DIRTY-PAPER TRELLIS CODES FOR WATERMARKING

Matt L. Miller, Gwenaël J. Doërr, Ingemar J.Cox

ABSTRACT

Informed coding is the practice of representing watermark messages with patterns that are dependent on the cover Works. This requires the use of a *dirty-paper code*, in which each message is represented by a large number of alternative vectors. Most previous dirty-paper codes are based on lattice codes, in which each code vector, or pattern, is a point in a regular lattice. While such codes are very efficient to implement, they suffer from inherent weakness against valumetric scaling, such as changes in audio volume or image brightness.

In the present paper, we present an alternative to lattice codes that is *inherently* robust to valumetric scaling. This code is based on a trellis that has been modified so that each bit value may be coded by traversing several alternative arcs. A Viterbi decoder is used in the detector to identify the path with the highest correlation to the input Work. Since relative correlation values are unaffected by valumetric scaling, the same message will be detected no matter how the input has been scaled.

1. INTRODUCTION

In recent years, several researchers [8, 1, 4] have recognized that watermarking with blind detection can be modeled as communication with side-information at the transmitter [17]. This realization has led to the design of algorithms for *informed embedding* and *informed coding*. In informed embedding, each watermark pattern is tailored according to the cover Work, attempting to attain an optimal trade-off between estimates of perceptual fidelity and robustness. In informed coding, a watermark is represented with a pattern that is dependent on the cover Work. The reader is directed to [7] for a detailed discussion of these concepts.

The use of informed coding in watermarking was inspired by the results of Costa [6]. Costa studied the capacity of a communications channel that consists of two additive, white Gaussian noise sources, the first of which is completely known to the transmitter, while the receiver has no knowledge of either. Surprisingly, Costa showed that the first noise source has no effect on channel capacity. Costa's work was first brought to the attention of the watermarking community by Chen, who realized that the cover Work is analogous to the first noise source [3]. More recently, Moulin and O'Sullivan [15] extended Costa's analysis to more realistic models of watermarking.

The implication of Costa's analysis to watermarking is substantial – it implies that the channel capacity of a watermarking system should be independent of the cover Work. That is, in principle, the data payload of a watermarking system need not be limited by interference from the cover Work. Since, in most early watermarking systems, this interferance is the *dominant* limit on payload, the idea that its effect can be *eliminated* holds the promise of watermarks with vastly higher data payloads.

Realizing this promise, however, is not trivial. Costa's proof involves the use of a special type of code, which we refer to as a *dirty-paper code*. He showed how to build suitable random dirty-paper codes, but did not address the practical problem of efficient search. With random dirty-paper codes and exhaustive search, it is only possible to implement watermarks with very limited payloads (see, for example, the system studied in [11]). Thus, if we are to achieve large data payloads, we must introduce a structured code that allows for more efficient searches.

Most of the structured codes that have been proposed [1, 10] are built around the idea of a lattice code. Here, all the code vectors lie on a regular lattice, and each message is represented by the set of vectors on one sub-lattice. These codes are efficient to implement, and allow for very large payloads without seriously distorting the cover Works. However, lattice codes are inherently susceptable to valumetric scaling (multiplication of every audio sample or pixel by a constant scaling factor). This means that a simple distortion such as changing audio volume or image brightness can render lattice-coded watermarks undetectable. Some researchers have suggested solving this problem by performing non-linear projections that are invariant to valumetric scaling [16, 2]. More recently, Eggers, Bäuml, and Girod [9] have proposed a method for estimating and inverting valumetric scaling at the detector.

In the present paper, we present an alternative to lattice codes that is *inherently* robust to valumetric scaling, and so may be used without non-linear projections or estimation of the scaling parameter. It is also suitable for use with the informed embedding method described in [14]. In Section 2 we review the basic idea of dirty-paper codes. Section 3 then presents our novel dirty-paper code. We test this code experimentally in Section 4, showing that it outperforms a comparable blind coding method in a simple image watermarking system. Finally, Section 5 presents some conclusions.

2. DIRTY-PAPER CODES

In a dirty-paper code, each message is represented by a variety of alternative vectors. Using a dirty-paper code[1], $\mathcal{W}$, to transmit a message, m, over a dirty-paper channel, the transmit-

Matt L. Miller and Ingemar J. Cox are with the NEC Research Institute, Princeton, NJ, 08540 USA.

Gwenaël J. Doërr is with the Eurécom Institute, Sophia-Antipolis, France.

[1]Our notation here differs from that used by Costa. Rather than denoting code vectors with $\mathcal{U}$ and $\mathbf{u}$, we use $\mathcal{W}$ and $\mathbf{w}$ to emphasize their relationship to watermark patterns. Furthermore, we denote the signal from the first noise source with $\mathbf{c_o}$, to emphasize its relationship with the original cover Work.

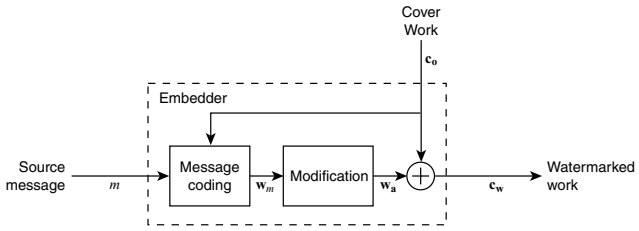

Fig. 1. *Structure of embedder with informed coding and blind embedding. The coding of the watermark message, m, is dependent on the cover Work, $\mathbf{c_o}$. The modification of the resulting pattern, $\mathbf{w}$, is independent of $\mathbf{c_o}$.*

ter performs the following steps:

1. Identify a coset of the code, $\mathcal{W}_m \subset \mathcal{W}$, associated with the desired message. This is the set of all vectors that can represent message m.
2. Search through $\mathcal{W}_m$ to find the code vector, $\mathbf{w}$, that is closest to the vector, $\mathbf{c_o}$, which will be added by the first noise source (i.e. $\mathbf{w}$ is the vector that is most similar to the cover Work, $\mathbf{c_o}$).
3. Transmit $\mathbf{w_a} = f(\mathbf{w}, \mathbf{c_o})$, where $f(\cdot,\cdot)$ is a function that is analogous to informed embedding [12]. In Costa's construction, $f(\mathbf{w}, \mathbf{c_o}) = \mathbf{w} - \alpha\mathbf{c_o}$, where α is a constant.

To decode a received signal, $\mathbf{c}$, using a dirty paper code, $\mathcal{W}$, the receiver performs the following steps:

1. Search the entire codebook for the closest code vector, $\hat{\mathbf{w}}$.
2. Identify the coset, $\mathcal{W}_{\hat{m}} \subset \mathcal{W}$, that contains $\hat{\mathbf{w}}$, and report reception of the message, $\hat{m}$, associated with that subset.

In this paper, we focus on the design of the dirty-paper code itself, and not the function $f(\cdot,\cdot)$ employed in step 3 of the transmitter (embedder). For this reason, the tests reported in Section 4 were conducted using blind embedding, where $f(\mathbf{w}, \mathbf{c_o}) = \alpha\mathbf{w}$ (this is considered *blind* because it is independent of $\mathbf{c_o}$). Thus the embedder used in those tests was structured as shown in Figure 1. In [13], we combine the present informed coding method with the informed embedding method of [14].

3. DIRTY-PAPER TRELLIS CODES

A practical dirty paper code must be structured in a way that allows efficient search in both the watermark embedder (transmitter) and detector (receiver). In the detector, we must quickly search the entire code to find the vector, $\hat{\mathbf{w}}$ that is closest to a given received Work, $\mathbf{c}$. This is the same as the problem handled in traditional error-correction codes (ECC's). In the embedder, however, we must search a *subset* of the code to find the vector, $\mathbf{w}$, that is closest to a given cover Work, $\mathbf{c_o}$. Traditional ECC's are not designed to allow efficient search of such subsets, so novel codes must be developed. In this section, we propose a simple modification of a trellis code to produce a dirty-paper code.

3.1. Traditional trellis codes

Figure 2 shows an example of a traditional trellis code. Each possible message corresponds to a path through the trellis from

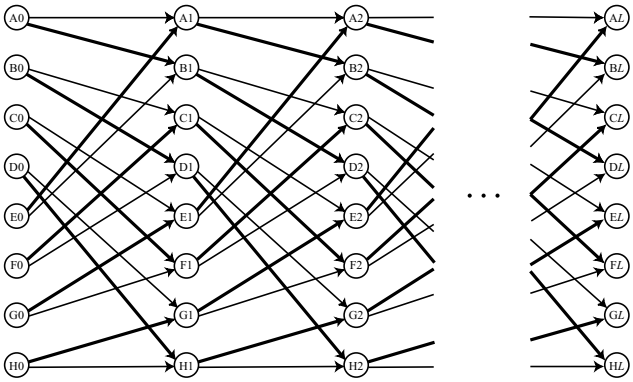

Fig. 2. *Simple, 8-state trellis.*

node A0 (state A at time 0) to one of the nodes at the right (any state at time L). We refer to the transition from one column of nodes to the next column of nodes as a *step*, and each such step corresponds to one bit in the coded message. A bold arc is traversed if the corresponding bit is a 1, a non-bold arc is traversed if the corresponding bit is a 0.

Each arc in the trellis is labelled with a randomly-generated, length N vector. Each path, and thus each message, is coded with a length $L \times N$ vector that is the concatenation of the labels for the arcs it contains. This vector can be used as a watermark pattern.

3.2. Proposed modification

To create a dirty paper code, the trellis is modified so that multiple alternative code vectors can be obtained for each message. The basic idea is to have more than two arcs enter and exit each state, but still use each step of the trellis to encode a single bit. An example is shown in Figure 3. This code has 8 states and 4 arcs per state. Two of the 4 arcs exiting each state are bold, representing 1 bits, and two are non-bold, representing 0 bits. Thus, a given message can be represented by a number of different paths, and hence a number of different length $L \times N$ code vectors. We further increase the number of possible vectors for each message by allowing paths to start at any state at the left.

The number of possible vectors for each message is easy to calculate. Assume we have a code with S states and A arcs per step, so A/S arcs exit and enter each state. The number, n, of alternative code vectors for representing a given L-bit message is

$$n = S\left(\frac{A}{2S}\right)^L. \tag{1}$$

We must now define how the embedder selects a path from the set of paths that represent the desired message. Conceptually, this can be thought of as being done in two steps. First, we modify the trellis to eliminate all paths that *do not* encode the desired message. This is a simple matter of removing bold arcs from steps that should encode 0's, and removing non-bold arcs from steps that should encode 1's. In the resulting trellis, *every* possible path represents the desired message. An example of such a modified trellis is shown in Figure 4. This modified trellis can be

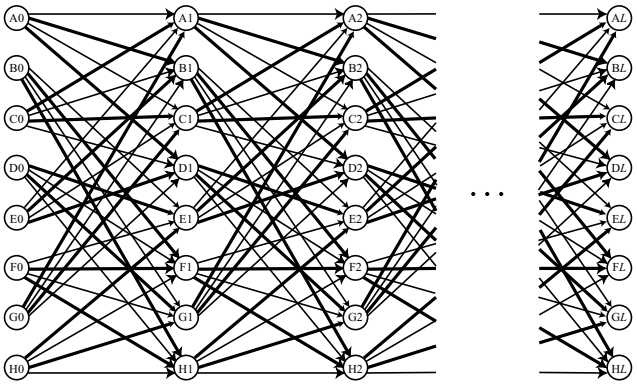

Fig. 3. *Dirty-paper trellis with 8 states and 4 arcs per state.*

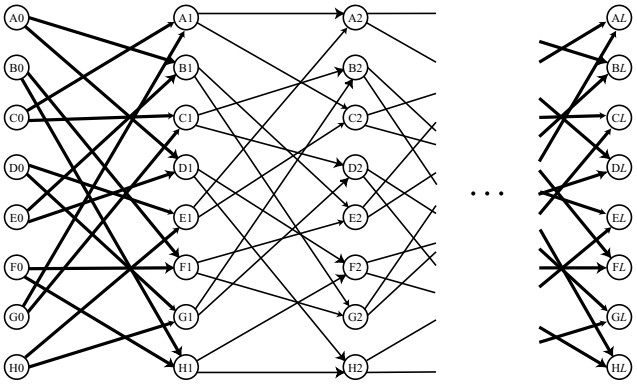

Fig. 4. *Version of the dirty-paper trellis in Figure 3 modified to represent a message beginning with binary* 1 0 0 *and ending with* 1. *The first step in this trellis, from states* A0 ... H0 *to states* A1 ... H1, *has been modified by removing all the non-bold arcs, so every path represents a message that begins with* 1. *The second step, from* A1 ... H1 *to* A2 ... H2, *has had all the bold arcs removed, so the second bit in every path is a* 0. *And so on to the last step.*

thought of as a compact representation of the code vector coset, $\mathcal{W}_m$.

Second, we apply the Viterbi decoding algorithm [18] to the cover Work, $\mathbf{c_o}$, to find the path through the modified trellis that yields the highest correlation. The length $L \times N$ vector for this path is the closest code vector, $\mathbf{w} \in \mathcal{W}_m$.

During the detection process, the detector applies the Viterbi algorithm using the *entire* trellis. This identifies the path that yields the highest correlation with the received Work, $\mathbf{c}$. The received message is then decoded by looking at the bits represented by the arcs in that path.

Note that, because the detector finds the code vector with the highest correlation to the received Work, and valumetric scaling scales all correlations by a constant, detection will not be effected by valumetric scaling. That is, if a vector for message m has the highest correlation with $\mathbf{c}$, then it will also have the highest correlation with $k\mathbf{c}$ ($k > 0$).

3.3. Trellis structure

Given the general framework of this code, the trellis may have many possible structures. In particular, different combinations of numbers of arcs, A, and states, S, can have different impacts on the effectiveness of the system.

- If the number of arcs per state is greater than the number of states ($A/S > S$), there will be some *parallel* arcs in the trellis, i.e there will be several arcs linking the same pair of states.
- If the number of arcs per state is equal to the number of states ($A/S = S$), the trellis is fully connected i.e. each state is connected exactly once with itself and every other state.
- If the number of arcs per state is lower than the number of states ($A/S < S$), not all the states can be reached from any given state.

After some experimentation (see [13]), we decided that the best case may be the one in which the number of arcs per state is equal to the number of states ($A/S = S$).

4. EXPERIMENTS AND RESULTS

To test the effect of using the code described above, we implemented a simple image watermarking system. The embedder for this system performed the following steps:

1. Convert the image into the 8×8 block-DCT domain.
2. Place low-frequency AC terms of the blocks into a single, length $L \times N$ vector, $\mathbf{v}$, in random order. We refer to this as the *extracted vector*.
3. Use a dirty-paper trellis code to encode the desired message, m, into a watermark vector, $\mathbf{w}$. This was done by running Viterbi's algorithm on $\mathbf{v}$ using a trellis modified for message m.
4. Embed $\mathbf{w}$ into $\mathbf{v}$ with blind embedding: $\mathbf{v_w} = \mathbf{v} + \alpha\mathbf{w}$, where α is the embedding strength.
5. Place the values of $\mathbf{v_w}$ into the low-frequency AC terms of the block-DCT of the cover image, in the same order as used in step 2.
6. Convert the image back into the spatial domain. This resulted in an image that, when input to the extraction process of steps 1 and 2, would yield the vector $\mathbf{v_w}$.

The detector performed the following steps[2]:

1. Extract a vector, $\hat{\mathbf{v}}$, from the image in the same manner as in steps 1 and 2 of the embedding algorithm.
2. Apply the Viterbi algorithm to $\hat{\mathbf{v}}$, using the whole trellis, to identify the path whose code vector yields the highest correlation.
3. Report that the message associated with the path found in step 2, $\hat{m}$, is embedded in the image.

Our trellis had 64 states and 64 arcs per state. Each arc was labeled with a vector of length $N = 128$. The label for each 1 arc was drawn from an independent, identically distributed Gaussian

[2]Note that this detection algorithm did not attempt to determine whether or not the image contained a watermark.

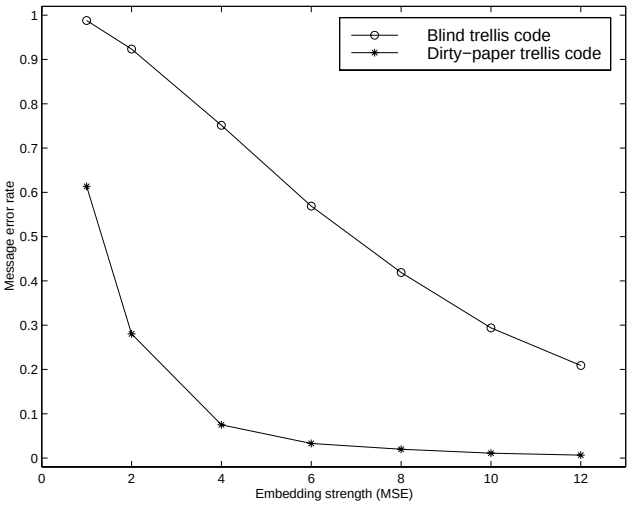

Fig. 5. *Embedding effectiveness results for 2000 images.*

distribution. The label for each 0 arc was the negation of one of the 1-arc labels from the same node. The labels were scaled so that the mean squared error (MSE) between marked and unmarked images would equal the embedding strength, α.

The images used for the test were 368×240 pixels. We used the 12 lowest-frequency AC coefficients from each 8×8 block, giving us a total of $12 \times (368 \times 240/64) = 16560$ coefficients. We discarded 48 randomly-chosen coefficients to obtain an extracted vector of length $L \times N = 16512$. With $N = 128$, this enabled us to embed $L = 129$ bits.

For comparison, we also implemented a watermarking system with blind coding. This system was essentially the same as the informed-coding system, except that it employed a 64-state traditional trellis code (2 arcs per state).

Both the informed-coding and blind-coding embedders were used to embed random watermarks in 2000 images from the Corel database [5] with various embedding strengths. The watermarked images were then decoded by their respective watermark detectors. If even one bit of the detected message differed from the embedded message, we counted this as a message error, or failure to embed.

Figure 5 shows the results. At an embedding strength of 2, the system with informed coding succeeded in embedding watermarks into more than 70% of the images. This level of distortion and embedding effectiveness might be acceptable for several applications. In contrast, blind coding did not achieve similar levels of embedding effectiveness until the embedding strength was raised to 10, at which point the watermark was quite visible.

5. CONCLUSIONS

We have presented a novel, structured dirty-paper code based on a modified trellis code. Unlike most structured dirty-paper codes presented to date, our code is not based on a lattice and is inherently robust against valumetric scaling. We have shown experimentally that use of this code can significantly improve embedding effectiveness for a 129-bit watermark.

However, by itself, this method does not allow for payloads much larger than that we tested. For larger payloads – on the order of 1000 bits in our 368×240 images – the method must be combined with methods for informed embedding and perceptual shaping. In another paper, we report results obtained with such a combined system [13]. There, we succeed in embedding 1380 bits into images in a manner that is robust to substantial valumetric distortions, including increasing and decreasing image brightness, addition of white noise, significant low-pass filtering, and JPEG compression with a quality factor of 30%. The present informed coding method is critical to achieving those results.

6. REFERENCES

[1] B. Chen and G. W. Wornell. An information-theoretic approach to the design of robust digital watermarking systems. *IEEE Transactions on Acoustics, Speech, and Signal Processing*, 1999.

[2] B. Chen and G. W. Wornell. Preprocessed and postprocessed quantization index modulation methods for digital watermarking. In *Security and Watermarking of Multimedia Contents II*, volume SPIE-3971, pages 48–59, 2000.

[3] B. Chen and G. W. Wornell. Quantization index modulation: A class of provably good methods for digital watermarking and information embedding. In *Proc. Int. Symp. Inform. Theory (ISIT-2000)*, 2000.

[4] Jim Chou, S. Sandeep Pradhan, and Kannan Ramchandran. On the duality between distributed source coding and data hiding. *Thirty-third Asilomar conference on signals, systems, and computers*, 2:1503–1507, 1999.

[5] Corel Stock Photo Library 3, Corel Corporation, Ontario, Canada.

[6] M. Costa. Writing on dirty paper. *IEEE Trans. Inform. Theory*, 29:439–441, 1983.

[7] I. J. Cox, M. L. Miller, and J. A. Bloom. *Digital Watermarking*. Morgan Kaufmann, 2001.

[8] I. J. Cox, M. L. Miller, and A. McKellips. Watermarking as communications with side information. *Proc. IEEE*, 87(7):1127–1141, 1999.

[9] J. J. Eggers, R. Bäuml, and B. Girod. Estimation of amplitude modifications before scs watermark detection. In *Proc. of SPIE on Security and Watermarking of Multimedia Contents*, volume 4675, 2002.

[10] J. J. Eggers, J. K. Su, and B. Girod. A blind watermarking scheme based on structured codebooks. In *IEE Seminar on Secure Images and Image Authetication*, pages 4/1–4/21, 2000.

[11] M. L. Miller. Watermarking with dirty-paper codes. In *IEEE International Conference on Image Processing*, September 2001.

[12] M. L. Miller, I. J. Cox, and J. A. Bloom. Informed embedding: Exploiting image and detector information during watermark insertion. In *IEEE International Conference on Image Processing*, September 2000.

[13] M. L. Miller, G. J. Doërr, and I. J. Cox. Applying informed coding and embedding to design a robust, high capacity watermark. *Submitted to IEEE Transactions on Image Processing*.

[14] M. L. Miller, G. J. Doërr, and I. J. Cox. Informed embedding for multi-bit watermarks. *Submitted to The 6th Int. Conf. on Signal Processing*.

[15] P. Moulin and J. A. O'Sullivan. Information-theoretic analysis of information hiding. *preprint*, available from http://www.ifp.uiuc.edu/m̃oulin/Papers, 1999.

[16] R. Petrovic, J. M. Winograd, K. Jemili, and E. Metois. Data hiding within audio signals. In *Fourth International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services*, 1999.

[17] C. E. Shannon. Channels with side information at the transmitter. *IBM Journal of Research and Development*, pages 289–293, 1958.

[18] A. J. Viterbi. *CDMA: principles of spread spectrum communications*. Addison Wesley Longman Inc., 1995.