IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 4, 2016, accepted May 13, 2016, date of publication May 19, 2016, date of current version June 13, 2016.

Digital Object Identifier 10.1109/ACCESS.2016.2569421

A Review of Compressive Sensing in Information Security Field

YUSHU ZHANG[1,2,4], LEO YU ZHANG[2,4], JIANTAO ZHOU[2], (Member, IEEE), LICHENG LIU[3], FEI CHEN[4], AND XING HE[1]

[1]Chongqing Key Laboratory of Nonlinear Circuits and Intelligent Information Processing, School of Electronics and Information Engineering, Southwest University, Chongqing 400715, China
[2]Department of Computer and Information Science, University of Macau, Macau 999078, China
[3]College of Electrical and Information Engineering, Hunan University, Changsha 410082, China
[4]College of Computer Science and Engineering, Shenzhen University, Shenzhen 518060, China

Corresponding author: F. Chen (chenfeiorange@163.com; fchen@szu.edu.cn)

This work was supported in part by the Macau Science and Technology Development Fund under Grant FDCT/009/2013/A1 and Grant FDCT/046/2014/A1, in part by the Research Committee within the University of Macau under Grant MRG007/ZJT/2015/FST, Grant MRG021/ZJT/2013/FST, Grant MYRG2014-00031-FST, and Grant MYRG2015-00056-FST, in part by the Research Foundation of the Education Department of Jiangxi Province under Grant GJJ150462, in part by the Fundamental Research Funds for the Shenzhen University under Grant 201533, and in part by the National Natural Science Foundation of China under Grant 61502399, Grant 61402547, Grant 61502314, and Grant 61572089.

ABSTRACT The applications of compressive sensing (CS) in the field of information security have captured a great deal of researchers' attention in the past decade. To supply guidance for researchers from a comprehensive perspective, this paper, for the first time, reviews CS in information security field from two aspects: theoretical security and application security. Moreover, the CS applied in image cipher is one of the most widespread applications, as its characteristics of dimensional reduction and random projection can be utilized and integrated into image cryptosystems, which can achieve simultaneous compression and encryption of an image or multiple images. With respect to this application, the basic framework designs and the corresponding analyses are investigated. Specifically, the investigation proceeds from three aspects, namely, image ciphers based on chaos and CS, image ciphers based on optics and CS, and image ciphers based on chaos, optics, and CS. A total of six frameworks are put forward. Meanwhile, their analyses in terms of security, advantages, disadvantages, and so on are presented. At last, we attempt to indicate some other possible application research topics in future.

INDEX TERMS Compressive sensing, theoretical security, application security, image cipher, chaos, optics.

I. INTRODUCTION

Since compressive sensing (CS) [1]–[3] theory has come into the world, it has been widely applied in many fields including 5G system [4], cloud monitoring [5], image coding [6], and so on. It was claimed that both sampling and compression can be performed simultaneously to reduce the sampling rate at the expense of a high computation complexity at the reconstruction stage. By virtue of the sparsity, a signal, which is randomly projected at the encoder side, can be reconstructed by searching the optimal solution of an underdetermined linear system at the decoder side.

In terms of information security, CS has been developed from both the theoretical aspect and the application aspect in recent years. The basic research object in theoretical security is to enable measurement matrix to be a key known by the encoder and the decoder. This idea is originally mentioned in a foundational work [7] of CS. An original signal to be sampled can be regarded as plaintext, and its random measurements as ciphertext. The secrecy of these random measurements was formally considered in [8], in which the perfect secrecy was proved unachievable but the computational secrecy can be guaranteed. Taking the measurement matrix as a key, the works [9]–[12] successively investigated the robustness of CS framework against additive noise, the weaker sense perfect secrecy under some assumptions and the perfect secrecy when measuring constant energy signals. From the perspective of physical layer security, the CS framework was utilized to establish secure communication over wiretap channel [13]–[18]. Multiclass encryption by CS was also discussed in [19]–[21] to achieve the objective that when receiving the same measurements, different decoders can recover the original signal with different quality levels.

For application security, CS was mainly connected with multimedia and cloud computing scenarios. As a typical

form of multimedia data, image is encrypted using CS frequently combined with other cryptographic techniques, such as chaos theory and optical transform, to enjoy higher security level and realize simultaneous encryption and compression [22]–[42], which can realize simultaneous encryption and compression. Besides CS-based image encryption, there exist some research works on image watermarking [43]–[49], image hiding [50]–[54], image hashing [55]–[58], image authentication [59]–[61] and others [62]–[65] based on CS. For video data, CS-based privacy protection and watermarking frameworks were proposed in [66]–[69]. On the audio side, CS based hash algorithm was designed in [70]. Very recently, an emerging technology for providing multimedia services and applications is multimedia cloud computing [71]. Under the background of cloud multimedia computing, the CS technique offered privacy-preserving multimedia cloud computing [72], outsourcing of image reconstruction service [73], multimedia data storage [74], healthcare monitoring system [75] and support-set-assured parallel outsourcing of sparse reconstruction service [76]. In addition, there existed a few security scenarios such as crowdsensing network [77], 5G system [4], emergency healthcare system [78], and industrial high-voltage insulation systems [79].

In the area of image encryption, it is well known that chaos theory and optical transform are two of the most widespread and important technologies [80]–[90], since chaotic systems possess some instinctive properties such as ergodicity, pseudo-randomness and sensitivity to initial conditions and control parameters and optical transforms are noted for their high speed, parallel processing and large storage memories. Till now, the characteristics of CS, dimensional reduction and random projection, have been utilized and integrated into the image ciphers based on chaos or optics, which can achieve simultaneous compression and encryption of an image or multiple images [22]–[42]. In this paper, some design frameworks and their corresponding analyses are investigated with respect to image ciphers based on CS. Specifically, our investigation proceeds from three aspects, image ciphers based on chaos and CS, image ciphers based on optics and CS, and image ciphers based on chaos, optics and CS. A total of six frameworks are put forward. Meanwhile, their analyses in terms of security, advantages, disadvantages, future research topics, etc. are given.

The remaining sections of this paper are organized as follows. The next section introduces the basics of CS. Sections 3 and 4 review the theoretical security and application security, respectively. Section 5 discusses the basic frameworks of image ciphers based on CS combined with chaos or optics, and gives the corresponding analyses. The last section investigates some future research topics.

II. COMPRESSIVE SENSING BASICS

Assume a signal $\mathbf{x} \in \mathbb{R}^n$ has a sparse representation under basis $\mathbf{\Psi} \in \mathbb{R}^{n\times n}$, i.e., $\mathbf{x} = \mathbf{\Psi\theta}$ with $\|\boldsymbol{\theta}\|_0 = k \ll n$. The sampling process acts as a random linear projection, $\mathbf{y} = \mathbf{\Phi x} = \mathbf{\Phi\Psi\theta}$, where $\mathbf{\Phi} \in \mathbb{R}^{m\times n}$ and $\mathbf{y} \in \mathbb{R}^m$ with $m < n$. After receiving the measurement vector $\mathbf{y}$, one can resort to l_0 norm optimization problem, which is a popular algorithm, to reconstruct $\mathbf{x}$. Due to its complexity, one can relax it as l_1 norm optimization problem as follows:

$$\hat{\boldsymbol{\theta}} = \arg\min_{\boldsymbol{\theta}} \|\boldsymbol{\theta}\|_1 \quad \text{s.t. } \|\mathbf{y} - \mathbf{\Phi\Psi\theta}\|_2 \leq \varepsilon,$$

where ε indicates noise level. To guarantee a sparse and stable solution of this optimization problem, it is necessary that the measurement matrix $\mathbf{\Phi}$ obeys the Restricted Isometry Property (RIP) of order k with $\delta_k \in (0, 1)$, i.e.,

$$(1 - \delta_k)\|\mathbf{z}\|_2^2 \leq \|\mathbf{\Phi z}\|_2^2 \leq (1 + \delta_k)\|\mathbf{z}\|_2^2,$$

for all k-sparse signals $\mathbf{z}$ [91].

III. THEORETICAL SECURITY

A. MEASUREMENT MATRIX AS A KEY

In the case of using measurement matrix as a key, the secrecy of CS was firstly investigated in [8]. It has been demonstrated that the perfect secrecy defined by Shannon is not achievable, but the computational secrecy can be guaranteed. Specifically, It studied the possibility of an adversary who tries to recover $\mathbf{x}$ with knowledge of $\mathbf{y}$ and $\mathbf{\Psi}$, and the sparsity of $\mathbf{x}$. For the perfect secrecy, the linearity of CS-based encryption model determines that it is impossible to meet the statistical independent requirement $P(X = \mathbf{x}|Y = \mathbf{y}) = P(X = \mathbf{x})$. The computational secrecy lies in whether or not the adversary can succeed in recovering $\mathbf{x}$ by trying all possible keys and using the state-of-the-art computing capabilities. Once a k-sparse solution is found, the correct key will be revealed. The difficulty depends on the key space, which should be large enough to provide computational secrecy. The security was further discussed by considering an informed signal processing attacker which leverages the symmetry and sparsity structure inherent in CS [9], in which, besides, CS based encryption is proved to be robust against some level of noise, i.e., robust encryption, meaning that even if $\mathbf{y}$ is contaminated by noise, the reconstruction algorithmcan still tolerate some amount of degradation. Although the perfect secrecy is not achievable, a weaker sense perfect secrecy can be achieved under the assumption of countable infinity cardinality of the random variable X and uniformity [10]. Meanwhile, the mutual information between $\mathbf{x}$ and $\mathbf{y}$ is approximated to analyze the perfect secrecy problem in general when no specific statistical distribution is assumed. Recently, Bianchi et al. [11], [12] demonstrated that when $\mathbf{\Phi}$ is composed of zero mean independent and identically distributed (i.i.d.) Gaussian entries, random linear measurements $\mathbf{y}$ acquired reveal only the energy of $\mathbf{x}$, i.e., only the energy of $\mathbf{y}$ leaks information of $\mathbf{x}$. Thus, the case of sensing $\mathbf{x}$ with constant energy using Gaussian random matrix is perfectly secure. Moreover, when $\mathbf{y}$ is normalized, then perfect secrecy will be irrespective of the distribution of $\mathbf{x}$.

B. PHYSICAL LAYER SECURITY

Different from the prefect and computational secrecy, an intermediate notion of secrecy, called Wolfowitz secrecy, was proposed to establish secure physical layer communication over a Wyner wiretap channel via CS, which cloud handle channel asymmetry to guarantee that it is possible for the legitimate receiver to decode sparse signals with high probability but impossible for the eavesdropper [13]. A CS inspired multiplicative Gaussian wire-tap channel was studied in [14] to reveal that by calculating the lower and upper bounds on the secrecy capacity, the corresponding secrecy capacity is almost same as the capacity without any secrecy constraint under the assumption that the intended receiver outperforms the eavesdropper in terms of the channel. Furthermore, the linear feedback shift register (LFSR) was also integrated into wireless physical layer security to construct the measurement matrix [15]. The physical layer secrecy performance of the amplify-and-forward compressed sensing scheme framework was assessed in [16] and [17], provided that malicious eavesdropping nodes are listening. It was demonstrated that this framework can achieve perfect secrecy when facing a small number of eavesdroppers and shown that to perfectly reconstruct the signal, a great many eavesdropping nodes are essential. In addition, an MIMO precoding and postcoding system was designed to fulfill the physical layer data secrecy [18], where the CS based recovery algorithms can be utilized to reconstruct the transmitted signal. If full channel state information is available, the precoder can maximize the received signal-to-noise. If the partial is available, a modified Lloyd algorithm was presented to construct codebooks for representing the precoder. Besides, a low-complexity postcoder was proposed for compensating the signal-to-noise loss.

C. MULTICLASS ENCRYPTION

Cambareri et al. [19] proposed a two-class information concealing system based on CS. The basic principle is to introduce controlled perturbation to flip the sign of a subset of the elements of $\mathbf{\Phi}$. Specifically, let $\mathbf{\Phi}^{(0)}$ denote an initial measurement matrix and C a subset of $c < mn$ elements chosen from $\mathbf{\Phi}^{(0)}$ at random. If the matrix coordinate $(i, j) \in C$, then the perturbed matrix $\mathbf{\Phi}^{(1)}_{i,j} = -\mathbf{\Phi}^{(0)}_{i,j}$; otherwise, $\mathbf{\Phi}^{(1)}_{i,j} = \mathbf{\Phi}^{(0)}_{i,j}$. The encoding process is $\mathbf{y} = \mathbf{\Phi}^{(1)}\mathbf{x}$, and then the receiver with knowledge of the true measurement matrix $\mathbf{\Phi}^{(1)}$ can be able to recover the exact $\mathbf{x}$ while only knowing the $\mathbf{\Phi}^{(0)}$, the reconstructed $\mathbf{x}$ will be subjected to some noise. This two-class system was further extended to a multiclass encryption model [20], in which the same measurements are distributed to receivers with different measurement matrix, enabled to obtain $\mathbf{x}$ having different reconstruction quality. The error bound and security performance were also elaborated to show that asymptotic spherical secrecy is achievable. Some sources such as speech segments, electrocardiographic signals and images containing sensitive text protected by multiclass encryption have been confirmed. This theoretical and empirical evidence clarifies that, the security of multiclass encryption was further clarified that although not perfectly secure, it features a noteworthy level of security against a particular form of known-plaintext attack [21] (only one pair of plaintext and ciphertext is available).

IV. APPLICATION SECURITY

A. IMAGE SECURITY

1) IMAGE ENCRYPTION

The CS together with chaos theory was employed for hybrid image compression-encryption algorithms [22]–[30]. After an image is compressively sensed, a block Arnold transformation followed by bitwise XOR operation is executed to permute the positions of measurements then dissipate the Gaussian distribution [22]. The chaotic sequences generated by Logistic map serve as the parameters of block Arnold scrambling and the pseudorandom sequence for XOR operation. Experiments demonstrated that this method is robust against consecutive packet loss and malicious shear attack. A parallel image encryption mode was further designed in [23], which possesses the block cipher structure consisting of linear measurement, scrambling, mixing, S-box and chaotic lattice XOR so as to resist against chosen-plaintext attack. Zhou et al. designed a novel key-controlled measurement matrix, which is established by leveraging the circulant matrices and manipulating the original row vectors of the circulant matrices with Logistic map [24]. They also adopted the partial Hadamard matrix as measurement matrix conducted by chaotic map and the generated measurements are further scrambled [26]. George and Pattathil constructed measurement matrix using multiple chaotic maps for secure CS of images [28]. Specifically, there are eight different one dimensional chaotic maps used, two of which are randomly selected based on the external secret keys. Moreover, they constructed a random measurement matrix based on LFSR [27]. The basic idea is to normalize the different states of LFSR to get i.i.d. random variables, which are then selected as the random entries of the measurement matrix. Lately, Zhou et al. suggested an efficient image compression-encryption method based on hyper-chaotic system and 2D CS to reduce the possible transmission burden [29]. Liu et al. manipulated CS and chaos to simultaneously compress, fuse and encrypt multi-modal images [30], in which the key-controlled pseudo-random measurement matrix is constructed by using logistic map and the measurements are fused by the adaptive weighted fusion rule.

The combination of CS and optical technique has been utilized to design similar algorithms [31]–[34]. An image is first sampled by using the characteristics of CS, i.e., dimensional reduction and random projection, and then encrypted by double random phase encoding (DRPE) [31]. A DRPE encryption algorithm incorporating compressive fractional Fourier transformation (FrFT) with iterative kernel steering regression was proposed in [32]. The FrFT enhances the degree of freedom and kernel regression is applied for image denoising. Furthermore, multiple-image encryption by space

multiplexing based on CS and DRPE was presented [33], in which the space multiplexing method is introduced to integrate multiple-image data, resulting in a nonlinear encryption framework so as to overcome the vulnerability of classical DRPE. The authors in [34] developed a simultaneous image encryption and compression scheme based on random convolution and random subsampling. This scheme can be tailored for a single image unlike the existing joint optical encryption and compression schemes for multiple images and has similar architecture with DRPE.

Chaos theory and optical technique are able to be both integrated in CS to achieve joint image compression and encryption [35]–[38]. In [35], the optical technique, CS module, block Arnold transform and DRPE, are sequentially executed to guarantee image information security. The input image is split into four parts and then the pixels of the two adjacent parts are exchanged randomly by random matrices, which are bound with the measurement matrices. In [36], the measurement matrix and the random phase masks are constituted by chaotic sequences. Lang and Zhang came up with a unique perspective of transmitting only a few measurements intermittently chosen from the masks rather than the real keys and the tremendous masks codes [37], since the parameters of the chaotic maps can be inferred from the received measurements without error so that the correct random phase-amplitude masks can be obtained and used for decrypting the encoded information. The further review of image encryption based on CS is shown in the following sections. The DRPE based block CS was designed for image encryption, which aims to encrypt each image block using a chaos-based random phase encoding in fractional Fourier domain [38].

In addition, from the the viewpoint that digital devices can only store the samples at a finite precision, Zhang et al. suggested a joint quantization and diffusion approach for the real-valued measurements based on the distribution of measurements of natural images sensed by structurally random ensemble [39]. The issue of creating a CS-based symmetric cipher under the key reuse circumstance was tackled in [40]. Specifically, a bi-level protected CS mode was projected by taking use of the advantage of the non-RIP measurement matrix construction. It was validated that the mode can be resistant to common attacks even a fixed measurement matrix is used multiple times. In [41], Zhang et al. proposed some possible encryption models for CS and then demonstrated random permutation is an acceptable permutation with overwhelming probability, which can effectively relax the RIP for parallel CS. Random permutation is used for creating a secure parallel CS scheme and the corresponding security analysis indicates the asymptotic spherical secrecy. In orde to resist chosen-plaintext attacks, Fay introduced the counter mode of operation to CS-based encryption and it can achieve probabilistic encryption [42].

2) IMAGE WATERMARKING

A robust image watermarking scheme for image tampering identification and localization based on CS and distributed source coding principles was described in [43]. The basic idea is to form a hash, which is robustly embedded as a watermark in the image. The introduced modification can be recovered in case that tampering is sufficiently sparse or compressible in some basis. Zhang et al. put forward a watermarking scheme with flexible self-recovery quality based on compositive reconstruction [44]. The CS is used to retrieve the coefficients by developing the sparseness in the DCT domain when the amount of extracted data is not large enough. A watermarking scheme for copyright protection was designed to reconstruct the image to some extent with knowledge of very few amounts of transmitted coefficients and relationships between coefficients [45]. In [46], CS was considered as a watermarking attack. If watermark is constructed as a pseudorandom sequence and then embedded into the DCT domain, CS, as a watermarking attack, can provide recovery of the image with small number of measurements. The scheme [47] embedded the watermark into the randomly selected samples from image blocks, and the total variation minimization is then employed for image reconstruction. A robust watermarking algorithm in encrypted domain based on CS was proposed in [48], in which the image content and watermark are separable. The similar watermarking method in encrypted domain was also presented in [49], which validated the strong robustness, high correct bit extraction rate, flexible data embedding capacity and hierarchical security.

3) IMAGE HIDING

A data hiding method based on subsampling and CS was scheduled in [50]. By relying on the properties of CS including sparsity and random projection, the secret data can be embedded in the observation domain of the image. The method [50] was further extended to an image steganography algorithm [51] in terms of some details on design procedures and experiments, but they are roughly consistent in the train of thought. Xiao and Chen designed separable data hiding for an encrypted image based on stream cipher algorithm, Arnold scrambling and CS [52], consisting of image encryption, data hiding, data extraction and image recovery phases. The embedding rate has a big boost in comparison with the existing separable data hiding method in the encrypted image. An over-complete dictionary was implemented for multimedia data hiding by discussing the minimum norm formulation and sparse formulation, respectively, which motivates the future investigation in this field [53]. Considering that block CS can simultaneous compression and encryption, Li et al. presented a novel reversible data hiding scheme by embedding additional data into image measurements, which outperforms the other state-of-the-art schemes over encrypted images [54].

4) IMAGE HASHING

Kang et al. proposed a secure and robust image hashing scheme using CS and visual information fidelity [55]. The CS makes the hash size keep small while the visual

information fidelity helps to be robust against most image manipulations. Meanwhile, a CS based hashing technique was developed in [56], which takes effect on both the authentication and the tampering identification. The foundation is that if the tampering can be localized by solving a convex optimization problem with constraints forced by the transmitted hash, provided that it is sparse enough. Lately, Sun and Zhang introduced Fourier-Mellin transform and CS for a robust image hash [57]. Fourier-Mellin transform is incorporated to thwart rotation, scaling and transition attacks and the characteristic of dimension reduction inherent in CS is applied for hash device. Liu et al. exploited low-rank and sparse representation for robust image hashing with tampering recovery capability and strong robustness against content preserving modifications [58].

5) IMAGE AUTHENTICATION

An optical encryption technique based on CS was employed to create a cancelable biometric authentication scheme [59], which encrypts a finger vein image using a compressive imaging system when capturing image, while the raw finger vein image can only restored in the authentication server. A new point of view, encrypted sensing, based on DRPE and CS, was proposed for biometric authentication [60], which further improves the security to protect the biometric template. In addition, Xiao et al. employed CS for reversible image authentication, where there are two watermarks used, including a short one for image integrity authentication and a long one for tamper localization and recovery [61].

6) OTHERS

Kang et al. presented a secure *transcoding* scheme for compressive multimedia sensing so as to securely deliver compressively sensed multimedia over networks [62]. Pillari et al. exploited CS for secure and robust iris recognition, which can simultaneously deal with three challenges: ability to handle unconstrained acquisition, robust and accurate matching and privacy enhancement without compromising security in a non-contact biometrics-based authentication system [63]. Liu also utilized CS and Shamir's (t, n)-threshold scheme to design a real-time and progressive secret image sharing scheme with flexible-size shadows [64]. Qi et al. came up with a hybrid security and compressive sensing-based scheme for multimedia sensor data gathering, which possesses light security mechanism, thus decreasing the complexity and energy consumption of system [65].

B. VIDEO AND AUDIO SECURITY

Cossalter et al. proposed a privacy-assured tracking system for video surveillance by taking advantage of recent findings of CS [66]. It is not necessary to reconstruct the original content of the video sequence and then the system can leverage a fixed camera to analyze the video frames and detects a possible moving object in the scene. Tong et al. also applied the emerging CS theory for privacy-enabled video surveillance, where the scrambling is performed on privacy regions via block CS for quantized coefficients [67]. Meanwhile, a video authentication algorithm combined semi-fragile watermarking and CS was for the purpose of tamper detection of MPEG-2 [68] and a video watermarking method proposed in [69] was based on CS, Arnold transform, sum of absolute deviation and SVD to protect the ownership information in a robust way. Besides, audio content protection based on CS was studied in [70], which put the framework of CS and distributed source coding into audio to generate a compact hash signature for detecting and identifying illegitimate manipulations.

C. CLOUD SECURITY SCENARIO

In cloud security scenario, privacy-assured multimedia cloud computing based on CS and sparse representation was investigated in [72], which discussed some compressive multimedia applications, including multimedia compression, adaptation, editing/manipulation, enhancement, retrieval, and recognition. Wang et al. [73] proposed a privacy-preserving outsourcing of image reconstruction service from CS in cloud. Different domain technologies were synthesized to fulfill the prospective on the aspects of security, efficiency and complexity. They further widened the outsourcing of image construction service to healthcare monitoring system [75]. In order to simultaneously perform secure watermark detection and privacy-protected multimedia data storage in a cloud computing application scenario, Wang et al. designed such a framework based on CS and secure multiparty computation protocols under the hypothesis of the semi-honest adversary model [74]. Outsourcing sparse reconstruction service to multi-clouds in parallel was described in [76] by the assumption that multi-clouds cannot collude with each other in private. The privacy of the original signal can be guaranteed, since each cloud only has a small amount of information of both the measurements and asymmetric support-set.

D. OTHER SECURITY SCENARIOS LIKE 5G SYSTEM

The CS can also be applied to some other security scenarios. For example, aiming at a crowdsensing network, Wu et al. suggested a privacy-preserving RSS map generation project in order to deal with the difficulty, that the sampling data and location information from participants that existing RSS gathering schemes require often lead to a privacy threat [77]. With respect to 5G system, a variety of scenarios based on CS was discussed in [4]. This work showed that sparse signal processing can be a viable source for an innovative 5G system and meanwhile, introduced a few other applications including compressive channel-source network coding, embedded security, etc. In addition, the localization privacy in emergency healthcare [78] and industrial high-voltage insulation systems [79] was studied with the help of CS theory and sparse representation.

For the sake of clarity, Table 1 depicts the sketch of the above two sections.

TABLE 1. The sketch about theoretical security and application security.

Theoretical security	Measurement matrix as a key	[8]–[12]
	Physical layer security	[13]–[18]
	Multiclass encryption	[19]–[21]
Application security	Image security	Image encryption [22]–[42] Image watermarking [43]–[49] Image hiding [50]–[54] Image hashing [55]–[58] Image authentication [59]–[61] Others [62]–[65]
	Video and audio security	[66]–[70]
	Cloud security scenario	[72]–[76]
	Other security scenarios like 5G system	[4], [77]–[79]

FIGURE 1. The sketch of Framework 1.

V. CS-BASED IMAGE ENCRYPTION FRAMEWORK AND ANALYSIS

A. IMAGE CIPHERS BASED ON CHAOS AND CS

Chaos and CS used in image ciphers are instantiated in two aspects: precedence relationship and nesting relationship. The former means one after the other while the latter is to embed one in the other. Thus, we have the following two basic frameworks.

Framework 1: Chaos-based encryption model is executed after CS, as shown in Fig. 1.

An image is firstly encrypted by CS, when the measurement matrix is considered as secret key [7]. The acquired measurements are then encrypted by chaos-based models including permutation and diffusion. It should be noted that it is almost impossible to exploit chaos followed by CS due to the fact that chaos-based encryption always breaks the correlations between pixels and removes the redundancy farthest such that the sparsity which CS relies on cannot be guaranteed. In the following, we will take a case study for further illustration.

Case 1: Reference [23].

Huang et al. designed a parallel image encryption method based on CS and chaotic encryption models including Arnold scrambling, mixing, S-box and chaotic lattice XOR. The original image is block-wise measured in parallel using Gaussian measurement matrix and quantized through the Lloyd quantizer. Then the data are reallocated for the purpose of the collision-free property that a communication unit exchanges data among the multiple processors without collision. Arnold scrambling is then used to permtutate the quantized mesurements' positions followed by the mixing operation which makes a single alteration affect the final output. S-box substitution and block-wise XOR are finally used for diffusion.

Analysis: With respect to the only CS-based encryption scheme, i.e., measurement matrix as a key, the security has been discussed in [8]–[11], which demonstrated that the perfect secrecy is unachievable but the case of sensing x with constant energy using Gaussian random matrix is perfectly secure. Moreover, it is not secure against chosen plaintext attack by choosing some particular sparse vector containing only one non-zero entry. However, in Framework 1, a great number of chaotic encryption techniques are able to remedy the security defect However, there is no tight relationship between chaotic cipher and CS model reported so far. For the measurement values by CS, the chaotic cipher model designed should be tailored, for example, one can take account of the distribution of the measurements into the architecture of chaotic cipher. Otherwise, simple combination of CS and any chaotic encryption model can be adopted. Besides, there is a bunch of chaotic encryption models ensuring the security but a large proportion of them suffered by the problem of high computation complexity and unfriendly hardware realization. Consequently, it is desirable to embed chaos in CS in some way.

Framework 2: Chaos is embedded in CS, as shown in Fig. 2.

In this model, the generation process of the measurement matrix is under the control of chaotic sequence, which is produced by chaotic system with initial values. Specifically, initial conditions or control parameters, which can be treated as secret keys, of the employed chaos system are used to generate the measurement matrix. This facilitates transmission and sharing that only requires a few values instead of the whole measurement matrix. At last, chaos-based CS samples images. There are many ways of implementing chaos to construct the measurement matrix, as illustrated in the following cases.

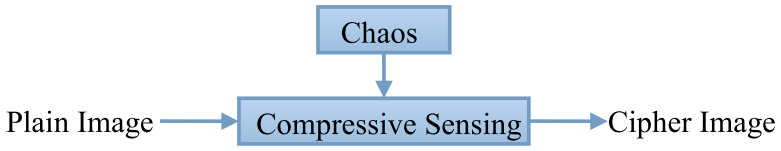


FIGURE 2. The sketch of Framework 2.

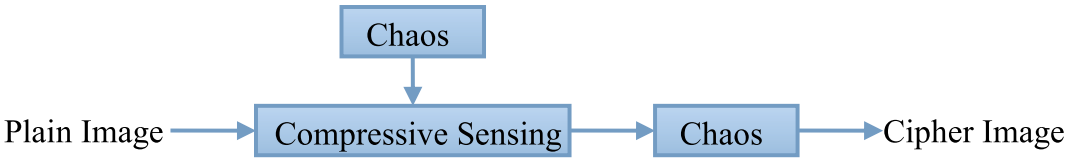


FIGURE 3. The sketch of Framework 3.

Case 1: Reference [28].

George and Pattathil employed eight one dimensional chaotic maps to generate the random measurement matrix. It has four stages: randomly selecting pairwise chaotic maps; calculating the initial values for the selected pair; iterating the selected chaotic maps; generating the random measurement matrix with zero mean and variance $1/n$. This matrix is adopted for block CS of images.

Case 2: Reference [27].

George and pattathil utilized linear feedback shift register (LFSR) for secure measurement matrix generation. Different states of LFSR are selected and normalized as the random entries of the measurement matrix. In order to withstand known plaintext attack, each block of an image is sampled by different measurement matrices, which are constructed by the LFSR system with a modulo division circuit and logistic map. It avoided the memory overload.

Case 3: Reference [26].

In the case of measurement matrix as a key, to make the key be easily distributed, stored and memorized, Zhou *et al.* created the improved circulant matrices by manipulating their original row vectors under the control of logistic map. The original image is partitioned into four blocks and two of them in the adjacent locations exchange their pixels randomly. The random matrices used for exchanging the random pixel are tied up with measurement matrices.

Analysis: Framework 2 together with these three cases need to be aware of some problems. Prior to the image sampling, whether or not the newly generated measurement matrix by chaos satisfies the RIP condition should be demonstrated. The work [92], in which CS with chaotic sequence has been verified in theory, can serve as a reference. Furthermore, the optimal reconstruction algorithm should be developed for better matching with the image sampling method. Meanwhile, the quantization is also worth considering for the purpose of real-time transmission. For security consideration, the initial values of the employed chaotic system require frequently alteration, otherwise they will be suffered by known-plaintext attack. Alternatively, to enhance the security, some appropriate chaotic encryption models may be added.

Framework 3: A hybrid of Framework 1 and Framework 2, as shown in Fig. 3.

Not only can chaos control CS, but also provide some encryption models after the CS sampling. As illustrated in Fig. 3, permutation and diffusion operations can be appropriately introduced to resist plaintext attacks after the CS sampling.

Case 1: Reference [24].

Zhou *et al.* adopted the partial Hadamard matrix controlled by chaos map as the measurement matrix. The image sampling is followed by a scrambling using the chaotic index sequence generated by the logistic map.

Case 2: Reference [25].

Zhang et al. [25] suggested a scalable encryption framework based on block CS together with Sobel edge detector and cascade chaotic map for the purpose of protecting significant image regions. After an image is performed by Sobel edge detector, chaos-based structurally random matrix is applied to significant block encryption whereas chaos-based random convolution and subsampling are used for the remaining insignificant ones. This framework adopts lightweight subsampling and severe sensitivity encryption for the significant blocks and severe subsampling and lightweight robustness encryption for the insignificant ones in parallel.

Analysis: It is generally known that CS-based image ciphers are robust against noise, called robust encryption. However, in the above three basic frameworks, robust encryption may be broken by chaos effect. It is mainly due to the introduced chaotic encryption models. If only an permutation operation is employed, it does not affect the robustness; on the contrary, it may make the robustness more strong. For example, an acceptable permutation can relax the RIP condition [93], which may even reduce the block effects to some extent. If an diffusion operation is employed, the robustness must be broken since diffusion offers certain level of avalanche effect. In summary, Framework 2 is robust while Framework 1 and Framework 3 are uncertain.

FIGURE 4. The sketch of Framework 4.

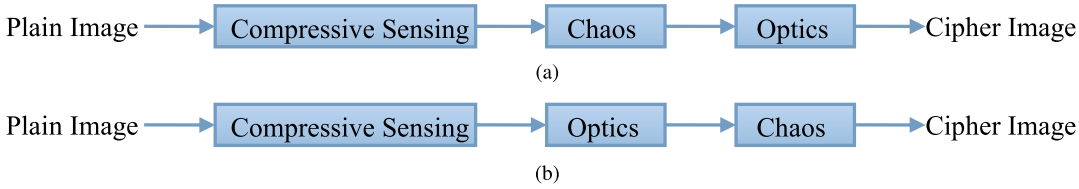


FIGURE 5. The sketch of Framework 5.

Apparently, a hybrid of Framework 1 and Framework 2 is more secure than their individual counterparts. As mentioned earlier, stronger security is at the expense of higher computation complexity and more chaotic encryption techniques, thereby a trade-off between security and overall complexity has to be examined.

B. IMAGE CIPHERS BASED ON OPTICS AND CS

The basic framework of optical image encryption is the double random phase encoding (PRPE) [94]. The most possible encryption combination of DRPE and CS is CS followed by DRPE.

Framework 4: CS is followed by DRPE, as shown in Fig. 4.

An image is firstly sampled by CS, and the acquired measurements are encrypted by the structure of DRPE. This can be validated by the following three cases.

Case 1: Reference [31].

Lu *et al.* proposed such a simple combination. The CS is used to directly encrypt and compress an image and then the DRPE is used for re-encryption.

Case 2: Reference [32].

Different from [31], Rawat *et al.* implemented an image quality enhancement procedure using iterative kernel steering regression algorithm [95] before performing Framework 4 and utilized the fractional Fourier transform instead of Fourier transform for DRPE.

Case 3: Reference [33].

On the basis of Framework 4, Deepan *et al.* introduced space multiplexing [96] for multiple-image encryption. The multiple images are measured by CS respectively, and are then integrated by space multiplexing. It was claimed that this scheme is able to overcome the vulnerability [97]–[100] of classical DRPE due to its nonlinearity.

Analysis: Although Framework 4 realizes optical image compression and encryption, CS and DRPE only have a precedence relationship. It is of great significance to investigate their nesting relationship from the imaging prospective. A heuristic investigation is the work [101], which demonstrated the possibility of achieving super-resolution with a single exposure by combining DRPE and CS. Additionally, a bottleneck of CS in optics is to carry out the reconstruction algorithm using optical techniques, although it is easy for the sampling. As a consequence, the computing device has to be relied on. Besides DRPE, some classic optical encryption techniques can also be infused in Framework 4 to be a novel scheme like multiple-image encryption [33]. This joint optical multiple-image compression and encryption work based on CS differs from the general ones [102]–[104]. In the end, another point of thought, some cryptographic features may be embedded in the existing CS-based imaging schemes [105]–[108].

C. IMAGE CIPHERS BASED ON CHAOS, OPTICS AND CS

When all the three techniques including chaos, optics and CS are applied, the corresponding framework is naturally a fusion of the above four frameworks.

Framework 5: A hybrid of Framework 1 and Framework 4, as shown in Fig. 5.

After the CS, one of chaotic encryption models and DRPE is exploited, and then the other follows.

Case 1: Reference [35].

Liu *et al.* employed a common chaotic permutation way, Arnold transformation, which is used to scramble the measurements obtained by CS. The results are again encrypted by DRPE, where two random phase masks are generated by sequences of irrational number.

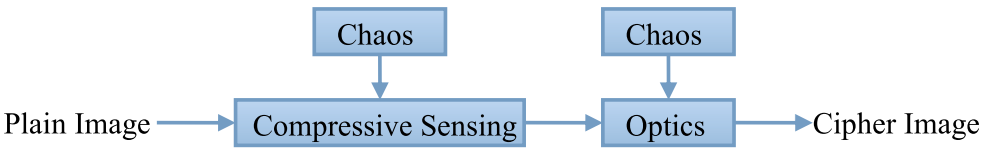


FIGURE 6. The sketch of Framework 6.

Analysis: Generally speaking, this type of framework is secure enough, since three different encryption techniques can be fully utilized. However, there is nothing special but a simple combination. This approach will inevitably lead to a higher computation complexity. It is hopeful that the three are further integrated.

Framework 6: A hybrid of Framework 2 and Framework 4, as shown in Fig. 6.

This framework means that chaos is embedded in not only CS but also optics. It is already clear that chaotic systems are able to supply the values to the orders of fractional transforms or random phase masks [109].

Case 1: Reference [36].

Liu *et al.* implemented chaos-based DRPE to encrypt CS measurements. In DRPE, the common Fourier transform is replaced by the fractional Fourier transform. The measurement matrix and the random phase masks are furnished by pseudo-random sequences produced from logistic map. In fact, this scheme can be further improved in the way that the fractional orders are also offered by logistic map such that the whole encryption process is controlled by chaos.

Analysis: In this framework, chaos is embedded in both CS and optics, and there is a large advantage that both the huge measurement matrix and double random phase matrices are generated from a few initial values, which facilitates the sharing of the keys. Meanwhile, the introduction of chaos does not break the robustness of CS and DRPE architecture. Thus, Framework 6 is a robust encryption scheme but Framework 5 may not. More importantly, the initial value sensitiveness can be guaranteed. So far, Framework 6 is the preferred candidate for simultaneous compression and encryption of images.

In fact, there also exist a framework of image ciphers based on CS itself, as shown in [39]–[42], which combine neither chaos nor optics. Finally, what is worth mentioning is a particular image cryptosystem using chaotic phase-amplitude masks and least-data-driven decryption by CS [37]. The highlight lies in that it transmits only a few measurements intermittently chosen from the masks rather than the real keys and the enormous mask codes. In the decryption side, utilizing the theories in [110] and [111] and refining the series expansions, the decoder can infer the correct parameters of the chaotic map. This scheme motivates us to fully excavate some new proposed theories on the relationships among CS, chaos and optics for further study image cipher design.

VI. FUTURE RESEARCH TOPICS

A. FINITE FIELDS

In practice, the signal to be sampled is not always real-valued and the corresponding quantization may cause loss of accuracy, thus the CS over finite fields has been studied in a few literatures [112]–[114]. It is well-know that cryptography is inseparable from finite fields. In particular, asymmetric ciphers are built upon finite alphabets. As a result, it may be worth exploring the relationship between cryptography and CS over finite fields. For example, there exists an interesting phenomenon that both CS and asymmetric ciphers have inconsistent computation complexity, i.e., lightweight computation overhead in the encoding (or encryption) phase and heavy computing cost in the decoding (or decryption) phase. The CS as an asymmetric cipher may be found to make up the blank in the theoretical security, since the findings about the relationship between symmetric cipher and CS, such as measurement as a key, physical layer security and multiclass encryption, as previously mentioned, have been researching so far.

B. COMBINATION WITH CHAOS

The measurement matrix in CS always has a big size and takes up too much space, leading to a lot of inconveniences for communication and sharing. To address this issue, one possible solution is to generate it using chaotic sequences through iterating certain chaotic system from its initial values. It only requires for transmitting the initial values. Till now, such measurement matrices have been investigated in [92] and [115]–[119], , which brings a benefit for secure multimedia CS scheme design like [24]. Not only that, but the chaotic properties such as the sensitivity to initial values, pseudo-randomness and ergodicity can be infused in those CS based multimedia encryption schemes due to being closely connected to cryptographic features. In other words, joint multimedia compression and encryption can be realized by combining CS and chaos, where CS mainly aims at compression and chaos is intended to provide security assurance.

C. COMBINATION WITH OPTICS

The future research topics on combination CS with optics are twofold. On one hand, in recent years, optical imaging based on CS is a hot topic, which has been emerged in a number of important research results [105]–[108], [120], [121]. Interestingly, we can attempt the problem of how to embed cryptographic features in these compressive imaging schemes. Secure compressive imaging will further have a wide range of applications. On the other hand, a few joint optical image compression and encryption schemes have been proposed in [102]–[104] and [122]. However, these schemes are only suitable for multiple images. Few references involve the case of a single image, but CS offers such an opportunity. Instead of the simple combination of CS and DRPE [33], [36], the fusion of both will be possibly established to simultaneously compress and encrypt an image, as shown in [34].

D. ROBUST ENCRYPTION

The existing data encryption schemes mostly consider the sensitivity encryption, which often leads to low-quality decrypted data or even is incapable of correct decryption when a part of encrypted data lose. This likely happens in transmission channel, for example, long burst errors can occur in the wireless channel or an intermediate blocking will lead to a temporarily declining physical link as a result of the

fading effect. A strategy of tackling this issue is to exploit the robust encryption, which means that the loss of partial data scarcely affects or even does not affect the equality of the decrypted data. So far, few work [123], [124] is involved with this study, due to the fact that designing robust encryption is a far greater deal of difficulty than doing sensitivity encryption. Fortunately, CS is a good candidate of dealing with robust encryption. For instance, A CS-based robust image encryption was devised in [22] which can be against consecutive packet loss and malicious shear attack.

E. ROBUST CODING OVER ENCRYPTED DOMAIN

Signal processing over encrypted domain is an extremely hot research field since its appearance [125]. A new research hotspot in this field is to carry out robust image encoding over encrypted domain [126], since the previous studies aim at either robust coding of natural images or the effective compression of encrypted images. The encoding subtly adopts a structurally random matrix [127] in CS. The coder can be applied in a particular scenario that a sender needs a semi-trusted channel provider to encode and transmit the encrypted image to a receiver. This enables the sender to first encrypt an image and then send the encrypted image to channel provider who encodes the encrypted image. Through an imperfect channel with packet loss, the receiver obtains the lost data and reconstructs the original image. The CS technique opens the possibility of decorating robust coder over encrypted domain. Moreover, this kind of coder may be extended to cloud outsourcing security field. For example, we consider an interesting case of lossy channel between client and cloud, which still has not been mentioned in the existing computation outsourcing works.

F. CLOUD SCENARIO

In cloud scenario, some security issues related to CS can be investigated. As aforementioned, signal processing over encrypted domain [125] has become popular, especially because of the rise of cloud computing and big data, which enables this field to produces practical significance of the modern world. The CS as a new sampling theory in signal processing can also be considered to be implemented in encrypted domain, i.e., CS in encrypted domain. Second, the sampling in CS is easy to achieve, but the reconstruction algorithm has a very high computation complexity. Associating with the cloud having the powerful computing resources and the huge of volume of storage, we can outsource the reconstruction algorithm to the cloud. It is of great importance to deliberate the privacy-assured outsourcing of CS reconstruction service in cloud. Third, assume that a signal is sampled using CS by an owner, then the sampled signal needs cloud for storage purpose. When the owner or a new user wants to see what the original signal is, the cloud performs the recovery. However, the cloud is often curious or even malicious, thereby the appropriate encryption processing has to be done prior to transmission. After the sampling, the measurements can be encrypted through mildly linear mode [73], simple exchange primitives [76] or severely homomorphic manner [128]. Receiving the measurements, the cloud storages them and then performs the reconstruction if necessary. Alternatively, the owner simultaneously compresses and encrypts the signal while the cloud operates the joint decompression and decryption to obtain the original signal.

REFERENCES

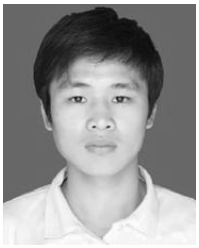
[1] E. J. Candès, J. Romberg, and T. Tao, "Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 489–509, Feb. 2006.
[2] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.
[3] E. J. Candès and M. B. Wakin, "An introduction to compressive sampling," *IEEE Signal Process. Mag.*, vol. 25, no. 2, pp. 21–30, Mar. 2008.
[4] G. Wunder, H. Boche, T. Strohmer, and P. Jung, "Sparse signal processing concepts for efficient 5G system design," *IEEE Access*, vol. 3, pp. 195–208, 2015.
[5] H. Kung, C.-K. Lin, and D. Vlah, "CloudSense: Continuous fine-grain cloud monitoring with compressive sensing," in *Proc. HotCloud*, 2011, pp. 1–6.
[6] X. Liu, D. Zhai, J. Zhou, X. Zhang, D. Zhao, and W. Gao, "Compressive sampling-based image coding for resource-deficient visual communication," *IEEE Trans. Image Process.*, vol. 25, no. 6, pp. 2844–2855, Jun. 2016.
[7] 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.
[8] 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.
[9] A. Orsdemir, H. O. Altun, G. Sharma, and M. F. Bocko, "On the security and robustness of encryption via compressed sensing," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, San Diego, CA, USA, Nov. 2008, pp. 1–7.
[10] S. A. Hossein, A. E. Tabatabaei, and N. Zivic, "Security analysis of the joint encryption and compressed sensing," in *Proc. 20th Telecommun. Forum (TELFOR)*, Belgrade, Serbia, Nov. 2012, pp. 799–802.
[11] T. Bianchi, V. Bioglio, and E. Magli, "On the security of random linear measurements," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Florence, Italy, May 2014, pp. 3992–3996.
[12] 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.
[13] S. Agrawal and S. Vishwanath, "Secrecy using compressive sensing," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Paraty, Brazil, Oct. 2011, pp. 563–567.
[14] G. Reeves, N. Goela, N. Milosavljevic, and M. Gastpar, "A compressed sensing wire-tap channel," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Paraty, Brazil, Oct. 2011, pp. 548–552.
[15] R. Dautov and G. R. Tsouri, "Establishing secure measurement matrix for compressed sensing using wireless physical layer security," in *Proc. Int. Conf. Comput. Netw. Commun. (ICNC)*, San Diego, CA, USA, Jan. 2013, pp. 354–358.
[16] J. E. Barceló-Lladó, A. Morell, and G. Seco-Granados, "Amplify-and-forward compressed sensing as a PHY-layer secrecy solution in wireless sensor networks," in *Proc. IEEE 7th Sensor Array Multichannel Signal Process. Workshop (SAM)*, Hoboken, NJ, USA, Jun. 2012, pp. 113–116.
[17] J. E. Barceló-Lladó, A. Morell, and G. Seco-Granados, "Amplify-and-forward compressed sensing as a physical-layer secrecy solution in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 5, pp. 839–850, May 2014.
[18] C.-H. Lin, S.-H. Tsai, and Y.-P. Lin, "Secure transmission using MIMO precoding," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 5, pp. 801–813, May 2014.
[19] V. Cambareri, J. Haboba, F. Pareschi, H. R. Rovatti, G. Setti, and K.-W. Wong, "A two-class information concealing system based on compressed sensing," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, Beijing, China, May 2013, pp. 1356–1359.

[20] 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.
[21] V. Cambareri, M. Mangia, F. Pareschi, R. Rovatti, and G. Setti, "On known-plaintext attacks to a compressed sensing-based encryption: A quantitative analysis," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 10, pp. 2182–2195, Oct. 2015.
[22] 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. (IIH-MSP)*, 2011, pp. 105–108.
[23] R. Huang, K. H. Rhee, and S. Uchida, "A parallel image encryption method based on compressive sensing," *Multimedia Tools Appl.*, vol. 72, no. 1, pp. 71–93, 2014.
[24] N. Zhou, A. Zhang, F. Zheng, and L. Gong, "Novel image compression–encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing," *Opt. Laser Technol.*, vol. 62, pp. 152–160, Oct. 2014.
[25] Y. S. Zhang *et al.*, "A block compressive sensing based scalable encryption framework for protecting significant image regions," *Int. J. Bifurcat. Chaos*, in press, 2016.
[26] N. Zhou, A. Zhang, J. Wu, D. Pei, and Y. Yang, "Novel hybrid image compression–encryption algorithm based on compressive sensing," *Optik-Int. J. Light Electron Opt.*, vol. 125, no. 18, pp. 5075–5080, 2014.
[27] S. N. George and D. P. Pattathil, "A secure LFSR based random measurement matrix for compressive sensing," *Sens. Imag.*, vol. 15, no. 1, pp. 1–29, 2014.
[28] S. N. George and D. P. Pattathil, "A novel approach for secure compressive sensing of images using multiple chaotic maps," *J. Opt.*, vol. 43, no. 1, pp. 1–17, 2014.
[29] N. Zhou, S. Pan, S. Cheng, and Z. Zhou, "Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing," *Opt. Laser Technol.*, vol. 82, pp. 121–133, Aug. 2016.
[30] X. Liu, W. Mei, and H. Du, "Simultaneous image compression, fusion and encryption algorithm based on compressive sensing and chaos," *Opt. Commun.*, vol. 366, pp. 22–32, May 2016.
[31] P. Lu, Z. Xu, X. Lu, and X. Liu, "Digital image information encryption based on compressive sensing and double random-phase encoding technique," *Optik-Int. J. Light Electron Opt.*, vol. 124, no. 16, pp. 2514–2518, 2013.
[32] N. Rawat, R. Kumar, and B.-G. Lee, "Implementing compressive fractional Fourier transformation with iterative kernel steering regression in double random phase encoding," *Optik-Int. J. Light Electron Opt.*, vol. 125, no. 18, pp. 5414–5417, 2014.
[33] B. Deepan, C. Quan, Y. Wang, and C. J. Tay, "Multiple-image encryption by space multiplexing based on compressive sensing and the double-random phase-encoding technique," *Appl. Opt.*, vol. 53, no. 20, pp. 4539–4547, 2014.
[34] Y. Zhang and L. Y. Zhang, "Exploiting random convolution and random subsampling for image encryption and compression," *Electron. Lett.*, vol. 51, no. 20, pp. 1572–1574, 2015.
[35] X. Liu, Y. Cao, P. Lu, X. Lu, and Y. Li, "Optical image encryption technique based on compressed sensing and arnold transformation," *Optik-Int. J. Light Electron Opt.*, vol. 124, no. 24, pp. 6590–6593, 2013.
[36] X. Liu, W. Mei, and H. Du, "Optical image encryption based on compressive sensing and chaos in the fractional Fourier domain," *J. Modern Opt.*, vol. 61, no. 19, pp. 1570–1577, 2014.
[37] J. Lang and J. Zhang, "Optical image cryptosystem using chaotic phase-amplitude masks encoding and least-data-driven decryption by compressive sensing," *Opt. Commun.*, vol. 338, pp. 45–53, Mar. 2015.
[38] H. Liu, D. Xiao, Y. Liu, and Y. Zhang, "Securely compressive sensing using double random phase encoding," *Optik-Int. J. Light Electron Opt.*, vol. 126, no. 20, pp. 2663–2670, 2015.
[39] L. Y. Zhang, K.-W. Wong, Y. Zhang, and Q. Lin, "Joint quantization and diffusion for compressed sensing measurements of natural images," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2015, pp. 2744–2747.
[40] L. Y. Zhang, K.-W. Wong, Y. Zhang, and J. Zhou, "Bi-level protected compressive sampling," *IEEE Trans. Multimedia*, to be published.
[41] Y. Zhang *et al.*, "Embedding cryptographic features in compressive sensing," *Neurocomputing*, to be published.
[42] R. Fay, "Introducing the counter mode of operation to compressed sensing based encryption," *Inf. Process. Lett.*, vol. 116, no. 4, pp. 279–283, 2016.
[43] G. Valenzise, M. Tagliasacchi, S. Tubaro, G. Cancelli, and M. Barni, "A compressive-sensing based watermarking scheme for sparse image tampering identification," in *Proc. 16th IEEE Int. Conf. Image Process. (ICIP)*, Nov. 2009, pp. 1265–1268.
[44] X. Zhang, Z. Qian, Y. Ren, and G. Feng, "Watermarking with flexible self-recovery quality based on compressive sensing and compositive reconstruction," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 4, pp. 1223–1232, Dec. 2011.
[45] H.-C. Huang, F.-C. Chang, C.-H. Wu, and W.-H. Lai, "Watermarking for compressive sampling applications," in *Proc. 8th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process. (IIH-MSP)*, 2012, pp. 223–226.
[46] I. Orović, A. Draganić, and S. Stanković, "Compressive sensing as a watermarking attack," in *Proc. 21st Telecommun. Forum (TELFOR)*, Nov. 2013, pp. 741–744.
[47] I. Orović and S. Stanković, "Combined compressive sampling and image watermarking," in *Proc. IEEE 55th Int. Symp. ELMAR*, Sep. 2013, pp. 41–44.
[48] D. Xiao, M.-M. Deng, and Y.-S. Zhang, "Robust and separable watermarking algorithm in encrypted image based on compressive sensing," *J. Electron. Inf. Technol.*, vol. 37, no. 5, pp. 1248–1254, 2015.
[49] H. Liu, D. Xiao, R. Zhang, Y. Zhang, and S. Bai, "Robust and hierarchical watermarking of encrypted images based on compressive sensing," *Signal Process., Image Commun.*, vol. 45, pp. 41–51, Jul. 2016.
[50] W. Li, J.-S. Pan, L. Yan, C.-S. Yang, and H.-C. Huang, "Data hiding based on subsampling and compressive sensing," in *Proc. 9th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, 2013, pp. 611–614.
[51] J.-S. Pan, W. Li, C.-S. Yang, and L.-J. Yan, "Image steganography based on subsampling and compressive sensing," *Multimedia Tools Appl.*, vol. 74, no. 21, pp. 9191–9205, 2015.
[52] D. Xiao and S. Chen, "Separable data hiding in encrypted image based on compressive sensing," *Electron. Lett.*, vol. 50, no. 8, pp. 598–600, 2014.
[53] G. Hua, Y. Xiang, and G. Bi, "When compressive sensing meets data hiding," *IEEE Signal Process. Lett.*, vol. 23, no. 4, pp. 473–477, Apr. 2016.
[54] M. Li, D. Xiao, and Y. Zhang, "Reversible data hiding in block compressed sensing images," *ETRI J.*, vol. 38, no. 1, pp. 159–163, 2016.
[55] L.-W. Kang, C.-S. Lu, and C.-Y. Hsu, "Compressive sensing-based image hashing," in *Proc. 16th IEEE Int. Conf. Image Process. (ICIP)*, Nov. 2009, pp. 1285–1288.
[56] M. Tagliasacchi, G. Valenzise, and S. Tubaro, "Hash-based identification of sparse image tampering," *IEEE Trans. Image Process.*, vol. 18, no. 11, pp. 2491–2504, Nov. 2009.
[57] R. Sun and W. Zeng, "Secure and robust image hashing via compressive sensing," *Multimedia Tools Appl.*, vol. 70, no. 3, pp. 1651–1665, Jun. 2014.
[58] H. Liu, D. Xiao, Y. Xiao, and Y. Zhang, "Robust image hashing with tampering recovery capability via low-rank and sparse representation," *Multimedia Tools Appl.*, to be published.
[59] H. Suzuki, M. Suzuki, T. Urabe, T. Obi, M. Yamaguchi, and N. Ohyama, "Secure biometric image sensor and authentication scheme based on compressed sensing," *Appl. Opt.*, vol. 52, no. 33, pp. 8161–8168, 2013.
[60] H. Suzuki, M. Takeda, T. Obi, M. Yamaguchi, N. Ohyama, and K. Nakano, "Encrypted sensing for enhancing security of biometric authentication," in *Proc. 13th Workshop Inf. Opt. (WIO)*, 2014, pp. 1–3.
[61] D. Xiao, M. Deng, and X. Zhu, "A reversible image authentication scheme based on compressive sensing," *Multimedia Tools Appl.*, vol. 74, no. 18, pp. 7729–7752, 2015.
[62] L.-W. Kang *et al.*, "Secure transcoding for compressive multimedia sensing," in *Proc. 18th IEEE Int. Conf. Image Process. (ICIP)*, Sep. 2011, pp. 917–920.
[63] J. K. Pillai, V. M. Patel, R. Chellappa, and N. K. Ratha, "Secure and robust iris recognition using random projections and sparse representations," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 33, no. 9, pp. 1877–1893, Sep. 2011.
[64] L. Liu, A. Wang, C.-C. Chang, and Z. Li, "A novel real-time and progressive secret image sharing with flexible shadows based on compressive sensing," *Signal Process., Image Commun.*, vol. 29, no. 1, pp. 128–134, 2014.
[65] J. Qi, X. Hu, Y. Ma, and Y. Sun, "A hybrid security and compressive sensing-based sensor data gathering scheme," *IEEE Access*, vol. 3, pp. 718–724, 2015.
[66] M. Cossalter, M. Tagliasacchi, and G. Valenzise, "Privacy-enabled object tracking in video sequences using compressive sensing," in *Proc. 6th IEEE Int. Conf. Adv. Video Signal Based Surveill.*, Sep. 2009, pp. 436–441.

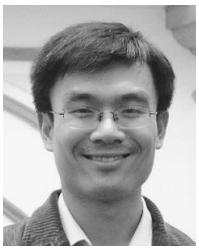
[67] L. Tong, F. Dai, Y. Zhang, J. Li, and D. Zhang, "Compressive sensing based video scrambling for privacy protection," in *Proc. IEEE Vis. Commun. Image Process. (VCIP)*, Nov. 2011, pp. 1–4.
[68] X. Chen and H. Zhao, "A novel video content authentication algorithm combined semi-fragile watermarking with compressive sensing," in *Proc. 2nd Int. Conf. Intell. Syst. Design Eng. Appl. (ISDEA)*, 2012, pp. 134–137.
[69] L. G. Jyothish, V. K. Veena, and K. P. Soman, "A cryptographic approach to video watermarking based on compressive sensing, Arnold transform, sum of absolute deviation and SVD," in *Proc. Annu. Int. Conf. Emerg. Res. Areas*, 2013, pp. 1–5.
[70] G. Valenzise, G. Prandi, M. Tagliasacchi, and A. Sarti, "Identification of sparse audio tampering using distributed source coding and compressive sensing techniques," *J. Image Video Process.*, vol. 2009, Jan. 2009, Art. no. 158982.
[71] W. Zhu, C. Luo, J. Wang, and S. Li, "Multimedia cloud computing," *IEEE Signal Process. Mag.*, vol. 28, no. 3, pp. 59–69, May 2011.
[72] L.-W. Kang, K. Muchtar, J.-D. Wei, C.-Y. Lin, D.-Y. Chen, and C.-H. Yeh, "Privacy-preserving multimedia cloud computing via compressive sensing and sparse representation," in *Proc. Int. Conf. Inf. Secur. Intell. Control (ISIC)*, 2012, pp. 246–249.
[73] C. Wang, B. Zhang, K. Ren, and J. M. Roveda, "Privacy-assured outsourcing of image reconstruction service in cloud," *IEEE Trans. Emerg. Topics Comput.*, vol. 1, no. 1, pp. 166–177, Jun. 2013.
[74] Q. Wang, W. Zeng, and J. Tian, "A compressive sensing based secure watermark detection and privacy preserving storage framework," *IEEE Trans. Image Process.*, vol. 23, no. 3, pp. 1317–1328, Mar. 2014.
[75] C. Wang, B. Zhang, K. Ren, J. M. Roveda, C. W. Chen, and Z. Xu, "A privacy-aware cloud-assisted healthcare monitoring system via compressive sensing," in *Proc. INFOCOM*, Apr./May 2014, pp. 2130–2138.
[76] Y. Zhang, J. Zhou, L. Y. Zhang, F. Chen, and X. Lei, "Support-set-assured parallel outsourcing of sparse reconstruction service for compressive sensing in multi-clouds," in *Proc. Int. Symp. Secur. Privacy Social Netw. Big Data (SocialSec)*, 2015, pp. 1–6.
[77] X. Wu, P. Yang, S. Tang, X. Zheng, and Y. Xiong, "Privacy preserving RSS map generation for a crowdsensing network," *IEEE Wireless Commun.*, vol. 22, no. 4, pp. 42–48, Aug. 2015.
[78] L. Wan, G. Han, L. Shu, and N. Feng, "The critical patients localization algorithm using sparse representation for mixed signals in emergency healthcare system," *IEEE Syst. J.*, to be published.
[79] L. Wan, G. Han, L. Shu, S. Chan, and N. Feng, "PD source diagnosis and localization in industrial high-voltage insulation system via multimodal joint sparse representation," *IEEE Trans. Ind. Electron.*, vol. 63, no. 4, pp. 2506–2516, Apr. 2016.
[80] Z. Hua and Y. Zhou, "Image encryption using 2D Logistic-adjusted-Sine map," *Inf. Sci.*, vol. 339, pp. 237–253, Apr. 2016.
[81] Y. Zhang and D. Xiao, "Self-adaptive permutation and combined global diffusion for chaotic color image encryption," *AEU-Int. J. Electron. Commun.*, vol. 68, no. 4, pp. 361–368, Apr. 2014.
[82] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Process.*, vol. 92, no. 4, pp. 1101–1108, Apr. 2012.
[83] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "2D Sine Logistic modulation map for image encryption," *Inf. Sci.*, vol. 297, pp. 80–94, Mar. 2015.
[84] O.-Y. Lui, K.-W. Wong, J. Chen, and J. Zhou, "Chaos-based joint compression and encryption algorithm for generating variable length ciphertext," *Appl. Soft Comput.*, vol. 12, no. 1, pp. 125–132, 2012.
[85] L. Y. Zhang, X. Hu, Y. Liu, K.-W. Wong, and J. Gan, "A chaotic image encryption scheme owning temp-value feedback," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 10, pp. 3653–3659, Oct. 2014.
[86] W. Wen, Y. Zhang, Z. Fang, and J.-X. Chen, "Infrared target-based selective encryption by chaotic maps," *Opt. Commun.*, vol. 341, pp. 131–139, Apr. 2015.
[87] J.-X. Chen, Z.-L. Zhu, Z. Liu, C. Fu, L.-B. Zhang, and H. Yu, "A novel double-image encryption scheme based on cross-image pixel scrambling in gyrator domains," *Opt. Exp.*, vol. 22, no. 6, pp. 7349–7361, Mar. 2014.
[88] Y. Zhang, D. Xiao, W. Wen, and Y. Tian, "Edge-based lightweight image encryption using chaos-based reversible hidden transform and multiple-order discrete fractional cosine transform," *Opt. Laser Technol.*, vol. 54, pp. 1–6, Dec. 2013.
[89] J.-X. Chen, Z.-L. Zhu, C. Fu, L.-B. Zhang, and Y. Zhang, "Cryptanalysis and improvement of an optical image encryption scheme using a chaotic Baker map and double random phase encoding," *J. Opt.*, vol. 16, no. 12, p. 125403, Oct. 2014.
[90] J.-X. Chen, Z.-L. Zhu, C. Fu, L.-B. Zhang, and H. Yu, "Analysis and improvement of a double-image encryption scheme using pixel scrambling technique in gyrator domains," *Opt. Lasers Eng.*, vol. 66, pp. 1–9, Mar. 2015.
[91] E. J. Candès and T. Tao, "Decoding by linear programming," *IEEE Trans. Inf. Theory*, vol. 51, no. 12, pp. 4203–4215, Dec. 2005.
[92] L. Yu, J. P. Barbot, G. Zheng, and H. Sun, "Compressive sensing with chaotic sequence," *IEEE Signal Process. Lett.*, vol. 17, no. 8, pp. 731–734, Aug. 2010.
[93] H. Fang, S. A. Vorobyov, H. Jiang, and O. Taheri, "Permutation meets parallel compressed sensing: How to relax restricted isometry property for 2D sparse signals," *IEEE Trans. Signal Process.*, vol. 62, no. 1, pp. 196–210, Jan. 2014.
[94] P. Refregier and B. Javidi, "Optical image encryption using input plane and Fourier plane random encoding," *Opt. Lett.*, vol. 20, no. 7, pp. 767–769, Apr. 1995.
[95] H. Takeda, S. Farsiu, and P. Milanfar, "Kernel regression for image processing and reconstruction," *IEEE Trans. Image Process.*, vol. 16, no. 2, pp. 349–366, Feb. 2007.
[96] Q. Gong, X. Liu, G. Li, and Y. Qin, "Multiple-image encryption and authentication with sparse representation by space multiplexing," *Appl. Opt.*, vol. 52, no. 31, pp. 7486–7493, Nov. 2013.
[97] U. Gopinathan, D. S. Monaghan, T. J. Naughton, and J. T. Sheridan, "A known-plaintext heuristic attack on the Fourier plane encryption algorithm," *Opt. Exp.*, vol. 14, no. 8, pp. 3181–3186, Apr. 2006.
[98] X. Peng, P. Zhang, H. Wei, and B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," *Opt. Lett.*, vol. 31, no. 8, pp. 1044–1046, Apr. 2006.
[99] Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, "Resistance of the double random phase encryption against various attacks," *Opt. Exp.*, vol. 15, no. 16, pp. 10253–10265, Aug. 2007.
[100] Y. Zhang, D. Xiao, W. Wen, and H. Liu, "Vulnerability to chosen-plaintext attack of a general optical encryption model with the architecture of scrambling-then-double random phase encoding," *Opt. Lett.*, vol. 38, no. 21, pp. 4506–4509, Nov. 2013.
[101] Y. Rivenson, A. Stern, and B. Javidi, "Single exposure super-resolution compressive imaging by double phase encoding," *Opt. Exp.*, vol. 18, no. 14, pp. 15094–15103, Jul. 2010.
[102] A. Alfalou and C. Brosseau, "Optical image compression and encryption methods," *Adv. Opt. Photon.*, vol. 1, no. 3, pp. 589–636, 2009.
[103] A. Alfalou and C. Brosseau, "Exploiting root-mean-square time-frequency structure for multiple-image optical compression and encryption," *Opt. Lett.*, vol. 35, no. 11, pp. 1914–1916, 2010.
[104] A. Alfalou, C. Brosseau, N. Abdallah, and M. Jridi, "Simultaneous fusion, compression, and encryption of multiple images," *Opt. Exp.*, vol. 19, no. 24, pp. 24023–24029, 2011.
[105] W.-K. Yu, M.-F. Li, X.-R. Yao, X.-F. Liu, L.-A. Wu, and G.-J. Zhai, "Adaptive compressive ghost imaging based on wavelet trees and sparse representation," *Opt. Exp.*, vol. 22, no. 6, pp. 7133–7144, 2014.
[106] G. Oliveri, L. Poli, P. Rocca, and A. Massa, "Bayesian compressive optical imaging within the Rytov approximation," *Opt. Lett.*, vol. 37, no. 10, pp. 1760–1762, 2012.
[107] J. Greenberg, K. Krishnamurthy, and D. Brady, "Compressive single-pixel snapshot X-ray diffraction imaging," *Opt. Lett.*, vol. 39, no. 1, pp. 111–114, 2014.
[108] X. Lin, G. Wetzstein, Y. Liu, and Q. Dai, "Dual-coded compressive hyperspectral imaging," *Opt. Lett.*, vol. 39, no. 7, pp. 2044–2047, 2014.
[109] Y. Zhang and D. Xiao, "Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform," *Opt. Lasers Eng.*, vol. 51, no. 4, pp. 472–480, Apr. 2013.
[110] W.-X. Wang, R. Yang, Y.-C. Lai, V. Kovanis, and C. Grebogi, "Predicting catastrophes in nonlinear dynamical systems by compressive sensing," *Phys. Rev. Lett.*, vol. 106, no. 15, p. 154101, Apr. 2011.
[111] W.-X. Wang, R. Yang, Y.-C. Lai, V. Kovanis, and M. A. F. Harrison, "Time-series–based prediction of complex oscillator networks via compressive sensing," *Europhys. Lett.*, vol. 94, no. 4, p. 48006, May 2011.
[112] S. C. Draper and S. Malekpour, "Compressed sensing over finite fields," in *Proc. IEEE Int. Conf. Symp. Inf. Theory*, Jun./Jul. 2009, pp. 669–673.
[113] A. K. Das and S. Vishwanath, "On finite alphabet compressive sensing," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, May 2013, pp. 5890–5894.
[114] V. Bioglio, G. Coluccia, and E. Magli, "Sparse image recovery using compressed sensing over finite alphabets," in *Proc. IEEE Int. Conf. Image Process. (ICIP)*, Oct. 2014, pp. 1287–1291.

[115] L. Yu, J. P. Barbot, G. Zheng, and H. Sun, "Toeplitz-structured chaotic sensing matrix for compressive sensing," in *Proc. 7th Int. Symp. Commun. Syst. Netw. Digit. Signal Process. (CSNDSP)*, Jul. 2010, pp. 229–233.
[116] V. Kafedziski and T. Stojanovski, "Compressive sampling with chaotic dynamical systems," in *Proc. 19th Telecommun. Forum (TELFOR)*, Nov. 2011, pp. 695–698.
[117] M. Frunzete, L. Yu, J.-P. Barbot, and A. Vlad, "Compressive sensing matrix designed by tent map, for secure data transmission," in *Proc. Signal Process. Algorithms, Archit., Arrangements, Appl. (SPA)*, 2011, pp. 1–6.
[118] G. Chen, D. Zhang, Q. Chen, and D. Zhou, "The characteristic of different chaotic sequences for compressive sensing," in *Proc. 5th Int. Congr. Image Signal Process. (CISP)*, 2012, pp. 1475–1479.
[119] H. Gan, Z. Li, J. Li, X. Wang, and Z. Cheng, "Compressive sensing using chaotic sequence based on Chebyshev map," *Nonlinear Dyn.*, vol. 78, no. 4, pp. 2429–2438, 2014.
[120] S. Evladov, O. Levi, and A. Stern, "Progressive compressive imaging from Radon projections," *Opt. Exp.*, vol. 20, no. 4, pp. 4260–4271, 2012.
[121] H. Shen *et al.*, "Spinning disk for compressive imaging," *Opt. Lett.*, vol. 37, no. 1, pp. 46–48, 2012.
[122] A. Alfalou, A. Loussert, A. Alkholidi, and R. El Sawda, "System for image compression and encryption by spectrum fusion in order to optimize image transmission," in *Proc. IEEE Future Generat. Commun. Netw.*, vol. 2. Dec. 2007, pp. 590–593.
[123] M. Abdalla, M. Bellare, and G. Neven, "Robust encryption," in *Theory of Cryptography*. Springer, Zurich, Switzerland, 2010, pp. 480–497.
[124] 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.
[125] A. Piva and S. Katzenbeisser, "Signal processing in the encrypted domain," *EURASIP J. Inf. Secur.*, vol. 2007, 2007, Art. no. 82790.
[126] Y. Zhang, K.-W. Wong, L. Y. Zhang, W. Wen, J. Zhou, and X. He, "Robust coding of encrypted images via structural matrix," *Signal Process., Image Commun.*, vol. 39, pp. 202–211, Nov. 2015.
[127] 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.
[128] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proc. STOC*, vol. 9. 2009, pp. 169–178.

YUSHU ZHANG received the B.S. degree from the Department of Mathematics, North University of China, Shanxi, China, in 2010, and the Ph.D. degree from the College of Computer Science, Chongqing University, Chongqing, China, in 2014. Since 2015, he has been an Associate Professor with the School of Electronics and Information Engineering, Southwest University, Chongqing, China. He held various research positions with the City University of Hong Kong and the University of Macau. His research interests include multimedia coding and security, secure signal processing through lossy channel, and compressive sensing security.



LEO YU ZHANG received the bachelor's and master's degrees in computational mathematics from Xiangtan University, in 2009 and 2012, respectively, and the Ph.D. degree from the Department of Electronic Engineering, City University of Hong Kong, Hong Kong. From 2012 to 2013, he was with the State Grid Electric Power Research Institute of China as a Development Engineer. His research interests include multimedia security and compressive sensing.



JIANTAO ZHOU (M'11) received the B.Eng. degree from the Department of Electronic Engineering, Dalian University of Technology, Dalian, China, in 2002, the M.Phil. degree from the Department of Radio Engineering, Southeast University, Nanjing, China, in 2005, and the Ph.D. degree from the Department of Electronic and Computer Engineering, Hong Kong University of Science and Technology, Hong Kong, in 2009. He held various research positions with the University of Illinois at Urbana–Champaign, the Hong Kong University of Science and Technology, and McMaster University. He is currently an Assistant Professor with the Department of Computer and Information Science, Faculty of Science and Technology, University of Macau. His research interests include multimedia security and forensics, and high-fidelity image compression. He was a co-author of a paper that received the best paper award in the IEEE Pacific-Rim Conference on Multimedia in 2007.

LICHENG LIU received the B.S. degree in information and computational science from the China University of Geosciences, Wuhan, China, in 2010, the M.S. degree in applied mathematics from Hunan University, Changsha, China, in 2012, the Ph.D. degree from the Department of Computer and Information Science, Faculty of Science and Technology, University of Macau, Macau, China. His research interests include image processing, sparse representation, computer vision, and machine learning.

FEI CHEN received the B.Eng. and M.S. degrees in computer science and engineering from Chongqing University, China, and the Ph.D. degree in computer science and engineering from The Chinese University of Hong Kong. He visited the Distributed Systems Group with the Vienna University of Technology in 2014. He also interned with the Database Team, Alibaba Group, in 2013, and the State Key Laboratory of Information Security of the Chinese Academy of Science in 2009. He joined the College of Computer Science and Engineering, Shenzhen University, China, as a Lecturer in 2015. His research interests include information and network security, data protection, and privacy.

XING HE received the B.S. degree in mathematics and applied mathematics from the Department of Mathematics, Guizhou University, Guiyang, China, in 2009, and the Ph.D. degree in computer science and technology from Chongqing University, Chongqing, China, in 2013. He is currently an Associate Professor with the School of Electronics and Information Engineering, Southwest University, Chongqing. From 2012 to 2013, he was a Research Assistant with Texas A&M University at Qatar, Doha, Qatar. His research interests include neural networks, bifurcation theory, optimization method, smart grid, and nonlinear dynamical system.