Robust Coding of Encrypted Images via Structural Matrix

Yushu Zhang, Kwok-Wo Wong, *Senior Member, IEEE*, Leo Yu Zhang, Di Xiao, *Member, IEEE*,

arXiv:1405.6843v1 [cs.CR] 27 May 2014

Abstract—The robust coding of natural images and the effective compression of encrypted images have been studied individually in recent years. However, little work has been done in the robust coding of encrypted images. The existing results in these two individual research areas cannot be combined directly for the robust coding of encrypted images. This is because the robust coding of natural images relies on the elimination of spatial correlations using sparse transforms such as discrete wavelet transform (DWT), which is ineffective to encrypted images due to the weak correlation between encrypted pixels. Moreover, the compression of encrypted images always generates code streams with different significance. If one or more such streams are lost, the quality of the reconstructed images may drop substantially or decoding error may exist, which violates the goal of robust coding of encrypted images. In this work, we intend to design a robust coder, based on compressive sensing with *structurally random matrix*, for encrypted images over packet transmission networks. The proposed coder can be applied in the scenario that Alice needs a semi-trusted channel provider Charlie to encode and transmit the encrypted image to Bob. In particular, Alice first encrypts an image using globally random permutation and then sends the encrypted image to Charlie who samples the encrypted image using a *structural matrix*. Through an imperfect channel with packet loss, Bob receives the compressive measurements and reconstructs the original image by joint decryption and decoding. Experimental results show that the proposed coder can be considered as an efficient multiple description coder with a number of descriptions against packet loss.

Index Terms—Multiple description code, packet loss, robust coding of encrypted image, structural matrix.

I. Introduction

THE traditional approach of transmitting an image via a communication channel is to perform compression preceding encryption at the sender side; and to decrypt the cipher-image followed by decompression at the receiving side. However, consider a particular scenario in which Alice needs to transmit an image to Bob but wants to keep the image confidential to an untrusted channel provider Charlie. This implies that Alice should encrypt the image moderately and Charlie has to compress the encrypted image without any knowledge of the cryptographic key. At the receiving side, Bob performs both decompression and decryption to reconstruct the original image.

Some works for compressing encrypted images have been reported in recent years. A scheme for compressing encrypted images using a 2-D source model and LDPC codes was developed in [1]. It is based on the finding that encrypted

Y. Zhang, D. Xiao are with College of Computer Science, Chongqing University, Chongqing, 400044 China (e-mail: yushuboshi@163.com; xiaodi_cqu@hotmail.com)

K.W. Wong and L. Zhang are with Department of Electronic Engineering, City University of Hong Kong, Kowloon, Hong Kong (e-mail: itkwwong@cityu.edu.hk; leocityu@gmail.com)

data are as compressible as unencrypted ones by considering the problem as distributed source coding. The lossless compression of encrypted grayscale and color images has been presented in [2], by decomposing the image pixels into bit-planes. By applying the approach of [3] to the prediction error domain, a better lossless compression performance on the encrypted grayscale and color images is achieved [4]. A progressive compression approach for processing an encrypted image has been suggested, in which the decoder needs to study the local statistics of a low-resolution image and then decodes the next resolution level [5]. Meanwhile, the lossy compression of encrypted images was also studied to achieve higher compression ratios [3, 6–10]. For example, based on the results of [3], a practical model for compressing encrypted binary image has been developed in [6]. Zhang proposed a novel scheme for the lossy compression of an encrypted image at a flexible compression ratio [7], in which a pseudorandom permutation is used to encrypt the plain-image. Making use of the process of masking the original pixel values by a modulo-256 addition with pseudorandom numbers, Zhang *et al.* further proposed a scheme for the scalable coding of encrypted images [8]. In [9], the compression is performed on an encrypted image with multi-layer decomposition. Zhou *et al.* designed an efficient encryption-then-compression scheme for images via error clustering, in which both lossless and lossy compressions were considered [10]. The above-mentioned approaches of compressing encrypted images are not suitable for high packet loss transmission in non-feedback systems, since the resultant coded streams have substantially unequal importance such that the loss of some codewords may cause severe error propagation and results in unsatisfactory decoded result.

Multiple description coding is a common approach to deal with packet loss during transmission. In general, a multiple description coder generates two or more sub-streams referred to as descriptions. The packets of each description are transmitted over multiple disjoint paths. After receiving each description, the decoder is able to perform a low-quality reconstruction. If all the descriptions have been received, the reconstruction quality is the best. Such a protocol allows a channel with network congestion or packet loss to perform the decoding at the expense of reconstruction quality. Multiple description coding of natural images has been extensively studied in [11–14], where spatial correlations are often eliminated by using sparse transforms like DWT. However, they are not suitable for encrypted images since sparse transforms are nearly ineffective on encrypted images due to the low correlation between the pixels. A multiple description coder especially designed for encrypted images is rarely reported so far.

Consider the scenario that Alice needs the semi-trusted channel coder Charlie to transmit an encrypted image to Bob. When a high packet loss is encountered in the chan-

nel between Charlie and Bob, Charlie should first encode the encrypted image for error control. This motivates us to explore a multiple description coder aiming at the robust coding of encrypted images. In this work, we design such a coder based on compressive sensing (CS) with a structurally random matrix (SRM). The proposed coder is comprised of three parts: permutation-based encryption by Alice, encoding using structural matrix (SM) by Charlie, and joint decryption and decoding by Bob. In particular, Alice first encrypts an image using globally random permutation and then sends the encrypted image to the semi-trusted channel encoder Charlie who samples the encrypted image using a structural matrix. Through a channel with high packet loss, Bob receives the compressive measurements and reconstructs the original image by joint decryption and decoding. Moreover, we discuss the relationship between our approach and existing algorithms and describe two other cryptographic applications of SRM. In the performance evaluation, we explore the relationship between packet loss rate and sampling rate and then introduce a feasible quantization approach to the compressive measurements of encrypted images. Finally, we investigate the robustness of the proposed coder at different parameter settings. It is verified that the proposed coder can be regarded as an efficient multiple description coder with a number of descriptions against packet loss.

The rest of this paper is organized as follows. Section II is a brief review of the theory of CS using SRM. In Section III, the robust coding of encrypted images based on CS with SM is proposed. Further discussions can be found in Section IV while the performance evaluation is reported in Section V. Finally, we conclude the paper with some remarks in Section VI.

II. Compressive Sensing by Structurally Random Matrix

The fundamental Shannon/Nyquist sampling theory is widely-accepted as the keystone in signal acquisition and reconstruction. It governs the sampling process from the perspective of signal bandwidth. Nevertheless, the number of required measurements can be so large that the storage becomes unbearable and the acquisition time can be very long. Compressive sensing [15, 16] is a new sampling theory which allows the exact recovery of a sparse signal from a few linear projections lower than the Nyquist rate. The underlying property of CS is the sparsity of interest. A signal $\mathbf{x}$ of length N is said to be K-sparse or compressible if it can be well approximated using only $K \ll N$ coefficients over some sparsifying basis $\mathbf{\Psi}$ as follows

$$\mathbf{x} = \mathbf{\Psi s}, \tag{1}$$

where $\mathbf{s}$ is the transform coefficient vector that contains at most K significant nonzero entries. Compressive sensing theory indicates that $\mathbf{x}$ can be acquired by the following random measurement

$$\mathbf{y} = \mathbf{\Phi x}, \tag{2}$$

where $\mathbf{\Phi}$ is a $M \times N$ $(M < N)$ random measurement matrix and $\mathbf{y}$ represents the measurement coefficient vector. $\mathbf{x}$ can be faithfully recovered from only $M = \mathcal{O}(K \log N)$ measurements through l_1-minimization

$$\min \|\mathbf{s}\|_1 \text{ s.t. } \mathbf{y} = \mathbf{\Phi \Psi s}, \tag{3}$$

where the measurement matrix $\mathbf{\Phi}$ should be highly incoherent with the sparsifying basis $\mathbf{\Psi}$.

The design of an efficient measurement matrix is still a big challenge in CS. Do *et al.* [17] introduced a fast and efficient measurement matrix for practical CS. The matrix is called a structurally random matrix (SRM), which, in many aspects, outperforms the existing popular sensing matrices such as Gaussian, Bernoulli and Fourier matrices [18–20]. Gaussian and Bernoulli matrices require high computation complexity and huge memory buffering due to their completely unstructured nature while Fourier matrix works well only if the sparsifying basis is an identity matrix. Do *et al.* also pointed out that SRM possesses the following features: optimal or near-optimal sensing performance; universality; low complexity; hardware/optical implementation friendless. In particular, it is defined as a product of three matrices

$$\mathbf{\Phi} = \sqrt{\frac{N}{M}} \mathbf{DFR} \tag{4}$$

where $\mathbf{R} \in \mathbb{R}^{N \times N}$ is either a uniform random permutation matrix or a diagonal random matrix whose diagonal entries are Bernoulli random variables. $\mathbf{F} \in \mathbb{R}^{N \times N}$ represents an orthonormal matrix that is selected among popular fast computable transforms such as Fast Fourier Transform (FFT), Discrete Cosine Transform (DCT) and Walsh-Hadamard Transform (WHT). $\mathbf{D} \in \mathbb{R}^{N \times N}$ is a subsampling operator selecting a random subset of rows of the matrix $\mathbf{FR}$. Interested readers can refer to [17] for more details on SRM.

III. Robust Coding of Encrypted Image via Structural Matrix

Compressing encrypted images is a big challenge due to the fact that an effective encryption algorithm must have already removed or lowered the correlation among neighbouring image pixels to increase the entropy. However, classical image compression schemes like JPEG 2000 always make use of the high correlation and non-uniformity of image pixels. Some lightweight encryption techniques only permute the pixels or mask the pixel values by a keystream. As a result, the encrypted image may still be compressed to certain extent by leveraging some particular coding techniques [1–10]. The lightweight encryption schemes are usually not secure enough, but they are employed in some specific application scenarios. The proposed scheme does not aim at improving the compression performance on encrypted images but focuses on designing a robust coder for the transmission of encrypted images over a channel with high packet loss rate.

The proposed coder is based on SRM. The basic idea is to split the measurement matrix $\mathbf{\Phi} = \sqrt{N/M} \mathbf{DFR}$ in (4) into two matrices: the matrix $\mathbf{R}$ and the matrix $\sqrt{N/M} \mathbf{DF}$. $\mathbf{R}$ is a random permutation matrix which can serve as a lightweight

encryption tool while $\sqrt{N/M}\mathbf{DF}$ can be considered as a new measurement matrix in the proposed coder. First, Alice encrypts an image using $\mathbf{R}$ and then sends the encrypted image to the channel coder Charlie who samples the encrypted image using $\sqrt{N/M}\mathbf{DF}$. Through a high packet loss channel, Bob receives the compressive measurements and reconstructs the original image by joint decryption and decoding using $\sqrt{N/M}\mathbf{DFR}$, as illustrated in Fig. 1. The random permutation $\mathbf{R}$ is constructed from a secret seed known to both Alice and Bob.

The robust coding of encrypted images by structural matrices is composed of three steps: permutation-based encryption by Alice, encoding using structural matrix by Charlie, and joint decryption and decoding by Bob.
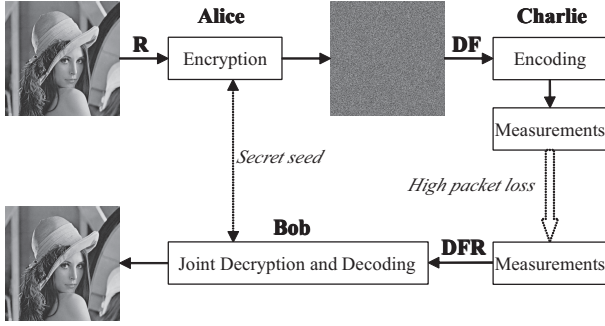

Fig. 1. A block diagram of the proposed coder.

A. Permutation-based Encryption by Alice

The encrypted image is obtained by applying random spatial permutation on the image. Alice converts the original image $\mathbf{X}$ of size $N_1 \times N_2$ into a vector $\mathbf{x}$ with length $N = N_1 \times N_2$. Then she encrypts $\mathbf{x}$ to the cipher sequence $\mathbf{x}_{en}$ by applying a random permutation matrix $\mathbf{R} \in \mathbb{R}^{N \times N}$, governed by

$$\mathbf{x}_{en} = \mathbf{R}\mathbf{x}. \tag{5}$$

$\mathbf{x}_{en}$ is rearranged into a 2-D cipher image $\mathbf{X}_{en}$, which is then sent to Charlie who obtains the encrypted sequence $\mathbf{x}_{en}$ by arranging $\mathbf{X}_{en}$. The conversion between vector and matrix is known to both Alice and Charlie. The random permutation matrix $\mathbf{R}$ is a binary matrix in which each row or column has exactly one 1 and the rest are all zero. It is generated by a pseudo-random generator with initial random seed shared between Alice and Bob. The reader may refer to [21, 22] for more illustrations on the encryption methods based on permutation matrix. It should be noticed that permutation-based decryption is performed by multiplying the cipher image with the inverse permutation matrix. Interestingly, it is not necessary to invert the matrix since the inverse matrix is obtained by transposing the permutation matrix itself, i.e., $\mathbf{R}^{-1} = \mathbf{R}^{T}$. The key space is $N!$ so that it is not likely for Charlie to launch a brute force search when N is sufficiently large. Permutation-based encryption cannot hide the statistical information of the original image due to its unaltered histogram. In spite of this, it can still be employed in applications where high secrecy is not a must.

B. Encoding using Structural Matrix by Charlie

After the encrypted image has been received, Charlie constructs a special measurement matrix to sample it. This matrix is tailored to the encrypted image and is called structural matrix (SM). It is governed by

$$\mathbf{A} = \sqrt{\frac{N}{M}}\mathbf{DF}, \tag{6}$$

where $\mathbf{D}$ and $\mathbf{F}$ are as described in (4). Encoding using SM is expressed as

$$\mathbf{y} = \mathbf{A}\mathbf{x}_{en}. \tag{7}$$

Obviously, SM is derived from SRM due to the fact that $\mathbf{y} = \mathbf{A}\mathbf{x}_{en} = \sqrt{N/M}\mathbf{DF}\mathbf{x}_{en} = \sqrt{N/M}\mathbf{DFR}\mathbf{x} = \mathbf{\Phi}\mathbf{x}$. The scenario that SM is applied for permuted or encrypted images is the same as that SRM is employed for spatial images. Structural matrix is expediently selected among some popular computable matrices such as FFT, SCT, WHT or their block diagonal versions. The M rows are extracted at random from SM. These matrices have stable structures like SRM and they outperform Gaussian and Bernoulli matrices in terms of computational complexity and memory requirement. It can be easily inferred that the performance of SM measuring the encrypted image is the same as that of SRM sampling the original image. It has been mathematically proved in [17] that entries of $\mathbf{AR\Psi}$ asymptotically form a normal distribution $\mathcal{N}\left(0, \sigma^2\right)$, where $\mathbf{\Psi}$ is an arbitrary orthonormal matrix and $\sigma^2 \leq \mathcal{O}\left(\frac{1}{N}\right)$, under some mild assumptions: $\mathbf{F}$ is an unit-row matrix whose entries have absolute magnitude in the order of $\sigma^2 \leq \mathcal{O}\left(\frac{1}{N}\right)$ and the sum of entries in each row is equal to zero; $\mathbf{\Psi}$ is an unit-norm column matrix with entries having maximal absolute magnitude in the order of $\mathcal{O}\left(1\right)$ and the average sum of entries in each column in the order of $\sigma^2 \leq \mathcal{O}\left(\frac{1}{N}\right)$. The entries in each row of $\mathbf{F}$ and each column of $\mathbf{\Psi}$ are not all equal. Do *et al.* also found that SRM supports block-based models with high incoherence between $\mathbf{FR}$ and $\mathbf{\Psi}$. It should be noticed that the randomization $\mathbf{D}$ can induce a new application scenario, which will be described later.

C. Joint decryption and decoding by Bob

At the receiving side, Bob obtains the compressive measurements $\mathbf{y}$ and applies joint decryption and decoding to recover the original image using the following algorithm:

$$\min \|\mathbf{s}\|_1 \text{ s.t. } \mathbf{y} = \mathbf{AR\Psi}\mathbf{s} = \sqrt{\frac{N}{M}}\mathbf{DFR\Psi}\mathbf{s} \tag{8}$$

As a result, $\mathbf{x} = \mathbf{\Psi}\mathbf{s}$. The recovery criterion has been stated in [17]: with a probability of at least $1 - \delta$, the sensing framework using SRM can exactly recover K-sparse signals if $M \geq \mathcal{O}\left(\frac{N}{B}K\log^2\frac{N}{\delta}\right)$, where B is the block size. Theoretically, this guarantees the capability of SM in encoding the encrypted image.

IV. FURTHER DISCUSSIONS

In some references [23–26], CS was applied for natural image coding but this is not an appropriate approach in terms of compression efficiency [27]. Nevertheless, in view of the robustness property of multiple description coder, CS can be a good candidate [14, 28, 29]. A representative work was presented by Deng *et al.* in [14], in which the compressive measurements can be viewed as a number of descriptions mainly because of their *democracy* properties. If the measurement matrix follows the Gaussian distribution, each CS measurement possesses a similar amount of information of the original signal [30]. Specifically, the sampling is performed on the frequency coefficients generated by two-dimensional DWT and at the decoding side, two different recovery algorithms are developed for the low-frequency and high-frequency subbands, respectively, by fully exploiting the intra-scale and inter-scale correlation of multiscale DWT. Although experimental results showed that this CS-based codec is much more robust for lossy channels in comparison with existing CS-based coding schemes [14], it is not suitable for processing encrypted images. This is because the efficiency of sparse transforms like DWT mainly depends on strong correlation between pixels, which must be weakened by the encryption process, even if a lightweight one is employed.

CS-based compression of encrypted image has been explored in only two references [31, 32], both of which aimed at the linear transformation encryption operations. Both coders adopt the block-to-block structure which possesses a straightforward advantage, i.e., parallel CS encoding and decoding. Unfortunately, such a block encryption manner suffers from three drawbacks. Firstly, individual block operation makes the cipher more insecure than global image transform. In order to enhance the security, different blocks may be endowed with different keys and more keys need to be transmitted. Secondly, a plain image is divided into a number of non-overlapping blocks having different statistical features and unequal significance. When these blocks are individually sampled, the measurements have unequal significance. As a result, both coders cannot be considered as efficient multiple description coders. Thirdly, blocking artifact cannot be avoided. In addition, a random matrix is chosen as the measurement matrix. In practical sensing applications, this is costly as very high computational complexity and huge memory buffering are required due to the completely unstructured nature of the matrix [20]. The proposed coder does not suffer from the above drawbacks. Global permutation is a common lightweight image encryption technique which is more secure than individual block permutation. The random permutation $\mathbf{R}$ relocates all the pixels globally. It destroys the image structure and converts a meaningful image into one look like white noise [17]. The structural matrix $\mathbf{A}$ in sampling the permuted image supports block processing, meaning that parallel CS encoding can be applied. $\mathbf{R}$ disperses the energy of the whole image and $\mathbf{F}$ further spreads the energy over all the measurements. Consequently, the sampled measurements obtained by SM roughly have the same significance. The proposed coder is a multiple description coder with a number of descriptions

whose capability in resisting against packet loss is verified in the next section. There is no blocking artifact as a unified decoder is used to reconstruct the whole image. Compared with random matrix, SM facilitates fast computation and low-complexity electronic or optical implementation.

It is worth mentioning that SRM also induces two other applications related to coding and encryption due to the randomness of $\mathbf{R}$ and $\mathbf{D}$. The first application is illustrated in Fig. 2(a). Alice still permutes the image with $\mathbf{R}$ while Charlie can further encrypt the permuted image with $\mathbf{DF}$. This is because the matrix $\mathbf{D}$ is a random selection operation which can serve as a secret key shared between Charlie and Bob. Another application is the direct encryption by Alice using $\mathbf{DFR}$, as shown in Fig. 2(b). Both applications can be considered as joint coding and encryption schemes. The size of the key space due to $\mathbf{D}$ is given by the combinatorial number $\begin{pmatrix} M \\ N \end{pmatrix}$. It seems that the current size of key space upgraded as $N! + \begin{pmatrix} M \\ N \end{pmatrix}$ is sufficiently large to resist brute-force attack. Unfortunately, the encryption schemes based on CS with SRM is probably insecure against some potential attacks such as known-plaintext attack and chosen-plaintext attack due to its linearity [33]. As a consequence, the security level of CS needs to be analyzed. For example, a low-complexity multiclass encryption scheme has been designed in [34, 35], which possesses strong resistance against known-plaintext attacks.
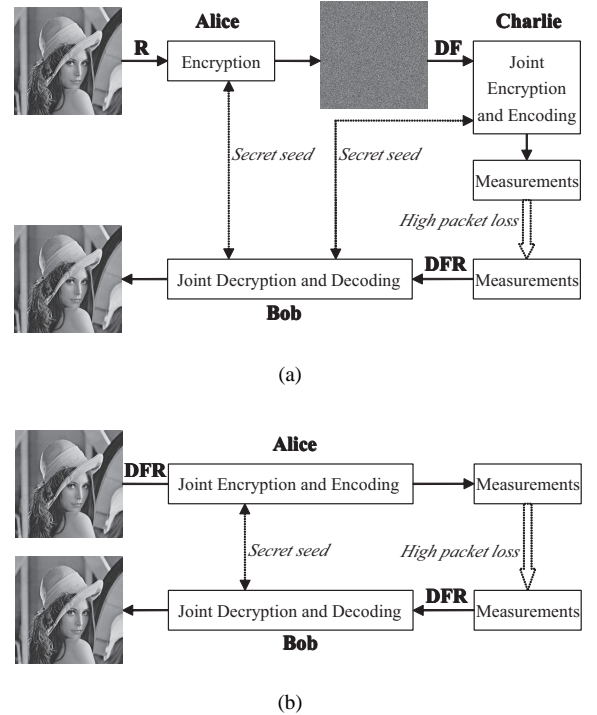

(a)

(b)

Fig. 2.   Two other applications of SRM.

V. PERFORMANCE EVALUATION

Our simulation settings are similar to those using SRM [17]. Four natural images of size 512×512 including *Lena*, *Peppers*,
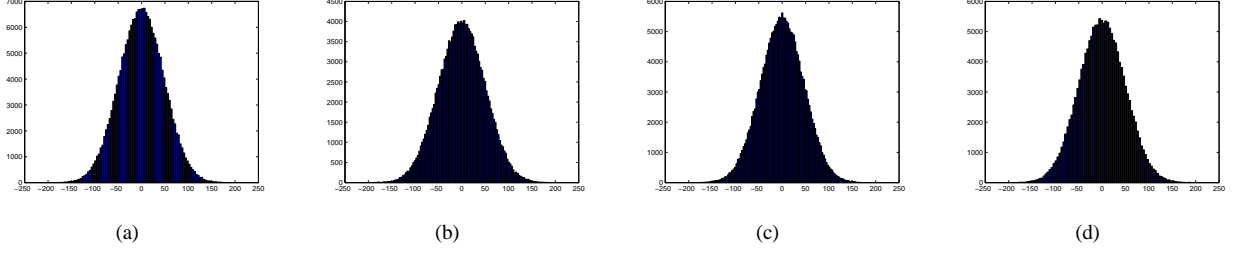
Fig. 4. Histograms of the encoded images for the cases: (a) Lena, SR=0.8, BDCT32, PLR=0.05; (b) Peppers, SR=0.6, BWHT32, PLR=0.10; (c) Boat, SR=0.8, BDCT32, PLR=0.15; (d) Goldhill, SR=0.6, BWHT32, PLR=0.20.
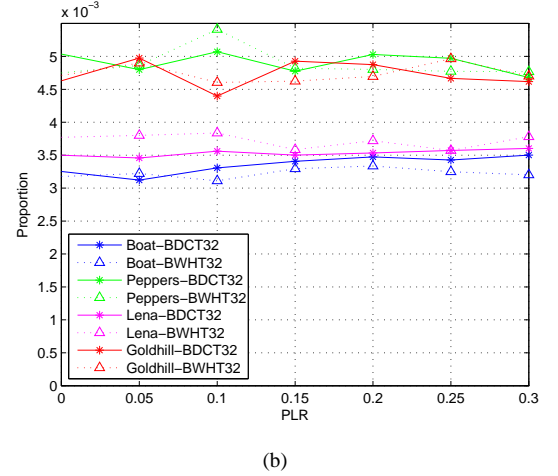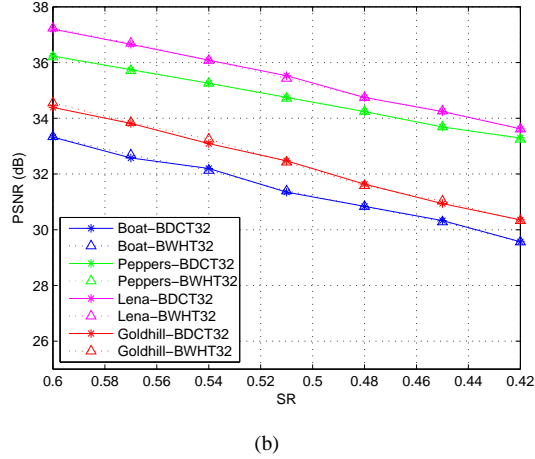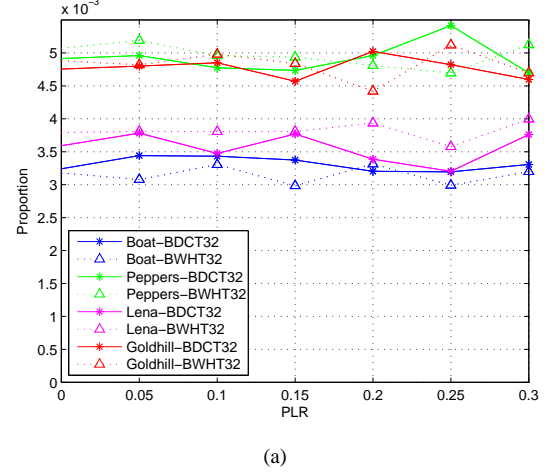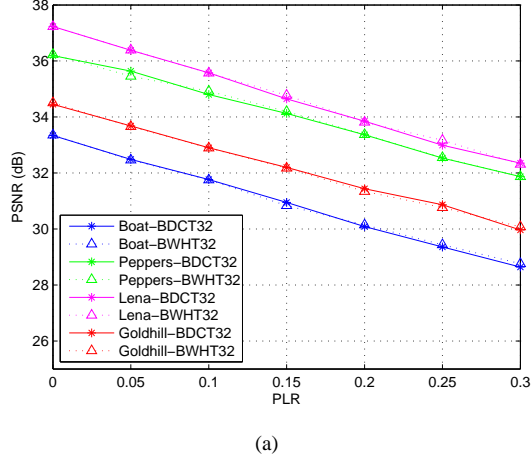

Fig. 3. PSNRs of the reconstructed images with respect to (a) PLR; (b) SR.

Fig. 5. The values of γ versus PLR for (a) SR=0.6; (b) SR=0.8.

Boat and *Goldhill* are used for testing. The sparsifying basis $\mathbf{\Psi}$ is Daubechies 9/7 wavelet transform. The reconstruction algorithm is GRSR in [36]. $\mathbf{R}$ and $\mathbf{D}$ are generated using MATLAB commands and $\mathbf{F}$ is chosen as block diagonal DCT (BDCT) and block diagonal WHT (BWHT). The packet size is set to 100 unless specified. We first explore the relationship between packet loss rate and sampling rate and then describe a feasible quantization approach for the compressive measurements of encrypted images. Finally, the robustness of the proposed coder at different parameter settings is investigated.

A. Relationship between packet loss rate and sampling rate

The compressive measurements $\mathbf{y}$ of length M can be partitioned, at equal intervals, into a number of packets. Each packet carries a similar amount of information of the original image since all the measurements have roughly equal importance. If a packet contains m measurements, there are $\lceil M/m \rceil$ packets in total. Lost packets always occur randomly and Bob will update $\mathbf{D}$ according to the received packets. We denote packet loss rate as PLR which can be up to 30% in real cases [37]. The sampling rate (SR) is defined as $SR = M/N$. For example, if $M = 157290$ and $m = 100$,
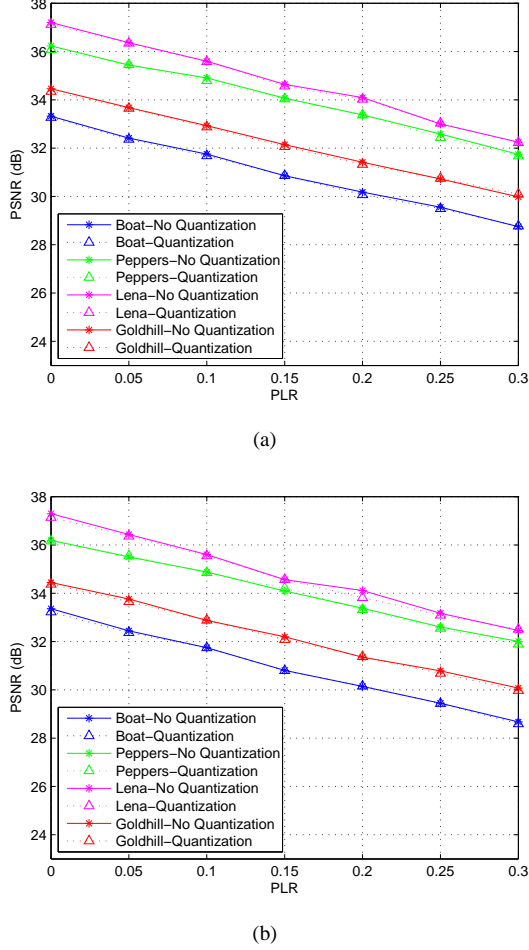
(a)

(b)

Fig. 6. Rate-Distortion performance of the quantization for (a) SR=0.6, BDCT32; (b) SR=0.6, BWHT32.

then $SR = 157290/512^2 = 0.60$ and the number of packets is $\lceil 157290/100 \rceil = 1573$. If $PLR = 0.20$, the number of lost packets is $1573 \times 0.2 \doteq 315$ and the number of received packets is 1258. In other words, Charlie sends 512^2 measurements and Bob receives about 125800 measurements among them. This is similar to the case that the sampling rate is changed to $SR' = 125800/512^2 \doteq 0.48$. In fact, this equivalence is reasonable due to the roughly equal importance of the measurements. This example inspires us a relationship between SR and PLR.

In general, for a given $SR = \alpha$ $(0 < \alpha < 1)$, $PLR = \beta$ $(0 \le \beta \le 0.3)$ is basically equivalent to $SR = \alpha (1 - \beta)$. This can be verified in Fig. 3, where BDCT32 and BWHT32, corresponding to the solid line and the dashed line, respectively, mean that each sub-matrix in the diagonal of $\mathbf{F}$ has a size of 32×32. It can be observed that the effects of BDCT and BWHT are consistent since each pair of solid and dashed lines coincides with each other while other conditions are identical. The value of SR is set as SR=0.6 in Fig. 3(a). $PLR = \beta$ in Fig. 3(a) corresponds to $SR = 0.6 \times (1 - \beta)$ in Fig. 3(b). A comparison between Fig. 3(a) and Fig. 3(b) shows that the former PSNR roughly coincides with the latter one. Both starting points have the same PSNR value, i.e., $PLR = 0$

in Fig. 3(a) and SR=0.6 in Fig. 3(b). However, with the increase of PLR and the reduction of SR, the PSNR value of the former is sightly lower than that of the latter. There are three factors causing this difference: (i) Weak correlations exist between adjacent measurements. The amount of information of the whole packet containing m successive measurements is gracefully greater than that provided by the m randomly-sampled measurements; (ii) After packing the measurements, the number of measurements m' in the last packet is less than m as long as M is not divisible by m. The last packet will not be lost with high probability $(1 - \beta)$ such that the actual $SR = \alpha(m(\lceil M/m \rceil (1 - \beta) - 1) + m')/M < \alpha(1 - \beta)$. (iii) The rounding effect of $\lceil M/m \rceil \beta$ possibly results in the actual $PLR = round(\lceil M/m \rceil \cdot \beta)/\lceil M/m \rceil > \beta$. Revealing such a connection of PLR and SR helps to adjust the SR according to the PLR in real-time transmission. Bob distinguishes the PLR according to the received packets and then feeds back to Charlie who adjusts the SR to guarantee a certain PSNR value for the image received by Bob.
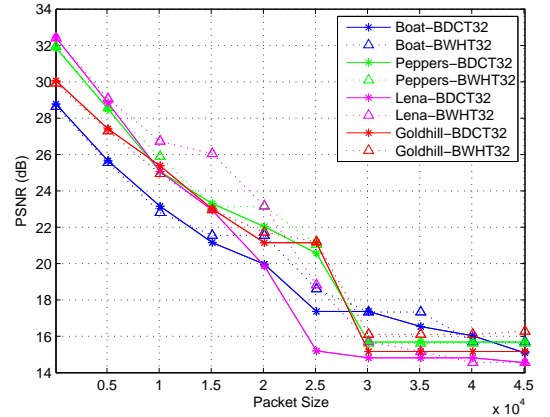
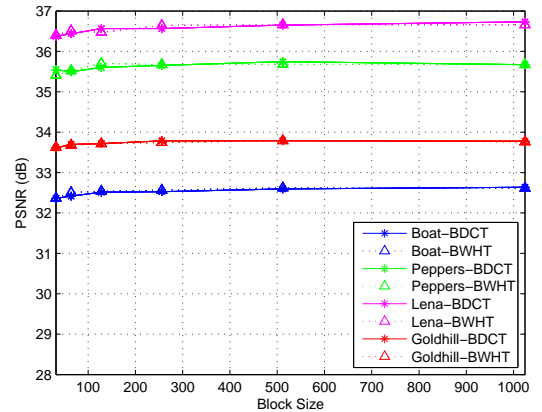

Fig. 10. PSNR versus packet size when SR=0.6 and PLR=0.3.

Fig. 11. PSNR versus block size of SM when SR=0.6 and PLR=0.05.

Fig. 7. The reconstructed images and their PSNR values under SR=0.8: (a) PSNR=35.7965, PLR=0.2, BWHT32; (b) PSNR=33.8944, PLR=0.3, BWHT32; (c) PSNR=35.2942, PLR=0.2, BDCT32; (d) PSNR=33.2762, PLR=0.3, BDCT32.

Fig. 8. The reconstructed images and their PSNR values under SR=0.5: (a) PSNR=32.6432, PLR=0.2, BWHT32; (b) PSNR=31.2287, PLR=0.3, BWHT32; (c) PSNR=32.0629, PLR=0.2, BDCT32; (d) PSNR=30.7208, PLR=0.3, BDCT32.

Fig. 9. The reconstructed images and their PSNR values under SR=0.2: (a) PSNR=26.2722, PLR=0.2, BWHT32; (b) PSNR=25.4766, PLR=0.3, BWHT32; (c) PSNR=26.1835, PLR=0.2, BDCT32; (d) PSNR=24.9015, PLR=0.3, BDCT32.

TABLE I
PSNR VERSUS ROUND-OFF AND WITHOUT ROUND-OFF (LENA, SR=0.6, BDCT32).

PLR	0	0.05	0.10	0.15	0.20	0.25	0.30
Round-off	37.18	36.37	35.54	34.59	33.79	33.16	32.15
Without round-off	37.22	36.37	35.66	34.61	34.00	33.25	32.34
Difference	0.04	0.00	0.12	0.02	0.21	0.09	0.19

B. Quantization of Compressive Measurements of Cipher Image

When the compressive measurements are transmitted over a communication channel, they need to be efficiently quantized and encoded. Therefore, the measurements' statistics are required and an optimal quantizer should be tailored to the measurements for minimizing the amount of distortion during reconstruction. The statistical distribution of compressive measurements obtained by SRM has been well studied [38]. It has been pointed out that the encryption performed by a random permutation on the pixel indices makes the measurements suitable for quantization by causing the measurements' distribution roughly normal. The measurements obtained by applying SM to the encrypted image approximately yield a Gaussian distribution. This is also observed in Fig. 4, which depicts the histograms of various encoded images in different cases.

A uniform scalar quantization is employed to round each entity of y to the nearest integer. The difference in distortion caused by the round-off is extremely subtle, as shown in Tables I and II. Moreover, we can observe from Fig. 4 that the measurement values roughly lie between -150 and 150. The farther the measurement value deviates from zero, the fewer

TABLE II
PSNR VERSUS ROUND-OFF AND WITHOUT ROUND-OFF (LENA, SR=0.8, BWHT32).

PLR	0	0.05	0.10	0.15	0.20	0.25	0.30
Round-off	40.96	39.27	38.21	36.82	35.70	34.69	33.96
Without round-off	41.01	39.54	38.34	36.82	35.72	35.02	34.00
Difference	0.05	0.27	0.13	0.00	0.02	0.33	0.04

the number of measurements are required. Our quantization method only reserves and rounds the values located within the interval $[-127.5, 127.5)$. Others are discarded due to two reasons: (i) The discarded measurements make up only a low proportion, marked as γ, of the whole measurements. Figure 5 lists the values of γ at different parameter settings. γ is basically smaller than 0.0055, which implies that either the PLR rises slightly to $PLR = \beta + \gamma$ or the SR drops a small portion $\alpha\gamma$ by the reason of the approximately equal importance among the measurements; (ii) The reserved measurement values can be one-to-one mapped to the interval $[0, 255]$ through adding 128 to every value. The integers in $[0, 255]$ not only can be fully represented by 8-bit numbers, but also match with the common-adopted 256 grayscales in the images. After the encoding process is completed, an image can still be stored in 8-bit format, which leads to great convenience in practical usage.

The quantization distortion is caused by two factors: the decimal round-off and the proportion of discarded measurements. The first factor is insignificant, as justified by the data listed in Tables I and II while the second one is the same because γ is basically smaller than 0.0055. It can also be justified by the rate-distortion curves plotted in Fig. 6, in which the dashed and solid lines correspond to cases with and without quantization, respectively. These two lines are almost identical and they indicate that the proposed quantization method works well.

C. Robustness

When the proposed coder is used in a packet network, the robustness is directly related to PLR and SR. Figures 7-9 show some reconstructed Lena and Peppers images at different values of SR and PLR. It can be observed that most of the visual information of the original images can be recovered even when $SR = 0.2$ and $PLR = 0.3$. This demonstrates that the proposed coder possesses high robustness against packet loss. Besides, the coder does not result in blocking artifacts. In the aforementioned experiments, the packet size is set to 100 while the block size of SM is 32×32. In fact, the robustness is more or less related to both values.

As analyzed previously, there are three factors causing the PSNR difference in exploring the relationship between SR and PLR. Yet these factors arise from the packet size m. Intuitively, with an increasing m, the PSNR value descends to some extent. This conjecture is justified by Fig. 10, where the parameter settings are $SR = 0.6$ and $PLR = 0.3$. The smaller the packet size, i.e., the more the number of descriptions, the better the reconstructed image quality is. Naturally, the best case is that each measurement forms a description. When the packet size is between 0 and 3×10^4,

the PSNR value drops with the reduction in the number of packets. However, when the packet size is larger than 3×10^4, the PSNR virtually has no change. This is because that the number of packets is basically reduced to two and remains unchanged. If one of these two packets is lost, it means that half of the successive measurements are sampled. This successional sampling violates the randomness of the down-sampling operator $\mathbf{D}$. The analyses indicate that if the transmission channel allows a small quantity of descriptions and the PLR is too large, for instance, only two descriptions and $PLR \geq 0.3$, the proposed coder cannot be regarded as an efficient multiple description coder. In order to fix this problem, Charlie has to improve the SR. Consider an extreme scenario that $SR = 1$, i.e., full redundancy without compression, the encoding process is changed to $\mathbf{y} = \mathbf{Fx}_{en}$. Such an encoder cannot be guaranteed by the theory of SRM and a great many successive measurements' loss will substantially affect the quality of the reconstructed image. Fortunately, a solution has been developed to cope with this scenario. Associating a realization of down-sampling operator $\mathbf{D}$ that truncates the first or M randomly-selected elements after arbitrarily permuting the signal, Charlie introduces a new random permutation $\mathbf{R}'$ known by Bob. The present encoding form is $\mathbf{y} = \mathbf{R}'\mathbf{Fx}_{en}$. When a packet containing many successive measurements is lost, Bob receives the information $\hat{\mathbf{y}} = \beta\mathbf{R}'\mathbf{Fx}_{en}$. Let $\mathbf{D}' = \beta\mathbf{R}'$, which can be considered as a down-sampling operator, then $\hat{\mathbf{y}} = \mathbf{D}'\mathbf{Fx}_{en}$. In other words, the PLR is the very SR. Even if $PLR = 0.8$, which is equivalent to $SR = 0.8$, the reconstructed image quality is still visually acceptable.

The purpose of having the measurement matrix in a block mode is to reduce storage space and computational complexity at the cost of a lower quality of the recovered signal. In the proposed coder, we investigate PSNR versus the block size of SM when $SR = 0.6$ and $PLR = 0.05$, as shown in Fig. 11. The greater the block size, the higher the PSNR is. However, the rate of increase is quite slow. Meanwhile, a larger block size of SM needs more memory and consumes more resources. Consequently, a trade-off between them is required. In general, the block size of SM is set as 32∼256.

VI. CONCLUSION

A novel and robust coder for processing encrypted images against packet loss has been designed. It is different from the existing approaches of the robust coding of natural images and the compression of encrypted images. The proposed coder based on SRM is composed of three parts: permutation-based encryption by Alice, encoding with structural matrix by Charlie, and joint decryption and decoding by Bob. In addition, we have investigated the relationship between the proposed

and the existing methods. Two other cryptographic applications of SRM have also been suggested. In the performance evaluation, we have explored the relationship between packet loss rate and sampling rate. A feasible approach for quantizing the compressive measurements of encrypted images has been introduced. Finally, we have investigated the robustness of the proposed coder at different parameter settings. It has been verified that our coder can be considered as an efficient multiple description coder with a number of descriptions to resist packet loss.

REFERENCES

[1] D. Schonberg, S. Draper, and K. Ramchandran, "On compression of encrypted images," in *Proc. IEEE Int. Conf. Image Process.*, pp. 269–272, Atlanta, GA, Oct. 2006.

[2] R. Lazzeretti and M. Barni, "Lossless compression of encrypted grey-level and color images," in *Proc. 16th Eur. Signal Process. Conf. (EUSIPCO 2008)*, Lausanne, Switzerlan, Aug. 2008.

[3] M. Johnson, P. Ishwar, V. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," *IEEE Trans. Signal Process.*, vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

[4] A. Anil Kumar and A. Makur, "Distributed source coding based encryption and lossless compression of gray scale and color images," in *Proc. 10th Workshop on Multimedia Signal Process. (MMSP)*, pp. 760–764, Cairns, Qld, Oct. 2008.

[5] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," *IEEE Trans. Image Process.*, vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[6] D. Schonberg, S. C. Draper, C. Yeo, and K. Ramchandran, "Toward compression of encrypted images and video sequences," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 4, pp. 749–762, Dec. 2008.

[7] X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 53–58, Mar. 2011.

[8] X. Zhang, G. Feng, Y. Ren, and Z. Qian, "Scalable coding of encrypted images," *IEEE Trans. Image Process.*, vol. 21, no. 6, pp. 3108–3114, Jun. 2012.

[9] X. Zhang, G. Sun, L. Shen, and C. Qin, "Compression of encrypted images with multi-layer decomposition," *Multimed. Tools Appl.*, pp. 1–14, Feb. 2013.

[10] J. Zhou, X. Liu, O. C. Au, and Y. Y. Tang, "Designing an efficient image encryption-then-compression system via prediction error clustering and random permutation," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 1, pp. 39–50, Jan. 2014.

[11] S. D. Servetto, K. Ramchandran, V. A. Vaishampayan, and K. Nahrstedt, "Multiple description wavelet based image coding," *IEEE Trans. Image Process.*, vol. 9, no. 5, pp. 813–826, May 2000.

[12] S.-H. Yang and P.-F. Cheng, "Robust transmission of spiht-coded images over packet networks," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 17, no. 5, pp. 558–567, May 2007.

[13] B. Li and L. Peng, "Balanced multifilter banks for multiple description coding," *IEEE Trans. Image Process.*, vol. 20, no. 3, pp. 866–872, Mar. 2011.

[14] C. Deng, W. Lin, B.-S. Lee, and C. T. Lau, "Robust image coding based upon compressive sensing," *IEEE Trans. Multimed.*, vol. 14, no. 2, pp. 278–290, Apr. 2012.

[15] 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.

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

[17] T. T. Do, L. Gan, N. H. Nguyen, and T. D. Tran, "Fast and efficient compressive sensing using structurally random matrices," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 139–154, Jan. 2012.

[18] E. J. Candès and T. Tao, "Near-optimal signal recovery from random projections: Universal encoding strategies?," *IEEE Trans. Inf. Theory*, vol. 52, no. 12, pp. 5406–5425, Dec. 2006.

[19] S. Mendelson, A. Pajor, and N. Tomczak-Jaegermann, "Uniform uncertainty principle for bernoulli and subgaussian ensembles," *Constr. Approx.*, vol. 28, no. 3, pp. 277–289, Dec. 2008.

[20] E. Candès and J. Romberg, "Sparsity and incoherence in compressive sampling," *Inverse problems*, vol. 23, no. 3, p. 969, Apr. 2007.

[21] A. Mitra, Y. V. S. Rao, S. Prasanna, *et al.*, "A new image encryption approach using combinational permutation techniques," *Int. J. Computer Sci.*, vol. 1, no. 2, pp. 127–131, 2006.

[22] Y. Zhang and D. Xiao, "An image encryption scheme based on rotation matrix bit-level permutation and block diffusion," *Commun. Nonlinear Sci. Numer. Simulat.*, vol. 19, no. 1, pp. 74–82, Jan. 2014.

[23] B. Han, F. Wu, and D. Wu, "Image representation by compressive sensing for visual sensor networks," *J. Vis. Commun. Image R.*, vol. 21, no. 4, pp. 325–333, May 2010.

[24] J. Wu, F. Liu, L. Jiao, X. Wang, and B. Hou, "Multivariate compressive sensing for image reconstruction in the wavelet domain: using scale mixture models," *IEEE Trans. Image Process.*, vol. 20, no. 12, pp. 3483–3494, Dec. 2011.

[25] J. Zhang, D. Zhao, C. Zhao, R. Xiong, S. Ma, and W. Gao, "Image compressive sensing recovery via collaborative sparsity," *IEEE J. Emerging Sel. Top. Circuits Syst.*, vol. 2, no. 3, pp. 380–391, Sep. 2012.

[26] Z. Gao, C. Xiong, L. Ding, and C. Zhou, "Image representation using block compressive sensing for compression applications," *J. Vis. Commun. Image R.*, vol. 24, no. 7, pp. 885–894, Oct. 2013.

[27] 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.

[28] D. Gao, D. Liu, Y. Feng, Q. An, and F. Yu, "A robust image transmission scheme for wireless channels based on compressive sensing," in *Springer Interlligence Lec-*

ture Notes in Computer Science (ILNCS), pp. 334–341, Springer, Sep. 2010.

[29] D. Liu, D. Gao, and G. Shi, "A new multiple description image coding scheme based on compressive sensing," in *Proc. IEEE 13th Int. Conf. Commun. Technol. (ICCT)*, pp. 385–388, Jinan, Sep. 2011.

[30] M. A. Davenport, J. N. Laska, P. T. Boufounos, and R. G. Baraniuk, "A simple proof that random matrices are democratic," 2009. [Online]. Available: http://arxiv.org/abs/0911.0736.

[31] A. A. Kumar and A. Makur, "Lossy compression of encrypted image by compressive sensing technique," in *Proc. IEEE Region 10 Conf. (TENCON 2009)*, pp. 1–5, Singapore, Jan. 2009.

[32] X. Zhang, Y. Ren, G. Feng, and Z. Qian, "Compressing encrypted image using compressive sensing," in *Proc. Seventh Int. Conf. Intelligent Inf. Hiding Multimed. Signal Process. (IIH-MSP)*, pp. 222–225, Dalian, Oct. 2011.

[33] Y. Rachlin and D. Baron, "The secrecy of compressed sensing measurements," in *Proc. 46th Annual Allerton Conf. Commun. Control.Comput.*, pp. 813–817, Urbana-Champaign, IL, Sep. 2008.

[34] V. Cambareri, M. Mangia, F. Pareschi, R. Rovatti, and G. Setti, "Low-complexity multiclass encryption by compressed sensing, part I: Definition and main properties," *arXiv preprint arXiv:1307.3360*, 2013.

[35] V. Cambareri, M. Mangia, F. Pareschi, R. Rovatti, and G. Setti, "Low-complexity multiclass encryption by compressed sensing, part II: Known-plaintext attacks," *arXiv preprint arXiv:1307.3360*, 2013.

[36] M. A. Figueiredo, R. D. Nowak, and S. J. Wright, "Gradient projection for sparse reconstruction: Application to compressed sensing and other inverse problems," *IEEE J. Sel. Top. Signal Process.*, vol. 1, no. 4, pp. 586–597, Dec. 2007.

[37] J. Zhao and R. Govindan, "Understanding packet delivery performance in dense wireless sensor networks," in *Proc. 1st Int. Conf. Embedded Networked Sens. Syst.*, pp. 1–13, Los Angeles, California, Nov. 2003.

[38] R. Haimi-Cohen and Y. M. Lai, "Distribution of compressive measurements generated by structurally random matrices," *arXiv preprint arXiv:1311.4834*, 2013.