Adaptive Informed Embedding Scheme with Low Complexity for Digital Watermarking

[1,] *Chi-Yuan Lin and [2]Jyun-Jie Wang

Abstract

This paper presents a novel low-complexity informed embedding algorithm based on a modified trellis structure for a digital watermarking system. The scheme can embed adaptive robust watermarked messages for various applications. This scheme uses the codewords of a nested block code to label the arcs in the trellis structure so that each codeword can carry different amounts of hidden payload. The proposed algorithm can perform iterations to determine a tradeoff between robustness and fidelity by using numerous controllable parameters. Finally, the experimental results demonstrate three objectives: (1) The effect of controllable parameter on the proposed watermarking scheme; (2) The robustness and fidelity performance of this algorithm in various attack channels, such as Gaussian noise and JPEG compression; (3) The computation complexity, which requires less operation complexity compared with Miller's informed embedding method.

Keywords: Informed embedding, Digital watermarking, Nested linear block code.

1. Introduction

Watermarking is a common technology where the secret message is protected under the cover data of some media. The primary goal of steganography is to minimize the fidelity and error probability of set go in communication transmission. In order to satisfy the mentioned above, binning scheme is one of the solutions. Binning scheme is a key technique of great significance in information theory [2-7] [12] [18].

The binning methods employed to embed data are commonly referred to as coding with side information, where the cover object or side information is referenced in an embedder when performing data embedding [17].

*CorrespondingAuthor: Chi-Yuan Lin
(E-mail: chiyuan@ncut.edu.tw)
Department of Computer Science & Information Engineering, National Chin-Yi University of Technology, No.57, Sec. 2, Zhongshan Rd., Taiping Dist., Taichung 41170, Taiwan (R.O.C.).

Referring to [1] and [2] for a comprehensive survey of data hiding codes, the considered watermarking system had no knowledge of the host signal in the receiver, that is, a watermarking system with a blind detector. To embed a watermark in such a system, a host signal can be viewed purely as noise called blind watermarking, or exploited as side information called informed watermarking. The corresponding system with a blind detector and informed watermarking can be modeled as communication with side information at the transmitter [3], and allows more effective watermark embedding and detection methods. In general, the encoding process of informed watermarking is divided into informed coding and informed embedding. The purpose of informed coding is to choose a message codeword from a collection of possible candidates to represent this watermark. This message codeword must have minimal perceptual distortion to the host signal compared with other candidates.

In common applications, channel coding is done with imperfect knowledge of the channel conditions or noise. To minimize the distortion of watermarking, we will employ the coset code based on trellis structure. For implementation concerns, we introduce the structure of a nested binning scheme. The data classification is achieved by means of a convolutional code structure in a binning method, like nested linear block code as well [2] [8-12]. In principle [13], the early work of Costa provides the extreme rate in binning methods when encoding the data is subject to noisy constraints. However, Costa's theory is only to show that there is an existence of coding scheme that achieves the fundamental bounds. Nonetheless, it provides neither a concrete codes nor computationally efficient algorithms [14-16]. When a coding scheme is built to reach such limit, two concerns are raised as follows: 1. With reference to a coding scheme, it requires a well coding structure, and usually work in sufficient large code length. 2. The efficient embedding algorithm is found on the basis of such a coding structure, when the first requirement is once met.

Instead of using randomly generated reference vectors as arc labels as in [13], we modified this trellis structure using the codewords of a nested block code to label the arcs in the trellis. The advantage of using such codewords is that they can be easily obtained in the tradeoff between embedding capacity and message robustness. We subsequently applied the characteristic of the linear nested codes to the trellis

partition. We propose a modified trellis structure, in which each arc is labeled with nested codewords for each trellis section. By using the input number and the memory state of a convolutional code, the embedded structure can modify the capacity and robustness of embedded messages. By adjusting the controllable parameters, the user can flexibly make a tradeoff between the embedding fidelity and embedding robustness.

The proposed algorithm is intended to meet two objectives. The first is to minimize the position of the changes of watermarked images in a trellis section by using an optimal quantized algorithm based on a nested block code [19-21]. The second is to embed a message based on the low-complexity section-based informed embedding (SBIE) algorithm, to minimize the amplitude of watermarked images. The SBIE algorithm is section-based, rather than using an entire trellis in iteration. The section-based method enables algorithm performance in each section with an iterative operation to find the suitable embedding watermarked images. The experiment indicated that the algorithm achieves a lower degree of complexity and excellent results under an AWGN attack at the cost of robustness. The proposed algorithm can be easily implemented with less complexity. The experiment with the proposed algorithm was compared with that in [13]. First, considering embedded distortion and capacity, the parameters are simulated as a function of watermarked image quality. Second, we report the robustness performance of this algorithm in terms of Gaussian noise. Finally, we briefly tabulate the complexity comparison.

The rest of the study is organized as follows: Section 2 presents a brief review of trellis-based informed embedding in [13]; Section 3 provides a description of our major work on informed embedding; Section 4 provides experimental results; and finally, Section 5 offers conclusions.

2. Basics of Informed Embedding

Linear block codes and convolutional codes have a natural trellis structure, in which every path represents a codeword. Let $S = \{s_0, s_1, \cdots, s_L\}$ represent one state sequence in a L-section trellis T and $y = \{y_1, \cdots, y_L\}$ denote the received sequence. Viterbi algorithm [22] is an efficient way to find an optimum state sequence S^*, or an equivalent optimum path, with respect to a maximum-likelihood criterion

$$S^* = \arg\max_{S \in T} \sum_{k=1}^{L} \ln p\left(y_k \mid s_{k-1}, s_k\right), \tag{1}$$

where $p\left(y_k \mid s_{k-1}, s_k\right)$ is the k-th branch metric between the states s_{k-1} and s_k in the trellis.

The main goal of informed embedding is to find a good watermarked image which is not only inside the decoding region of the message codeword, but also has the minimal perceptual distortion from the host signal. It is in general difficult to find this optimal watermarked image. However, there are several approaches to find other suboptimal watermarked images, such as trellis-based informed embedding by Miller etc. [13].

Assume each path in the trellis corresponds to a message codeword of a watermark. The trellis-based informed embedding in [13] employs the Viterbi decoder to find a good watermarked image. This embedding algorithm, as illustrated in Fig. 1, requires iteratively updating the watermarked signal by running the Viterbi decoder to identifying a vector, c^1 in the first iteration, which has the highest correlation with the current watermarked signal, $x^0 = v$. Using vectors c^1 and x^0, we then obtain a new watermarked signal x^1, which is closer to the decoding region of the message codeword w. The embedding process does not terminate until the final watermarked image falls inside the interior of the Voronoi region of w. The final watermarked image of this algorithm, x^2 in Fig. 1, might not be the same as the optimum one, x in Fig. 1. The complexity of this embedding process is high since Viterbi decoding is usually repeated many times before a final watermarked image is obtained.

This paper proposes a trellis-based informed embedding with controllable parameters by modifying the arc labels of the trellis structure in [13]. The basic block diagram of this embedding method is shown in Fig. 2. As done in [13], the watermark message is embedded in the frequency domain of the host signal, rather than on the host image itself. First, a host signal I_o with dimensions N = 512×512 is divided into 4096 blocks of size 8×8; then each block is converted into the frequency domain using the DCT transform. The first 12 low-frequency AC coefficients in each block, shown in Fig. 3 of [13], are extracted and concatenated to form the extracted vector v.

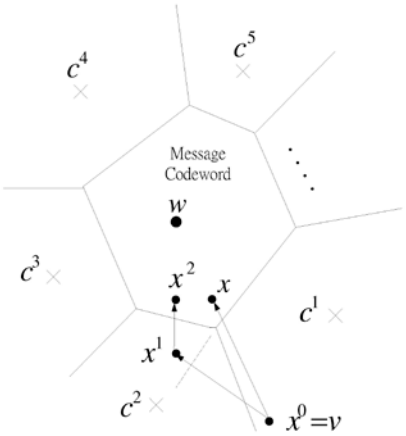

Figure 1: A trellis-based informed embedding [13]

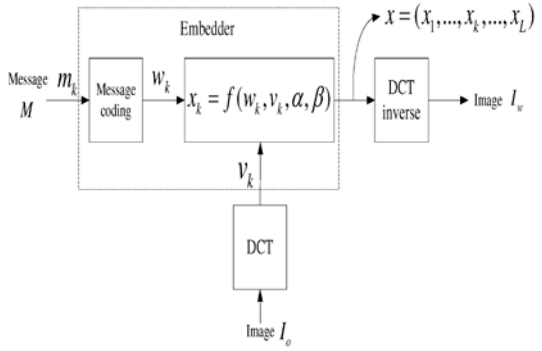

Figure 2: Informed embedding based on controllable parameters

Every *n* coefficients of *v* are then used to embed each bit of L bits watermark and form the watermarked image x, where L = 4096×12/*n*. Finally, we put the elements of *x* back into their respective DCT coefficients, and covert all DCT blocks back to the spatial domain, called I_w in Fig. 2.

Since the extracted vector *v* is available at the transmitter, the output of the informed embedding is denoted by $x = f(w, v, \alpha, \beta)$, where robust factor α and step factor β are controllable parameters for message codeword *w* and extracted vector *v* respectively. The embedding goal attempts to satisfy two conflicting criteria: *x* should be perceptually indistinguishable to *v,* and at the same time *x* should be also close enough to *w* for enhancing robustness.

3. Proposed Method

For the proposed informed embedding scheme, this paper used section-based embedding algorithm instead of the informed embedding algorithm of [13]. The four inputs to the embedder were the extracted vectors from the host sequence v={v1,v2,…,vL}, the message codeword w={w1,w2,…,wL}, and the controllable factors α and β, where the vk and wk are vectors of length n with $1 \le k \le L$. The parameters α and β control the quality of the watermarked image regarding fidelity and robustness.

The output of the embedder, watermarked sequence x, was subsequently passed through the attack channels, such as the Gaussian noise, JPEG compression, and so on, as illustrated in Fig. 2. The decoder produced the watermark estimate $\hat{m} = g(y)$, where y is the extracted vector of the received signal after the channel distortion, as illustrated in Fig. 2. The proposed informed embedding algorithm was based on trellis partition. In time k, the extracted vector vk of n components is one of the real spaces of dimension n. The real space of dimension n was partitioned into 2m regions by a (n, m) linear block codes Γ in each trellis section. We used a simplex as a linear block code. The purpose of using the simplex code is to obtain excellent robustness and space partition. Each trellis section is a mapping from the real space to the code space, which is represented by a codeword index set. The mapped B is mapped as

$$B: R^n \to \{c_1, c_2, ..., c_{2^m}\} \quad (2)$$

where $\Gamma=\{c_1, c_2,\ldots,c_2{}^m\}$ denotes the set of 2^m disjoint regions. Each region in the partition is associated with a represented codeword. The set of represented codewords is referred to as the object w_k of an extracted vector v_k. In this paper, the measure of distortion mean-squared error (MSE) distortion was as follows:

$$d(x_k, w_k) = E[|x_k - w_k|^2] \quad (3)$$

where x_k is an arbitrary vector over R^n, and w_k is a message codeword in the *k*th trellis section. In general, the $d(x_k, w_k)$ common choice is the Euclidean distance or Hamming distance.

3.1 Informed Embedding Using Nested Linear Codes

Researchers developed numerous embedding algorithms for minimizing the changes in binary embedding [19-21]. The subsection presents a discussion on minimizing the distortion of the changes of the watermarking vector *w.*

We first quantize the extracted vector *v* and watermarking vector *w* into binary symbols as $Q_2(v)$ and $Q_2(w)$, respectively. To minimize the distortion of the changes of watermarking vector in the binary domain is described as follows.

Given a nested block code (C_2, C_1), where C_2 = (*n*, k_2), C_1 = (*n*, k_1), $m_2 = n - k_2$, $m_1 = n - k_1$ and $k_1 > k_2$, the embedding rate R_m is $(k_1 - k_2) / n = (m_2 - m_1) / n$. The primary purpose of the C_2 code is to find the minimum quantization distortion. For an embedder realized using the nested binary codes, the average weight of the toggle vector E [w (e_{opt})] is estimated by the coset leader of a good fine code C_2. The nested block embedding code is constructed as follows. A (C_2, C_1) nested binary embedding code of length *n* bits is characterized by the use of a parity check matrix

$$H_2 = \begin{bmatrix} H_1 \\ H_\Delta \end{bmatrix} \quad (4)$$

where $H_\Delta \in \{0,1\}^{(m_2 - m_1)\times n}$ and $H_1 \in \{0,1\}^{m_1 \times n}$. H_2 and H_1 are two parity check matrices of binary linear fine codes C_1 and coarse codes C_2, respectively, where C_2 is nested in C_1, that is, . The C_2 code is defined as $C_2 = \{u \mid H_2 u = 0\}$, where the vector $u \in F_2^n$. The set consisting of the vector *u*, corresponding to the identical s_2, is referred to as the coset of the code C_2, defined as

$$C_2^{S_2} = \{u \mid H_2 u = s_2\} = \{c_2 + e_{opt} \mid c_2 \in C_2\}, \quad (5)$$

where e_{opt} denotes the coset leader which represents the minimal Hamming weight in each coset set. The Voronoi set $V_0 = \{e_{opt,\,i} \mid i = 1,\ldots, 2^{m_2}\}$ consists of all the coset leaders $e_{opt,\,i}$ for each coset. The C_1 is partitioned into $2^{m_2-m_1}$ coset of C_2 as

$$C_1 = \bigcup_{H_2 e_{opt,i}^T \in s_\Delta} C_2 + e_{opt,i}, i = 0,1,...,2^{m_2-m_1} - 1 \quad (6)$$

where $s_\Delta = [0\ldots\ 0\ s_l]$ and $s_l \in \{0,1\}^{m_2-m_1}$. We employ the nested scheme to realize the embedding algorithm and briefly describe the optimal embedding algorithm by using a nested block codes.

Considering the case where, given a host $Q_2(v) = u$, an optimal stego l' with syndrome s_l, is about to be determined. We assume the existence of a coset leader vector $e_{opt} = u + l'$, the closest to sequences u and l'. The host u and the optimal stego l' are of an optimal error vector e_{opt} with a constraint $E[w(e)] \le n\delta (0 \le \delta \le 0.5)$. To describe the quantizer C_2 used to determine the optimal stego vector l', we introduce the modulo-2 operation.

An arbitrary $u \in F_2^n$ can be quantized by the quantizer C_2, and the optimal quantization error e_u can be expressed as a decoding function, as

$$\begin{aligned} e_u &= f_{opt}(s_u) \\ &= f_{opt}(Hu) \\ &= \arg\min_{\hat{u} \in C_2} d(\hat{u}, u) + u \\ &\overset{\Delta}{=} u \bmod C_2 \end{aligned} \quad (7)$$

where $f_{opt}(\cdot)$ represents the maximum likelihood (ML) decoding for the quantizer C_2. Determined through ML decoding, the optimal quantization error e_u is added to u to recover the codeword $c \in C_2$, which is the closest to the vector u. We further illustrate the quantizer C_2 as C_2's coset, $C_2^{s\Delta} = C_2 + e_{opt,i} \subset C_1$, where $H_2 e_{opt,i}^T \in s_\Delta$. An arbitrary host vector $u \in F_2^n$ is quantized using $C_2^{s\Delta}$ as

$$\begin{aligned} e_u &= u \bmod C_2^{s\Delta} \\ &= u + l \bmod (C_2^{s\Delta} + l) \\ &= x \bmod C_2 \end{aligned} \quad (8)$$

where the $l \in C_2^{s\Delta}$ and $x \in F_2^n$

We offer a low bound D_{bound} to explain that the D_{opt} is limited under the bound D_{bound}. We describe the useful bound for a C_2 code as follows. A C_2 (n, k_2, λ_{min}) code is capable of correcting number of bits, so a standard array of size $2^{m_2-m_1} \times 2^k$ can be built in Fig. 4. Alternatively, the required coset leader can be precisely determined to perform binary data embedding, known as optimal embedding. Upon locating all the sequences in the coset leaders, the remaining is of a weight larger than $t + 1$. However, we assume such weight to be identical to $t + 1$, leading to a code referred to as the quasi-perfect code. The average Hamming code weight of the coset leaders within a standard array is given as follows.

$$D_{bound} = \frac{\sum_{i=0}^{t} i\binom{n}{i} + (t+1)\left(2^{n-k_2}\sum_{i=0}^{t}\binom{n}{i}\right)}{2^{n-k_2}} \quad (9)$$

The average block distortion D_{opt} of suboptimal or optimal decoding of an arbitrary linear code is higher than D_{bound}. However, in the case of a (n, k) perfect linear code, the preceding equation can be expressed as $D_{opt} = \left(\sum_i^t i\binom{n}{i}\right) / 2^{n-k}$.

We illustrate an embedding scheme with a standard array for an embedding quantizer. The quantization module in the embedding module attempts to determine the optimal toggle vector e_{opt}. To determine the optimal toggle vector e_{opt}, we use a standard array to explain the embedding procedures. A standard array is contained in Fig. 4. There exists a host corresponding to an arbitrary $u \in F_2^n$ vector of length n bits in the standard array. The syndrome $s_u = Hu^T$ is referred to as the host syndrome. A known $s_l' = (0\ldots0, sl)$ binary vector of length m_2 bits is intended for embedding. The coset leader $e_{opt} \in F_2^n$ is discovered within a set $C_2^{s_x}$ before a sequence, closest to u with syndrome s_l'. The syndrome s_x is determined by adding the logo vector s_l' to s_u. From the decoding view-point, the coset leader e_{opt} can be discovered through a decoding function, expressed as

$$\begin{aligned} e_{opt} &= f_{opt}(s_x) \\ &= f_{opt}(s_u + s_l') \\ &= f_{opt}(Hu^T + Hl^T) \\ &= f_{opt}(H(u^T + l^T)) \\ &= f_{opt}(Hx^T), \end{aligned} \quad (10)$$

where the stego vector $l = H^{-1}s_l^{'}$ and the notation $f(\cdot)$ are referred to as the ML decoding function. Suppose the existence of a vector is $x \in C_2^{s_x}$, which satisfies $s_x = Hx^T$ and represents a coset $C_2^{s_x}$ of the code C_2, which is intended to seek x with minimal weight, that is, e_{opt}, which is expressed as

$$\begin{aligned} e_{opt} &= x + \arg\min_{c \in C_2} dH(c, x) \\ &= x + Q_2(x) \\ &= x \bmod C_2 \end{aligned} \tag{11}$$

The above formula expresses the third step in the embedding procedures in Fig. 3. Once discovered, the coset leader e_{opt} is added to the host as u, $l' = u + eopt. l' \in C_2^{s_l} \subset C_1$ is the sequence closest to the sequence u within F_2^n dimensional space, and contains the logo sequence $s_l^{'}$.

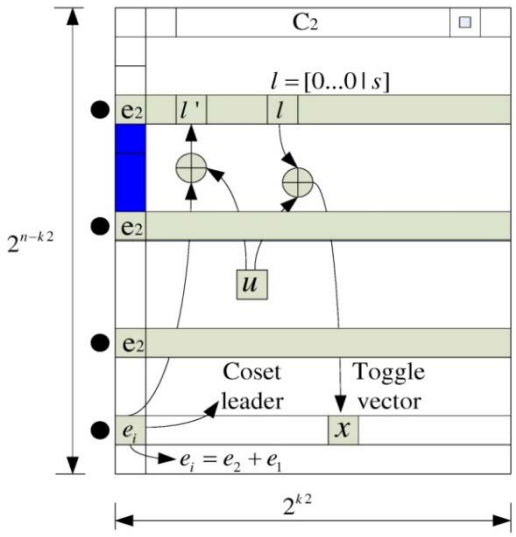

Figure 3: Embedding procedure

Although we adopt a good C_2 code quantizer for optimal embedding, the optimal embedding (i.e. ML decoding) leads to high decoding complexity for a sufficiently large C_2 code. A large value of k_2 renders the ML algorithm, combined with a standard array, infeasible when performing a binary embedding. As an uncommon approach, it is only viable for a small value of k_2.

In the receiver, the received signal is

$$y = l' + N, \tag{12}$$

where N is the channel attack. We also obtain the decoder output as

$$\begin{aligned} l' &= Q_1(y) \\ &= Q_1(l' + N,) \end{aligned} \tag{13}$$

where $Q_1(\cdot)$ is a ML decoding function. The l' is used to extract the embedding message s_l as

$$s_l = H_\Delta l'^T. \tag{14}$$

Finally, the receiver perfectly obtains the embedded message s_l.

In accordance with the aforementioned, the optimal toggle vector e_{opt} (i.e., the coset leader) is requested to be found for a nested course code C_2 and is intended, in the syndrome domain, to solve the equation $H_2 l^T + H_2 u^T = H_2 x^T$, where $(H_2)^{-1}(0,\ldots,0\ s_l) = l$. We consider the following as a simple and straightforward embedding method. Adopting a systematic nested coding with parity check matrix $H_2 = [P\ I]$ in the code domain, the aforementioned equation is identical to $s_x = H_s x = H_s(u + l)$. Given the arbitrary host u and the logo s_l, the toggle vector x can be determined immediately, assuming that $l = (0,\ldots,0, s_l)$, the front of s_l is padded $(n - m_2 + m_1)$'s zeros to generate the $l \in C_1$, is a solution and $H_2 l^T = (0,\ldots,0, s_l)^T$. Finally, we obtain the output $x = u + l$ of the embedder illustrated as follows.

Given a ($C_2(8,4,4)$, $C_1(8,6,2)$) nested block embedding code for binary embedding, a systematic parity check matrix is considered as follows.

$$H_S = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} H_1 \\ H_\delta \end{bmatrix}, \tag{15}$$

where the H_1 and H_δ are size 2×8. Suppose that there exists a logo vector l of length 8 bits within the C_1 code. Regard s_l = (11) as the logo symbol of length 2 bits intended for embedding into a cover u = (10001111), and with 6 number of 0's padded to its left, a vector l of length 0 bits is hence formed as

$$l = (000000 s_l) = (00000011) \tag{16}$$

Where $H_\delta l^T = s_l^T = (10)^T$, and the toggle vector x given by

$$x = l + u = (00000011) + (10001111) = (10001100) \tag{17}$$

The vector $x \in F_2^n$, corresponding to the sequence of length 8 bits, can thus be found. For the systematic form reason, a vector $l = (00000011) \in C_1$, corresponding to the syndrome s_l = (11), can be easily determined. Obtaining the toggle vector x does not guarantee an optimal one. To determine the optimal toggle vector e_{opt}, the toggle vector x can be decoded by ML algorithm as follows.

$$\begin{aligned} e_{opt} &= x + \arg\min_{c \in C_2} dH(x, c) \\ &= (10001100) + (10001110) \\ &= (00000010) \end{aligned} \tag{18}$$

Finally, the stego vector is obtained as
$l' = u + e_{opt} = (10001111) + (00000010) = (10001101)$
and $H_\delta l'^T = (11)^T$.

3.2 Section-based Informed Embedding (SBIE) Algorithm

Let $w = (w1,\ldots,w_L)$ be a valid path of the trellis, encoded from the watermark $m = (m_1,\ldots,m_L)$, and $v = (v_1,\ldots,v_L)$ be the extracted vector from the host signal. Each vector w_k is a codeword of length n in Γ. The embedder produces a watermarked sequence $x=\{x_1,x_2,\ldots, x_L\}$ by a section-by-section trellis-based function $x = f(w_i, v_i, \alpha, \beta)$, $1 \le i \le L$, where step factor $\beta \in [0,1]$ and robust factor $\alpha \ge 1$. The geometrical interpretation of the proposed embedding algorithm in the k-th section is shown in Fig. 4, in which the k-th component of watermarked image is iteratively updated toward to the decoding region of w_k.

In the k-th section of the trellis, we modify the k-th component of the extract vector v_k to form the k-th component of the watermarked image x_k iteratively. The proposed informed embedding attempts to find x_k such that x_k has minimum degradation from v_k, and at the same time is closer to αw_k , compared to other candidates $\alpha c, c \in \Gamma$, i.e.,

$$d(\alpha w_k, | x_k) \le d(\alpha c, x_k), \quad c \in \Gamma \text{ and } c \ne w_k, \qquad (19)$$

where $d(a, b)$ is the Euclidean distance between a and b. The detail procedure of finding such x_k is explained as follows.

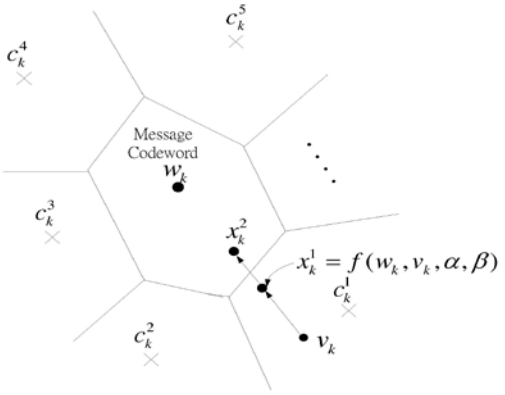

Figure 4: A geometrical interpretation of proposed informed embedding

Let h_k be the sign vector between v_k and w_k; i.e., for each component of v_k and w_k, we define

$$h_{k,i} = \text{sgn}(v_{k,i} \cdot w_{k,i}), \quad 1 \le i \le n, \qquad (20)$$

where sgn(a) = 1 if $a \ge 0$ and sgn(a) = -1 if $a < 0$. We then construct the i-th component of x_k as follows: if $h_{k,i} = 1$ then $x_{k,i}=v_{k,i}$, and if $h_{k,i} = -1$, then

$$x_{k,i} = \begin{cases} v_{k,i} - \beta \cdot d(\alpha w_k, v_k), & \text{if } v_{k,i} > 0 \\ v_{k,i} + \beta \cdot d(\alpha w_k, v_k), & \text{if } v_{k,i} \le 0 \end{cases} \qquad (21)$$

In other words, we move v_k toward to w_k by a distance $\beta d(\alpha w_k, v_k)$ for those positions in which v_k and w_k have different signs. If current x_k satisfy (19), we then move to the (k+1)-section, otherwise we substitute v_k by current x_k and repeat the procedures in (20) and (21). The proposed informed embedding causes perceptual degradation of the host signal for different α and β, and we can thus adjust the value of α and β to achieve good trade-off between the fidelity and robustness in watermarked images. The proposed informed embedding algorithm is summarized as follows.

1). Let $k = 1$ and initialize $x_k=v_k$. Choose a robust parameter $\alpha \ge 1$ and step parameter $\beta \in [0,1]$.
2). If the current x_k satisfy the criterion (19), move to step 4, otherwise substitute v_k by x_k.
3). Update the k-th watermarked image x_k by (20) and (21), and move to step 2.
4). If $k = L$ then terminate, otherwise let $k = k + 1$ and $x_k = v_k$, and go to step 2.

Above algorithm has much less complexity since the modification of x_k is executed section-by-section in the trellis without the accumulation of the distortion in the first (k - 1) components between the message codeword and the current watermarked image. We propose another informed embedding scheme by Viterbi algorithm that accumulates the total perceptual distortion to improve the fidelity between the message codeword and the current watermarked image.

First, we start with $x = v$, and initialize the state metric $\alpha_0(s_0 = 0) = 0$ and $\alpha_0(s_0 \ne 0) = \infty$ At the k-th time unit of the trellis, we then define the accumulation metric due to the label $c(s_{k-1}, s_k) \in \Gamma$ as the addition of the branch metric in $c(s_{k-1}, s_k)$ to the previously stored state metric $\alpha_{k-1}(s_{k-1})$, i.e.,

$$J_c(s_{k-1}, s_k) = \alpha_{k-1}(s_{k-1}) + d(\alpha c(s_{k-1}, s_k), x_k). \qquad (22)$$

Instead of using (19) as the criterion for the k-th component of the current watermarked sequence in the previous algorithm, we use the accumulation metric (22) as the criterion. That is, in the k-th section, we continue updating x_k until the accumulation metric with respect to the message codeword w_k is smaller than the accumulation metric with respect to any other codeword in Γ, i.e.,

$$J_{w_k}(s_{k-1}, s_k) < J_c(s_{k-1}, s_k), \quad c \in \Gamma \text{ and } c \ne w_k. \qquad (23)$$

The watermarked image based on the criterion (23) might lie in the boundary of the decoding region of the message codeword. We can increase the robustness of the watermarked image by subtracting some threshold value in (23):

$$J_{w_k}(s_{k-1}, s_k) < J_c(s_{k-1}, s_k) - R_k, \quad c \in \Gamma \text{ and } c \neq w_k. \qquad (24)$$

There are many ways to choose R_k. Here, we first choose a constant threshold R, and then let $R_k = k\frac{R}{L}$. We will use the same procedure, the equations (20) and (21), to update the current x_k until x_k satisfies the criterion (23) or (24). Moreover, after we find x_k for the k-th section, we then update each k-th state metric in the k-section by

$$\alpha_k(s_k) = \min_{s_{k-1}}\{\alpha_{k-1}(s_{k-1}) + d(\alpha c(s_{k-1}, s_k), x_k)\}, \qquad (25)$$

where the minimum is taken over those s_{k-1} connected to s_k. This informed embedding algorithm with distortion accumulation is summarized as follows.

1. Let $k = 1$ and initial $x_k = v_k$. Choose a robust parameter $\alpha \geq 1$ and step parameter $\beta \in [0,1]$.
2. If the current x_k satisfy the criterion (23), or (24) for some threshold R, move to step 4, otherwise substitute v_k by x_k.
3. Update the k-th watermarked image x_k by (20) and (21), and move to step 2.
4. If $k = L$ then terminate, otherwise let $k = k+1$ and $x_k = v_k$, update the state metric $\alpha_k(s_k)$ by (25), and go to step 2.

The complexity of this algorithm is higher since current optimum state metrices and paths have to be stored for each states in the trellis.

The proposed embedding system is built by a trellis code and each path through this trellis represents a specific watermark message. Let the extracted vector of the received sequence be denoted by $y=\{y_1,\ldots,y_L\}$, where each vector y_i is of length n. We then execute the Viterbi decoder [22] to find an optimum path which has the highest correlation with the extract vector y. Finally, the watermark message can be identified from this optimum message codeword.

4. Simulation Results

As shown in [13], a host signal with dimensions $N = 512 \times 512$ was first divided into 4096 blocks of size 8×8; subsequently, each block was converted into the frequency domain using its DCT transform. The first 12 low-frequency AC coefficients in each block, shown in Fig. 2 of [13], were extracted and concatenated, and every n = 31 coefficient was subsequently used for embedding each bit of a watermark of $L = 4096 \times 12/31 = 1585$ bits. The trellis was constructed by a $(2,1,2^{26-m_1}/2)$ convolutional code, and the labels of the trellis arcs were a $(C_2(31,5), C_1(31,31-m_1))$ nested simple code. The nested simple code has an embedding rate $R_m = (26-m_1)/31$. The parameter m_1 is capable of controlling the tradeoff between watermarking robustness and embedding rate. The experiment can be divided into two sections. We minimize the distortion of the changes of the watermarked images using the algorithm in Subsection 3.1 and then minimize the amplitude of different digital from the extraction using the SBIE algorithm described in Subsection 3.2. Subsequently, the watermarked image quality is defined as

$$\text{PSNR} = 10\log_{10}\frac{255^2}{\text{MSE}}, \qquad (26)$$

where MSE represents the mean squared error between the original image I_0 and watermarked image I_w:

$$\text{MSE} = \frac{1}{N}\sum_{i=1}^{512}\sum_{j=1}^{512}(I_o(i,j) - I_w(i,j))^2. \qquad (27)$$

Let the step parameter β = 0.1, Fig. 5 shows the PSNR performance verse the robust parameter α for the proposed embedding algorithms, consisting of proposed SBIE algorithm with threshold value R = 0, 5, 10, 20 ,respectively. As expected, the PSNR of the watermarked image decrease when the robust parameter increases. For the following simulations, we compare the BER performance of the watermark message under the same PSNR value of all embedding methods. Based on the simulation results of Fig. 5, we choose α = 10, and α = 45.3, 43.3, 42, and 39 ,respectively, whose threshold value is equal to R = 0, 5, 10, 20, respectively. The PSNR of these embedding methods is about 29.8 dB.

1). Tradeoff between watermarking robustness and embedding rate over AWGN channel

(1) Gaussian channel

A white Gaussian noise n with mean 0 and variance σ_n^2 is added to the watermarked image I_w:

$$r = I_w + n. \qquad (28)$$

The extract vector y of r is formed by block DCT transform, and the Viterbi decoding is executed on y to find the optimum watermark message. The experiment was repeated for variance ranging from 50 to 400, and the BER has been computed and shown in Fig.

6. Numerical results show that the BER of the proposed embedding method decreases when the threshold value R increases. Fig. 6 also shows that the proposed embedding method has better BER, compared to others in low noise variance. However, as the noise variance increases, the BER of the embedding method outperforms the BER of the embedding methods and in [13].

(2) JPEG compression

For the robust experiment on JPEG compression, all coefficients of the 8×8 DCT transform of the watermarked image is first multiplied by a global quantization level i, which is related to a quality factor (QF) by

$$\mu = \begin{cases} \dfrac{50}{QF}, & \text{if } 0 \le \text{QF} < 50 \\ 2 - 0.02 \cdot QF, & \text{if } 50 \le \text{QF} \le 100 \end{cases}. \qquad (29)$$

Then each coefficient of the modified DCT matrix above is multiplied by the corresponding value in the following quantization matrix

$$\begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}$$

We summary the numerical results in Fig. 7, expressed in terms of JPEG quality factor QF. The BER of the proposed methods decreases rapidly when QF<25, and achieves the error floor region when QF>25. Numerical results also show that the methods have better BER performance in low JPEG compression quality, compared to the algorithm in [13].

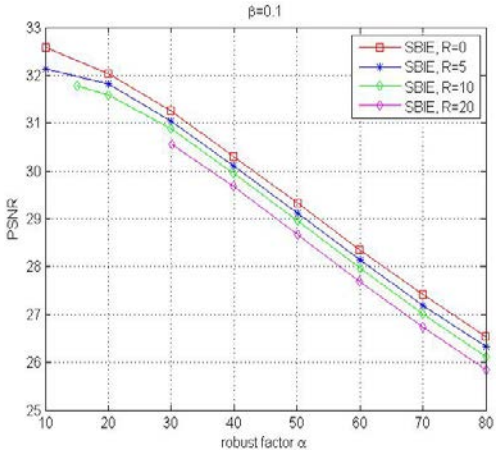

Figure 5: PSNR performace vs. robust factor.

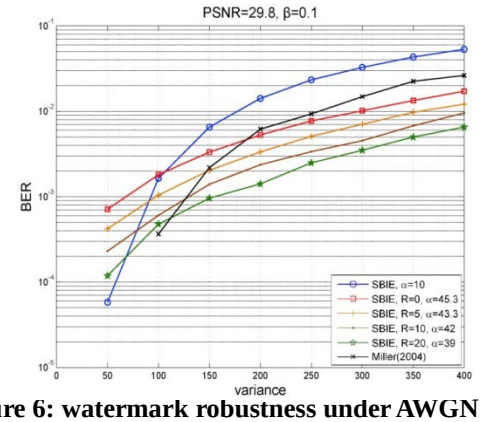

Figure 6: watermark robustness under AWGN

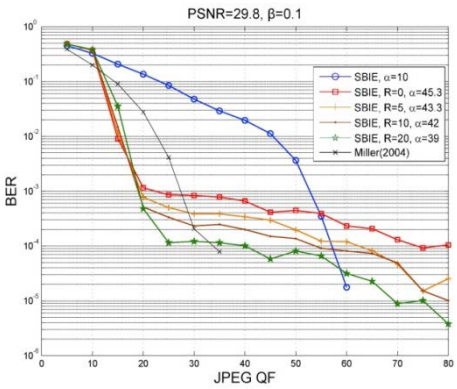

Figure 7: watermark robustness under JPEG compression.

2). Performance for parameters α and β

We simulated the fidelity, robustness and complexity by aiming at parameter α and β. The PSNR, as shown in Table 1, is presented as a function of α and increased with β. The parameter α is a constant controlling the embedding strength. We chose α to produce various robustness messages. The degradation in fidelity was measured using MSE distortion. For the large α value, the robustness is greater than for the small α value. Image quality depends on parameter β, the

iteration step factor. The higher the value of β, the lower average number of iterations required to reach the expected robustness of the objective codeword, with degrading image quality. Therefore, the value of β can be varied to change the operational complexity when the proposed algorithms are performed.

Table 1: Fidelity experiments with variant α and β

α	0	10	
PSNR	29.35	29.33	
BER($\sigma = 200$)	$1.2 * 10^{-2}$	$1.35 * 10^{-2}$	
β	0.025	0.05	
PSNR	29.87	29.82	
Number of iteration	8.34	6.32	
30	40	50	20
28.38	27.78	26.97	29.02
$2.24 * 10^{-3}$	$8.56 * 10^{-4}$	$12.34 * 10^{-5}$	$0.038 * 10^{-2}$
0.1	0.125	0.15	0.075
28.65	27.71	26.55	29.25
2.43	1.54	1.26	4.58

3). Computational complexity

We compared the algorithm complexity in [13] and that proposed in this study. The proposed algorithms for minimizing the distortion of the changes of watermarked images (Subsection 3.1) and minimizing the amplitude of the watermarked image (Subsection 3.2) incur major computational complexity. The number of codewords in the trellis section is restricted to the trellis structure of convolutional codes, and the total number of arcs is small. Therefore, the proposed algorithm in Subsection 3.1 easily obtained the optimal codeword candidate and only consumed a number of operational complexities. For the SBIE algorithm in Subsection 3.2, the Add-Compare-Select (ACS) operation in each section in the memory or the accumulated Viterbi algorithm leads to a more complex embedding algorithm, such as that in Miller's work, compared to that of a memoryless structure of operational complexity. Thus, three complexity parameters in the trellis structure are defined as follows: The decoding process in ours and Miller's algorithms are both based on the Viterbi algorithm. Assuming that there are C_a number of arcs in each trellis section, it is required to calculate the same number of Euclidean distances. With C_e symbolizing the complexity in evaluating each Euclidean distance, a total complexity of $C_a \times C_e$ is required for each section. In addition, the survival path depends on the ACS operations in each section, and the different informed embedding algorithm yields different number of ACS operations. Consequently, for the same length of the watermarked images, the computational complexity is directly related to the average number of ACS operations in each section. A larger number of ACS operations yield a higher complexity and a longer period to perform the operations. Assuming a trellis with 16 states, each with 2 arcs, the metric accumulated in the previous section pertains to the trellis states and the number of arcs. Because each current state is connected to two arcs, two adders are thus required to perform additions, which necessitate C_a number of adders in each section. Inasmuch as there are two arcs connected to each next state, a comparer is thus required for comparison. In brief, there are 16 next states and 32 arcs in each section, that is, 16 comparers and 32 adders. Hence, the ACS complexity C_s for each section is given as

$$C_s = C_a \times C_e + C_a \times adders + C_a \times comparers \quad (30)$$

As presented in Subsection, the proposed algorithm is a section-based informed embedding algorithm (i.e., a memoryless informed embedding approach performed independently in each section) that does not require any adder or comparer to perform accumulation operations. However, there are C_a number of comparers required in a search of all arcs for an object message codeword. The resultant complexity is expressed as

$$C_a \times C_e + C_a \times comparers \quad (31)$$

For operational complexity, the proposed algorithm must determine the minimal distance $d(\alpha c_k, x_k)$, regardless of whether the arc operation is closer to the selected codeword αw_k in the trellis section k. The computation required 16 comparer-operations. Finally, we compared with [13] and tabulated as Table 2.

Table 2: Number of operation for proposed algorithm and [13] algorithms

Algorithm	C_s
Proposed SBIE algorithm	$32 \times C_e$+16 comparers
[13]	$32 \times C_e$+ 32 adders+16 comparers
Algorithm	C_t
Proposed SBIE algorithm	$C_s \times 2.9643 \times 1585$
[13]	$C_s \times 72.651 \times 1585$

The experimental results in Table 2 confirm that our proposed scheme not only provides high embedding capacity with the adaptive parameter m_1, but also obtains low operational complexity compared to Miller's algorithm.

5. Conclusions

The paper proposed an informed embedding scheme for adaptive digital watermarking and used a modified trellis structure and nested simplex code to embed messages. These proposed algorithms used nested linear block codewords to label the trellis arcs, and subsequently adjusted the embedding rate and robustness of the watermarked images by using numerous controllable parameters. Although Miller's work offers good bit error rate performance, our experimental results confirm that the proposed algorithm possesses a higher embedding rate and lower complexity than that of Miller's work. The proposed algorithm provides two advantages: (1) An adaptive design of watermarking system (i.e., the tradeoff between the BER and the embedding complexity), and the embedding rate that can be easily altered to meet various applications. (2) The computation complexity, which requires less operation complexity compared with Miller's informed embedding method.

Acknowledgment

This study is supported in part by the National Science Council of the Republic of China under contract numbers NSC-101-2221-E-167-026 and NSC-102-2221-E-167-001.

References

[1] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*, New York: Morgan Kaufmann, 2001.

[2] P. Moulin and R. Koetter, "Data-hiding codes," *Proc. IEEE*, vol. 93, no. 12, pp. 2083-2126, Dec. 2005.

[3] I. J. Cox, M. L. Miller, and A. McKellips, "Watermarking as communications with side information," *Proc. IEEE*, vol. 87, pp. 1127-1141, Jul. 1999.

[4] M. H. M. Costa, "Writing on dirty report," *IEEE Trans. Inf. Theory*, vol. 29, pp. 439-441, 1993.

[5] Y. Sun, Y. Yang, A. D. Liveris, V. Stankovic, and Z. Xiong, "Near-capacity dirty-report code design: a source- channel coding approach," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3013-3031, Jul. 2009.

[6] R. Barron, B. Chen, and G. W. Wornell, "The duality between information embedding and source coding with side information and some applicaitons," *IEEE Trans. Inf. Theory*, vol. 49, no. 5, pp. 1159-1180, May 2003.

[7] S. S. Pradhan, J. Chou, and K. Ramchandran, "Duality bewteen source coding and channel coding and its extension to the side information case," *IEEE Trans. Inf. Theory*, vol. 49, no. 5, pp. 1181-1203, May 2003.

[8] R. Crandall. Some notes on steganography. Steganography Mailing List, 1998.

[9] J. Bierbrauer. On CrandallD's problem. Personal Communication, 1998.

[10] F. Galand and G. Kabatiansky. Information hiding by coverings. In Proceedings ITW2003, Paris, France, pp. 151–154, 2003.

[11] M. van Dijk and F. Willems. Embedding information in grayscale images. In Proceedings of the 22nd Symposium on Information and Communication Theory in the Benelux, Enschede, The Netherlands, pp. 147–154, May 2001.

[12] R. Zamir, S. Shamai, and U. Erez, "Nested linear/lattice codes for structured multierminal binning," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1250-1276, Jun. 2002.

[13] M. L. Miller, G. J. Doerr, and I. J. Cox, "Applying informed coding and embedding to design a robust high- capacity watermark," *IEEE Trans. Image Process.*, vol. 13, no. 6, pp. 792-807, Jun. 2004.

[14] M. L. Miller, I. J. Cox, and J. A. Bloom, "Informed embedding: exploiting image and detector information during watermark insertion," IEEE Int. Conf. on Image Processing, Sep. 2000.

[15] Chun-Shien Lu, "Towards robust image watermarking: combining content-dependent key, moment normalization, and side-informed embedding," *Signal Processing: Image Communication*, vol. 20, Issue 2, pp. 129-150, Feb. 2005.

[16] Claude Desset, Benot Macq, Luc Vandendorpe, "Block error-correcting codes for systems with a very high BER: Theoretical analysis and application to the protection of watermarks," *Signal Processing: Image Communication*, vol. 17, Issue 5, pp. 409-421, May 2002.

[17] L. Lin, G. Doerr, I. Cox, and M. Miller, "An efficient algorithm for informed embedding of dirty-report trellis codes for watermarking," *in* Proc. IEEE Int. Conf. Image Processing, Italy, 2005.

[18] [M. J. Wainwright, "Sparse graph codes for side information and binning," *IEEE Signal Processing Mag.*, vol. 24, no. 5, pp. 47-57, Sep. 2007.
[19] J. J. Wang and H. Chen, "A Suboptimal Embedding Algorithm With Low Complexity for Binary Data Hiding," IEEE International Conference on Acoustics' Speech, and Signal Processing (ICASSP), pp. 165-168, June 2012.
[20] J. J. Wang, H. Chen, C.Y. Lin and T. Y. Yang, "An embedding strategy for large payload using convolutional embedding codes," IEEE International Conference on ITS Telecommunications, pp.408-412, Nov. 2012.
[21] J. J. Wang, H. Chen, and C. Y. Lin , "An Adaptive Matrix Embedding Technique for Binary Hiding With an Efficient LIAE Algorithm", *WSEAS Transactions on Signal Processing*, Issue 2, Vol. 8, pp. 64-75, April 2012.
[22] G. D. Forney, "The Viterbi algorithm," *Proc. IEEE*, vol. 61, pp. 268-278, Mar. 1973.

Chi-Yuan Lin received the B.S. degree in Electronic Engineering from National Taiwan University of Science and Technology, Taiwan, in 1988, the M.S. degree in Electronic and Information Engineering from National Yunlin University of Science and Technology, Taiwan, in 1998, and the Ph.D. degree in Electrical Engineering from National Cheng Kung University, Taiwan, in 2004. Since 1983, he has been with the Department of Electronic Engineering at National Chin-Yi University of Technology in Taiwan where he is now an associate professor. His research interests include neural networks, multimedia coding, data hiding, and image processing.

Jyun-Jie Wang received the B.S. degree in Electronic Engineering from National Chi Yi University of Science and Technology, Taiwan, in 2003, the M.S. degrees and the Ph.D. degree in Electrical Engineering from National Chung Hsing University, Taiwan, in 2005 and 2012, respectively. He is also a member of IEEE. His research interests include multimedia, image processing, watermarking, information theory and coding theory.