Correlation-and-Bit-Aware Spread Spectrum Embedding for Data Hiding

Amir Valizadeh, *Student Member, IEEE*, and Z. Jane Wang, *Member, IEEE*

***Abstract*—This paper proposes a correlation-and-bit-aware concept for data hiding by exploiting the side information at the encoder side, and we present two improved data hiding approaches based on the popular additive spread spectrum embedding idea. We first propose the correlation-aware spread spectrum (CASS) embedding scheme, which is shown to provide better watermark decoding performance than the traditional additive spread spectrum (SS) scheme. Further, we propose the correlation-aware improved spread spectrum (CAISS) embedding scheme by incorporating SS, improved spread spectrum (ISS), and the proposed correlation-and-bit-aware concept. Compared with the traditional additive SS, the proposed CASS and CAISS maintain the simplicity of the decoder. Our analysis shows that, by efficiently incorporating the side information, CASS and CAISS could significantly reduce the host effect in data hiding and improve the watermark decoding performance remarkably. To demonstrate the improved decoding performance and the robustness by employing the correlation-and-bit-aware concept, the theoretical bit-error performances of the proposed data hiding schemes in the absence and presence of additional noise are analyzed. Simulation results show the superiority of the proposed data hiding schemes over traditional SS schemes.**

***Index Terms*—Correlator, data hiding, decoding performance, side information, spread spectrum.**

I. Introduction

THE growing use of the Internet allows users to access, share, manipulate, and distribute digital media data easily and it has affected our daily life profoundly. However, it also makes unauthorized proliferation of digital media much easier, which poses key challenges to the copyright industry and raises critical issues for intellectual protection of digital media.

To address the above concern, watermarking and data hiding have been applied as promising ways for postdelivery protection of digital media data. The basic idea of watermarking and data hiding is to embed some invisible information into the host media signal and the hidden data can later be extracted for desired purposes. The hidden information could be used for digital media authentication, copyright protection, information embedding, database annotation, traitor tracing, and so on.

Manuscript received July 25, 2010; revised December 09, 2010; accepted December 10, 2010. Date of publication December 30, 2010; date of current version May 18, 2011. This work was supported by the Canadian Natural Sciences and Engineering Research Council (NSERC) under Grant STPGP 365164-08 and Grant 11R82396. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Alessandro Piva.

The authors are with the Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, BC, V6T1Z4, Canada (e-mail: amirv@ece.ubc.ca; zjanew@ece.ubc.ca).

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/TIFS.2010.2103061

Depending on the applications, watermarking schemes could generally be categorized into two groups: *watermark detection* and *watermark decoding*. In the first group, the embedded information mainly serves for the verification purpose [1]–[3] where the main goal is to verify whether a specific embedded watermark signal (e.g., representing copyright information) is presented or not. Copyright protection and copy control are two typical applications. In the second group, the embedded information is considered as a hidden message which should be extracted (decoded) correctly at the decoder side [4]–[7]. Watermark detection and watermark decoding problems are formulated differently and different detection/decoding approaches are desired to serve different performance criteria. References [8], [9], [1], and [7] explicitly have pointed out this distinction in their works. This paper is categorized into the second group.

The primary issue in data hiding is the embedding scheme for hiding the information bits. Amongst the proposed embedding schemes for watermarking and data hiding, spread spectrum (SS) and quantization-based methods are two main approaches. Chen and Wornell [10] proposed quantization index modulation (QIM) which watermarks the host signal by quantizing it to the nearest lattice point. The scalar version of the QIM could also be used for fast coding and decoding [11]. One main disadvantage of this approach is its vulnerability against gain attack, even though some efforts have been taken to address this concern [12], [13]. Another main approach for data hiding is spread spectrum (SS)-based, which is probably the most popular watermarking approach. The SS scheme was originally proposed by Cox *et al.* [6] which basically spreads the information over the host signal. There are two types of SS at the encoder side: the additive SS and the multiplicative spread spectrum (MSS) schemes. In additive SS [14], [15], the embedded information is spread over the host signal uniformly while in MSS [16], [17], the embedded information spreads according to the content of the host signal. At the receiver side, since the original media signal is generally not available, a blind decoding scheme is normally employed (e.g., the correlator for the assumed Gaussian host signal). The capability of the SS scheme to embed the watermark corresponding to the content (e.g., in MSS), the simple structure of the decoder, and its robustness to additional noise make SS attractive for data hiding. Despite all these advantages of SS, one main drawback of SS embedding is the interference effect of the host signal which causes a degradation in decoding performance. To reduce the interference effect of the host signal, Malvar and Florencio proposed the improved spread spectrum (ISS) [18] by exploiting the side information at the encoder side. The ISS scheme uses the correlation between the host signal and the key to modulate the embedding power and it has led to the best theoretical decoding performance for the category of SS schemes. It is worth mentioning that although the SS scheme

was originally proposed for image watermarking [6], it is a general embedding framework which could also be used for audio [19]–[21] and video [22]–[24] data hiding.

In this paper, our main purpose is to propose an improved embedding scheme based on SS which could efficiently decrease the interference effect of the host signal. Inspired by the success of ISS [18], we propose a correlation-and-bit-aware concept for data hiding by exploring the correlation between the host signal and the watermark key as well as the information bit to be embedded into the host signal as the side information at the encoder. The proposed approaches are referred as correlation-aware data hiding approaches. By incorporating the correlation-and-bit-aware concept with the SS scheme, a new correlation-aware SS (CASS) data hiding scheme is proposed. Our theoretical analysis shows that CASS is superior to the SS counterpart in terms of watermark decoding performance. To further improve the decoding performance of ISS, a correlation-aware improved spread spectrum (CAISS) data hiding scheme is proposed which is a combination of the SS, ISS, and the correlation-and-bit-aware concept. Having introduced the CAISS scheme, we will show theoretically that it outperforms the ISS scheme by yielding higher decoding performance. In addition, we will prove that the proposed CASS scheme is more robust against the interference effect than the traditional SS. Similarly, better robustness of the proposed CAISS over the ISS will be shown. Moreover, it will be shown that employing the proposed CASS and CAISS schemes could increase the payload.

Further assuming additional Gaussian noise is added to the received signal, we derive the corresponding test statistic distribution at the decoder side. Based on the derived distributions, the error probability of the CASS and CAISS schemes in the presence of noise will be presented. The simulation results verify the integrity of the derived theoretical decoding performances and support the claim that the proposed correlation-aware schemes can provide better decoding performances in the presence or absence of additional noise. It is worth emphasizing that, compared with the traditional blind SS scheme, the proposed correlation-aware data hiding approaches do not require additional information at the decoder side and do not change the simple decoder structure.

The rest of the paper is organized as follows. In Section II, the basic idea of SS embedding is described briefly. The correlation-and-bit-aware concept and the CASS scheme are presented in Section III and the improvements of CASS over SS are shown. In Section IV, the CAISS scheme is proposed and its superiority over other SS schemes is illustrated. The performance analyses of the proposed correlation-aware data hiding schemes in the presence of the noise are accomplished in Section V. Simulation results are provided in Section VI and concluding remarks are given in Section VII.

II. Conventional SS Scheme

In the conventional SS scheme, the bit message b with amplitude $A > 0$ is embedded into the host signal. The information bit to be hidden in the host signal is usually from the binary set $b \in \{-1, +1\}$. For simplicity, it is assumed that the host signal $\mathbf{x} = [x_1, x_2, \ldots, x_N]^T$ follows Gaussian independent and identical distributions (i.i.d.) with zero mean and variance σ_x^2, i.e., $\mathbf{x} \sim \mathcal{N}(\mathbf{0}_N, \sigma_x^2 \mathbf{I}_N)$, where $\mathbf{I}_N$ and $\mathbf{0}_N$ are the $N \times N$ identity matrix and zero vector with dimension N, respectively. Here, N is the number of the host coefficients used for conveying one information bit. The SS scheme employs the key signal $\mathbf{s} = [s_1, s_2, \ldots, s_N]^T$ for the sake of security and this key is assumed to be selected from a binary set $s_i \in \{-1, +1\}$. Based on the SS embedding, the watermarked signal $\mathbf{r} = [r_1, r_2, \ldots, r_N]^T$ can be represented in the following form:

$$r_i = x_i + s_i A b, \quad i = 1, 2, \ldots, N. \tag{1}$$

Generally, the distortion due to any watermark embedding can be defined as

$$D = \frac{1}{N} E\{\|\mathbf{r} - \mathbf{x}\|^2\} \tag{2}$$

where $E\{\cdot\}$ means the expectation operator and $\|\cdot\|$ is defined as the norm of a vector.

Since the host coefficients are assumed to be Gaussian i.i.d.'s, the optimal decoder is the correlation between the received data and the key. The correlator estimates the hidden information bit as

$$\hat{b} = \text{sign}\{z\} \tag{3}$$

where

$$z = \mathbf{r}^T \mathbf{s} \tag{4}$$

and $\text{sign}\{\cdot\}$ function gives out $+1$, -1, and 0 if its argument is positive, negative, and zero, respectively.

Given $b = +1$ and $b = -1$, the probability distribution functions (pdfs) of the sufficient statistic $z = \mathbf{r}^T \mathbf{s}$ could be determined as follows:

$$f_Z(z \mid b = +1) = \mathcal{N}(NA, N\sigma_x^2) \tag{5}$$

$$f_Z(z \mid b = -1) = \mathcal{N}(-NA, N\sigma_x^2). \tag{6}$$

From the above pdfs, it is clear that the SS embedding scheme is not error-free even in the absence of any additional noise. The explanation of this phenomenon is that the host signal is actually treated as noise in SS embedding. Since the host signal power is generally much higher than the embedding signal (watermark) power due to the imperceptibility requirement of data hiding, this noise effect of the host signal results in a degradation in the decoding performance of SS.

To reduce the interference effect of the host signal, Malvar and Florencio proposed the improved spread spectrum embedding [18] by modulating the energy of the inserted signal in the following form:

$$\mathbf{r} = \mathbf{x} + \mathbf{s} A b - \lambda \mathbf{s}\mathbf{s}^T \mathbf{x} \tag{7}$$

where λ is a free parameter to be designed.

III. CASS Data Hiding Approach

As introduced in Section II, in SS embedding, the host signal is the source of uncertainty at the decoder side. The fundamental reason is that, as implied in (6) and (5), the pdf leakage causes the decoding error. The leakage means that the test statistic given in (4) could get negative and positive values when we send the bit b of $+1$ and -1, respectively. This phenomenon has been

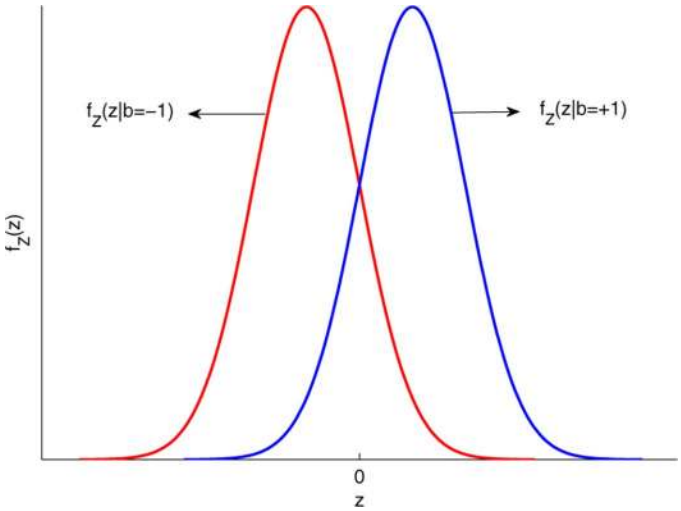

Fig. 1. Illustration of the pdfs in (6) and (5) of the test statistic z in (4) for the SS scheme.

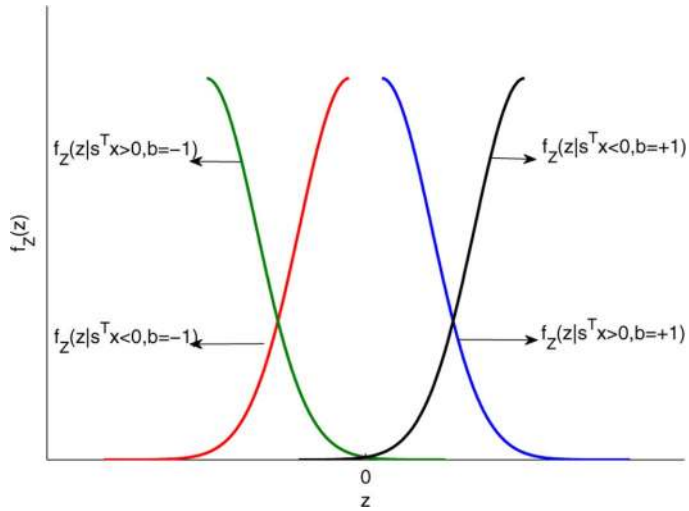

Fig. 2. Illustration of the pdfs in (10)–(13) of the test statistic z in (9) for the proposed CASS scheme.

demonstrated clearly in Fig. 1. To reduce this interference effect of the host signal, the correlation-and-bit-aware concept is introduced in this section. The SS-based correlation-and-bit-aware concept is motivated by the prior knowledge that we know the decoder structure is the correlation between the received signal and the key. Such correlation is a summation of the correlation between the host signal and the key and the correlation between the key and the modulated hidden information. As the encoder side, since we know the correlation between the host signal and the key and the bit message b to be embedded in advance, we could exploit such side information in a smart way to reduce the original pdf leakage in SS. By exploring the correlation-and-bit-aware concept in SS embedding, we therefore propose an embedding scheme, referred as correlation-aware spread spectrum (CASS), as follows:

$$\mathbf{r} = \begin{cases} \mathbf{x} + \mathbf{s}A_1, & \text{if} \quad \mathbf{s}^T\mathbf{x} \geq 0, \quad b = +1 \\ \mathbf{x} - \mathbf{s}A_2, & \text{if} \quad \mathbf{s}^T\mathbf{x} \geq 0, \quad b = -1 \\ \mathbf{x} - \mathbf{s}A_1, & \text{if} \quad \mathbf{s}^T\mathbf{x} < 0, \quad b = -1 \\ \mathbf{x} + \mathbf{s}A_2, & \text{if} \quad \mathbf{s}^T\mathbf{x} < 0, \quad b = +1 \end{cases} \tag{8}$$

where A_1 and A_2 $(0 < A_1 < A_2)$ are two amplitude levels determined with respect to the allowed distortion.

The intuitive idea behind the CASS embedding scheme is to modulate the bit message of information by two amplitude levels based on the correlation between the host signal and the key as well as the bit message to be embedded. More specifically, suppose that the message bit $+1$ needs to be embedded: if the correlation between the host signal and the key is positive then the smaller amplitude A_1 should be used for modulation; if the correlation is negative then the larger amplitude A_2 should be employed. Suppose the bit message -1 is to be embedded: if the correlation of the host signal and the key is negative then the smaller amplitude is used, and if the correlation is positive then the larger amplitude is used. The underlying advantage of the proposed CASS embedding is cleared when the sufficient statistic of the decoder is investigated shortly.

We can prove that, with the assumption that the host signal follows Gaussian i.i.d., the optimal decoder for the CASS embedding scheme (8) is the correlator as defined in (3) with the test statistic z defined in (4). The detailed proof is omitted here since CASS can be treated as a particular case of CAISS with $\lambda_h = 0$, while we will describe CAISS and provide the proof of CAISS in Section IV.

With the optimal decoder in (3), the sufficient statistic z in (4) using CASS embedding in (8) can be expressed by the following form:

$$z = \begin{cases} \mathbf{s}^T\mathbf{x} + NA_1, & \text{if} \quad \mathbf{s}^T\mathbf{x} \geq 0, \quad b = +1 \\ \mathbf{s}^T\mathbf{x} - NA_2, & \text{if} \quad \mathbf{s}^T\mathbf{x} \geq 0, \quad b = -1 \\ \mathbf{s}^T\mathbf{x} - NA_1, & \text{if} \quad \mathbf{s}^T\mathbf{x} < 0, \quad b = -1 \\ \mathbf{s}^T\mathbf{x} + NA_2, & \text{if} \quad \mathbf{s}^T\mathbf{x} < 0, \quad b = +1. \end{cases} \tag{9}$$

Since the host signal is assumed to follow Gaussian distribution, given the bit message b and the sign of the correlation between the host signal and the key, the sufficient statistic z consists of four conditional half-Gaussian pdfs as follows:

$$f_Z(z \,|\, \mathbf{s}^T\mathbf{x} \geq 0, b = +1) = 2\mathcal{N}\left(NA_1, N\sigma_x^2\right) u(z - NA_1) \tag{10}$$

$$f_Z(z \,|\, \mathbf{s}^T\mathbf{x} < 0, b = +1) = 2\mathcal{N}\left(NA_2, N\sigma_x^2\right) u(-(z - NA_2)) \tag{11}$$

$$f_Z(z \,|\, \mathbf{s}^T\mathbf{x} \geq 0, b = -1) = 2\mathcal{N}\left(-NA_2, N\sigma_x^2\right) u(z + NA_2) \tag{12}$$

$$f_Z(z \,|\, \mathbf{s}^T\mathbf{x} < 0, b = -1) = 2\mathcal{N}\left(-NA_1, N\sigma_x^2\right) u(-(z + NA_1)) \tag{13}$$

where $u(\cdot)$ defines the step function.

The above pdfs of the sufficient statistic z provide us more insight into the underlying advantages of the proposed CASS embedding scheme and the superiority of CASS over SS. The pdfs in (10)–(13) of the sufficient statistic are shown in Fig. 2. It depicts how CASS embedding could reduce the host-interference effect. It is seen that when the message bit is $+1$ and the correlation between the host signal and the key is positive, there is no pdf leakage. Similarly, when the bit message is -1 and the correlation is negative, there is no pdf leakage. For the cases that the bit message is $+1$ and the correlation is negative and that the bit message is -1 and the correlation is positive, there might still be some pdf leakage. Therefore, from comparing Figs. 1 and 2, it is justified intuitively that the pdf leakage for the CASS scheme

is less than the conventional SS where the message bit is modulated by a single amplitude level regardless of the correlation between the host signal and the key.

Having intuitively explained the underlying advantage of CASS data hiding, we now proceed to analyze the decoding performance of CASS by deriving the bit-error rate (BER). The probability of error of CASS data hiding is defined as

$$\begin{aligned} P_e &= Pr\{\hat{b} \neq b\} \\ &= \frac{1}{4} \times \Pr\{\hat{b} = +1 \,|\, b = -1, \mathbf{s}^T\mathbf{x} > 0\} \\ &\quad + \frac{1}{4} \times \Pr\{\hat{b} = +1 \,|\, b = -1, \mathbf{s}^T\mathbf{x} < 0\} \\ &\quad + \frac{1}{4} \times \Pr\{\hat{b} = -1 \,|\, b = +1, \mathbf{s}^T\mathbf{x} < 0\} \\ &\quad + \frac{1}{4} \times \Pr\{\hat{b} = -1 \,|\, b = +1, \mathbf{s}^T\mathbf{x} > 0\} \end{aligned} \tag{14}$$

where $\hat{b}$ is the decoded bit. As discussed earlier, the second and the fourth terms are zero since there are no pdf leakages. Therefore, the error probability is simplified to the following expression:

$$P_{e-\mathrm{CASS}} = Q\left(\frac{NA_2}{\sqrt{N\sigma_x^2}}\right) \tag{15}$$

where $Q(x) = (1)/(2\pi)\int_x^\infty \exp((-u^2)/(2))du$. To fairly compare different data hiding algorithms, the same distortion D due to embedding should be assumed. The distortion defined in (2) due to CASS embedding in (8) can be expressed as

$$D = \left(A_1^2 + A_2^2\right)/2. \tag{16}$$

Thus, using (15) and (16), the error probability of CASS in terms of the distortion D is expressed as

$$P_{e-\mathrm{CASS}} = Q\left(\frac{N\sqrt{2D - A_1^2}}{\sqrt{N\sigma_x^2}}\right). \tag{17}$$

It is noteworthy that, since $0 < A_1 < A_2$, according to the distortion expression in (16), the amplitudes A_1 and A_2 always satisfy the following inequalities:

$$0 < A_1 < \sqrt{D} < A_2 < \sqrt{2D}. \tag{18}$$

To compare the error probability of CASS with that of SS, we need to provide the error probability of the SS scheme in terms of D. We can show that

$$P_{e-\mathrm{SS}} = Q\left(\frac{N\sqrt{D}}{\sqrt{N\sigma_x^2}}\right). \tag{19}$$

The superiority of the proposed CASS over SS is presented as a proposition as follows.

Proposition 1: With the assumption that the host signal follows Gaussian i.i.d., the proposed CASS scheme in (8) yields smaller error probability (17) than the traditional SS in (19).

Proof: For CASS to have better decoding performance than that of SS, the error probability of the CASS scheme should always be smaller than that of SS. In other words, we should have

$$Q\left(\frac{N\sqrt{2D - A_1^2}}{\sqrt{N\sigma_x^2}}\right) < Q\left(\frac{N\sqrt{D}}{\sqrt{N\sigma_x^2}}\right). \tag{20}$$

Since $Q(\cdot)$ is a monotonic decreasing function, to satisfy the aforementioned expression, we need to show that $\sqrt{2D - A_1^2} > \sqrt{D}$. It is pretty straightforward to show that it requires $0 < A_1 < \sqrt{D}$. From (18), it is obvious that this constraint is always satisfied. Therefore, it is concluded that the CASS always outperforms the SS scheme in decoding performance. □

The superiority of the CASS over SS scheme in the sense of decoding has been proved so far. In the rest of this section, we aim at quantitatively investigating the improvement of CASS in terms of error probability, robustness, and payload. We attempt to answer the question of how much improvement is obtained by employing the CASS scheme. We define the error probability improvement factor (EPIF) as follows:

$$\mathrm{EPIF}_{1-2} \triangleq \frac{P_1}{P_2} \tag{21}$$

where P_1 and P_2 are two probability of error functions to be compared. EPIF represents the improvement ratio and a smaller value implies a better improvement. In data hiding, it is more appropriate to express EPIF as a function of the document to watermark ratio (DWR) defined in the following form:

$$\mathrm{DWR} \triangleq 10\log\left(\frac{\sigma_x^2}{D}\right). \tag{22}$$

When comparing the error probabilities of CASS (17) and SS (19), we have the EPIF as

$$\mathrm{EPIF}_{\mathrm{CASS-SS}} = Q\left(\frac{N\sqrt{2D - A_1^2}}{\sqrt{N\sigma_x^2}}\right) \Bigg/ Q\left(\frac{N\sqrt{D}}{\sqrt{N\sigma_x^2}}\right). \tag{23}$$

Since $0 < A_1 < \sqrt{D}$, it could be shown that the $\mathrm{EPIF}_{\mathrm{CASS-SS}}$ is bounded as follows:

$$\frac{Q(10^{-\mathrm{DWR}/20}\sqrt{2N})}{Q(10^{-\mathrm{DWR}/20}\sqrt{N})} < \mathrm{EPIF}_{\mathrm{CASS-SS}} < 1. \tag{24}$$

The lower bound represents the best achievable improvement given the DWR and the number of host coefficients.

We proposed using EPIF as a measure to investigate the error probability improvement of the CASS over SS under a fixed distortion. As discussed earlier, the host signal is an interference source for decoding. It is important to measure the robustness of the embedding schemes against interference. We now proceed to investigate how much more host-interference CASS could tolerate compared with the SS scheme, given a fixed error probability and distortion due to embedding. It should be clarified that the robustness discussed here is referred to the interference effect of the host signal and not to other additional noise. To quantify the robustness, assuming equal error probability and

equal distortion due to embedding, we define the interference robustness improvement factor (IRIF) as

$$\mathrm{IRIF}_{2-1} \triangleq \frac{\sigma_1^2}{\sigma_2^2} \tag{25}$$

where σ_1^2 and σ_2^2 represent the corresponding host signal powers of two embedding schemes to be compared. Let us denote $\sigma^2_{x-\mathrm{CASS}}$ and $\sigma^2_{x-\mathrm{SS}}$ the host signal powers in CASS and SS, respectively, when the error probability and the distortion are assumed to be the same in two embedding schemes. With equal error probability and equal distortion due to embedding, referring to the error probabilities in (17) and (19), we have

$$\frac{2D - A_1^2}{\sigma^2_{x-\mathrm{CASS}}} = \frac{D}{\sigma^2_{x-\mathrm{SS}}}. \tag{26}$$

According to the IRIF definition in (25), we have

$$\mathrm{IRIF}_{\mathrm{CASS-SS}} = \frac{1}{2-\eta} \tag{27}$$

where

$$A_1^2 = \eta D, 0 < \eta < 1. \tag{28}$$

It is straightforward to show that since $0 < \eta < 1$ the $\mathrm{IRIF}_{\mathrm{CASS-SS}}$ is bounded as

$$\frac{1}{2} < \mathrm{IRIF}_{\mathrm{CASS-SS}} < 1. \tag{29}$$

The IRIF robustness in (29) reveals that CASS is more robust to the host interference than SS, and CASS can tolerate the interference power up to twice the conventional SS scheme.

Another advantage of the CASS scheme is its increased payload. Given the same error probability and distortion due to embedding, more information bits could be embedded into the host signal in the CASS scheme than SS. We define the payload improvement factor (PIF) as a payload measure in the following:

$$\mathrm{PIF}_{2-1} \triangleq \frac{N_1}{N_2} \tag{30}$$

where N_1 and N_2 are the numbers of host coefficients used for conveying one bit of information where the error probability and the distortion are assumed to be same in the embedding schemes. Referring to the PIF definition and the error probabilities in (17) and (19), we have the following expression

$$N_{\mathrm{CASS}}(2D - A_1^2) = N_{\mathrm{SS}} D \tag{31}$$

where N_{CASS} and N_{SS} are the required numbers of host coefficients for the CASS and SS schemes. This expression results in the following PIF using (28)

$$\mathrm{PIF}_{\mathrm{CASS-SS}} = 2 - \eta. \tag{32}$$

We can see that the obtained PIF is always greater than one, meaning that the CASS scheme could increase the payload of data hiding in comparison with SS.

IV. CAISS Data Hiding Approach

In this section, we proceed to exploit the correlation-and-bit-aware concept for designing an improved embedding scheme based on ISS. As mentioned earlier, the ISS embedding scheme [18] was introduced to improve the decoding performance of the traditional SS. We plan to incorporate the ISS with the correlation-and-bit-aware idea to further improve the decoding performance of ISS.

By taking a look at Fig. 2, we can see that the main source of decoding error is the pdf leakage from two cases: one is that $b = +1$ and $\mathbf{s}^T\mathbf{x}$ is negative, and the other is that $b = -1$ and $\mathbf{s}^T\mathbf{x}$ is positive. Intuitively, squeezing the two pdfs involving the leakage (e.g., as in ISS) could improve the decoding performance. Therefore, the basic idea of the CAISS scheme is to combine CASS and ISS: for the cases that there is no pdf leakage (i.e., when $b = +1$ and $\mathbf{s}^T\mathbf{x}$ is positive, and when $b = -1$ and $\mathbf{s}^T\mathbf{x}$ is negative), employ the CASS scheme because there is no interference effect at the decoding side; for the left two cases that there is leakage, the ISS embedding is employed since ISS can modulate the embedding energy to compensate for the host signal interference. We describe the proposed CAISS embedding scheme as follows:

$$\mathbf{r} = \begin{cases} \mathbf{x} + \mathbf{s}A_1, & \text{if } \mathbf{s}^T\mathbf{x} \geq 0,\ b = +1 \\ \mathbf{x} - \mathbf{s}A_2 - \lambda_h \mathbf{s}(\mathbf{s}^T\mathbf{x}), & \text{if } \mathbf{s}^T\mathbf{x} \geq 0,\ b = -1 \\ \mathbf{x} - \mathbf{s}A_1, & \text{if } \mathbf{s}^T\mathbf{x} < 0,\ b = -1 \\ \mathbf{x} + \mathbf{s}A_2 - \lambda_h \mathbf{s}(\mathbf{s}^T\mathbf{x}), & \text{if } \mathbf{s}^T\mathbf{x} < 0,\ b = +1 \end{cases} \tag{33}$$

where λ_h is a parameter determined by the allowed distortion. We will later show that the following bound on λ_h holds

$$0 \leq \lambda_h \leq \frac{1}{N}. \tag{34}$$

Before we can show why the CAISS scheme can yield better decoding performance than that of both CASS and ISS, we need first to obtain the optimal decoder, and so the following proposition is provided.

Proposition 2: With the assumption of Gaussian i.i.d. host signal samples, the optimal decoder for the CAISS scheme (33) which minimizes the error probability is the correlator defined in (3) with the test statistic z in (4).

Proof: The optimal decoder minimizing the error probability $Pe = \Pr\{\hat{b} \neq b\}$ is obtained by the maximum likelihood (ML) criterion. The ML estimate $\hat{b}$ is expressed as

$$\hat{b} = \underset{b \in \{\pm 1\}}{\operatorname{argmax}} f_{\mathbf{R}}(\mathbf{r} \,|\, b, A_1, A_2, \mathbf{s}), \tag{35}$$

where $f_{\mathbf{R}}(\mathbf{r} \,|\, b, A_1, A_2, \mathbf{s})$ represents the conditional pdf of $\mathbf{r}$ given the bit message, amplitudes, and the key. Therefore, the decoder decides $\hat{b} = +1$ if

$$f_{\mathbf{R}}(\mathbf{r} \,|\, b = +1, A_1, A_2, \mathbf{s}) > f_{\mathbf{R}}(\mathbf{r} \,|\, b = -1, A_1, A_2, \mathbf{s}). \tag{36}$$

It is clear that the conditional pdfs are needed to obtain the decision rule. Assuming that the host signal coefficients are Gaussian i.i.d.'s with zero-mean and variance σ_x^2, we can show

that the conditional pdfs regarding the CAISS embedding in (33) are in the following form:

$$\begin{aligned} f_{\mathbf{R}}&(\mathbf{r}|b=+1, A_1, A_2, \mathbf{s}) \\ &= \frac{1}{2\left(\sqrt{2\pi\sigma_x^2}\right)^N} \exp\left\{\frac{-1}{2\sigma_x^2}(\mathbf{r}-\mathbf{s}A_1)^T(\mathbf{r}-\mathbf{s}A_1)\right\} \\ &\quad + \frac{1}{2|\mathbf{M}|\left(\sqrt{2\pi\sigma_x^2}\right)^N} \\ &\quad \times \exp\left\{\frac{-1}{2\sigma_x^2}(\mathbf{r}-\mathbf{s}A_2)^T\mathbf{M}^{-2}(\mathbf{r}-\mathbf{s}A_2)\right\} \end{aligned} \tag{37}$$

$$\begin{aligned} f_{\mathbf{R}}&(\mathbf{r}\,|\,b=-1, A_1, A_2, \mathbf{s}) \\ &= \frac{1}{2\left(\sqrt{2\pi\sigma_x^2}\right)^N} \exp\left\{\frac{-1}{2\sigma_x^2}(\mathbf{r}+\mathbf{s}A_1)^T(\mathbf{r}+\mathbf{s}A_1)\right\} \\ &\quad + \frac{1}{2|\mathbf{M}|\left(\sqrt{2\pi\sigma_x^2}\right)^N} \\ &\quad \times \exp\left\{\frac{-1}{2\sigma_x^2}(\mathbf{r}+\mathbf{s}A_2)^T\mathbf{M}^{-2}(\mathbf{r}+\mathbf{s}A_2)\right\} \end{aligned} \tag{38}$$

where

$$\mathbf{M} = \mathbf{I}_N - \lambda_h \mathbf{s}\mathbf{s}^T \tag{39}$$

and $|\cdot|$ denotes the determinant operator. By plugging the conditional pdfs (37) and (38) into the decoder in (36), with some calculations, we have that the decoder decides $\hat{b} = +1$ if the inequality (40) is satisfied

$$\begin{aligned} &\exp\left\{\frac{2\mathbf{r}^T\mathbf{s}A_1}{\sigma_x^2}\right\} \\ &\quad + \frac{1}{|\mathbf{M}|}\exp\left\{\frac{\mathbf{r}^T(A_1\mathbf{I}_N + A_2\mathbf{M}^{-2})\mathbf{s}}{\sigma_x^2}\right. \\ &\qquad\qquad - \frac{\mathbf{r}^T(\mathbf{M}^{-2}-\mathbf{I}_N)\mathbf{r}}{2\sigma_x^2} \\ &\qquad\qquad \left. - \frac{\mathbf{s}^T(A_2^2\mathbf{M}^{-2} - A_1^2\mathbf{I}_N)\mathbf{s}}{2\sigma_x^2}\right\} \\ &\quad > 1 + \frac{1}{|\mathbf{M}|}\exp\left\{\frac{\mathbf{r}^T(A_1\mathbf{I}_N - A_2\mathbf{M}^{-2})\mathbf{s}}{\sigma_x^2}\right. \\ &\qquad\qquad - \frac{\mathbf{r}^T(\mathbf{M}^{-2}-\mathbf{I}_N)\mathbf{r}}{2\sigma_x^2} \\ &\qquad\qquad \left. - \frac{\mathbf{s}^T(A_2^2\mathbf{M}^{-2} - A_1^2\mathbf{I}_N)\mathbf{s}}{2\sigma_x^2}\right\}. \end{aligned} \tag{40}$$

Now, we want to show that if $\mathbf{r}^T\mathbf{s}$ is positive, then the above inequality holds. If $\mathbf{r}^T\mathbf{s} > 0$, then the first term in the left-hand side of (40) would be larger than one. To show that the second term in the left side is larger than the second term in the right side of inequality (40), we need to prove that

$$\mathbf{r}^T(A_1\mathbf{I}_N + A_2\mathbf{M}^{-2})\mathbf{s} > \mathbf{r}^T(A_1\mathbf{I}_N - A_2\mathbf{M}^{-2})\mathbf{s}. \tag{41}$$

With (39) and using Woodbury equation, we have

$$\mathbf{M}^{-2} = \mathbf{I}_N + \beta\mathbf{s}\mathbf{s}^T \tag{42}$$

where

$$\beta = \alpha^2 N - 2\alpha, \alpha = \frac{1}{N - \frac{1}{\lambda_h}}. \tag{43}$$

Therefore, with (42) and (43), now (41) becomes

$$\mathbf{r}^T\mathbf{s}[A_1 + A_2(1+\beta N)] > \mathbf{r}^T\mathbf{s}[A_1 - A_2(1+\beta N)]. \tag{44}$$

To satisfy (44), the parameter $(1+\beta N)$ is required to always be positive. It is easy to show that $(1+\beta N) = (\alpha N - 1)^2$ and thus is always positive.

Therefore, the decoder decides $\hat{b} = +1$ when $\mathbf{r}^T\mathbf{s} > 0$. Similarly, we can show that the decoder decides $\hat{b} = -1$ when $\mathbf{r}^T\mathbf{s} < 0$. We thus conclude that the optimal decoder is the correlator defined in (3) with the test statistic z in (4). □

By comparing the embedding schemes in (8) and (33), it is clear that CASS is a particular case of CAISS with $\lambda_h = 0$. Therefore, we can similarly show that the same correlator decoder is optimal for CASS, and the performance analysis of the CASS scheme presented in Section III can be considered a special case of CAISS.

We have shown that the correlator is the optimal decoder for the CAISS scheme. One important issue is to determine an appropriate value of the parameter λ_h in CAISS. We propose determining λ_h by minimizing the error probability. For CAISS in (33), the test statistic z in (4) can be expressed as

$$z = \begin{cases} \mathbf{s}^T\mathbf{x} + NA_1, & \text{if } \mathbf{s}^T\mathbf{x} \geq 0,\ b=+1 \\ \mathbf{s}^T\mathbf{x}(1-\lambda_h N) - NA_2, & \text{if } \mathbf{s}^T\mathbf{x} \geq 0,\ b=-1 \\ \mathbf{s}^T\mathbf{x} - NA_1, & \text{if } \mathbf{s}^T\mathbf{x} < 0,\ b=-1 \\ \mathbf{s}^T\mathbf{x}(1-\lambda_h N) + NA_2, & \text{if } \mathbf{s}^T\mathbf{x} < 0,\ b=+1. \end{cases} \tag{45}$$

Given b and the correlation between key and the host signal, the conditional pdfs of the test statistic z are in the following form:

$$f_Z(z\,|\,\mathbf{s}^T\mathbf{x} \geq 0, b=+1) = 2\mathcal{N}\left(NA_1, N\sigma_x^2\right) u(z - NA_1) \tag{46}$$

$$\begin{aligned} f_Z(z\,|\,\mathbf{s}^T\mathbf{x} < 0, b=+1) =& 2\mathcal{N}\left(NA_2, N\sigma_x^2(1-\lambda_h N)^2\right) \\ &\times u(-(z - NA_2)) \end{aligned} \tag{47}$$

$$\begin{aligned} f_Z(z\,|\,\mathbf{s}^T\mathbf{x} \geq 0, b=-1) =& 2\mathcal{N}\left(-NA_2, N\sigma_x^2(1-\lambda_h N)^2\right) \\ &\times u(z + NA_2) \end{aligned} \tag{48}$$

$$\begin{aligned} f_Z(z\,|\,\mathbf{s}^T\mathbf{x} < 0, b=-1) =& 2\mathcal{N}\left(-NA_1, N\sigma_x^2\right) \\ &\times u(-(z + NA_1)). \end{aligned} \tag{49}$$

Now we proceed to derive the theoretical BER performance of the proposed CAISS data hiding scheme. The distortion (2) due to CAISS embedding (33) is expressed as

$$D = \frac{1}{2}\left(A_1^2 + A_2^2 + \lambda_h^2 N\sigma_x^2\right). \tag{50}$$

Referring to the distributions of the statistics given in (46)–(49), the distortion in (50), and the bit-error probability defined in (14), we can show that the BER of the CAISS scheme is obtained as

$$P_{e-\mathrm{CAISS}} = Q\left(\frac{N\sqrt{2D - A_1^2 - \lambda_h^2 N\sigma_x^2}}{\sqrt{(1-\lambda_h N)^2 N\sigma_x^2}}\right). \tag{51}$$

We now can determine the optimal value of the parameter λ_h by minimizing the above error probability. Since the Q function

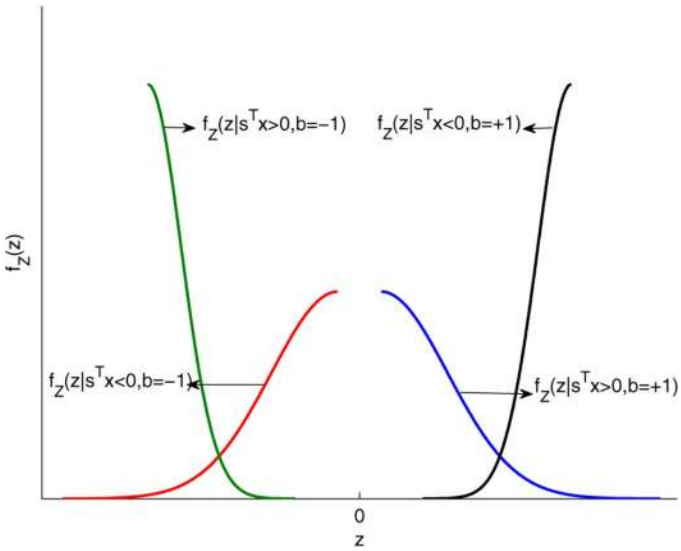

Fig. 3. Illustration of the pdfs in (46)–(49) of the test statistic z in (45) for the proposed CAISS scheme.

is monotonically decreasing, it is equivalent to maximizing its argument. Taking the derivative of the argument and letting it to be zero and some simplifications lead us to

$$\lambda_h = \begin{cases} \frac{1}{N}, & \text{if } D > \frac{\sigma_x^2 + A_1^2 N}{2N} \\ \frac{2D - A_1^2}{\sigma_x^2}, & \text{if } D \leq \frac{\sigma_x^2 + A_1^2 N}{2N}. \end{cases} \tag{52}$$

To provide more insight into the parameter λ_h, we further show that the inequality in (34) always holds. From (52), it is clear that λ_h is a function of the distortion D, i.e., $\lambda_h(D)$. To prove the inequality in (34), we show that when the distortion approaches zero and infinity, λ_h approaches zero and $1/N$, respectively, and that $\lambda_h(D)$ is a monotonically increasing function of the distortion D. It is pretty easy to verify that

$$\lim_{D \to 0} \lambda_h = 0, \lim_{D \to \infty} \lambda_h = \frac{1}{N}. \tag{53}$$

To show that $\lambda_h(D)$ is a monotonically increasing function of D, the derivative of (52) with respect to D is taken and we see that $(d\lambda_h)/(dD) \geq 0$. Thus, we can conclude that λ_h is an increasing function of the distortion. Therefore, together with (53), the inequality in (34) is verified.

From the monotonically increasing behavior of $\lambda_h(D)$ and the pdfs in (47) and (48), we can see that increasing the embedding distortion could decrease the variance in the related pdfs and thus improve the decoding performance. To intuitively explain the superior performance of CAISS over CASS, we plot the pdfs of the test statistic z in (46)–(49) in Fig. 3. Compared with the pdfs in Fig. 2, we can see that, similar to CASS, the correlation-and-bit-aware concept could separate two pdfs completely in CAISS, and that the left two pdfs are better separated in CAISS than in CASS due to smaller variances in the related distributions. Therefore, substantial reduction of pdf leakage is observed in CAISS and thus leads to the reduced interference effect of the host signal.

We have shown in Section III that the proposed CASS is superior to SS. Here similarly, we show that the proposed CAISS outperforms both SS and ISS, with more details provided in the following Proposition.

Proposition 3: With the assumption of Gaussian i.i.d. host signal samples, the error probability of the CAISS embedding scheme in (51) is smaller than that of ISS, i.e., $P_{e-\mathrm{CAISS}} < P_{e-\mathrm{ISS}}$.

Proof: The proof details are given in the Appendix. □

It should be noted that since SS is a particular case of ISS and has worse performance than that of ISS, the above proposition implies that the error probability of CAISS is smaller than that of SS.

So far, we have proved that the proposed CAISS data hiding scheme provides better decoding performance than that of the SS and ISS schemes. We now proceed to quantify the performance improvement of CAISS over SS and ISS in terms of error probability, robustness, and payload. We first examine the EPIF measure for BER performance improvement of CAISS over SS. According to the error probabilities in (51) and (19), the EPIF is obtained as

$$\mathrm{EPIF}_{\mathrm{CAISS-SS}} = Q\left(\frac{N\sqrt{2D - A_1^2 - \lambda_h^2 N\sigma_x^2}}{\sqrt{(1-\lambda_h N)^2 N\sigma_x^2}}\right) \Big/ Q\left(\frac{N\sqrt{D}}{\sqrt{N\sigma_x^2}}\right). \tag{54}$$

Since $0 < A_1 < \sqrt{D}$ and $0 \leq \lambda_h \leq 1/N$, it could be shown that the above EPIF is bounded as

$$0 \leq \mathrm{EPIF}_{\mathrm{CAISS-SS}} < 1. \tag{55}$$

By comparing (55) with (24) for the CASS scheme, a smaller lower-bound is observed for CAISS, implying a further improvement of CAISS over SS. Similarly, referring to the error probabilities in (51) and (85), the improvement of CAISS over ISS can be described by

$$\mathrm{EPIF}_{\mathrm{CAISS-ISS}} = Q\left(\frac{N\sqrt{2D - A_1^2 - \lambda_h^2 N\sigma_x^2}}{\sqrt{(1-\lambda_h N)^2 N\sigma_x^2}}\right) \Big/ Q\left(\frac{N\sqrt{D - \lambda^2 N\sigma_x^2}}{\sqrt{(1-\lambda N)^2 N\sigma_x^2}}\right). \tag{56}$$

We can show that the above EPIF is bounded as

$$0 \leq \mathrm{EPIF}_{\mathrm{CAISS-ISS}} < 1. \tag{57}$$

We now proceed to investigate the robustness of CAISS against the host signal effect. With a fixed error probability, we have the following Proposition 4, which shows that the CAISS scheme is more robust against the interference effect of the host signal than ISS.

Proposition 4: With the assumption that the host signal follows Gaussian i.i.d., the IRIF for the CAISS (33) and ISS (7) schemes is less than one, i.e., $\mathrm{IRIF}_{\mathrm{CAISS-ISS}} < 1$, where

$$\mathrm{IRIF}_{\mathrm{CAISS-ISS}} = \frac{\sigma_{x-\mathrm{ISS}}^2}{\sigma_{x-\mathrm{CAISS}}}. \tag{58}$$

The parameters $\sigma_{x-\mathrm{ISS}}^2$ and $\sigma_{x-\mathrm{CAISS}}^2$ are the corresponding variances of the host signal in the ISS and CAISS schemes, with the error probability and the distortion being assumed the same in both embedding schemes. It could be shown that, referring to the error probabilities in (51) for CAISS and in (85) for ISS, and assuming equal error probability, we further have the expression

(59), shown at the bottom of the page, where σ^2 has been used to denote $\sigma^2_{x-\mathrm{CAISS}}$ for notation simplicity.

Proof: The proof details are given in the Appendix. □

Based on Proposition 4, it is straightforward to show that, with the assumption of i.i.d. Gaussian host signal samples, $\mathrm{IRIF}_{\mathrm{CAISS-SS}}$ is less than one where

$$\mathrm{IRIF}_{\mathrm{CAISS-SS}} = \frac{\sigma^2_{x-SS}}{\sigma^2_{x-\mathrm{CAISS}}}. \tag{60}$$

The parameter $\sigma^2_{x-\mathrm{SS}}$ and $\sigma^2_{x-\mathrm{CAISS}}$ are the variances of the host signal in the SS and CAISS schemes, respectively, with the error probability and the distortion being assumed the same. Using (59) leads us to the following expression:

$$\mathrm{IRIF}_{\mathrm{CAISS-SS}} = \frac{D(1-\lambda_h N)^2}{2D - A_1^2 - \lambda_h^2 N\sigma^2} \tag{61}$$

where we use σ^2 to denote $\sigma^2_{x-\mathrm{CAISS}}$.

We further prove that the CAISS scheme can increase the payload in data hiding in comparison with both SS and ISS schemes. Referring to the error probabilities in (19) and (51) and the PIF definition in (41), we can show that

$$\mathrm{PIF}_{\mathrm{CAISS-SS}} = \frac{2D - A_1^2 - \lambda_h^2 N\sigma_x^2}{D(1-\lambda_h N)^2} \tag{62}$$

where for notation simplicity we use N to denote N_{CAISS}. Since the PIF in (62) is the inverse of the IRIF for the CAISS and SS scheme, it is larger than one, meaning that the CAISS scheme increases the payload in data hiding.

The proof of the superiority of the CAISS scheme over ISS in terms of payload is not as easy as the case of SS. We provide the following proposition, with the proof details given in the Appendix.

Proposition 5: With the assumption of Gaussian i.i.d. host signal samples, for a given error probability and embedding distortion, the PIF for the CAISS and the ISS schemes is larger than one, i.e., $\mathrm{PIF}_{\mathrm{CAISS-ISS}} > 1$, where by using (28) we have

$$\mathrm{PIF}_{\mathrm{CAISS-ISS}} = 2 - \eta. \tag{63}$$

In summary, we have shown that the proposed correlation-and-bit-aware concept could improve the performance of the conventional SS and ISS schemes from several aspects: given a fixed embedding distortion, CASS and CAISS yield better decoding performances; for a fixed error probability, CASS and CAISS are more robust against the interference effect of the host signal; and they can increase the payload of data hiding.

V. CASS and CAISS in the Presence of Additional Noise

In Sections III and IV, the concept of correlation-and-bit-aware data hiding was introduced and two versions of correlation-aware embedding schemes, called the CASS and CAISS schemes, were presented. We so far have proved the superiority of CASS and CAISS over the SS and ISS schemes in the absence of additional noise. In practice, the received watermarked-signal might be contaminated with additional noise and thus its effects on the proposed correlation-aware data hiding schemes should be investigated. Therefore, in this section, we first show that the optimal decoder for both CASS and CAISS in the presence of additional Gaussian noise is still in the form of the correlator defined in (3) and (4). Then, the decoding performances of the proposed CASS and CAISS schemes in the presence of additional Gaussian noise are analyzed.

Since CASS can be considered as a particular case of CAISS with $\lambda_h = 0$, we only need to prove the optimality of the correlator decoder for CAISS. The optimality of the correlator for CASS could be simply shown by assuming $\lambda_h = 0$ in CAISS.

With additional Gaussian noise, the received noisy signal in the CAISS scheme could be described as

$$\mathbf{r} = \begin{cases} \mathbf{x} + \mathbf{s}A_1 + \mathbf{n}, & \text{if } \mathbf{s}^T\mathbf{x} \geq 0,\ b = +1 \\ \mathbf{x} - \mathbf{s}A_2 - \lambda_h \mathbf{s}(\mathbf{s}^T\mathbf{x}) + \mathbf{n}, & \text{if } \mathbf{s}^T\mathbf{x} \geq 0,\ b = -1 \\ \mathbf{x} - \mathbf{s}A_1 + \mathbf{n}, & \text{if } \mathbf{s}^T\mathbf{x} < 0,\ b = -1 \\ \mathbf{x} + \mathbf{s}A_2 - \lambda_h \mathbf{s}(\mathbf{s}^T\mathbf{x}) + \mathbf{n}, & \text{if } \mathbf{s}^T\mathbf{x} < 0,\ b = +1 \end{cases} \tag{64}$$

where $\mathbf{n} = [n_1, n_2, \ldots, n_N]^T$ includes the i.i.d. Gaussian noise samples with zero-mean and variance of σ_n^2. We can show that the pdf of the received signal model in (70) has the following form:

$$\begin{aligned} f_{\mathbf{R}}&\left(\mathbf{r} \,|\, b = +1, A_1, A_2, \sigma_n^2, \mathbf{s}\right) \\ &= \frac{1}{2\left(\sqrt{2\pi\sigma_x^2}\right)^N} \exp\left\{\frac{-1}{2\sigma_x^2}(\mathbf{r} - \mathbf{s}A_1)^T(\mathbf{r} - \mathbf{s}A_1)\right\} \\ &\quad + \frac{1}{2\sqrt{(2\pi\sigma_x^2)^N\,|\mathbf{C}_y|}} \\ &\quad \times \exp\left\{\frac{-1}{2}(\mathbf{r} - \mathbf{s}A_2)^T\mathbf{C}_y^{-1}(\mathbf{r} - \mathbf{s}A_2)\right\} \end{aligned} \tag{65}$$

$$\begin{aligned} f_{\mathbf{R}}&(\mathbf{r} \,|\, b = -1, A_1, A_2, \sigma_n^2, \mathbf{s}) \\ &= \frac{1}{2\left(\sqrt{2\pi\sigma_x^2}\right)^N} \exp\left\{\frac{-1}{2\sigma_x^2}(\mathbf{r} + \mathbf{s}A_1)^T(\mathbf{r} + \mathbf{s}A_1)\right\} \\ &\quad + \frac{1}{2\sqrt{(2\pi\sigma_x^2)^N\,|\mathbf{C}_y|}} \\ &\quad \times \exp\left\{\frac{-1}{2}(\mathbf{r} + \mathbf{s}A_2)^T\mathbf{C}_y^{-1}(\mathbf{r} + \mathbf{s}A_2)\right\} \end{aligned} \tag{66}$$

where

$$\mathbf{C}_y = \sigma_n^2\mathbf{I}_N + \mathbf{M}^2\sigma_x^2. \tag{67}$$

By plugging (65) and (66) into (36), we can show that the optimal decoder decides $\hat{b} = +1$ if $\mathbf{r}^T\mathbf{C}_y^{-1}\mathbf{s} > 0$. Referring to (67) and Woodbury equation, the aforementioned decision expression changes to $(\mathbf{r}^T\mathbf{s})/((\lambda_h N - 1)^2 + \sigma_x^{-2}\sigma_n^2) > 0$. Since

$$\mathrm{IRIF}_{\mathrm{CAISS-ISS}} = \frac{D(1-\lambda_h N)^2}{2D(1-\lambda N)^2 - A_1^2(1-\lambda N)^2 - \lambda_h^2 N\sigma^2(1-\lambda N)^2 + \lambda^2 N\sigma^2(1-\lambda_h N)^2} \tag{59}$$

the denominator is positive, the decision rule becomes the correlator defined in (4).

Having obtained the correlator as the optimal decoder, we proceed to analyze the error probability of the CAISS and CASS schemes in the presence of the noise. The probability of error for the CAISS scheme is first derived, and the corresponding error probability for the CASS embedding scheme can be obtained by substituting $\lambda_h = 0$ in the analysis.

Applying the correlator for the received signal of the CAISS embedding scheme (70) leads the test statistic z (4) be expressed in the following form:

$$z = \begin{cases} \mathbf{s}^T\mathbf{x} + NA_1 + \mathbf{s}^T\mathbf{n}, & \text{if } \mathbf{s}^T\mathbf{x} \geq 0,\ b = +1 \\ \mathbf{s}^T\mathbf{x}(1-\lambda_h N) - NA_2 + \mathbf{s}^T\mathbf{n}, & \text{if } \mathbf{s}^T\mathbf{x} \geq 0, b = -1 \\ \mathbf{s}^T\mathbf{x} - NA_1 + \mathbf{s}^T\mathbf{n}, & \text{if } \mathbf{s}^T\mathbf{x} < 0,\ b = -1 \\ \mathbf{s}^T\mathbf{x}(1-\lambda_h N) + NA_2 + \mathbf{s}^T\mathbf{n}, & \text{if } \mathbf{s}^T\mathbf{x} < 0,\ b = +1. \end{cases} \tag{68}$$

Since the test statistic in (68) is a sum of one Gaussian random variable and one random variable with half-Gaussian distribution, it is non-Gaussian distributed. This is the distinct point making the analysis of the CAISS scheme in the presence of additional noise different from the noise-free scenario in Sections III and IV. We first derive the pdf for the case that $\mathbf{s}^T\mathbf{x} \geq 0, b = +1$. Similarly, the pdf for other cases can be derived. We let $v = w + x$ where $x = \mathbf{s}^T\mathbf{n}$ and $w = \mathbf{s}^T\mathbf{x}, w > 0$. It can be shown that the distribution of v could be described in the form

$$\begin{aligned} f_V(v) &= B_1 + B_2 \\ &= \int_0^{\infty} (2\pi N\sigma_n^2)^{\frac{-1}{2}} \\ &\quad \times \exp\left\{\frac{-(v-y)^2}{2N\sigma_n^2}\right\} (2\pi N\sigma_x^2)^{\frac{-1}{2}} \\ &\quad \times \exp\left\{\frac{-y^2}{2N\sigma_x^2}\right\} dy + \int_{-\infty}^{0} (2\pi N\sigma_n^2)^{\frac{-1}{2}} \\ &\quad \times \exp\left\{\frac{-(v+y)^2}{2N\sigma_n^2}\right\} (2\pi N\sigma_x^2)^{\frac{-1}{2}} \\ &\quad \times \exp\left\{\frac{-y^2}{2N\sigma_x^2}\right\} dy. \end{aligned} \tag{69}$$

Because of the symmetric characteristics of the integrals B_1 and B_2, we have $B_1 = B_2$. We can show that B_2 has the following form:

$$\begin{aligned} B_2 = \left(4\pi^2 N^2\sigma_n^2\sigma_x^2\right)^{\frac{-1}{2}} \exp\left\{\frac{-v^2}{2N\left(\sigma_n^2+\sigma_x^2\right)}\right\} \\ \times \int_{-\infty}^{\frac{v\sigma_x^2}{\sigma_n^2+\sigma_x^2}} \exp\left\{\frac{-\left(\sigma_n^2+\sigma_x^2\right)t^2}{2N\sigma_n^2\sigma_x^2}\right\} dt. \end{aligned} \tag{70}$$

Using the definition of Q function and combining (69) and (70), we have the distribution of v as

$$\begin{aligned} f_V(v) = \frac{2}{\sqrt{2\pi N\left(\sigma_n^2+\sigma_x^2\right)}} \exp\left\{\frac{-v^2}{2N\left(\sigma_n^2+\sigma_x^2\right)}\right\} \\ \times \left[1 - Q\left(\frac{v\sigma_x}{\sigma_n\sqrt{N\left(\sigma_n^2+\sigma_x^2\right)}}\right)\right]. \end{aligned} \tag{71}$$

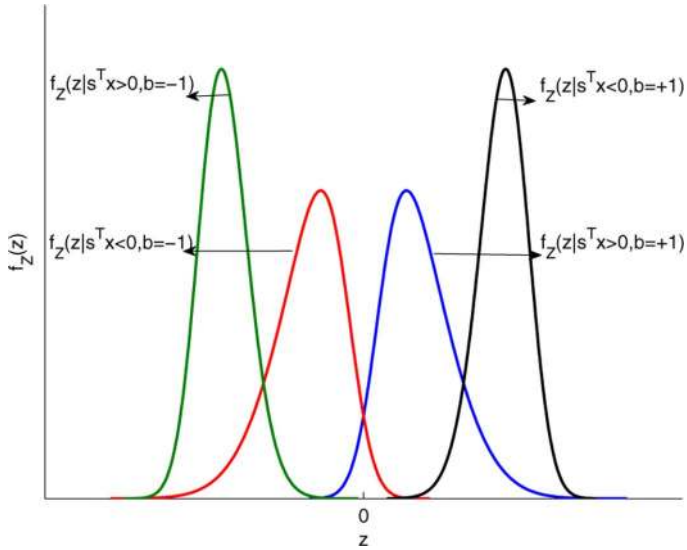

Fig. 4. With additional noise: Illustration of the pdfs in (72), (75), (73), and (74) of the test statistic z in (68) for the CAISS scheme.

Therefore, regarding the test statistic (70) and above expression, we have

$$\begin{aligned} f_Z(z \,|\, \mathbf{s}^T\mathbf{x} \geq 0, b = +1) = \frac{2}{\sqrt{2\pi N\left(\sigma_n^2+\sigma_x^2\right)}} \\ \times \exp\left\{\frac{-(z-NA_1)^2}{2N\left(\sigma_n^2+\sigma_x^2\right)}\right\} \left[1 - Q\left(\frac{(z-NA_1)\sigma_x}{\sigma_n\sqrt{N\left(\sigma_n^2+\sigma_x^2\right)}}\right)\right]. \end{aligned} \tag{72}$$

Applying a similar derivation to (71) and regarding the test statistic (70), the following distributions are obtained:

$$\begin{aligned} f_Z(z \,|\, \mathbf{s}^T\mathbf{x} < 0, b = +1) \\ = \frac{2}{\sqrt{2\pi N\left(\sigma_n^2+\sigma_x^2(1-\lambda_h N)^2\right)}} \\ \times \exp\left\{\frac{-(z-NA_2)^2}{2N\left(\sigma_n^2+\sigma_x^2(1-\lambda_h N)^2\right)}\right\} \\ \times Q\left(\frac{(z-NA_2)\sigma_x(1-\lambda_h N)}{\sigma_n\sqrt{N\left(\sigma_n^2+\sigma_x^2(1-\lambda_h N)^2\right)}}\right) \end{aligned} \tag{73}$$

$$\begin{aligned} f_Z(z \,|\, \mathbf{s}^T\mathbf{x} \geq 0, b = -1) \\ = \frac{2}{\sqrt{2\pi N\left(\sigma_n^2+\sigma_x^2(1-\lambda_h N)^2\right)}} \\ \times \exp\left\{\frac{-(z+NA_2)^2}{2N\left(\sigma_n^2+\sigma_x^2(1-\lambda_h N)^2\right)}\right\} \\ \times \left[1 - Q\left(\frac{(z+NA_2)\sigma_x(1-\lambda_h N)}{\sigma_n\sqrt{N\left(\sigma_n^2+\sigma_x^2(1-\lambda_h N)^2\right)}}\right)\right] \end{aligned} \tag{74}$$

$$\begin{aligned} f_Z(z \,|\, \mathbf{s}^T\mathbf{x} < 0, b = -1) \\ = \frac{2}{\sqrt{2\pi N\left(\sigma_n^2+\sigma_x^2\right)}} \\ \times \exp\left\{\frac{-(z+NA_1)^2}{2N\left(\sigma_n^2+\sigma_x^2\right)}\right\} Q\left(\frac{(z+NA_1)\sigma_x}{\sigma_n\sqrt{N\left(\sigma_n^2+\sigma_x^2\right)}}\right). \end{aligned} \tag{75}$$

Fig. 4 shows the above distributions of z and it is observed from it that in the presence of additional noise, pdf leakage exists even for the cases that $f_Z(z \,|\, \mathbf{s}^T\mathbf{x} \geq 0, b = +1)$ and that

$f_Z(z \mid \mathbf{s}^T\mathbf{x} < 0, b = -1)$, and thus apparently more bit decoding errors will be expected. It is due to the fact that the additional Gaussian noise makes the distribution interfere.

Referring to the distributions in (72)–(75) and the probability of error expressed in (14), we can calculate the bit error probability of CAISS in the presence of additional Gaussian noise as it is provided

$$\begin{aligned} P_{e-\mathrm{CAISS}} &= \int_{-\infty}^{-NA_1} \frac{1}{\sqrt{2\pi N\left(\sigma_n^2+\sigma_x^2\right)}} \\ &\quad \times \exp\left\{\frac{-z^2}{2N\left(\sigma_n^2+\sigma_x^2\right)}\right\} \\ &\quad \times \left[1-Q\left(\frac{z\sigma_x}{\sigma_n\sqrt{N\left(\sigma_n^2+\sigma_x^2\right)}}\right)\right] dz \\ &\quad + \int_{NA_2}^{\infty} \frac{1}{\sqrt{2\pi N\left(\sigma_n^2+\sigma_x^2(1-\lambda_h N)^2\right)}} \\ &\quad \times \exp\left\{\frac{-z^2}{2N\left(\sigma_n^2+\sigma_x^2(1-\lambda_h N)^2\right)}\right\} \\ &\quad \times \left[1-Q\left(\frac{z\sigma_x(1-\lambda_h N)}{\sigma_n\sqrt{N\left(\sigma_n^2+\sigma_x^2(1-\lambda_h N)^2\right)}}\right)\right] dz. \end{aligned} \tag{76}$$

It should be noted that the second and the fourth terms of (14) are no longer zero and thus also contribute to decoding errors, therefore, the error probability could be rewritten in the form of (77), shown at the bottom of the page.

It is worth mentioning that the error probability in (77) does not have a closed form expression and should be calculated numerically. To simplify the calculation, an approximation for Q function can be used. Using the approximation in [25], we have the error probability in the form of (78), shown at the bottom of the page, where $c_n = ((-1)^{n+1}(1.98)^n)/(1.135\sqrt{\pi}(\sqrt{2})^{n+1}n!)$.

The parameter n_a in (78) determines the approximation accuracy, i.e., a higher value of n_a means a more accurate approximation of Q function. Without loss of generality, n_a is assumed to be odd and consequently the error probability in (78) has the following closed form expression:

$$\begin{aligned} P_{e-\mathrm{CAISS}} \approx\ & P_1\left(A_1,\sigma_x^2\right) - P_1\left(A_2,\sigma_x^2(1-\lambda_h N)^2\right) \\ & + P_2\left(\sigma_x^2(1-\lambda_h N)^2\right) + P_3\left(n-1,2,A_1,\sigma_x^2\right) \\ & - P_3\left(2,1,A_2,\sigma_x^2(1-\lambda_h N)^2\right) \end{aligned} \tag{79}$$

where

$$\begin{aligned} P_1(A_i,\sigma^2) &= \sqrt{\frac{\sigma_n^2}{\sigma_n^2+\sigma^2}}\, Q\left(\frac{NA_i}{\sqrt{N\sigma_n^2}}\right) c_1 \\ &\quad + \frac{N\sigma_n^2 c_2}{\sqrt{2\pi N\left(\sigma_n^2+\sigma^2\right)}} \exp\left\{\frac{-NA_i^2}{2\sigma_n^2}\right\} \end{aligned} \tag{80}$$

$$P_2(\sigma^2) = Q\left(\frac{NA_2}{\sqrt{N\left(\sigma_n^2+\sigma^2\right)}}\right) \tag{81}$$

and $P_3(k_1,k_2,A_i,\sigma^2)$ is obtained using the expression (82), shown at the bottom of the next page.

In practice, one issue is to determine the parameters A_1 and λ_h in the presence of additional noise. Due to the complex expression of the error probability in (79) for CAISS, finding a closed form solution of the parameters is not feasible and a numerical approach should be employed. The parameters A_1

$$\begin{aligned} P_{e-\mathrm{CAISS}} =& Q\left(\frac{NA_2}{\sqrt{N\left(\sigma_x^2(1-\lambda_h N)^2+\sigma_n^2\right)}}\right) - \int_{-\infty}^{-NA_1} \frac{1}{\sqrt{2\pi N\left(\sigma_n^2+\sigma_x^2\right)}} \exp\left\{\frac{-z^2}{2N\left(\sigma_n^2+\sigma_x^2\right)}\right\} Q\left(\frac{z\sigma_x}{\sigma_n\sqrt{N\left(\sigma_n^2+\sigma_x^2\right)}}\right) dz \\ &+ Q\left(\frac{NA_1}{\sqrt{N\left(\sigma_x^2+\sigma_n^2\right)}}\right) - \int_{NA_2}^{\infty} \frac{1}{\sqrt{2\pi N(\sigma_n^2+\sigma_x^2(1-\lambda_h N)^2)}} \\ &\times \exp\left\{\frac{-z^2}{2N\left(\sigma_n^2+\sigma_x^2(1-\lambda_h N)^2\right)}\right\} Q\left(\frac{z\sigma_x(1-\lambda_h N)}{\sigma_n\sqrt{N\left(\sigma_n^2+\sigma_x^2(1-\lambda_h N)^2\right)}}\right) dz \end{aligned} \tag{77}$$

$$\begin{aligned} P_{e-\mathrm{CAISS}} \approx& Q\left(\frac{NA_1}{\sqrt{N\left(\sigma_x^2+\sigma_n^2\right)}}\right) + Q\left(\frac{NA_2}{\sqrt{N\left(\sigma_x^2(1-\lambda_h N)^2+\sigma_n^2\right)}}\right) - \int_{-\infty}^{-NA_1} \frac{1}{\sqrt{2\pi N\left(\sigma_n^2+\sigma_x^2\right)}} \exp\left\{\frac{-z^2}{2N(\sigma_n^2+\sigma_x^2)}\right\} \\ &\times \left[1-\exp\left\{\frac{-z^2\sigma_x^2}{2\sigma_n^2 N\left(\sigma_n^2+\sigma_x^2\right)}\right\} \sum_{n=1}^{n_a} c_n(-1)^{n-1} \left(\frac{\sigma_x}{\sigma_n\sqrt{N(\sigma_n^2+\sigma_x^2)}}\right)^{n-1} z^{n-1}\right] dz - \int_{NA_2}^{\infty} \frac{1}{\sqrt{2\pi N\left(\sigma_n^2+\sigma_x^2(1-\lambda_h N)^2\right)}} \\ &\times \exp\left\{\frac{-z^2}{2N\left(\sigma_n^2+\sigma_x^2(1-\lambda_h N)^2\right)}\right\} \exp\left\{\frac{-z^2\sigma_x^2(1-\lambda_h N)^2}{2\sigma_n^2 N\left(\sigma_n^2+\sigma_x^2(1-\lambda_h N)^2\right)}\right\} \sum_{n=1}^{n_a} c_n \left(\frac{\sigma_x(1-\lambda_h N)}{\sigma_n\sqrt{N\left(\sigma_n^2+\sigma_x^2(1-\lambda_h N)^2\right)}}\right)^{n-1} z^{n-1} dz \end{aligned} \tag{78}$$

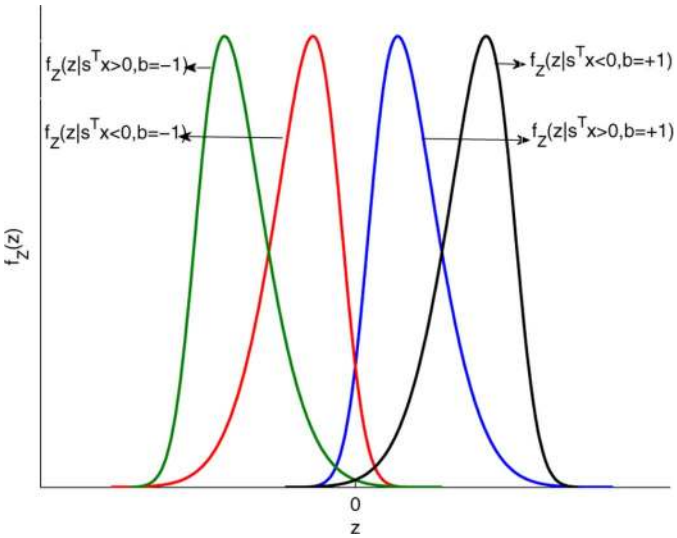

Fig. 5. With additional noise: Illustration of the pdfs in (72)–(75) of the test statistic z in (68) when $\lambda_h = 0$ for the CASS scheme.

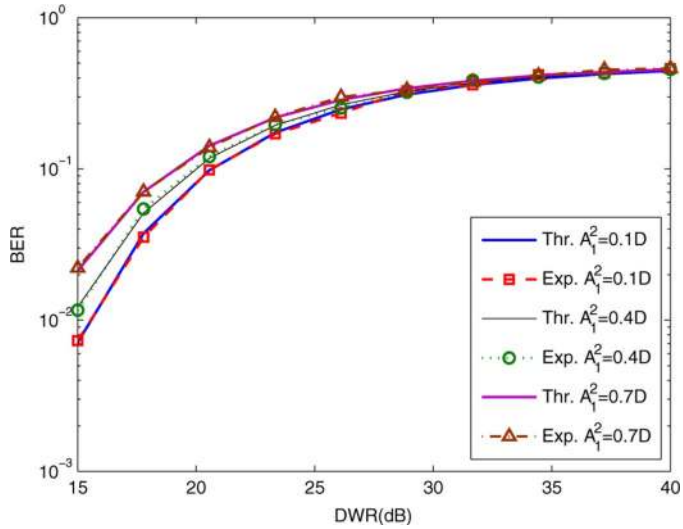

Fig. 6. Theoretical and experimental error probabilities versus DWR for the CASS scheme with different A_1^2.

and λ_h could be obtained by solving the following constrained two-dimensional minimization problem:

$$(A_1, \lambda_h) = \underset{0<\bar{A}_1<\sqrt{D}, \bar{\lambda}_h \le \sqrt{\frac{2D-\bar{A}_1^2}{N\sigma_x^2}}}{\operatorname{argmin}} P_{e-\mathrm{CAISS}}(\bar{A}_1, \bar{\lambda}_h). \quad (83)$$

We can employ standard numerical methods to solve the above minimization problem and obtain the desired parameters. With $\lambda_h = 0$, referring to the error probability for the CAISS scheme, we could obtain the corresponding error probability for the CASS scheme as follows:

$$P_{e-\mathrm{CASS}} \approx P_1\left(A_1, \sigma_x^2\right) - P_1\left(A_2, \sigma_x^2\right) + P_2\left(\sigma_x^2\right) + P_3\left(n-1, 2, A_1, \sigma_x^2\right) - P_3\left(2, 1, A_2, \sigma_x^2\right). \quad (84)$$

Fig. 5 depicts the distribution of the test statistic for the CASS scheme. It is clear that CASS leads to more pdf leakage when compared with CAISS in Fig. 4.

VI. Simulation Results

In this section, we conduct extensive simulations to verify the analysis results derived for the proposed CASS and CAISS schemes. The simulation results have been obtained by employing the Monte Carlo simulations using $N = 100$ unless stated otherwise. For the noiseless cases, the value of the parameter λ_h is determined for each DWR based on the expressions in (52), and for the additional Gaussian noise cases, λ_h is obtained by numerically solving the minimization problem in (83).

To show the preciseness of the obtained error probability for the CASS scheme in (17), both the theoretical and simulation results versus DWR are shown in Fig. 6, where different values of the amplitude A_1 are investigated. From this figure, excellent matches between the theoretical and simulation results are observed. It also reveals that a smaller value of the amplitude A_1 yields a better decoding performance. In the absence of any additional noise, given a fixed embedding distortion, a smaller value of A_1 would save embedding distortion and thus lead to a larger value of A_2. Since for the noise-free case the pdfs relating to A_1 have no leakage, intuitively a larger value of A_2 makes the pdfs leading to leakage be further apart from each other and thus reduces the decoding error.

Fig. 7 illustrates the theoretical (51) and experimental error probabilities for the CAISS scheme. Almost perfect match between the results is observed, which verifies the correctness of the theoretical derivations. Similar to the CASS case, due to

$$P_3(k_1, k_2, A_i, \sigma^2) = \frac{1}{\sqrt{2\pi}} \sum_{n\in\{3,5,\ldots,n_a-1\}} c_n(-1)^{k_1}\left[N(\sigma^2+\sigma_n^2)\right]^{\frac{-n}{2}} \times \left[\sum_{r=1}^{\frac{n-3}{2}}\left[(NA_i)^{2r-1}(N\sigma_n^2)^{\frac{n+1}{2}-r}\exp\left\{\frac{-NA_i^2}{2\sigma_n^2}\right\}\prod_{t=0}^{\frac{n-1}{2}-r}(n-2-2t)\right] + \sqrt{2\pi}\left(N\sigma_n^2\right)^{\frac{n}{2}} Q\left(\frac{NA_i}{\sqrt{N\sigma_n^2}}\right) \times \prod_{t=0}^{\frac{n-3}{2}}(n-2-2t) + (NA_i)^{n-2}\left(N\sigma_n^2\right) \times \exp\left\{\frac{-NA_i^2}{2\sigma_n^2}\right\}\right] - \frac{(-1)^{k_2}}{\sqrt{2\pi}}\left(N\sigma_n^2\right)\exp\left\{\frac{-NA_i^2}{2\sigma_n^2}\right\} \times \sum_{n\in\{4,6,\ldots,n_a\}} c_n(-1)^{k_1}\left[N\left(\sigma^2+\sigma_n^2\right)\right]^{\frac{-n}{2}}\left[\sum_{r=1}^{\frac{n-2}{2}}\left[(NA_i)^{2r-2}\left(N\sigma_n^2\right)^{\frac{n}{2}-r}\prod_{t=0}^{\frac{n-2}{2}-r}(n-2-2t)\right] + (NA_i)^{n-2}\right] \quad (82)$$

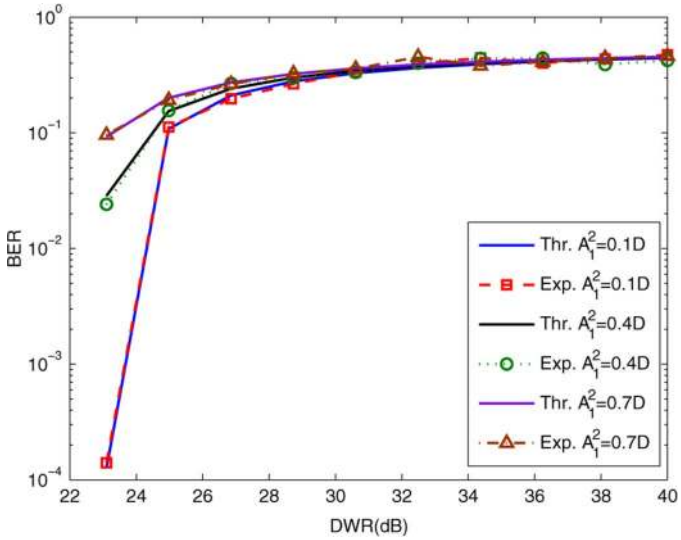

Fig. 7. Theoretical and experimental error probabilities versus DWR for the CAISS scheme with different A_1^2.

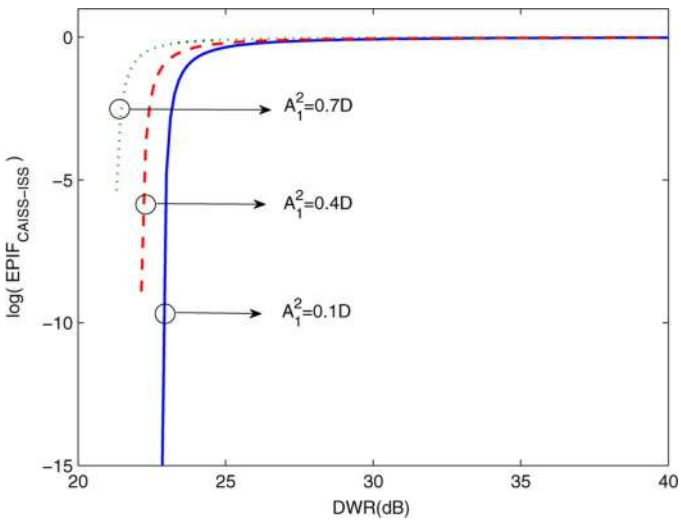

Fig. 8. Logarithm of EPIF versus DWR curves for evaluating of decoding performance improvements of the proposed CAISS over the ISS scheme.

the reasoning that $A_1 = 0$ would save embedding distortion without sacrificing error probability in the absence of noise, we can see that a smaller A_1 yields better decoding error probability in CAISS. We also evaluate the decoding improvement of CAISS using the EPIF measure in (56). Fig. 8 clearly shows a substantial decoding performance improvement of the CAISS data hiding scheme over ISS. Though not reported specifically, we would like to mention that the proposed CAISS yields significant decoding performance improvement over the SS scheme as well. It is also noted from Fig. 8 that the EPIF has an asymptotic behavior for high DWR, which represents the low embedding distortion region. Basically, it means that when the embedding distortion is very small, CAISS and CASS yield similar decoding performances. Based on (53), it is noted that λ_h approaches zero for a small embedding distortion (i.e., for a high DWR), and a similar observation for λ is noted. Therefore, by taking this into consideration and referring to the expression in (56), we can show that in the asymptotic case (i.e., for high DWR), the EPIF of CAISS over ISS approaches

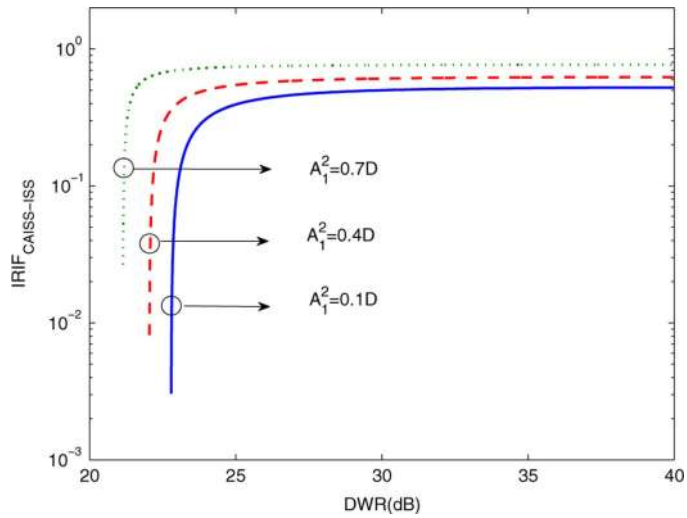

Fig. 9. IRIF versus DWR curves to illustrate the improvement of the proposed CAISS over ISS. Different A_1^2 values are illustrated.

$Q((N\sqrt{2D - A_1^2})/(\sqrt{N\sigma_x^2}))/Q((N\sqrt{D})/(\sqrt{N\sigma_x^2}))$ which is close to one for a small distortion. Thus, the observed asymptotic behavior is intuitively explained. It is also worth mentioning that, since both λ_h and λ approach zero in the asymptotic case, CAISS performs similarly as CASS and ISS performs similarly as SS asymptotically for a small embedding distortion.

The result of IRIF defined in (59) for comparing CAISS and ISS is shown in Fig. 9. It is clear that the CAISS scheme is more robust against the interference than the ISS scheme. Based on the expression of (59), it could be shown that the IRIF of CAISS and ISS asymptotically approaches $D/(2D - A_1^2)$ for the high DWR region. In Fig. 9, it is noted that a smaller value of A_1 leads to better robustness against the interference effect of the host signal. Once again, intuitively this is because that in the absence of noise, a smaller value of A_1 reduces the pdf leakage and thus allows the correlation-aware schemes to tolerate more host-interference effect for a fixed error probability and embedding distortion. Even though the result of IRIF for the CAISS and ISS scheme has been reported here, since the ISS scheme outperforms the SS scheme, we can easily show that the CAISS scheme enhances the robustness against the interference effect of the host signal when compared with SS. In addition, because of the inverse relationship between IRIF and PIF for the CAISS and SS schemes, it is clear that the proposed CAISS scheme improves the payload for data hiding.

To verify the derivation of the distributions of the test statistic z in the presence of additional Gaussian noise, Fig. 10 plots both the theoretical pdf in (72) and the experimental one. In this figure, we have used the notion watermark-to-noise ratio (WNR) defined as $\mathrm{WNR} = 10\log((D)/(\sigma_n^2))$, and have set $\mathrm{WNR} = 0$ dB. The simulation results in Fig. 10 demonstrate the accuracy of the theoretical derivation of the pdf and thus support the correctness of the derivation.

To verify the derived decoding performances for CASS (84) and CAISS (79) in the presence of additional Gaussian noise, the error probability versus DWR curves are plotted in Figs. 11 and 12, respectively, where $n_a = 30$ and different WNR are studied. The figures illustrate the consistence between the theoretical and

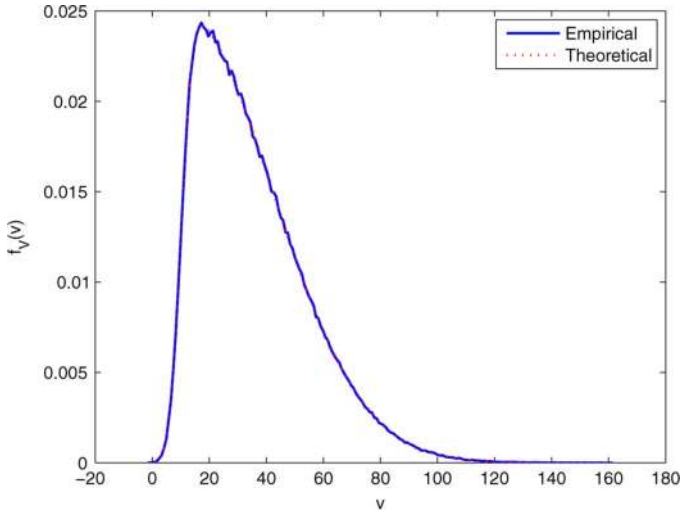

Fig. 10. Theoretical and experimental results of the pdf expressed in (72).

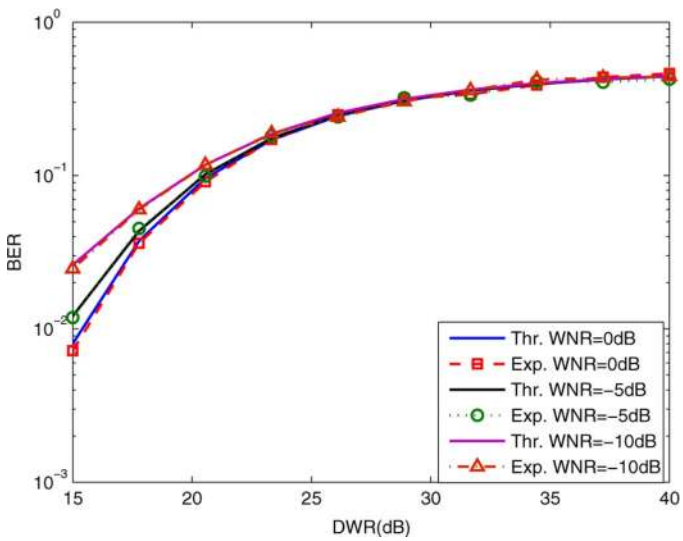

Fig. 11. Theoretical and experimental error probabilities versus DWR for the CASS scheme with different WNR.

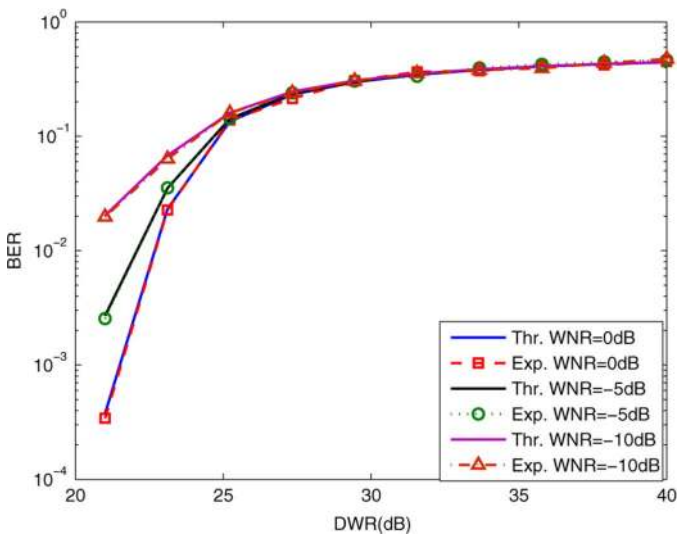

Fig. 12. Theoretical and experimental error probabilities versus DWR for the CAISS scheme with different WNR.

empirical results and prove the correctness of the theoretical analysis.

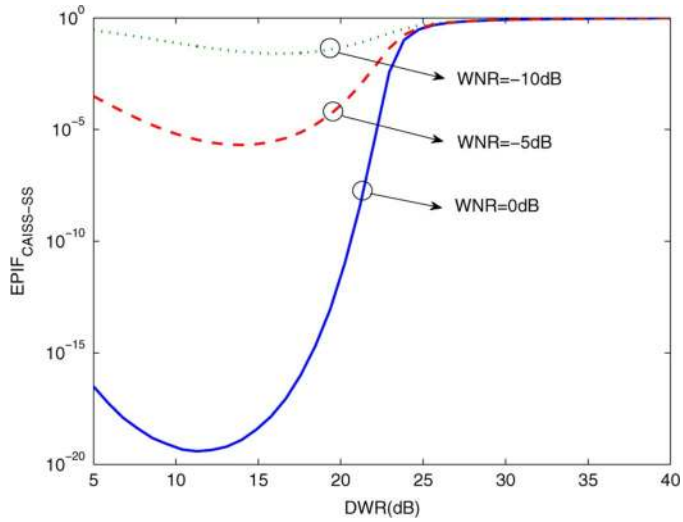

Fig. 13. EPIF versus DWR curves to demonstrate the improvement of the proposed CAISS over SS. Different WNR values are illustrated.

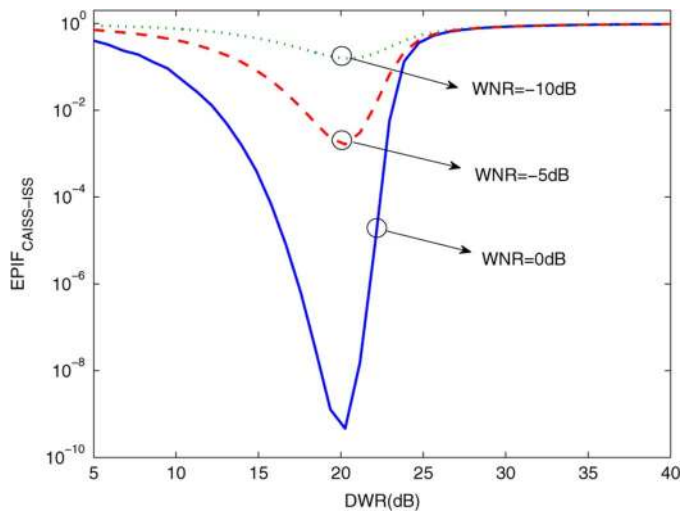

Fig. 14. EPIF versus DWR curves to demonstrate the improvement of the proposed CAISS over ISS. Different WNR values are illustrated.

To demonstrate the decoding performance improvements of CAISS over both SS and ISS even in the presence of additional Gaussian noise, the EPIF curves are shown in Figs. 13 and 14. We can see that the proposed CAISS scheme is still superior to the SS and ISS schemes. It is observed that the EPIF does not demonstrate a monotonic behavior in these figures: as the DWR decreases, the EPIF decreases first and then increases. For Fig. 13, we can show that the corresponding EPIF is a complicated function, where the error probability of the CAISS scheme is expressed in (79) and the error probability of SS can be derived as $Q(N\sqrt{D}/\sqrt{N(\sigma_x^2+\sigma_n^2)})$, and thus theoretical justification of this behavior is not easy. Numerically, we note that at the minimal point, the parameter λ_h tends to take the extreme value of $1/N$ in order to maximally reject the effect of the host signal. An intuitive explanation of the observed non-monotonic behavior is as follows. With additional Gaussian noise, there are two conflicting factors contributing to the overall decoding performance: the embedding distortion D and the additional noise with variance σ_n^2. A larger distortion, which means a higher watermark power, leads to a smaller decoding error rate, while a larger noise variance σ_n^2 results in more pdf leakage and

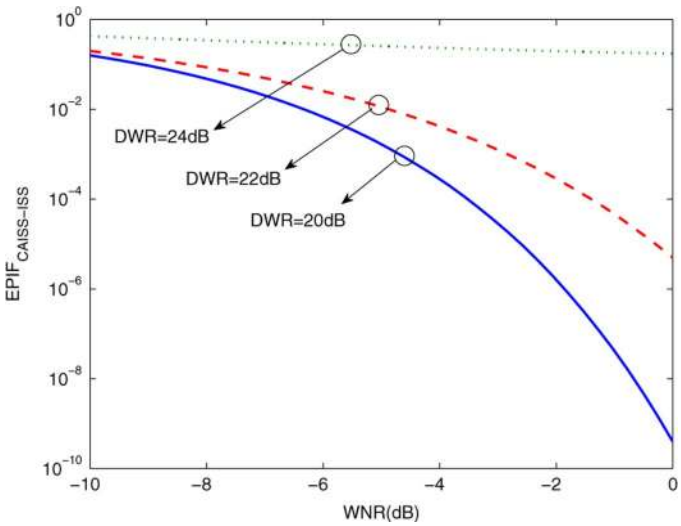

Fig. 15. EPIF versus WNR curves to demonstrate the improvement of the proposed CAISS over ISS. Different DWR values are illustrated.

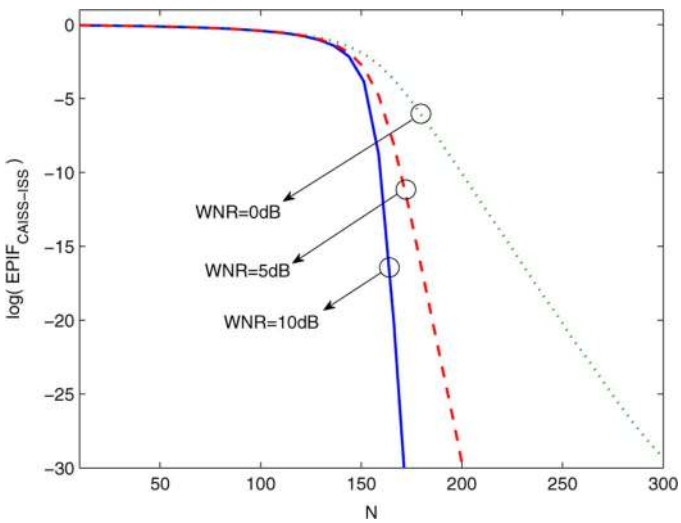

Fig. 16. Logarithm of EPIF versus N curves to demonstrate the improvement of the proposed CAISS over ISS where DWR $= 25$ dB. Different WNR values are illustrated.

thus increases the decoding error rate. Since for each curve in Fig. 13, we fix the WNR, D and σ_n^2 increase or decrease simultaneously. Given a WNR, as we first decrease the DWR (i.e., increasing D), the factor of D is dominant and thus the performance measure EPIF decreases (until the parameter λ_h approaches $1/N$); as we further decrease the DWR, λ_h does not change anymore, while the noise variance σ_n^2 is larger and causes more pdf leakage, and thus becomes the dominant factor and leads to the increased EPIF measure. The behavior in Fig. 14 can be similarly explained. We also want to mention that, to provide a good trade-off between decoding performance and imperceptibility in practical data hiding, the DWR cannot be too large and meanwhile it cannot be too small.

To study the performance of CAISS against WNR, three different values of DWR are studied in Fig. 15. It is noted that the CAISS scheme consistently yields better performance, even at a low WNR. Fig. 16 shows the logarithm of the EPIF measure as a function of the number of host coefficients when DWR $=$ 25 dB. We can see clear improvements of the CAISS scheme over ISS, especially when N, the number of the host coefficients, increases. We also note an asymptotic behavior of EPIF when N is small. At the extreme case when the number of the host coefficients is small, we note that both λ_h and λ numerically approach zero. To have a rough idea regarding the asymptotic behavior, we can simply consider the noise-less case (e.g., assuming a high WNR). Since both λ_h and λ tend to be zero, the EPIF of CAISS over ISS is reduced to the EPIF of CASS over SS as expressed in (23). Applying an approximation of the Q function, i.e., $Q(x) \approx 1/(x\sqrt{2\pi})\exp\{-x^2/2\}$, we can show that the EPIF expression in (23) can be approximated as $\sqrt{D/(2D-A_1^2)}\exp\{-N(D-A_1^2)/(2\sigma_x^2)\}$. For a small N, and considering the fact that DWR $= 25$ dB is used in Fig. 16, the exponential term in the above approximation tends to be 1, and the EPIF asymptotically approaches $\sqrt{D/(2D-A_1^2)}$. Thus, the observed asymptotic behavior can be explained.

VII. Conclusion

In this paper, the correlation-and-bit-aware concept for spread spectrum embedding has been introduced. We have shown that the proposed CASS and CAISS data hiding schemes can improve the performance of the traditional SS and ISS schemes by taking into consideration the correlation between the host signal and the key and the bit message to be embedded. Thorough theoretical analysis on decoding error probability has been provided to prove that the CASS scheme outperforms the SS scheme and that the CAISS scheme outperforms the ISS scheme. We have also proved the superior robustness of the proposed CASS and CAISS data hiding schemes against the interference effect of the host signal. Furthermore, our analysis shows that using the proposed correlation-and-bit-aware data hiding schemes could increase the payload. In addition, the theoretical BER performances of the proposed schemes in the presence of additional noise have been derived. Extensive simulation results confirm the theoretical analysis and demonstrate the superiority of the the proposed CAISS scheme over the traditional SS and ISS schemes.

Appendix

Proof of Proposition 3: To compare the proposed CAISS scheme with the ISS scheme, we recall that the error probability of the ISS [18] can be obtained as

$$P_{e-\mathrm{ISS}} = Q\left(\frac{N\sqrt{D-\lambda^2 N\sigma_x^2}}{\sqrt{N\sigma_x^2(1-\lambda N)^2}}\right) \tag{85}$$

where

$$\lambda = \begin{cases} \frac{1}{N}, & \text{if } D > \frac{\sigma_x^2}{N} \\ \frac{D}{\sigma_x^2}, & \text{if } D \le \frac{\sigma_x^2}{N}. \end{cases} \tag{86}$$

To prove that the proposed CAISS provides a better decoding performance, referring to the error probabilities in (51) and (85), we should prove that

$$\frac{D-\lambda^2 N\sigma_x^2}{(1-\lambda N)^2} \le \frac{2D-A_1^2-\lambda_h^2 N\sigma_x^2}{(1-\lambda_h N)^2}. \tag{87}$$

We can show that (87) can be equivalently expressed as $g \geq 0$ where

$$g = \lambda^2 \left(2DN^2 - A_1^2N^2 + N\sigma_x^2\right) - \lambda_h^2 \left(N\sigma_x^2 + DN^2\right) + \lambda \left(2A_1^2N - 4DN\right) + 2\lambda_h DN + 2\lambda\lambda_h N^2\sigma_x^2(\lambda_h - \lambda) + \left(D - A_1^2\right). \quad (88)$$

With λ_h in (52) and λ in (86), three cases may occur: the first one is when $D \leq (\sigma_x^2 + A_1^2N)/(2N)$; the second one is when $(\sigma_x^2 + A_1^2N)/(2N) < D \leq (\sigma_x^2)/(N)$; and the third one is when $D > (\sigma_x^2)/(N)$. We now prove the inequality in (87) for each of the three cases.

Case I: With $D \leq (\sigma_x^2 + A_1^2N)/(2N)$, referring to (52) and (86), we have $\lambda_h = (2D - A_1^2)/\sigma_x^2$ and $\lambda = D/\sigma_x^2$. So, we have $g = 2N^2(D - A_1^2)(D - (A_1^2N + \sigma_x^2)/(2N))(D - (\sigma_x^2)/(N))$. Based on the assumption that $D \leq (\sigma_x^2 + A_1^2N)/(2N)$ and the fact that $0 < A_1 < \sqrt{D}$, it could be concluded that $g \geq 0$ and thus the inequality in (87) holds for Case I.

Case II: With $(\sigma_x^2 + A_1^2N)/(2N) < D \leq (\sigma_x^2)/(N)$, referring to (52) and (86), we have $\lambda_h = 1/N$ and $\lambda = D/\sigma_x^2$. So, now g in (88) becomes $g = 2N^2(D - (\sigma_x^2 + A_1^2N)/(2N))(D - (\sigma_x^2)/(N))^2$. Based on the assumption on D in this case, we can see that $g \geq 0$ and thus the inequality (87) holds for Case II.

Case III: With $D > (\sigma_x^2)/(N)$, referring to (52) and (86), we have $\lambda_h = 1/N$ and $\lambda = 1/N$. It is straightforward to show that $g = 0$ for this case.

Based on the above three cases, we can conclude that $g \geq 0$ and thus the CAISS embedding scheme has better decoding performance than the ISS scheme. □

Proof of Proposition 4: To prove that $\mathrm{IRIF}_{\mathrm{CAISS-ISS}} < 1$, referring to (59), it is equivalently to show that $h \geq 0$ with

$$h = \lambda_h^2 \left(-DN^2 + 2\lambda N^2\sigma_x^2 - N\sigma_x^2\right) - \lambda_h \left(2N^2\lambda^2\sigma_x^2 + 2ND\right) + \lambda^2\sigma_x^2N + 2N^2D\lambda^2 - N^2A_1^2\lambda^2 + D - 4ND\lambda + 2NA_1^2\lambda + A_1^2. \quad (89)$$

We need to prove $h \geq 0$ for two cases as follows.

Case I: In this case, it is assumed that $D \leq (\sigma^2 + A_1^2N)/(2N)$ and thus $\lambda_h = (2D - A_1^2)/(\sigma^2)$. We now can write h as

$$h = -\left(D - \frac{\sigma^2 + A_1^2N}{2N}\right) g(A_1) \quad (90)$$

where

$$g(A_1) = A_1^2(4\lambda N^2\sigma^2 - 2DN^2 - 2N\sigma^2) + 2\lambda^2N^2\sigma^4 - 8DN^2\sigma^2\lambda + 4D^2N^2 + 2DN\sigma^2. \quad (91)$$

To prove $h \geq 0$, it is equivalent to prove that $g(A_1)$ is positive. From (91), it is noticed that $g(A_1)$ is a quadratic function in the form of $g(A_1) = aA_1^2 + c$. Therefore, to prove that $g(A_1)$ is positive, we need to show that both $g(0)$ and $g(\sqrt{D})$ are positive. For $A_1 = 0$, we can write $g(0) = f(\lambda) = 2\lambda^2N\sigma^4 - 8DN\sigma^2\lambda + 4D^2N + 2D\sigma^2$. Since $f(\lambda)$ is a quadratic convex function, to show that it is always positive, it is equivalent to prove that $f(\lambda)$ has no real root. Referring to $f(\lambda)$, we have $\Delta = (4DN\sigma^2)^2 - 4(N\sigma^4)(2D^2N + D\sigma^2) = 4DN\sigma^4(2DN - \sigma^2)$. Since it is assumed $D \leq (\sigma^2 + A_1^2N)/(2N)$ and $A_1 = 0$, we have $D < (\sigma^2)/(2N)$. Therefore, the discriminator Δ is negative and consequently $f(\lambda)$ and $g(0)$ are positive.

It is pretty straightforward to show that we have $g(\sqrt{D}) = 2(\lambda N\sigma^2 - DN)^2$, which is positive always. Therefore, we complete the proof that $h \geq 0$ for Case I.

Case II: $D > (\sigma^2 + A_1^2N)/(2N)$ is assumed for Case II and thus $\lambda_h = (1/N)$. Therefore, referring to (59), we have $h > 0$ where $h = (1 - \lambda N)^2(2D - A_1^2 - (\sigma^2)/(N))$. □

Proof of Proposition 5: Let us denote that $M = N_{\mathrm{ISS}}$ and $N = N_{\mathrm{CAISS}}$ for simplicity. Assuming an equal error probability for the CAISS and ISS schemes, referring to (51) and (85), we have

$$\frac{M\left(D - \lambda^2M\sigma_x^2\right)}{(1 - \lambda M)^2} = \frac{N\left(2D - A_1^2 - \lambda_h^2N\sigma_x^2\right)}{(1 - \lambda_h N)^2}. \quad (92)$$

The above expression can be rewritten as

$$M^2\left(-\lambda^2\sigma_x^2 + 2\lambda_h N\lambda^2\sigma_x^2 - 2ND\lambda^2 + NA_1^2\lambda^2\right) + M\left(D + D\lambda_h^2N^2 - 2\lambda_h ND + 4ND\lambda - 2NA_1^2\lambda - 2\lambda\lambda_h^2N^2\sigma_x^2\right) - 2ND + NA_1^2 + \lambda_h^2N^2\sigma_x^2 = 0. \quad (93)$$

Two cases are proved here to complete the Proof of Proposition 5.

Case I: $\lambda_h = (2D - A_1^2)/\sigma_x^2$ and $\lambda = D/\sigma_x^2$ are assumed for Case I. Based on these assumptions and (93), we can have PIF as in (63) and thus $\mathrm{PIF}_{\mathrm{CAISS-ISS}} > 1$.

Case II: We have $\lambda_h = 1/N$ for Case II. To have (93) still hold, λ should tend to be $1/M$. Referring to (52) and (86), it could be seen that we should have $M = (2 - \eta)N$ which implies the PIF expression as in (63). □

REFERENCES

[1] Q. Cheng and T. S. Huang, "Robust optimum detection of transform domain multiplicative watermarks," *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 906–924, Apr. 2003.

[2] W. Liu, L. Dong, and W. Zeng, "Optimum detection for spread-spectrum watermarking that employs self-masking," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 4, pp. 645–654, Dec. 2007.

[3] N. Merhav and E. Sabbag, "Optimal watermark embedding and detection strategies under limited detection resources," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 255–274, Jan. 2008.

[4] A. Briassouli, P. Tsakalides, and M. Strintzis, "Hidden messages in heavy-tails: DCT-Domain watermark detection using alpha-stable models," *IEEE Trans. Multimedia*, vol. 7, no. 4, pp. 700–715, Aug. 2005.

[5] F. Perez-Gonzalez, F. Balado, and J. R. H. Martin, "Performance analysis of existing and new methods for data hiding with known-host information in additive channels," *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 960–980, Apr. 2003.

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

[7] M. Barni, F. Bartolini, A. De Rosa, and A. Piva, "Optimum decoding and detection of multiplicative watermarks," *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 1118–1123, Apr. 2003.

[8] X. Huang and B. Zhang, "Statistically robust detection of multiplicative spread-spectrum watermarks," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 1, pp. 1–13, Mar. 2007.

[9] 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.

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

[11] J. J. Eggers, R. Bauml, R. Tzschoppe, and B. Girod, "Scalar costa scheme for information embedding," *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 1003–1019, Apr. 2003.
[12] F. Perez-Gonzales, C. Mosquera, M. Barni, and A. Abrardo, "Rational dither modulation: A high-rate data-hiding method invariant to gain attacks," *IEEE Trans. Signal Process.*, vol. 53, no. 10, pp. 3960–3975, Oct. 2005.
[13] A. Abrardo and M. Barni, "Informed watermarking by means of orthogonal and quasi-orthogonal dirty paper coding," *IEEE Trans. Signal Process.*, vol. 53, no. 2, pp. 824–833, Feb. 2005.
[14] Q. Cheng and T. S. Huang, "An additive approach to transform-domain information hiding and optimum detection structure," *IEEE Trans. Multimedia*, vol. 3, no. 3, pp. 273–284, Sep. 2001.
[15] A. K. Mairgiotis, N. P. Galatsanos, and Y. Yang, "New additive watermark detectors based on A hierarchical spatially adaptive image model," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 1, pp. 29–37, Mar. 2008.
[16] J. Cannons and P. Moulin, "Design and statistical analysis of a hash-aided image watermarking system," *IEEE Trans. Image Process.*, vol. 13, no. 10, pp. 1393–1408, Oct. 2004.
[17] A. Valizadeh and Z. J. Wang, "A framework of multiplicative spread spectrum embedding for data hiding: Performance, decoder and signature design," in *Proc. Global Commun. (GLOBECOM)*, Dec. 2009, pp. 1–6.
[18] H. S. Malvar and D. A. Florencio, "Improved spread spectrum: A new modulation technique for robust watermarking," *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 898–905, Apr. 2003.
[19] D. Kirovski and H. S. Malvar, "Spread spectrum watermarking of audio signals," *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 1020–1033, Apr. 2003.
[20] 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.
[21] Z. Li, Q. Sun, and Y. Lian, "Design and analysis of a scalable watermarking scheme for the scalable audio coder," *IEEE Trans. Signal Process.*, vol. 54, no. 8, pp. 3064–3077, Aug. 2006.
[22] U. Budhia, D. Kundar, and T. Zourntos, "Digital video steganalysis exploiting statistical visibility in the temporal domain," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 4, pp. 502–516, Dec. 2006.
[23] S. Biswas, S. R. Das, and E. M. Petriu, "An adaptive compressed MPEG-2 video watermarking scheme," *IEEE Trans. Instrum. Meas.*, vol. 54, no. 5, pp. 1853–1861, Oct. 2005.
[24] A. M. Alattar, E. T. Lin, and M. U. Celik, "Digital watermarking of low bit-rate advanced simple profile MPEG-4 compressed video," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 787–800, Aug. 2003.
[25] Y. Isukapalli and B. D. Rao, "An analytically tractable approximation for the gaussian q-function," *IEEE Trans. Commun. Lett.*, vol. 12, no. 9, pp. 669–671, Sep. 2008.

Amir Valizadeh (S'09) received the B.Sc. and M.Sc. degrees in electrical engineering from Shiraz University, Shiraz, Iran, in 2004 and 2007, respectively. Since 2008, he has been working toward the Ph.D. degree in electrical and computer engineering, University of British Columbia, Vancouver, BC, Canada.

His research interests are in the broad areas of statistical signal processing with focus on multimedia security and multimedia signal processing.

Mr. Valizadeh was a recipient of the University Graduate Fellowship (UGF) from the University of British Columbia in 2009.

Z. Jane Wang (S'01–M'02) received the B.Sc. degree from Tsinghua University, China, in 1996, with the highest honor, and the M.Sc. and Ph.D. degrees from the University of Connecticut in 2000 and 2002, respectively, all in electrical engineering.

She was Research Associate of the Electrical and Computer Engineering Department at the University of Maryland, College Park. Since Aug. 1, 2004, she has been with the Department Electrical and Computer Engineering at the University of British Columbia, Canada. Her research interests are in the broad areas of statistical signal processing theory and applications, with focus on information security and biomedical signal processing and modeling.

Dr. Wang coreceived the EURASIP Journal on Applied Signal Processing (JASP) Best Paper Award 2004, and the IEEE Signal Processing Society Best Paper Award 2005. She is serving as Associate Editor for several IEEE journals, and she is the Chair and founder of the IEEE Signal Processing Chapter at Vancouver.