IET Image Processing

Research Article

IET Journals
The Institution of Engineering and Technology

Amplitude-adaptive spread-spectrum data embedding

ISSN 1751-9659
Received on 17th February 2015
Revised on 7th August 2015
Accepted on 21st August 2015
doi: 10.1049/iet-ipr.2015.0128
www.ietdl.org

Ming Li[1] ✉, *Qian Liu*[2], *Yanqing Guo*[1], *Bo Wang*[1], *Xiangwei Kong*[1]

[1]*School of Information and Communication Engineering, Dalian University of Technology Dalian, Liaoning 116024, People's Republic of China*
[2]*Department of Computer Science and Engineering, University of New York at Buffalo, Buffalo, NY 14260, USA*
✉ *E-mail: mli@dlut.edu.cn*

Abstract: In this study, the authors consider additive spread-spectrum (SS) data embedding in transform-domain host data. Conventional additive SS embedding schemes use an equal-amplitude modulated carrier to deposit one information symbol across a group of host data coefficients which act as interference to SS signal of interest. If there is a flexibility of assigning different amplitudes across symbol bits, the probability of error can be further reduced by adaptively allocating amplitude to each symbol bit based on its own host/interference. In this study, they present a novel amplitude-adaptive SS embedding scheme. Particularly, symbol-by-symbol adaptive amplitude allocation algorithms are developed to compensate for the impact from the known interference. They aim at designing the SS embedding amplitude for each symbol adaptively in order to minimise the receiver bit-error-rate (BER) at any given distortion level. Then, optimised amplitude allocation for multi-carrier/multi-message embedding in the same host data is studied as well. Finally, they consider the problem of amplitude optimisation for an ideal scenario where no external noise is introduced during embedding and transmission. Extensive experimental results illustrate that the proposed amplitude-adaptive SS embedding scheme can provide order-of-magnitude performance improvement over several other state-of-the-art SS embedding schemes.

1 Introduction

The rapid advances in information and communication technologies allow people to easily transfer and exchange massive amounts of digital multimedia such as digital images, video, and audio. Consequently, it has become extremely important to ensure the security of the exchanged information. As a result, digital data embedding has raised extensive attention in recent years with the development of various security/privacy protection applications such as annotation, copyright marking, watermarking, ownership protection, authentication, digital fingerprint, and covert communications or steganography [1–8]. Different applications of data embedding require different satisfactory tradeoffs between the following four basic attributes [9]: payload, robustness, transparency, and security.

Determining the embedding process is the most important step in the design of a data embedding system for a particular application. Payload rate, distortion, data detector design, and recovery performance depend directly on how the data is inserted into the host. Data embedding can be performed in the original time or spatial domain [10–14]. While embedding directly in the original host signal domain may be desirable for system complexity purposes, embedding in a transform domain can take advantage of the particular transform-domain properties [15–23].

Spread-spectrum (SS) data embedding [24–33] is an important branch of transform-domain data embedding technologies and enjoys wide popularity in data hiding community. In SS embedding, the secret signal is spread over a wide range of host frequency coefficients. In direct analogy to SS digital communications systems, conventional additive SS embedding methods [24–30] use an equal-amplitude modulated carrier to deposit one information symbol across a group of host data coefficients or a linearly transformed version of the host data coefficients. While a constant embedding amplitude is used in the additive SS embedding, in the multiplicative SS embedding [31–33] the embedding amplitude is propositional to the value of the host signal. In both additive and multiplicative embedding algorithms, the host signal always behaves as a source of interference to the embedded data of interest. Nevertheless, it should also be aware that this interference is known to the embedder. Such knowledge can be exploited appropriately to facilitate the task of the receiver at the other end and minimise the recovery error rate for a given host distortion level.

Utilising the knowledge of the second-order statistics of host, the recently presented eigen-design optimal carrier [27] can maximise the signal-to-interference-noise ratio (SINR) at the output of the corresponding maximum-SINR linear filter. Since the impact of interference from the host signal is explicitly known to the embedders, the known interference can be further alleviated at embedder side with appropriate operation. If there is a flexibility of assigning different amplitudes across symbol bits, the probability of error can be further reduced by allocating amplitude to each symbol bit adaptively with its own host/interference.

The problem of designing different amplitudes for SS embedding to provide better recovery performance was first investigated in [30] where two levels of amplitude are designed by exploring the correlation between the host and the carrier as well as the information bit. This scheme is shown to provide better watermark decoding performance than the traditional SS schemes. However, the knowledge of the host signal is not fully exploited by using just two levels of embedding amplitude. Clearly, if each symbol bit is assigned any positive-valued amplitude, the performance of recovery can be further improved.

In this study, we present a novel amplitude-adaptive SS embedding scheme. Symbol-by-symbol adaptive amplitude allocation algorithms are developed to compensate for the impact from the known interference. We aim at designing the SS embedding amplitude for each symbol adaptively in order to minimise the receiver bit-error-rate (BER) at any given distortion level and to minimise – conversely – the distortion at any target

BER. We assign an embedding amplitude for each symbol (i.e. the message) adaptively based on the symbol value and its corresponding host vector. A computationally expensive Karush–Kuhn–Tucker (KKT)-conditions-based optimal amplitude allocation algorithm and two light-complexity waterfilling-based sub-optimal amplitude allocation algorithms are developed to adaptively assign amplitude to each symbol bit with any given total distortion budget. Extensive experimental results illustrate that the proposed amplitude-adaptive SS embedding approach can provide order-of-magnitude data recovery performance improvement over other state-of-the-art SS embedding schemes. Particularly, the proposed prioritised waterfilling-based embedding amplitude allocation can offer satisfactory recovery performance with all allowable distortion levels as well as has very low computational complexity. In addition, similar to the conventional SS schemes, the proposed amplitude-adaptive SS embedding scheme does not require any additional information at the data detector side and the simple data detector does not need to be modified.

Our effort is also extended to develop amplitude-adaptive multi-carrier (multi-message) SS embedding scheme. In practice, an embedder may favour multi-carrier SS transform-domain embedding to increase payload rate and/or to deliver distinct messages to different receipts. In this case, we aim to minimise average BER over all embedded messages at any given distortion level as well as guarantee the fairness of messages. Finally, we consider an ideal scenario where no external noise is introduced during embedding and transmission and the amplitude optimisation is investigated for this case.

The rest of this paper is organised as follows. In Section 2, the state-of-the-art SS embedding schemes are reviewed and summarised. Then, in Section 3 amplitude-adaptive SS embedding scheme is presented and three amplitude allocation algorithms are developed. In Section 4, the studies of adaptive amplitude allocation are extended to multi-carrier SS embedding scheme. In Section 5, amplitude allocation for SS embedding without external noise is investigated as an ideal scenario. Section 6 is devoted to experimental studies and comparisons. Finally, a few concluding remarks are drawn in Section 7.

The following notation is used throughout this paper. Boldface lower-case letters indicate column vectors and boldface upper-case letters indicate matrices; $\mathbb{R}$ denotes the set of all real numbers; $()^{\mathrm{T}}$ denotes matrix transpose; $\boldsymbol{I}_L$ is the $L \times L$ identity matrix; $\mathrm{sgn}\{\cdot\}$ denotes zero-threshold quantisation; $\mathbb{E}\{\cdot\}$ represents statistical expectation; $|\cdot|$ and $\|\cdot\|$ are the scalar magnitude and vector norm, respectively; and finally, $|\{\cdot\}|$ denotes the cardinality of a set.

2 Conventional SS embedding schemes

Consider a host image $\boldsymbol{H} \in \mathcal{M}^{N_1 \times N_2}$ where $\mathcal{M}$ is the finite image alphabet and $N_1 \times N_2$ is the image size in pixels. Without loss of generality, the image $\boldsymbol{H}$ is partitioned into M local non-overlapping blocks of size N_1N_2/M. Each block, $\boldsymbol{H}_1, \boldsymbol{H}_2, \ldots, \boldsymbol{H}_M$, is to carry one embedded information bit. Embedding is performed in a two-dimensional transform-domain $\mathcal{T}$ such as discrete cosine transform (DCT), discrete wavelet transform (DWT) etc. After transform calculation and vectorisation (for example, by conventional zig-zag scanning), we obtain $\mathcal{T}(\boldsymbol{H}_i) \in \mathbb{R}^{(N_1N_2/M)}$, $i = 1, 2, \ldots, M$. From the transform-domain vectors $\mathcal{T}(\boldsymbol{H}_i)$, we choose a fixed subset of $L \leq (N_1N_2/M)$ coefficients (bins) to form the final host vectors $\boldsymbol{x}_i \in \mathbb{R}^L$, $i = 1, 2, \ldots, M$. It is common and appropriate to avoid the dc coefficient (if applicable) due to high perceptual sensitivity in changes of the dc value.

To draw a parallelism with SS communications systems, conventional SS embedding treats embedded data as the SS signal of interest transmitted through a noisy 'channel' (the host). The disturbance to the SS signal of interest is the host data themselves plus potential external noise due to physical transmission of the watermarked data and/or processing/attacking. In particular, the classic transform-domain SS embedding is carried out by

$$\boldsymbol{y}_i = Ab_i\boldsymbol{s} + \boldsymbol{x}_i + \boldsymbol{n}, \quad i = 1, \ldots, M, \tag{1}$$

where information bit $b_i \in \{\pm 1\}$ is embedded in the transform-domain host vector $\boldsymbol{x}_i \in \mathbb{R}^L$ via additive SS embedding by means of a (normalised) carrier (spreading sequence/signature) $\boldsymbol{s} \in \mathbb{R}^L$, $\|\boldsymbol{s}\| = 1$, with a corresponding embedding amplitude $A \geq 0$. For the sake of generality, $\boldsymbol{n}$ represents potential external noise [External noise is frequently viewed as a suitable model for quantisation errors, channel transmission disturbances, and/or image processing attacks.] of mean $\boldsymbol{0}$ and autocorrelation matrix $\sigma_n^2\boldsymbol{I}_L$, $\sigma_n^2 > 0$.

In an effort to reduce the interference from the host signal, the host vectors $\boldsymbol{x}_i$, $i = 1, \ldots, M$, can be steered away from the embedding carrier using an operator of the form $(\boldsymbol{I}_L - c\boldsymbol{s}\boldsymbol{s}^{\mathrm{T}})$ with a parameter $c \in \mathbb{R}$, and the carrier $\boldsymbol{s} \in \mathbb{R}^L$. The composite signal of additive SS embedding on linearly transformed host data is

$$\boldsymbol{y}_i = Ab_i\boldsymbol{s} + (\boldsymbol{I}_L - c\boldsymbol{s}\boldsymbol{s}^{\mathrm{T}})\boldsymbol{x}_i + \boldsymbol{n}, \quad i = 1, \ldots, M, \tag{2}$$

where information bit b_i is embedded in the ith linearly transformed host data vector $(\boldsymbol{I}_L - c\boldsymbol{s}\boldsymbol{s}^{\mathrm{T}})\boldsymbol{x}_i$. The optimal design of the parameter c has been investigated in [25–27]. The SS embedding scheme in (2) is often referred to as improved SS (ISS) embedding.

The linear transformation operation on the host aims to suppress the interference/host $\boldsymbol{x}_i$ in the second-order statistics sense and the embedding amplitude A is fixed for all information bits. However, it should be noted that the interference from the host signal is explicitly known to the embedders. Motivated by this prior knowledge, in [30] Valizadeh and Wang proposed the correlation-aware ISS (CAISS) embedding scheme by incorporating ISS and the correlation-and-bit-aware concept. Particularly, in [30] two levels of amplitude are designed by exploring the correlation between the host and the carrier as well as the information bit. The CAISS embedding scheme can be described as follows

$$\boldsymbol{y}_i = \begin{cases} \boldsymbol{x}_i + \boldsymbol{s}A_1 + \boldsymbol{n}, & \text{if } \boldsymbol{s}^{\mathrm{T}}\boldsymbol{x}_i \geq 0,\ b_i = +1, \\ \boldsymbol{x}_i - \boldsymbol{s}A_2 - \lambda_h\boldsymbol{s}(\boldsymbol{s}^{\mathrm{T}}\boldsymbol{x}) + \boldsymbol{n}, & \text{if } \boldsymbol{s}^{\mathrm{T}}\boldsymbol{x}_i \geq 0,\ b_i = -1, \\ \boldsymbol{x}_i - \boldsymbol{s}A_1 + \boldsymbol{n}, & \text{if } \boldsymbol{s}^{\mathrm{T}}\boldsymbol{x}_i < 0,\ b_i = -1, \\ \boldsymbol{x}_i + \boldsymbol{s}A_2 - \lambda_h\boldsymbol{s}(\boldsymbol{s}^{\mathrm{T}}\boldsymbol{x}) + \boldsymbol{n}, & \text{if } \boldsymbol{s}^{\mathrm{T}}\boldsymbol{x}_i < 0,\ b_i = +1, \end{cases} \tag{3}$$

where λ_h is a parameter determined by the allowed distortion.

This CAISS scheme has been shown to provide better embedded data decoding performance than the traditional SS and ISS embedding schemes. However, the knowledge of the host signal $\boldsymbol{x}_i$ has not been fully exploited and only two levels of embedding amplitude are considered in the CAISS scheme. Clearly, if each symbol bit is adaptively assigned an embedding amplitude, the recovery performance can be further improved.

In the next section, we present a novel amplitude-adaptive SS embedding scheme. Symbol-by-symbol adaptive amplitude allocation algorithms are developed to compensate for the impact from the known interference. We aim at designing the SS embedding amplitude for each symbol adaptively to minimise the receiver BER at any given distortion level.

3 Amplitude-adaptive SS embedding

In parallel to (1), our proposed amplitude-adaptive SS embedding scheme has a form of

$$\boldsymbol{y}_i = A_ib_i\boldsymbol{s} + \boldsymbol{x}_i + \boldsymbol{n}, \quad i = 1, \ldots, M, \tag{4}$$

where the embedding amplitudes $A_i \geq 0$, $i = 1, \ldots, M$, need to be adaptively optimised.

Squared Euclidean metric is a common choice to measure the distortion. The squared distortion to the ith host vector (i.e. the ith

block of image) *due to the embedded data only* is

$$\mathcal{D}_i = \|(A_i b_i \boldsymbol{s} + \boldsymbol{x}_i) - \boldsymbol{x}_i\|^2 = A_i^2, \quad i = 1, \ \ldots, \ M. \tag{5}$$

Total squared distortion to whole image is

$$\mathcal{D}^{\mathrm{t}} = \sum_{i=1}^{M} A_i^2 \tag{6}$$

and the mean-squared (MS) distortion is

$$\mathcal{D}^{\mathrm{MS}} = \mathbb{E}\{\|A_i b_i\|^2\} = \frac{1}{M}\mathcal{D}^{\mathrm{t}}. \tag{7}$$

The intended recipient of the message can perform embedded bit detection by looking at the sign of the output of a filter $\boldsymbol{w}$

$$\hat{b}_i = \mathrm{sgn}\{\boldsymbol{w}^{\mathrm{T}}\boldsymbol{y}_i\}. \tag{8}$$

Matched filter $\boldsymbol{w} = \boldsymbol{s}$ has been widely adopted by the intended recipient to detect embedded bits

$$\begin{aligned}\hat{b}_i &= \mathrm{sgn}\{\boldsymbol{s}^{\mathrm{T}}\boldsymbol{y}_i\} \\ &= \mathrm{sgn}\{A_i b_i + \boldsymbol{s}^{\mathrm{T}}\boldsymbol{x}_i + \boldsymbol{s}^{\mathrm{T}}\boldsymbol{n}\} \\ &= \mathrm{sgn}\{A_i b_i + \rho_i + n\}\end{aligned} \tag{9}$$

where we define $\rho_i \triangleq \boldsymbol{s}^{\mathrm{T}}\boldsymbol{x}_i$ which is the interference from the host $\boldsymbol{x}_i$ to the information bit b_i. In particular, the interference ρ_i can be approximately viewed as having Laplace distribution [34] with zero mean and variance

$$\sigma_\rho^2 \triangleq \mathbb{E}\{\rho^2\} = \boldsymbol{s}^{\mathrm{T}}\boldsymbol{R}_x\boldsymbol{s}$$

$$\boldsymbol{R}_x \triangleq \mathbb{E}\{\boldsymbol{x}\boldsymbol{x}^{\mathrm{T}}\} = \frac{1}{M}\sum_{i=1}^{M}\boldsymbol{x}_i\boldsymbol{x}_i^{\mathrm{T}}$$

is the autocorrelation matrix of the host data $\boldsymbol{x}$. The Gaussian noise n has zero mean and variance σ_n^2.

In the application of data embedding, the host/interference $\boldsymbol{x}_i$, $i = 1, \ \ldots, \ M$, is known before embedding. With a carrier $\boldsymbol{s}$ and host vectors $\boldsymbol{x}_i$, $i = 1, \ \ldots, \ M$, the interference $\rho_i \triangleq \boldsymbol{s}^{\mathrm{T}}\boldsymbol{x}_i$, $i = 1, \ \ldots, \ M$, in the detector (9) is deterministic and known at the embedding side. Therefore, instead of treating ρ_i as an unknown or partially known interference, we attempt to fully exploit the knowledge of ρ_i for embedding. If there is flexibility in assigning *different* amplitudes A_i, $i = 1, \ \ldots, \ M$, across symbol bits, the probability of error can be further reduced by allocating amplitude to each symbol bit adaptively with its own interference ρ_i. In this paper, we aim to seek symbol-by-symbol adaptive amplitude allocation/optimisation to minimise the probability of error with a given total distortion budget, or minimise – conversely – the total distortion level at any target probability of error. We aim at minimising the probability of error of detector (9) at any given total distortion level $\mathcal{D}^{\mathrm{t}}$ (or MS distortion $\mathcal{D}^{\mathrm{MS}}$).

We rewrite the detector (9) as

$$\begin{aligned}\hat{b}_i &= \mathrm{sgn}\{(A_i + \rho_i b_i)b_i + n\} \\ &= \mathrm{sgn}\{(A_i + \alpha_i)b_i + n\}\end{aligned} \tag{10}$$

where we define $\alpha_i \triangleq \rho_i b_i = \boldsymbol{s}^{\mathrm{T}}\boldsymbol{x}_i b_i$. Before embedding, α_i, $i = 1, \ \ldots, \ M$, can be pre-computed with known carrier $\boldsymbol{s}$, host $\boldsymbol{x}_i$, and information bit b_i. With assumption that ρ_i has zero-mean symmetric distribution such as the Laplace distribution and α_i has the same distribution as ρ_i.

Now SS data embedding can be viewed as a communication system with M individual sub-channels: in each sub-channel (i.e. each block), the information bit b_i is multiplied with a coefficient $(A_i + \alpha_i)$ and then transmitted over a noisy channel. If it is allowed to model the external noise n as white Gaussian random variable with zero mean and variance σ_n^2, the probability of error of the ith detected embedded bit is [We need to emphasise that Pe_i in (11) has range from 0 to 1 because coefficient $A_i + \alpha_i$ might be negative while Pe_i is not >0.5 in common communication systems.]

$$\mathrm{Pe}_i = Q\left(\frac{A_i + \alpha_i}{\sigma_n}\right), \quad i = 1, \ \ldots, \ M, \tag{11}$$

where

$$Q(a) = \int_a^\infty \frac{1}{\sqrt{2\pi}}\,\mathrm{e}^{-\tau^2/2}\,\mathrm{d}\tau$$

The probability of error of the ith bit Pe_i depends on both the deterministic coefficient α_i and the embedding amplitude A_i which is a limited resource with a given total distortion level $\mathcal{D}^{\mathrm{t}} = \sum_{i=1}^{M} A_i^2$. In this study, with prior knowledge of α_i, $i = 1, \ \ldots, \ M$, we aim to efficiently allocate embedding amplitude $A_i \geq 0$ (equivalently allocate distortion $\mathcal{D}_i = A_i^2$), $i = 1, \ \ldots, \ M$, for each symbol bit to minimise the average probability of error

$$\underset{A_i, i=1,\ldots,M}{\arg\min}\ \overline{\mathrm{Pe}} \triangleq \frac{1}{M}\sum_{i=1}^{M}\mathrm{Pe}_i \tag{12}$$

$$\text{s.t.} \quad \sum_{i=1}^{M} A_i^2 = \mathcal{D}^{\mathrm{t}}, \tag{13}$$

$$A_i \geq 0, \quad i = 1, \ \ldots, \ M. \tag{14}$$

3.1 KKT-conditions-based embedding amplitude allocation

We first attempt to solve non-linear optimisation problems (12)–(14) by examining the KKT conditions [35]. The findings are summarised in the following proposition whose proof is provided in the Appendix.

Proposition 1: Consider optimisation problems (12)–(14). Then, A_i, $i = 1, \ \ldots, \ M$, satisfying the following KKT conditions is a strict local optimum

$$-\frac{1}{\sqrt{2\pi}\sigma_n M}\mathrm{e}^{-\left((A_i+\alpha_i)^2/2\sigma_n^2\right)} + 2\lambda A_i = 0, \quad i = 1, \ \ldots, \ M, \tag{15}$$

$$\sum_{i=1}^{M} A_i^2 = \mathcal{D}^{\mathrm{t}}, \tag{16}$$

$$A_i > 0, \quad i = 1, \ \ldots, \ M, \tag{17}$$

$$\lambda > 0, \tag{18}$$

$$\frac{A_i + \alpha_i}{\sqrt{2\pi}\sigma_n^3 M}\mathrm{e}^{-\left((A_i+\alpha_i)^2/2\sigma_n^2\right)} + 2\lambda \geq 0, \quad i = 1, \ \ldots, \ M. \tag{19}$$

There is unfortunately no closed-form expressions for A_i, $i = 1, \ \ldots, \ M$, from above KKT conditions. However, we can pursue a numerical solution. With a given $\lambda > 0$, we can numerically find roots, say $A_i(\lambda)$, $i = 1, \ \ldots, \ M$, of each of M equations in (15) using, for example, Newton's method. Smaller $\lambda > 0$ will provide a larger root $A_i(\lambda)$ (with appropriate root selection to satisfy (19) if multiple roots are found); larger $\lambda > 0$ will provide a smaller root $A_i(\lambda)$. Therefore, the optimisation problem can be numerically solved by searching a $\lambda^{\mathrm{opt}} > 0$ such that the corresponding roots $A_i(\lambda^{\mathrm{opt}})$, $i = 1, \ \ldots, \ M$, satisfy (19) and $|\sum_{i=1}^{M}[A_i(\lambda^{\mathrm{opt}})]^2 - \mathcal{D}^{\mathrm{t}}| < \varepsilon$, where ε is a small positive value serving as stopping threshold.

IET Image Process., 2016, Vol. 10, Iss. 2, pp. 138–148

The KKT-conditions-based amplitude allocation algorithm is summarised in Fig. 1.

3.2 Waterfilling-based embedding amplitude allocation

Solving the optimisation problems (12)–(14) by KKT conditions has very heavy computational complexity. In addition, it also requires the knowledge of the variance of the external noise σ_n^2 and the assumption that the external noise is Gaussian such that the probability of error can be expressed as a Q-function. Realistically, embedder may have limited knowledge of the potential external noise coming from image processing attacks and/or physical transmission etc. All these obstacles limit its application in the reality. In this section, we attempt to provide a sub-optimal waterfilling-based embedding amplitude allocation solution which has very light computational complexity and is independent with the external noise.

Instead of minimising the average probability of error $\overline{\text{Pe}}$, we turn to minimise the maximum probability of error among all M channels/symbols, $\max\{\text{Pe}_i,\ i=1,\ \ldots,\ M\}$, which is the upper bound of $\overline{\text{Pe}}$, $\overline{\text{Pe}} \le \max\{\text{Pe}_i,\ i=1,\ \ldots,\ M\}$. Then, the substitute objective function is

$$\underset{A_i,\, i=1,\ldots,M}{\arg\min}\ \max\{\text{Pe}_i,\ i=1,\ \ldots,\ M\} \tag{20}$$

$$\text{s.t.}\quad \sum_{i=1}^{M} A_i^2 = \mathcal{D}^{\text{t}}, \tag{21}$$

$$A_i \ge 0,\quad i=1,\ \ldots,\ M. \tag{22}$$

We see that Pe_i is a monotonically decreasing function of $(A_i+\alpha_i)$ regardless the distribution type of the external noise and its variance. Then, minimising the maximum Pe_i, $i=1,\ \ldots,\ M$, is equivalent to maximising the minimum $A_i+\alpha_i$, $i=1,\ \ldots,\ M$, and the amplitude allocation problem becomes

$$\underset{A_i,\, i=1,\ldots,M}{\arg\max}\ \min\{A_i+\alpha_i,\ i=1,\ \ldots,\ M\} \tag{23}$$

$$\text{s.t.}\quad \sum_{i=1}^{M} A_i^2 = \mathcal{D}^{\text{t}}, \tag{24}$$

$$A_i \ge 0,\quad i=1,\ \ldots,\ M. \tag{25}$$

This well-known max–min fairness optimisation problem can be easily solved by classic waterfilling method [35]

$$A_i = (u-\alpha_i)^+,\quad i=1,\ \ldots,\ M, \tag{26}$$

where $(a)^+ \triangleq \max\{a,\ 0\}$, u is a constant (water-line) chosen such that the distortion constraint $\sum_{i=1}^{M} A_i^2 = \mathcal{D}^{\text{t}}$ is met with equality. The water-line u can be computed by bi-section search method.

The proposed waterfilling adaptive embedding amplitude allocation algorithm has very light computational complexity and does not require any prior knowledge of external noise. With waterfilling-based amplitude allocation algorithm, $A_i+\alpha_i \ge u$, $\forall\, i=1,\ \ldots,\ M$, is always true. If the external noise can be modelled as having Gaussian distribution with zero mean and variance σ_n^2, the probability of error of each symbol has an upper bound $\text{Pe}_i \le Q(u/\sigma_n)$, $\forall\, i=1,\ \ldots,\ M$, and consequently the average probability of error has an upper bound $\overline{\text{Pe}} \le Q(u/\sigma_n)$. Conversely, for a given probability of error target $\overline{\text{Pe}}$, to minimise the host distortion due to embedding, the water-line u should be set as $u=\sigma_n Q^{-1}(\overline{\text{Pe}})$ and the total distortion with such u can be calculated by

$$\mathcal{D}^{\text{t}} = \sum_{i=1}^{M} A_i^2 = \sum_{i=1}^{M} [(u-\alpha_i)^+]^2$$

or the following proposition whose proof is offered in the Appendix.

Proposition 2: If the α_i can be modelled as Laplace distribution with variance σ_α^2, then the total distortion induced by waterfilling amplitude algorithm (26) with a water-line u is

$$\mathcal{D}^{\text{t}} = M \times \left(u^2+\sigma_\alpha^2 - \frac{1}{2}\sigma_\rho^2\, \text{e}^{-(\sqrt{2}u/\sigma_\alpha)}\right) \tag{27}$$

and the MS distortion is

$$\mathcal{D}^{\text{MS}} = \left(u^2+\sigma_\alpha^2 - \frac{1}{2}\sigma_\rho^2\, \text{e}^{-(\sqrt{2}u/\sigma_\alpha)}\right). \tag{28}$$

3.3 Prioritised waterfilling-based embedding amplitude allocation

The experimental studies show that the probability of error of SS embedding with waterfilling algorithm is very close to KKT solution with a sufficient distortion budget. When the distortion budget is relatively insufficient, the waterfilling algorithm may have performance degradation. This is because that the deduction of the probability of error is, in general, not a linear function of allocated amplitude. For example, the Q-function which is an error function for unit-variance Gaussian external noise is shown in Fig. 2. It can be observed that the error function has a rapid decreasing rate at interval around zero and a very slow decreasing rate when input is too large or small. Insufficient distortion budget will result in a low water-line u. Then those bits with α_i close to zeros can provide higher payback (the reduction on the probability of error) but are not allocated enough amplitude, while ironically the bits with low values of α_i cost too much distortion resources

Input: $\mathcal{D}^t$, α_i, $i=1,\ldots M$.

Output: A_i, $i=1,\ldots M$.

Initialize $\lambda = 10^{-4}$.

While

Find $A_i(\lambda)$ in (15), $1=1,\ldots,M$.

Select appropriate root $A_i(\lambda)$ satisfying (17) and (19)

$\mathcal{D}' = \sum_{i=1}^{M}[A_i(\lambda)]^2$

If $|\mathcal{D}' - \mathcal{D}^t| < \varepsilon$

Break and output $A_i(\lambda)$, $i=1,\ldots,M$.

Else

$\lambda := \lambda\frac{\mathcal{D}'}{\mathcal{D}^t}$.

Endif

End while

Fig. 1 *KKT-conditions-based amplitude allocation algorithm*

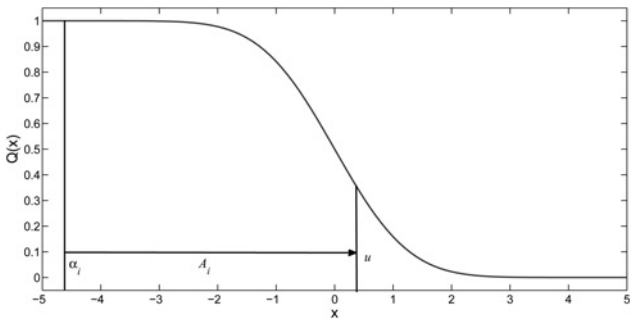

Fig. 2 *Plot of the Q-function*

and payback rate is low. Therefore, the distortion budget should be preferentially allocated to those bits with α_i close to zero in order to potentially achieve larger deduction on the probability of error with a limited distortion budget. Motivated by this observation, in this section we propose a prioritised waterfilling-based embedding amplitude allocation algorithm which can successively allocate amplitudes to sets of bits based on their priorities.

We first prioritise bits into $P+1$ sets based on the values of corresponding α_i as $\mathcal{S}_j \triangleq \{i: q_{j-1} \le |\alpha_i| < q_j,\ i = 1,\ \ldots,\ M\}$, $j = 1,\ \ldots,\ P$, and $\mathcal{S}_{P+1} \triangleq \{i: |\alpha_i| \ge q_P\}$, where $0 = q_0 < q_1 < \cdots < q_P$, are priority partition boundaries. Bits in set $\mathcal{S}_1$ have the highest priority to be assigned amplitude and bits in set $\mathcal{S}_{P+1}$ have the lowest priority. We first allocate amplitudes to bits in set $\mathcal{S}_1$ by following waterfilling algorithm:

$$A_i = \begin{cases} (u_1 - \alpha_i)^+, & i \in \mathcal{S}_1, \\ 0, & \text{otherwise.} \end{cases} \tag{29}$$

where water-line u_1 satisfies $\sum_{i \in \mathcal{S}_1} A_i^2 = \mathcal{D}^{\mathrm{t}}$. If the resulting water-line u_1 is less than a pre-defined water-line threshold u_0, then the distortion budget is insufficient and only bits in set $\mathcal{S}_1$ are allocated amplitudes; otherwise, distortion budget is sufficient to allocate amplitudes to more bits in lower priority sets and waterfilling algorithm is re-executed with an extended set $\mathcal{S}_1 \cup \mathcal{S}_2$. This procedure is successively executed until the resulting water-line is less than u_0 or all sets are included. This prioritised waterfilling (P-waterfilling) amplitude allocation algorithm is summarised in Fig. 3.

The selection of the number of priority partition sets P, the partition boundaries $q_1,\ \ldots,\ q_P$, and the water-line threshold u_0 is crucial for prioritised waterfilling algorithm. Larger P can potentially improve performance but increases complexity. To balance performance and complexity, we suggest to select $P = 6$, $q_1 = (1/2)\sigma_\alpha$, $q_2 = \sigma_\alpha$, $q_3 = (3/2)\sigma_\alpha$, $q_4 = 2\sigma_\alpha$, $q_5 = 3\sigma_\alpha$, $q_6 = 4\sigma_\alpha$, and $u_0 = (1/2)\sigma_\alpha$ where $\sigma_\alpha = \sqrt{(1/M)\sum_{i=1}^{M} \alpha_i^2}$ is the standard deviation of α_i. Experimental studies show that our proposed P-waterfilling algorithm with these setting has very close performance to the KKT solution for any given distortion budget level.

Input: $\mathcal{D}^{\mathrm{t}}$, α_i, $i = 1, \ldots, M$.

Output: A_i, $i = 1, \ldots, M$.

Initialize parameters P, q_i, $i = 1, \ldots, P$, and u_0.

Prioritize bits into sets $\mathcal{S}_i$, $i = 1, \ldots, P+1$.

Initialize $\mathcal{S} := \emptyset$, $j := 0$.

While $u_j \ge u_0$ and $j \le P+1$

$j := j + 1$.

$\mathcal{S} := \mathcal{S} \bigcup \mathcal{S}_j$.

Allocate amplitudes A_i to bits in set $\mathcal{S}$ by waterfilling algorithm

and update the water-line u_j.

End

Fig. 3 *Prioritised waterfilling-based amplitude allocation algorithm*

4 Multi-carrier SS embedding

In this section, we attempt to generalise the signal model in (4) to cover multi-carrier/multi-message embedding of the form

$$\boldsymbol{y}_i = \sum_{k=1}^{K} A_{k,i} b_{k,i} \boldsymbol{s}_k + \boldsymbol{x}_i + \boldsymbol{n}, \quad i = 1,\ 2,\ \ldots,\ M, \tag{30}$$

where bits $b_{k,i} \in \{\pm 1\}$, $k = 1,\ 2,\ \ldots,\ K$, coming potentially from K distinct messages, are embedded simultaneously in the transform-domain host vectors $\boldsymbol{x}_i$ with corresponding amplitudes $A_{k,i} \ge 0$, $k = 1, \ldots, K$, and carriers $\boldsymbol{s}_k \in \mathbb{R}^L$, $\|\boldsymbol{s}_k\| = 1$, $k = 1, 2, \ldots, K$.

After matched-filtering, the embedded bit $\{b_{k,i}\}$, $k = 1,\ \ldots,\ K$, $i = 1,\ \ldots,\ M$, can be detected by

$$\begin{aligned} \hat{b}_{k,i} &= \mathrm{sgn}\{\boldsymbol{s}_k^{\mathrm{T}} \boldsymbol{y}_i\} \\ &= \mathrm{sgn}\left\{A_{k,i} b_{k,i} + \sum_{j=1, j \ne k}^{K} A_{k,i} b_{k,i} \boldsymbol{s}_k^{\mathrm{T}} \boldsymbol{s}_j + \boldsymbol{s}_k^{\mathrm{T}} \boldsymbol{x}_i + \boldsymbol{s}_k^{\mathrm{T}} \boldsymbol{n}\right\} \end{aligned} \tag{31}$$

where the second term is multi-message interference which can be eliminated if orthogonal carriers/signatures, $\boldsymbol{s}_k^{\mathrm{T}} \boldsymbol{s}_j = 0$, $\forall k \ne j$, are adopted. The contribution of each individual embedded message bit $b_{k,i}$ to the composite signal is $A_{k,i} b_{k,i} \boldsymbol{s}_k$ and the distortion to the original host data $\boldsymbol{x}_i$ *due to the embedded message k alone* is

$$\mathcal{D}_{k,i} = \| A_{k,i} b_{k,i} \boldsymbol{s}_k \|^2 = A_{k,i}^2, \quad k = 1,\ \ldots,\ K,\ i = 1,\ \ldots,\ M.$$

With orthogonal carriers, distortion to the original host data $\boldsymbol{x}_i$ by all K messages is

$$\mathcal{D}_i = \sum_{k=1}^{K} A_{k,i}^2, \quad i = 1,\ \ldots,\ M, \tag{32}$$

and the total distortion of image is

$$\mathcal{D}^{\mathrm{t}} = \sum_{i=1}^{M} \sum_{k=1}^{K} A_{k,i}^2. \tag{33}$$

Similar to the single-carrier SS embedding discussed in the previous section, the performance of multi-carrier SS data embedding system can be further improved if we are allowed to assign different amplitudes not only across messages but also to symbol bits of each message. In the following, utilising the findings in the previous section, we aim to find optimal amplitudes for each symbol bit $b_{k,i}$ with total distortion constraint. With orthogonal carriers, the embedded bit detection (31) can be reformulated as

$$\begin{aligned} \hat{b}_{k,i} &= \mathrm{sgn}\{A_{k,i} b_{k,i} + \boldsymbol{s}_k^{\mathrm{T}} \boldsymbol{x}_{k,i} + \boldsymbol{s}_k^{\mathrm{T}} \boldsymbol{n}\} \\ &= \mathrm{sgn}\{A_{k,i} b_{k,i} + \rho_{k,i} + n\} \\ &= \mathrm{sgn}\{(A_{k,i} + \alpha_{k,i}) b_{k,i} + n\} \end{aligned} \tag{34}$$

where $\rho_{k,i} \triangleq \boldsymbol{s}_k^{\mathrm{T}} \boldsymbol{x}_{k,i}$ and $\alpha_{k,i} \triangleq \rho_{k,i} b_{k,i}$. The probability of error of bit $b_{k,i}$ is $\mathrm{Pe}_{k,i} = Q(A_{k,i} + \alpha_{k,i}/\sigma_n)$ if the external noise can be modelled as white Gaussian and the probability of error of the kth message is $\overline{\mathrm{Pe}}_k \triangleq (1/M)\sum_{i=1}^{M} \mathrm{Pe}_{k,i}$, $k = 1,\ \ldots,\ K$. Our objective is to minimise the average probability of error across all bits of all

IET Image Process., 2016, Vol. 10, Iss. 2, pp. 138–148

messages with a total distortion constraint

$$\arg\min_{A_{k,i},k=1,\ldots,K,i=1,\ldots,M} \overline{\mathrm{Pe}} = \frac{1}{MK}\sum_{k=1}^{K}\sum_{i=1}^{M}\mathrm{Pe}_{k,i} \tag{35}$$

$$\text{s.t.} \quad \sum_{k=1}^{K}\sum_{i=1}^{M}A_{k,i}^2 = \mathcal{D}^{\mathrm{t}}, \tag{36}$$

$$A_{k,i} \geq 0, \quad k=1,\ \ldots,\ K,\ i=1,\ \ldots,\ M. \tag{37}$$

This optimisation problem is essentially same as single-carrier case in (12)–(14) but with K times more amplitudes to be optimised. The KKT solution has heavy computational complexity and is not suggested for multi-carrier amplitude optimisation. Therefore, we suggest solving it by the water-filling method

$$A_{k,i} = (u - \alpha_{k,i})^{+} \tag{38}$$

where $(a)^{+} \triangleq \max\{a,\ 0\}$, constant u satisfies $\sum_{k=1}^{K}\sum_{i=1}^{M}A_{k,i}^2 = \mathcal{D}^{\mathrm{t}}$.

Similar to the single-carrier case, the waterfilling algorithm has performance degradation when the distortion budget is relatively insufficient. To solve this problem, we extend the prioritised waterfilling amplitude allocation algorithm for single-carrier SS embedding in Fig. 3 to the multi-carrier SS embedding. The detailed algorithm is described in Fig. 4.

5 SS embedding without external noise

Finally, as the last technical development in this paper, we consider an ideal case in which no external noise is introduced during the embedding processing and transmission. We focus directly on multi-carrier SS embedding where single-carrier SS embedding is a special case with $K=1$. Without external noise, the detection of bit $b_{k,i}$ (34) becomes

$$\hat{b}_{k,i} = \mathrm{sgn}\{(A_{k,i} + \alpha_{k,i})b_{k,i}\}, \quad k=1,\ \ldots,\ K,\ i=1,\ \ldots,\ M,$$

It indicates that $b_{k,i}$ can be correctly detected if and only if $(A_{k,i}+\alpha_{k,i}) > 0$. Therefore, if $\alpha_{k,i} > 0$, symbol bit $b_{k,i}$ can be correctly detected with $A_{k,i}=0$ (i.e. no embedding); if $\alpha_{k,i} \leq 0$, $b_{k,i}$ needs to be embedded with an amplitude $A_{k,i} > -\alpha_{k,i}$ such that $b_{k,i}$ can be correctly detected. To assure correct detection for all bits, we can assign embedding amplitude as

$$A_{k,i} = \begin{cases} -\alpha_{k,i} + \epsilon, & \text{if } \alpha_{k,i} \leq 0, \\ 0, & \text{otherwise,} \end{cases} \tag{39}$$

where ϵ is a small positive constant. Let $\mathcal{C}$ denote the set of $\{k,\ i\}$ such that $\alpha_{k,i} \leq 0$, $\mathcal{C} \triangleq \{\{k,\ i\}:\alpha_{k,i} \leq 0,\ k=1,\ \ldots,\ K, i=1,\ \ldots,\ M\}$. SS embedding with the amplitude allocation in (39) will introduce total distortion

$$\mathcal{D}^{\mathrm{t}} = \sum_{k=1}^{K}\sum_{i=1}^{M}A_{k,i}^2 \simeq \sum_{\{k,i\}\in\mathcal{C}}\alpha_{k,i}^2$$

Conversely, with a sufficient distortion budget $\mathcal{D}^{\mathrm{t}} > \sum_{\{k,i\}\in\mathcal{C}}\alpha_{k,i}^2$, we can allocate embedding amplitude as (39) to provide errorless data embedding.

If the total distortion budget is not large enough to let all coefficients $A_{k,i}+\alpha_{k,i}$, $k=1,\ \ldots,\ K$, $i=1,\ \ldots,\ M$, be positive, that is, $\mathcal{D}^{\mathrm{t}} < \sum_{\{k,i\}\in\mathcal{C}}\alpha_{k,i}^2$, then the error of bit detection occurs and the probability of error for message-k is defined as

$$\mathrm{Pe}_k = \frac{\mathrm{Ne}_k}{M}, \quad k=1,\ \ldots,\ K,$$

where Ne_k is the number of error bits of message-k, that is, $\mathrm{Ne}_k = |\{(A_{k,i}+\alpha_{k,i}) \leq 0,\ i=1,\ \ldots,\ M\}|$. In an effort to minimise overall probability of error with a concern of fairness among all K messages, our objective is to assign the embedding amplitude $A_{k,i}$ to minimise the maximum probability of error Pe_k with a given

Input: $\mathcal{D}^t$, $\alpha_{k,i}$, $k=1,\ldots,K$, $i=1,\ldots,M$.

Output: $A_{k,i}$, $k=1,\ldots,K$, $i=1,\ldots,M$.

Initialize parameters P, $q_{k,i}$, $k=1,\ldots,K$, $i=1,\ldots,P$, and u_0.

Prioritize bits into sets $\mathcal{S}_{k,i}$, $k=1,\ldots,K$, $i=1,\ldots,P+1$.

Initialize $\mathcal{S} := \emptyset$, $j := 0$.

While $u_j \geq u_0$ and $j \leq P+1$

$j := j+1$.

$\mathcal{S} := \mathcal{S} \bigcup \mathcal{S}_{1,j} \bigcup \ldots \bigcup \mathcal{S}_{K,j}$.

Allocate amplitudes to bits in set $\mathcal{S}$ by waterfilling algorithm

and obtain amplitudes $A_{k,i}$, $\{k,i\} \in \mathcal{S}$, and a water-line u_j.

End

Fig. 4 *Prioritised waterfilling-based amplitude allocation algorithm for multi-carrier embedding*

Given $\mathcal{D}^t$, $\alpha_{k,i}$, $k=1,\ldots,K$, $i=1,\ldots M$.

Initialize $A_{k,i} := 0, \forall\ k=1,\ldots,K,\ i=1,\ldots M$.

Find set $\mathcal{C}$ of $\{k,i\}$ such that $\alpha_{k,i} \leq 0$, $k=1,\ldots,K$, $i=1\ldots,M$.

If $\sum_{\{k,i\}\in\mathcal{C}}\alpha_{k,i}^2 < \mathcal{D}^t$

Assign amplitudes $A_{k,i} := -\alpha_{k,i} + \epsilon$, $\forall\ \{k,i\} \in \mathcal{C}$.

Else

Find $Ne_k = |\{i : \alpha_{k,i} \leq 0, i=1,\ldots,M\}|$, $k=1,\ldots,K$.

While

Find k^* such that $Ne_{k^*} \geq Ne_k$, $k=1,\ldots,K$.

Find i^* such that $\alpha_{k^*,i^*} \geq \alpha_{k^*,i}$, $\forall\{k^*,i\} \in \mathcal{C}$.

If $\sum_{k=1}^{K}\sum_{i=1}^{M}A_{k,i}^2 + \alpha_{k^*,i^*}^2 < \mathcal{D}^t$

$A_{k^*,i^*} := -\alpha_{k^*,i^*} + \epsilon$;

$\mathcal{C} := \mathcal{C} - \{k^*,i^*\}$;

$Ne_{k^*} := Ne_{k^*} - 1$.

Else

Break.

Endif

End while

Endif

Fig. 5 *Amplitude allocation for SS embedding without external noise*

total distortion budget $\mathcal{D}^{\mathrm{t}}$

$$\arg\min_{A_{k,i},\,k=1,\ldots,K,\,i=1,\ldots,M} \quad \max\{\mathrm{Pe}_k,\ k=1,\ \ldots,\ K\} \tag{40}$$

$$\text{s.t.} \quad \sum_{k=1}^{K}\sum_{i=1}^{M} A_{k,i}^2 = \mathcal{D}^{\mathrm{t}}, \tag{41}$$

$$A_{k,i} \geq 0, \quad k=1,\ \ldots,\ K,\ i=1,\ \ldots,\ M. \tag{42}$$

The amplitude allocation algorithm to achieve above goal is straightforward. Initially, let $A_{k,i} := 0$, $\forall\ k = 1,\ \ldots,\ K,\ i = 1,\ \ldots,\ M$. Next, we select one message, say message-k^*, which has the largest number of errors $\mathrm{Ne}_{k^*} \geq \mathrm{Ne}_k$, $k = 1,\ \ldots,\ K$, and then find the i^*th bit in message-k^* which has the largest $\alpha_{k^*,i}$, $\alpha_{k^*,\,i^*} \geq \alpha_{k^*,i}$, $\forall\{k^*,\ i\} \in \mathcal{C}$. In message-$k^*$, b_{k^*,i^*} needs the least amplitude to let $A_{k^*,i^*} + \alpha_{k^*,\,i^*}$ change from negative to positive. We assign amplitude $A_{k^*,i^*} := \alpha_{k^*,i^*} + \varepsilon$ to b_{k^*,i^*}, the i^*th bit of message-k^*, and update set $\mathcal{C} := \mathcal{C} - \{k^*,\ i^*\}$ and $\mathrm{Ne}_{k^*} := \mathrm{Ne}_{k^*} - 1$. We iteratively execute the above procedure until all total distortion is consumed. The amplitude allocation algorithm for SS embedding without external noise is summarised in Fig. 5.

6 Experimental studies

In the following, we present extensive experimental results that we obtained from the implementation of the developed amplitude-adaptive SS embedding algorithms. To carry out an experimental study of the developments presented in the previous sections, we consider the familiar grey-scale 512×512 'Baboon' image as a host example. We perform 8×8-block DCT single-carrier embedding (4) over all 63 bins except the dc coefficient. Hence, our carrier length is $L = 63$ and we embed $512^2/8^2 = 4096$ bits. In our experiment, we use arbitrary carrier generated by Gaussian distribution. With an 8×8-block mean square error (MSE) distortion $\mathcal{D}^{\mathrm{MS}}$, the peak signal-to-noise ratio (PSNR) of the image due to embedding can be calculated by $\mathrm{PSNR} \triangleq 20\log_{10}(255) - 10\log_{10}(\mathcal{D}^{\mathrm{MS}}/64)$. Another metric that reflects the relationship between host and embedding distortion is the block document-to-watermark power ratio (DWR) defined as $\mathrm{DWR} \triangleq 10\log_{10}\sigma_x^2 - 10\log_{10}(\mathcal{D}^{\mathrm{MS}})$ where $\sigma_x^2 \triangleq \mathrm{Tr}\{\boldsymbol{R}_x\}$ is the (total) host block variance. The value of σ_x^2 depends on the nature of each host image and is provided in each experiment that we run (see figure captions) to facilitate translation by the reader between MSE and DWR if desired. For the sake of generality, in our studies we also incorporate white Gaussian noise of variance $\sigma_n^2 = 3$ dB.

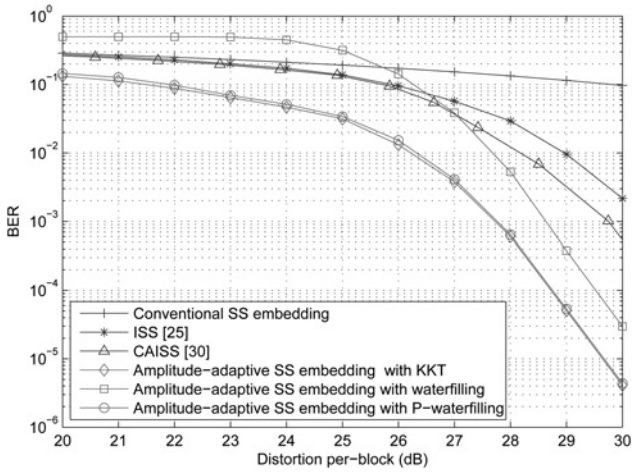

Fig. 6 *BER versus allowable per-message distortion, (512×512 Baboon, single-carrier SS embedding, $L = 63$, $\sigma_n^2 = 3$ dB, $\sigma_x^2 = 46.49$ dB)*

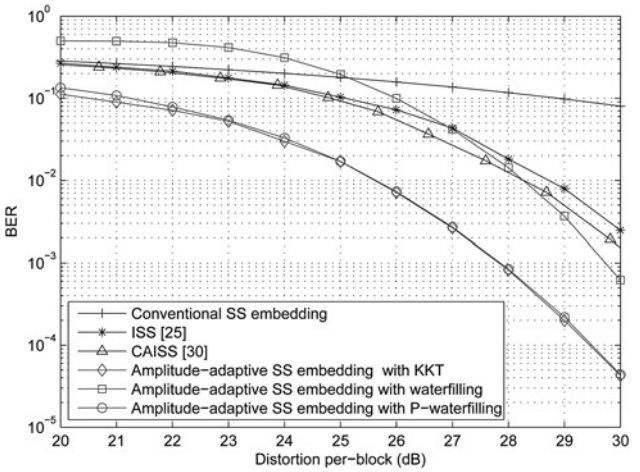

Fig. 7 *BER versus allowable per-message distortion, (512×512 Bridge, single-carrier SS embedding, $L = 63$, $\sigma_n^2 = 3$ dB, $\sigma_x^2 = 45.90$ dB)*

We evaluate the performance of six different embedding schemes: (i) SS embedding (1) with equal amplitudes, (ii) ISS embedding scheme (2) proposed in [25], (iii) CAISS embedding scheme (3) proposed in [30], (iv) the proposed amplitude-adaptive SS embedding with by KKT solution, (v) proposed amplitude-adaptive SS embedding with waterfilling solution, and (vi) the proposed amplitude-adaptive SS embedding with prioritised waterfilling (P-waterfilling) solution.

Fig. 6 shows the recovery BER created by the embedded data for above six embedding schemes as a function of the MS distortion $\mathcal{D}^{\mathrm{MS}}$ per-block [With block MS distortion $\mathcal{D}^{\mathrm{MS}}$, the PSNR of the image due to embedding can be calculated by $\mathrm{PSNR} = 20\log_{10}(255) - 10\log_{10}(\mathcal{D}^{\mathrm{MS}}/64)$. Total distortion is $\mathcal{D}^{\mathrm{t}} = M\mathcal{D}^{\mathrm{MS}}$.]. It is demonstrated that the use of proposed symbol-by-symbol adaptive amplitude allocation significantly improves the BER performance over conventional equal-amplitude SS embedding and also outperforms recently developed ISS and CAISS embedding schemes. Particularly, if the BER requirement is 10^{-5}, then the proposed P-waterfilling algorithm can reduce more than 2 dB distortion compared with ISS and CAISS; if the distortion budget is 30 dB, then the P-waterfilling algorithm can reduce BER from 10^{-3} to 10^{-5} (i.e. two orders of magnitude) over ISS and CAISS. Compared with the benchmark KKT method, we can also observe that the sub-optimal P-waterfilling solution has very close BER performance to the optimal KKT solution for all

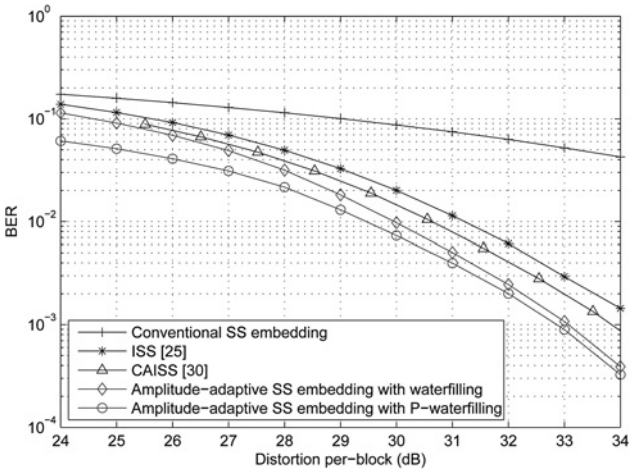

Fig. 8 *BER versus allowable per-message distortion, (average findings over more than 100 images [36], 8×8-block partition, single-carrier SS embedding, $L = 63$, $\sigma_n^2 = 3$ dB)*

IET Image Process., 2016, Vol. 10, Iss. 2, pp. 138–148

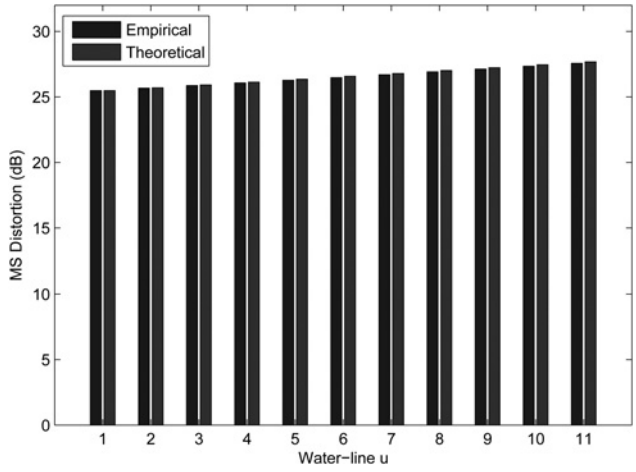

Fig. 9 *Theoretical MS distortion in (28) and the empirical MS distortion under different water-lines u. The experiment is carried out with a data set of 1300 images [36]*

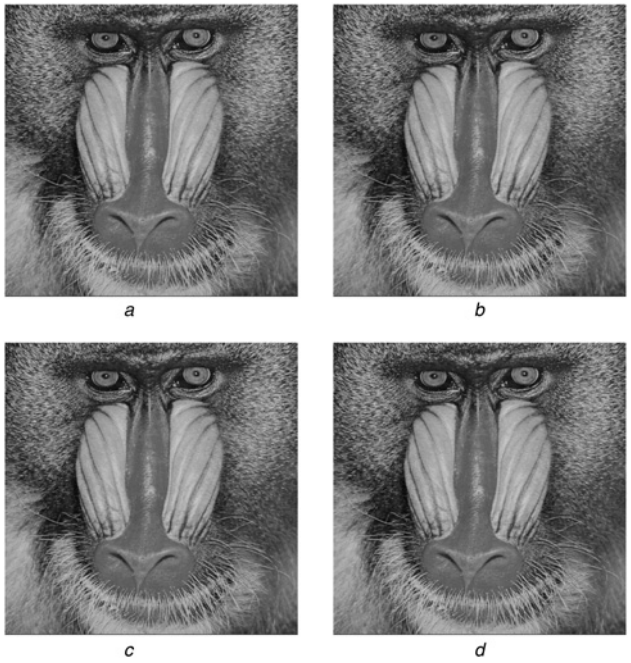

Fig. 10 *Embedding distortion on the image*

a Original Baboon image
b Data-embedded image by our proposed P-waterfilling embedding algorithm
c Data-embedded image by ISS [25]
d Data-embedded image by CAISS [30]

distortion range. Therefore, P-waterfilling amplitude allocation algorithm is always suggested due to its simplicity and satisfactory performance for all distortion levels. In Fig. 7, we repeat the same experiment for grey-scale 512×512 'Bridge' image and the same conclusion can be drawn. To address the need for experimental verification of highest credibility, now we examine the average performance of the proposed amplitude-adaptive SS embedding algorithm over an image database. We randomly select more than 100 images from image data set [36] which have great variety (e.g. outdoor/indoor, daylight/night, natural/man-made). Recovery performance plots are given in Fig. 8. Similar conclusion can be drawn as in previous individual image host experimentations. It is worth pointing out that each image may have quite different log-scale BER curve due to the large variation of image contents. When we attempt to show the average BER over all images, the performance improvement looks not very significant as the individual image experiment.

To validate Proposition 2, in Fig. 9 we show both the theoretical MS distortion computed by Proposition 2 (28) and the empirical MS distortion under different water-line u. The experiment is carried out with a data set of 1300 images [36] and the average distortions are obtained and illustrated. We can observe from Fig. 9 that the theoretical MS distortion computed by Proposition 2 match the empirical MS distortion. This result validates the accuracy of Proposition 2.

To demonstrate the embedding distortion on the image, in Fig. 10 we show (a) original Baboon image, (b) data-embedded image by our proposed P-waterfilling embedding algorithm, (c) data-embedded image by ISS [25], and (d) data-embedded image by CAISS [30]. The MS distortion is fixed at $\mathcal{D}^{\mathrm{MS}} = 30\,\mathrm{dB}$ for all three embedding algorithms. We cannot observe notable distortion on all three data-embedded images. To further illustrate the distribution of embedding distortion on the image, we evaluate the difference between cover image and data-embedded images $\boldsymbol{I}_{\mathrm{diff}} = \mathrm{ABS}(\boldsymbol{I}_c - \boldsymbol{I}_s)$ where $\boldsymbol{I}_c$ and $\boldsymbol{I}_s$ are the cover image and data-embedded image, respectively, and $\mathrm{ABS}(\cdot)$ denotes taking the absolute values. To achieve better visualisation, we amplify the difference $\boldsymbol{I}_{\mathrm{diff}}$ five times and show $\boldsymbol{I}_{\mathrm{diff}} \times 5$ in Fig. 11. All three embedding algorithms have similar distortion patterns. In Figs. 12 and 13, we repeat the same experiment on the Bridge image and the same conclusion can be drawn.

Next, we consider the problem of multi-carrier SS embedding. We still use the 'Baboon' and 'Bridge' images as the host and wish to hide $K = 16$ data messages of length 4096 bits each. With the total distortion $\mathcal{D}^{\mathrm{t}}$ to the host image, the MS per-message per-block distortion is $\mathcal{D}^{\mathrm{MS}} = \mathcal{D}^{\mathrm{t}}/M/K$. As before, for the sake of generality, we add to the host white Gaussian external noise of variance 3 dB. We study three different multi-carrier embedding schemes: (i) conventional SS embedding equal amplitudes, (ii) proposed amplitude-adaptive SS embedding with waterfilling solution, and (iii) the proposed amplitude-adaptive SS embedding with P-waterfilling amplitude allocation. Compared with the experiments in Figs. 6 and 7,

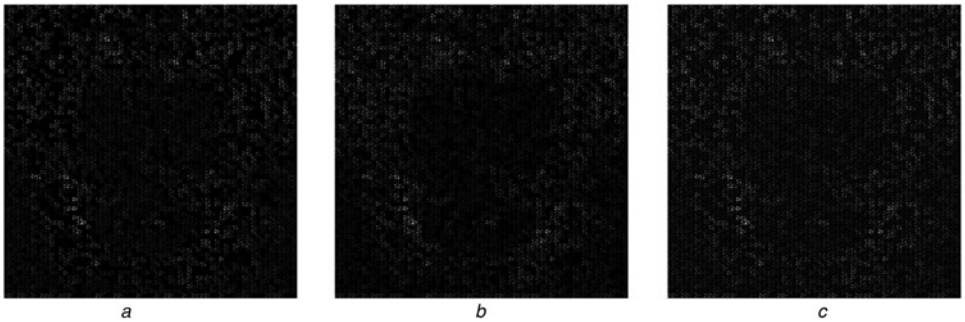

Fig. 11 *Difference between Baboon cover image and data-embedded images ABS($\boldsymbol{I}_c - \boldsymbol{I}_s$) × 5*

a Data-embedded image by our proposed P-waterfilling embedding algorithm
b Data-embedded image by ISS [25]
c Data-embedded image by CAISS [30]

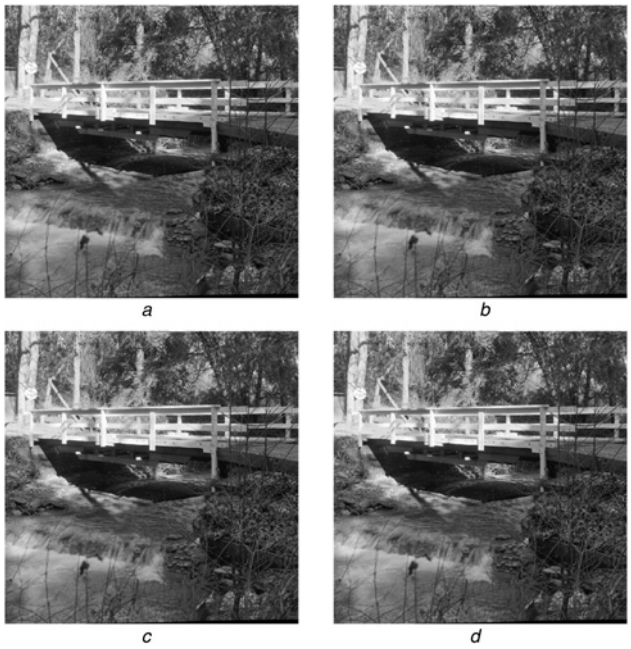

Fig. 12 *Experiment on the Bridge image*

a Original bridge image
b Data-embedded image by our proposed P-waterfilling embedding algorithm
c Data-embedded image by ISS [25]
d Data-embedded image by CAISS [30]

amplitude-adaptive SS embedding with the KKT solution is excluded due to extremely high computational complexity. ISS and CAISS embedding schemes, which were originally developed for single-carrier SS embedding, are not considered in these experiments. Figs. 14 and 15 show BERs of three multi-carrier SS embedding schemes versus distortion per-message per-block. Similar results as single-carrier case, the proposed amplitude-adaptive SS embedding can significantly improve the BER performance of SS embedding. In Fig. 16, we show the average BER of multi-carrier embedding over multiple images and similar conclusion can be drawn.

Finally, we turn to examine the performance of SS embedding when no external noise is introduced. We carry out the same experiment studies for the multi-carrier SS embedding but no external noise is added to the host. The results of Fig. 17 illustrate that the proposed adaptive amplitude allocation optimisation can always provide significant performance improvement for various images.

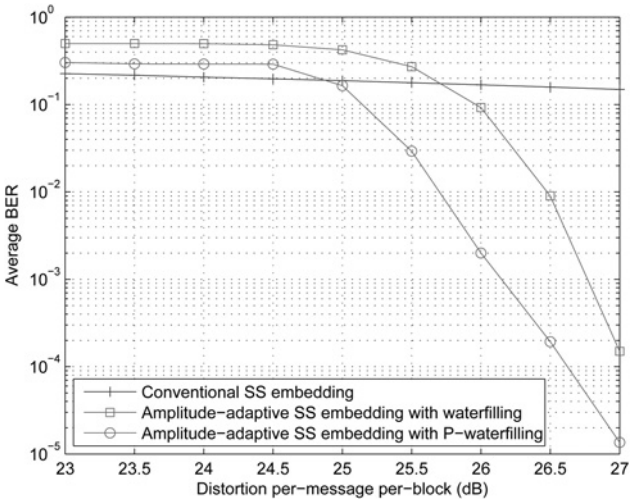

Fig. 14 *BER versus allowable per-message per-block distortion, (512 × 512 Baboon, multi-carrier SS embedding, L = 63, K = 16, $\sigma_n^2 = 3$ dB, $\sigma_x^2 = 46.49$ dB)*

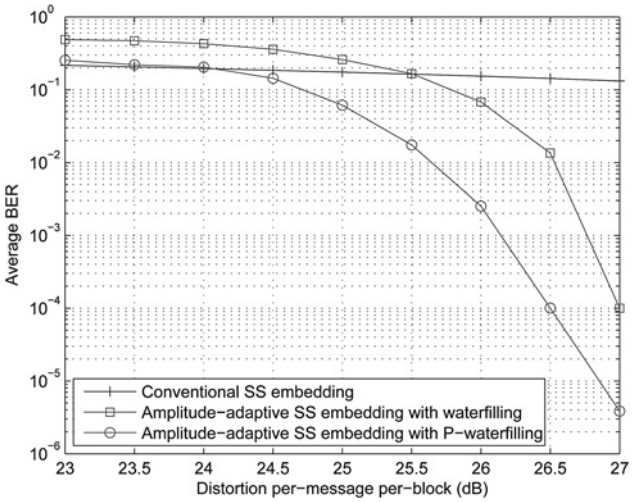

Fig. 15 *BER versus allowable per-message per-block distortion, (512 × 512 Bridge, multi-carrier SS embedding, L = 63, K = 16, $\sigma_n^2 = 3$ dB, $\sigma_x^2 = 45.90$ dB)*

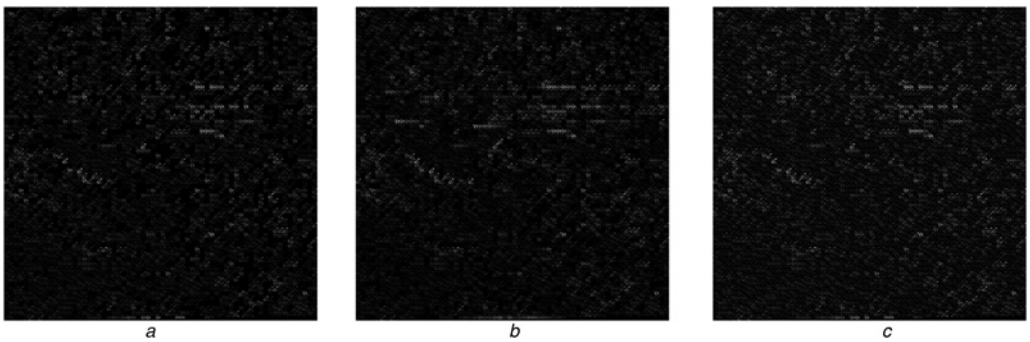

Fig. 13 *Difference between Bridge cover image and data-embedded images ABS($\mathbf{I}_c - \mathbf{I}_s$) × 5*

a Data-embedded image by our proposed P-waterfilling embedding algorithm
b Data-embedded image by ISS [25]
c Data-embedded image by CAISS [30]

IET Image Process., 2016, Vol. 10, Iss. 2, pp. 138–148

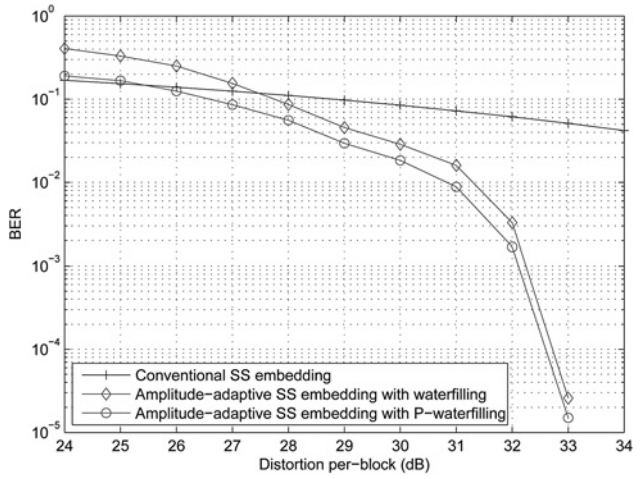

Fig. 16 *BER versus allowable per-message distortion, (average findings over more than 100 images [36], 8 × 8-block partition, multiple-carrier SS embedding, L = 63, $\sigma_n^2 = 3$ dB)*

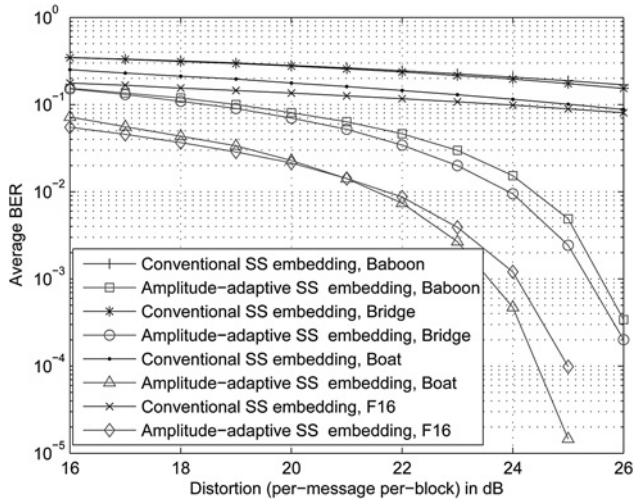

Fig. 17 *BER versus allowable per-message distortion, noiseless embedding case, (512 × 512 Boat, multi-carrier SS embedding, L = 63, K = 15)*

7 Conclusions

We considered the problem of embedding data in a digital media host via SS embedding in an arbitrary transform domain. We presented a novel amplitude-adaptive SS embedding scheme in which each symbol bit is assigned an embedding amplitude based on its known interference from the host. A computationally expensive KKT-conditions-based amplitude allocation algorithm and two light-complexity water-filling-based amplitude allocation algorithms were developed to adaptively assign amplitude to each symbol bit with any given total distortion budget. We showed that the use of symbol-by-symbol adaptive amplitude allocation dramatically further improves the performance of additive SS embedding in terms of the probability of error over conventional equal-amplitude allocation and also outperforms recently developed ISS and CAISS embedding schemes. Particularly, the proposed P-waterfilling amplitude allocation algorithm is always suggested due to its simplicity and satisfactory performance.

To take these findings one step further, we extended our single-carrier/single-message to multi-carrier/multi-message embedding and developed amplitude optimisation algorithm which can provide, once again, improvements in the probability of error as well as assure the fairness among all embedded messages. Finally, we investigated amplitude allocation for an ideal case in which no external noise is introduced during the embedding processing and transmission and proposed an iterative amplitude assignment algorithm to fairly minimise the number of errors of each message with total distortion budget.

While the most common squared Euclidean distortion is used as metric in this paper, we should be aware that there are many more reasonable metrics measuring the embedding distortion according to the human visual system (HVS) such as the just-notable-distortion [37, 38]. Owing to the limitation of the space, we did not consider HVS in this paper but will concentrate our focus on it in our future works. In this paper, without loss of generality, in both algorithm development and experiment, we added Gaussian external noise to emulate the image processing attacks (e.g. compression, scaling, rotation, cropping, filtering etc.). Clearly, the real image processing attacks behave quite differently. We will also investigate the effects of various attacks and testify the robustness of the proposed algorithms in our future studies.

8 Acknowledgment

This work is supported by the Fundamental Research Funds for the Central Universities (grant no. DUT14RC(3)103), the Open Fund of Artificial Intelligence Key Laboratory of Sichuan Province (grant no. 2012RZJ01), the National Natural Science Foundation of China (grant no. 61172109 and 61402079), and the Foundation for Innovative Research Groups of the National Science Foundation of China (NSFC) (grant no. 71421001).

9 References

1 Swanson, M.D., Kobayashi, M., Tewfik, A.H.: 'Multimedia data-embedding and watermarking technologies', *Proc. IEEE*, 1998, **86**, (6), pp. 1064–1087
2 Cox, I.J., Miller, M.L., Bloom, J.A.: 'Digital watermarking' (Morgan-Kaufmann Press, San Francisco, 2002)
3 Huang, Y., Liu, C., Tang, S., *et al.*: 'Steganography integration into a low-bit rate speech codec', *IEEE Trans. Inf. Forensics Sec.*, 2012, **7**, (6), pp. 1865–1875
4 Liu, S.-C., Tsai, W.-H.: 'Line-based cubism-like image – a new type of art image and its application to lossless data hiding', *IEEE Trans. Inf. Forensics Sec.*, 2012, **7**, (5), pp. 1448–1458
5 Yi, Y., Li, R., Chen, F., *et al.*: 'A digital watermarking approach to secure and precise range query processing in sensor networks'. Proc. IEEE INFOCOM, Turin, Italy, April 2013, pp. 1950–1958
6 Feng, X., Zhang, H., Wu, H.-C., *et al.*: 'A new approach for optimal multiple watermarks injection', *IEEE Signal Proc. Lett.*, 2011, **18**, (10), pp. 575–578
7 Tew, Y., Wong, K.: 'An overview of information hiding in H.264/AVC compressed video', *IEEE Trans. Circuits Syst. Video Technol.*, 2014, **24**, (2), pp. 305–319
8 Fridrich, J.: 'Steganography in digital media, principles, algorithms, and applications' (Cambridge University Press, Cambridge, UK, 2010)
9 Wang, Y., Moulin, P.: 'Perfectly secure steganography: capacity, error exponents, and code constructions', *IEEE Trans. Inf. Theory*, 2008, **54**, (6), pp. 2706–2722
10 Wu, M., Liu, B.: 'Data hiding in binary image for authentication and annotation', *IEEE Trans. Multimedia*, 2004, **6**, (4), pp. 528–538
11 Tseng, H.-W., Leng, H.-S.: 'High-payload block-based data hiding scheme using hybrid edge detector with minimal distortion', *IET Image Process.*, 2014, **8**, (11), pp. 647–654
12 Feng, B., Lu, W., Sun, W.: 'Secure binary image steganography based on minimizing the distortion on the texture', *IEEE Trans. Inf. Forensics Sec.*, 2015, **10**, (2), pp. 243–255
13 Zhu, T., Xiong, P., Li, G., *et al.*: 'Correlated differential privacy: hiding information in non-IID data set', *IEEE Trans. Inf. Forensics Sec.*, 2015, **10**, (2), pp. 229–242
14 Cao, H., Kot, A.C.: 'On establishing edge adaptive grid for bilevel image data hiding', *IEEE Trans. Inf. Forensics Sec.*, 2013, **8**, (9), pp. 1508–1518
15 Cox, I.J., Kilian, J., Leighton, F.T., *et al.*: 'Secure spread spectrum watermarking for multimedia', *IEEE Trans. Image Process.*, 1997, **6**, (12), pp. 1673–1687
16 Barni, M., Bartolini, F., De Rosa, A., *et al.*: 'Optimum decoding and detection of multiplicative watermarks', *IEEE Trans. Signal Process.*, 2003, **51**, (5), pp. 1118–1123
17 Barni, M., Bartolini, F., De Rosa, A., *et al.*: 'A new decoder for the optimum recovery of nonadditive watermarks', *IEEE Trans. Image Process.*, 2001, **10**, (8), pp. 755–766
18 Barni, M., Bartolini, F., De Rosa, A., *et al.*: 'Capacity of full frame DCT image watermarks', *IEEE Trans. Image Process.*, 2000, **9**, (1), pp. 1450–1455
19 Qiang, C., Huang, T.S.: 'An additive approach to transform-domain information hiding and optimum detection structure', *IEEE Trans. Multimedia*, 2001, **3**, (3), pp. 273–284
20 Tian, H., Zhao, Y., Ni, R., *et al.*: 'LDFT-based watermarking resilient to local desynchronization attacks', *IEEE Trans. Cybern.*, 2013, **43**, (6), pp. 2190–2201

21 Zareian, M., Tohidypour, H.R.: 'Robust quantisation index modulation-based approach for image watermarking', *IET Image Process.*, 2013, **7**, (5), pp. 432–441
22 Moulin, P., Ivanović, A.: 'The zero-rate spread-spectrum watermarking game', *IEEE Trans. Signal Process.*, 2003, **51**, (4), pp. 1098–1117
23 Xiao, D., Chen, S.: 'Separable data hiding in encrypted image based on compressive sensing', *Electron. Lett.*, 2014, **50**, (8), pp. 598–600
24 Fei, C., Kundur, D., Kwong, R.H.: 'Analysis and design of watermarking algorithms for improved resistance to compression', *IEEE Trans. Image Proc.*, 2004, **13**, (2), pp. 126–144
25 Malvar, H.S., Florencio, D.A.: 'Improved spread spectrum: a new modulation technique for robust watermarking', *IEEE Trans. Signal Process.*, 2003, **51**, (4), pp. 898–905
26 Gkizeli, M., Pados, D.A., Medley, M.J.: 'SINR, bit error rate, and Shannon capacity optimized spread-spectrum steganography'. Proc. IEEE Int. Conf. Image Processing (ICIP), Singapore, October 2004, pp. 1561–1564
27 Gkizeli, M., Pados, D.A., Medley, M.J.: 'Optimal signature design for spread-spectrum steganography', *IEEE Trans. Image Process.*, 2007, **16**, (2), pp. 391–405
28 Li, M., Kulhandjian, M., Pados, D.A., *et al.*: 'Extracting spread-spectrum hidden data from digital media', *IEEE Trans. Inf. Forensics Sec.*, 2013, **8**, (7), pp. 1201–1210
29 Li, M., Kulhandjian, M., Pados, D.A., *et al.*: 'Steganalysis for spread-spectrum steganography'. Proc. IEEE Int. Conf. Image Processing (ICIP), Brussels, Belgium, September 2011, pp. 1957–1960
30 Valizadeh, A., Wang, Z.J.: 'Correlation-and-bit-aware spread spectrum embedding for data hiding', *IEEE Trans. Inf. Forensics Sec.*, 2011, **6**, (2), pp. 267–282
31 Cannons, J., Moulin, P.: 'Design and statistical analysis of a hash-aided image watermarking system', *IEEE Trans. Image Process.*, 2004, **13**, (10), pp. 1393–1408
32 Valizadeh, A., Wang, J.: 'A framework of multiplicative spread spectrum embedding for data hiding: performance, decoder and signature design'. Proc. IEEE GLOBECOM, Honolulu, HI, December 2009, pp. 1–6
33 Valizadeh, A., Wang, J.: 'An improved multiplicative spread spectrum embedding scheme for data hiding', *IEEE Trans. Inf. Forensics Sec.*, 2012, **7**, (4), pp. 1127–1143
34 Lam, E.Y., Goodman, J.W.: 'A mathematical analysis of the DCT coefficient distributions for images', *IEEE Trans. Image Process.*, 2000, **9**, (10), pp. 1661–1666
35 Boyd, S., Vandenberghe, L.: 'Convex optimization' (Cambridge University Press, Cambridge, UK, 2004)
36 Schaefer, G., Stich, M.: 'UCID – an uncompressed colour image database'. Proc. SPIE, Storage and Retrieval Methods and Applications for Multimedia, San Jose, CA, January 2004
37 Li, W., Zhang, Y., Yang, C.: 'A survey of JND models in digital image watermarking'. Proc. Int. Conf. Inf. Technology Software Engineering (ITSE), Beijing, China, December 2012, pp. 765–774
38 Wang, C., Ni, J., Huang, J.: 'An informed watermarking scheme using hidden Markov model in the wavelet domain', *IEEE Trans. Inf. Forensics Sec.*, 2012, **7**, (3), pp. 853–867

10 Appendix

10.1 Proof of KKT conditions (15)–(19)

We combine the function to be optimised with the constraints and form the Lagrangian

$$\mathcal{L} = \frac{1}{M}\sum_{i=1}^{M} Q\left(\frac{A_i+\alpha_i}{\sigma_n}\right) + \lambda\left(\sum_{i=1}^{M} A_i^2 - \mathcal{D}^{\mathrm{t}}\right) - \sum_{i=1}^{M}\mu_i A_i$$

where λ, $\mu_i \geq 0$, $i=1, \ldots, M$, are the KKT multipliers. The KKT necessary conditions of the optimisation problems (12)–(14) consist of the conditions $\partial\mathcal{L}/\partial A_i = 0$, $i=1, \ldots, M$, the complementary slackness conditions, and the primal and dual constraints [35]

$$-\frac{1}{\sqrt{2\pi}\sigma_n M}\,\mathrm{e}^{-\left((A_i+\alpha_i)^2/2\sigma_n^2\right)} + 2\lambda A_i - \mu_i = 0, \quad i=1, \ldots, M, \tag{43}$$

$$\mu_i A_i = 0, \quad i=1, \ldots, M, \tag{44}$$

$$\sum_{i=1}^{M} A_i^2 = \mathcal{D}^{\mathrm{t}}, \tag{45}$$

$$A_i \geq 0, \quad i=1, \ldots, M, \tag{46}$$

$$\mu_i \geq 0, \quad i=1, \ldots, M. \tag{47}$$

To simultaneously satisfy conditions (43), (44), and (47), it can be found that $\mu_i = 0$, $A_i > 0$, $\forall\, i = 1, \ldots, M$, and then the KKT necessary conditions become

$$-\frac{1}{\sqrt{2\pi}\sigma_n M}\,\mathrm{e}^{-\left((A_i+\alpha_i)^2/2\sigma_n^2\right)} + 2\lambda A_i = 0, \quad i=1, \ldots, M, \tag{48}$$

$$\sum_{i=1}^{M} A_i^2 = \mathcal{D}^{\mathrm{t}}, \tag{49}$$

$$A_i > 0, \quad i=1, \ldots, M. \tag{50}$$

Since the first normal term in (48) is always negative, the second term $2\lambda A_i$ has to be positive and consequently $\lambda > 0$ with constraint $A_i > 0$, $i=1, \ldots, M$.

The objective function (12) is not convex [The Q-function $Q(a)$ is not convex because its second derivative $Q''(a) = \left(1/\sqrt{2\pi}\right)a\,\mathrm{e}^{(a^2/2)} < 0$ when $a < 0$.]. In addition, A_i, $i=1, \ldots, M$, and λ satisfy above KKT necessary conditions are not sufficient for local optimality. To provide strict local minimisers, we also need following second-order sufficient conditions

$$\frac{\partial^2\mathcal{L}}{\partial^2 A_i} = \frac{A_i+\alpha_i}{\sqrt{2\pi}\sigma_n^3 M}\,\mathrm{e}^{-\left((A_i+\alpha_i)^2/2\sigma_n^2\right)} + 2\lambda \geq 0, \quad i=1, \ldots, M. \tag{51}$$

10.2 Proof of Proposition 2

The α_i can be modelled as Laplace distribution with variance σ_α^2, that is

$$P(x) = \frac{1}{\sqrt{2}\sigma_\alpha}\exp\left(-\frac{\sqrt{2}}{\sigma_\alpha}|x|\right)$$

With water-line u, the average distortion of each host is

$$\mathcal{D}^{\mathrm{MS}} = \int_{-\infty}^{u} \frac{1}{\sqrt{2}\sigma_\alpha}\exp\left(-\frac{\sqrt{2}}{\sigma_\alpha}|x|\right)(u-x)^2\,\mathrm{d}x \tag{52}$$

$$= \int_{-\infty}^{0} \frac{1}{\sqrt{2}\sigma_\alpha}\exp\left(\frac{\sqrt{2}}{\sigma_\alpha}x\right)(u-x)^2\,\mathrm{d}x + \int_{0}^{u} \frac{1}{\sqrt{2}\sigma_\alpha}\exp\left(-\frac{\sqrt{2}}{\sigma_\alpha}x\right)(u-x)^2\,\mathrm{d}x \tag{53}$$

We calculate the two integrations separately as follows

$$\int_{-\infty}^{0} \frac{1}{\sqrt{2}\sigma_\alpha}\exp\left(\frac{\sqrt{2}}{\sigma_\alpha}x\right)(u-x)^2\,\mathrm{d}x = \frac{u^2}{2} + \frac{u\sigma_\alpha}{\sqrt{2}} + \frac{\sigma_\alpha^2}{2} \tag{54}$$

$$\int_{0}^{u} \frac{1}{\sqrt{2}\sigma_\alpha}\exp\left(-\frac{\sqrt{2}}{\sigma_\alpha}x\right)(u-x)^2\,\mathrm{d}x = \frac{u^2}{2} - \frac{u\sigma_\alpha}{\sqrt{2}} + \frac{\sigma_\alpha^2}{2} - \frac{1}{2}\sigma_\rho^2\,\mathrm{e}^{-(\sqrt{2}u/\sigma_\alpha)} \tag{55}$$

Then the MS distortion is $\mathcal{D}^{\mathrm{MS}} = u^2 + \sigma_\alpha^2 - (1/2)\sigma_\rho^2\,\mathrm{e}^{-(\sqrt{2}u/\sigma_\alpha)}$ and the total distortion is $\mathcal{D}^{t} = M \times \mathcal{D}^{\mathrm{MS}} = M \times \left(u^2 + \sigma_\alpha^2 - (1/2)\sigma_\rho^2\,\mathrm{e}^{-(\sqrt{2}u/\sigma_\alpha)}\right)$.

IET Image Process., 2016, Vol. 10, Iss. 2, pp. 138–148