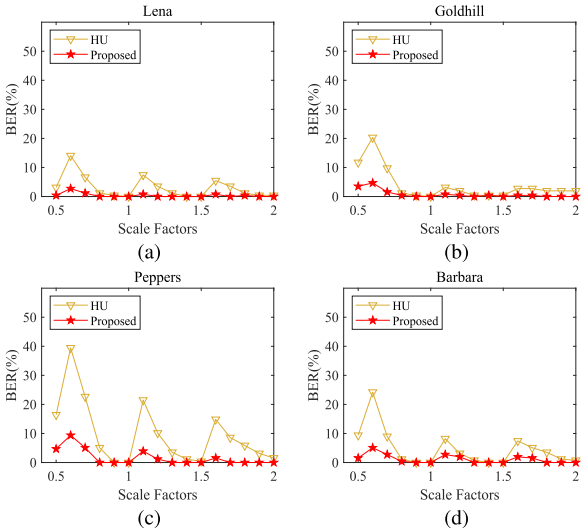


Fig. 18. Robustness to the scaling operations in case of 256-bit robust watermarking.

from the fact that high-order PZMs and Zernike moments used in the case of a larger capacity are more sensitive to rotation operation, and the more auxiliary information for reversibility affects the robust watermark detection. As the developed optimized embedding strategy and rounded error compensation in the proposed scheme remarkably decrease the amount of auxiliary information, the proposed scheme leads to higher robustness than HU.

Comparison between Figs. 18 and 12 clearly shows that the robustness of HU decreases significantly for some specific scaling factors, while the proposed scheme achieves highly competitive performance. This demonstrates the effectiveness of the adaptive normalization, optimized embedding strategy, and rounded error compensation proposed in the proposed scheme. It is noted that these two approaches obtain worse robustness on Image Peppers, which indicates once again that Zernike moments and PZMs are more sensitive to images with more bright regions.

G. Comparative Studies Under Compressive Sensing Attacks

Compressive sensing (CS) [42], [43], [44] is a signal processing technique for efficient signal acquisition and reconstruction. CS theory indicates that an image which is sparse in a certain basis can be reconstructed using a significantly reduced number of samples. For this reason, CS has been widely applied to image compression [45], [46], [47]. Compared with JPEG and JPEG2000, CS achieves the same reconstructed image quality at a lower compression rate, which provides better compression performance [46], [47] and implies that CS is more aggressive. To better evaluate the proposed scheme, we further test its robustness performance against CS.

There are several implementation methods of CS in the literature, e.g. parallel compressive sensing (PCS) [48], block compressive sensing (BCS) [49], and two-dimensional compressive sensing (2DCS) [50]. Among them, 2DCS is chosen as the CS attack for its ability to maintain the intrinsic

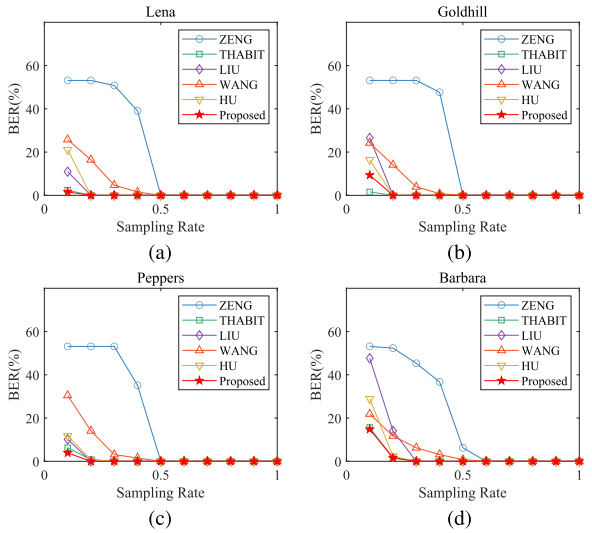


Fig. 19. Robustness to 2DCS in case of 128-bit robust watermark.

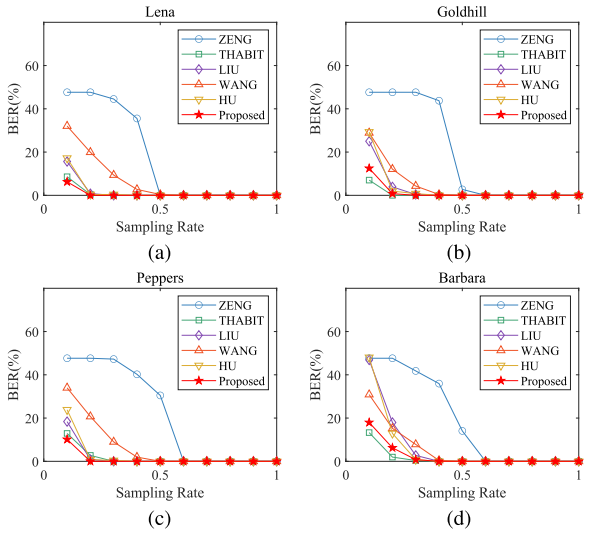


Fig. 20. Robustness to 2DCS in case of 256-bit robust watermark.

image spatial structure and its low computational complexity. As different sampling rates directly affect the reconstructed image quality of 2DCS, the sampling rate is considered a robustness assessment index. Suppose that $S_R = S^2/N^2$ denotes the sampling rate of 2DCS, where S and N represent the length of sampling matrix and image, respectively. The lower the sampling rate is, the stronger the attack by 2DCS would be.

To evaluate the robustness against 2DCS, ZENG, THABIT, LIU, WANG, HU, and the proposed scheme are compared, and their parameters are set as shown in Tables I and II. For fair comparison, all six approaches first embed the same robust watermark of 128 and 256 random bits into four test images involving Lena, Goldhill, Peppers, and Barbara, respectively, all watermarked images are then sampled and reconstructed using 2DCS with different sampling rates, and the watermark detection is finally performed on the reconstructed images to obtain the corresponding BERs. In the simulation, the sampling rate of 2DCS is set as $S_R \in [0.1, 1]$ with step 0.1. Results for 128- and 256-bit watermark are given in Figs. 19 and 20, respectively.

Fig. 19 illustrates that all approaches achieve zero BERs when the sampling rate of 2DCS is greater than 0.6, while their robustness degrades to some extent when the sampling rate is less than 0.6. Among all six compared methods, the proposed scheme obtains the best performance, which achieves BERs below 20% for four typical images under all sampling rates. This is because PZMs represent global features of an image and thus the watermark can be probably recovered even if a small portion of the watermarked image is sampled by 2DCS. It is also seen that, the proposed scheme outperforms HU, which demonstrates once again that PZMs in the proposed scheme have higher robustness than Zernike moments in the HU method. In addition, the robustness of ZENG decreases significantly for sampling rate smaller than 0.5. This is because ZENG embeds the watermark by modifying the arithmetic difference of non-overlapping blocks, and if the reconstructed image resulting from 2DCS fails to recover pixel values at specific positions, the watermark would be difficult to be extracted properly.

Compared with Fig. 19, it can be seen from Fig. 20 that BERs of HU increase significantly at low sampling rates, which is explained as follows. When the watermark bit number increases, HU needs to embed the watermark into higher order Zernike moments corresponding to high-frequency content [51], which is difficult to be reconstructed by 2DCS at low sampling rates. By contrast, as the proposed scheme embeds the same robust watermark in PZMs and develops the adaptive normalization to give different watermark strengths for moments of different orders, it significantly improves robustness.

V. Conclusion

In this paper, we have improved the robustness and capacity of the robust reversible watermarking through embedding optimization and rounded error compensation. The proposed scheme includes two stages, i.e., the first stage inserts the robust watermark for copyright protection while the second stage embeds the reversible watermark for reversibility of the original image. In the first stage, PZMs are first calculated from the original image, PZMs suitable for watermarking are then selected, and a robust watermark is finally inserted in the selected PZMs. In robust watermark embedding, the normalization adaptive to the PZM order is developed, the conventional DC-QIM is enhanced by forcing quantization errors to be integers, and rounded errors in watermarked image generation from watermarked PZMs are compensated. In the second stage, the reversible watermark is constructed by involving quantization errors, reconstruction errors, hashing values for integrity authentication, and LSBs extracted for reserving the room for hashing values storage, and then inserted in regions outside the inscribed circle of the robustly watermarked image. After receiving an image, hashing values are extracted and compared with the newly generated version from the received image. If this integrity authentication shows that no attacks are imposed on the watermarked image, both the robust watermark and the original image are recovered in a

reverse way; otherwise, only the robust watermark is obtained from the received image. Extensive experimental simulations show that the proposed scheme achieves high robustness against CSP such as AWGN, salt-and-pepper noise, JPEG, JPEG2000, median filtering, and mean filtering, geometrical deformations including rotation and scaling, and compressive sensing attacks exemplified by 2DCS. Also, the proposed scheme obtains significant improvement in terms of BER over the state-of-the-arts.

As PZMs in our work are mainly selected in a random way, part of them may be not sufficiently robust to CSP and geometrical deformations. Thus, how to choose more robust PZMs become an interesting topic and deserves further research in future. In our work, one PZM is used as a carrier for one watermark bit, and the subsequent study could investigate how to introduce the patchwork algorithm [52], [53] to implement one watermark bit embedded into multiple PZMs to improve the robustness. In addition, the concerned geometrical deformations in our work are mainly global transformations, RRW methods resilient to local geometrical deformations are required to be investigated in future research.

REFERENCES

[1] O. Evsutin and K. Dzhanashia, "Watermarking schemes for digital images: Robustness overview," *Signal Process., Image Commun.*, vol. 100, Jan. 2022, Art. no. 116523.

[2] Y.-Q. Shi, X. Li, X. Zhang, H.-T. Wu, and B. Ma, "Reversible data hiding: Advances in the past two decades," *IEEE Access*, vol. 4, pp. 3210–3237, 2016.

[3] A. Menendez-Ortiz, C. Feregrino-Uribe, R. Hasimoto-Beltran, and J. J. Garcia-Hernandez, "A survey on reversible watermarking for multimedia content: A robustness overview," *IEEE Access*, vol. 7, pp. 132662–132681, 2019.

[4] C. W. Honsinger, P. W. Jones, M. Rabbani, and J. C. Stoffel, "Lossless recovery of an original image containing embedded data," U.S. Patent US6 278 791 B1, Aug. 21, 2001.

[5] C. D. Vleeschouwer, J. F. Delaigle, and B. Macq, "Circular interpretation of bijective transformations in lossless watermarking for media asset management," *IEEE Trans. Multimedia*, vol. 5, no. 1, pp. 97–105, Mar. 2003.

[6] Z. Ni, Y. Q. Shi, N. Ansari, W. Su, Q. Sun, and X. Lin, "Robust lossless image data hiding designed for semi-fragile image authentication," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 18, no. 4, pp. 497–509, Apr. 2008.

[7] D. Zou, Y. Q. Shi, Z. Ni, and W. Su, "A semi-fragile lossless digital watermarking scheme based on integer wavelet transform," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 10, pp. 1294–1300, Oct. 2006.

[8] R. T. Mohammed and B. E. Khoo, "Robust reversible watermarking scheme based on wavelet-like transform," in *Proc. IEEE Int. Conf. Signal Image Process. Appl.*, Oct. 2013, pp. 354–359.

[9] S. Yu, J. Li, and J. Wang, "A novel robust reversible watermarking scheme based on IWT," in *Cloud Computing and Security*. Cham, Switzerland: Springer, Jun. 2017, pp. 39–48.

[10] D. Coltuc and J. M. Chassery, "Very fast watermarking by reversible contrast mapping," *IEEE Signal Process. Lett.*, vol. 14, no. 4, pp. 255–258, Apr. 2007.

[11] X.-T. Zeng, L.-D. Ping, and X.-Z. Pan, "A lossless robust data hiding scheme," *Pattern Recognit.*, vol. 43, no. 4, pp. 1656–1667, Apr. 2010.

[12] L. An, X. Gao, X. Li, D. Tao, C. Deng, and J. Li, "Robust reversible watermarking via clustering and enhanced pixel-wise masking," *IEEE Trans. Image Process.*, vol. 21, no. 8, pp. 3598–3611, Aug. 2012.

[13] X. Wang, X. Li, and Q. Pei, "Independent embedding domain based two-stage robust reversible watermarking," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 30, no. 8, pp. 2406–2417, Aug. 2020.

[14] X. Liang and S. Xiang, "Robust reversible audio watermarking based on high-order difference statistics," *Signal Process.*, vol. 173, Aug. 2020, Art. no. 107584.

[15] D. Coltuc, "Towards distortion-free robust image authentication," *J. Phys., Conf.*, vol. 77, Jul. 2007, Art. no. 012005.

[16] D. Coltuc and J.-M. Chassery, "Distortion-free robust watermarking: A case study," in *Proc. Secur., Steganography, Watermarking Multimedia Contents IX*, vol. 6505, Feb. 2007, pp. 585–592.

[17] L. An, X. Gao, Y. Yuan, D. Tao, C. Deng, and F. Ji, "Content-adaptive reliable robust lossless data embedding," *Neurocomputing*, vol. 79, pp. 1–11, Mar. 2012.

[18] L. An, X. Gao, Y. Yuan, and D. Tao, "Robust lossless data hiding using clustering and statistical quantity histogram," *Neurocomputing*, vol. 77, no. 1, pp. 1–11, Feb. 2012.

[19] X. Liu et al., "A novel robust reversible watermarking scheme for protecting authenticity and integrity of medical images," *IEEE Access*, vol. 7, pp. 76580–76598, 2019.

[20] N. H. Lestriandoko and D. Rosiyadi, "Reversible image watermarking based on histogram modification and virtual border," in *Proc. 8th Int. Conf. Telecommun. Syst. Services Appl. (TSSA)*, May 2007, pp. 93–104.

[21] C. C. Chang, P. Y. Lin, and J. S. Yeh, "Preserving robustness and removability for digital watermarks using subsampling and difference correlation," *Inf. Sci.*, vol. 179, no. 13, pp. 2283–2293, Jun. 2009.

[22] R. Rajkumar and A. Vasuki, "Reversible and robust image watermarking based on histogram shifting," *Cluster Comput.*, vol. 22, no. 5, pp. 12313–12323, Sep. 2019.

[23] R. Hu and S. Xiang, "Cover-lossless robust image watermarking against geometric deformations," *IEEE Trans. Image Process.*, vol. 30, pp. 318–331, 2021.

[24] R. Hu and S. Xiang, "Lossless robust image watermarking by using polar harmonic transform," *Signal Process.*, vol. 179, Feb. 2021, Art. no. 107833.

[25] W. Wang, J. Ye, T. Wang, and W. Wang, "Reversible data hiding scheme based on significant-bit-difference expansion," *IET Image Process.*, vol. 11, no. 11, pp. 1002–1014, Sep. 2017.

[26] R. Kumar and K.-H. Jung, "Robust reversible data hiding scheme based on two-layer embedding strategy," *Inf. Sci.*, vol. 512, pp. 96–107, Feb. 2020.

[27] S. Xiang and Y. Wang, "Distortion-free robust reversible watermarking by modifying and recording IWT means of image blocks," in *Digital-Forensics and Watermarking*. Cham, Switzerland: Springer, Mar. 2016, pp. 337–349.

[28] I. A. Ansari, M. Pant, and C. W. Ahn, "Artificial bee colony optimized robust-reversible image watermarking," *Multimedia Tools. Appl.*, vol. 76, no. 17, pp. 18001–18025, Sep. 2017.

[29] L. Xiong, X. Han, C.-N. Yang, and Y.-Q. Shi, "Robust reversible watermarking in encrypted image with secure multi-party based on lightweight cryptography," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 32, no. 1, pp. 75–91, Jan. 2022.

[30] X. Liang, S. Xiang, L. Yang, and J. Li, "Robust and reversible image watermarking in homomorphic encrypted domain," *Signal Process., Image Commun.*, vol. 99, Nov. 2021, Art. no. 116462.

[31] H. H. Tsai, H. C. Tseng, and Y. S. Lai, "Robust lossless image watermarking based on α-trimmed mean algorithm and support vector machine," *J. Syst. Softw.*, vol. 83, no. 6, pp. 1015–1028, Jun. 2010.

[32] C.-H. Teh and R. Chin, "On image analysis by the methods of moments," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. PAMI-10, no. 4, pp. 496–513, Jul. 1988.

[33] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y. Q. Shi, "Reversible watermarking algorithm using sorting and prediction," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 7, pp. 989–999, Jul. 2009.

[34] A.-W. Deng and C.-Y. Gwo, "Fast and stable algorithms for high-order pseudo Zernike moments and image reconstruction," *Appl. Math. Comput.*, vol. 334, pp. 239–253, Oct. 2018.

[35] S. Gishkori and B. Mulgrew, "Pseudo-Zernike moments based sparse representations for SAR image classification," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 55, no. 2, pp. 1037–1044, Apr. 2019.

[36] S. X. Liao and M. Pawlak, "On the accuracy of Zernike moments for image analysis," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 20, no. 12, pp. 1358–1364, Dec. 1998.

[37] M. Pawlak and S. X. Liao, "On the recovery of a function on a circular domain," *IEEE Trans. Inf. Theory*, vol. 48, no. 10, pp. 2736–2753, Oct. 2002.

[38] Y. Xin, S. Liao, and M. Pawlak, "Circularly orthogonal moments for geometrically robust image watermarking," *Pattern Recognit.*, vol. 40, no. 12, pp. 3740–3752, Dec. 2007.

[39] N. Kamila, S. Mahapatra, and S. Nanda, "RETRACTED: Invariance image analysis using modified Zernike moments," *Pattern Recognit. Lett.*, vol. 26, no. 6, pp. 747–753, May 2005.

[40] R. Thabit and B. E. Khoo, "A new robust lossless data hiding scheme and its application to color medical images," *Digit. Signal Process.*, vol. 38, pp. 77–94, Mar. 2015.
[41] SIPI Image Database. (1997). [Online]. Available: https://sipi.usc.edu/database/database.php
[42] E. J. Candès, J. Romberg, and T. Tao, "Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 489–509, Feb. 2006.
[43] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.
[44] E. J. Candès and T. Tao, "Near-optimal signal recovery from random projections: Universal encoding strategies?" *IEEE Trans. Inf. Theory*, vol. 52, no. 12, pp. 5406–5425, Dec. 2006.
[45] V. K. Goyal, A. K. Fletcher, and S. Rangan, "Compressive sampling and lossy compression," *IEEE Signal Process. Mag.*, vol. 25, no. 2, pp. 48–56, Mar. 2008.
[46] X. Yuan and R. Haimi-Cohen, "Image compression based on compressive sensing: End-to-end comparison with JPEG," *IEEE Trans. Multimedia*, vol. 22, no. 11, pp. 2889–2904, Nov. 2020.
[47] Z. Chen et al., "Compressive sensing multi-layer residual coefficients for image coding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 30, no. 4, pp. 1109–1120, Apr. 2020.
[48] H. Fang, S. A. Vorobyov, H. Jiang, and O. Taheri, "Permutation meets parallel compressed sensing: How to relax restricted isometry property for 2D sparse signals," *IEEE Trans. Signal Process.*, vol. 62, no. 1, pp. 196–210, Jan. 2014.
[49] L. Gan, "Block compressed sensing of natural images," in *Proc. 15th Int. Conf. Digit. Signal Process.*, Jul. 2007, pp. 403–406.
[50] G. Chen, D. Li, and J. Zhang, "Iterative gradient projection algorithm for two-dimensional compressive sensing sparse image reconstruction," *Signal Process.*, vol. 104, pp. 15–26, Nov. 2014.
[51] A. Khotanzad and Y. H. Hong, "Invariant image recognition by Zernike moments," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 12, no. 5, pp. 489–497, May 1990.
[52] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Syst. J.*, vol. 35, nos. 3–4, pp. 313–336, 1996.
[53] I.-K. Yeo and H. J. Kim, "Modified patchwork algorithm: A novel audio watermarking scheme," *IEEE Trans. Speech Audio Process.*, vol. 11, no. 4, pp. 381–386, Jul. 2003.

Yichao Tang received the B.S. and M.S. degrees from East China Jiaotong University in 2016 and 2020, respectively. He is currently pursuing the Ph.D. degree with South China Agricultural University.

His research interests include multimedia information security, reversible data hiding, and robust data hiding.

Shuai Wang received the B.S. degree from South China Agricultural University, China, in 2021, where he is currently pursuing the M.S. degree.

His research interests include multimedia information security, reversible data hiding, and robust data hiding.

Chuntao Wang (Member, IEEE) received the B.S. and Ph.D. degrees from Sun Yat-sen University, China, in 2002 and 2007, respectively.

From October 2007 to September 2008, he was a Post-Doctoral Fellow with Korea University, South Korea. From November 2008 to November 2010, he was a Post-Doctoral Researcher at Sun Yat-sen University. He is currently an Associate Professor with the School of Mathematics and Informatics, South China Agricultural University. His research interests include information hiding and multimedia signal processing.

Shijun Xiang (Member, IEEE) received the B.S. degree from Chang'an University, China, in 1997, the M.S. degree from Guizhou University, China, in 2000, and the Ph.D. degree from Sun Yat-sen University, China, in 2006.

From 2006 to 2007, he was a Post-Doctoral Researcher with Korea University, Seoul, South Korea. He is currently a Full Professor with the College of Information Science and Technology, Jinan University, Guangzhou, China. He has authored or coauthored over 100 peer-reviewed papers, including the IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE (PAMI), the IEEE TRANSACTIONS ON IMAGE PROCESSING (TIP), the IEEE TRANSACTIONS ON MULTIMEDIA (TMM), and the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY (TCSVT). His current research interests include robust watermarking, reversible data hiding, secure signal processing in encrypted domain, and face spoofing.

Yiu-Ming Cheung (Fellow, IEEE) received the Ph.D. degree from the Department of Computer Science and Engineering, The Chinese University of Hong Kong, Hong Kong, in 2000.

He is currently a Full Professor with the Department of Computer Science, Hong Kong Baptist University, Hong Kong. His research interests include machine learning, computer vision, pattern recognition, data mining, multi-objective optimization, and information hiding.

Dr. Cheung is a fellow of the American Association for the Advancement of Science (AAAS), the Institution of Engineering and Technology (ET), and the British Computer Society (BCS). He serves as an Associate Editor for the IEEE TRANSACTIONS ON CYBERNETICS, the IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTATIONAL INTELLIGENCE, the IEEE TRANSACTIONS ON COGNITIVE AND DEVELOPMENTAL SYSTEMS, the IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS from 2014 to 2020, *Pattern Recognition*, and *Neurocomputing*. For details, please refer to: http://www.comp.hkbu.edu.hk/-ymc.