IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 11, 2021, accepted February 25, 2021, date of publication March 9, 2021, date of current version March 18, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3064700

A Novel Efficient Secure and Error-Robust Scheme for Internet of Things Using Compressive Sensing

GAJRAJ KULDEEP, (Student Member, IEEE), AND QI ZHANG, (Member, IEEE)
DIGIT, Department of Electrical and Computer Engineering, Aarhus University, 8000 Aarhus, Denmark

Corresponding author: Qi Zhang (qz@ece.au.dk)

This work was supported in part by the Innovation Fund Denmark under Grant 8057-00059B, and in part by the Digitalisation, Big Data and Data Analytics (DIGIT) Center, Aarhus University.

ABSTRACT In most of existing Internet of Things (IoT) applications, data compression, data encryption and error/erasure correction are implemented separately. To achieve reliable communication, in particular, in harsh wireless environment with strong interference, error/erasure correction codes with higher correction capability or Automatic repeat request (ARQ) scheme are desirable but at the cost of increasing complexity and energy consumption. Due to resource-constrained IoT device, it is often challenging to implement all of them. In this paper, we propose a novel lightweight efficient secure error-robust scheme, ENCRUST, which is able to achieve these three functions using simple matrix multiplication. ENCRUST is built on the new theoretical foundation of projection-based encoding presented in this paper, by leveraging the sparsity inherent in the signal. We perform theoretical analysis and experimental study of the proposed scheme in comparison with the conventional schemes. It shows that the proposed scheme can work in low SINR range and the reconstructed signal quality shows graceful degradation. Furthermore, we apply the proposed scheme on real-life electrocardiogram (ECG) dataset and images. The results demonstrate that ENCRUST achieves decent compression, information secrecy as well as strong error recovery in one go.

INDEX TERMS Error robust encryption, joint compression and error recovery, projection matrix, wireless body area network, resource-constrained, Industrial Internet of Things.

I. INTRODUCTION

The Internet of Things (IoT) has been developing at an accelerating pace in the recent years. A variety of IoT services are solving business problems or create added values across different verticals ranging from industrial automation, smart city all the way to E-health. To facilitate the sustainable development of IoT, we need to tackle multiple critical challenges in IoT.

The massive number of installed IoT device devices generates a huge amount of data. On the one hand, data compression methods can handle exponential IoT data growth to alleviate the stress on the communication network infrastructure and data storage. On the other hand, data compression introduces additional processing complexity in IoT devices. Furthermore, conventional compression schemes typically make the compressed data sensitive to channel errors as well; hence, forward error correction (FEC) is needed to ensure good quality of decompressed data.

The associate editor coordinating the review of this manuscript and approving it for publication was Kashif Sharif.

Fast deployment of IoT solutions globally and massive IoT devices are exacerbating the issue of interference in IoT. Wireless interference can cause channel errors, even long burst errors and erasures.

Apart from data compression and interference there is increasing concern about data security and privacy, which calls for sensor data encryption at resource constrained IoT device to keep data confidentiality in the end-to-end solution. However, the existing data encryption schemes are very sensitive to channel errors, which is referred to as sensitivity encryption, as channel errors can result in decryption failure or low-quality decrypted data [1]. For example, due to the avalanche property of advanced encryption algorithm (AES) [2], the decrypted plaintext will be completely corrupted when there is only a single bit of error. One way to protect encrypted data from channel errors is to apply forward error correction (FEC) codes with high error correction capability. Its drawback is the increased processing complexity and energy consumption at IoT device, since higher error correction capability is often realized through longer codewords and lower coding rate (i.e., higher redundancy overhead).

Therefore, it is highly desirable to design robust encryption scheme that errors / erasures in data barely affect the quality of decrypted data, in particular, in harsh wireless environment with various co-channel and external interferences, e.g., industrial IoT and E-health.

Although most of IoT applications desire data compression, data secrecy and error correction, it is challenging or not always feasible to implement them all at resource constrained IoT device. In the existing IoT solutions, these functions are typically implemented separately by independent processing modules as shown in Fig. 1. Namely, sensor data have to go through Nyquist sampling, data compression, data encryption and FEC encoding processing module sequentially.

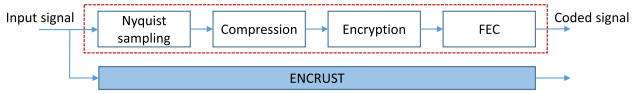

FIGURE 1. Block diagram of the general communication system and the ENCRUST scheme.

In this paper, we aim at designing a feasible scheme that can perform data compression, encryption and error recovery within one single processing module at resource constrained IoT device. We propose the efficient secure error-robust (ENCRUST) scheme by leveraging the true potential of compressed sensing (CS). The encoding process of ENCRUST is a simple matrix operation which is extremely beneficial for resource constrained IoT device. The decoding of ENCRUST is composed of two l_1 minimization processes, the first one for error recovery, and the second one for sparse signal recovery. The decoding is typically performed at edge server or cloud in the IoT ecosystem.

ENCRUST does not only simplify the system design and reduce the system complexity by eliminating the need of additional compression and ciphering blocks, but also provides several salient features. For example, in the conventional approach with separate operations, it is difficult to perform compressed-domain processing, e.g., rate adaption [12], particularly under time-variant channel conditions. However, one single processing module has the potential to provide maximum flexibility in dealing with rate adaptation, namely, determining the amount of data for information representation and the amount of data redundancy for error recovery. The ENCRUST scheme can flexibly tune its encoding parameters, e.g., encoded signal length L, the dimension reduction ratio M/N, and the error recovery capacity ρ_0, for every signal block as per the channel condition. In this sense, the ENCRUST scheme can be categorized as a de facto opportunistic encryption algorithm. Furthermore, the ENCRUST scheme provides graceful degradation of the reconstructed signal when the number of errors exceeding the designed error recovery capability ρ_0. This is very different from the behavior of FEC codes. As we know, the conventional FEC codes usually have drastic data quality drop when they are not able to correct all the errors in the codeword, especially the input message of the FEC codes is encrypted data.

There has been advancement in the feasibility to perform simultaneous sensing and compression by incorporating CS in hardware [5]–[7] for time series signals. Therefore, it is expected that a customized hardware can be designed based on the ENCRUST scheme to realize sensing, compression, secrecy and error recovery in one operation. Designing a hardware of the proposed scheme is beyond the scope of this paper. Consequently, we work on the Nyquist samples to conduct the performance evaluation of the proposed scheme.

It has been studied and empirically shown that usages of conventional data compression methods such as Wavelet transform coding, discrete cosine transform in resource-constrained IoT devices decrease energy efficiency as compared to the uncompressed data [10], [11]. These studies also demonstrate that compressive sensing based compression is energy efficient in resource-constrained IoT devices. Due to no efficient implementation of conventional compression methods for resource-constrained IoT devices in the literature, it is unclear whether those methods are still suitable for resource-constrained IoT devices. Therefore, in this paper, we compare the proposed scheme with the existing solution that consists of both AES encryption and RS codes. Though conventional compression method has better compression ratio than CS, if it is included, then it will worsen the overall energy performance, which is not appropriate for IoT use cases.

A. OUR CONTRIBUTION

Our main contributions in this paper are as follows.

- It is proved that the ENCRUST scheme can be used for compression as well as error recovery. This is shown using projection based encoding and decoding.
- Security analysis of the ENCRUST scheme is performed. It is proved that if the sensing matrix is changed for each encoding then the ENCRUST can provide asymptotic perfect secrecy for constant energy signals.
- We evaluate the ENCRUST scheme using the exactly sparse signal as well as the approximately sparse signals in real life, i.e., electrocardiogram (ECG) dataset [8], [9] and images. For simulations we use a standard noise model including additive white Gaussian noise as well as interference.
- We compare the performance of the ENCRUST scheme with the existing schemes, e.g., conventional CS, AES plus Reed-Solomon (RS) codes. The study results show that ENCRUST achieves not only much better reconstructed signal quality but also higher transmission efficiency under various inference channel conditions.

B. RELATED WORK

Magli *et al.* [12] made a first attempt at designing two algorithms for joint source, channel coding and secrecy. The work was inspired by duality between source and channel coding. One algorithm used arithmetic codes for error correction and the computational secrecy was achieved through randomized arithmetic coders. The second algorithm was based on turbo

codes. The compression was achieved through puncturing the parity bits and the computational secrecy was achieved by hiding the parameters in the encoding process, i.e., the interleaver, the puncturing pattern, and the scrambling pattern. It was also shown that these schemes are weakly secure as compared to AES. Our ENCRUST scheme can achieve asymptotically perfect secrecy which is stronger from cryptanalysis perspective. In addition, it is feasible to incorporate sensing process in ENCRUST, while the algorithms in [12] can only work on Nyquist sampled data.

CS enables sub-Nyquist sampling rate for sparse signal, thereby achieving simultaneous sensing and dimension reduction [13], [14]. CS has been explored in various areas such as wireless communications, image processing, magnetic resonance imaging, remote sensing imaging, and information secrecy. In wireless communication, inherent sparsity present in the channel impulse response (CIR) is more suitable to CS. The CIR sparsity can be exploited in massive MIMO systems [15]. CS has also shown potential in wireless sensor networks for data gathering [16], data aggregation [17], spectrum sensing [18], and non-orthogonal multiple access for massive machine type of communications [19].

Image compression in visible/near-infrared range using CS has been studied in [20] for remote sensing. Speech compression using CS has been explored in [21]. Image compression using CS has been proposed and compared with JPEG [22]. This scheme performs comparable to JPEG in terms of decoded image quality versus data rate. Quantization effect on CS compressed data is studied in [23].

CS can also be used for error correction through matrix and vector multiplication [24], [25] on the Nyquist sampled data. The error correction methods using CS with change in sensing matrices and reconstruction algorithms have been studied in [26]–[28]. Dense error correction for face images using l_1 minimization has explored in [27]. Error correction based on Fourier CS and projective geometry has been studied in [29]. General CS based error correction schemes are in the continuous domain, thereby requiring more bits to represent CS codewords as compared to their traditional counterparts FEC codes.

It has been shown that the CS can provide information secrecy if the entries of the sensing matrix are taken from Gaussian distribution and updated for every sensing [30]. It is proved that CS measurements are perfectly secure using one-time Gaussian distributed sensing matrix [31] for constant energy signal. Recently, it has been shown that perfect secrecy can be achieved using CS encoding for a general class of signals [32].

In recent studies, CS has been considered to be a very good candidate for resource-constrained IoT devices due to the attractive feature of joint compression and encryption [3], [4], [39]. An energy-efficient CS-based scheme for compression and secrecy in a body-to-body network has been realized in [33]. Asymmetrical encryption algorithm is proposed using semitensor CS for wireless body area networks [34]. Medical image compression and encryption using CS has been proposed in [35]. An algorithm based on CS is proposed which simultaneously compress and encrypt audio signals [36]. In this scheme the audio signal is segmented in frames which are then transformed in encrypted frames using CS. CS has been explored to achieve joint compression and multi-class encryption in resource-constrained IoT devices [40], [41].

General symmetric cryptographic algorithms are not capable to deal with corrupted ciphertext, which results in low quality of decrypted data [3], [12], [37]. Due to the greater difficulty in designing error robust encryption compared to sensitivity encryption [3], few work [37], [38] is available in the literature. Opportunistic encryption using AES [37] is suggested to make a tradeoff between security and throughput. CS-based robust image encryption was developed in [38] to combat consecutive packet loss in ciphertext.

Our work is beyond the state-of-the-art solutions mentioned above, because we manage to incorporate compression, encryption and error recovery in one unified framework using compressive sensing.

The paper is organized as follows. In Section II we describe the theoretical fundamentals of CS. Section III presents our theory of projection-based encoding and the design of ENCRUST scheme. In Section IV security analysis of the ENCRUST scheme is performed. Section V presents the simulation setup and results as well as discussion on computation complexity. Finally, Section VI concludes the paper.

Notations: In this paper, all the boldface uppercase, e.g., $\mathbf{X}$, and all the boldface lowercase, e.g., $\mathbf{x}$, letters represent matrices and vectors, respectively. $\mathbf{x}^T$ is transpose of $\mathbf{x}$ and $\mathbf{x}^H$ is Hermitian transpose of $\mathbf{x}$. Double lined upper case characters $\mathbb{E}$ is used for expectation of a random variable. The italic letters represent variables. l_p norm of a vector $\mathbf{x}$ is represented as $(\sum_{i=1}^{N} |x_i|^p)^{\frac{1}{p}}$.

II. THEORETICAL FUNDAMENTALS

An overview of compressive sensing based error correction and cryptosystem is presented in this section. First, we review the basics of compressive sensing.

Let $\mathbf{x}$ be a signal which is either exactly K-sparse in the canonical form or approximately sparse in the transform domain. An exactly K-sparse signal is defined as $||\mathbf{x}||_0 = K$ whereas an approximately sparse signal, $\mathbf{x} = \Psi\theta$, is defined as $||\theta||_0 = K$ which means most of signal information is contained in the K coefficients of the signal $\mathbf{x}'$s transformed representation. We represent l_p norm of a vector $\mathbf{x}$ as $(\sum_{i=1}^{N} |x_i|^p)^{\frac{1}{p}}$.

Compression in CS is achieved by taking random linear measurements using a sensing matrix, $\Phi \in \mathbf{R}^{M\times N}$. CS measurement vector, $\mathbf{y}$, is given as,

$$\mathbf{y} = \Phi\mathbf{x}. \tag{1}$$

The measured signal, $\mathbf{x}$, can be recovered using convex optimization if the signal satisfies the sparsity constraint, and the sensing matrix satisfies the restricted isometric property (RIP) [42].

If the entries of the sensing matrix are chosen from i.i.d. Gaussian distribution and the number of measurements, M, should be in the order of $Klog(N/K)$ [25], then it satisfies the RIP with probability one. If the sensing matrix satisfies the RIP then the signal can be recovered using l_1 minimization by solving the following optimization problem,

$$\hat{\mathbf{x}} = \arg\min_{\mathbf{x}\in\mathbb{C}^N} ||\mathbf{x}||_1, \text{ s.t. } \mathbf{y} = \Phi\mathbf{x}, \tag{2}$$

where the signal $\mathbf{x}$ is sparse in canonical form [13], [14]. In the case when signal is approximately sparse, then the optimization problem [43], [44] becomes,

$$\hat{\theta} = \arg\min_{\theta\in\mathbb{C}^N} ||\theta||_1, \text{ s.t. } \mathbf{y} = \Phi\Psi\theta. \tag{3}$$

A. CS FOR ERROR CORRECTION

The basic framework for error correction is described in the following. Assume a signal $\mathbf{x} \in \mathbb{C}^U$, is encoded to a coded signal, $\mathbf{c}$, using a generator matrix $\mathbf{G} \in \mathbb{C}^{V\times U}$ as,

$$\mathbf{c} = \mathbf{G}\mathbf{x}. \tag{4}$$

The coded signal contains redundant information because $V > U$. The received coded signal, $\mathbf{c}_{rx}$, is represented as

$$\mathbf{c}_{rx} = \mathbf{G}\mathbf{x} + \mathbf{e}, \tag{5}$$

where $\mathbf{e} \in \mathbb{C}^V$ denotes an error vector introduced in the channel. The parity-check matrix $\mathbf{H} \in \mathbb{C}^{W\times V}$ is chosen such that it spans the null space of the generator matrix, i.e., $\mathbf{HG} = \mathbf{0}$. When the corrupted received signal is projected on the parity-check matrix, we obtain the error syndrome vector, $\mathbf{s}$, as

$$\mathbf{s} = \mathbf{He}. \tag{6}$$

The error vector, $\mathbf{e}$, can be recovered from Eq. 6 by performing l_1 minimization. Error vector can be estimated perfectly from Eq. 6, if $||\mathbf{e}||_0 \leq t$ and $W = O(t\ log(\frac{V}{t}))$ [25].

B. SECRECY OF CS BASED CRYPTOSYSTEM

A CS-based encryption algorithm is considered to be computationally secure if sensing matrix is used only once and its entries are Gaussian distributed. It is computationally infeasible to reconstruct the signal without the knowledge of the sensing matrix [30].

CS-based encryption algorithm also provides asymptotic perfect secrecy for Gaussian sensing matrix with constraints on the input signal. An encryption algorithm is perfectly secure if the following is true,

$$P(\mathbf{x}_i|\mathbf{y}_i) = P(\mathbf{x}_i),\ \forall i \tag{7}$$

where $P(\mathbf{x}_i|\mathbf{y}_i)$ and $P(\mathbf{x}_i)$ are a posteriori probability and a priori probability of plaintext, respectively. Perfect secrecy for CS-based encryption algorithm is studied in [31], [45]. The authors proved that for constant energy signals CS-based encryption algorithm satisfies Eq. (7), if the sensing matrix is Gaussian distributed and used only once. Mutual information between a pair of plaintext and ciphertext is given as [31],

$$\begin{aligned} I(\mathbf{x}_i; \mathbf{y}_i) &= I(E_{\mathbf{x}_i}; \mathbf{y}_i), \\ &= I(E_{\mathbf{x}_i}; E_{\mathbf{y}_i}), \end{aligned} \tag{8}$$

where $E_{\mathbf{x}_i}$ and $E_{\mathbf{y}_i}$ are energy of $\mathbf{x}_i$ and $\mathbf{y}_i$, respectively.

Eq. (8) guarantees asymptotic perfect secrecy for constant energy input signals. CS based secrecy algorithms can be compared with the symmetric key algorithms for the case when sensing matrix is changed for each measurement and sensing matrices are constructed using a pseudorandom number generator.

TABLE 1. Symbols for frequently used variables.

N	Signal length
K	Signal sparsity
M	Compressed signal dimension
L	Measurement length
ρ_0	Error correction capability
η_I	Interference rate
γ	Signal to interference noise ratio
α_1,α_2	Constants
$\mathbf{x}$	Signal
$\mathbf{A}, \mathbf{B}, \Phi$	Matrices for CS
$\mathbf{P}$	Projection matrix
$\mathbf{P}^{\perp}$	Orthogonal projection matrix
$\mathbf{y}$	Measurement vector
$\mathbf{y}_e$	Noisy measurement vector
$\mathbf{y}_i^{rx}$	i^{th} received measurement vector
$\hat{\mathbf{y}}_i^{rx}$	i^{th} estimated measurement vector
$\hat{\mathbf{y}}_i^{dec}$	i^{th} decoded measurement vector
$\mathbf{Y}^{rx}$	Complete received measurement matrix
$\mathbf{e}$	Noise vector
$\mathbf{ep}$	Projected noise vector
$\hat{\mathbf{e}}$	Estimated Noise vector
$\hat{\mathbf{x}}$	Recovered signal

III. LIGHTWEIGHT SECURE ERROR ROBUST COMPRESSION SCHEME

In this section, first, we introduce a novel projection-based encoding for error recovery, then the ENCRUST is designed using the concept of the projection-based encoding. We have seen from Eq. 1 that the compression achieved by CS is by reducing the dimension of the signal, i.e., signal dimension reduced from N to M. On the contrary, to provide error correction signal dimension is increased from U to V as in Eq. 4. The frequently used notations are given in Table 1.

A. PROJECTION-BASED ENCODING FOR ERROR RECOVERY

In this subsection, we prove that error recovery is possible without increasing the signal length. First, we prove that the projection matrix satisfies null space property (NSP), then show that the projection-based encoding achieves error correction capability.

NSP is necessary and sufficient condition for perfect recovery of K-sparse signal using basis pursuit [46].

Definition 1: A matrix $\mathbf{A} \in \mathbb{C}^{M\times N}$ satisfies null space property of order K if any vector $\mathbf{x} \in ker(\mathbf{A})\backslash\{0\}$ can be

represented as,

$$||\mathbf{x}_I||_1 \leq ||\mathbf{x}_{\bar{I}}||_1, \tag{9}$$

where $card(I) \leq K$ and I is index set. $ker(\mathbf{A})$ and $card(I)$ are kernel of matrix $\mathbf{A}$ and cardinality of set I, respectively.

NSP is used to show that the projection-based encoding is possible and l_1 minimization can be used for perfect recovery. In the theorem below, it is proved that the projection matrix satisfies NSP of order K.

Theorem 1: Given that matrix $\mathbf{A} \in \mathbb{C}^{M\times N}$ with rank M satisfies NSP of order K then its projection matrix $\mathbf{P} = \mathbf{A}^H(\mathbf{A}\mathbf{A}^H)^{-1}\mathbf{A}$ also satisfies NSP of order K.

Proof 1: For any vector $\mathbf{x}$ from $ker(\mathbf{A})$ we have $\mathbf{A}\mathbf{x} = \mathbf{0}$. Therefore for the matrix $\mathbf{P}$ we get,

$$\mathbf{P}\mathbf{x} = \mathbf{A}^H(\mathbf{A}\mathbf{A}^H)^{-1}\mathbf{A}\mathbf{x} = \mathbf{0}. \tag{10}$$

From Eq. 10 we obtain $ker(\mathbf{A}) \in ker(\mathbf{P})$. Since the rank of matrix $\mathbf{P}$ is equal to the rank of matrix $\mathbf{A}$, we have $ker(\mathbf{A}) = ker(\mathbf{P})$. This proves that the matrix $\mathbf{P}$ satisfies the NSP of order K.

Some of the important properties of the projection matrix are: $\mathbf{P}^2 = \mathbf{P}$, $\mathbf{A}\mathbf{P} = \mathbf{A}$, and $\mathbf{P}^H = \mathbf{P}$ [47]. Orthogonal projection matrix is represented as $\mathbf{P}^\perp = \mathbf{I} - \mathbf{P}$. We prove the projection-based encoding, which uses the sparsity present in the signal for symbol error recovery in the theorem below.

Theorem 2: A length N signal, $\mathbf{x}$, of sparsity K is encoded as,

$$\mathbf{y}_p = \mathbf{P}\mathbf{x}, \tag{11}$$

where $\mathbf{P} \in \mathbb{C}^{N\times N}$ is a projection matrix with NSP of order K. If $\mathbf{P}^\perp$ satisfies NSP of order ρ_0 ($\rho_0 \geq ||\mathbf{e}||_0$) and $\mathbf{P}^\perp\mathbf{P} = \mathbf{0}$, then the signal $\mathbf{x}$ can be recovered from the corrupted measurement, $\mathbf{y}_e$, as given below,

$$\mathbf{y}_e = \mathbf{P}\mathbf{x} + \mathbf{e}, \tag{12}$$

where $\mathbf{e} \in \mathbb{C}^{\mathbf{N}}$ is a noise vector.

Proof 2: To estimate the error vector, $\mathbf{e}$, $\mathbf{y}_e$ is multiplied with $\mathbf{P}^\perp$ and then there is

$$\begin{aligned}\mathbf{P}^\perp\mathbf{y}_e &= \mathbf{P}^\perp\mathbf{P}\mathbf{x} + \mathbf{P}^\perp\mathbf{e},\\ \mathbf{e}\mathbf{p} &= \mathbf{P}^\perp\mathbf{e}.\end{aligned} \tag{13}$$

Since $\mathbf{P}^\perp$ satisfies NSP of order ρ_0, error vector, $\mathbf{e}$, in Eq. 13 can be recovered using l_1 minimization. The optimization problem can be formulated as,

$$\hat{\mathbf{e}} = \arg\min_{\mathbf{e}\in\mathbb{C}^N} ||\mathbf{e}||_1, \quad s.t. \mathbf{e}\mathbf{p} = \mathbf{P}^\perp\mathbf{e}. \tag{14}$$

The estimated error, $\hat{\mathbf{e}}$, is subtracted from $\mathbf{y}_e$ and the signal, $\mathbf{x}$, can be reconstructed by performing l_1 minimization because $\mathbf{x}$ is K-sparse and $\mathbf{P}$ satisfies NSP of order K. To reconstruct the signal, $\mathbf{x}$, the optimization problem can be formulated as,

$$\hat{\mathbf{x}} = \arg\min_{\mathbf{x}\in\mathbb{C}^N} ||\mathbf{x}||_1, \quad s.t. \mathbf{y}_e - \hat{\mathbf{e}} = \mathbf{P}\mathbf{x}. \tag{15}$$

In a nutshell, to reconstruct the signal, $\mathbf{x}$, l_1 minimization is performed twice. First using the orthogonal projection matrix to recover the error vector from the received measurement vector, $\mathbf{y}_e$. After the estimation of the error vector, $\mathbf{e}$, l_1 minimization is performed using the projection matrix to reconstruct the signal, $\mathbf{x}$.

B. ENCRUST

In Theorem 2, it is shown that we can achieve error recovery for exactly sparse and approximately sparse signals without increasing the dimension of the signal. Nevertheless, the projection-based encoding does not achieve dimension reduction of the encoded signal. To incorporate dimension reduction and information secrecy, we propose the ENCRUST scheme. It can be observed from theorem 3 that dimensionality reduction and error recovery can be incorporated in the sensing process.

Theorem 3: For Gaussian distributed matrices $\mathbf{A} \in \mathbb{C}^{L\times M}$ and $\mathbf{B} \in \mathbb{C}^{M\times N}$, the encoding of the ENCRUST scheme is given as,

$$\mathbf{y} = \mathbf{A}\mathbf{B}\mathbf{x}, \tag{16}$$

for a K-sparse and of length N signal, $\mathbf{x}$, can be recovered from the corrupted measurement, $\mathbf{y}_e$, as given below,

$$\mathbf{y}_e = \mathbf{A}\mathbf{B}\mathbf{x} + \mathbf{e}, \tag{17}$$

where $\mathbf{e} \in \mathbb{C}^L$ is an error vector, if M is in the order of $Klog(N/K)$ and $L - M$ is in the order of $\rho_0 log(L/\rho_0)$ and $||\mathbf{e}||_0 \leq \rho_0$.

Proof 3: Construct a matrix $\mathbf{P}^\perp$ such that $\mathbf{P}^\perp\mathbf{A} = \mathbf{0}$. Multiplying $\mathbf{y}_e$ in Eq. 17 with $\mathbf{P}^\perp$ we get,

$$\mathbf{e}\mathbf{p} = \mathbf{P}^\perp\mathbf{e}, \tag{18}$$

which is equivalent to the projection-based encoding. The error vector $\mathbf{e}$ can be recovered from $\mathbf{e}\mathbf{p}$ by performing the l_1 minimization, as the rank of the matrix $\mathbf{P}^\perp$ is $L - M$ which is in the order of $\rho_0 log(L/\rho_0)$ [25]. Similarly, the signal $\mathbf{x}$ can be recovered by first subtracting the estimated error from Eq. 17 and then performing l_1 minimization as given below,

$$\hat{\mathbf{x}} = \arg\min_{\mathbf{x}\in\mathbb{C}^N} ||\mathbf{x}||_1, \quad s.t. \mathbf{A}^H(\mathbf{y}_e - \hat{\mathbf{e}}) = \mathbf{A}^H\mathbf{A}\mathbf{B}\mathbf{x}. \tag{19}$$

Since matrices $\mathbf{A}$ and $\mathbf{B}$ are Gaussian distributed, matrix $\mathbf{A}^H\mathbf{A}$ is invertible with high probability. The rank of the matrix $\mathbf{A}^H\mathbf{A}\mathbf{B}$ is M and in the order of $Klog(N/K)$. This means that the encoded signal presented in Eq. 16 is able to correct maximum ρ_0 errors.

The block compressed sensing technique was introduced for images in [48]. Block based compressed decoding methods were improved in [49] using directional transforms such as contourlets and complex valued dual tree wavelets. Generally, block based compressed sensing is applied on images. Consider an image of size $R \times R$ and block size of $N \times N$. The i^{th} signal $\mathbf{x}_i$ is constructed by vectorizing the i^{th} block in the raster scanning. The total number of sensing matrix for such an image is given as $J = (\frac{R}{N})^2$. If the sensing matrix Φ is constructed using matrices $\mathbf{A}$ and $\mathbf{B}$ as given in Eq. 16, the encoding process for the i^{th} block is given as,

$$\mathbf{y}_i = \Phi_i\mathbf{x}_i. \tag{20}$$

The corrupted i^{th} block at the receiver is given as,

$$\mathbf{y}_i^{rx} = \Phi_i \mathbf{x}_i + \mathbf{e}_i. \tag{21}$$

Since the i^{th} block is encoded using the sensing matrix Φ_i, the erroneous signal can be reconstructed using the ENCRUST scheme. The complete received corrupted measurements for an image is given as,

$$\mathbf{Y}^{rx} = [\mathbf{y}_1^{rx}, \mathbf{y}_2^{rx}, \ldots, \mathbf{y}_J^{rx}], \tag{22}$$

The decoding method for robust recovery for the ENCRUST scheme is defined in the Algorithm 1. I_{max} is the number of iterations and $\mathbf{P}^{\perp}{}_i$ is the i^{th} orthogonal projection matrix constructed using matrix $\mathbf{A}_i$. In the second step error, $\hat{\mathbf{e}}_i$ is estimated for each image blocks, which is then subtracted from the receive measurement vector, $\mathbf{y}_i^{rx}$. This process is done for all image blocks. In the third step for each image block first reconstruction matrix, $\hat{\Phi}_i$, is constructed then estimated measurement vector, $\hat{\mathbf{y}}_i^{rx}$, is projected on matrix $\mathbf{A}$ to get the decoded measurement vector, $\mathbf{y}_i^{dec}$. In the fourth step initial image blocks are constructed by projecting the decoded measurement vector, $\mathbf{y}_i^{dec}$, on the matrix, $\hat{\Phi}_i$, for all image blocks. The fifth step is performed to reconstruct the original image from the initial image blocks and corresponding decoding matrix, $\hat{\Phi}$. Wiener filtering is applied to remove noise in the time-domain. Thresholding and projection operations are performed to exploit the fact the signal is sparse in some sparsifying domain [48], [49]. We use discrete cosine transform in our experiments. After the execution of fifth step the reconstructed image is given as $\mathbf{X}^{I_{max}}$.

Information secrecy can be achieved in the ENCRUST scheme by using the matrices $\mathbf{A}$ and $\mathbf{B}$ once. Encryption and decryption process of ENCRUST encryption algorithm can be described similarly to the symmetric key algorithm.

Encryption: Let $\mathbf{x}_i \in \mathbb{C}^N$ be the i^{th} block of plaintext. By applying the CS encoding on, $\mathbf{x}_i$, we obtain the i^{th} measurement vector as:

$$\mathbf{y}_i = \mathbf{A}_i \mathbf{B}_i \mathbf{x}_i, \tag{23}$$

where $\mathbf{y}_i \in \mathbb{C}^L$ is called ciphertext and $\mathbf{A}_i \in \mathbb{C}^{L \times M}$ and $\mathbf{B}_i \in \mathbb{C}^{M \times N}$ are Gaussian distributed matrix.

Decryption: Decryption is performed using Theorem 3.

The measurement dimension of L in Eq. 16 is in the order $Klog(N/K) + \rho_0 log(L/\rho_0)$ and it can be represented as $L = \alpha_1 K + \alpha_2 \rho_0$ for positive α_1 and α_2. L is dependent on signal sparsity and error correction capability. Therefore, for a K-sparse signal, L can be configured to be smaller than N providing moderate error recovery capability. L can also be configured to be greater than N, thereby providing very high error recovery capability. The dimension reduction is achieved when $L < N$ and the overall compression ratio (CR) is defined as $1 - LQ_2/NQ_1$, where Q_1 is the bit width for the input signal, and Q_2 is the bit width for the measurements. It is worth mentioning that the ENCRUST scheme's coding rate is $\frac{N}{L}$ with the error recovery capability of $\rho_0 = \frac{L-\alpha_1 K}{\alpha_2}$. The ENCRUST scheme is categorized as an opportunistic encryption algorithm because its parameter L can be tuned as per channel conditions. The ENCRUST scheme can be regarded as error robust encryption because it recovers signals from the corrupted ciphertext.

Algorithm 1 Decoding Procedure

Input: $\mathbf{Y}^{rx}$, I_{max}, $\mathbf{A}_i$ and $\mathbf{B}_i$ for $i = 1$ to J ;
** Error estimation and removal **/
for $i = 1$ *to* J **do**
  $\hat{\mathbf{e}}_i = \arg\min_{\mathbf{e}_i \in \mathbb{R}^N} ||\mathbf{e}_i||_1, s.t. \mathbf{ep}_i = \mathbf{P}^{\perp}{}_i \mathbf{e}_i.$;
  $\hat{\mathbf{y}}_i^{rx} = \mathbf{y}_i^{rx} - \hat{\mathbf{e}}_i$
end for ;
** Signal reconstruction **/
for $i = 1$ *to* J **do**
  $\hat{\Phi}_i = \mathbf{A}_i^T \mathbf{A}_i \mathbf{B}_i$;
  $\mathbf{y}_i^{dec} = \mathbf{A}_i^T \hat{\mathbf{y}}_i^{rx}$
end for ;
$\mathbf{X}^0 = [\hat{\Phi}_1^T \mathbf{y}_1^{dec}, \hat{\Phi}_2^T \mathbf{y}_2^{dec}, \ldots, \hat{\Phi}_J^T \mathbf{y}_J^{dec}]$
for $r = 0$ *to* $I_{max} - 1$ **do**
  ** Filtering & projection **/
  $\mathbf{X}^w = Wiener(\mathbf{X}^r)$;
  $\hat{\mathbf{X}}^r = \mathbf{X}^w + [\hat{\Phi}_1^T(\hat{\Phi}_1 \hat{\Phi}_1^T)^{-1}(\mathbf{y}_1^{dec} - \hat{\Phi}_1 \mathbf{x}_1^w), \ldots, \hat{\Phi}_J^T(\hat{\Phi}_J \hat{\Phi}_J^T)^{-1}(\mathbf{y}_J^{dec} - \hat{\Phi}_J \mathbf{x}_J^w)]$;
  ** Thresholding & projection **/
  $\mathbb{N}^r = \Psi^{-1} thresold(\Psi \hat{\mathbf{X}}^r)$;
  $\mathbf{X}^{r+1} = \mathbb{N}^r + [\hat{\Phi}_1^T(\hat{\Phi}_1 \hat{\Phi}_1^T)^{-1}(\mathbf{y}_1^{dec} - \hat{\Phi}_1 \mathbf{x}_1^r), \ldots, \hat{\Phi}_J^T(\hat{\Phi}_J \hat{\Phi}_J^T)^{-1}(\mathbf{y}_J^{dec} - \hat{\Phi}_J \mathbb{N}_J^r)]$
end for ;
Output: $\mathbf{X}^{I_{max}}$

IV. SECURITY ANALYSIS OF ENCRUST

Security analysis of Eq. 1 has been performed in [31], [45] for Gaussian one-time sensing (GOTS). GOTS cryptosystem is known to be perfectly secure, as long as each plaintext has constant energy [31]. Furthermore, for constant energy signals GOTS cryptosystem system achieves asymptotic Indistinguishability [45]. To show that the ENCRUST scheme also achieves the same level of security we present Theorem 4 and 5.

Theorem 4: If the matrices $\mathbf{A}_i$ and $\mathbf{B}_i$ are used once and the entries of these matrices are i.i.d. Gaussian distributed with zero mean and variance σ_A^2 and σ_B^2, then the mutual information satisfies the following relation,

$$I(\mathbf{y}_i; \mathbf{x}_i) = I(\mathbf{y}_i; \varepsilon_{\mathbf{x}_i}), \tag{24}$$

where $\varepsilon_{\mathbf{x}_i}$ is the energy of $\mathbf{x}_i$.

Proof 4: Suppose conditional probability density function of the i^{th} measurement vector is given as $f(\mathbf{y}_i/\mathbf{x}_i)(\mathcal{Y}_i)$. Let $\mathbf{z}_i$ be a random variable $\mathbf{y}_i$ given $\mathbf{x}_i$, i.e., $f(\mathbf{z}_i) = f(\mathbf{y}_i/\mathbf{x}_i)$. The mean of $\mathbf{z}_i$ is zero, because $\mathbb{E}(\mathbf{z}_i) = \mathbb{E}(\mathbf{A}_i \mathbf{B}_i \mathbf{x}_i) = \mathbb{E}(\mathbf{A}_i)\mathbb{E}(\mathbf{B}_i)\mathbf{x}_i = 0$. The variance of $\mathbf{z}_i$ is given as,

$$\mathbb{E}(\mathbf{z}_i \mathbf{z}_i^H) = \mathbb{E}(\mathbf{A}_i \mathbf{B}_i \mathbf{x}_i \mathbf{x}_i^H \mathbf{B}_i^H \mathbf{A}_i^H), \tag{25}$$

$$= M \varepsilon_{\mathbf{x}_i} \sigma_A^2 \sigma_B^2 \mathbf{I}_L, \tag{26}$$

where $\mathbf{I}_L$ is the identity matrix of size $L \times L$. The conditional probability density function, $f(\mathbf{y}_i/\mathbf{x}_i)(\mathcal{Y}_i)$, is Gaussian distributed with zero mean and variance $M\varepsilon_{\mathbf{x}_i}\sigma_A^2\sigma_B^2\mathbf{I}_L$. Now according to the proof of **Proposition 1** in [31], we obtain $I(\mathbf{y}_i; \mathbf{x}_i) = I(\mathbf{y}_i; \varepsilon_{\mathbf{x}_i})$.

Another way to achieve information secrecy is by fixing the dimension reduction matrix $\mathbf{B}_i$ and changing Gaussian distributed matrix $\mathbf{A}_i$ for every plaintext block, which can be given as,

$$\mathbf{y}_i = \mathbf{A}_i\mathbf{B}\mathbf{x}_i. \tag{27}$$

Theorem 5: If the matrix $\mathbf{A}_i$ is used once and its entries are i.i.d. Gaussian distributed with zero mean and variance σ_A^2 then the mutual information satisfies the following relation,

$$I(\mathbf{y}_i; \mathbf{x}_i) = I(\mathbf{y}_i; \varepsilon_{\mathbf{B}\mathbf{x}_i}), \tag{28}$$

where $\varepsilon_{\mathbf{B}\mathbf{x}_i}$ is the energy of $\mathbf{B}\mathbf{x}_i$.

Proof 5: Proof is similar to Theorem 4.

It can be observed that Eq. 27 is also perfectly secure for constant energy signals because it follows the same structure as given in Theorem 4. Theorem 4 and 5 prove that for constant energy signals the joint sensing and error recovery scheme is perfectly secure considering the ciphertext-only attack and assuming that the signal energy is known prior. Because by considering ciphertext-only attack, the adversary can learn the energy of the signal. However, most of the natural signals are not constant energy. To hide signal energy [50] uses an energy obfuscation variable which is multiplied with the sensed measurement vector before transmission, that is represented as, $\mathbf{y}_i = a\Phi_i\mathbf{x}_i$, where a is an energy obfuscating variable and log-normal distributed, Φ_i is Gaussian distributed sensing matrix. Nevertheless, the energy obfuscation scheme does not achieve perfect secrecy. In the recent study it has been shown that the CS-based encryption schemes are not secure against ciphertext-only attack when N is not sufficiently large [51] because real life signals do not have constant energy. In the following, one possible way to construct a constant energy signal is presented [32].

Let $\mathbf{x} \in \mathbb{C}^{N-1}$ be an arbitrary signal. The maximum possible energy of a signal from this signal space is ε_{max}. A new signal space is defined by adding an energy concealing variable. The energy concealing transformation T_ε is defined as, $T_{\varepsilon_{max}} : \mathbb{C}^{N-1} \rightarrow \mathbb{C}^N$. In the vector form this transformation is visualized by adding an element to each vector such as it falls on the surface of the sphere in the higher dimension.

A new vector $\mathbf{x}'$ is constructed by adding an energy concealing variable c to the $\mathbf{x}$ such that energy of $\mathbf{x}'$ is constantly equal to ε_{max}. Let $\mathbf{x}$ be given as,

$$\mathbf{x} = [x_1, x_2, \ldots, x_{N-1}]^T. \tag{29}$$

The energy concealing variable, c, is generated as

$$c = \sqrt{\varepsilon_{max} - ||\mathbf{x}||_2^2}. \tag{30}$$

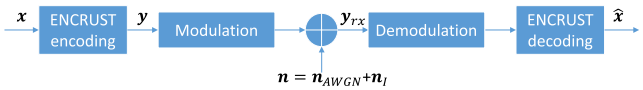

FIGURE 2. Performance evaluation model. x is the sensed signal, n is channel noise, and y is transmitted signal. y_{rx} and $\hat{x}$ are received and reconstructed signal at the cloud, respectively.

Signal $\mathbf{x}'$ is constructed by concatenating c with $\mathbf{x}$ as given in Eq. 29. We get

$$\mathbf{x}' = [c, x_1, x_2, \ldots, x_{N-1}]^T. \tag{31}$$

From Eq. 30 and 31, it is clear that the new signal, $\mathbf{x}'$, has constant energy, i.e. ε_{max}. From Eq. 28 we know that the measurements leak only the signal energy. If the maximum energy of the signal is made public, the adversary does not learn anything new from the measurements. In a nutshell, the ENCRUST scheme provides confidentiality without additional cost. The only requirement is that sensing matrix should be changed for each sensing.

A key-based pseudorandom number generator can be used to construct a sensing matrix in a resource-constrained IoT device. We have recently proposed an energy-efficient linear feedback shift register-based random sequence generator [32]. This generator can be used to construct approximately Gaussian distributed sequence as well as Bernoulli sequence depending on the security requirements. Encryptor and decryptor share the secret key, and sensing matrix can be generated using this key. In the ENCRUST, one of the matrices can be generated using this key-based random number generator at the encryptor. The decryptor has the same key. Hence, it can generate the same sensing matrix and can reconstruct plaintext by applying l_1 minimization. This type of construction is similar to symmetric key encryption.

V. SIMULATION RESULTS

In this section, we aim to compare the ENCRUST scheme with the other conventional schemes under different channel conditions. We use the reconstructed signal quality as the primary performance metric which is calculated between the original signal and the reconstructed signal, as shown in Fig. 2.

Since the ENCRUST scheme is designed using CS concepts, we use means square error (MSE) as the performance metric for K-sparse signals. If the MSE is less than 10^{-6}, then the reconstruction is regarded as successful [24], [52]. To measure the error recovery capability, we use different channel parameters as discussed in the following subsection.

Image reconstruction quality is measured using average peak signal-to-noise ratio (APSNR) given as,

$$\text{APSNR} = \mathbb{E}(10log(\frac{255^2}{\text{IMSE}})), \tag{32}$$

where IMSE is image mean square error. For ECG signals, the measure of signal quality uses average percentage root-mean-squared difference (PRD), which measures the distortion between the reconstructed signal and the original signal.

It is given as,

$$\text{PRD} = \left(\sqrt{\frac{\sum_{i=1}^{N}|x_i - \hat{x}_i|^2}{\sum_{i=1}^{N}|x_i|^2}}\right)100. \tag{33}$$

We use the ECG signal quality classification table from [10], where reconstructed signals with PRD values below 9 are considered to be of good quality. Therefore, in order to use the classification table, we calculate PRD after removing the DC component from the signals as [10].

In CS, the reconstruction depends on the selection of a sparsifying basis of the signal. It has been shown that the reconstruction quality using an over-complete dictionary is better compared to one orthogonal transform dictionary [53]. Considering the IoT ecosystem, the reconstruction will be performed either on the edge or core cloud. Therefore we also use the over-complete dictionary for reconstruction. Empirically, we observed that the combination of discrete cosine transform, symmlet [54] (sym4, wpsym4), and discrete sine transform gives a better result for ECG signals. For the image reconstruction algorithm, we use a single dictionary based on the discrete cosine transform.

A. CHANNEL MODELS

In this subsection, we consider a channel model consisting of additive white Gaussian noise (AWGN) and sparse interference to characterize a harsh wireless environment with sporadic high interference. This channel model is relevant for the IoT because wireless interference is prevalent, e.g., Wi-Fi interference in low power ZigBee IoT systems [1], [55], [56].

Assume signal has constant power P_0, in this way we can use average signal to interference noise ratio (SINR) to characterize the channel with interference. In other words, when there is no inference in the channel, the channel becomes an AWGN channel which can be simply characterized by average signal to noise ratio (SNR), $\Gamma = 10log(P_0/N_0)$. If the average interference power is I_0 and AWGN is N_0, then average SINR $\gamma = 10logP_0/(N_0 + I_0)$. The average of interference power I_0 is determined by the number of interference occurrences ρ during one transmission block, N, i.e., the transmitted signal length and the amplitude of interference signals. We define the rate of interference occurrence as $\eta_I = \rho/N$. For a sporadic interference or sparse interference signal $\mathbf{n}_I$, there is $||\mathbf{n}_I||_0 = \rho$. When one encoded signal sample is represented by multiple modulation symbols, we assume each modulation symbol has equal symbol error probability due to interference. The duration of each interference occurrence is then assumed equal to the modulated symbol duration. Due to strong interference, each interference occurrence causes not only error but even erasure. The consecutive interference occurrences lead to burst errors. For the ENCRUST scheme, it can be observed that the sparse errors and burst errors will have the same effect as far as the number of symbol errors are below ρ_0.

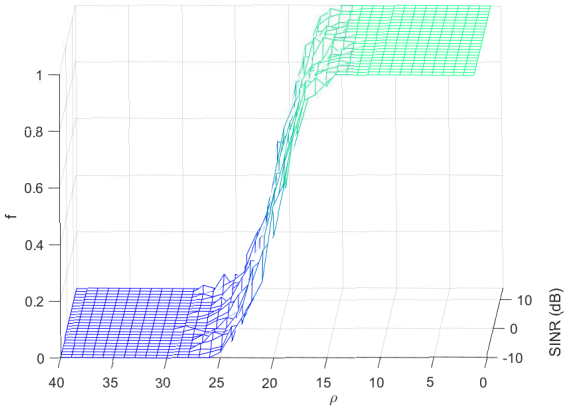

FIGURE 3. Frequency of prefect reconstruction of a sparse random signal, ($N = 1024$, $K = 100$, $\rho_0 = 40$, and $L = 700$).

B. EXACTLY SPARSE SIGNAL

The ENCRUST scheme's performance is evaluated under the condition of AWGN noise power $N_0 = 10^{-2}P_0$ and SINR changing from -10 dB to 20 dB with the ρ being the number of interference occurrences, i.e., the number of spikes. For this simulation, we chose a random signal with sparsity $K = 100$ and length $N = 1024$. The ENCRUST scheme is designed for $\rho_0 = 40$ and constants $\alpha_1 = 5$ and $\alpha_2 = 5$, which gives us $L = 700$. In this configuration, it achieves CR equal to $1 - L/N$, i.e, 31.64%. Each element of the input vector and the encoded measurement vector is represented in 16-bit. The measurement vector of length L is divided into four-column vectors each of length L, so that each element of the new resulted vectors can be represented in 4-bit and is modulated using 16QAM. The modulation symbols go through the interference channel described in Subsection V-A.

The exact reconstruction frequency f of the ENCRUST scheme is calculated for 100 simulation runs. The frequency of the exact reconstruction of a K-sparse signal for the changing values of SINR and ρ is shown in Fig. 3. It can be observed from Fig. 3 that the ENCRUST scheme can recovery more than 10 errors even for SINR equal to -10 dB, i.e., the exact reconstruction frequency f equal to 1 when $\rho \leq 10$. Note that the channel with low SINR characterizes a kind of erasure channel, as the amplitude of interference is so high that it completely corrupts the modulation symbols. We designed $\rho_0 = 40$ in this experimental study, but as explained in the previous paragraph for one measurement element, four modulation symbols are needed. Therefore, the actually achieved ρ is around 10, which is consistent with the theoretical analysis.

ENCRUST scheme is compared with Reed-Solomon (RS) codes in terms of error correction capabilities for K-sparse signals for $K = 100$. RS (255, 223) code is used, which can correct 16 errors. To make a fair comparison, the signal length, N, is chosen such a way that it is divisible by 223. Therefore, we choose the K-sparse signal of $N = 1115$. To show the performance of both high power interference and low power interference scenarios, ENCRUST is simulated for

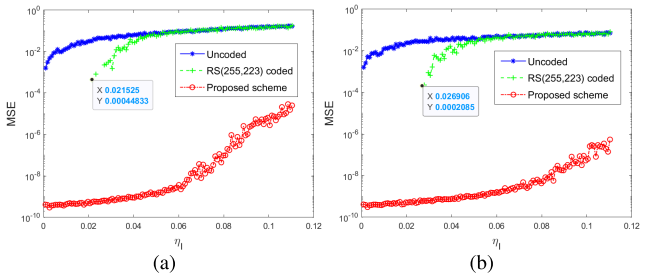

FIGURE 4. MSE comparison of the reconstructed exactly sparse random signal, ($N = 1115$, $K = 100$, and $N_0 = 10^{-3}P_0$) (a) $\gamma = -10$ dB (b) $\gamma = 10$ dB.

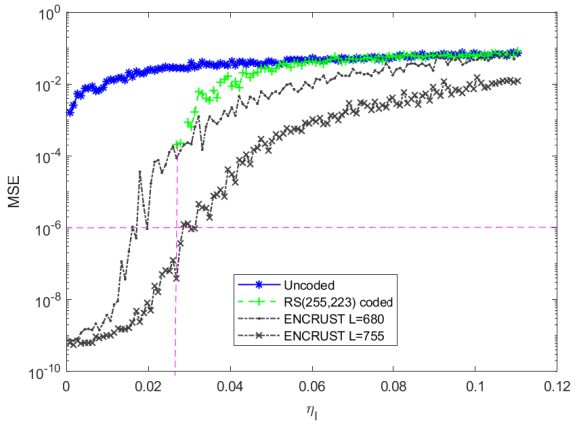

FIGURE 5. MSE comparison for the reconstructed sparse random signal using ENCRUST, RS codes and uncoded scheme ($N = 1115$, $K = 100$).

$\gamma = -10$ and $\gamma = 10$, respectively. The ENCRUST is also designed for $L = 1115$ with constant $\alpha_1 = 5$ to have a fair comparison with RS codes. It should be noted that for these settings the code rate for ENCRUST is 1 and RS code is 0.8745. The input elements and measurements are represented in 16-bit and modulated using 16QAM, as explained previously, and the channel's AWGN noise power $N_0 = 10^{-3}P_0$. MSE performance of the uncoded signal, RS coded signal, and ENCRUST scheme under different interference channel conditions are shown in Fig. 4. It can be observed from Fig. 4(a) and (b) that RS codes can completely recover signals, i.e., MSE equal to zero, when SINR $\gamma = -10$ dB and interference rate $\eta_I \leq 2.1\%$ and at $\gamma = 10$ dB and interference rate $\eta_I \leq 2.6\%$. For $\gamma = -10$ dB and $\gamma = 10$ dB, MSE performance of the ENCRUST scheme is less than 10^{-6} even if the interference rate, η_I, is below 8% and 11%, respectively.

Now we study the error recovery capability of ENCRUST when L is configured less than N. We set SINR $\gamma = 10$ dB, and keep the other parameters as described for Fig. 4. It can be observed from Fig. 5 that for $L = 755$, the proposed scheme achieves MSE below 10^{-6} when $\eta_I < 2.6\%$, which is equivalent to RS coded signal. Note that using RS codes (255, 223), the MSE of the reconstructed signal is zero when $\eta_I < 2.6\%$, but the MSE dramatically jumps to 10^{-4} when $\eta_I > 2.6\%$. In this setting, the proposed scheme simultaneously achieves compression, at CR = 32.29% and error recovery capability. It is worth mentioning that the ENCRUST scheme provides graceful degradation in MSE when the channel errors exceed the error recovery capability, whereas this is not possible with RS codes.

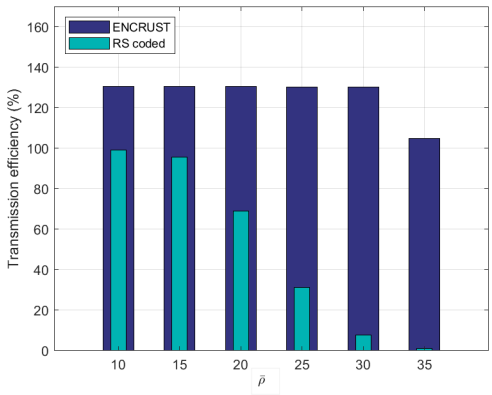

FIGURE 6. Transmission efficiency of the ENCRUST scheme and RS coded signal ($N = 1115$, $L = 855$).

C. APPROXIMATELY SPARSE SIGNALS

In this subsection, we compare the ENCURST scheme with the conventional schemes using the real-life data, i.e., ECG dataset and image. To study the ENCRUST scheme's performance on the ECG database, we use physical units, which are represented in 16-bit. We choose signal length $N = 1115$, AWGN noise power $N_0 = 10^{-2}P_0$, $\gamma = 10$dB and ρ following a Binomial distribution with mean $\bar{\rho}$ and probability 0.5. ENCRUST scheme is configured as $\rho_0 = 51$ and $L = 855$. For these parameters, CR achieved by the ENCRUST scheme is 23%. The encoded signal is modulated using 16QAM, as described in Subsection V-B. We evaluate the transmission efficiency of the ENCRUST scheme and the RS(255, 223) codes for ECG signals. ECG record 230 is used for simulation. The signal reconstruction is regarded as successful if the PRD is below 9, otherwise retransmission is required. The transmission efficiency of the ENCRUST scheme for the transmission failure probability, P_f, is calculated as $(1 - P_f)N/L$. The simulation is run for 1000 times.

Transmission efficiency of the ENCRUST scheme and the RS codes is shown in Fig. 6. It can be observed that the transmission efficiency for ENCRUST is more than 100%. This is because compression is inherent in the ENCRUST scheme. The transmission efficiency of the RS encoded signal decreases significantly with increase in the $\bar{\rho}$. When $\bar{\rho}$ reaches 35, the transmission efficiency of the RS coded signal reaches zero, which means that at this channel condition it is no longer possible to use the RS codes to achieve reliable transmission. On the contrary, the transmission efficiency of the ENCRUST scheme is much higher than that of the RS coded signal and it is still higher than 100% even when $\bar{\rho}$ reaches 35.

We also compare the PDR performance of ECG signals using the ENCRUST scheme, the normal CS (the number of measurements equal to L), RS codes, and uncoded scheme, as shown in Fig. 7. From the figure, it can be observed that the

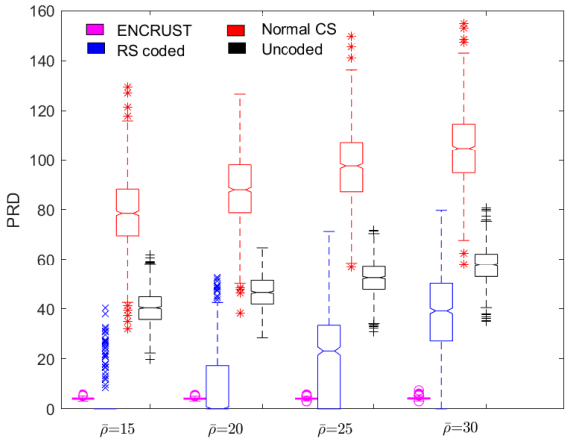

FIGURE 7. Comparison of ECG signal reconstruction quality (PRD) between ENCRUST and the other encoding schemes.

ENCRUST scheme's PRD value is well below nine, whereas the normal CS and uncoded scheme have average PRD more than 30. Note that the reconstruction quality of an ECG signal is considered good if the PRD$<$ 9 [10]. For the RS codes, if the channel errors are below its error correction capability, then it reconstructs the ECG signal with PRD equal to zero; otherwise, it fails to reconstruct the ECG signal. As the $\bar{\rho}$ increases, the reconstruction quality for RS decreases drastically, whereas ENCRUST consistently performs well.

Now, application of ENCRUST is shown to achieve error-robust information secrecy for images. We choose advanced encryption standard (AES) for information secrecy and RS (255,223) code for error correction to compare with the ENCRUST. We use image of size 512 $\times$ 512. In the conventional settings first image is encrypted using AES after that the RS (255,223) coding is applied and then modulated using 16QAM symbols. To emulate noise signal we use the channel model described in subsection V-A.

For the ENCRUST image is divided into block of size 32 $\times$ 32. Each block is vectorized into a vector of length $N = 1024$. ENCRUST is designed for $M = 307$ and $L = 407$ and each vectorized image block is encoded using Eq. 20. For these parameters, CR achieved by the ENCRUST scheme is 60%. Each element of the encoded measurement vector is represented in 8-bit and modulated into two 16QAM symbols. The decoding is performed using the decoding algorithm described in Algorithm 1. The APSNR is used as the performance metric to evaluate the reconstructed image quality. The APSNR of Lenna image is shown in Fig. 8 for the channel condition of AWGN noise power $N_0 = 10^{-2}P_0$, and $\gamma = 10$ dB. It can be observed from Fig. 8 that once the errors are more than the number of error correction capability of the RS codes, the reconstruction quality decreases drastically. In contrast, ENCRUST's degradation in reconstruction quality is graceful.

It can also be observed from Fig. 8 that for the ENCRUST scheme, APSNR is greater than 30 dB for $\eta_I \leq 4.1\%$, whereas the AES+RS solution can achieve APSNR greater than 30 dB only if $\eta_I \leq 1.9\%$. Furthermore, we use image

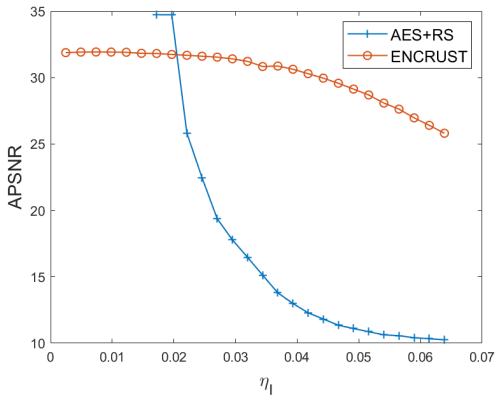

FIGURE 8. APSNR performance of the ENCRUST scheme and AES+RS scheme for images under various η_I.

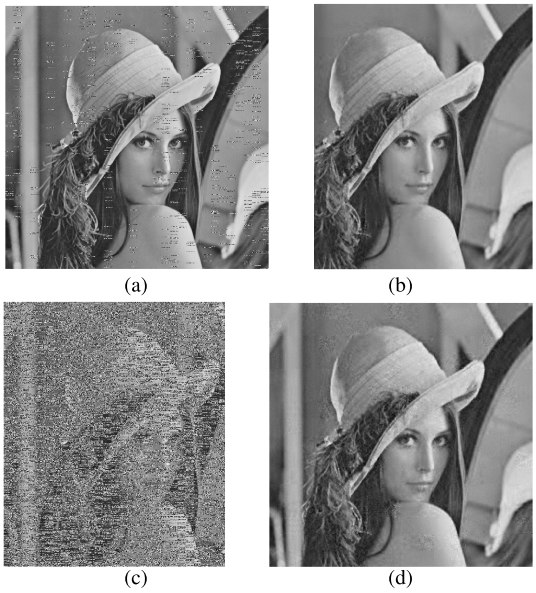

FIGURE 9. Illustration of robustness of the ENCRUST scheme and AES+RS on images. Images (a) and (c) are reconstructed using AES+RS, and (b) and (d) are reconstructed using ENCRUST for $\eta_I = 2.4\%$ and $\eta_I = 4.9\%$, respectively.

visualization to demonstrate the robustness of the ENCRUST scheme. Fig. 9 (a) and (b) show the reconstructed images under $\eta_I = 2.4\%$, while Fig. 9 (c) and (d) show those reconstructed images under $\eta_I = 4.9\%$. It can be observed from Fig. 9(a) and (c) that reconstruction quality using the AES+RS solution deteriorates significantly, whereas the reconstructed images using the ENCRUST scheme in Fig. 9(b) and (d) have much better quality. In addition, using the proposed scheme the reconstruction quality decrease is very mild even when the channel errors exceed its error recovery capability.

D. DISCUSSION

The ENCRUST scheme uses the concept of compressive sensing to achieve compression, secrecy, and error recovery. The ENCRUST scheme requires $O(LN)$ computation to perform all the functions, whereas the state-of-the-art

schemes require way more than this. For example, a simple sparsifying transform will require $O(N^2)$ computations followed by Huffman coding will require $O(SlogS)$ for S elements in the Huffman dictionary [57]. Forward error correcting encoding will also require slightly less than $O(n^2)$, where n is codeword size [58]. Apart from these, to provide information secrecy additional cryptographic algorithm is needed. Traditional ways of achieving compression, information secrecy, and error recovery are challenging to be implemented in resource constrained IoT devices. As in [10], it is experimentally shown that the life of IoT sensor decreases using Wavelet+Huffman coding as compared to the unncoded signal transmission. Besides the low computation complexity of the ENCRUST scheme, it is feasible to incorporate the sensing process into the proposed scheme, which makes it a promising solution for IoT sensor devices.

VI. CONCLUSION

In this paper, we prove that the projection-based encoding can be used for error recovery exploiting the sparsity present in the signal without expanding the signal dimension. Using the projection-based encoding and CS framework, we design the ENCRUST scheme which is able to realize compression, encryption and error recovery through simple matrix multiplications. We evaluate the performances of the proposed scheme under various inference channel conditions in comparison with the exiting schemes. The proposed scheme consistently shows its great performance even under erasure channel with low SINR. This is desirable for diverse IoT solutions that are operated in harsh wireless environment with high interference. Furthermore, it is proved that ENCRUST achieves asymptotic perfect secrecy for constant energy signals.

In the future, we plan to implement ENCRUST in resource-constrained IoT devices such as TelosB mote and carry out energy measurements to quantitatively analyze energy gain of ENCRUST. The ENCRUST scheme's performance will also be evaluated using a universal software radio peripheral (USRP) development kit.

REFERENCES

[1] J. Jeong and C. T. Ee, "Forward error correction in sensor networks," in *Proc. Int. Workshop Wireless Sensor Netw. (WWSN)*, 2007, pp. 1–6. [Online]. Available: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.449.6441&rep=rep1&type=pdf

[2] W. Stallings, *Cryptography and Network Security: Principles and Practice*. Upper Saddle River, NJ, USA: Prentice-Hall, 1999.

[3] Y. Zhang, L. Y. Zhang, J. Zhou, L. Liu, F. Chen, and X. He, "A review of compressive sensing in information security field," *IEEE Access*, vol. 4, pp. 2507–2519, 2016.

[4] H. Djelouat, A. Amira, and F. Bensaali, "Compressive sensing-based IoT applications: A review," *J. Sens. Actuator Netw.*, vol. 7, no. 4, p. 45, Oct. 2018.

[5] D. Gangopadhyay, E. G. Allstot, A. M. R. Dixon, K. Natarajan, S. Gupta, and D. J. Allstot, "Compressed sensing analog front-end for bio-sensor applications," *IEEE J. Solid-State Circuits*, vol. 49, no. 2, pp. 426–438, Feb. 2014.

[6] A. Anvesha, S. Xu, J. Romberg, and A. Raychowdhury, "A 65 nm compressive-sensing time-based ADC with embedded classification and INL-aware training for arrhythmia detection," in *Proc. IEEE Biomed. Circuits Syst. Conf. (BioCAS)*, Oct. 2017, pp. 1–4.

[7] J. Sheng, C. Yang, and M. C. Herbordt, "Hardware-efficient compressed sensing encoder designs for WBSNs," in *Proc. IEEE High Perform. Extreme Comput. Conf. (HPEC)*, Sep. 2015, pp. 1–7.

[8] A. L. Goldberger, L. A. N. Amaral, L. Glass, J. M. Hausdorff, P. C. Ivanov, R. G. Mark, J. E. Mietus, G. B. Moody, H. E. Stanley, and C.-K. Peng, "PhysioBank, PhysioToolkit, and PhysioNet: Components of a new research resource for complex physiologic signals," *Circulation*, vol. 101, no. 23, pp. e215–e220, Jun. 2000.

[9] G. B. Moody and R. G. Mark, "The impact of the MIT-BIH arrhythmia database," *IEEE Eng. Med. Biol. Mag.*, vol. 20, no. 3, pp. 45–50, May/Jun. 2001.

[10] H. Mamaghanian, N. Khaled, D. Atienza, and P. Vandergheynst, "Compressed sensing for real-time energy-efficient ECG compression on wireless body sensor nodes," *IEEE Trans. Biomed. Eng.*, vol. 58, no. 9, pp. 2456–2466, Sep. 2011.

[11] C. Karakus, A. C. Gurbuz, and B. Tavli, "Analysis of energy efficiency of compressive sensing in wireless sensor networks," *IEEE Sensors J.*, vol. 13, no. 5, pp. 1999–2008, May 2013.

[12] E. Magli, M. Grangetto, and G. Olmo, "Joint source, channel coding, and secrecy," *EURASIP J. Inf. Secur.*, 2007, Art. no. 79048, doi: 10.1155/2007/79048.

[13] E. J. Candès, J. Romberg, and T. Tao, "Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 489–509, Feb. 2006.

[14] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.

[15] Z. Gao, L. Dai, S. Han, C.-L. I, Z. Wang, and L. Hanzo, "Compressive sensing techniques for next-generation wireless communications," *IEEE Wireless Commun.*, vol. 25, no. 3, pp. 144–153, Jun. 2018.

[16] D. Ebrahimi and C. Assi, "On the interaction between scheduling and compressive data gathering in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2845–2858, Apr. 2016.

[17] B. Khalfi, B. Hamdaoui, M. Guizani, and N. Zorba, "Efficient spectrum availability information recovery for wideband DSA networks: A weighted compressive sampling approach," *IEEE Trans. Wireless Commun.*, vol. 17, no. 4, pp. 2162–2172, Apr. 2018.

[18] A. Ali and W. Hamouda, "Advances on spectrum sensing for cognitive radio networks: Theory and applications," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1277–1304, 2nd Quart., 2017.

[19] M. Alam and Q. Zhang, "Non-orthogonal multiple access with sequence block compressed sensing multiuser detection for 5G," *IEEE Access*, vol. 6, pp. 63058–63070, 2018.

[20] J. Li, Y. Fu, G. Li, and Z. Liu, "Remote sensing image compression in visible/near-infrared range using heterogeneous compressive sensing," *IEEE J. Sel. Topics Appl. Earth Observ. Remote Sens.*, vol. 11, no. 12, pp. 4932–4938, Dec. 2018.

[21] T. S. Gunawan, O. O. Khalifa, A. A. Shafie, and E. Ambikairajah, "Speech compression using compressive sensing on a multicore system," in *Proc. 4th Int. Conf. Mechatronics (ICOM)*, Kuala Lumpur, Malaysia, May 2011, pp. 1–4.

[22] X. Yuan and R. Haimi-Cohen, "Image compression based on compressive sensing: End-to-end comparison with JPEG," *IEEE Trans. Multimedia*, vol. 22, no. 11, pp. 2889–2904, Nov. 2020.

[23] V. K. Goyal, A. K. Fletcher, and S. Rangan, "Compressive sampling and lossy compression," *IEEE Signal Process. Mag.*, vol. 25, no. 2, pp. 48–56, Mar. 2008.

[24] E. Candes, M. Rudelson, T. Tao, and R. Vershynin, "Error correction via linear programming," in *Proc. 46th Annu. IEEE Symp. Found. Comput. Sci. (FOCS)*, Pittsburgh, PA, USA, 2005, pp. 295–308.

[25] E. J. Candes and T. Tao, "Decoding by linear programming," *IEEE Trans. Inf. Theory*, vol. 51, no. 12, pp. 4203–4215, Dec. 2005.

[26] A. HesamMohseni, M. Babaie-Zadeh, and C. Jutten, "Inflating compressed samples: A joint source-channel coding approach for noise-resistant compressed sensing," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Taipei, Taiwan, Apr. 2009, pp. 2957–2960.

[27] J. Wright and Y. Ma, "Dense error correction via ℓ_1-minimization," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Apr. 2009, pp. 3033–3036.

[28] M. S. Mohammadi, Q. Zhang, and E. Dutkiewicz, "Reading damaged scripts: Partial packet recovery based on compressive sensing for efficient random linear coded transmission," *IEEE Trans. Commun.*, vol. 64, no. 8, pp. 3296–3310, Aug. 2016.

[29] B. S. Adiga, M. G. Chandra, and S. Sapre, "Guaranteed error correction based on Fourier compressive sensing and projective geometry," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2011, pp. 3744–3747.
[30] Y. Rachlin and D. Baron, "The secrecy of compressed sensing measurements," in *Proc. 46th Annu. Allerton Conf. Commun., Control, Comput.*, Urbana, IL, USA, Sep. 2008, pp. 813–817.
[31] T. Bianchi, V. Bioglio, and E. Magli, "Analysis of one-time random projections for privacy preserving compressed sensing," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 2, pp. 313–327, Feb. 2016.
[32] G. Kuldeep and Q. Zhang, "Energy concealment based compressive sensing encryption for perfect secrecy for IoT," in *Proc. GLOBECOM-IEEE Global Commun. Conf.*, Taipei, Taiwan, Dec. 2020, pp. 1–6, doi: 10.1109/GLOBECOM42002.2020.9322181.
[33] H. Peng, Y. Tian, J. Kurths, L. Li, Y. Yang, and D. Wang, "Secure and energy-efficient data transmission system based on chaotic compressive sensing in body-to-body networks," *IEEE Trans. Biomed. Circuits Syst.*, vol. 11, no. 3, pp. 558–573, Jun. 2017.
[34] Z. Niu, M. Zheng, Y. Zhang, and T. Wang, "A new asymmetrical encryption algorithm based on semitensor compressed sensing in WBANs," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 734–750, Jan. 2020.
[35] K. Ashwini, R. Amutha, R. R. Immaculate, and P. Anusha, "Compressive sensing based medical image compression and encryption using proposed 1-D chaotic map," in *Proc. Int. Conf. Wireless Commun. Signal Process. Netw. (WiSPNET)*, Chennai, India, Mar. 2019, pp. 435–439.
[36] R. Moreno-Alvarado, E. Rivera-Jaramillo, H. Perez-Meana, and M. Nakano, "Joint encryption and compression of audio based on compressive sensing," in *Proc. 42nd Int. Conf. Telecommun. Signal Process. (TSP)*, Budapest, Hungary, Jul. 2019, pp. 58–61.
[37] C. Nanjunda, M. A. Haleem, and R. Chandramouli, "Robust encryption for secure image transmission over wireless channels," in *Proc. IEEE Int. Conf. Commun. (ICC)*, vol. 2, May 2005, pp. 1287–1291.
[38] R. Huang and K. Sakurai, "A robust and compression-combined digital image encryption method based on compressive sensing," in *Proc. 7th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, Oct. 2011, pp. 105–108.
[39] Y. Zhang, Y. Xiang, L. Y. Zhang, Y. Rong, and S. Guo, "Secure wireless communications based on compressive sensing: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1093–1111, 2nd Quart., 2019.
[40] G. Kuldeep and Q. Zhang, "Compressive sensing based multi-class privacy-preserving cloud computing," in *Proc. GLOBECOM-IEEE Global Commun. Conf.*, Taipei, Taiwan, Dec. 2020, pp. 1–6, doi: 10.1109/GLOBECOM42002.2020.9348093.
[41] V. Cambareri, M. Mangia, F. Pareschi, R. Rovatti, and G. Setti, "Low-complexity multiclass encryption by compressed sensing," *IEEE Trans. Signal Process.*, vol. 63, no. 9, pp. 2183–2195, May 2015, doi: 10.1109/TSP.2015.2407315.
[42] E. J. Candès, "The restricted isometry property and its implications for compressed sensing," *Compte Rendus de L'Academie des Sci.*, vol. 346, nos. 9–10, pp. 589–592, 2008.
[43] R. Baraniuk, "Compressive sensing [lecture notes]," *IEEE Signal Process. Mag.*, vol. 24, no. 4, pp. 118–121, Jul. 2007, doi: 10.1109/MSP.2007.4286571.
[44] E. J. Candes and M. B. Wakin, "An introduction to compressive sampling," *IEEE Signal Process. Mag.*, vol. 25, no. 2, pp. 21–30, Mar. 2008, doi: 10.1109/MSP.2007.914731.
[45] N. Y. Yu, "Indistinguishability and energy sensitivity of Gaussian and Bernoulli compressed encryption," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 7, pp. 1722–1735, Jul. 2018.
[46] S. Foucart and H. Rauhut, *A Mathematical Introduction to Compressive Sensing*. Basel, Switzerland: Birkhauser, 2013.
[47] K. Hoffman and R. Kunze, *Linear Algebra*. Upper Saddle River, NJ, USA: PHI Learning, 2004.
[48] L. Gan, "Block compressed sensing of natural images," in *Proc. 15th Int. Conf. Digit. Signal Process.*, Cardiff, U.K., Jul. 2007, pp. 403–406.
[49] S. Mun and J. E. Fowler, "Block compressed sensing of images using directional transforms," in *Proc. Data Compress. Conf.*, Cairo, Egypt, Nov. 2009, pp. 3021–3024.
[50] M. Testa, T. Bianchi, and E. Magli, "Energy obfuscation for compressive encryption and processing," in *Proc. IEEE Workshop Inf. Forensics Secur. (WIFS)*, Dec. 2017, pp. 1–6.
[51] G. Kuldeep and Q. Zhang, "Revisiting compressive sensing based encryption schemes for IoT," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Seoul, South Korea, May 2020, pp. 1–6, doi: 10.1109/WCNC45663.2020.9120785.
[52] H. Zorlein, D. Lazich, and M. Bossert, "Performance of error correction based on compressed sensing," in *Proc. 8th Int. Symp. Wireless Commun. Syst.*, Aachen, Germany, Nov. 2011, pp. 301–305, doi: 10.1109/ISWCS.2011.6125372.
[53] E. Miandji, "Sparse representation of visual data for compression and compressed sensing," Ph.D. Dissertation. Dept. Sci. Technol., Linköping Univ., Linköping, Sweden, 2018.
[54] S. Mallat, *A Wavelet Tour of Signal Processing*. NewYork, NY, USA: Elsevier, 1999.
[55] C.-J.-M. Liang, N. B. Priyantha, J. Liu, and A. Terzis, "Surviving Wi-Fi interference in low power ZigBee networks," in *Proc. 8th ACM Conf. Embedded Netw. Sensor Syst. (SenSys)*, 2010, pp. 309–322.
[56] B. Vejlgaard, M. Lauridsen, H. Nguyen, I. Z. Kovacs, P. Mogensen, and M. Sorensen, "Interference impact on coverage and capacity for low power wide area IoT networks," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, San Francisco, CA, USA, Mar. 2017, pp. 1–6, doi: 10.1109/WCNC.2017.7925510.
[57] P. T. Chiou, Y. Sun, and G. S. Young, "A complexity analysis of the JPEG image compression algorithm," in *Proc. 9th Comput. Sci. Electron. Eng. (CEEC)*, Colchester, U.K., Sep. 2017, pp. 65–70, doi: 10.1109/CEEC.2017.8101601.
[58] D. A. Spielman, "The complexity of error-correcting codes," in *Fundamentals of Computation Theory* (Lecture Notes in Computer Science), vol. 1279. Berlin, Germany: Springer, 1997.

GAJRAJ KULDEEP (Student Member, IEEE) received the B.Tech. degree in electronics and communication from NIT Calicut, in 2005, the M.Tech. degree in communication engineering from IIT Delhi, in 2015, and the M.S. degree in information technology security from Masaryk University, Brno, in 2019. He worked in the areas of signal processing and security for than ten years in industry. His research interests include signal processing and security in the Internet of Things.

QI ZHANG (Member, IEEE) received the M.Sc. and Ph.D. degrees in telecommunications from the Technical University of Denmark (DTU), Denmark, in 2005 and 2008, respectively. She is currently an Associate Professor with the Department of Engineering, Aarhus University, Aarhus, Denmark. Besides her academic experiences, she has various industrial experiences. Her research interests include the Internet of Things, mobile edge computing, tactile Internet, compressive sensing, and sensor data compression and storage. She was the Co-Chair of the Co-operative and Cognitive Mobile Networks (CoCoNet) Workshop, ICC Conference, from 2010 to 2015, and the TPC Co-Chair of BodyNets. She is serving as an Editor for *EURASIP Journal on Wireless Communications and Networking*.