Transportation Spherical Watermarking

Yuan-Gen Wang, *Member, IEEE*, Guopu Zhu, *Senior Member, IEEE*, and Yun-Qing Shi, *Fellow, IEEE*

***Abstract*— During the past twenty years, there has been a great interest in the study of spread spectrum (SS) watermarking. However, it is still a challenging task to design a secure and robust SS watermarking method. In this paper, we first define a family of secure SS watermarking methods, named as spherical watermarking (SW). The watermarked correlation of SW is defined to be uniformly distributed on a spherical surface, and this makes SW be key-secure against the watermarked-only attack. Then, we propose an implementation of SW, called transportation SW (TSW), which is designed to decrease embedding distortion in a recursive manner using the transportation theory, meanwhile keeping the security of SW. Moreover, we present a theoretical analysis of the embedding distortion and robustness of the proposed method. Finally, extensive experiments are conducted on simulated signals and real images. The experimental results show that TSW is more robust than existing secure SS watermarking methods.**

***Index Terms*— Spread spectrum watermarking, security, watermarked-only attack, embedding distortion, robustness, transportation theory.**

I. Introduction

WATERMARKING security has received more and more attention in the watermarking community. It has been borrowed heavily from cryptology to develop its own theory and methodologies [1]–[9]. In particular, the well-known Kerckhoffs' principle [10], originally introduced in cryptology, provides a basis for the study of watermarking security. Kerckhoffs' principle states that a watermarking system should be secure even if everything about the watermarking method is publicly known, except for the secret key used in message embedding and decoding. Thus, the goal of security attacks is to gain knowledge about the secret key. According to the type of information available to attackers, security attacks can be classified into four categories [2], [7]: known-original attack (KOA), known-message attack (KMA), constant-message attack (CMA), and watermarked-only attack (WOA). Among these four categories, WOA is the most widely studied one and is also the focus of this paper. WOA refers to the scenario where watermarking attackers can only know several watermarked signals, where different and independent messages were embedded. In other words, neither the original versions of watermarked signals nor the embedded messages are available to the attackers. Within the WOA framework, the security can be classified into four levels for spread spectrum (SS) watermarking [7], which are, in order of increasing security, insecurity, key-security, subspace-security, and stego-security, respectively.

Spread spectrum watermarking is one of the most commonly used watermarking techniques [7], [11]–[16]. It performs watermark embedding by adding a modulated pseudo-random sequence to the host signal. The traditional SS watermarking methods, such as the additive SS watermarking [11], the attenuated SS watermarking [12], and the improved SS (ISS) watermarking [13], keep their watermark carriers secret. However, with the knowledge of several watermarked signals, an attacker can disclose the secret carriers of the traditional SS watermarking methods up to a signed permutation. Subsequently, the attacker can launch malicious attacks such as unauthorized decoding and removal.

So far, some studies have been conducted to address the security issue faced by the traditional SS watermarking methods [5], [7], [17]–[21]. In [5], [7], and [17], Bas and Cayre introduced a new class of SS watermarking called circular watermarking (CW) for achieving security against the estimation of secret carriers. CW is defined such that the distribution of its watermarked correlation[1] is circularly symmetric, i.e., is invariant under orthogonal transformations. In addition, they also presented two implementations of CW, namely natural watermarking (NW) and circular extension of improved SS (CW-ISS), respectively. NW can achieve stego-security in the WOA framework [7]. That is to say, attackers cannot get any information about the secret carriers of NW, no matter how many watermarked signals they have. However, the robustness of NW is very poor. Compared with NW, CW-ISS gain much better robustness at the cost of security. Note that CW-ISS is key-secure since the subspace of its secret carriers

Manuscript received July 14, 2016; revised March 2, 2017, August 11, 2017, and December 14, 2017; accepted January 4, 2018. Date of publication January 23, 2018; date of current version February 8, 2018. This work was supported in part by the National Natural Science Foundation of China under Grant 61672554, Grant 61572489, and Grant 61772007, in part by the Basic Research Program of Shenzhen under Grant JCYJ20150630114942312, in part by the Youth Innovation Promotion Association of CAS under Grant 2015299, in part by the NSF of Guangdong Province under Grant 2014A030310112 and Grant 2015A030313602, and in part by the Science and Technology Plan Project of Guangdong Province under Grant 2016B010124014. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Patrick Le callet. *(Corresponding author: Guopu Zhu.)*

Y.-G. Wang is with the School of Computer Science and Education Software, Guangzhou University, Guangzhou 510006, China (e-mail: wangyg@gzhu.edu.cn).

G. Zhu is with the Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, Shenzhen, GD 518055, China, and also with State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China (e-mail: guopu.zhu@gmail.com).

Y.-Q. Shi is with the Department of Electrical and Computer Engineering, New Jersey Institute of Technology, Newark, NJ 07102, USA (e-mail: shi@njit.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIP.2018.2795745

[1] Watermarked correlation refers to the correlation between the watermarked signal and the secret carriers [21].

can be estimated from several watermarked signals. In [19], Mathon *et al.* proposed to apply transportation theory [22] to minimize the embedding distortion of NW, meanwhile keeping the security at the same level. Recently, in [21] they further studied the implementation of transportation NW (TNW) [19] in still images. However, it is still an open problem to apply transportation theory to reduce embedding distortion for robust CW methods, such as CW-ISS. This is because, unlike NW, the components of the watermarked correlation of CW-ISS are not mutually independent. In [18], Mathon *et al.* proposed a novel watermarking method, here named the Hungarian-based CW-ISS (HCW-ISS), to minimize the embedding distortion of CW-ISS by using Hungarian method [23] instead of transportation theory. As a result, HCW-ISS improves the robustness of CW-ISS but does not decrease the security. However, as mentioned in [21], HCW-ISS has a few disadvantages, such as poor performance for long watermark messages, and huge requirement of computational memory.

The aim of this paper is to present a new SS watermarking method that is secure against the watermarked-only attack and is also robust to common image processing operations such as filtering, noise adding, and lossy compression. To do so, we first define a family of secure SS watermarking methods, of which the watermarked correlation has a uniform distribution on a spherical surface. Owing to the distribution of its watermarked correlation, this family of SS watermarking methods is named as spherical watermarking (SW), and achieves key-security. Then, based on SW, we propose a watermarking method called transportation SW (TSW), which can recursively minimize embedding distortion using transportation theory, but without compromising the security of SW. However, the proposed embedding has no guarantee to obtain the global minimal distortion under the SW constraints. Experimental results on both simulated signals and real images demonstrate the superiority of TSW over existing secure SS watermarking methods in terms of robustness.

This paper is a significant extension of our previous conference paper [24]. The extension mainly includes 1) a more detailed survey of related work, 2) a brief introduction of the SS watermarking and transportation theory, 3) the mathematical derivation of the TSW embedding and a discussion of its limitation, 4) a theoretical analysis of the robustness and a more detailed analysis of the embedding distortion, 5) extensive experiments tested on real images and some discussions on the new experimental results. It should also be pointed out that both the proposed method and that of [21] (i.e., TNW) apply the transportation theory to reduce embedding distortion, but there are significant differences between these two methods. First, in [21] the transportation theory is applied to natural watermarking (NW), whereas in this paper it is applied to spherical watermarking. Spherical watermarking and NW are two different SS watermarking schemes. The watermarked correlation of NW is i.i.d. Gaussian, while that of spherical watermarking is uniformly distributed on a spherical surface. Second, in [21] the components of watermarked correlation are independent and Gaussian, so the transport map can be applied directly and independently to each component of the host correlation. In this paper, the components of watermarked correlation are neither independent nor Gaussian. In this case, the transport map is applied to the components of the host correlation one by one in a recursive way. Third, TNW is stego-secure, and the proposed method is key-secure. TNW has a higher security level, but is much less robust than the proposed method and the other key-secure SS watermarking methods (such as CW-ISS [7] and HCW-ISS [18]), as shown in our experiments.

The rest of the paper is organized as follows. In Section II, some notations and preliminaries are briefly introduced. Section III describes the proposed secure SS watermarking method (namely, TSW) in detail. Then, the performance of TSW is theoretically analyzed in Section IV. In Section V, the experimental results on both simulated signals and real images are provided, followed by our conclusion in Section VI.

II. Notations and Background

A. Notations

Throughout the paper, we use bold uppercase letters to denote matrices, bold lowercase letters to denote vectors, and italic lowercase letters to denote scalars. In addition, we have the following notations:

i) $\mathbb{R}^N$ and $\mathbb{R}^{N\times M}$ denote the set of all N-dimensional real vectors and the set of all $N \times M$ real matrices, respectively; $\mathbf{0}$ denotes a zero column vector; $\mathbf{I}_N$ denotes the identity matrix of size $N \times N$.

ii) N_v denotes the dimension of the host (or watermarked) signal vector; N_c denotes the size of the watermark message (in bits).

iii) $\mathbf{m}_{N_c} = [\mathbf{m}_{N_c}(1), ..., \mathbf{m}_{N_c}(N_c)]^T \in \{0, 1\}^{N_c}$ denotes the watermark message; $m \in \{0, 1\}$ denotes a one-bit message. It is assumed that the components of $\mathbf{m}_{N_c}$ are independently Bernoulli distributed with success probability of $1/2$.

iv) $\mathbf{U}_{N_c} = [\mathbf{u}_1, \ldots, \mathbf{u}_{N_c}] \in \mathbb{R}^{N_v\times N_c}$ denotes the secret carriers of an SS watermarking method. The secret carriers $\mathbf{U}_{N_c}$ are also regarded as the secret key. Generally, $\mathbf{U}_{N_c}$ is designed such that $\mathbf{U}_{N_c}^T\mathbf{U}_{N_c} = \mathbf{I}_{N_c}$.

v) $\mathbf{x}$, $\mathbf{w}$ and $\mathbf{s} \in \mathbb{R}^{N_v}$ denote the host, watermark and watermarked signals, respectively. The host signal $\mathbf{x}$ is assumed to be normally distributed with zero mean and covariance matrix $\sigma_{\mathbf{x}}^2\mathbf{I}_{N_v}$.

vi) $\mathbf{z}_{\mathbf{v}}^{N_c} = \mathbf{U}_{N_c}^T\mathbf{v}$ denotes the projection of the vector $\mathbf{v}$ onto span$\{\mathbf{U}_{N_c}\}$. Especially, $\mathbf{z}_{\mathbf{x}}^{N_c} = \mathbf{U}_{N_c}^T\mathbf{x}$ and $\mathbf{z}_{\mathbf{s}}^{N_c} = \mathbf{U}_{N_c}^T\mathbf{s}$ denote the host and watermarked correlations, respectively. Note that the randomness of the watermarked correlation comes from the randomness of both the host signal and the watermark message.

vii) $\mathcal{N}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$ denotes the normal distribution with mean vector $\boldsymbol{\mu}$ and covariance matrix Σ; $\phi(\cdot)$ and $\Phi(\cdot)$ denote the probability density function (PDF) and cumulative density function (CDF) of the univariate standard normal distribution, respectively.

viii) $\mathcal{B}(a, b)$ denotes the beta distribution with parameters a and b. The PDF of $\mathcal{B}(a, b)$ is given by

$$p(v) = \frac{v^{a-1}(1-v)^{b-1}}{\mathrm{B}(a, b)}, \quad v \in [0, 1], \tag{1}$$

where $\mathrm{B}(a, b)$ denotes the beta function defined by

$$\mathrm{B}(a, b) = \int_0^1 t^{a-1}(1-t)^{b-1}\mathrm{d}t, \quad a > 0, b > 0. \quad (2)$$

Moreover, we set $\mathrm{B}(\cdot, 0) = 1$ in this paper.

ix) $\mathcal{S}(N, R)$ denotes the uniform distribution on the surface of an N-sphere with radius R. For $N \geq 2$, the PDF of $\mathcal{S}(N, R)$ is given by

$$p(\mathbf{v}) = \begin{cases} \frac{\Gamma(\frac{N}{2})}{2\pi^{\frac{N}{2}} R^{N-1}}, & \|\mathbf{v}\|_2 = R \\ 0, & \text{else} \end{cases}, \quad (3)$$

where $\Gamma(z) = \int_0^{+\infty} t^{z-1}/e^t \mathrm{d}t$ denotes the Gamma function; for $N = 1$, the PDF of $\mathcal{S}(N, R)$ is given by

$$p(v) = \frac{1}{2}[\delta(v - R) + \delta(v + R)], \quad (4)$$

where $\delta(\cdot)$ denotes the Dirac function.

x) $\mathcal{S}^{\mathbf{m}_N}(N, R)$ denotes a truncated version of $\mathcal{S}(N, R)$. For $N \geq 2$, the PDF of $\mathcal{S}^{\mathbf{m}_N}(N, R)$ is given by

$$p(\mathbf{v}) = \begin{cases} \frac{2^{N-1}\Gamma(\frac{N}{2})}{\pi^{\frac{N}{2}} R^{N-1}}, & \mathbf{v} \in \mathbf{\Omega}_{\mathbf{m}_N} \\ 0, & \text{else} \end{cases}, \quad (5)$$

where $\mathbf{\Omega}_{\mathbf{m}_N} = \{\mathbf{v} \big| \|\mathbf{v}\|_2 = R, \ \mathrm{sgn}(\mathbf{v}(i)) = (-1)^{\mathbf{m}_N(i)} \text{ for } \forall i \in [N]\}$, and $\mathrm{sgn}(\cdot)$ denotes the sign function. For $N = 1$, the PDF of $\mathcal{S}^{\mathbf{m}_1}(N, R)$ is given by

$$p(v) = \begin{cases} 1, & v = (-1)^{\mathbf{m}_1} R, \\ 0, & \text{else.} \end{cases} \quad (6)$$

Note that by the law of total probability [25], we obtain $\mathbf{v} \sim \mathcal{S}(N, R)$ if $\mathbf{v}\big|\mathbf{m}_N \sim \mathcal{S}^{\mathbf{m}_N}(N, R)$ and the components of $\mathbf{m}_{N_c}$ are independently Bernoulli distributed with success probability of $1/2$.

xi) $\mathcal{S}_u(N, R)$ denotes the univariate marginal distribution of $\mathcal{S}(N, R)$. For $N \geq 2$, the PDF of $\mathcal{S}_u(N, R)$ is given by

$$p(v) = \frac{1}{R\mathrm{B}\left(\frac{N-1}{2}, \frac{1}{2}\right)} \left(\frac{R^2 - v^2}{R^2}\right)^{\frac{N-3}{2}}, \ v \in [-R, R]. \quad (7)$$

Note that the distribution $\mathcal{S}_u(N, R)$ with $N = 1$ is not used in this paper, so the description of its PDF is omitted.

xii) $\mathcal{S}_u^m(N, R)$, for $N \geq 2$, denotes a truncated version of $\mathcal{S}_u(N, R)$, where $m \in \{0, 1\}$. Specifically, $\mathcal{S}_u^0(N, R)$ and $\mathcal{S}_u^1(N, R)$ denote the distributions of $\mathcal{S}_u(N, R)$ truncated in the intervals $[0, R]$ and $[-R, 0]$, respectively. Note that by the law of total probability [25], we obtain $v \sim \mathcal{S}_u(N, R)$ if $v\big|m \sim \mathcal{S}_u^m(N, R)$ and m is Bernoulli distributed with success probability of $1/2$.

xiii) $\Psi_N(\cdot)$, for $N \geq 2$, denotes a function on $[0, 1]$ defined by

$$\Psi_N(v) = 2\int_0^v p_N(t)\mathrm{d}t, \ 0 \leq v \leq 1, \quad (8)$$

where $p_N(\cdot)$ denotes the PDF of $\mathcal{S}_u(N, 1)$. Note that $\Psi_N(\cdot)$ is monotonically increasing on the interval $[0, 1]$, therefore, $\Psi_N(\cdot)$ is invertible on $[0, 1]$. For $N \geq 2$, we denote $\Psi_N^{-1}(\cdot)$ as the inverse function of $\Psi_N(\cdot)$. In addition, we set $\Psi_1^{-1}(\cdot) = 1$ in this paper.

B. SS Watermarking

In general, an SS watermarking method consists of two parts, namely the watermark embedding and the watermark decoding. In the embedding part, a watermark signal $\mathbf{w}$ is first generated with the host signal $\mathbf{x}$ and the watermark message $\mathbf{m}_{N_c}$. Then, the watermarked signal $\mathbf{s}$ is obtain by the following embedding rule:

$$\mathbf{s} = \mathbf{x} + \mathbf{w} = \mathbf{x} + \sum_{i=1}^{N_c} \chi(\mathbf{m}_{N_c}(i), \mathbf{x})\mathbf{u}_i, \quad (9)$$

where $\chi(\mathbf{m}_{N_c}(i), \mathbf{x})$ denotes a modulation of the message $\mathbf{m}_{N_c}(i)$ on $\mathbf{x}$. Note that the security of the above process is provided by the secret key $\mathbf{U}_{N_c}$. In the receiver part, a possibly corrupted signal of $\mathbf{s}$, denoted as $\mathbf{y}$, is received by the decoder. Usually, the received signal $\mathbf{y}$ is modeled as

$$\mathbf{y} = \mathbf{s} + \mathbf{n}, \quad (10)$$

where $\mathbf{n}$ denotes the noise caused during the transmission of the watermarked signal $\mathbf{s}$, and is assumed, in our theoretical analysis, to be an additive white Gaussian noise (AWGN) with zero-mean and covariance matrix $\sigma_{\mathbf{n}}^2 \mathbf{I}_{N_v}$. With the help of the secret key $\mathbf{U}_{N_c}$, the watermark message is decoded by

$$\hat{\mathbf{m}}_{N_c}(i) = \mathrm{sgn}\left(\mathbf{z}_{\mathbf{y}}^{N_c}(i)\right), \quad i \in [N_c], \quad (11)$$

where $\mathbf{z}_{\mathbf{y}}^{N_c} = \mathbf{U}_{N_c}^T \mathbf{y}$ and $\hat{\mathbf{m}}_{N_c}$ denotes the estimate of the watermark message.

Here we also review three commonly used measures of digital watermarking, which are the watermark-to-content power ratio (WCR), the signal-to-noise power ratio (SNR) and the bit error rate (BER), respectively. The WCR is used to evaluate the embedding distortion, and is defined by

$$\mathrm{WCR}_{[\mathrm{dB}]} = 10\log_{10}\left(\frac{\sigma_{\mathbf{w}}^2}{\sigma_{\mathbf{x}}^2}\right), \quad (12)$$

where $\sigma_{\mathbf{w}}^2$ and $\sigma_{\mathbf{x}}^2$ denote the powers of the watermark signal and the host signal, respectively. The SNR is used to evaluate the intensity of the transmission noise, and is defined by

$$\mathrm{SNR}_{[\mathrm{dB}]} = 10\log_{10}\left(\frac{\sigma_{\mathbf{x}}^2}{\sigma_{\mathbf{n}}^2}\right), \quad (13)$$

where $\sigma_{\mathbf{n}}^2$ denote the power of the transmission noise. The BER is used to evaluate the decoding performance, and is defined by

$$P_e = \frac{1}{N_c}\sum_{i=1}^{N_c} \Pr\{\hat{\mathbf{m}}(i) \neq \mathbf{m}(i)\}, \quad (14)$$

where $\Pr\{A\}$ denotes the probability that the event A occurs.

C. Basic Theories for TSW

In this subsection, we briefly introduce two basic theories that will be applied to the proposed method. The first is the transportation theory developed by Monge [26] and Kantorovich [27]. Given a random vector $\mathbf{x} \sim \mathcal{X}$ and a target distribution $\mathcal{S}$, Monge [26] proposed to find a map $T : \mathbf{y} = T(\mathbf{x})$ such that $\min\{\int c(\mathbf{x}, \mathbf{y}) \mathrm{d}\mathcal{X}(\mathbf{x}) | \mathcal{Y} = \mathcal{X} \circ T^{-1}\}$ is achieved, where c denotes a cost function, and $\circ$ denotes the composition of functions. We define $h(\mathbf{x} - \mathbf{y}) = c(\mathbf{x}, \mathbf{y})$. If $\mathbf{x}$ is one-dimensional and h is a convex function, then the optimal map T is obtained by

$$T = P_{\mathcal{Y}}^{-1} \circ P_{\mathcal{X}}, \tag{15}$$

where $P_{\mathcal{X}}$ and $P_{\mathcal{Y}}^{-1}$ denote the CDF of $\mathcal{X}$ and the inverse (or quantile) CDF of $\mathcal{Y}$, respectively. Moreover, the result of Eq. (15) can be extended to the multidimensional case if the Knott-Smith criterion [22] is satisfied. However, Monge's problem described above is ill-posed for some cases. To address this limitation, Kantorovich [27] generalized Monge's problem by finding a joint distribution of $\mathbf{x}$ and $\mathbf{s}$, denoted as γ, to realize $\min\{\int c(\mathbf{x}, \mathbf{y}) \mathrm{d}\gamma(\mathbf{x}, \mathbf{y}) | \gamma \in \Pi(\mathcal{X}, \mathcal{Y})\}$, where $\Pi(\mathcal{X}, \mathcal{Y})$ denotes the set of all distributions whose marginals on the spaces of $\mathbf{x}$ and $\mathbf{y}$ are $\mathcal{X}$ and $\mathcal{Y}$, respectively.

The second is about the uniform distribution on a spherical surface, which is described by the following theorem:

Theorem 1 [28], [29]: Let $\mathbf{v} = [v_1, \ldots, v_N] \in \mathbb{R}^N$ denote a random vector. For $i \in [N]$, we set $\mathbf{v}^{(i)} = [v_1, v_2, \ldots, v_{i-1}, v_{i+1}, \ldots, v_N] \in \mathbb{R}^{N-1}$. Then $\mathbf{v} \sim \mathcal{S}(N, R)$ if and only if for any $i \in [N]$, $v_i \sim \mathcal{S}_u(N, R)$ and $\mathbf{v}^{(i)} \big| (v_i = r_i) \sim \mathcal{S}(N-1, \sqrt{R^2 - r_i^2})$.

For details of the proof of Theorem 1, refer to [28, Lemma 2] or [29, Th. 2.6].

III. Proposed Method

A. Spherical Watermarking

Before introducing a new specific watermarking method, a family of secure watermarking methods, called spherical watermarking (SW), is defined as follows:

Definition 1: A watermarking method is called spherical if its watermarked correlation is uniformly distributed on a spherical surface.

By Definition 1, the distribution of the watermarked correlation of an SW method depends only on the distance to the origin. Hence, SW can be regarded as a kind of the CW introduced in [7]. Note that both NW and CW-ISS (i.e., the two main implementations of CW) do not belong to the family of SW, because, as shown in [7, Figs. 7 and 8], their watermarked correlations are not uniformly distributed on a spherical surface; that is, any implementation of SW, including the following proposed method, is essentially different from NW and CW-ISS. It should also be pointed out that the watermarked correlation of CW-ISS will be exactly distributed on a spherical surface if the attenuation factor λ in [7] is manually set to 1. However, the parameter λ of CW-ISS is determined, not by a manual setting, but by minimizing the error probability of decoding, as done in ISS [13]. From [13, Eq. 20] and [30, Eq. 13], we can see that it is impossible for the optimal λ to take 1, unless $\sigma_{\mathbf{n}}^2 = 0$ (i.e., there is not any attack noise). Evidently, the condition that $\sigma_{\mathbf{n}}^2 = 0$ is totally impractical for digital watermarking.

In the WOA framework, the security of an SS watermarking method is determined by the distribution of its watermarked correlation. Under the assumption of normal distribution of the host signal, we can conclude that the host correlation is normally distributed. Thus, the watermarked correlation of an SW method does not have the same distribution as the host correlation. This means that SW is not stego-secure. However, by Definition 1, the distribution of the watermarked correlation of SW is also circular. As stated in [7], the circularity of the distribution implies key-security. Therefore, SW is key-secure in the WOA framework.

B. TSW Embedding

In the following, we propose an implementation of SW, named transportation SW (TSW), which aims to minimize the embedding distortion with transportation theory [22]. The embedding function of TSW is expressed by

$$\mathbf{s} = \mathbf{x} + \mathbf{U}_{N_c} \left(F_{N_c} \left(\mathbf{m}_{N_c}, \mathbf{z}_{\mathbf{x}}^{N_c} \right) - \mathbf{z}_{\mathbf{x}}^{N_c} \right), \tag{16}$$

where $F_{N_c}(\mathbf{m}_{N_c}, \mathbf{z}_{\mathbf{x}}^{N_c})$ (note that $\mathbf{z}_{\mathbf{s}}^{N_c} = F_{N_c}(\mathbf{m}_{N_c}, \mathbf{z}_{\mathbf{x}}^{N_c})$ is obtained by left multiplying Eq. (16) by $\mathbf{U}_{N_c}^T$) is designed to

$$\begin{aligned} \min \quad & E\left[\left\| \mathbf{z}_{\mathbf{s}}^{N_c} - \mathbf{z}_{\mathbf{x}}^{N_c} \right\|_2^2 \right] \\ \text{s.t.} \quad & \mathbf{z}_{\mathbf{s}}^{N_c} \big| (\mathbf{m}_{N_c}, R_0) \sim \mathcal{S}^{\mathbf{m}_{N_c}} (N_c, R_0), \end{aligned} \tag{17}$$

where $R_0 = \alpha\sqrt{N_c}$, and α is the embedding strength of TSW. In Eq. (17), the first term $\min E[\|\mathbf{z}_{\mathbf{s}}^{N_c} - \mathbf{z}_{\mathbf{x}}^{N_c}\|_2^2]$ is used to minimize the average embedding distortion of the proposed method; while the second term $\mathbf{z}_{\mathbf{s}}^{N_c} \big| (\mathbf{m}_{N_c}, R_0) \sim \mathcal{S}^{\mathbf{m}_{N_c}} (N_c, R_0)$ leads to $\mathbf{z}_{\mathbf{s}}^{N_c} \big| R_0 \sim \mathcal{S}(N_c, R_0)$, as noted in x) of Section II-A. This makes the proposed method be a spherical watermarking method.

The constrained optimization problem given by Eq. (17) can be regarded as a Monge-Kantorovich problem [26], [27]. However, the non trivial distribution of the watermarked correlation of SW makes it difficult to directly perform optimal transport. In order to solve the optimization problem with the transportation theory, we propose a recursive solution, in which each recursive step has two problems to be addressed. Let $\mathbf{m}_{N_c-i} = [\mathbf{m}_{N_c}(1), ..., \mathbf{m}_{N_c}(N_c - i)]^T$, $\mathbf{U}_{N_c-i} = [\mathbf{u}_1, \ldots, \mathbf{u}_{N_c-i}]$, $\mathbf{z}_{\mathbf{x}}^{N_c-i} = \mathbf{U}_{N_c-i}^T \mathbf{x}$, and $\mathbf{z}_{\mathbf{s}}^{N_c-i} = \mathbf{U}_{N_c-i}^T \mathbf{s}$ for $i \in [N_c - 1]$. Then, at the i-th recursive step ($i = 0, \ldots, N_c - 2$), the two problems can be described as follows:

Problem 1: Find an optimal map $\mathbf{z}_{\mathbf{s}}^{N_c-i}(N_c - i) = f_{N_c-i}(\mathbf{m}_{N_c-i}(N_c - i), \mathbf{z}_{\mathbf{x}}^{N_c-i}(N_c - i))$ to address the problem as follows:

$$\begin{aligned} \min \ & E\left[\left(\mathbf{z}_{\mathbf{s}}^{N_c-i}(N_c - i) - \mathbf{z}_{\mathbf{x}}^{N_c-i}(N_c - i) \right)^2 \right] \\ \text{s.t.} \ & \mathbf{z}_{\mathbf{s}}^{N_c-i}(N_c - i) \big| (\mathbf{m}_{N_c-i}(N_c - i), R_i) \\ & \quad \sim \mathcal{S}_u^{\mathbf{m}_{N_c-i}(N_c-i)} (N_c - i, R_i), \end{aligned} \tag{18}$$

where $R_i = \sqrt{\alpha^2\ N_c - \sum_{j=0}^{i-1}(\mathbf{z}_\mathbf{s}^{N_c-j}(N_c-j))^2}$. As explained in xii) of Section II-A, the second term of Eq. (18) means $\mathbf{z}_\mathbf{s}^{N_c-i}(N_c-i)\big|R_i \sim \mathcal{S}_u\left(N_c-i, R_i\right)$.

Problem 2: Find a map $\mathbf{z}_\mathbf{s}^{N_c-1-i} = F_{N_c-1-i}(\mathbf{m}_{N_c-1-i}, \mathbf{z}_\mathbf{x}^{N_c-1-i})$ by the following optimization:

$$\begin{aligned} &\min\ E\left[\left\|\mathbf{z}_\mathbf{s}^{N_c-1-i} - \mathbf{z}_\mathbf{x}^{N_c-1-i}\right\|_2^2\right] \\ &\text{s.t. } \mathbf{z}_\mathbf{s}^{N_c-1-i}\big|(\mathbf{m}_{N_c-1-i}, R_{i+1}) \\ &\quad \sim \mathcal{S}^{\mathbf{m}_{N_c-1-i}}\left(N_c-1-i, R_{i+1}\right). \end{aligned} \tag{19}$$

Also, as explained in x) of Section II-A, the second term of Eq. (19) means $\mathbf{z}_\mathbf{s}^{N_c-1-i}\big|R_{i+1} \sim \mathcal{S}\left(N_c-1-i, R_{i+1}\right)$.

It should be pointed out that at the i-th recursive step ($i = 0, \ldots, N_c-2$) of the above method, Problem 2 has the same type as the original problem given in Eq. (17), except for the dimension of the input (i.e., the host correlation and the watermark message). To tackle Problem 2, we further divide it into two problems at the next recursive step in the same way. Thus, the original problem is solved by calling itself recursively with simpler and simpler inputs, and, in fact, the main task of the recursive method is to solve Problem 1.

As shown by Eq. (18), Problem 1 can be regarded as an optimization problem described in Section II-C. Therefore, we solve it by using the transportation theory. Note that $\mathbf{m}_{N_c-i}(N_c-i) = \mathbf{m}_{N_c}(N_c-i)$, $\mathbf{z}_\mathbf{x}^{N_c-i}(N_c-i) = \mathbf{z}_\mathbf{x}^{N_c}(N_c-i)$, and $\mathbf{z}_\mathbf{s}^{N_c-i}(N_c-i) = \mathbf{z}_\mathbf{s}^{N_c}(N_c-i)$. For brevity, in the following we use $\mathbf{m}_{N_c}(N_c-i)$, $\mathbf{z}_\mathbf{x}^{N_c}(N_c-i)$, and $\mathbf{z}_\mathbf{s}^{N_c}(N_c-i)$ to denote $\mathbf{m}_{N_c-i}(N_c-i)$, $\mathbf{z}_\mathbf{x}^{N_c-i}(N_c-i)$, and $\mathbf{z}_\mathbf{s}^{N_c-i}(N_c-i)$, respectively. Since the constraint $\mathbf{z}_\mathbf{s}^{N_c}(N_c-i)\big|(\mathbf{m}_{N_c}(N_c-i), R_i) \sim \mathcal{S}_u^{\mathbf{m}_{N_c}(N_c-i)}(N_c-i, R_i)$ in Eq. (18) should be satisfied, we have, for $i = 0, \ldots, N_c-2$,

$$\begin{cases} \mathbf{z}_\mathbf{s}^{N_c}(N_c-i)\big|(\mathbf{m}_{N_c}(N_c-i) = 0, R_i) \sim \mathcal{S}_u^0(N_c-i, R_i), \\ \mathbf{z}_\mathbf{s}^{N_c}(N_c-i)\big|(\mathbf{m}_{N_c}(N_c-i) = 1, R_i) \sim \mathcal{S}_u^1(N_c-i, R_i). \end{cases} \tag{20}$$

Moreover, we can easily obtain $\mathbf{z}_\mathbf{x}^{N_c}(N_c-i) \sim \mathcal{N}\left(0, \sigma_\mathbf{x}^2\right)$ by modeling the distribution of $\mathbf{x}$ as the Gaussian distribution $\mathcal{N}(\mathbf{0}, \sigma_\mathbf{x}^2\mathbf{I}_{N_v})$. Then, according to the transportation theory expressed by Eq. (15), we further have, for $i = 0, \ldots, N_c-2$,

$$\begin{cases} f_{N_c-i}\left(0, \mathbf{z}_\mathbf{x}^{N_c}(N_c-i)\right) = P_{\mathcal{S}_u^0}^{-1}\left(\Phi\left(\frac{\mathbf{z}_\mathbf{x}^{N_c}(N_c-i)}{\sigma_\mathbf{x}}\right)\right), \\ f_{N_c-i}\left(1, \mathbf{z}_\mathbf{x}^{N_c}(N_c-i)\right) = P_{\mathcal{S}_u^1}^{-1}\left(\Phi\left(\frac{\mathbf{z}_\mathbf{x}^{N_c}(N_c-i)}{\sigma_\mathbf{x}}\right)\right), \end{cases} \tag{21}$$

where $P_{\mathcal{S}_u^0}^{-1}$ and $P_{\mathcal{S}_u^1}^{-1}$ denote the quantile CDFs of the distributions $\mathcal{S}_u^0(N_c-i, R_i)$ and $\mathcal{S}_u^1(N_c-i, R_i)$, respectively. From Eqs. (8) and (20), we obtain, for $i = 0, \ldots, N_c-2$,

$$\begin{cases} P_{\mathcal{S}_u^0}^{-1}(v) = R_i\Psi_{N_c-i}^{-1}(v), \\ P_{\mathcal{S}_u^1}^{-1}(v) = -R_i\Psi_{N_c-i}^{-1}(1-v), \end{cases} \tag{22}$$

where $\Psi_{N_c-i}^{-1}(\cdot)$ denotes the inverse function of $\Psi_{N_c-i}(\cdot)$. Substituting (22) into (21), we have, for $i = 0, \ldots, N_c-2$,

$$\begin{cases} f_{N_c-i}\left(0, \mathbf{z}_\mathbf{x}^{N_c}(N_c-i)\right) = R_i\Psi_{N_c-i}^{-1}\left(\Phi\left(\frac{\mathbf{z}_\mathbf{x}^{N_c}(N_c-i)}{\sigma_\mathbf{x}}\right)\right), \\ f_{N_c-i}\left(1, \mathbf{z}_\mathbf{x}^{N_c}(N_c-i)\right) = -R_i\Psi_{N_c-i}^{-1}\left(1-\Phi\left(\frac{\mathbf{z}_\mathbf{x}^{N_c}(N_c-i)}{\sigma_\mathbf{x}}\right)\right). \end{cases} \tag{23}$$

Considering that $\mathbf{z}_\mathbf{s}^{N_c}(N_c-i) = f_{N_c-i}(\mathbf{m}_{N_c}(N_c-i), \mathbf{z}_\mathbf{x}^{N_c}(N_c-i))$ and $\Phi(-t) = 1-\Phi(t)$, we get from Eq. (23) that for $i = 0, \ldots, N_c-2$,

$$\begin{aligned} \mathbf{z}_\mathbf{s}^{N_c}(N_c-i) &= (-1)^{\mathbf{m}_{N_c}(N_c-i)}R_i \\ &\quad \times\Psi_{N_c-i}^{-1}\left(\Phi\left(\frac{(-1)^{\mathbf{m}_{N_c}(N_c-i)}\mathbf{z}_\mathbf{x}^{N_c}(N_c-i)}{\sigma_\mathbf{x}}\right)\right), \end{aligned} \tag{24}$$

where $R_i = \sqrt{\alpha^2\ N_c - \sum_{j=0}^{i-1}(\mathbf{z}_\mathbf{s}^{N_c}(N_c-j))^2}$.

At the last recursive call, i.e., the (N_c-2)-th recursive call, Problem 2 becomes a one-dimensional optimization problem, as shown by Eq. (19). Then, according to the constraint $\mathbf{z}_\mathbf{s}^1|(\mathbf{m}_1, R_{N_c-1}) \sim \mathcal{S}^{\mathbf{m}_1}(1, R_{N_c-1})$ in Eq. (19) (note that the PDF of $\mathcal{S}^{\mathbf{m}_1}(1, \cdot)$ is given by Eq. (6)), we directly obtain

$$\mathbf{z}_\mathbf{s}^{N_c}(1) = (-1)^{\mathbf{m}_{N_c}(1)}R_{N_c-1}, \tag{25}$$

where $R_{N_c-1} = \sqrt{\alpha^2\ N_c - \sum_{j=0}^{N_c-2}(\mathbf{z}_\mathbf{s}^{N_c}(N_c-j))^2}$.

Finally, because $F_{N_c}(\mathbf{m}_{N_c}, \mathbf{z}_\mathbf{x}^{N_c}) = \mathbf{z}_\mathbf{s}^{N_c}$, the embedding function of TSW can be obtained by incorporating Eqs. (24) and (25) into Eq. (16); whereas, the watermark decoding of TSW is performed using Eq. (11), just as most other SS watermarking methods did.

As shown in the derivation of Eq. (24), for $i = 2, \ldots, N_c$, $\mathbf{z}_\mathbf{s}^{N_c}(i)$ is calculated to satisfy the constraint of Eq. (18), hence we obtain that $\mathbf{z}_\mathbf{s}^{N_c}(i)\big|R_{N_c-i} \sim \mathcal{S}_u\left(i, R_{N_c-i}\right)$. Then, by the sufficiency part of Theorem 1, from $i = 1$ to N_c-1, if $\mathbf{z}_\mathbf{s}^i\big|R_{N_c-i} \sim \mathcal{S}\left(i, R_{N_c-i}\right)$ holds, $\mathbf{z}_\mathbf{s}^{i+1}\big|R_{N_c-i-1} \sim \mathcal{S}\left(i+1, R_{N_c-i-1}\right)$ also holds. When $i = 1$, according to Eq. (25), we have $\mathbf{z}_\mathbf{s}^1\big|R_{N_c-1} \sim \mathcal{S}(1, R_{N_c-1})$. Therefore, by mathematical induction, we have $\mathbf{z}_\mathbf{s}^{N_c}\big|R_0 \sim \mathcal{S}\left(N_c, \alpha\sqrt{N_c}\right)$. This means that TSW really belongs to the family of SW, thus, as discussed in Section III-A, is key-secure. Note that the derivation of Eq. (24) is based on the assumption of i.i.d. Gaussian host signal. If the host signal is not i.i.d. Gaussian, then the watermarked correlation of TSW is no longer uniformly distributed on a spherical surface and then the key-security of TSW cannot be guaranteed. So, i.i.d. Gaussian host signal is absolutely needed for the proposed method.

It is also worth noting that the solution given by Eqs. (24) and (25) does not guarantee the global minimization of the problem defined by Eq (17). As shown in Eqs. (24) and (25), the map from $\mathbf{z}_\mathbf{x}^{N_c}(i)$ to $\mathbf{z}_\mathbf{s}^{N_c}(i)$ depends only on $\mathbf{z}_\mathbf{x}^{N_c}(i)$, ..., $\mathbf{z}_\mathbf{x}^{N_c}(N_c)$ for $i \in [N_c]$. Therefore, the Jacobian matrix of the transport map from $\mathbf{z}_\mathbf{x}^{N_c}$ to $\mathbf{z}_\mathbf{s}^{N_c}$ is an upper triangular matrix, not a symmetric and positive semi-definite matrix. Then, by the Knott-Smith criterion [22], the sufficient conditions of the minimization are not satisfied, and the optimality of the transport map is not guaranteed.

IV. Performance Analysis

In this section, we theoretically analyze the performance of the proposed method, called TSW, in terms of the WCR and BER by modeling the host signals as independent and identically distributed (i.i.d.) Gaussian signals. Note that as mentioned in Section II-B, the WCR and BER are usually used to evaluate the embedding distortion and robustness of watermarking, respectively.

A. Embedding Distortion

By Eqs. (9) and (16), we have $\mathbf{w} = \mathbf{s} - \mathbf{x} = \mathbf{U}_{N_c}(\mathbf{z}_\mathbf{s}^{N_c} - \mathbf{z}_\mathbf{x}^{N_c})$. Since $\mathbf{U}_{N_c}^T\mathbf{U}_{N_c} = \mathbf{I}_{N_c}$, the power of watermark signal of TSW can be expressed by

$$\begin{aligned} E\left[\mathbf{w}^T\mathbf{w}\right] &= E\left[\left(\mathbf{U}_{N_c}(\mathbf{z}_\mathbf{s}^{N_c} - \mathbf{z}_\mathbf{x}^{N_c})\right)^T \mathbf{U}_{N_c}(\mathbf{z}_\mathbf{s}^{N_c} - \mathbf{z}_\mathbf{x}^{N_c})\right] \\ &= E\left[(\mathbf{z}_\mathbf{s}^{N_c} - \mathbf{z}_\mathbf{x}^{N_c})^T(\mathbf{z}_\mathbf{s}^{N_c} - \mathbf{z}_\mathbf{x}^{N_c})\right] \\ &= E\left[\sum_{i=1}^{N_c}(\mathbf{z}_\mathbf{s}^{N_c}(i) - \mathbf{z}_\mathbf{x}^{N_c}(i))^2\right]. \end{aligned} \tag{26}$$

As analyzed in Section III-B, $\mathbf{z}_\mathbf{s}^{N_c} \sim \mathcal{S}(N_c, \alpha\sqrt{N_c})$ and $\mathbf{z}_\mathbf{x}^{N_c}(i) \sim \mathcal{N}\left(0, \sigma_\mathbf{x}^2\right)$ for every $i \in [N_c]$. Hence, from Eq. (26) we have

$$E\left[\mathbf{w}^T\mathbf{w}\right] = \alpha^2 N_c + \sigma_\mathbf{x}^2 N_c - 2\sum_{i=1}^{N_c} E\left[\mathbf{z}_\mathbf{s}^{N_c}(i)\mathbf{z}_\mathbf{x}^{N_c}(i)\right]. \tag{27}$$

According to Eqs. (24) and (25), we obtain that for $i \in [N_c]$,

$$\begin{aligned} \mathbf{z}_\mathbf{s}^{N_c}(i)\mathbf{z}_\mathbf{x}^{N_c}(i) &= (-1)^{\mathbf{m}_{N_c}(i)} R_{N_c-i} \\ &\quad \times \Upsilon_i\left(\frac{(-1)^{\mathbf{m}_{N_c}(i)}\mathbf{z}_\mathbf{x}^{N_c}(i)}{\sigma_\mathbf{x}}\right)\mathbf{z}_\mathbf{x}^{N_c}(i), \end{aligned} \tag{28}$$

where

$$R_{N_c-i} = \sqrt{\alpha^2 N_c - \sum_{j=0}^{N_c-i-1}(\mathbf{z}_\mathbf{s}^{N_c}(N_c - j))^2}, \tag{29}$$

$$\Upsilon_i(t) = \Psi_i^{-1}(\Phi(t)), \tag{30}$$

and $\Psi_i^{-1}(\cdot)$ is defined in Section II-A. Note that here $\Upsilon_1(\cdot) = 1$ since we set $\Psi_1^{-1}(\cdot) = 1$. From Eqs. (24) and (25), we can conclude that $\sum_{j=0}^{N_c-i-1}(\mathbf{z}_\mathbf{s}^{N_c}(N_c - j))^2$ is only dependent on $\mathbf{z}_\mathbf{x}^{N_c}(i+1), \ldots, \mathbf{z}_\mathbf{x}^{N_c}(N_c)$ for any $i \in [N_c]$. Moreover, as shown in [2], $\mathbf{z}_\mathbf{x}^{N_c}(1), \ldots, \mathbf{z}_\mathbf{x}^{N_c}(N_c)$ are mutually uncorrelated. Therefore, $\sum_{j=0}^{N_c-i-1}(\mathbf{z}_\mathbf{s}^{N_c}(N_c - j))^2$ is uncorrelated with $\mathbf{z}_\mathbf{x}^{N_c}(i)$ and further uncorrelated with $(-1)^{\mathbf{m}_{N_c}(i)}\mathbf{z}_\mathbf{x}^{N_c}(i)$ for $i \in [N_c]$. Then, for every $i \in [N_c]$, we have

$$\begin{aligned} E\left[\mathbf{z}_\mathbf{s}^{N_c}(i)\mathbf{z}_\mathbf{x}^{N_c}(i)\right] &= E\left[R_{N_c-i}\right] \\ &\quad \times E\left[(-1)^{\mathbf{m}_{N_c}(i)}\mathbf{z}_\mathbf{x}^{N_c}(i)\Upsilon_i\left(\frac{(-1)^{\mathbf{m}_{N_c}(i)}\mathbf{z}_\mathbf{x}^{N_c}(i)}{\sigma_\mathbf{x}}\right)\right]. \end{aligned} \tag{31}$$

To further calculate $E\left[\mathbf{z}_\mathbf{s}^{N_c}(i)\mathbf{z}_\mathbf{x}^{N_c}(i)\right]$, in the following we first consider the first term of the right side of Eq. (31). Because $\sum_{j=0}^{N_c-1}\left(\frac{\mathbf{z}_\mathbf{s}^{N_c}(N_c-j)}{\alpha\sqrt{N_c}}\right)^2 = 1$, it follows that for $i \in [N_c]$,

$$\begin{aligned} R_{N_c-i} &= \sqrt{\alpha^2 N_c - \sum_{j=0}^{N_c-i-1}(\mathbf{z}_\mathbf{s}^{N_c}(N_c - j))^2} \\ &= \alpha\sqrt{N_c}\sqrt{1 - \sum_{j=0}^{N_c-i-1}\left(\frac{\mathbf{z}_\mathbf{s}^{N_c}(N_c - j)}{\alpha\sqrt{N_c}}\right)^2} \\ &= \alpha\sqrt{N_c}\sqrt{\sum_{j=N_c-i}^{N_c-1}\left(\frac{\mathbf{z}_\mathbf{s}^{N_c}(N_c - j)}{\alpha\sqrt{N_c}}\right)^2} \\ &= \alpha\sqrt{N_c}\sqrt{\sum_{j=1}^{i}\left(\frac{\mathbf{z}_\mathbf{s}^{N_c}(j)}{\alpha\sqrt{N_c}}\right)^2}, \end{aligned} \tag{32}$$

Since $\mathbf{z}_\mathbf{s}^{N_c} \sim \mathcal{S}(N_c, \alpha\sqrt{N_c})$, by the property of the uniform distribution $\mathcal{S}$ [28], [31], for $i \in [N_c]$, the random variable $\sum_{j=1}^{i}\left(\frac{\mathbf{z}_\mathbf{s}^{N_c}(j)}{\alpha\sqrt{N_c}}\right)^2$ has a beta distribution with parameters $\frac{i}{2}$ and $\frac{N_c-i}{2}$, i.e.,

$$\sum_{j=1}^{i}\left(\frac{\mathbf{z}_\mathbf{s}^{N_c}(j)}{\alpha\sqrt{N_c}}\right)^2 \sim \mathcal{B}\left(\frac{i}{2}, \frac{N_c - i}{2}\right). \tag{33}$$

Furthermore, based on the property of beta distribution [32], we obtain that for $i \in [N_c]$,

$$E\left[\sqrt{\sum_{j=1}^{i}\left(\frac{\mathbf{z}_\mathbf{s}^{N_c}(j)}{\alpha\sqrt{N_c}}\right)^2}\right] = \frac{\mathrm{B}\left(\frac{i+1}{2}, \frac{N_c-i}{2}\right)}{\mathrm{B}\left(\frac{i}{2}, \frac{N_c-i}{2}\right)}. \tag{34}$$

Then, from Eqs. (32) and (34), we have that for $i \in [N_c]$,

$$\begin{aligned} E\left[R_{N_c-i}\right] &= \alpha\sqrt{N_c}E\left[\sqrt{\sum_{j=1}^{i}\left(\frac{\mathbf{z}_\mathbf{s}^{N_c}(j)}{\alpha\sqrt{N_c}}\right)^2}\right] \\ &= \alpha\sqrt{N_c}\frac{\mathrm{B}\left(\frac{i+1}{2}, \frac{N_c-i}{2}\right)}{\mathrm{B}\left(\frac{i}{2}, \frac{N_c-i}{2}\right)}. \end{aligned} \tag{35}$$

Note that in this paper, we set $\mathrm{B}(\cdot, 0) = 1$, which corresponds to $E\left[\sqrt{\sum_{j=1}^{N_c}\left(\frac{\mathbf{z}_\mathbf{s}^{N_c}(j)}{\alpha\sqrt{N_c}}\right)^2}\right] = 1$.

Let $b_i = \frac{\mathbf{z}_\mathbf{x}^{N_c}(j)}{\sigma_\mathbf{x}}$ for $i \in [N_c]$. Since $\mathbf{m}_{N_c}$ is equiprobable in $\{0, 1\}^{N_c}$, the second term of the right side of Eq. (31) can be calculated as follows:

$$\begin{aligned} &E\left[(-1)^{\mathbf{m}_{N_c}(i)}\mathbf{z}_\mathbf{x}^{N_c}(i)\Upsilon_i\left(\frac{(-1)^{\mathbf{m}_{N_c}(i)}\mathbf{z}_\mathbf{x}^{N_c}(i)}{\sigma_\mathbf{x}}\right)\right] \\ &\quad = \frac{\sigma_\mathbf{x}}{2}E\left[b_i\Upsilon_i(b_i) - b_i\Upsilon_i(-b_i)\right], \end{aligned} \tag{36}$$

for every $i \in [N_c]$. As mentioned above, for $i \in [N_c]$, $\mathbf{z}_\mathbf{x}^{N_c}(i) \sim \mathcal{N}\left(0, \sigma_\mathbf{x}^2\right)$, thus $b_i \sim \mathcal{N}(0, 1)$. Then, for $i \in [N_c]$, Eq. (36) can be rewritten as

$$E\left[(-1)^{\mathbf{m}_{N_c}(i)}\mathbf{z}_{\mathbf{x}}^{N_c}(i)\Upsilon_i\left(\frac{(-1)^{\mathbf{m}_{N_c}(i)}\mathbf{z}_{\mathbf{x}}^{N_c}(i)}{\sigma_{\mathbf{x}}}\right)\right]=\sigma_{\mathbf{x}}\mathcal{E}(i), \tag{37}$$

where

$$\mathcal{E}(i)=\frac{1}{2}\int_{-\infty}^{+\infty}[t\Upsilon_i(t)-t\Upsilon_i(-t)]\phi(t)\mathrm{d}t. \tag{38}$$

Note that $\mathcal{E}(i)$ is only determined by i, and $\mathcal{E}(1)=0$.

Combining Eqs. (27), (31), (35) and (37) yields

$$E[\mathbf{w}^T\mathbf{w}]=\alpha^2\ N_c+\sigma_{\mathbf{x}}^2N_c-2\alpha\sigma_{\mathbf{x}}\sqrt{N_c}\sum_{i=1}^{N_c}\mathcal{A}(i), \tag{39}$$

where

$$\mathcal{A}(i)=\mathcal{E}(i)\frac{\mathrm{B}\left(\frac{i+1}{2},\frac{N_c-i}{2}\right)}{\mathrm{B}\left(\frac{i}{2},\frac{N_c-i}{2}\right)}. \tag{40}$$

It is worth pointing out that in Eq. (40), $\mathcal{A}(1)=0$, and $\mathcal{A}(N_c)=\mathcal{E}(N_c)$. Finally, according to Eqs. (12) and (39), the WCR of the TSW embedding can be expressed as follows:

$$\begin{aligned}\mathrm{WCR}_{[\mathrm{dB}]}^{\mathrm{TSW}}&=10\log_{10}\left(\frac{E[\|\mathbf{w}\|_2^2]}{E[\|\mathbf{x}\|_2^2]}\right)\\&=10\log_{10}\left(\frac{\alpha^2\ N_c+\sigma_{\mathbf{x}}^2N_c-2\alpha\sigma_{\mathbf{x}}\sqrt{N_c}\sum_{i=1}^{N_c}\mathcal{A}(i)}{\sigma_{\mathbf{x}}^2N_\upsilon}\right).\end{aligned} \tag{41}$$

From Eq. (41), the WCR of TSW achieves its minimum value at $\alpha=\frac{\sigma_{\mathbf{x}}\sum_{i=1}^{N_c}\mathcal{A}(i)}{\sqrt{N_c}}$. Let $\mathrm{WCR}_{\min}$ denote the minimum value of the WCR. Then, we obtain that

$$\mathrm{WCR}_{\min}=10\log_{10}\left(\frac{N_c-\left(\sum_{i=1}^{N_c}\mathcal{A}(i)\right)^2}{N_\upsilon}\right). \tag{42}$$

According to Eq. (42), $\mathrm{WCR}_{\min}$ is only determined by N_c and N_υ. However, from Eq. (42), it seems not easy to see how $\mathrm{WCR}_{\min}$ evolves as N_c increases. So, the curves of $\mathrm{WCR}_{\min}$ with respect to N_c are plotted in Fig. 1. It is shown from Fig. 1 that the value of $\mathrm{WCR}_{\min}$ increases with the increase of N_c, no matter what N_υ is.

In practice, the target WCR should be set larger than $\mathrm{WCR}_{\min}$. Also from Eq. (41), we see that two different values of α may yield the same value of the WCR. In order to get smaller BER, we need to take the larger value of α for the target WCR (note that BER is monotonically decreasing with α, as shown in Eq. (55)). Therefore, to obtain a target WCR value, the embedding parameter α of TSW is set by

$$\alpha=\frac{\sigma_{\mathbf{x}}}{\sqrt{N_c}}\left(\sqrt{N_\upsilon 10^{\frac{W_T}{10}}-N_c+\left(\sum_{i=1}^{N_c}\mathcal{A}(i)\right)^2}+\sum_{i=1}^{N_c}\mathcal{A}(i)\right), \tag{43}$$

where W_T denotes the target WCR value.

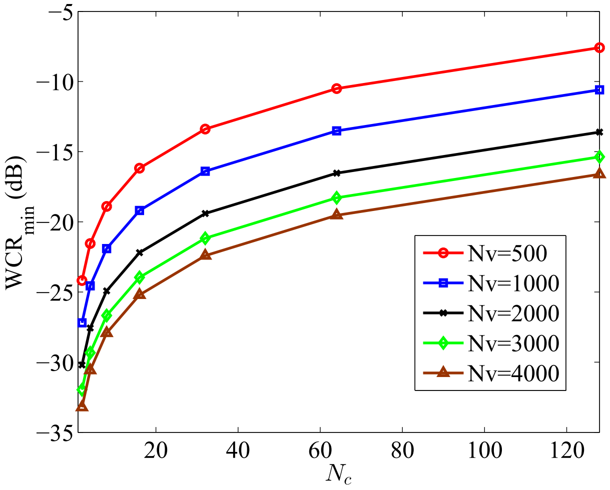


Fig. 1. Curves of $\mathrm{WCR}_{\min}$ with respect to N_c.

B. Robustness

As defined in Eq. (14), the BER of the proposed method is given by

$$P_e=\frac{1}{N_c}\sum_{i=1}^{N_c}\Pr\{\hat{\mathbf{m}}_{N_c}(i)\neq\mathbf{m}_{N_c}(i)\}, \tag{44}$$

where $\hat{\mathbf{m}}_{N_c}(i)=\mathrm{sgn}(\mathbf{z}_{\mathbf{y}}^{N_c}(i))$ for $i\in[N_c]$, and $\mathbf{z}_{\mathbf{y}}^{N_c}=\mathbf{U}_{N_c}^T\mathbf{y}$. Then, we set, for $i\in[N_c]$,

$$P_e(i)=\Pr\{\hat{\mathbf{m}}_{N_c}(i)\neq\mathbf{m}_{N_c}(i)\}. \tag{45}$$

Since $\mathbf{z}_{\mathbf{s}}^{N_c}\sim\mathcal{S}\left(N_c,\alpha\sqrt{N_c}\right)$, then by the law of total probability [25], Eq. (45) is rewritten as

$$P_e(i)=\int_{\mathbf{v}\in\Omega}\Pr\{\hat{\mathbf{m}}_{N_c}(i)\neq\mathbf{m}_{N_c}(i)\big|\mathbf{z}_{\mathbf{s}}^{N_c}=\mathbf{v}\}p_{\mathbf{z}_{\mathbf{s}}^{N_c}}(\mathbf{v})\mathrm{d}\mathbf{v}, \tag{46}$$

where $\Omega=\{\mathbf{v}\big|\|\mathbf{v}\|_2=\alpha^2N_c\}$, and $p_{\mathbf{z}_{\mathbf{s}}^{N_c}}(\cdot)$ denotes the PDF of the distribution $\mathcal{S}\left(N_c,\alpha\sqrt{N_c}\right)$. Considering that the probabilities $\Pr\{\hat{\mathbf{m}}_{N_c}(i)\neq\mathbf{m}_{N_c}(i)\big|\mathbf{z}_{\mathbf{s}}^{N_c}=\mathbf{v}\}$ over Ω are the same for a given value of $\mathbf{z}_{\mathbf{s}}^{N_c}(i)$, we rewrite Eq. (46) as

$$\begin{aligned}P_e(i)=\int_{-\alpha\sqrt{N_c}}^{\alpha\sqrt{N_c}}&\Pr\{\hat{\mathbf{m}}_{N_c}(i)\neq\mathbf{m}_{N_c}(i)\big|\mathbf{z}_{\mathbf{s}}^{N_c}(i)=\upsilon\}\\&\times p_{\mathbf{z}_{\mathbf{s}}^{N_c}(i)}(\upsilon)\mathrm{d}\upsilon,\end{aligned} \tag{47}$$

where $p_{\mathbf{z}_{\mathbf{s}}^{N_c}(i)}(\cdot)$ is the PDF of the distribution $\mathcal{S}_u\left(N_c,\alpha\sqrt{N_c}\right)$ (see Eq. (7)). Noting that $p_{\mathbf{z}_{\mathbf{s}}^{N_c}(i)}(\cdot)$ for $i\in[N_c]$ are the same, in the following we use $\bar{p}_{\mathbf{z}_{\mathbf{s}}^{N_c}}(\cdot)$ to denote $p_{\mathbf{z}_{\mathbf{s}}^{N_c}(i)}(\cdot)$ for brevity. Again by the law of total probability [25], we further have, for $i\in[N_c]$,

$$\begin{aligned}P_e(i)=\int_{-\alpha\sqrt{N_c}}^{\alpha\sqrt{N_c}}&\Big\{\Pr{}^0(i)\Pr(\mathbf{m}_{N_c}(i)=0)\\&+\Pr{}^1(i)\Pr(\mathbf{m}_{N_c}(i)=1)\Big\}\bar{p}_{\mathbf{z}_{\mathbf{s}}^{N_c}}(\upsilon)\mathrm{d}\upsilon,\end{aligned} \tag{48}$$

where

$$\begin{aligned}\mathrm{Pr}^0(i) &= \mathrm{Pr}\left(\mathbf{z}_{\mathbf{y}}^{N_c}(i) < 0 \middle| \mathbf{m}_{N_c}(i) = 0, \mathbf{z}_{\mathbf{s}}^{N_c}(i) = \upsilon\right)\\ \mathrm{Pr}^1(i) &= \mathrm{Pr}\left(\mathbf{z}_{\mathbf{y}}^{N_c}(i) > 0 \middle| \mathbf{m}_{N_c}(i) = 1, \mathbf{z}_{\mathbf{s}}^{N_c}(i) = \upsilon\right). \quad (49)\end{aligned}$$

Since $\mathbf{m}_{N_c}(i)$ is equiprobable in $\{0, 1\}$ for $i \in [N_c]$, Eq. (48) can be simplified as follows:

$$P_e(i) = \frac{1}{2}\int_{-\alpha\sqrt{N_c}}^{\alpha\sqrt{N_c}} \left\{\mathrm{Pr}^0(i) + \mathrm{Pr}^1(i)\right\} \bar{p}_{\mathbf{z}_{\mathbf{s}}^{N_c}}(\upsilon)\mathrm{d}\upsilon. \quad (50)$$

According to Eq. (10), we get that for $i \in [N_c]$,

$$\mathbf{z}_{\mathbf{y}}^{N_c}(i) = \mathbf{z}_{\mathbf{s}}^{N_c}(i) + \mathbf{z}_{\mathbf{n}}^{N_c}(i), \quad (51)$$

where $\mathbf{n} \sim \mathcal{N}(\mathbf{0}, \sigma_{\mathbf{n}}^2\mathbf{I}_{N_\upsilon})$. By Eqs. (49) and (51), $\mathrm{Pr}^0(i)$ is derived as follows:

$$\begin{aligned}\mathrm{Pr}^0(i) &= \mathrm{Pr}\left(\mathbf{z}_{\mathbf{n}}^{N_c}(i) < -\mathbf{z}_{\mathbf{s}}^{N_c}(i) \middle| \mathbf{m}_{N_c}(i) = 0, \mathbf{z}_{\mathbf{s}}^{N_c}(i) = \upsilon\right)\\ &= \mathrm{Pr}\left(\mathbf{z}_{\mathbf{n}}^{N_c}(i) < -\upsilon \middle| \mathbf{m}_{N_c}(i) = 0, \mathbf{z}_{\mathbf{s}}^{N_c}(i) = \upsilon\right). \quad (52)\end{aligned}$$

Since $\mathbf{n} \sim \mathcal{N}(\mathbf{0}, \sigma_{\mathbf{n}}^2\mathbf{I}_{N_\upsilon})$ and $\|\mathbf{u}_i\|_2^2 = 1$, then $\mathbf{z}_{\mathbf{n}}^{N_c}(i) \sim \mathcal{N}(0, \sigma_{\mathbf{n}}^2)$. Because $\mathbf{z}_{\mathbf{n}}^{N_c}(i) \sim \mathcal{N}(0, \sigma_{\mathbf{n}}^2)$, and $\mathbf{z}_{\mathbf{n}}^{N_c}(i)$ is independent to $\mathbf{z}_{\mathbf{s}}^{N_c}(i)$ and $\mathbf{m}_{N_c}(i)$ for $i \in [N_c]$, $\mathrm{Pr}^0(i)$ is calculated from Eq. (52) as

$$\begin{aligned}\mathrm{Pr}^0(i) &= \mathrm{Pr}\left(\mathbf{z}_{\mathbf{n}}^{N_c}(i) < -\upsilon\right)\\ &= \Phi\left(-\frac{\upsilon}{\sigma_{\mathbf{n}}}\right). \quad (53)\end{aligned}$$

In the same way, we also obtain that for $i \in [N_c]$,

$$\mathrm{Pr}^1(i) = \Phi\left(-\frac{\upsilon}{\sigma_{\mathbf{n}}}\right). \quad (54)$$

Finally, combining Eqs. (44), (50), (53), (54), and (7) yields

$$P_e = \frac{2}{\mathrm{B}\left(\frac{N_c-1}{2}, \frac{1}{2}\right)}\int_0^1 \Phi\left(-\frac{\alpha\sqrt{N_c}}{\sigma_{\mathbf{n}}}\upsilon\right)\left(1 - \upsilon^2\right)^{\frac{N_c-3}{2}} \mathrm{d}\upsilon. \quad (55)$$

From Eq. (55), we see that, given the watermark message length N_c, the BER P_e of the proposed method is only determined by the embedding strength parameter α and the noise power $\sigma_{\mathbf{n}}$.

V. Experimental Results

A number of experiments have been carried out to evaluate the performance of the proposed method (i.e., TSW). These experiments consist of the following two parts.

A. Experiments on Simulated Signals

In the first part of the experiments, the host signals for testing are simulated Gaussian signals, and the experimental results are averaged over 10,000 i.i.d. Gaussian host signals.

First, we demonstrate the reduction process of the embedding distortion of the proposed method. To show the reduction, we compare TSW to the spherical watermarking scheme without using transportation theory (abbreviated as SW-WoT). Given a host signal $\mathbf{x}$, a watermark message $\mathbf{m}_{N_c}$, and the secret carriers $\mathbf{u}_1, \ldots, \mathbf{u}_{N_c}$, the embedding of SW-WoT was implemented as follows:

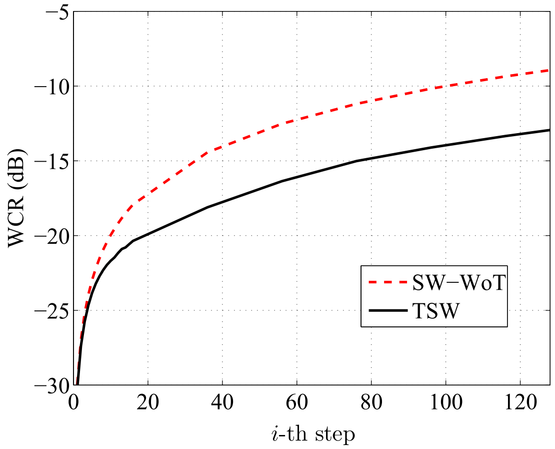


Fig. 2. Timing comparison of WCRs between TSW and SW-WoT. Note that SW-WoT denotes the spherical watermarking scheme without using transportation theory. Here, $\sigma_{\mathbf{x}}^2 = 1$, $\alpha = 1$, and $N_\upsilon = 2,000$.

$$\mathbf{s} = \mathbf{x} + \sum_{i=1}^{N_c}\left[\alpha\sqrt{N_c}\frac{(-1)^{\mathbf{m}_{N_c}(i)}\mathrm{sgn}(\mathbf{z}_{\mathbf{x}}^{N_c}(i))}{\| \mathbf{z}_{\mathbf{x}}^{N_c} \|_2} - 1\right]\mathbf{z}_{\mathbf{x}}^{N_c}(i)\mathbf{u}_i. \quad (56)$$

where $\mathbf{s}$ and $\mathbf{z}_{\mathbf{x}}^{N_c}$ denote the watermarked signal and the host correlation, respectively. In the experiment, we set $N_c = 128$. For TSW, a reduction of embedding distortion is achieved in the embedding of each message bit, and the message bits are embedded into the host signal one by one. Therefore, in the experiment there are total 128 steps in the reduction of the embedding distortion. A timing comparison of WCRs between TSW and SW-WoT is shown in Fig. 2. It is clearly shown that the difference of embedding distortion between TSW and SW-WoT becomes larger and larger as the number of the reduction steps increases. This means that each step in the TSW embedding process contributes to the reduction of the embedding distortion.

In order to demonstrate the advantages of the proposed method, in the following we conducted experiments to compare it with existing methods. Fig. 3 shows the WCR comparison among CW-ISS [7], HCW-ISS [18], and TSW. Note that these three methods are all key-secure, i.e., have the same security level. For a fair comparison, the embedding strength parameters of the three watermarking methods were turned to make their BERs the same at the same SNR level. Here, the BERs and SNRs are set to 0.05 and 16 dB, respectively. From Fig. 3, we see that TSW can achieve the lowest WCR in all cases. Especially, the larger the bit length N_c of the hidden message, the greater the WCR reduction achieved by TSW. We also see that HCW-ISS has the nearly same good results as TSW when N_c takes a small value, such as $N_c = 2$; whereas it performs bad sharply when N_c takes a large value, such as $N_c \geq 16$. This indicates that, as stated in [21], HCW-ISS has poor performance for long watermark messages. Note that the theoretical WCR curve of TSW is also ploted in Fig. 3. It is seen that the theoretical and simulated WCR curves of TSW follow each other closely, which confirms the theoretical analysis presented in Section IV-A.

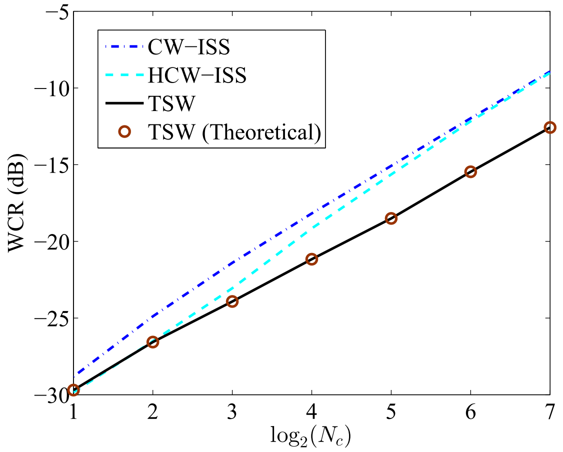


Fig. 3. Comparison of WCRs among CW-ISS [7], HCW-ISS [18], and TSW. Here, $\sigma_{\mathbf{x}}^2 = 1$ and $N_v = 2,000$. Besides, we set $N_m = 3,000$ for HCW-ISS.

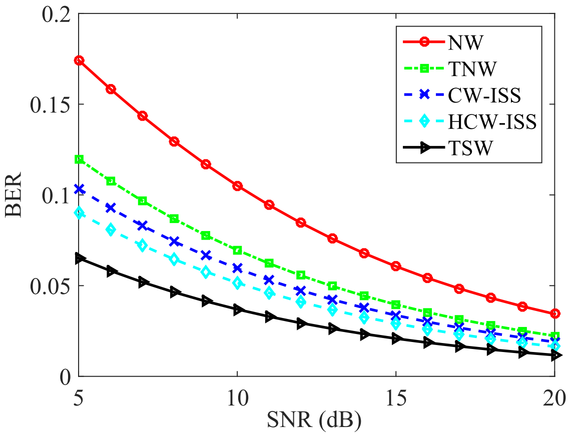


Fig. 4. Comparison of BERs among NW [7], TNW [21], CW-ISS [7], HCW-ISS [18], and TSW. Here, $\sigma_{\mathbf{x}}^2 = 1$, $N_c = 16$. We set $N_v = 2,000$ for TNW, CW-ISS, HCW-ISS, and TSW, and $N_v = 4,766$ for NW. Besides, we set $N_m = 3,000$ for HCW-ISS.

Finally, the comparison of BER values among NW [7], TNW [21], CW-ISS [7], HCW-ISS [18], and TSW are shown in Fig. 4. For a fair comparison, the embedding strength parameters of these watermarking methods and the length of the host signals are adjusted to keep their WCRs at the same value. In this experiment, the WCR is set to -21.73 dB. It is shown in Fig. 4 the BER of the proposed method is significantly lower than those of the other four methods. This means that the proposed method performs the best in terms of robustness.

B. Experiments on Real Images

In the second part of our experiments, the host signals for testing are extracted from real images. The test images consist of 2,000 images, which were randomly chosen from BOWS2-IMAGES database [33], and include landscape images, plant images, animal images, building images, and so on. All of the test images are gray-scale images with pixel values in the range [0, 255] and with size 512×512. To extract the host signals from real images, the 5-level 9/7 Daubechies DWT [34] was performed on each full image, then the DWT coefficients of low- and mid-frequencies (except for the first low-frequency) were selected for message embedding.

Before embedding, the projection operation introduced in [21] was performed on the DWT coefficients to make them asymptotically i.i.d. Gaussian distributed. Let $\tilde{\mathbf{x}}$ denote the N_t-dimensional DWT coefficients, and let $\mathbf{a}_i$, for $i \in [N_v]$, denote the pseudo random vectors generated according to the following distribution: $\mathbf{a}_i(j)$, for $i \in [N_v]$ and $j \in [N_t]$, are independent and $\mathbf{a}_i(j) \sim \mathcal{U}(-\sqrt{3/N_c}, \sqrt{3/N_c})$, where $\mathcal{U}(a, b)$ denotes the uniform distribution on $[a, b]$. Then, the projection in [20] is defined as

$$\mathbf{x}(i) = \tilde{\mathbf{x}}^T \mathbf{a}_i, \quad \text{for } \forall i \in [N_v], \tag{57}$$

where $\mathbf{x}$ denotes the host signal to be embedded. By Eq. (57), two conclusions can be drawn. First, $\mathbf{x}(i)$, for $i \in [N_v]$, is asymptotically Gaussian distributed with zero mean due to the center limit theory (CLT) (note that N_t, which was set to be not smaller than 768 in our experiments, can be regarded as a large enough number). Second, the components of the host signal $\mathbf{x}$ are orthogonal to each other (this can be proved as follows. For $\forall i, j \in [N_v]$ and $i \neq j$, by Eq. (57), we have $\mathbf{x}(i) = \tilde{\mathbf{x}}^T \mathbf{a}_i$ and $\mathbf{x}(j) = \tilde{\mathbf{x}}^T \mathbf{a}_j$. Since $\mathbf{a}_i$, $\mathbf{a}_j$ and $\tilde{\mathbf{x}}$ are independent to each other and $E[\mathbf{a}_i] = E[\mathbf{a}_j] = \mathbf{0}$, we have $E[\mathbf{x}(i)\mathbf{x}(j)] = E[\tilde{\mathbf{x}}^T \mathbf{a}_i \tilde{\mathbf{x}}^T \mathbf{a}_j] = E[\mathbf{a}_i^T] E[\tilde{\mathbf{x}}\tilde{\mathbf{x}}^T] E[\mathbf{a}_j] = 0$). Based on the above two conclusions, we obtain that the components of $\mathbf{x}$ are i.i.d. Gaussian variables, which is because that zero-mean Gaussian-distributed signals are independent if they are orthogonal [25].

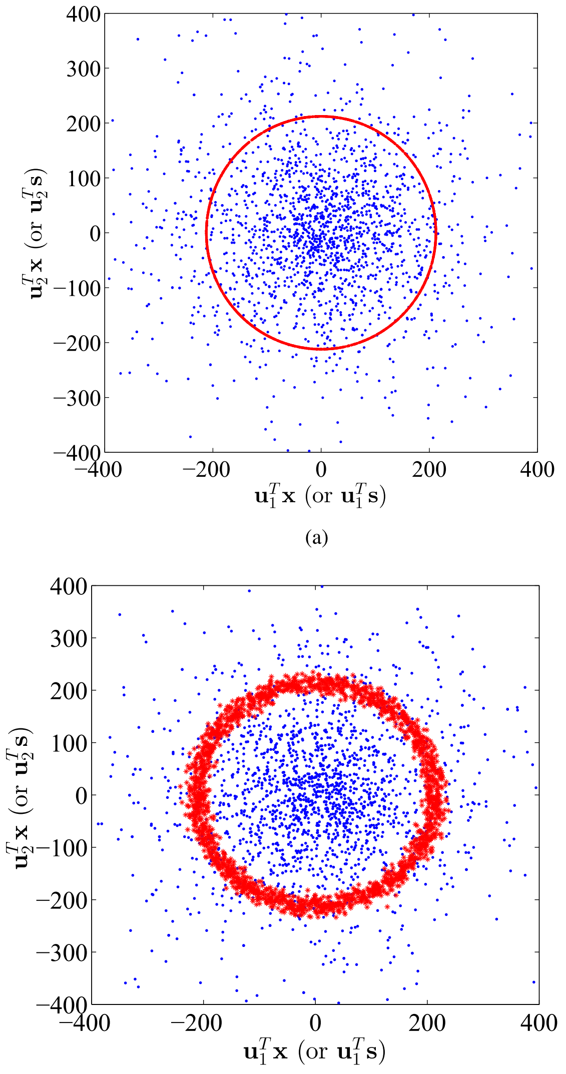
The psycho-visual masking proposed in [35] was also applied in the practical implementation to improve the imperceptibility of the watermarked images. Let $\mathbf{I}(i, j)$, $\mathbf{I}^w(i, j)$, and $\mathbf{I}^m(i, j)$ denote the pixels of the original image, the watermarked image without the masking, and the watermarked image with the masking, respectively, where (i, j) denotes the pixel coordinate. Then, the TSW embedding with the masking of [35] can be expressed by

$$\mathbf{I}^m(i, j) = \mathbf{I}(i, j) + \beta(i, j)[\mathbf{I}^w(i, j) - \mathbf{I}(i, j)]. \tag{58}$$

where $\beta(i, j) = \sigma(i, j)/\sigma_{max}$, $\sigma_{max} = \max_{i,j}\{\sigma(i, j)\}$, and $\sigma(i, j)$ is calculated as the variance of the pixel $\mathbf{I}(i, j)$ and its eight nearest neighbors. Unlike other maskings (including the pixel-wise maskings of [36] and [37]), the psycho-visual masking used in this paper was performed after, not during, the embedding of watermark, that is, it can be regarded as a post-processing of watermark embedding. Since different images have different masking properties, we used different spatial maskings for different images. However, for a fair comparison, all of the compared methods adopted the same masking for the same image. Here, two points should be noted. First, as discussed in Section III-B, if the host signal is not i.i.d. Gaussian, then the key-security of the proposed method is no longer guaranteed. In our experiments on real images, the i.i.d. Gaussian host signal was achieved by using the projection operation of [21]. The psycho-visual masking is a post-processing of the watermark embedding. Therefore, it has no effect on the distribution of the host signal. Namely, the i.i.d. Gaussian distribution can be preserved for the host signal after the application of the psycho-visual masking. Although the pixel-wise maskings of [36] and [37] should be more effective in improving the BER performance than the psycho-visual masking, the application of the pixel-wise maskings will distort the distribution of the host signal, and so may degrade the security of the proposed method. Therefore, from the aspect of security, this kind of maskings is not appropriate to be applied to the proposed method. Second, for the proposed method, the link between the targeted WCR and the embedding parameter α is given by Eq. (43). Without the application of the psycho-visual masking, the link between the targeted PSNR and the WCR of the proposed method can be described by [30, eq. 23] . In the implementation of the proposed method on images, the psycho-visual masking was performed after the inverse DWT. That is, the psycho-visual masking was performed, not in the embedding domain, but in the pixel domain. This makes the link between the targeted PSNR and the WCR more complicated and really difficult to formulate. Therefore, in our experiments, the target PSNRs of the watermarked images of the proposed method (with the psycho-visual masking) were set by tuning the parameter α.

In order to evaluate the robustness of the test methods, various attacks were performed on the watermarked images, which include amplitude scaling, AWGN, salt & pepper noising, Gaussian filtering, median filtering, and JPEG compression. The details of these attacks are as follows: (1) in the amplitude scaling attack, the pixel values of each watermarked image were scaled by 0.75, 1.25, and 1.5, separately; (2) in the AWGN attack, each watermarked image was corrupted by the AWGNs with standard deviations 10, 20, and 30, separately (note that the pixel values of the corrupted images were still restricted to the range $[0, 255]$); (3) in the salt & pepper noising attack, each watermarked image was degraded by adding salt & pepper noise with probabilities 0.01, 0.02, and 0.03, separately; (4) in the Gaussian filtering attack, each watermarked image was smoothed by the Gaussian filters with standard deviation 0.5 and sizes 3×3, 5×5, and 7×7, separately; (5) in the median filtering attack, each watermarked image was smoothed by the median filters with sizes 3×3, 5×5, and 7×7, separately; (6) in the JPEG compression attack, each watermarked image was JPEG compressed with quality factors 50, 40, and 30, separately.

Five experiments were conducted in this part. First, we evaluated the security of the proposed method by investigating: (1) the distribution of its watermarked correlation and (2) its resistance to blind signal separation attack [2], [5]. We show in Fig. 5 the distributions of the host and watermarked correlations of the TSW embedding for a two-dimensional case (i.e., $N_c = 2$). Since the psycho-visual masking is a post-processing of the TSW embedding, it can distort the distribution of the watermarked correlation of the TSW embedding. In order to show the undistorted distribution of the watermarked correlation, the watermarked correlation shown in Fig. 5 (a) was obtained by disabling the psycho-visual masking. It is seen from Fig. 5 (a) that the watermarked correlation is modulated from the i.i.d. Gaussian distribution of the host correlation to a uniform distribution on a circle, which verifies that TSW belongs to the family of SW. Thus, as discussed in Section III-A, TSW should be key-secure. Fig. 5 (b) shows the distribution of the watermarked correlation with the random distortion caused by the psycho-visual masking. We can see that the distorted distribution is still circular, which means that the key security of the TSW embedding is preserved after the psycho-visual masking. In the same two-dimensional case, we also tried to estimate the two secret carriers for 500 different trials by using the ICA-based carrier estimation method introduced in [5]. Figs. 6 (a) and (b) show the normalized correlations between the two estimated secret carriers and the real ones for the TSW embeddings without and with the psycho-visual masking, respectively. It is shown that the points (i.e., the pairs of the normalized correlation values) in Fig. 6 are randomly, uniformly distributed on a unitary circle, and those in Fig. 6 (b) are also distorted, but still circularly distributed. As analyzed



(a)

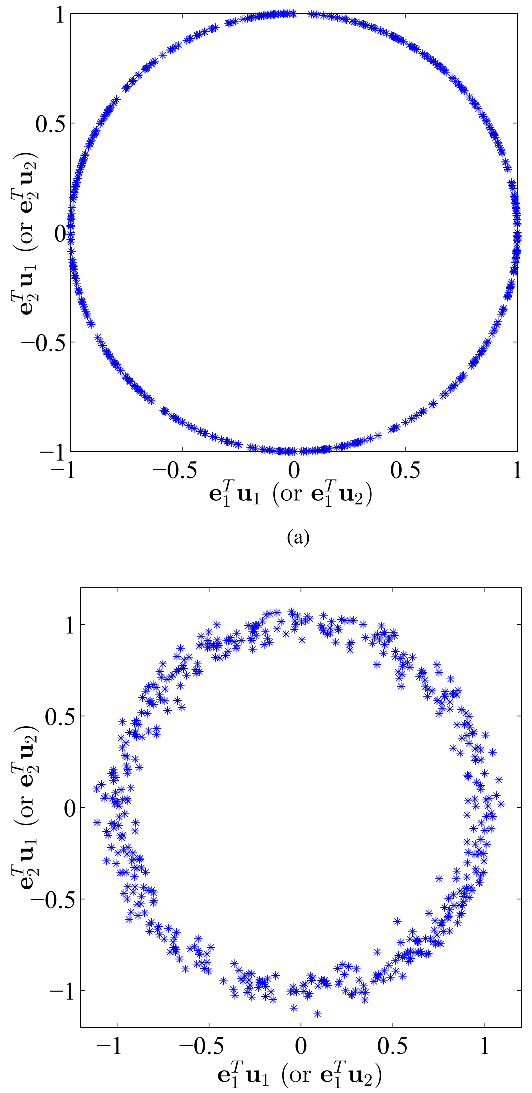
(b)

Fig. 5. Distributions of the host and watermarked correlations of TSW. The host correlation pairs $(\mathbf{u}_1^T\mathbf{x}, \mathbf{u}_2^T\mathbf{x})$ and the watermarked correlation pairs $(\mathbf{u}_1^T\mathbf{s}, \mathbf{u}_2^T\mathbf{s})$ are represented by the blue and red dots, respectively. Here $\alpha = 150$, $N_c = 2$, $N_v = 2,048$, and the average PSNR is 56 dB. (a) Without the masking. (b) With the masking.

TABLE I

TEN KINDS OF COMBINATIONS OF DWT SUBBANDS

No.	Combination	Number of coefficients
1	HL5, LH5, HH5	768
2	HL5, LH5, HH5, HL4, LH4, HH4	3,840
3	HL5, LH5, HH5, HL4, LH4, HH4, HL3, LH3, HH3	16,128
4	HL5, LH5, HH5, HL4, LH4, HH4, HL3, LH3, HH3, HL2, LH2, HH2	65,280
5	HL4, LH4, HH4	3,072
6	HL4, LH4, HH4, HL3, LH3, HH3	14,336
7	HL4, LH4, HH4, HL3, LH3, HH3, HL2, LH2, HH2	64,512
8	HL3, LH3, HH3	12,288
9	HL3, LH3, HH3, HL2, LH2, HH2	61,440
10	HL2, LH2, HH2	49,152



(a)

(b)

Fig. 6. Normalized correlations between the two estimated secret carriers and the original ones. The blue points represent the correlation pairs $(\mathbf{e}_1^T\mathbf{u}_1, \mathbf{e}_2^T\mathbf{u}_1)$ and $(\mathbf{e}_1^T\mathbf{u}_2, \mathbf{e}_2^T\mathbf{u}_2)$, where $\mathbf{e}_1$ and $\mathbf{e}_2$ denote the estimates of $\mathbf{u}_1$ and $\mathbf{u}_2$, respectively. (a) Without the masking. (b) With the masking.

in [7], this phenomenon indicates that the subspace of the secret carriers can be estimated by using the ICA-based estimation method, but it is impossible to exactly estimate the secret carriers. That is to say, TSW is key-secure, but not subspace-secure.

Second, an experiment was carried out to show how the performance of the proposed method varies when the range and number of the DWT coefficients are changed. After applying the 5-level 9/7 Daubechies DWT to a host image, we can obtain 16 DWT subbands, which include, from low to high frequencies, LL5, HL5, LH5, ..., HL1, LH1, and HH1. We investigated ten kinds of combinations of these subbands (except for the lowest frequency subband LL5 and the highest frequency subbands HL1, LH1, and HH1), which are listed in Table I. For each combination, only the subbands included in the combination were used for message embedding. In this experiment, $N_c = 16$, $N_v = 2,048$, and the average PSNR of the watermarked images was set to about 40 dB. It is seen from Tables II and III that Combinations 1, 3, and 8 do not perform well under most of the attacks; Combination 6 does not perform well under amplitude scaling and Salt & Pepper noise addition; Combination 8 does not perform well under AWGN noise addition, Salt & Pepper noise addition, and JPEG compression; Combinations 4, 7, 9, and 10 perform very badly under median filtering; although Combination 2 does not achieve the best result under each of the attacks, it performs quite well overall. Therefore, Combination 2 was adopted in our other experiments.

Third, we also performed an experiment to see how the BER performance of the proposed method varies with the change of the embedding bit-rate. In the experiment, the PSNRs of the watermarked images are fixed to about 36 dB, that is, the qualities of the watermarked images are set to almost the same level. The experimental results are listed in the Tables IV and V. It is seen from Tables IV and V that the BER performance of the proposed method decreases as the embedding bit-rate (measured by N_c) increases. This consists with the fact that there is a trade-off between the robustness and payload in watermarking schemes. It is worthy mentioning that, as discussed in Section IV-A, there is a lowest WCR for the TSW embedding, so the PSNR of a watermarked image of TSW is constrained to be smaller than a certain value. In the case of $N_c = 128$, most of the PSNRs of the watermarked images cannot reach to 37 dB. Therefore, in this experiment, the target PSNR is set to 36 dB for all the cases.

TABLE II

BER Performance of the Proposed Method Under Various DWT Subband Combinations. The BER (%) Results Were Averaged Over the 2,000 Test Images. Here, $N_v = 2,048$, $N_c = 16$, and the PSNRs of the Watermarked Images are About 40 dB

Combination No.	Amplitude Scaling			AWGN (σ)			Salt & Pepper (p)		
	0.75	1.25	1.5	10	20	30	0.01	0.02	0.03
1	1.94	3.57	5.23	5.13	7.66	10.72	6.38	10.25	16.35
2	0.00	1.13	2.41	1.31	2.54	3.29	0.47	1.59	2.86
3	1.37	2.85	4.39	1.19	2.41	3.17	1.86	3.21	4.72
4	0.81	1.46	2.73	0.05	0.92	1.63	0.84	1.76	2.95
5	0.96	1.75	3.47	1.88	3.11	4.38	1.37	2.18	3.36
6	0.63	1.32	2.98	0.00	0.84	1.27	1.54	2.29	3.87
7	0.00	0.97	1.91	0.03	0.95	1.65	0.38	1.46	2.63
8	0.04	1.02	1.94	1.64	2.79	3.76	1.40	2.25	3.80
9	0.00	0.78	1.56	0.00	0.02	0.83	0.01	0.83	1.49
10	0.00	0.56	1.37	0.00	0.00	0.81	0.00	0.52	1.23

TABLE III

BER Performance of the Proposed Method Under Various DWT Subband Combinations. The BER (%) Results Were Averaged Over the 2,000 Test Images. Here, $N_v = 2,048$, $N_c = 16$, and the PSNRs of the Watermarked Images are About 40 dB

Combination No.	Gaussian Filter			Median Filter			JPEG (QF)		
	3×3	5×5	7×7	3×3	5×5	7×7	50	40	30
1	3.75	5.66	8.64	4.15	5.83	7.86	0.95	2.16	3.46
2	0.04	1.17	2.48	1.88	2.70	3.52	0.00	0.07	1.15
3	0.59	1.34	2.97	2.24	3.50	4.65	0.70	1.28	2.17
4	0.06	0.77	1.82	5.89	7.48	9.27	0.71	1.62	2.44
5	1.16	2.08	3.17	0.05	0.77	1.26	0.70	1.21	2.20
6	0.00	0.55	1.63	0.00	0.59	1.13	0.00	0.08	1.02
7	0.00	0.07	0.59	4.82	5.67	7.49	0.42	1.04	1.83
8	0.00	0.41	1.14	0.00	0.09	0.87	0.67	1.16	1.98
9	0.00	0.00	0.42	4.86	6.75	8.24	0.32	1.04	1.76
10	0.00	0.18	0.83	8.90	11.72	13.58	0.08	0.90	1.63

TABLE IV

BER Performance of the Proposed Method Under Various Bit-Rates. The BER (%) Results Were Averaged Over the 2,000 Test Images

Bit-rate (N_c)	Amplitude Scaling			AWGN (σ)			Salt & Pepper (p)		
	0.75	1.25	1.5	10	20	30	0.01	0.02	0.03
8	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
16	0.00	0.00	0.00	0.00	0.06	0.25	0.00	0.11	0.47
32	0.00	0.00	0.71	0.05	0.28	1.02	0.14	0.53	1.68
64	0.00	0.87	2.56	0.30	0.93	3.77	0.60	2.06	3.97
128	0.00	2.54	7.63	1.58	3.26	10.58	2.74	7.19	11.03

Fourth, the proposed method was compared, in terms of robustness, with four existing secure SS watermarking methods, including NW [7], TNW [21], CW-ISS [7], and HCW-ISS [18]. For a fair comparison, we set $N_c = 16$, $N_v = 2,048$, and fixed the PSNRs averaged over 2,000 watermarked images to about 40 dB for all the compared methods. Note that CW-ISS, HCW-ISS, and TSW have an embedding strength parameter to tune their PSNRs. However, both NW and TNW do not have such a parameter, and their PSNRs are determined by which DWT subbands are used. For CW-ISS, HCW-ISS, and TSW, the subbands HL5, LH5, HH5, HL4, LH4, and HH4 ($N_t = 3,840$) were used for message embedding, then the means of their PSNRs were tuned to be 40.10 dB, 39.74 dB, and 39.83 dB, respectively, and the variances of their PSNRs are 0.73 dB, 0.22 dB, and 0.24 dB, respectively; for TNW, the subbands used for embedding are the same as those of CW-ISS, HCW-ISS, and TSW, the mean and variance of its PSNR are 40.26 dB and

TABLE V

BER Performance of the Proposed Method Under Various Bit-Rates. The BER (%) Results Were Averaged Over the 2,000 Test Images

Bit-rate (N_c)	Gaussian Filter			Median Filter			JPEG (QF)		
	3×3	5×5	7×7	3×3	5×5	7×7	50	40	30
8	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.00
16	0.00	0.00	0.07	0.00	0.15	0.58	0.00	0.00	0.00
32	0.00	0.04	0.42	0.06	0.65	1.97	0.00	0.00	0.17
64	0.11	0.25	1.87	0.30	1.52	3.31	0.00	0.19	0.54
128	0.46	1.57	7.64	1.84	5.32	9.59	0.83	1.45	2.58

TABLE VI

Comparison of BERs (%) Among NW [7], TNW [21], CW-ISS [7], HCW-ISS [18], and TSW. The BER Results Were Averaged Over the 2,000 Test Images, and the Best Results are in Bold

Method	Amplitude Scaling			AWGN (σ)			Salt & Pepper (p)		
	0.75	1.25	1.5	10	20	30	0.01	0.02	0.03
NW [7]	4.16	4.87	5.93	5.42	6.76	8.83	5.38	6.61	7.47
TNW [21]	2.04	2.92	3.45	3.17	4.35	5.90	2.51	3.12	4.14
CW-ISS [7]	1.68	2.35	3.44	3.10	4.29	5.81	2.43	3.04	4.00
HCW-ISS [18]	**0.00**	1.54	2.76	1.83	2.91	4.18	0.76	1.93	3.07
TSW	**0.00**	**1.13**	**2.41**	**1.32**	**2.54**	**3.29**	**0.47**	**1.59**	**2.86**

TABLE VII

Comparison of BERs (%) Among NW [7], TNW [21], CW-ISS [7], HCW-ISS [18], and TSW. The BER Results Were Averaged Over the 2,000 Test Images, and the Best Results are in Bold

Method	Gaussian Filter			Median Filter			JPEG (QF)		
	3×3	5×5	7×7	3×3	5×5	7×7	50	40	30
NW [7]	5.77	6.59	7.32	8.59	9.11	9.65	2.31	4.78	6.43
TNW [21]	3.18	4.05	4.61	4.85	5.32	5.78	0.05	2.11	3.62
CW-ISS [7]	2.83	3.78	4.22	4.63	4.96	5.45	0.04	1.96	3.17
HCW-ISS [18]	0.72	2.08	2.99	2.84	3.27	4.00	**0.00**	0.53	2.04
TSW	**0.04**	**1.17**	**2.48**	**1.88**	**2.70**	**3.52**	**0.00**	**0.07**	**1.15**

1.07dB, respectively; while for NW, to obtain about the same PSNR, a different set of DWT subbands, including HL4, LH4, and HH4 ($N_t = 3,072$), were chosen, and the mean and variance of its PSNR are 39.81 dB and 0.45 dB, respectively. Besides, the special parameter of HCW-ISS, denoted as N_m in [18], was set to $3,000$, and the N_m-map was calculated with the host and watermarked correlations from $3,000$ real images, which were randomly selected from the remainder $8,000$ BOWS2 images (i.e., excluding the $2,000$ test images). The BER values of the five compared methods are given in Tables VI and VII. In this experiment, each of the BER values was averaged over the 2,000 images. As expected, we see that there is an increase in the performance of all the five methods with the decrease of the intensity of these attacks. We also see from Tables VI and VII that the proposed method achieves the best robustness among the five secure watermarking methods. Moreover, note that all the five watermarking methods make a linear change of the host images. So, the bits decoded from the original and the scaled watermarked images should be the same, and then the decoding error should be zero. But, it is shown in Table VI that the BERs under amplitude scaling are not zero in some cases, and the BERs under up-scaling are larger than that under down-scaling. This is due to the following two reasons. First, as mentioned above, the psycho-visual masking used in this paper is performed after message embedding. Thus, it can also be considered as an attack for watermark decoding, and may causes some decoding errors. Second, the pixel truncation happens when the scaling factor is larger than 1. This results in more decoding errors in the case of up-scaling.

Finally, the application of channel coding, which has not been considered in the related works [7], [18], [21], was investigated for the proposed method. For a communication system, the BER can be reduced by utilizing channel coding. This is because channel coding has the ability of error correction by adding redundant bits. However, for an image watermarking system, there is an inherent trade-off between the bit-rate and the embedding distortion. That is,

TABLE VIII

COMPARISON OF BERS (%) AMONG TSW, THE TSW WITH THE BCH CODE (TSW-BCH), AND THE TSW WITH THE CONVOLUTION CODE (TSW-CONV). THE BER RESULTS WERE AVERAGED OVER THE 2,000 TEST IMAGES. HERE, $N_c = 16$, AND THE PSNRS OF THE WATERMARKED IMAGES ARE ABOUT 40 dB

Method	Amplitude Scaling			AWGN (σ)			Salt & Pepper (p)		
	0.75	1.25	1.5	10	20	30	0.01	0.02	0.03
TSW	0.00	1.13	2.41	1.32	2.54	3.29	0.47	1.59	2.86
TSW-BCH	0.00	1.10	2.35	1.31	2.42	3.26	0.39	1.51	2.77
TSW-Conv	0.00	1.07	2.11	1.25	2.28	3.09	0.24	1.25	2.43

TABLE IX

COMPARISON OF BERS (%) AMONG TSW, THE TSW WITH THE BCH CODE (TSW-BCH), AND THE TSW WITH THE CONVOLUTION CODE (TSW-CONV). THE BER RESULTS WERE AVERAGED OVER THE 2,000 TEST IMAGES. HERE, $N_c = 16$, AND THE PSNRS OF THE WATERMARKED IMAGES ARE ABOUT 40 dB

Method	Gaussian Filter			Median Filter			JPEG (QF)		
	3×3	5×5	7×7	3×3	5×5	7×7	50	40	30
TSW	0.04	1.17	2.48	1.88	2.70	3.52	0.00	0.07	1.15
TSW-BCH	0.04	1.06	2.37	1.54	2.31	3.18	0.00	0.05	1.00
TSW-Conv	0.02	1.04	2.12	1.36	2.25	3.00	0.00	0.00	0.67

the embedding distortion will increase with the increase of the bit-rate. Therefore, if channel coding is applied to image watermarking, some decoding errors may be corrected, whereas there is a need for more bit-rate to code the redundant bits, which then leads to the increase of embedding distortion. To evaluate the practical performance of the application of channel coding, we conducted an experiment on the $2,000$ test images. In the experiment, two classical channel codes, namely the BCH code and the convolution code [38], have been implemented for comparison. The experimental results are given in Tables VIII and IX. It is shown that both the applications of these two channel codes can slightly, but not significantly, improve the performance of the proposed method.

VI. CONCLUSION

In this paper, we have proposed a novel secure spread spectrum (SS) watermarking method called transportation spherical watermarking (TSW), of which the watermarked correlation follows a uniform distribution on a spherical surface, and the embedding distortion is recursively minimized with the transportation theory. A theoretical analysis of embedding distortion and robustness has also been presented for the proposed method. According to the distribution of its watermarked correlation and our practical analysis on its security, TSW is key-secure, but not subspace-secure, in the framework of watermarked-only attack. That is to say, the secret key of TSW cannot be estimated accurately but there remains a possibility for removal attack since a basis of the private subspace can be estimated. Compared with existing secure SS watermarking methods, TSW achieves less embedding distortion and better robustness.

In future works, we would like to address some issues in the application of TSW to images. First, the application of TSW could be extended to color images. For color images, we can embed the watermark in their luminance component by TSW. Certainly, this is a straightforward extension of TSW from gray to color images, and hence may not be a good means of handling colors images. More sophisticated extension would be explored by utilizing the other two components. Second, advanced perceptual models would be considered in developing more effective masking technique. It is worth noting that the masking technique to be developed should not only improve the quality of watermarked images, but also preserve the security of TSW. Third, much effort would be devoted to the choice of an appropriate channel code for TSW to find a good trade-off between the decrease of decoding errors and the increase of embedding distortion.

REFERENCES

[1] M. Barni, F. Bartolini, and T. Furon, "A general framework for robust watermarking security," *Signal Process.*, vol. 83, no. 10, pp. 2069–2084, 2003.

[2] F. Cayre, C. Fontaine, and T. Furon, "Watermarking security: Theory and practice," *IEEE Trans. Signal Process.*, vol. 53, no. 10, pp. 3976–3987, Oct. 2005.

[3] L. Pérez-Freire, P. Comesaña, and F. Pérez-González, "Information-theoretic analysis of security in side-informed data hiding," in *Proc. Int. Workshop Inf. Hiding*, Barcelona, Spain, Jun. 2005, pp. 131–145.

[4] T. Furon, "A survey of watermarking security," in *Proc. Int. Workshop Digit. Watermarking*, vol. 3710. Siena, Italy, Sep. 2005, pp. 201–215.

[5] P. Bas and F. Cayre, "Achieving subspace or key security for WOA using natural or circular watermarking," in *Proc. ACM Workshop Multimedia Secur.*, Geneva, Switzerland, Sep. 2006, pp. 80–88.

[6] L. Pérez-Freire, P. Moulin, and F. Pérez-González, "Security of spread-spectrum-based data hiding," in *Security, Steganography, and Watermarking of Multimedia Contents IX*, vol. 6505, E. J. Delp, III, and P. W. Wong, Eds. San Jose, CA, USA: SPIE, 2007.

[7] F. Cayre and P. Bas, "Kerckhoffs-based embedding security classes for WOA data hiding," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 1, pp. 1–15, Mar. 2008.

[8] L. Pérez-Freire and F. Pérez-González, "Spread-spectrum watermarking security," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 1, pp. 2–24, Mar. 2009.

[9] Y.-G. Wang, G. Zhu, S. Kwong, and Y.-Q. Shi, "A study on the security levels of spread-spectrum embedding schemes in the WOA framework," *IEEE Trans. Cybern.*, to be published, doi: 10.1109/TCYB.2017.2735989.

[10] A. Kerckhoffs, "La cryptographie militaire," *J. Sci. Militaires*, vol. 9, pp. 5–38, Jan. 1883.

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

[12] P. Moulin and A. Ivanović, "The zero-rate spread-spectrum watermarking game," *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 1098–1117, Apr. 2003.

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

[14] J. Zhong and S. Huang, "An enhanced multiplicative spread spectrum watermarking scheme," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 12, pp. 1491–1506, Dec. 2006.

[15] J. M. Guo and Y. F. Liu, "High capacity data hiding for error-diffused block truncation coding," *IEEE Trans. Image Process.*, vol. 21, no. 12, pp. 4808–4818, Dec. 2012.

[16] Y. Xiang, I. Natgunanathan, Y. Rong, and S. Guo, "Spread spectrum-based high embedding capacity watermarking method for audio signals," *IEEE/ACM Trans. Audio, Speech, Language Process.*, vol. 23, no. 12, pp. 2228–2237, Dec. 2015.

[17] P. Bas and F. Cayre, "Natural watermarking: A secure spread spectrum technique for WOA," in *Proc. Int. Workshop Inf. Hiding*, Alexandria, VA, USA, Jul. 2006, pp. 1–14.

[18] B. Mathon, P. Bas, F. Cayre, and F. Pérez-González, "Distortion optimization of model-based secure embedding schemes for data-hiding," in *Proc. Int. Workshop Inf. Hiding*, Santa Barbara, CA, USA, May 2008, pp. 325–340.

[19] B. Mathon, P. Bas, F. Cayre, and B. Macq, "Optimization of natural watermarking using transportation theory," in *Proc. ACM Workshop Multimedia Secur.*, Princeton, NJ, USA, 2009, pp. 33–38.

[20] J. Cao and J. Huang, "Controllable secure watermarking technique for tradeoff between robustness and security," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 821–826, Apr. 2012.

[21] B. Mathon, F. Cayre, P. Bas, and B. Macq, "Optimal transport for secure spread-spectrum watermarking of still images," *IEEE Trans. Image Process.*, vol. 23, no. 4, pp. 1694–1705, Apr. 2014.

[22] M. Knott and C. S. Smith, "On the optimal mapping of distributions," *J. Optim. Theory Appl.*, vol. 43, no. 1, pp. 39–49, 1984.

[23] H. W. Kuhn, "The Hungarian method for the assignment problem," *Naval Res. Logistics*, vol. 2, pp. 83–97, Mar. 1955.

[24] Y.-G. Wang, J. Cao, and G. Zhu, "Recursive optimization of spherical watermarking using transportation theory," in *Proc. IEEE Int. Conf. Image Process.*, Quebec City, QC, Canada, Sep. 2015, pp. 3793–3796.

[25] A. Papoulis and S. U. Pillai, *Probability, Random Variables, and Stochastic Processes*, 4th ed. New York, NY, USA: McGraw-Hill, 2002.

[26] G. Monge, "Memoire sur la theorie des deblais et des remblais," in *Proc. Histoire Acad. Roy. Sci.*, Paris, France, 1781, pp. 666–704.

[27] L. V. Kantorovich, "On a problem of Monge," *Usp. Math. Nauk*, vol. 3, pp. 225–226, 1948.

[28] S. Cambanis, S. Huang, and G. Simons, "On the theory of elliptically contoured distributions," *J. Multivariate Anal.*, vol. 11, no. 3, pp. 368–385, 1981.

[29] K.-T. Fang, S. Kotz, and K. W. Ng, *Symmetric Multivariate and Related Distributions*. London, U.K.: Chapman & Hall, 1990.

[30] B. Mathon, P. Bas, F. Cayre, and B. Macq, "Comparison of secure spread-spectrum modulations applied to still image watermarking," *Ann. Telecommun.*, vol. 64, pp. 801–813, Dec. 2009.

[31] M. L. Eaton, "On the projections of isotropic distributions," *Ann. Statist.*, vol. 9, no. 2, pp. 391–400, 1981.

[32] *The Beta Distribution*. Accessed: Jun. 29, 2016. [Online]. Available: http://www.math.uah.edu/stat/special/Beta.html

[33] P. Bas and T. Furon, *Break Our Watermarking System*, 2nd ed. Washington, DC, USA: BOWS, 2007.

[34] A. Cohen, I. Daubechies, and J.-C. Feauveau, "Biorthogonal bases of compactly supported wavelets," *Commun. Pure Appl. Math.*, vol. 45, no. 5, pp. 485–560, 1992.

[35] A. Piva, M. Barni, F. Bartolini, and V. Cappellini, "DCT-based watermark recovering without resorting to the uncorrupted original image," in *Proc. IEEE Int. Conf. Image Process.*, Santa Barbara, CA, USA, Oct. 1997, pp. 520–523.

[36] M. Barni, F. Bartolini, and A. Piva, "Improved wavelet-based watermarking through pixel-wise masking," *IEEE Trans. Image Process.*, vol. 10, no. 5, pp. 783–791, May 2001.

[37] L. Cui and W. Li, "Adaptive multiwavelet-based watermarking through JPW masking," *IEEE Trans. Image Process.*, vol. 20, no. 4, pp. 1047–1060, Apr. 2011.

[38] S. Lin and D. J. Costello, *Error Control Coding: Fundamentals and Applications*. Upper Saddle River, NJ, USA: Prentice-Hall, 1983.

Yuan-Gen Wang received the B.S. degree in physics from Jiangxi Normal University, Nanchang, China, in 1999, and the M.E. and Ph.D. degrees in communication and information system from Sun Yat-Sen University, Guangzhou, China, in 2006 and 2013, respectively. He was with the Zhongkai University of Agriculture and Engineering, Guangzhou, China, as a Lecturer from 2006 to 2011 and as an Associate Professor from 2011 to 2017. From 2015 to 2016, he was a Research Scholar with the New Jersey Institute of Technology, Newark, NJ, USA. He is currently an Associate Professor with Guangzhou University, Guangzhou, China. He has authored or co-authored over ten papers in the SCI journals. His research interests include digital watermarking, forensics, and image processing.

Guopu Zhu (SM'14) received the B.S. degree from Jilin University, China, in 2002, and the M.S. and Ph.D. degrees from the Harbin Institute of Technology, China, in 2004 and 2007, respectively. He was a Post-Doctoral Fellow with Sun Yat-sen University, Guangzhou, China. He was also a Senior Research Associate with the City University of Hong Kong, Hong Kong. He is currently a Professor with the Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences (CAS), China. He has authored or co-authored over 20 papers in SCI journals. His main research areas are multimedia security, image processing, and control theory. He is currently an Associate Editor of the *Journal of Information Security and Applications*. He is a member of the Youth Innovation Promotion Association, CAS.

Yun-Qing Shi (M'88–SM'92–F'05) received the M.S. degree from Shanghai Jiao Tong University, China, and the Ph.D. degree from the University of Pittsburgh, U.S. He has joined New Jersey Institute of Technology, U.S., since 1987. He has authored/co-authored over 300 papers, one book, and five book chapters, and an editor of ten books. He holds 30 U.S. patents and has been a Fellow of National Academy of Inventors, since 2017. His research interests include data hiding, forensics and information assurance, and visual signal processing and communications He served as the Technical Program Chair of IEEE ICME07, the Co-Technical Chair of IWDW, since 2006, and the IEEE MMSP05, the Co-General Chair of the IEEE MMSP02, and a Distinguished Lecturer of the IEEE CASS. He has been a member of few IEEE technical committees. He has served as an Associate Editor for the IEEE TRANSACTIONS ON SIGNAL PROCESSING, the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, and the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS, and an editorial board member of few journals.