ROBUST WATERMARKING OF COMPRESSIVE SENSED MEASUREMENTS UNDER IMPULSIVE AND GAUSSIAN ATTACKS

Mehmet Yamaç, Çağatay Dikici, Bülent Sankur

Boğaziçi University, Electrical and Electronics Engineering
Bebek 34342, Istanbul, Turkey

ABSTRACT

This paper considers the watermark embedding problem onto Compressive Sensed measurements of a signal that is sparse in a proper basis. We propose a novel watermark encoding-decoding algorithm that exploits the sparsity of the signal to achieve dense watermarking. The proposed algorithm is robust under additive white Gaussian noise as well as impulsive noise or their mixture. The experimental results show also that the algorithm achieves an embedding capacity superior to those of classical ℓ_2 and ℓ_1 embedding algorithms.

Index Terms— Watermarking, Compressive Sensing, Sparse Signals

1. INTRODUCTION

Traditional methods in data acquisition follow Shannon /Nyquist sampling theorem; one must sample a band-limited signal by at least two times faster than the signal bandwidth. However, signals that we encounter in many applications are sparse in some proper base, and it is advantageous to compress data by using their sparse representations for efficient storage and transmission. Compressive Sensing (CS) shows that certain signals can be captured from far fewer samples as compared to conventional methods, and they can be reconstructed by developing effective non-linear reconstruction algorithms [1], [2], [3].

In addition to efficiently transmitting or storing CS-based measurements, one may wish to embed a watermark onto these measurements. Hence, the copyright information or meta-data can be embedded onto CS measurements. Such a watermarking scheme must satisfy the following properties: i) the watermark information must be decoded exactly, and ii) the reconstruction of the signal must not suffer at the decoder side.

Channel decoding counterpart of the CS has been developed in [4] for linear decoding of a message from erroneous version under unbounded sparse noise. Sheikh and Baraniuk use this idea to embed watermark onto a sparse signal (e.g. DCT coefficients of an image) [5]. In our recent work [6], we proposed a watermarking scheme that embeds

watermark directly onto CS measurements. This enables to embed watermark information while sensing. In this paper, we extend our recent work [6] and propose a robust reconstruction algorithm when the watermarked samples are subject to i) an additive white Gaussian noise, and ii) sum of an unbounded impulsive noise and an additive white Gaussian noise.

This paper is structured as follows: Section 2 gives a brief review of Compressive Sensing and robust recovery approaches in the presence of i) additive white Gaussian noise, and ii) impulsive noise. In section 3, we present our watermarking scheme and reconstruction method in the presence of i) additive white Gaussian noise, and ii) sum of an unbounded impulsive noise and an additive white Gaussian noise. Experimental results of the proposed methods are presented in Section 4.

2. COMPRESSIVE SENSING

A signal $x \in \mathbb{R}^N$ is a k-sparse if and only if at most k entries of x are non-zero. Let $s \in \mathbb{R}^N$ be a k-sparse signal in the ψ space that is expressed as a linear combination of N orthonormal vectors that form a basis ψ, such that

$$s = \psi x. \tag{1}$$

Instead of using traditional data acquisition and compression methods as in Shannon/Nyquist sampling theorem; the data is transformed to a basis where it can be represented sparsely using $x = \psi^T s$. One can sample data directly from the signal using CS as

$$y = \Phi s, \tag{2}$$

where $y \in \mathbb{R}^m$ is the measurement vector and Φ is an $m \times N$ measurement matrix. Rearranging the equation yields

$$y = \Phi s = \Phi \psi x = A x, \tag{3}$$

where A is an $m \times N$ matrix and the nature of the CS requires $m \ll N$ so that CS method has advantages we discussed

above on traditional Nyquist-Shannon based data acquisition.

The reconstruction method aims to estimate the signal $\hat{x}$ which has at most k non-zero values, from the underdetermined system of equations (2), (3). Note that, a sparse basis ψ can be chosen at reconstruction time and is not directly needed for acquisition. Although the equation $y = Ax$ is underdetermined for the case $k < m \ll N$, if the matrix A satisfies the Restricted Isometry Property (RIP), $\hat{x}$ can be reconstructed exactly using proper reconstruction algorithm. Candes and Tao introduces RIP in [4] as follows:

Definition: A matrix A satisfies RIP of order k if there exists a $\delta_k \in (0,1)$ such that

$$(1 - \delta_k)\|x\|_2^2 \le \|Ax\|_2^2 \le (1 + \delta_k)\|x\|_2^2) \qquad (4)$$

holds for all $x \in \Sigma_k$ where $\Sigma_k = \{x : \|x\|_0 \le k\}$.

If A satisfies the RIP of order $2k$ with $\delta_{2k} < \sqrt{2} - 1$, the k-sparse vector x given in equation (3) can be reconstructed exactly by solving the following convex optimization problem

$$\hat{x} = \arg\min_x \ \|x\|_{\ell_1} \ \text{ s.t. } \ y - Ax = 0. \qquad (5)$$

When A is a random matrix with Gaussian or sub-Gaussian entries, then $m \ge O((k)\log(N/k))$ measurements suffice to recover the signal exactly with overwhelming probability [7].

In a more realistic scenario, the measurement may be corrupted by a noise:

$$y = Ax + z. \qquad (6)$$

In this paper, we consider measurement vector corrupted by both i) Gaussian noise and ii) impulsive noise.

2.1. CS Measurements under Additive White Gaussian Noise (AWGN)

If the CS measurement vector is corrupted by a bounded noise provided that $\|z\|_{\ell_2} \le \epsilon$, it is possible to approximate x by solving the optimization problem

$$\hat{x} = \arg\min_x \ \|x\|_{\ell_1} \ \text{ s.t. } \ \|y - Ax\|_{\ell_2} \le \epsilon. \qquad (7)$$

Optimization problem defined in equation (7) is known as Basis Pursuit Denoising (BPDN) [8] and if RIP is satisfied with $\delta_{2k} < \sqrt{2} - 1$, it is possible to approximate x with a bounded error :

$$\|x - \hat{x}\|_{\ell_2} \le C_0 \epsilon, \qquad (8)$$

where C_0 depends on δ_{2k} [7].

If the elements of $z \in \mathbb{R}^m$ given in equation (6) are i.i.d. according to a Gaussian distribution with zero mean and variance σ^2, the squared norm $\|z\|_{\ell_2}^2$ becomes a chi-squared random variable with mean $\sigma^2 m$ and standard deviation $\sigma^2 \sqrt{2m}$. It is well-known that the probability that $\|z\|_{\ell_2}^2$ exceeds its mean plus two or three standard deviation is small. Then, solving the optimization problem given in equation (7) with

$$\epsilon = \sigma \sqrt{(m + \lambda\sqrt{2m})} \qquad (9)$$

gives an approximation of x with bounded error as in equation (8) [9].

Thus we have considered the case of measurement vector that is corrupted by noise with bounded energy. The situation when measurement vector $y = Ax$ is corrupted by a bounded noise model has been considered in [9], [10].

2.2. CS Measurements under Impulsive Noise

In a realistic scenario, measurement vector can be corrupted by an impulsive noise due to shot noise, malfunctioning hardware, transmission errors [11]. In this scenario, portions of the measurement vector can be completely corrupted by a malicious user. In these scenarios, impulsive noise variance may be very large, and it may lead to a large reconstruction error in equation (8). Impulsive noise model has been investigated in [12], where the authors use probabilistic approach and propose a non-convex optimization program to recover the signal. In [4], impulsive noise model has been investigated, but in the context of error correction coding. In [11], noise model that is sparse in a proper basis has been considered in wide range of amplitudes and error rates. In this study, the measurement vector that is corrupted by a noise is modeled as

$$y_n = Ax + \Omega z = \begin{bmatrix} A \mid \Omega \end{bmatrix} \begin{bmatrix} x \\ z \end{bmatrix}, \qquad (10)$$

where the signal x is k-sparse, the noise z is L-sparse, and the matrix Ω is $m \times m$ unit basis. In this model, one can solve the following optimization problem

$$\begin{bmatrix} \hat{x} \\ \hat{z} \end{bmatrix} = \arg\min_{[x \, z]^{\mathrm{T}}} \ \left\| \begin{bmatrix} x \\ z \end{bmatrix} \right\|_{\ell_1} \ \text{ s.t. } \ y_n - \begin{bmatrix} A \mid \Omega \end{bmatrix} \begin{bmatrix} x \\ z \end{bmatrix} = 0. \qquad (11)$$

3. PROBLEM STATEMENT AND THE PROPOSED METHOD

While sending the signal with the measurements given in equation (2), we also want to transmit additional, which can be a secret message. In this scenario, we wish to embed
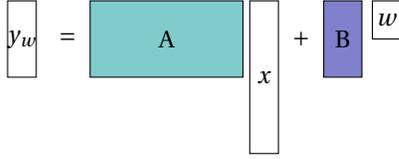
Fig. 1. Pictorial representation of y_w

an M bit dense message (watermark) $w \in \{-a, +a\}^M$ onto this measurement vector y. In this paper, we model watermarked measurement $y_w \in \mathbb{R}^m$ as $y_w = Ax + Bw$, where B is an $m \times M$ coding matrix generated by a secret seed, known to both encoder and decoder where $M < m \ll N$. A pictorial representation of the embedding scheme can be found in Fig. 1. In order to meet the embedding power constraint $\|Bw\|_{\ell_2} \leq P$, a is chosen accordingly. The watermarked measurements can be altered by a malicious user or by channel imperfections, and the decoder receives

$$y_n = Ax + Bw + z. \tag{12}$$

Then the watermarked compressive sensing measurement problem is formulated as follow: Recover the k-sparse x signal and M bit watermark w from the knowledge of y_n. In the case where the noise term vanishes, the recovery of x should be exact; otherwise it should be a close approximation to the true signal. On the other hand, we assume that the watermark information can not tolerate any loss. In either case, recovering of w should be exact. In the light of these requirements, we look for maximum achievable embedding rate $\mathcal{R} = M/m$ in bits/measurement for $\text{Prob}(w \neq \hat{w}) \to 0$. In the meantime, we are interested in the reconstruction of x with a small mean error $\mathbb{E}\{\|x - \hat{x}\|_2\}$.

3.1. Case 1: Decoding under Additive White Gaussian Noise (AWGN)

The watermarked compressive sensed measurements can be corrupted by additive Gaussian noise and this can be modelled as $z \sim \mathcal{N}(0, \sigma^2 I)$. We can rearrange equation (12) as follows

$$y_n = C \begin{bmatrix} x \\ w \end{bmatrix} + z, \tag{13}$$

where $C = [A|B]$.

3.1.1. Classical ℓ_2 Minimization

One classical solution of underdetermined system given in equation (13) can be the minimum norm solution. The solution $\hat{x}$ and $\hat{w}$ that minimizes $\|A\hat{x} + B\hat{w} - y_n\|_{\ell_2}$ is

$$\begin{bmatrix} \hat{x} \\ \hat{w} \end{bmatrix} = C^T (CC^T)^{-1} y_n. \tag{14}$$

3.1.2. ℓ_1 Minimization

Alternatively, as in Section 2.1, the problem can be formed as BPDN, which is solved by minimizing a $(k+M)$-sparse vector $[x \; w]^T$ of length $N + M$. This can be done in two steps. First, the vector $[\tilde{x} \; \tilde{w}]^T$ can be found via

$$\begin{bmatrix} \tilde{x} \\ \tilde{w} \end{bmatrix} = \arg\min_{[x \; w]^T} \left\| \begin{bmatrix} x \\ w \end{bmatrix} \right\|_{\ell_1} \text{ s.t. } \left\| y_n - C \begin{bmatrix} x \\ w \end{bmatrix} \right\|_{\ell_2} \leq \epsilon_1. \tag{15}$$

If C satisfies the RIP of order $2(k+M)$ with $\delta_{2(k+m)} < \sqrt{2} - 1$, the k-sparse x and the dense w can be reconstructed approximately by using $m \geq O((K+M)\log((N+M)/(K+M)))$ measurements with bounded error such that

$$\left\| \begin{bmatrix} x \\ w \end{bmatrix} - \begin{bmatrix} \tilde{x} \\ \tilde{w} \end{bmatrix} \right\|_{\ell_2} \leq C_1 \epsilon_1. \tag{16}$$

Secondly, an additional step can be performed to increase the maximum achievable embedding rate $\mathcal{R} = M/m$ in bits/measurement when $\text{Prob}(w \neq \text{sgn}(\tilde{w})) \to 0$. Since it is known that watermark information $w_i \in \{-a, +a\}$, $i \in \{1, 2, .., M\}$, $\hat{w}$ can be estimated by thresholding $\tilde{w}$ as follows

$$\hat{w}_i = a * \text{sgn}(\tilde{w}_i). \tag{17}$$

After the estimation of $\hat{w}$ using equation (17), we can estimate $\hat{x}$ by solving

$$\hat{x} = \arg\min_x \|x\|_{\ell_1} \text{ s.t. } \|(y_n - B\hat{w}) - Ax\|_{\ell_2} \leq \epsilon_1. \tag{18}$$

By using equation (15), (17) and (18), it is possible to reconstruct k-sparse signal $\hat{x}$ and watermark information $\hat{w}$. It is relatively intuitive that the optimization problem given in equation (15) is not the optimal set-up for our problem, since w is dense. Because of this reason, we propose the following robust recovery approach to decode the watermarking scheme in equation (12).

3.1.3. Proposed Method

Proposed decoding algorithm can be decomposed into three steps:

a) We construct a matrix F which annihilates the matrix B on the left, i.e., such that $FB = 0$. Then apply F to $y_n = Ax + Bw + z$, gives $\tilde{y} = F(Ax + Bw + z) = FAx + \tilde{z}$, where $\tilde{z} = Fz$. Then, a k-sparse signal $\tilde{x}$ can be estimated via

$$\tilde{x} = \arg\min_x \|x\|_{\ell_1} \text{ s.t. } \|\tilde{y} - FAx\|_{\ell_2} \leq \epsilon_1. \tag{19}$$

The important point in this system is that the matrix FA must satisfy the RIP of order $2k$.

b) In the second step, since B is a tall matrix, if we use $\tilde{x}$ that is found in step one, the least-squares method gives us an approximate estimate $\tilde{w}$ as follows

$$\tilde{w} = (B^T B)^{-1} B^T (y_n - A\tilde{x}). \qquad (20)$$

c) As we discussed in the ℓ_1 minimization method, since it is known that watermark information w_i is either $-a$ or $+a$, $\hat{w}$ can be estimated using $\hat{w}_i = a * \text{sgn}(\tilde{w}_i)$, and $\hat{x}$ can be found as in the equation (18).

3.2. Case 2: Decoding under Sum of Impulsive and Gaussian Noise (AWGN)

If watermarked measurements are corrupted by the sum of impulsive noise and additive white Gaussian noise, we can model this system as

$$y_n = Ax + Bw + z_I + z_G, \qquad (21)$$

where $z_G \sim \mathcal{N}(0, \sigma_G^2 I)$ and z_I is L-sparse noise.

3.2.1. ℓ_1 Minimization

One possible solution for this system is to use ℓ_1 minimization of a $(k + M + L)$-sparse vector $[x \ \ w \ \ z_I]^T$ of length $N + M + m$. This can be done in two steps. First, the vector $[\tilde{x} \ \ \tilde{w} \ \ \tilde{z}_I]^T$ can be found via

$$\begin{bmatrix} \tilde{x} \\ \tilde{w} \\ \tilde{z}_I \end{bmatrix} = \arg\min_{[x \ w \ z]^T} \left\| \begin{bmatrix} x \\ w \\ z \end{bmatrix} \right\|_{\ell_1} \ \text{s.t.} \ \left\| y_n - [A | B | I] \begin{bmatrix} x \\ w \\ z \end{bmatrix} \right\|_{\ell_2} \leq \epsilon_1. \qquad (22)$$

Secondly, an additional step can be performed as we did in Section 3.1.3. Since it is known that watermark information w_i is either $-a$ or $+a$, $\hat{w}$ can be estimated as $\hat{w}_i = a * \text{sgn}(\tilde{w}_i)$. Then, $\hat{x}$ can be estimated via

$$\hat{x} = \arg\min_x \ \|x\|_{\ell_1} \ \text{s.t.} \ \left\| (y_n - B\hat{w} - \tilde{z}_I) - Ax \right\|_{\ell_2} \leq \epsilon_1. \qquad (23)$$

However, it is possible to reconstruct k-sparse signal x and M bit watermark w using equation (22) and (23), it is not optimal set-up as we discussed before, because w is not a sparse vector.

3.2.2. Proposed Method

The proposed decoding algorithm can be decomposed into three steps:

a) We construct a matrix F which annihilates the matrix B on the left, i.e., such that FB = 0. Then apply F to $y_n = Ax + Bw + z_I + z_G$, gives $\tilde{y} = F(Ax + Bw + z_I + z_G) = FAx + Fz_I + \tilde{z}$, where $\tilde{z} = Fz_G$. Then, $[\tilde{x} \ \ \tilde{z}_I]^T$ can be estimated via

$$\begin{bmatrix} \tilde{x} \\ \tilde{z}_I \end{bmatrix} = \arg\min_{[x \ z]^T} \ \left\| \begin{bmatrix} x \\ z \end{bmatrix} \right\|_{\ell_1} \ \text{s.t.} \ \left\| \tilde{y} - [FA | F] \begin{bmatrix} x \\ z \end{bmatrix} \right\|_{\ell_2} \leq \epsilon_1. \qquad (24)$$

b) In the second step, since B is a tall matrix, if we use $\tilde{x}$ that is found in step one, watermark $\tilde{w}$ can be estimate using least-squares method as follows:

$$\tilde{w} = (B^T B)^{-1} B^T (y_n - A\tilde{x} - \tilde{z}_I). \qquad (25)$$

c) Finally, since it is known that watermark information w_i is either $-a$ or $+a$, $\hat{w}$ can be estimated using $\hat{w}_i = a * \text{sgn}(\tilde{w}_i)$ and $\hat{x}$ can be found via

$$\hat{x} = \arg\min_x \ \|x\|_{\ell_1} \ \text{s.t.} \ \left\| (y_n - B\hat{w} - \tilde{z}_I) - Ax \right\|_{\ell_2} \leq \epsilon_1. \qquad (26)$$

4. EXPERIMENTAL RESULTS

In this section, we present performance results of the proposed decoding algorithms. We embed M bit length watermark message on to $k = 30$-sparse signal of N = 512 using $m = 145$ measurements. We look for maximum achievable embedding rate $\mathcal{R}$ in bits/measurement when $\text{Prob}(w \neq \hat{w}) \to 0$. And also, we are interested in keeping reconstruction error $\mathbb{E}\{\|x - \hat{x}\|_2\}$ at reasonable level such that $\mathbb{E}\{\|x - \hat{x}\|_2\} \leq \epsilon$. In our experiments, we generate x, w vectors such that $\|x\|_{\ell_2} = 1$, $\|w\|_{\ell_2} = 0.25$, and produce matrices A and F as random Gaussian matrices. Then, columns of the encoding matrix B are obtained from span of null space of F. For each M value, experiments are conducted 250 times, and corresponding $\text{Prob}(w \neq \hat{w})$ and $\mathbb{E}\{\|x - \hat{x}\|_2\}$ values are reported.

When we consider the Gaussian noise for $\sigma = 0.001$ in equation (13), Fig. 2 shows that the proposed method given in Section 3.1.3 achieves $\mathcal{R} \leq 20/145$ bit/measurement, $\text{Prob}(w \neq \hat{w}) \to 0$. Furthermore, for the maximum achievable rate, the expected mean squared error of the reconstruction error is bounded by $\mathbb{E}\{\|x - \hat{x}\|_2\} \leq 4 * 10^{-2}$ as seen in Fig. 3. Proposed method outperforms both ℓ_1 and ℓ_2 decoding algorithms.

Secondly, we set the noise levels in equation (21) as $\sigma_G = 0$ and $\|z_I\|_{\ell_2} = 10$ where z_I is L = 5-spar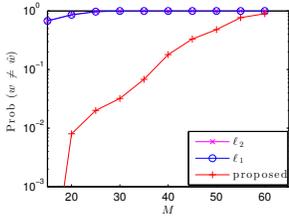se impulsive noise. Fig. 4 shows that the proposed method in Section 3.2.2 achieves $\mathcal{R} \leq 16/145$ bit/measurement and Fig. 5 shows $\mathbb{E}\{\|x - \hat{x}\|_2\} \leq 6 * 10^{-2}$.

Finally, we set the noise levels in equation (21) as $\sigma_G = 0.001$ and $\|z_I\|_{\ell_2} = 10$ where z_I is L = 5-sparse impulsive noise. Fig. 6 shows that the proposed method in

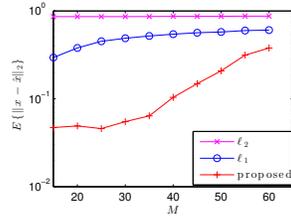**Fig. 2**. M vs. Prob($w \neq \hat{w}$) for $\sigma_G = 0.001$

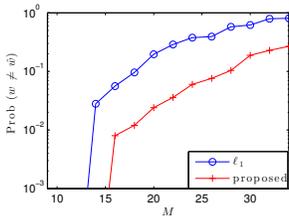**Fig. 3**. M vs. $\mathbb{E}\{\|x - \hat{x}\|_2\}$ for $\sigma_G = 0.001$

Fig. 4. M vs. Prob($w \neq \hat{w}$) for $\|z_I\|_{\ell_2} = 10$
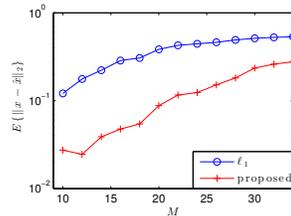

Fig. 5. M vs. $\mathbb{E}\{\|x - \hat{x}\|_2\}$ for $\|z_I\|_{\ell_2} = 10$

Section 3.2.2 achieves $\mathcal{R} \leq 16/145$ bit/measurement and Fig. 7 shows $\mathbb{E}\{\|x - \hat{x}\|_2\} \leq 10^{-1}$.

In all three cases the proposed algorithms outperforms classical ℓ_2 and ℓ_1 decoding methods in watermark extraction and signal recovery.
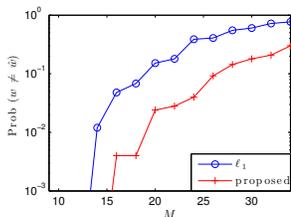

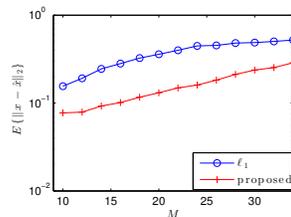**Fig. 6**. M vs. Prob($w \neq \hat{w}$) for $\|z_I\|_{\ell_2} = 10$, $\sigma_G = 0.001$

Fig. 7. M vs. $\mathbb{E}\{\|x - \hat{x}\|_2\}$ for $\|z_I\|_{\ell_2} = 10$, $\sigma_G = 0.001$

5. CONCLUSION

This paper proposes a robust watermarking algorithm in order to embed a dense message w onto CS samples Ax. Two novel decoding methods are proposed; while first one handles Gaussian noise, second one copes with sum of Gaussian and impulsive noises. The proposed methods outperform both classical ℓ_2 and ℓ_1 methods.

7. REFERENCES

[1] R. Baraniuk, "Compressive sensing," *IEEE Signal Processing Mag*, pp. 118–120, 2007.

[2] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inform. Theory*, vol. 52, pp. 1289–1306, 2006.

[3] G. Kutyniok, "Compressed sensing: Theory and applications," *CoRR*, vol. abs/1203.3815, 2012.

[4] E. J. Candès and T. Tao, "Decoding by linear programming," *IEEE Transactions on Information Theory*, vol. 51, no. 12, pp. 4203–4215, 2005.

[5] M. Sheikh and R. Baraniuk, "Blind error-free detection of transform-domain watermarks," in *Image Processing, 2007. ICIP 2007. IEEE International Conference on*, vol. 5, 16 2007-oct. 19 2007, pp. V–453–456.

[6] M. Yamac, C. Dikici, and B. Sankur, "Watermarking of Compressive Sensed Measurements," in *SPARS 2013, Lausanne*, Jul 2013.

[7] E. J. Candès, "The restricted isometry property and its implications for compressed sensing," *C. R. Acad. Sci. Paris S'er. I Math.*, vol. 346, pp. 589–592, 2008.

[8] S. S. Chen, D. L. Donoho, Michael, and A. Saunders, "Atomic decomposition by basis pursuit," *SIAM Journal on Scientific Computing*, vol. 20, pp. 33–61, 1998.

[9] E. J. Candès, J. K. Romberg, and T. Tao, "Stable signal recovery from incomplete and inaccurate measurements," *Communications on Pure and Applied Mathematics*, vol. 59, no. 8, pp. 1207–1223, 2006.

[10] J. Haupt and R. Nowak, "Signal reconstruction from noisy random projections," *IEEE Trans. Inform. Theory*, vol. 52, pp. 4036–4048, 2006.

[11] J. N. Laska, M. A. Davenport, and R. G. Baraniuk, "Exact signal recovery from sparsely corrupted measurements through the pursuit of justice," in *Proceedings of the 43rd Asilomar conference on Signals, systems and computers*, ser. Asilomar'09, 2009, pp. 1556–1560.

[12] R. E. Carrillo, K. E. Barner, and T. C. Aysal, "Robust sampling and reconstruction methods for sparse signals in the presence of impulsive noise," *J. Sel. Topics Signal Processing*, vol. 4, no. 2, pp. 392–408, 2010.