Digital Signal Processing 48 (2016) 188–200

Contents lists available at ScienceDirect

Digital Signal Processing

www.elsevier.com/locate/dsp

Hiding data in compressive sensed measurements: A conditionally reversible data hiding scheme for compressively sensed measurements

Mehmet Yamaç [a,*], Çağatay Dikici [b,a], Bülent Sankur [a]

[a] Boğaziçi University, Electrical and Electronics Engineering, Bebek 34342, Istanbul, Turkey
[b] Imagination Technologies, WD4 8LZ London, United Kingdom

ARTICLE INFO

Article history:
Available online 28 September 2015

Keywords:
Compressive sensing
Information hiding
Steganography
Data hiding

ABSTRACT

Most of the real-world signals we encounter in real-life applications have low information content. In other words, these signals can be well approximated by sparse signals in a proper basis. Compressive sensing framework uses this fact and attempts to represent signals by using far fewer measurements as compared to conventional acquisition systems. While the CS acquisition is linear, the reconstruction of the signal from its sparse samples is nonlinear and complex. The sparse nature of the signal allows enough room for some additional data sequence to be inserted and exactly recovered along with the reconstructed signal. In this study, we propose to linearly embed and hide data in compressively sensed signals and nonlinearly reconstruct both of them using a deflationary approach. We investigate the embedding capacity as a function of signal sparsity and signal compression, as well as the noise sensitivity of the proposed algorithm.

1. Introduction

Nyquist–Shannon sampling theorem states that a continuous-time bandlimited signal must be represented in terms of N uniformly spaced samples taken at least two times faster than the signal bandwidth in order to be exactly reconstructed. However, a great majority of the signals that we encounter in practical applications exhibit a rapid decay when expressed in an appropriate basis. In fact, this is the idea that has given birth to most of the lossy compression techniques such as JPEG [1], JPEG 2000 [2], etc. Many transform coding-based compression techniques like JPEG keep only large coefficients which constitute most of the signal energy, and discard small ones. Although these techniques are widespread and standard in applications, one may need to look beyond the Nyquist–Shannon scheme in niche applications.

Compressive Sensing (CS) has attracted considerable attention since its first introduction by Donoho [3] and Candes et al. [4]. This new paradigm, in contrast to conventional data acquisition systems, attempts to sense signals by using far fewer measurements than the conventional methods. Roughly speaking, CS tries to combine acquisition and compression processes into one step. This is a sensing strategy that enables significantly lower data rate and computation cost in the sensing part. On the other hand, signal recovery in compressive sensing framework is generally achieved by non-linear reconstruction methods that are relatively costly. Therefore, the computational complexity is shifted from encoder to the decoder site, which is especially convenient whenever economies in energy and computation effort are needed at the acquisition site. For instance, CS framework has received attention in Wireless Sensor Networks which requires a low-cost data acquisition system. Recently, Mamaghain et al. [5] have proposed a wireless body sensor network (WBSN) system, where sensors sample ECG signals using compressive sensing, then they transmit these measurements to a remote monitoring center over a wireless channel. Xiang et al. [6] propose a compressive sensing video scheme over wireless channel. Their system is equipped with a single-pixel camera which is an extreme example of compressive sensing built by Takhar et al. [7].

There are cases where one wants to embed metadata on compressively sensed measurements. For example in a WBSN application, embedding of patient's information may be required. Attaching patient metadata to biosensory measurements using a data hiding scheme would enhance the application. Recall that data hiding is the set of techniques to embed information in a media signal imperceptibly and it is often used for copyright protection, data indexing, image captioning or even for hidden communication in military applications [8–10].

The problem of data hiding in compressive sensing framework has been addressed in [11–15]. Sheikh and Baraniuk [11] have studied the data embedding problem in transform domain (e.g.

* Corresponding author.
E-mail addresses: mehmet.yamac@boun.edu.tr (M. Yamaç), cagatay.dikici@imgtec.com (Ç. Dikici), bulent.sankur@boun.edu.tr (B. Sankur).

http://dx.doi.org/10.1016/j.dsp.2015.09.017
1051-2004/

DCT for images) by assuming sparsity of the host signal, that is, image. In the data embedding part, they first obtain a sparse representation of the cover signal of interest based on some convenient transform and hard thresholding these coefficients. Then, they embed the hidden data by spreading it out onto the sparse coefficients. The marked image is then obtained by using the inverse DCT transform before transmission/storage. In the decoding part, they jointly decode both sparse DCT coefficients and embedded data using ℓ_1 minimization and linear decoding [16]. Using similar logic, Zhang et al. [12] have exploited compressive sensing in a content reconstruction problem. Recently, C. Delpha et al. [13] have proposed an informed data hiding scheme where some data, known itself to be sparse, is hidden additively on the non-zero coefficients of the sparse representation of the signal. The rest of the procedure is similar to that in [11] except that they use Costa's quantization based data hiding scheme [17] to obtain the sparse data to be secretly embedded. If one has already a sparse representation of the signal of interest, these approaches are convenient strategies before storage or transmission.

Apart from these works, Valenzise et al. [14] have proposed a CS based algorithm that identifies and localizes forgeries. Patsakis et al. [15] have used compressive sensing to detect the existence of stego content in images.

In this study we introduce a data hiding scheme that embeds an additional information directly onto the CS measurements. This enables data hiding while sensing. Our proposed scheme differs from those in [11–13] in two important aspects. First, data hiding is realized during compressive sensing. More explicitly, we do not use compressive sensing for data hiding, but propose a data hiding method for CS measurements, that is, a scheme where hidden data is carried only by the CS measurements. Second, the hidden data co-exists with the cover signal only in the compressed form, so that, when the compressively sensed cover data is recovered, the hidden data is not only recovered, but is also simultaneously removed from it.

Finally, motivated by the need for real-time implementation, we develop further our method into an embedding scheme that achieves fast joint signal reconstruction and embedded data recovery. A preliminary version of this work was presented at EUSIPCO [18]. This version addressed only, as a proof of concept, the small signal case, and did not elaborate on the theoretical limits for exact recovery conditions, as given in Lemma 2, Theorem 3.

2. Compressive sensing basics

In this section, we provide a brief overview of the CS framework and point out to theorems relevant to the data hiding problem. Recent theoretical results related to the stability of reconstruction methods are also discussed in view of the necessity to recover the embedded data exactly and the document, i.e., the carrier message within a tolerable error bound.

Let $S \in \mathbb{R}^N$ be our signal of interest and Ψ be a basis so that S has a unique representation in that basis such that $S = \Psi x$. We also assume that the elements of the combiner vector x are arranged in descending order of magnitude i.e., $|x|^{(1)} \geq |x|^{(2)} \geq \ldots \geq |x|^{(N)}$. If this basis Ψ is properly chosen according to the class of signal of interest, $S \in \mathbb{R}^N$, then these sorted magnitudes terminate at the kth term for k-sparse signals, and decay to zero rapidly, often according to a power law if the signal S is compressible [19]. In other words, if $N-k$ of the coefficients of x are negligibly small, then the signal x is denoted as compressible or approximately k-sparse (typically $N >> k$) with respect to the sparsifying basis Ψ. A signal x is also termed as strictly k-sparse if it has at most k non-zero coefficients, i.e., $\|x\|_{\ell_0^N} \leq k$, where $\|.\|_{\ell_p^N}$ represents the ℓ_p-norm over N terms. In this work we assume the signal of interest, S to possess a unique and strictly k-sparse representation in an orthonormal basis Ψ. A discussion on how to extend it to approximately sparse signals takes places in the Discussion section.

In CS framework, the signal is linearly sensed by taking $m << N$ measurements,

$$y = \Phi S = \Phi \Psi x = Ax, \tag{1}$$

where Φ is an $m \times N$ measurement operator and $A = \Phi\Psi$. Therefore, we would like to reconstruct x, from the measurements, y. However, (1) is an underdetermined system of linear equations that has infinitely many solutions under the assumption that A is full row rank. We need one or more constraints to achieve a unique solution. Under the assumption that x is k-sparse, one can choose the sparsest solution $\hat{x}$ from among infinite varieties of solutions x. The solution can be cast as

$$(P_0): \min_x \ \|x\|_{\ell_0^N} \text{ subject to } Ax = y. \tag{2}$$

Donoho et al. [20] showed that a unique solution to P_0 can be achieved if $m \geq 2k$. However, ℓ_0-norm minimization requires combinatorial search, and it is an NP hard problem. Although there are alternative solutions to overcome this hurdle [21], such as Greedy Algorithms [22,23], we will focus on convex relaxation, since despite some advances in recent years, the theoretical analysis of the conditions for a guaranteed solution in the greedy methods are still shaky [24]. Most of the greedy algorithms either do not have any theoretical guarantee or offer weaker theoretical bounds compared to convex optimization approaches [25]. P_0 can be relaxed to P_1 [26] as follows

$$(P_1): \min_x \ \|x\|_{\ell_1^N} \text{ subject to } Ax = y. \tag{3}$$

It has been shown that the ℓ_1 minimization is exact in noise free and exactly sparse case if the measurement matrix, A, obeys the following Restricted Isometry Property of order $2k$ [27].

Definition 1 *(Restricted Isometry Property).* Let A be an $m \times N$ matrix and let $\delta_k \in (0,1)$ be the smallest quantity such that

$$(1-\delta_k)\,\|x\|_{\ell_2^N}^2 \leq \|Ax\|_{\ell_2^m}^2 \leq (1+\delta_k)\,\|x\|_{\ell_2^N}^2 \tag{4}$$

for all k-sparse signals, x in $\mathbb{R}^N$, then the matrix A satisfies the Restricted Isometry Property (RIP) of order of k with the restricted isometry constant $\delta_k(A)$.

In real life conditions, we can expect the measurements, y, to be corrupted with random noise pattern, z, such that the received signal becomes $y_n = Ax + z$. Thus, a reconstruction method is expected to be stable in the presence of noise. The stability of the solution implies that a small change in the measurement vector should not lead to substantial changes in the recovered signal. Mathematically speaking, for the perturbed measurements, $y_n = Ax + z$, a stable solution $\hat{x}$ would yield

$$\left\|x - \hat{x}\right\|_{\ell_2^N} \leq \kappa \,\|z\|_{\ell_2^m} \tag{5}$$

with a small positive constant κ, and where $\hat{x}$ is the reconstructed signal.

If the measurements are corrupted by some noise process with bounded energy such that $\|z\|_{\ell_2^m} \leq \epsilon$ [28,29], then (P_1) can be relaxed to

$$(P_1^{\epsilon}): \min_x \ \|x\|_{\ell_1^N} \ \text{ s.t. } \ \|y - Ax\|_{\ell_2^m} \leq \epsilon, \tag{6}$$

under certain conditions discussed below.

Restricted Isometry Property implies the stability of (P_1^{ϵ}). Although we will focus on strictly sparse signals, RIP also implies stability when we deal with approximately sparse signals, i.e.,