TRANSFORM CODER IDENTIFICATION

Marco Tagliasacchi* *Marco Visentini-Scarzanella*† *Pier Luigi Dragotti*† *Stefano Tubaro**

* Dipartimento di Elettronica e Informazione, Politecnico di Milano
† EEE Department, Imperial College London

ABSTRACT

The widespread popularity of transform coding has made it central to a wide range of methods in forensics, quality assessment and digital restoration. However, most approaches require prior knowledge of the transform coding parameters. In this paper, we consider the challenging problem of identifying the transform matrix as well as the quantization step sizes of a transform coder, given a set of P non-overlapping N-dimensional vectors observed as its output. We formulate the problem in terms of finding the lattice with the largest determinant that contains all observed vectors and we propose an algorithm that is able to find the optimal solution. Our experimental analysis shows that the probability of success of the algorithm quickly approaches 1 for small values of $(P - N)$. The complexity of the proposed algorithm grows linearly with the dimensionality N.

Index Terms— Transform coding, lattice theory.

1. INTRODUCTION

The possibility of reverse-engineering complex chains of operators starting from the available output signals has a great potential for applications in a wide range of scenarios including, e.g.,: i) forensics, in order to address tasks such as source device identification [1] or tampering detection [2][3]; ii) quality assessment, to enable no-reference methods that rely solely on the received signals [4][5]; iii) digital restoration, which requires prior knowledge about the chain of operations that affected a digital signal [6].

Signals are often compressed in a lossy coding format. Transform coding [7] is, by far, the most widely adopted coding tool for lossy compression of signals with memory, as indicated by its adoption in all multimedia communication standards. As such, several works exploited the footprints left by transform coding in the literature in the case of single [8], double [9][3] or multiple [10] JPEG compression. Similar techniques were also applied to video signals [11][12][13][14][15].

All the aforementioned works require prior knowledge of the type of standard being considered. This implies that the specific transform in use is assumed to be known, whereas the quantization step sizes need to be estimated. Although earlier standards (e.g., JPEG, MPEG-2 and MPEG-4) adopted the Discrete Cosine Transform (DCT) on 8×8 blocks, more recent coding architectures (e.g., JPEG2000 [16], H.264/AVC [17], HEVC [18]) are more diversified in terms of both the type of transform being used and the block size. These differences were recently exploited in [19] to identify the video coding standard used to compress a sequence.

Given the centrality of transform coding in multimedia applications, it is natural to try and develop a universal theory of transform coder identification that is independent of the specific application at hand. To this end, in this paper we consider a general model of transform coding that can be tailored to describe a large variety of practical implementations that are found in lossy coding systems, including those adopted in multimedia communication.

Given the output produced by a specific transform coding chain, we investigate the problem of identifying its parameters. We assume both the size and the alignment of the transform to be known, as they can be estimated with methods available in the literature [12][8]. We propose an algorithm that receives as input a set of P transform decoded vectors embedded in a N-dimensional vector space and produces as output an estimation of the transform adopted, as well as the quantization step sizes. We propose an algorithm that is able to solve the problem and we formally study its convergence properties. Our analysis shows that it is possible to successfully identify both the transform and the quantization step sizes with high probability when $P > N$. In addition, the complexity of the algorithm is shown to grow linearly with N.

The proposed method is related to Euclid's algorithm, which is used to find the greatest common divisor (GCD) between two integer numbers. Euclid's algorithm finds application in the analysis of 1-dimensional signals, e.g., to determine the periodicity of signals from incomplete observations [20][21]. This is equivalent to estimating the step size of a scalar quantizer, since the transform is trivially defined. Conversely, the proposed method is tailored to work with N-dimensional signals, thus broadly enriching the scope of the applications that can be addressed.

To the best of the authors' knowledge, the problem of identifying a linear mapping based on the footprint left by quantization was addressed only in [22], with the goal of investigating the color compression history, i.e., the colorspace used in JPEG compression. However, the solution proposed in [22] is tailored to work in a 3-dimensional vector space, thus avoiding the challenges that arise in higher dimensional spaces.

2. BACKGROUND ON LATTICE THEORY

In this section we provide the necessary background on lattice theory. Further details can be found, e.g., in [23][24][25]. The symbols x, $\mathbf{x}$ and $\mathbf{X}$ denote, respectively, a scalar, a column vector and a matrix. A $M \times N$ matrix $\mathbf{X}$ can be written in terms of its columns, $\mathbf{X} = [\mathbf{x}_1, \ldots, \mathbf{x}_N]$. Let $\mathcal{L}$ denote a lattice of full rank embedded in $\mathbb{R}^N$. Let $\mathbf{B} = [\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_N]$, $\mathbf{b}_i \in \mathbb{R}^N$, denote a basis for the lattice $\mathcal{L}$. That is,

$$\mathcal{L} = \{\mathbf{x} \in \mathbb{R}^N | a_1\mathbf{b}_1 + a_2\mathbf{b}_2 + \ldots + a_N\mathbf{b}_N, a_i \in \mathbb{Z}\}. \quad (1)$$

In order to make the mapping between a basis and the corresponding lattice explicit, the latter can be expressed as $\mathcal{L}(\mathbf{B})$. Any lattice basis

The project REWIND acknowledges the financial support of the Future and Emerging Technologies (FET) programme within the Seventh Framework Programme for Research of the European Commission, under FET-Open grant number:268478.

also describes a fundamental parallelotope according to

$$\mathcal{P}(\mathbf{B}) = \left\{ \mathbf{x} \in \mathbb{R}^N | \mathbf{x} = \sum_{i=1}^{N} \theta_i \mathbf{b}_i, 0 \leq \theta_i < 1 \right\}. \qquad (2)$$

That is, $\mathcal{P}(\mathbf{B})$ is a parallelotope with one vertex in the origin and edges parallel to the basis vectors. When $N = 2, 3$, $\mathcal{P}(\mathbf{B})$ is, respectively, a parallelogram or a parallelepiped. Given a point $\mathbf{z} \in \mathbb{R}^N$, let $\mathcal{P}_{\mathbf{z}}(\mathbf{B})$ denote the parallelotope enclosing $\mathbf{z}$. $\mathcal{P}_{\mathbf{z}}(\mathbf{B})$ is obtained by translating $\mathcal{P}(\mathbf{B})$ so that its origin coincides with one of the lattice points. Figure 1(b) illustrates $\mathcal{P}_{\mathbf{z}}(\mathbf{B})$ as a shaded region for the vector $\mathbf{z} = \tilde{\mathbf{x}}_3$.

Different bases for the same lattice lead to different fundamental parallelotopes. However, the volume of $\mathcal{P}(\mathbf{B})$ is the same for all bases of a given lattice. This volume equals the so-called *lattice determinant*. If the lattice is full rank, the lattice determinant equals the determinant of the matrix $\mathbf{B}$, $|\mathcal{L}| = |\det(\mathbf{B})|$.

Let $\underline{\mathcal{L}}$ denote a sub-lattice of $\mathcal{L}$. That is, for any vector $\mathbf{x} \in \underline{\mathcal{L}}$, then $\mathbf{x} \in \mathcal{L}$. A basis $\underline{\mathbf{B}}$ for $\underline{\mathcal{L}}$ can be expressed in terms of $\mathbf{B}$ as $\underline{\mathbf{B}} = \mathbf{B}\mathbf{U}$, where $\mathbf{U}$ is such that $u_{ij} \in \mathbb{Z}$. Moreover, let $\det(\mathbf{U}) = \pm m$, then $|\underline{\mathcal{L}}|/|\mathcal{L}| = |\det(\mathbf{U})| = m$ and we say that $\underline{\mathcal{L}}$ is a sub-lattice of $\mathcal{L}$ of index m. For example, the lattice in Figure 1(d) is a sub-lattice of index 3 of the lattice in Figure 1(e).

3. PROBLEM STATEMENT

Let $\mathbf{x}$ denote a N-dimensional vector and $\mathbf{W}$ a transform matrix, whose rows represent the transform basis functions. Transform coding is performed by applying scalar quantization to the transform coefficients $\mathbf{y} = \mathbf{W}\mathbf{x}$. Let $\mathcal{Q}_i(\cdot)$ denote the quantizer associated to the i-th transform coefficient. We assume that $\mathcal{Q}_i(\cdot)$ is a scalar uniform quantizer with step size Δ_i, $i = 1, \ldots, N$. The reconstructed block in the original domain is given by $\tilde{\mathbf{x}} = \mathbf{W}^{-1}\tilde{\mathbf{y}}$, where $\tilde{y}_i = \mathcal{Q}_i(y_i)$.

Let $\{\tilde{\mathbf{x}}_1, \ldots, \tilde{\mathbf{x}}_P\}$ denote a set of P observed N-dimensional vectors, which are the output of a transform coder. Due to quantization, the unobserved vectors representing quantized transform coefficients $\{\tilde{\mathbf{y}}_1, \ldots, \tilde{\mathbf{y}}_P\}$ are constrained to belong to a lattice $\mathcal{L}_y$ described by the basis $\mathbf{B}_y = \text{diag}(\Delta_1, \ldots, \Delta_N)$. Therefore, the observed vectors belong to a lattice $\mathcal{L}_x$ described by the basis $\mathbf{B}_x = \mathbf{W}^{-1}\mathbf{B}_y$,

In this paper we study the problem of determining $\mathbf{B}_x$ from a finite set of $P \geq N$ distinct vectors $\{\tilde{\mathbf{x}}_1, \ldots, \tilde{\mathbf{x}}_P\}$. That is, we seek to determine the parameters of a transform coder based on the footprints left on its output. We propose an algorithm to solve this problem and we study its convergence properties.

Note that when determining $\mathbf{B}_x$, the proposed method does not make any assumption on the structure of the transform matrix $\mathbf{W}$. In the general case, given $\mathbf{B}_x$, it is not possible to uniquely determine the quantization step sizes Δ_i, $i = 1, \ldots, N$. However, in the important case in which $\mathbf{W}$ represents an orthonormal transform, the quantization step sizes can be immediately obtained since they are equal to the lengths of the columns of $\mathbf{B}_x$.

4. AN ALGORITHM FOR TRANSFORM IDENTIFICATION

In this section we propose an algorithm that is able to determine the parameters of a transform coder from its output, i.e., a set of observed vectors $\{\tilde{\mathbf{x}}_1, \ldots, \tilde{\mathbf{x}}_P\}$. This is accomplished by finding a suitable lattice $\mathcal{L}^*$ such that $\{\tilde{\mathbf{x}}_1, \ldots, \tilde{\mathbf{x}}_P\} \subset \mathcal{L}^*$. In Section 6 we show that $\mathcal{L}^* \equiv \mathcal{L}_x$ with high probability, provided that $P - N > 0$.

ALGORITHM 1: `TI` algorithm

```
Input:  Set of observed vectors $\mathcal{O} = \{\tilde{\mathbf{x}}_1, \ldots, \tilde{\mathbf{x}}_P\}$
Output:  A basis $\mathbf{B}$ of the lattice solution of (3)
 1. $\mathbf{B}^{(0)} = \texttt{initBasis}(\mathcal{O})$;
 2. $\mathcal{S} = \{\mathbf{b}_1, \ldots, \mathbf{b}_N\}; \mathcal{U} = \mathcal{O} \setminus \mathcal{S}; r = 0$;
 3. while card$\{\mathcal{U}\} > 0$;
 4.     Pick $\tilde{\mathbf{x}}$ in $\mathcal{U}$;
 5.     $\mathcal{U} = \mathcal{U} \setminus \{\tilde{\mathbf{x}}\}$;
 6.     $\mathcal{S} = \mathcal{S} \cup \tilde{\mathbf{x}}$;
 7.     $\mathbf{B}^{(r+1)} = \texttt{recurseTI}(\mathbf{B}^{(r)}, \mathcal{S})$;
 8.     $r = r + 1$
 9. end
```

The problem of determining a basis for the lattice $\mathcal{L}_x$ is complicated by the fact that we typically observe a finite (and possibly small) number of vectors P embedded in a possibly large dimensional space. More precisely, the number of lattice points is equal to $2^{N\bar{R}}$, where $\bar{R}$ denote the average number of bits allocated to transform coefficients. Hence, this number increases exponentially with the dimension N and in most cases of practical relevance $P \ll 2^{N\bar{R}}$.

Another issue arises from the fact that, for a set of vectors $\{\tilde{\mathbf{x}}_1, \ldots, \tilde{\mathbf{x}}_P\}$, there are infinitely many lattices that include all of them. Indeed, any lattice $\bar{\mathcal{L}}$ such that $\mathcal{L}_x \subset \bar{\mathcal{L}}$ is compatible with the observed set of vectors. In order to resolve this ambiguity, we seek the lattice $\mathcal{L}^*$ that maximizes the lattice determinant $|\mathcal{L}|$, within this infinite set of compatible lattices. That is,

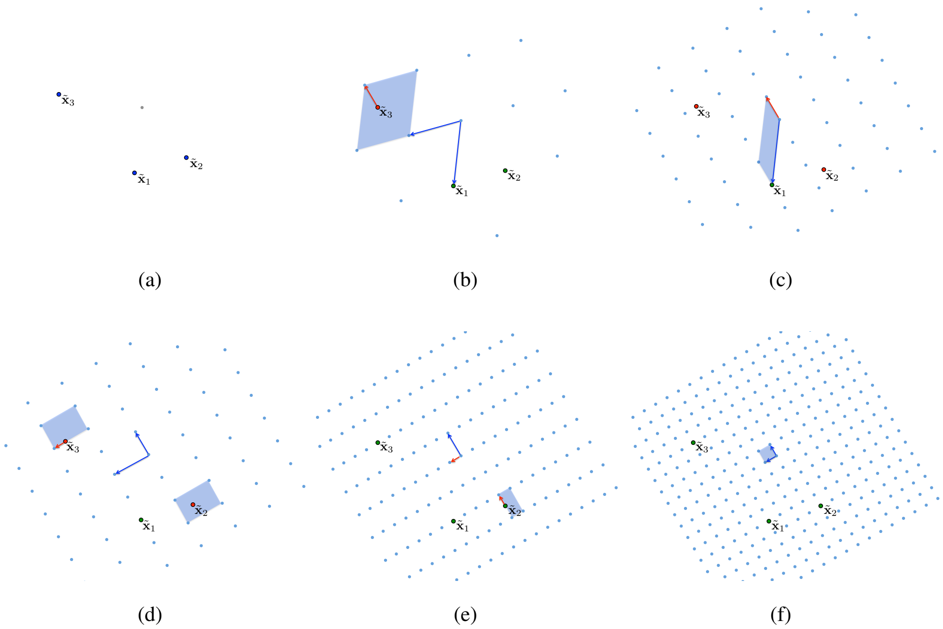
$$\begin{array}{ll} \underset{\mathcal{L}(\mathbf{B})}{\text{maximize}} & |\mathcal{L}(\mathbf{B})| \\ \text{subject to} & \{\tilde{\mathbf{x}}_1, \ldots, \tilde{\mathbf{x}}_P\} \subset \mathcal{L}(\mathbf{B}). \end{array} \qquad (3)$$

The proposed method used to solve the problem above is detailed in Algorithm 1. The method constructs an initial basis for an N-dimensional lattice (line 1). This is accomplished by considering the vectors in $\mathcal{O}$ until N linearly independent vectors are found. These vectors are used as columns of the starting estimate $\mathbf{B}^{(0)}$ and to populate the initial set of visited vectors $\mathcal{S}$. We denote with $\mathcal{U}$ the set of vectors in $\mathcal{O}$ that have not been visited yet. Then, the solution of (3) is constructed iteratively, by considering the remaining vectors in $\mathcal{U}$ one by one. At each iteration, the function `recurseTI` returns a basis for a lattice that solves (3), in which the constraint is imposed only on the subset of visited vectors $\mathcal{S}$, that is, $\mathcal{S} \subset \mathcal{L}(\mathbf{B})$. As such, the algorithm starts finding the solution of an under-constrained problem and additional constraints are added as more vectors are visited.

Figure 1 shows an illustrative example when $N = 2$ and three vectors $\{\tilde{\mathbf{x}}_1, \tilde{\mathbf{x}}_2, \tilde{\mathbf{x}}_3\}$ in Figure 1(a) are observed. The initial basis (line 1) is constructed using $\tilde{\mathbf{x}}_1$ and $\tilde{\mathbf{x}}_2$, since they are linearly independent. Then, the point $\tilde{\mathbf{x}}_3$ is selected (line 4) and the function `recurseTI` (line 10) is invoked returning a basis that solves (3), i.e., a basis with the largest lattice determinant that includes all observed vectors. Figure 1(f) illustrates such a basis.

The function `recurseTI` is detailed in Algorithm 2. It receives as input a set of visited vectors $\mathcal{S}$ and the current estimate of a basis $\mathbf{B}$ for the lattice $\mathcal{L}(\mathbf{B})$. In order to prevent numerical instability that might be induced by the inversion of the matrix $\mathbf{B}$, we perform basis reduction according to the LLL algorithm [26] (line 1) and we find a nearly orthogonal basis which is equivalent to $\mathbf{B}$, but has a smaller orthogonality defect. Figure 1(b) shows the reduced basis which is obtained from the initial basis $[\tilde{\mathbf{x}}_1, \tilde{\mathbf{x}}_2]$.

For each observed vector, we compute $\hat{\mathbf{x}} = \mathbf{B} \cdot \text{round}(\mathbf{B}^{-1}\tilde{\mathbf{x}})$, which represents one of the vertices of the parallelotope enclosing $\tilde{\mathbf{x}}$ (line 2 in Algorithm 2). If $\mathcal{S} \subset \mathcal{L}$, i.e., all the vectors in $\mathcal{S}$ belong to



(a) (b) (c)

(d) (e) (f)

Fig. 1. An example of transform identification. A set of three observed vectors is given in (a). Then, (b)-(h) show, step-by-step, how the solution to problem (3) is sought by Algorithm 1.

```
ALGORITHM 2: $\mathbf{B}_{\text{out}} = \texttt{recurseTI}(\mathbf{B}, \mathcal{S})$
Input:  Set of vectors $\mathcal{S} = \{\tilde{\mathbf{x}}_1, \ldots, \tilde{\mathbf{x}}_S\}$, a basis $\mathbf{B}$ of a lattice.
Output: A basis of a lattice $\mathcal{L}$ with maximum determinant $|\mathcal{L}|$,
        such that $\mathcal{S} \subset \mathcal{L}$
 1.  $\mathbf{B} = \texttt{LLL}(\mathbf{B})$
 2.  $\hat{\mathbf{x}}_i = \mathbf{B} \cdot \text{round}(\mathbf{B}^{-1}\tilde{\mathbf{x}}_i)$, $i = 1, \ldots, S$;
 3.  if $(\max_{j=1,\ldots,S} \|\tilde{\mathbf{x}}_j - \hat{\mathbf{x}}_j\|_2) = 0$
 4.      return $\mathbf{B}$
 5.  else
 6.      $f = \arg\min_{j \in \{l \mid \|\tilde{\mathbf{x}}_l - \hat{\mathbf{x}}_l\|_2 > 0\}} \|\tilde{\mathbf{x}}_j - \hat{\mathbf{x}}_j\|_2$;
 7.      $\mathbf{d} = \tilde{\mathbf{x}}_f - \hat{\mathbf{x}}_f$;
 8.      $\boldsymbol{\theta} = \mathbf{B}^{-1}\mathbf{d}$;
 9.      $l = \arg\min_{j \in \{p \mid \theta_p \neq 0\}} |\theta_j|$;
10.      $\mathbf{B}_{\text{out}} = \texttt{recurseTI}(\mathbf{B}_l, \mathcal{S})$; return $\mathbf{B}_{\text{out}}$;
11.  end
```

the lattice defined by $\mathbf{B}$, the recursion is terminated (line 3). Otherwise, one of the vectors $\mathbf{z} = \tilde{\mathbf{x}}_f$ that does not belong to $\mathcal{L}$ is selected as the one that minimizes the distance from the corresponding vertex (line 6), so as to minimize the length of the new basis vector $\mathbf{d}$. The intuition here is to capture a short vector that cannot be represented by the current lattice, and to modify the current basis in such a way that, upon convergence, it can be represented. Figure 1(b) shows the selected vector $\mathbf{z} = \tilde{\mathbf{x}}_3$, being the only one not belonging to $\mathcal{L}(\mathbf{B})$, as well as the corresponding difference vector $\mathbf{d}$.

Then, the updated basis is constructed by replacing one of the columns of $\mathbf{B}$ with $\mathbf{d}$. The choice of the new basis among the set of (up to) N candidate bases $\mathbf{B}_i$ (line 9) is to select the one that leads to the smallest lattice determinant, after excluding those that do not have rank N. From Cramer's rule, it follows that $\det(\mathbf{B}_i) = \theta_i \det(\mathbf{B})$, where $\boldsymbol{\theta} = \mathbf{B}^{-1}\mathbf{d}$ is the expansion of $\mathbf{d}$ in the basis $\mathbf{B}$. Hence, we replace the l-th column of $\mathbf{B}$, which is the one corresponding to the entry of $\boldsymbol{\theta}$ with the least strictly positive absolute value. Figure 1(c) shows the updated basis, obtained replacing one of the basis vectors with the difference vector identified in Figure 1(b).

The function `recurseTI` is recursively invoked (line 10), passing the updated basis as input. The basis shown in Figure 1(c) is reduced, as illustrated in Figure 1(d). In this case, neither $\tilde{\mathbf{x}}_2$ nor $\tilde{\mathbf{x}}_3$ belong to the lattice defined by the current basis. The vector $\tilde{\mathbf{x}}_3$ is selected (in this case, the tie between $\tilde{\mathbf{x}}_2$ and $\tilde{\mathbf{x}}_3$ is broken arbitrarily), and the corresponding difference vector is used to update the basis, as shown in Figure 1(e). A further recursive step is needed, since $\tilde{\mathbf{x}}_2$ does not belong to the current lattice, so as to lead to the solution illustrated in Figure 1(f), when the recursion can be terminated since all vectors belong to the lattice.

5. ANALYSIS OF CONVERGENCE

In this section we briefly illustrate a summary of the theoretical analysis of the proposed method. More details, including complete proofs are made available at [27].

Let $\mathbf{B}^{(0)}$ denote the initial estimate of a basis of the lattice. Let $\mathbf{B}^{(r)}$ denote the estimate obtained after the r-th call of the recursive function `recurseTI`. It is possible to prove the following lemma [27]:

Lemma 5.1. $|\mathcal{L}(\mathbf{B}^{(r+1)})| \leq |\mathcal{L}(\mathbf{B}^{(r)})|$, *with equality if and only if* $\mathcal{S} \subset \mathcal{L}(\mathbf{B}^{(r)}) = \mathcal{L}(\mathbf{B}^{(r+1)})$

Intuitively, Lemma 5.1 indicates that the volume of the fundamental parallelotope associated to the current lattice decreases with the recursion depth r, until convergence is achieved. Let R denote the smallest integer such that $|\mathcal{L}(\mathbf{B}^{(R)})| = |\mathcal{L}(\mathbf{B}^{(R+1)})|$. That is, R is the number of steps needed to achieve convergence. With this lemma, it is possible to prove the following theorem [27]:

Theorem 5.2. *Algorithm 1 converges to the solution of* (3).

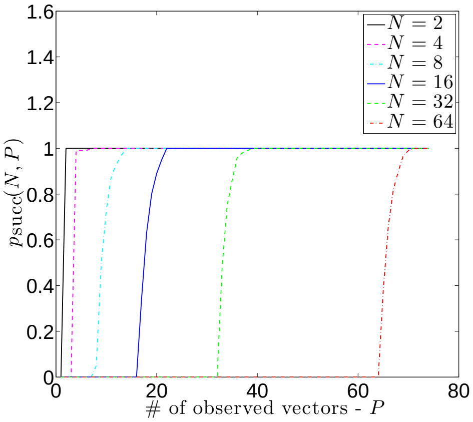


Fig. 2. Empirical probability of success of Algorithm 1 in identifying the coder parameters as a function of the number of observed vectors P and the dimensionality of the embedding vector space N.

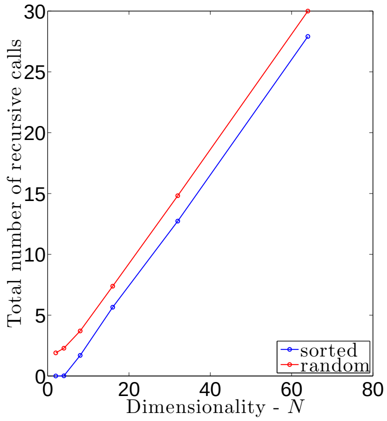


Fig. 3. Total number of recursive calls to `recurseTI` as a function of the dimensionality of the space N and the strategy adopted to visit the observed vectors.

Proof. (sketch) Let $\mathcal{L}^*$ denote the solution of (3), i.e., the lattice with maximum volume that includes all observed vectors $\mathcal{S}$. We need to prove that $\mathcal{L}(\mathbf{B}^{(R)}) = \mathcal{L}^*$.

First, we prove that $|\mathcal{L}(\mathbf{B}^{(R)})|$ cannot decrease beyond $|\mathcal{L}^*|$, i.e., $|\mathcal{L}^*| \leq |\mathcal{L}(\mathbf{B}^{(R)})|$. To this end, let $\mathcal{L}(\mathbf{B}^{(R-1)})$ denote the lattice obtained at the iteration just before convergence. Hence, there is at least one observed vector $\tilde{\mathbf{x}} \in \mathcal{L}^*$ such that $\tilde{\mathbf{x}} \notin \mathcal{L}(\mathbf{B}^{(R-1)})$. Lemma 5.1 establishes that $|\mathcal{L}(\mathbf{B}^{(R)})| < |\mathcal{L}(\mathbf{B}^{(R-1)})|$. Using the same arguments as for the proof of Lemma 5.1, it is also possible to show that $|\mathcal{L}(\mathbf{B}^{(R)})| \geq (1/m)|\mathcal{L}(\mathbf{B}^{(R-1)})| = |\mathcal{L}^*|$ where $|\mathcal{L}(\mathbf{B}^{(R-1)})|/|\mathcal{L}^*| = m$.

To prove that $|\mathcal{L}(\mathbf{B}^{(R)})| = |\mathcal{L}^*|$, it remains to be shown that cannot be $|\mathcal{L}(\mathbf{B}^{(R)})| > |\mathcal{L}^*|$. Indeed, if this were the case, $\mathcal{L}(\mathbf{B}^{(R)})$ would be the optimal solution of (3), since it includes all observed points $\mathcal{S}$ and has volume larger than $|\mathcal{L}^*|$. □

In [27], further analytical results are presented, which are related to two main aspects: i) the probability of converging to the lattice $\mathcal{L}_x$; ii) the rate of convergence of the algorithm. In Section 6, these aspects are investigated experimentally.

6. EXPERIMENTAL ANALYSIS

The solution $\mathcal{L}^*$ of problem (3) computed by the algorithm might converge to a sub-lattice of the original lattice $\mathcal{L}_x$, i.e., $\mathcal{L}^* \subseteq \mathcal{L}_x$. This is the case when all the observed points lie on a sub-lattice of $\mathcal{L}_x$. Let $p_{\text{fail}}(N, P)$ denote the probability of failing to detect the underlying lattice $\mathcal{L}_x$ of rank N, when P points are observed. Then, $p_{\text{succ}}(N, P) = 1 - p_{\text{fail}}(N, P)$. A failure occurs whenever all P vectors fall in any of the sub-lattices of index m. In this section, we empirically evaluate the probability of success. A full analytical derivation of a lower bound on $p_{\text{succ}}(N, P)$ is detailed in [27].

To this end, we generated data sets of N-dimensional vectors, whose elements are sampled from a Gaussian random variable $\mathcal{N}(0, \sigma^2)$. We considered the adverse case in which the elements are independent and identically distributed. Therefore, the distribution of the vectors is isotropic and no clue could be obtained from a statistical analysis of the distribution. Without loss of generality, we set $\sigma = 2$, $\mathbf{W} = \mathbf{I}$ and $\Delta_i = 1$, $i = 1, \ldots, N$. The same results were obtained using different transform matrices and quantization step sizes. Figure 2 shows the empirical probability of success when $N = 2, 4, 8, 16, 32, 64$, and the number of observed vectors P is varied, averaged over 100 realizations. As expected $p_{\text{succ}}(N, P) = 0$ when the number of vectors P does not exceed the dimensionality of the embedding vector space, i.e., $P \leq N$. Then, as soon as $P > N$, $p_{\text{succ}}(N, P)$ grows rapidly to one, when just a few additional vectors are visited. It is interesting to observe that the probability of failure/success depend solely on the difference $P - N$. Hence, the number P of observed vectors needed to correctly identify the underlying lattice grows linearly with the dimensionality N of the embedding vector space, despite the number of potential lattice points grows exponentially with N. In particular, it is possible to observe that, when $N > 2$, the number of observed vectors needs to exceed by 6-7 units the dimensionality, regardless of N.

At the same time, it is interesting to empirically evaluate the complexity of the proposed method. Figure 3 shows the total number of recursive calls needed to converge to the solution of (3). Note that when a large enough number P of vectors is observed, the algorithm converges to the correct lattice $\mathcal{L}_x$. Thus, visiting further vectors does not increase the number of recursive calls, since the base step of the recursion is always met. Figure 3 shows two cases, that differ in the way the set of observed vectors is visited, i.e., randomly, or sorted by their norms in ascending order. In both cases, the number of recursive calls grows linearly with N. For an analytical study on the rate of convergence, the reader is referred to [27].

7. CONCLUSIONS

In this paper we have shown how it is possible to exactly identify the parameters of a transform coder, given a limited set of P transform decoded vectors embedded in a N-dimensional space. Surprisingly, it is possible to successfully identify them when $P > N$ and the probability of failure decreases rapidly to zero when $P - N$ increases. While we focused on the noiseless case, it is possible for the signals to be processed by multiple cascaded transforms, thus introducing noise in the observed output. Extending the proposed method to noisy scenarios where the vectors do not exactly lie on lattice points represents an interesting research avenue and is the subject of current investigations.

8. REFERENCES

[1] J. Lukas, J. Fridrich, and M. Goljan, "Digital camera identification from sensor pattern noise," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 205–214, June 2006.

[2] M. Chen, J. J. Fridrich, M. Goljan, and J. Lukás, "Determining image origin and integrity using sensor noise," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 74–90, 2008.

[3] T. Bianchi and A. Piva, "Image forgery localization via block-grained analysis of JPEG artifacts," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 1003–1017, June 2012.

[4] G. Valenzise, S. Magni, M. Tagliasacchi, and S. Tubaro, "No-reference pixel video quality monitoring of channel-induced distortion," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 22, no. 4, pp. 605–618, 2012.

[5] M. Naccari, M. Tagliasacchi, and S. Tubaro, "No-reference video quality monitoring for H.264/AVC coded video," *IEEE Transactions on Multimedia*, vol. 11, no. 5, pp. 932–946, 2009.

[6] M.R. Banham and A.K. Katsaggelos, "Digital image restoration," *IEEE Signal Processing Magazine*, vol. 14, no. 2, pp. 24–41, 1997.

[7] V. K. Goyal, "Theoretical foundations of transform coding," *IEEE Signal Processing Magazine*, vol. 18, no. 5, pp. 9–21, September 2001.

[8] Z. Fan and R. L. de Queiroz, "Identification of bitmap compression history: JPEG detection and quantizer estimation," *IEEE Transactions on Image Processing*, vol. 12, no. 2, pp. 230–235, 2003.

[9] J. Lukás and J. Fridrich, "Estimation of primary quantization matrix in double compressed JPEG images," in *Proc. of DFRWS*, 2003.

[10] S. Milani, M. Tagliasacchi, and S. Tubaro, "Discriminating multiple jpeg compression using first digit features," in *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, march 2012, pp. 2253–2256.

[11] Y. Chen, K. S. Challapali, and M. Balakrishnan, "Extracting coding parameters from pre-coded MPEG-2 video," in *IEEE International Conference on Image Processing (ICIP)*, 1998, pp. 360–364.

[12] H. Li and S. Forchhammer, "MPEG2 video parameter and no reference PSNR estimation," in *Picture Coding Symposium (PCS)*, 2009, pp. 1–4.

[13] W. Luo, M. Wu, and J. Huang, "MPEG recompression detection based on block artifacts," in *Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series*, 2008, vol. 6819 of *Society of Photo-Optical Instrumentation Engineers (SPIE) Conference*.

[14] W. Wang and H. Farid, "Exposing digital forgeries in video by detecting double quantization," in *Proceedings of the 11th ACM workshop on Multimedia and security*, New York, NY, USA, 2009, MM&Sec, pp. 39–48, ACM.

[15] M. Tagliasacchi and S. Tubaro, "Blind estimation of the QP parameter in H.264/AVC decoded video," in *International Workshop on Image Analysis for Multimedia Interactive Services (WIAMIS), 2010*, 2010, pp. 1–4.

[16] C. Christopoulos, A. Skodras, and T. Ebrahimi, "The JPEG2000 still image coding system: an overview," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 4, pp. 1103–1127, November 2000.

[17] H.S. Malvar, A. Hallapuro, M. Karczewicz, and L. Kerofsky, "Low-complexity transform and quantization in H.264/AVC," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 7, pp. 598–603, July 2003.

[18] M. Winken, P. Helle, D. Marpe, H. Schwarz, and T. Wiegand, "Transform coding in the HEVC test model," in *IEEE International Conference on Image Processing (ICIP)*, 2011, pp. 3693–3696.

[19] P. Bestagini, A. Allam, S. Milani, M. Tagliasacchi, and S. Tubaro, "Video codec identification," in *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, 2012, pp. 2257–2260.

[20] S.D. Casey and B.M. Sadler, "Modifications of the euclidean algorithm for isolating periodicities from a sparse set of noisy measurements," *IEEE Transactions on Signal Processing*, vol. 44, no. 9, pp. 2260–2272, sep 1996.

[21] I.V.L. Clarkson, "Approximate maximum-likelihood period estimation from sparse, noisy timing data," *IEEE Transactions on Signal Processing*, vol. 56, no. 5, pp. 1779–1787, may 2008.

[22] R. Neelamani, R. de Queiroz, Z. Fan, S. Dash, and R.G. Baraniuk, "JPEG compression history estimation for color images," *IEEE Transactions on Image Processing*, vol. 15, no. 6, pp. 1365–1378, June 2006.

[23] J. H. Conway, N. J. A. Sloane, and E. Bannai, *Sphere-packings, lattices, and groups*, Springer-Verlag New York, Inc., New York, NY, USA, 1987.

[24] H. Cohen, *A Course in Computational Algebraic Number Theory*, vol. 138 of *Graduate Texts in Mathematics*, Springer, 1993.

[25] D. Wübben, D. Seethaler, J. Jaldén, and G. Matz, "Lattice reduction: A survey with applications in wireless communications," *IEEE Signal Processing Magazine*, vol. 28, no. 3, pp. 70–91, May 2011.

[26] A. K. Lenstra, H. W. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," *Mathematische Annalen*, vol. 261, pp. 515–534, 1982, 10.1007/BF01457454.

[27] M. Tagliasacchi, M. Visentini Scarzanella, P. L. Dragotti, and S. Tubaro, "Transform coder identification based on quantization footprints and lattice theory," *ArXiv e-prints, http://arxiv.org/abs/1211.3869*, November 2012.