Privacy-Assured FogCS: Chaotic Compressive Sensing for Secure Industrial Big Image Data Processing in Fog Computing

Yushu Zhang, *Member, IEEE*, Ping Wang, Hui Huang, Youwen Zhu*, Di Xiao, *Member, IEEE*, and Yong Xiang, *Senior Member, IEEE*

***Abstract*—In the age of the industrial big data, there are several significant problems such as high-overhead data acquisition, data privacy leakage, and data tampering. Fog computing capability is rapidly expanding to address not only network congestion issues but data security issues. This paper presents a chaotic compressive sensing (CS) scheme for securely processing industrial big image data in the fog computing paradigm, called Privacy-Assured FogCS. Specially, the Sine Logistic modulation map is used to drive the privacy-assured, authenticated, and block CS for secure image data collection in the sensor nodes. After sampling, the measurements are normalized in the fog nodes. The normalized measurements can achieve the perfect secrecy and their energy values are further masked through the proposed permutation-diffusion architecture. Finally, these relevant data are transmitted to the clouds (data centers) for storage, reconstruction, and authentication if required. In addition, a hardware implementation reference on a field programmable gate array (FPGA) is designed. Simulation analyses show the feasibility and efficiency of the Privacy-Assured FogCS scheme.**

***Index Terms*—Industrial big image data, chaotic compressive sensing, fog computing, Sine Logistic modulation map, FPGA.**

I. Introduction

With the advancement in science and technology, society is facing a data-driven world. There are many challenges related to dealing with big data because of its five-V inherent characteristics, i.e., high value, high veracity, high volume, high variety, and high velocity [1]. Therefore, the efficient and innovative processing techniques are of great significance for improving insight and decision-making [2]. The "pay-as-you-go" cloud computing paradigm [3], [4] has become an attractive choice for sharing resource to cope with the explosive growth of the amount of data. Cloud computing has various advantages such as low cost, high scalability, and high usability. The prevalence of Internet of Things (IoT) poses some tremendous challenges to the cloud computing paradigm [5] due to issues such as high latency and traffic congestion. To address these challenges, fog computing paradigm is presented by extending cloud computing capability to the edge of the network for reducing the data volume to the central clouds [6]–[8]. Fog computing can provide computing, storage, and network services by deploying servers between the end-users and the cloud. The infrastructure of fog computing is shown in Fig. 1.

Compressive sensing (CS), an advanced signal processing technology proposed by Candès *et al.* [9]–[11], claims that a signal can be simultaneously sampled and compressed with a low computation complexity by virtue of its sparsity and efficiently reconstructed by solving an underdetermined linear system. Thus, CS is considered for the wide use in the resource-limited data acquisition scenarios such as wireless sensor networks [12]. In addition to its low-complexity property, CS can also provide secure and authenticated data acquisition against data privacy leakage and data tampering.

CS can be viewed as a cryptosystem [13]–[15], in which the random measurement matrix acts as the shared secret between only the encoder and the decoder. Such a cryptosystem can realize secure data collection so as to be widely applied in IoT [16], Internet of multimedia things [17], wireless energy auditing networks [18], and wireless body area networks [19], [20]. Nevertheless, the design of resisting data tampering is missing in these CS-based privacy-preserving schemes. Wu and Ruland proposed a CS-based data integrity authentication scheme to detect the malicious tampering behaviors using the dimensionality-reducing property of CS [21], [22], but they did not consider the privacy leakage issue. With the development of fog computing, fog capability is also being used in the information security field [23], [24] except for addressing the issues of high latency and traffic congestion. In this paper, we propose a CS-based secure big image data processing scheme under fog computing circumstance, called Privacy-Assured FogCS, to address the above challenges.

The proposed scheme conveys several aspects of work. First, chaotic CS means that the measurement matrix is generated

This work was supported in part by the National Key R&D Program of China under Grant 2017YFB0802300, in part by the Chongqing Key Laboratory of Mobile Communications Technology under Grant cqupt-mct-201901, in part by the Six Talents Peak Project of Jiangsu Province under Grant RJFW-027, in part by the Australian Research Council under Grant LP190100594, in part by the Chongqing Research Program of Basic Research and Frontier Technology under Grant No. cstc2017jcyjBX0008, in part by the Chongqing Postgraduate Education Reform Project under Grant No. yjg183018, and in part by the Chongqing University Postgraduate Education Reform Project under Grant No. cquyjg18219.

Corresponding author: Youwen Zhu.

Y. Zhang and Y. Zhu are with the College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China and the Collaborative Innovation Center of Novel Software Technology and Industrialization, Nanjing 210023, China (e-mail: yushu@nuaa.edu.cn; zhuyw@nuaa.edu.cn).

P. Wang is with the College of Cybersecurity, Sichuan University, Chengdu 610207, China (e-mail: bruce_wp@163.com).

H. Huang and D. Xiao are with the College of Computer Science, Chongqing University, Chongqing 400044, China (e-mail: cqyyhuang@163.com; dixiao@cqu.edu.cn).

Y. Xiang is with the School of Information Technology, Deakin University, Melbourne, VIC 3125, Australia (e-mail: yong.xiang@deakin.edu.au).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2020.3008914, IEEE Transactions on Industrial Informatics

by iterating chaotic systems with several initial values and parameters. It can drastically reduce the storage space requirement of the measurement matrices relative to the traditional CS in which the size of the measurement matrices is much larger than the signal to be sampled [25]–[27]. Specifically, the circulant-structured chaotic measurement matrix (CSCMM) is constructed by iterating Sine Logistic modulation map (SLMM) [28]. Second, the block CS [29], [30] is used to decrease the processing time and maintain a much lower implementation cost compared with the traditional CS. Accordingly, the measurements are normalized to achieve the perfect secrecy and their energy values are further masked through a permutation-diffusion architecture in the fog nodes. Finally, the hardware implementation on a field programmable gate array (FPGA) [31] is introduced for the proposed scheme.

In the proposed Privacy-Assured FogCS scheme, a color image that can be sparsely represented by the discrete wavelet transformation (DWT) is simultaneously sampled and compressed using the block CS. The keyed SLMM is employed to construct the CSCMM used to perform the CS encode. When encoding the color image, an authentication matrix generated in a similar way with the measurement matrix is used to generate the authenticated measurements while sampling. The measurements and authenticated measurements are sent to the fog nodes. Moreover, the measurements are normalized to achieve Shannon's perfect secrecy and then the corresponding energy values are masked using the permutation-diffusion architecture in the fog nodes. Finally, these relevant data are transmitted to the data center for storage and reconstruction if required. To summarize, the main contributions of the proposed scheme are as follows.

- **Guaranteeing data integrity:** An efficient integrity authentication mechanism based on CS is designed to verify whether the received image has been tampered with.
- **Guaranteeing data confidentiality:** The normalized measurements can achieve the Shannon's perfect secrecy and the secrecy of the corresponding energy values is guaranteed by the proposed permutation-diffusion architecture.
- **Reducing storage space:** The storage space requirement of the sensing devices is dramatically reduced by adopting the block CS, the SLMM, and the CSCMM.
- **Accelerating reconstruction speed:** The block CS can clearly accelerate the reconstruction speed because of its parallel processing mode.

The remainder of this paper is organized as follows. Section II provides the background knowledge including CS, chaotic measurement matrix, and the CS-based data integrity authentication. The Privacy-Assured FogCS scheme is proposed in detail in Section III, including secure data collection in the sensor nodes, data postprocessing in the fog nodes, CS reconstruction and integrity authentication in the central cloud, and security discussion. Section IV introduces the hardware implementation of the proposed scheme on FPGA. Section V gives the simulation analyses in terms of tampering, key sensitivity, compression performance, and reconstruction time. Section VI concludes this work.

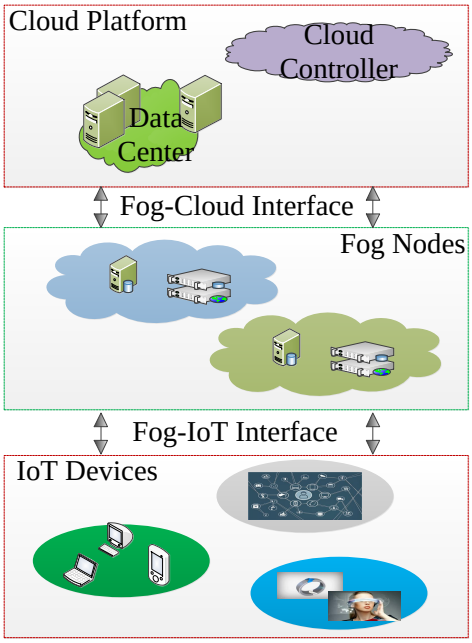


Fig. 1. The infrastructure of fog computing.

II. The Related Knowledge

A. Compressive Sensing

Suppose a discrete–time signal $\mathrm{x} \in R^{N\times 1}$ can be expressed as

$$\mathrm{x} = \sum_{i=1}^{N} \psi_i s_i = \Psi \mathrm{s}, \tag{1}$$

where $\Psi = [\psi_1, \psi_2, ..., \psi_N]$ $(\psi_i \in R^{N\times 1}, i = 1, 2, ..., N)$ is a proper orthogonal transform matrix and s is a coefficient vector. x is said to be k-sparse if s contains at most k nonzero coefficients in the Ψ domain. Note that x and s are two different expressions of the same signal. Unlike the traditional Nyquist sampling model, such a k-sparse signal x can be sampled and compressed simultaneously by

$$\mathrm{y} = \Phi \mathrm{x} = \Phi\Psi \mathrm{s} = \Theta \mathrm{s}, \tag{2}$$

where $\mathrm{y} \in R^{M\times 1}(M \ll N)$ denotes a measurement vector, $\Phi \in R^{M\times N}$ denotes a measurement matrix, and $\Theta \in R^{M\times N}$ denotes a sensing matrix. If the sampling-compression operation is performed in the transform domain, the above linear projection (2) can be expressed as

$$\mathrm{y} = \Phi \mathrm{s} = \Phi\Psi^T \mathrm{x} = \Theta \mathrm{s}, \tag{3}$$

where Φ and Θ are the same. Obviously, both the linear systems (2) and (3) have an infinite number of solutions because of their dimensionality-reducing transformation. As a result, it seems to be impossible to reconstruct x. However, by virtue of the sparsity of x, solving (2) and (3) can be transformed into the following optimization problem, i.e.,

$$\min_{\mathrm{s}} \|\mathrm{s}\|_0 \text{ s.t. } \mathrm{y} = \Theta \mathrm{s}, \tag{4}$$

where $\|\mathrm{s}\|_0$ denotes the l_0 norm of s. Solving (4) is a NP-hard problem because it has to exhaustively search over all

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2020.3008914, IEEE Transactions on Industrial Informatics

column subsets of Θ. However it can be transformed to solve the following l_1 norm problem, i.e.,

$$\min_{\mathrm{s}} \|\mathrm{s}\|_1 \text{ s.t. } \mathrm{y} = \Theta \mathrm{s}. \tag{5}$$

Solving (5) is a convex optimization problem that can be solved by the linear programming method.

It should be noted that Φ should be some information-preserving guarantees. One is that the row number M of Φ must be not less than $\mathrm{O}(k\log(N/k))$. The other is that Φ should be as incoherent as possible with Ψ. Φ is proved to be incoherent with Ψ if Φ satisfy a mathematical definition of Restricted Isometry Property (RIP) [32], in which a matrix Φ is said to satisfy the RIP of order k if for all k-sparse signals x there exists a constant $\delta_k \in (0,1)$ such that

$$1-\delta_k \le \frac{\|\Phi \mathrm{x}\|_2^2}{\|\mathrm{x}\|_2^2} \le 1+\delta_k. \tag{6}$$

Considering that image data often are large in size, it is unreasonable to utilize one large-size measurement matrix for the sampling. Block CS is proposed for image data to partition each image into many equal-sized blocks, e.g., 16×16, and then sample each block using the same measurement matrix [29], [30]. In the block CS framework, the size of the measurement matrix is greatly reduced compared with that in the normal CS. Besides, not only the sampling process but also the reconstruction process can be parallelized.

B. Chaotic measurement matrix

The one-dimension (1D) chaotic maps, such as the Logistic map, Sine map, Tent map, and Chebyshev map, can be used in cryptography due to their unpredictability, ergodicity, and sensitivity to the initial conditions and control parameters [33]. However, the 1D chaotic maps have quite a few drawbacks including poor efficiency, weak security, etc. To overcome these shortcomings, the SLMM [28] with better ergodicity, hyperchaotic property, and lower implementation cost is usually used in practice, which is defined as follows:

$$\begin{cases} x_{i+1} = \mu(\sin(\pi y_i)+\nu)x_i(1-x_i) \\ y_{i+1} = \mu(\sin(\pi x_{i+1})+\nu)y_i(1-y_i) \end{cases}, \tag{7}$$

where $\mu \in [0,1]$, $\nu \in [0,3]$ are two control parameters and $x_0 \in (0,1)$, $y_0 \in (0,1)$ are two initial input values. It can be easily found that the output values x_{i+1} and y_{i+1} of the SLMM are intertwined, resulting in that it is difficult to predict the output trajectories.

A chaotic sequence $\{h\}_{i=0}^{N-1}$ can be generated by iterating the above SLMM with two initial values (x_0, y_0). Then a CSCMM $\Phi \in R^{M\times N}$ can be created from the chaotic sequence as follows:

$$\Phi = \frac{1}{\sqrt{M}\delta}\begin{Bmatrix} h_{(N-1)} & h_{(N-2)} & \cdots & h_0 \\ h_0 & h_{(N-1)} & \cdots & h_1 \\ \vdots & \vdots & \ddots & \vdots \\ h_{(M-2)} & h_{(M-3)} & \cdots & h_{(M-1)} \end{Bmatrix}, \tag{8}$$

where $1\Big/\sqrt{M}\delta$ is used for normalization and δ^2 is the variance of $\{h\}_{i=0}^{N-1}$.

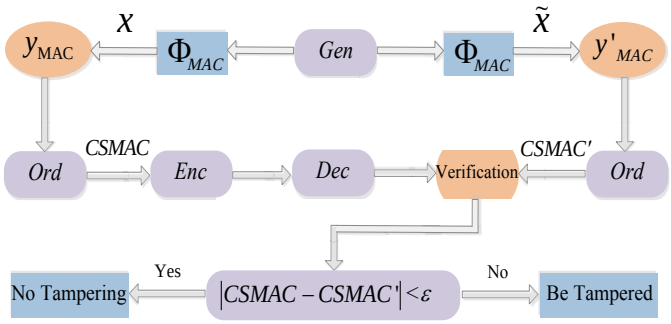


Fig. 2. The CS-based integrity authentication framework.

When x_0 and y_0 are viewed as the keys shared between only the encoder and the decoder, chaotic cryptographic features are embedded in CS, called chaotic CS. The use of CSCMM in the proposed scheme is due to several reasons. First, the large-size measurement matrix can be replaced by the few initial values of the SLMM in the process of transmission, resulting in a significant reduce of communication burden. Second, only N independent random variables generated through SLMM are required, thus the complexity of terminal sensing devices can be greatly reduced. Third, it is easier to implement CSCMM on hardware compared with the general measurement matrices such as Gaussian matrix and Bernoulli matrix. Finally, the SLMM juggles good cryptographic features and low computational complexity in contrast to other normal chaotic maps such as Tent map and Logistic map.

C. CS-based data integrity authentication

In the CS framework, the integrity of the reconstructed image should be able to be authenticated against some malicious tampering manipulations. Meanwhile, some inevitable and acceptable manipulations, such as lossy compression, quantization error, and channel noise, can be tolerated.

The CS-based data integrity authentication framework is shown in Fig. 2, which contains three core functions, namely

- The keyed matrix generator (*Gen*): Analogous to a pseudo random number generator (PRNG), *Gen* employs the size information and the initial input values to construct an unpredictable authentication matrix;
- The value order extraction function (*Ord*): *Ord* sorts the input sequence and then outputs the corresponding order sequence, for example, $Ord([4,5,1,-8,7]) = [3,4,2,1,5]$;
- The encryption and decryption function (*Enc* and *Dec*): *Enc* (or *Dec*) encrypts (or decrypts) the input sequence and then outputs the encrypted (or decrypted) data.

At the sending end, the authentication matrix Φ_{MAC} is generated from *Gen* to obtain the authenticated measurements y_{MAC} while compressively sampling and the input values of *Gen* is viewed as the key secretly shared between only the encoder and the decoder. The CS-based message authentication code ($CSMAC$) is acquired by extracting the value order of y_{MAC} with the help of *Ord*. At the receiving end, a new message authentication code $CSMAC'$ can be generated from

the reconstructed signal $\tilde{\mathrm{x}}$ in a way similar to the encoder after the same authentication matrix Φ_{MAC} is constructed though using the shared key, and the decoder is able to determine whether $\tilde{\mathrm{x}}$ is tampered by attackers through checking the l_1-norm distance between $CSMAC$ and $CSMAC'$. A threshold value ε is set up in advance. As long as the l_1-norm distance is less than ε, the reconstructed signal is accepted; otherwise, it is regarded to be tampered with.

The threshold value ε is determined by the empirical knowledge, which is related to the model of authentication sampling as well as the type of the signal to be sampled. *Gen* is also used to generate the measurement matrix. *Enc* and *Dec* are used to guarantee the security of $CSMAC$ transmitted from the encoder to the decoder. To achieve one-way property of the authentication sampling, the authentication matrix does not need to yield the RIP condition, conversely, it should break the RIP condition.

III. Privacy-Assured FogCS

The Privacy-Assured FogCS scheme is detailedly introduced in this section, composed of secure data collection in the sensor nodes, data postprocessing in the fog nodes, CS reconstruction and integrity authentication in the central cloud. Data postprocessing is to generate $CSMAC$ from the authenticated measurements and to extract and mask the energy information of the measurements, in which a permutation-diffusion architecture is proposed to hiding the energy information. Security discussion is given in the end.

A. Secure Data Collection

The secure collection process is based on the block CS, which involves three core operations, namely wavelet transform, matrix design, and compressive sampling. Specifically, a color image I with size $N \times N$ is converted from the time domain to the wavelet domain to acquire the transformed image X. The transformed image with size $N \times N$ is divided into l block images with equal size $B \times B$ and then every block image is simultaneously sampled and compressed to acquire measurements Y (i.e., sampling data) using an identical measurement matrix Φ with size $m \times n$, in which $n = B^2$, $l = (N/B)^2$, and $m \geq \mathrm{O}(k \log(n/k))$. To guarantee the integrity of the original color image, some additional measurements Y_{MAC} used for generating $CSMAC$ need to be acquired using an authentication matrix Φ_{MAC} with size $L \times N$.

1) Wavelet Transform: A color image, composed of red-plain image (R-plain image), green-plain image (G-plain image), and blue-plain image (B-plain image), is captured by the complementary metal-oxide-semiconductor (CMOS) sensor in the terminal node. When collecting the data, the discrete wavelet transform (DWT) is used to convert the plain-images from the time domain to the wavelet domain, which is expressed as

$$\begin{cases} X^R = DWT(I^R) \\ X^G = DWT(I^G) \\ X^B = DWT(I^B) \end{cases}, \tag{9}$$

where I^R, I^G, and I^B denote three channel images of the original image I, i.e., R-plain image, G-plain image, and B-plain image, respectively, and X^R, X^G, and X^B denote the corresponding transformed images, i.e., R-transformed image, G-transformed image, and B-transformed image, respectively.

2) Matrix Design: The measurement matrix $\Phi \in R^{m \times n}$ and the authentication matrix $\Phi_{MAC} \in R^{L \times N}$ are constructed by iterating SLMM. A chaotic sequence with length n can be generated as follows:

a. two sequences $\{x_i\}_{i=1}^{2n}$ and $\{y_i\}_{i=1}^{2n}$ are generated under the excitation of the initial values (x_0, y_0);
b. two more random sequences $\{x_i{}'\}_{i=1}^{n}$ and $\{y_i{}'\}_{i=1}^{n}$ are further acquired through discarding the first n numbers of the two sequences;
c. a new sequence $\{q_i\}_{i=1}^{n}$ is generated by computing $\{h_i\}_{i=1}^{n} = \frac{1}{2}(\{x_i{}'\}_{i=1}^{n} + \{y_i{}'\}_{i=1}^{n})$.

$\{q_i\}_{i=1}^{n}$ is scaled down in the interval $(-1, 1)$ to acquire a normal sequence $\{h_i\}_{i=1}^{n}$, i.e., $\{h_i\}_{i=1}^{n} = 2 \times \{q_i\}_{i=1}^{n} - 1$. Finally, $\{h_i\}_{i=1}^{n}$ is used to construct the measurement matrix Φ with size $m \times n$ referring to the CSCMM form. Note that the initial values of CSCMM are viewed as a shared key $k_1 = (x_0, y_0)$ between the encoder and the decoder. Under the excitation of the other key $k_2 = (x_0', y_0')$, a chaotic sequence $\{p_i\}_{i=1}^{N}$ can also be generated in a same way. $\{p_i\}_{i=1}^{N}$ is used to construct the authentication matrix Φ_{MAC} with size $L \times N$ referring to the CSCMM form.

Note that Φ need to be frequently updated by driving SLMM with the different initial values but Φ_{MAC} does not because of its one-way property. Moreover, the row number of Φ needs to satisfy the reconstruction requirement, but the row number of Φ_{MAC} does not. All in all, Φ is used to capture the measurements of having the potential of recovering the original image, but Φ_{MAC} is used to acquire the measurements of leaking nothing about the original image. Apparently, such two measurement matrices controlled by the SLMM greatly reduce the required storage space in comparison with the direct use of the original large-size matrix.

3) Compressive Sampling: For the transformed image, its three channel images are divided into l block images with the equal size $B \times B$. Considering the tradeoff between the calculation speed and the reconstruction effect, the value of B can be set to 16. For example, the transformed image with $N = 256$ will be divided into 256 blocks. Each block is measured by Φ to acquire the measurements as follows:

$$\begin{cases} Y_i^R = \Phi X_i^R \\ Y_i^G = \Phi X_i^G \\ Y_i^B = \Phi X_i^B \end{cases}, \tag{10}$$

where X_i^R, X_i^G, and X_i^B are the i-th R-transformed block image, G-transformed block image, and B-transformed block image, respectively and Y_i^R, Y_i^G, and Y_i^B are the corresponding block measurements. After the above parallel processing of block CS is done, the captured measurements, including $\{Y_i^R\}_{i=1}^{l}$, $\{Y_i^G\}_{i=1}^{l}$, and $\{Y_i^B\}_{i=1}^{l}$, are sent to the fog nodes to improve the confidentiality of sampling data.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2020.3008914, IEEE Transactions on Industrial Informatics

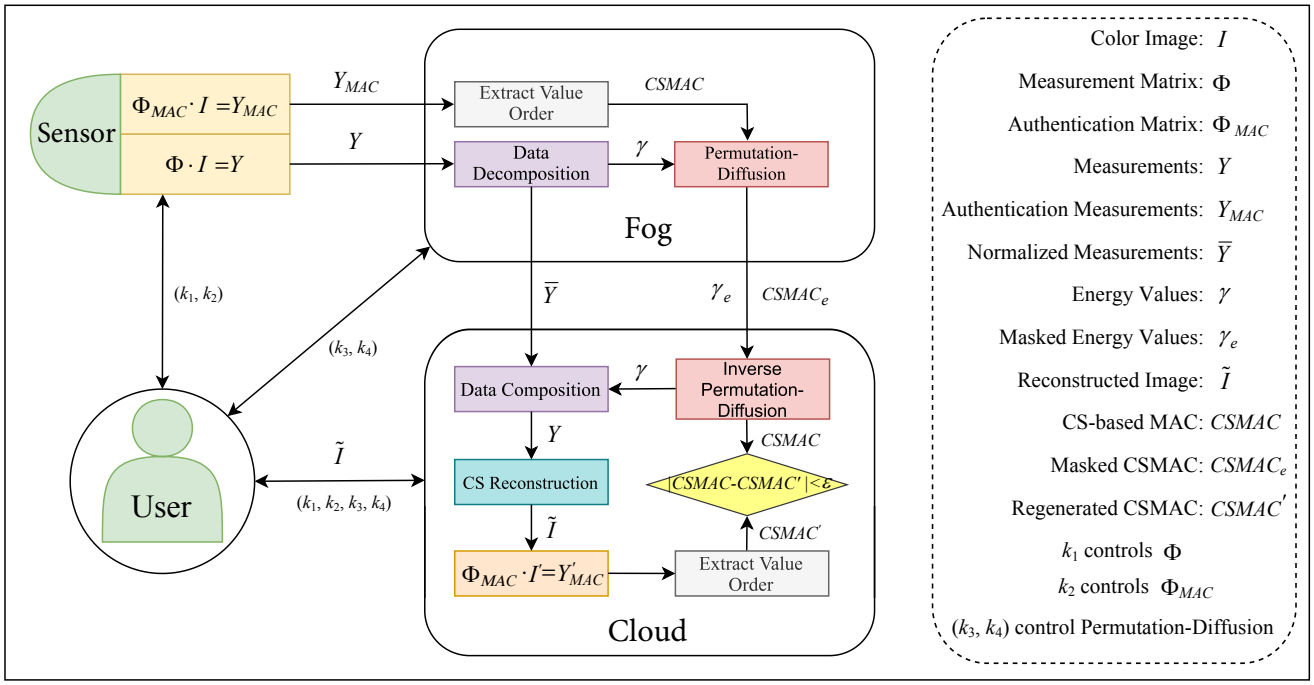


Fig. 3. The sketch of the proposed Privacy-Assured FogCS.

Meanwhile, the transformed image is synchronously measured by the authentication matrix Φ_{MAC} to obtain Y^R_{MAC}, Y^G_{MAC}, and Y^B_{MAC} as follows:

$$\begin{cases} Y^R_{MAC} = \Phi_{MAC} X^R \\ Y^G_{MAC} = \Phi_{MAC} X^G \\ Y^B_{MAC} = \Phi_{MAC} X^B \end{cases}. \tag{11}$$

Y^R_{MAC}, Y^G_{MAC}, and Y^B_{MAC} are also sent to the fog nodes.

B. Data postprocessing in the fog nodes

Considering that the confidentiality of the measurements is not enough, the energy information of the measurements, having the risk of revealing the valuable information about the original image, is masked in the fog nodes to release the burden of the terminal sensors. Besides, it is also finished in the fog nodes to generate $CSMAC$ from the authenticated measurements.

1) Extracting the value order: In the fog nodes, Y^R_{MAC}, Y^G_{MAC}, and Y^B_{MAC} are used to generate MAC for verifying the integrity of the reconstructed image. The corresponding $CSMAC^R$, $CSMAC^G$, and $CSMAC^B$ can be acquired as follows:

$$\begin{cases} CSMAC^R = Ord(Y^R_{MAC}) \\ CSMAC^G = Ord(Y^G_{MAC}) \\ CSMAC^B = Ord(Y^B_{MAC}) \end{cases}, \tag{12}$$

where $Ord(\cdot)$ denotes the value order extraction operation. To avoid tampering attacks, $CSMAC^R$, $CSMAC^G$, and $CSMAC^B$ need to be further encrypted using a permutation-diffusion algorithm, which is based on the following chaotic systems in this paper.

2) Decomposing the Measurements: Concealing the energy information of measurements is proved to enable the Shannon's perfect secrecy [34], [35]. So the captured measurements are normalized to guarantee the security of data transmitted from fog nodes to the data center. The normalization operation makes it nearly impossible for an attacker to acquire any useful information about the original image from the normalized measurements. The normalization operation is described by

$$\begin{cases} \bar{Y}^R_i = Y^R_i / \gamma^R_i \\ \bar{Y}^G_i = Y^G_i / \gamma^G_i \\ \bar{Y}^B_i = Y^B_i / \gamma^B_i \end{cases}, \tag{13}$$

where $\gamma^R_i = \left\|Y^R_i\right\|_2^2$, $\gamma^B_i = \left\|Y^B_i\right\|_2^2$ and $\gamma^G_i = \left\|Y^G_i\right\|_2^2$ represent the energy value of Y^R_i, Y^B_i and Y^G_i, respectively, and $\bar{Y}^R_i$, $\bar{Y}^B_i$ and $\bar{Y}^G_i$ are the corresponding normalized measurements. The normalized measurements is proved to satisfying the definition of the Shannon's perfect secrecy so as to directly transmitted to the cloud for storage and processing.

3) Masking the Energy Values: The energy values are sensitive data because they have the potential of leaking some valuable information about the original image. Guaranteeing the high confidentiality of the energy values is of crucial importance in the proposed scheme. A permutation-diffusion strategy is detailedly designed to mask these sensitive values. The diffusion and permutation are two essential properties in a cryptosystem. The diffusion operation changes the statistical properties of the image data to a large extent. The absence of diffusion will lead to a high probability that an adversary will launch a statistical attack successfully. The permutation operation makes the statistics redundancy of the plaintext dissipated in the statistics of ciphertext, which often matches with the diffusion operation in some way.

The energy values are partitioned into the fractional part and the integer part that are then masked with two different encryption approaches Assume that $\{\alpha_i^j\}_{i=1}^l$ and $\{\beta_i^j\}_{i=1}^l$ denote the fractional part and the integer part of the energy values $\{\gamma_i^j\}_{i=1}^l (j = R, G, B)$, respectively.

Chaotic encryption method is used to mask the fractional part $\{\alpha_i^j\}_{i=1}^l (j = R, G, B)$. Three random decimal sequences, i.e., $\{z_i^1\}_{i=1}^l$, $\{z_i^2\}_{i=1}^l$, and $\{z_i^3\}_{i=1}^l$, are generated through iterating the SLMM (or other chaotic maps), whose initial values are viewed as the key k_3 secretly shared with the decoder. Every value of the fractional part is erratically changed by

$$\begin{cases} \{\bar{\alpha}_i^R\}_{i=1}^l = \{\alpha_i^R\}_{i=1}^l \oplus \{z_i^1\}_{i=1}^l \\ \{\bar{\alpha}_i^G\}_{i=1}^l = \{\alpha_i^G\}_{i=1}^l \oplus \{z_i^2\}_{i=1}^l \\ \{\bar{\alpha}_i^B\}_{i=1}^l = \{\alpha_i^B\}_{i=1}^l \oplus \{z_i^3\}_{i=1}^l \end{cases}, \tag{14}$$

where $\{\bar{\alpha}_i^R\}_{i=1}^l$, $\{\bar{\alpha}_i^B\}_{i=1}^l$, and $\{\bar{\alpha}_i^G\}_{i=1}^l$ are the encrypted data of the fractional part and '$\oplus$' denotes XOR operation.

Prior to masking the integer part, we investigate a 10-digit binary number. Generally, the higher bit contributes more importance and more information than the lower bit. With respect to the i-th bit from right to left, the percentage P(i) of the total information occupied by the i-th bit can be calculated as

$$P(i) = \frac{2^i}{\sum_{j=0}^{9} 2^j}, \tag{15}$$

where i=0,1,...,9. According to the above formula, the information of the higher 5-bits accounts for 96.9697% of the total information. In other words, the majority of information is concentrated in the higher 5-bits for a 10-digit binary number. Based on the above result, we carry out encryption operation to the more significant 5-bits (MSB-5) of the integer part, which is a partial encryption method for the better resource usage compared with the full encryption.

To effectively implement the MSB-5 encryption operation, some proprocessing operations need to be done for the integer part $\{\beta_i^j\}_{i=1}^l (j = R, G, B)$. There are three possible cases for the integer part. The first case is that, if an integer β is no greater than 100, a proprocessing operation is performed by $\beta' = \sum_{i=0}^{9} 2^i - \beta$. Such a proprocessing operation can move some 1s in the lower bits into the higher bits and accordingly the MSB-5 encryption become more effective. Let the proprocessing result be $\beta' = \sum_{i=0}^{9} 2^i - \beta$, whose value range is $[923, 1023]$ in the first case. The second case is that β is greater than 100 but not greater than 992 and then $\sum_{i=0}^{9} 2^i - \beta$ is executed to guarantee $\beta' \in [31, 923)$. The third situation is that β is greater than 992. To distinguish the former two cases and ensure that the whole proprocessing operation reversible, the proprocessing operation is set to $\beta' = \beta + 31$ such that $\beta' > 1023$.

After the above proprocessing operation is finished, the MSB-5 encryption is performed, in which the higher 5 bits are changed by using the cycle shift operation and the lower 5 bits remain unchanged. Note that for the third case, in which β' usually contains 11 bits and the highest bit is 1, the higher 5 bits are selected from the 2nd to the 6th bit starting with the left. Based on the statistics of the integer part of the measurements when the block size is 16×16, the majority of integers belong to the second case and the other two cases account for a very small proportion.

In essence, the MSB-5 encryption method is also based on a chaotic system. Firstly, three chaotic sequences with the length l, i.e., $\{u_i^1\}_{i=1}^l$, $\{u_i^2\}_{i=1}^l$, and $\{u_i^3\}_{i=1}^l$, can be generated by iterating the SLMM, whose initial values are viewed as the key k_4. Then, three generated sequences are projected into three integer sequences respectively, i.e., $\{v_i^1\}_{i=1}^l$, $\{v_i^2\}_{i=1}^l$, and $\{v_i^3\}_{i=1}^l$, whose element is between 1 and 4 by

$$\begin{cases} \{v_i^1\}_{i=1}^l = floor\left(\{u_i^1\}_{i=1}^l \times 10^{13}\right) \bmod 5 + 1 \\ \{v_i^2\}_{i=1}^l = floor\left(\{u_i^2\}_{i=1}^l \times 10^{13}\right) \bmod 5 + 1 \\ \{v_i^3\}_{i=1}^l = floor\left(\{u_i^3\}_{i=1}^l \times 10^{13}\right) \bmod 5 + 1 \end{cases}, \tag{16}$$

where $floor(\cdot)$ denotes the round-off function. Finally, the loop shift operation is performed in the bit level to obfuscate the integer, as described by

$$\begin{cases} \{\bar{\beta}_i^R\}_{i=1}^l = Cycle\_shift\left(\{\beta_i^R\}_{i=1}^l, \{v_i^1\}_{i=1}^l\right) \\ \{\bar{\beta}_i^G\}_{i=1}^l = Cycle\_shift\left(\{\beta_i^G\}_{i=1}^l, \{v_i^2\}_{i=1}^l\right) \\ \{\bar{\beta}_i^B\}_{i=1}^l = Cycle\_shift\left(\{\beta_i^B\}_{i=1}^l, \{v_i^3\}_{i=1}^l\right) \end{cases}, \tag{17}$$

where $Cycle\_shift(\cdot,\cdot)$ represents the loop shift function, which aims at moving the higher 5 bits toward the right. For example, $Cycle\_shift(1000101010, 1) = 1100001010$, $Cycle\_shift(1000101010, 2) = 0110001010$. Performing such a function in the bit level acquires both the permutation effect and the diffusion effect.

It can be seen from the above that masking the fractional part is a diffusion operation and masking the integer part is a permutation-diffusion operation. Overall, the encryption approach to the energy values of CS measurements is a permutation-diffusion architecture based on the chaotic system. The masked results $\{\bar{\alpha}_i^j\}_{i=1}^l$ and $\{\bar{\beta}_i^j\}_{i=1}^l (j = R, G, B)$ are delivered to the cloud over the public channels.

C. Reconstruction and authentication in the cloud

CS reconstruction and integrity authentication operations are performed in the cloud. The verified reconstructed image is sent to the end-users.

1) Reconstruction: The decryption process is the inverse operation of the encryption process. Firstly, the anti-permutation-diffusion operation and the composition operation are successively carried out to acquire the measurements, i.e., Y^R, Y^G, and Y^B. Then, the CS reconstruction algorithm is implemented to obtain three transformed images, i.e., $\tilde{X}^R$, $\tilde{X}^G$, and $\tilde{X}^B$. Finally, the inverse wavelet transform operation is employed to acquire three channel images of the recovered image, including R-reconstructed image $\tilde{I}^R$, G-reconstructed image $\tilde{I}^G$, and B-reconstructed image $\tilde{I}^B$.

2) Authentication: After the transformed images $\tilde{X}^R$, $\tilde{X}^G$, and $\tilde{X}^B$ are acquired by the CS reconstruction algorithm, the integrity verification operation is performed to check whether the reconstructed image has been tampered with. Specifically,

the same authentication matrix Φ_{MAC} is generated by iterating SLMM in the data center (cloud). $\tilde{Y}^R_{MAC}$, $\tilde{Y}^G_{MAC}$, and $\tilde{Y}^B_{MAC}$ are obtained from $\tilde{X}^R$, $\tilde{X}^G$, and $\tilde{X}^B$ as follows:

$$\begin{cases} \tilde{Y}^R_{MAC} = \Phi_{MAC}\tilde{X}^R \\ \tilde{Y}^G_{MAC} = \Phi_{MAC}\tilde{X}^G \\ \tilde{Y}^B_{MAC} = \Phi_{MAC}\tilde{X}^B \end{cases}. \tag{18}$$

According to a way similar to the decoder, $CSMAC'^R$, $CSMAC'^G$ and $CSMAC'^B$ are extracted from $\tilde{Y}^R_{MAC}$, $\tilde{Y}^G_{MAC}$ and $\tilde{Y}^B_{MAC}$, respectively. It is easy to check the integrity of the received image by checking whether the l_1-norm distances between $CSMAC'^R$, $CSMAC'^G$, $CSMAC'^B$ and $CSMAC^R$, $CSMAC^G$, $CSMAC^B$ are all less than a constant ε or not, as described by

$$\begin{cases} \left\| CSMAC'^R - CSMAC^R \right\| < \varepsilon \\ \left\| CSMAC'^G - CSMAC^G \right\| < \varepsilon \\ \left\| CSMAC'^B - CSMAC^B \right\| < \varepsilon \end{cases}. \tag{19}$$

If (19) holds, the received image is said to be true or acceptable; otherwise, it is viewed as the tampered one.

D. Security discussion

The normalized measurements, whose energy information is hidden, have been proved to achieve the requirement of Shannon's perfect secrecy mathematically. Based on this research result, fog computing capability is used to extract and mask the energy information of the measurements for releasing the burden of the terminal sensors and enhancing the encryption efficiency.

In the proposed FogCS scheme, the confidentiality and integrity of the original image are provided by the CS framework from the terminal sensors to fog nodes. The confidentiality of the energy values of measurements depends on both the chaotic encryption and the proposed MSB-5 encryption from the fog nodes to the cloud servers. The normalized measurements is directly transmitted to the cloud servers. CS-based encryption and authentication operations are embedded in the process of compressive sampling to provide some degree of security guarantee without the additional cryptosystems. The volume of the energy values of the measurements is far less than that of the measurements. Masking the energy values of the measurements is a more efficient encryption approach than masking the measurements. Therefore, the confidentiality of the measurements depends on the CS-based encryption in the terminal sensors and the confidentiality of the energy values depends on the proposed encryption in the fog nodes. Besides, the integrity of the original image is guaranteed by the CS-based integrity authentication scheme and the normalized measurements are perfectly secure.

IV. FPGA DESIGN

The DE2-70 FPGA development board is the hardware platform in our experiments. The block diagram design of the hardware system is presented in Fig. 4. The components of the transmitter are the CMOS sensor, the sensor configuration, the format conversation, the buffer controller, the video graphics array (VGA), the synchronous dynamic random access memory (SDRAM), the synchronous static random access memory (SSRAM), the permutation-diffusion module, and the LCD display chip. The receiver is composed by the buffer controller, the VGA, the anti-permutation-diffusion module, and the LCD display chip. The functions of the these components are as follows:

a. CMOS sensor: transform the optical signal into an electrical signal that is converted into a digital signal by A/D chip;
b. Sensor configuration: adjust the output format, the output gain, and the exposure time of the CMOS images;
c. Format conversation: add color filter array based on the black and white image sensor to achieve color imaging;
d. VGA: image output module for displaying the final encryption result;
e. Buffer controller: use the data cache for the running space of the encryption program;
f. SDRAM: employ the data cache for image acquisition;
g. SSRAM: utilize the data cache for the encrypted image.

V. SIMULATION ANALYSES

Simulation experiments were carried out using MATLAB 2015b software on a computer with AMD A6-3420M and 2GB RAM. Two images ('Pepper' and 'Tiger') with size 256×256 are chosen as the test objects. Tampering analysis, key sensitivity analysis, compression performance analysis, and reconstruction time analysis are presented in detail.

TABLE I. The l_1-Norm Distance Between $CSMAC$ and $CSMAC'$ of 'Pepper'

Image Type	Original 'Pepper'	Noisy 'Pepper'	Tampered 'Pepper'
R	12.4140	15.4140	21.9180
G	13.9941	16.0695	25.3555
B	14.5918	15.6248	22.4961
RGB	13.6670	15.7028	23.2559

TABLE II. The l_1-Norm Distance Between $CSMAC$ and $CSMAC'$ of 'Tiger'

Image Type	Original 'Tiger'	Noisy 'Tiger'	Tampered 'Tiger'
R	19.0605	26.3578	37.6094
G	19.2266	24.7054	41.7754
B	22.1406	28.2173	28.1016
RGB	20.1426	26.4268	35.8291

A. Tampering analysis

The tampered image is likely to not only lose some significant information but also distort the original information. Therefore, the design of the data integrity authentication mechanism is indispensable in the communication systems. Considering that CS is a lossy compression technology and the reconstructed image is usually covered by some levels of noise in the practical applications, a noise-tolerant but tamper-resistant integrity MAC is generated through the CS framework in the proposed FogCS scheme. Depending on a large number of training tests, the threshold value ε can be set in advance.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2020.3008914, IEEE Transactions on Industrial Informatics

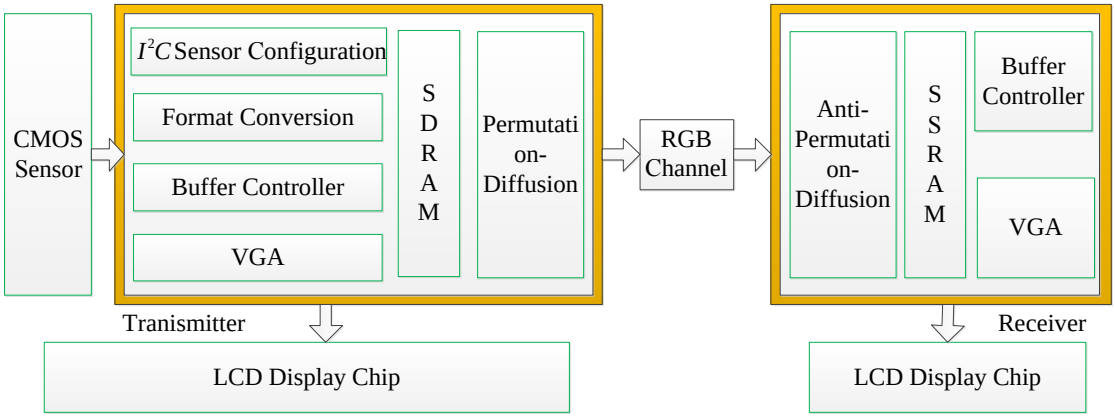


Fig. 4. The block diagram of the hardware system.

In this experiment, we considers 'Pepper' and 'Tiger' under three environments, i.e., an ideal environment, an noisy environment, and an attack environment. The original 'Pepper' and the corresponding three channel images are shown in Figs. 5(a)-(d), respectively. The noisy 'Pepper' and the corresponding three channel images are shown in Figs. 5(e)-(h), respectively. The tampered 'Pepper' and the corresponding three channel images are shown in Figs. 5(i)-(l), respectively. The original 'Tiger' and the corresponding three channel images are shown in Figs. 5(m)-(p), respectively. The noisy 'Tiger' and the corresponding three channel images are shown in Figs. 5(q)-(t), respectively. The tampered 'Tiger' and the corresponding three channel images are shown in Figs. 5(u)-(x), respectively. Tables I and II give the l_1-norm distances between $CSMAC$ and $CSMAC'$ for 'Pepper' and 'Tiger', respectively. It can be seen that the l_1-norm distances under an ideal environment are clearly smaller than that under a noisy environment and under an attack environment. Therefore, the data integrity of the received image can be easily verified by setting up a proper threshold value ε.

B. Key sensitivity analysis

An excellent cryptosystem must be extremely sensitive to the key, i.e., a tiny change in the key can cause a huge change for the ciphertext. To quantitatively describe the difference between the original image and the reconstructed one, the mean square error (MSE) is defined by

$$MSE = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N}[R(i,j) - O(i,j)]^2}{N \times N}, \tag{20}$$

where $R(i,j)$ and $O(i,j)$ are two corresponding pixel values of the reconstructed image and the original image, respectively, and N denotes the size of the reconstructed image and the original image.

Obviously, three keys k_1, k_3, k_4 are used to perform the CS-based encryption operation, mask the fractional part of the energy values, and mask the integer part of the energy values, respectively. To reveal the key sensitivity, the correct key and the false key are used to decode the cipher image. The deviation between the correct key and the false key is only 10^{-16}. Figs. 6(a)-(d) and 6(e)-(h) represent the reconstructed 'Pepper' and 'Tiger' images with different keys used. When the false key $k_4 + 10^{-16}$ is used, the indistinguishability of the reconstructed images owes to that the data distortion in the fractional part can barely the measurements. It is not hard to be concluded that both the CS-based encryption algorithm and the MSB-5 encryption algorithm have a strong sensitivity to the key.

TABLE III. The $PSNR$ (dB) of 'Pepper'

CR	R-'Pepper'	G-'Pepper'	B-'Pepper'	RGB-'Pepper'
0.3	23.8131	24.2915	25.1258	24.4101
0.4	27.3409	27.5170	28.4352	27.7644
0.5	31.1757	31.2196	32.1073	31.5009
0.6	35.1081	35.2748	36.1932	35.5254
0.7	39.8702	40.7130	40.6348	40.4060
0.8	46.7057	47.2375	47.3858	47.1097
0.9	54.9806	56.7339	54.9822	55.5656

C. Compression performance analysis

The relation between the decoded image quality and the compression ratios (CR) is revealed here. The peak signal-to-noise ratio ($PSNR$) is a widely used to evaluate the decoded image quality, which is defined by

$$PSNR = 10\log\frac{255^2}{\frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}[R(i,j) - O(i,j)]^2}, \tag{21}$$

Evidently, the smaller the MSE is, the larger the $PSNR$ is. The $PSNR$ of the 'Pepper' and 'Tiger' with different compression rates (30%, 40%, 50%, 60%, 70%, 80%, and 90%) are given in Tables III and IV, respectively. The corresponding trend graphs are further depicted in Figs. 7(a) and 7(b). It can be clearly observed that the compression ability in the proposed scheme is acceptable and flexible.

D. Reconstruction time analysis

The real-time multimedia services have become increasingly significant. How to acquire the real-time property is a challenging issue in the cloud-based applications, especially for

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2020.3008914, IEEE Transactions on Industrial Informatics

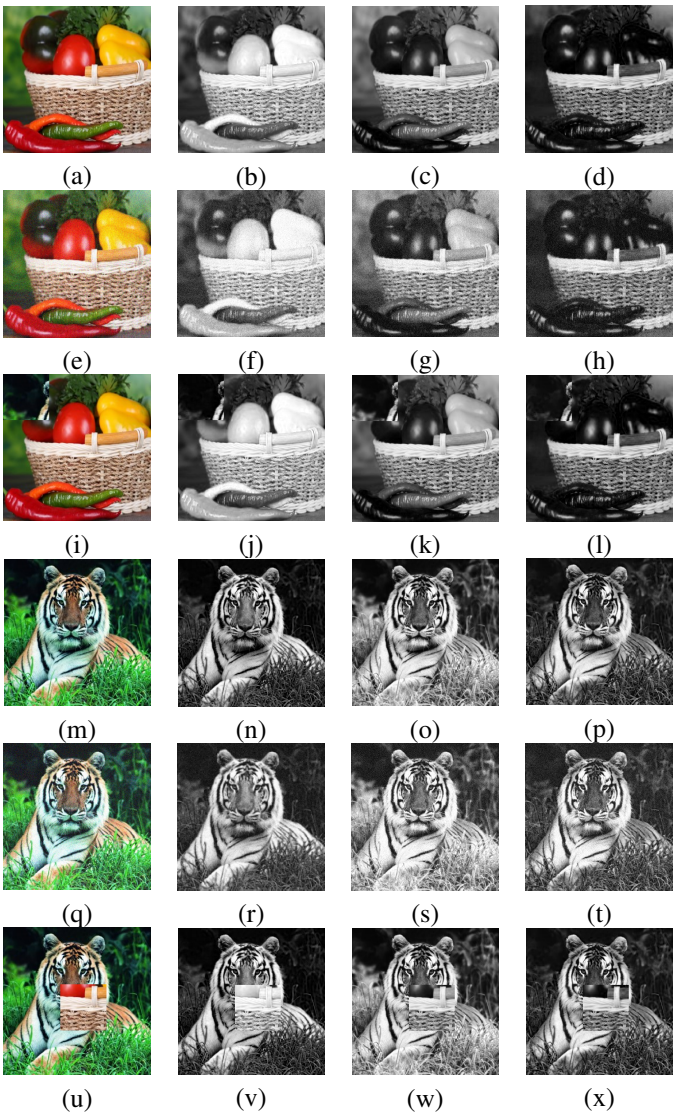


Fig. 5. Three cases of data distortion. (a) 'Pepper'; (b) R-'Pepper'; (c) G-'Pepper'; (d) B-'Pepper'; (e) noisy 'Pepper'; (f) noisy R-'Pepper'; (g) noisy G-'Pepper'; (h) noisy B-'Pepper'; (i) tampered 'Pepper'; (j) tampered R-'Pepper'; (k) tampered G-'Pepper'; (l) tampered B-'Pepper'; (m) 'Tiger'; (n) R-'Tiger'; (o) G-'Tiger'; (p) B-'Tiger'; (q) noisy 'Tiger'; (r) noisy R-'Tiger'; (s) noisy G-'Tiger'; (t) noisy B-'Tiger'; (u) tampered 'Tiger'; (v) tampered R-'Tiger'; (w) tampered G-'Tiger'; (x) tampered B-'Tiger'.

TABLE IV. The $PSNR$ (dB) of 'Tiger'

CR	R-'Tiger'	G-'Tiger'	B-'Tiger'	RGB-'Tiger'
0.3	18.9474	18.7868	20.1903	19.3082
0.4	21.5786	21.3829	22.4974	21.8196
0.5	24.5584	24.3020	25.1534	24.6713
0.6	27.2907	27.6428	27.9536	27.6290
0.7	30.7962	31.3439	31.4160	31.1854
0.8	35.9980	36.2167	36.1291	36.1146
0.9	42.6780	43.3636	42.6944	42.9120

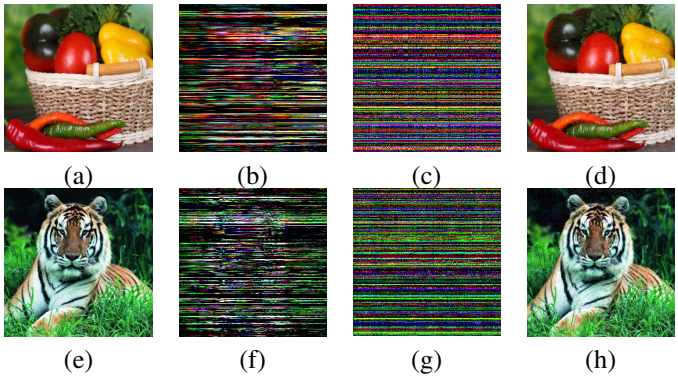


Fig. 6. The reconstructed results using the different keys. (a) 'Pepper', the correct key, MSE=57; (b) 'Pepper', k_1+10^{-16}, MSE=79438; (c) 'Pepper', k_3+10^{-16}, MSE=75431; (d) 'Pepper', k_4+10^{-16}, MSE=60; (e) 'Tiger', the correct key, MSE=139; (f) 'Tiger', k_1+10^{-16}, MSE=65664; (g) 'Tiger', k_3+10^{-16}, MSE=75590; (h) 'Tiger', k_4+10^{-16}, MSE=141.

the big images. To reduce the reconstruction time as much as possible, the block CS is employed to meet the real-time requirement. In essence, the block CS is a parallel processing model. Specifically, a big image is divided into several image blocks with the equal size and then kinds of operations are done for the image blocks, which can dramatically decrease the reconstruction time compared to the normal CS framework. Aiming at the industrial big image, the proposed FogCS scheme works under such a parallel processing model. Fig. 8 shows the reconstruction time of the block CS and the normal CS for 'Pepper' and 'Tiger'. Obviously, the proposed scheme can provide a better real-time multimedia service.

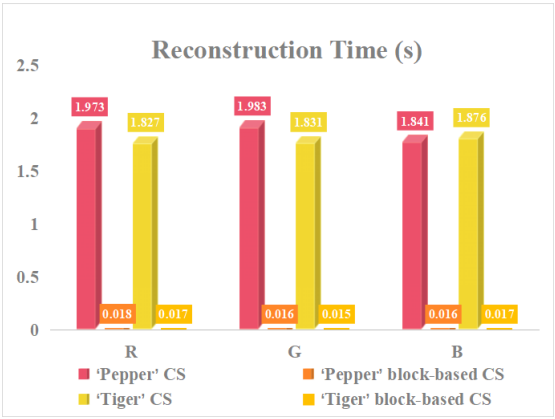


Fig. 8. Reconstruction time of CS and block-based CS.

VI. Conclusion

In this paper, a Privacy-Assured FogCS scheme is proposed for secure industrial big image data processing with the help of fog computing. The issues, including malicious data tamper, weak data confidentiality of the measurements, large storage space requirement of the measurement matrix, and long run time of CS reconstruction, are solved in the proposed scheme.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2020.3008914, IEEE Transactions on Industrial Informatics

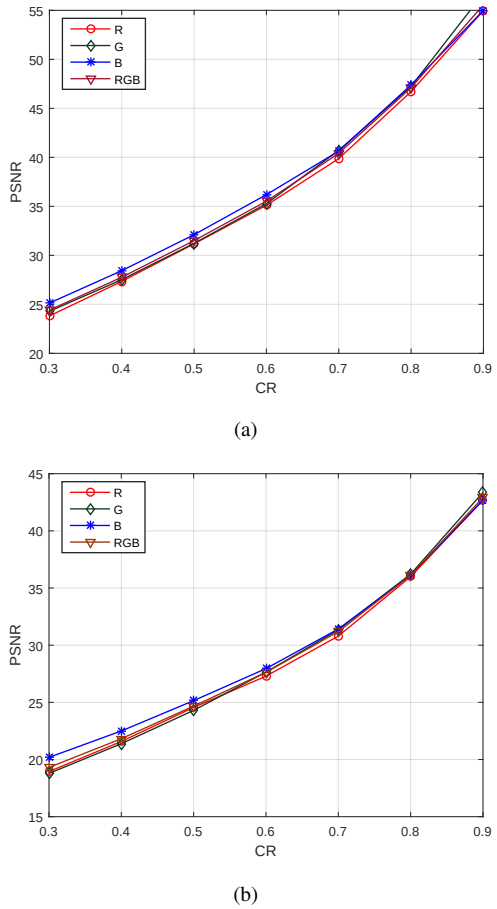


Fig. 7. Compression rate versus image service quality for (a) 'Pepper' image; (b) 'Tiger' image.

Specifically, the CS-based data integrity authentication mechanism is employed to check whether the reconstructed image has been tampered with. The proposed permutation-diffusion architecture is used to guarantee the confidentiality of the energy values of measurements in the process of transmission, in which a chaos-based partial encryption is designed to save resources. The CSCMM is constructed through only very few independent random variables to solve the problem of large storage space requirement, caused with the use of the common measurement matrix. The block CS is used to address the problem of long run time. The feasibility and efficiency of the proposed scheme is proven by the tampering analysis, the key sensitivity analysis, the compression performance analysis, and the reconstruction time analysis.

REFERENCES

[1] Y. Demchenko, C. De Laat, and P. Membrey, "Defining architecture components of the big data ecosystem," in *Proc. Int. Conf. Collaboration Techno. Syst.*, 2014, pp. 104–112.

[2] R. Bellazzi, "Big data and biomedical informatics: a challenging opportunity," *Yearbook of medical informatics*, vol. 23, no. 01, pp. 08–13, 2014.

[3] K. Bilal, S. U. R. Malik, S. U. Khan, and A. Y. Zomaya, "Trends and challenges in cloud datacenters," *IEEE Cloud Comput.*, vol. 1, no. 1, pp. 10–20, 2014.

[4] B. P. Rimal, E. Choi, and I. Lumb, "A taxonomy and survey of cloud computing systems," in *Proc. Fifth Int. Joint Conf. INC IMS IDC*, 2009, pp. 44–51.

[5] Z. Li, Z. Yang, and S. Xie, "Computing resource trading for edge-cloud-assisted Internet of things," *IEEE Trans. Indust. Infor.*, vol. 15, no. 6, pp. 3661–3669, 2019.

[6] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *Proc. First Edition MCC Workshop Mobile Cloud Comput.*, 2012, pp. 13–16.

[7] D. A. Chekired, L. Khoukhi, and H. T. Mouftah, "Industrial IoT data scheduling based on hierarchical fog computing: A key for enabling smart factory," *IEEE Trans. Indust. Infor.*, vol. 14, no. 10, pp. 4590–4602, 2018.

[8] M. Satyanarayanan, "The emergence of edge computing," *Computer*, vol. 50, no. 1, pp. 30–39, 2017.

[9] 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, 2006.

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

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

[12] S. Li, L. D. Xu, and X. Wang, "Compressed sensing signal and data acquisition in wireless sensor networks and internet of things," *IEEE Trans. Indust. Infor.*, vol. 9, no. 4, pp. 2177–2186, 2013.

[13] Y. Rachlin and D. Baron, "The secrecy of compressed sensing measurements," in *Proc. 46th Ann. Allerton Conf. Comm. Contr. Comput.*, 2008, pp. 813–817.

[14] 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, 2015.

[15] L. Y. Zhang, K. W. Wong, Y. Zhang, and J. Zhou, "Bi-level protected compressive sampling," *IEEE Trans. Multimedia*, vol. 18, no. 9, pp. 1720–1732, 2016.

[16] W. Xue, C. Luo, G. Lan, R. K. Rana, W. Hu, and A. Seneviratne, "Kryptein: a compressive-sensing-based encryption scheme for the internet of things," in *Proc. 16th ACM/IEEE Int. Conf. Inf. Process. Sensor Networks (IPSN)*, 2017, pp. 169–180.

[17] Y. Zhang, Q. He, Y. Xiang, L. Y. Zhang, B. Liu, J. Chen, and Y. Xie, "Low-cost and confidentiality-preserving data acquisition for internet of multimedia things," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3442–3451, 2018.

[18] R. Tan, S.-Y. Chiu, H. H. Nguyen, D. K. Yau, and D. Jung, "A joint data compression and encryption approach for wireless energy auditing networks," *ACM Trans. Sensor Networks (TOSN)*, vol. 13, no. 2, p. 9, 2017.

[19] R. Dautov and G. R. Tsouri, "Securing while sampling in wireless body area networks with application to electrocardiography," *IEEE J. Biomedical Health Inf.*, vol. 20, no. 1, pp. 135–142, 2016.

[20] H. Peng, Y. Tian, J. Kurths, L. Li, Y. Yang, and D. Wang, "Secure and energy-efficient data transmission system based on chaotic compressive sensing in body-to-body networks," *IEEE Trans. Biomedical Circ. Syst.*, vol. 11, no. 3, pp. 558–573, 2017.

[21] T. Wu and C. Ruland, "Authenticated compressive sensing imaging," in *Proc. Int. Symp. Networks Comput. Commun. (ISNCC)*, 2017, pp. 1–6.

[22] ——, "An improved authenticated compressive sensing imaging," in *Proc. 12th Int. Conf. Semant. Comput. (ICSC)*. IEEE, 2018, pp. 164–171.

[23] Y. Wang, W. Meng, W. Li, J. Li, W.-X. Liu, and Y. Xiang, "A fog-based privacy-preserving approach for distributed signature-based intrusion detection," *J. Parallel Distrib. Comput.*, vol. 122, pp. 26 – 35, 2018.

[24] J. Wu, M. Dong, K. Ota, J. Li, and Z. Guan, "FCSS: Fog-computing-based content-aware filtering for security services in information-centric social networks," *IEEE Trans. Emerg. Top. Comput.*, vol. 7, no. 4, pp. 553–564, 2019.

[25] 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, 2010.

[26] M. Frunzete, L. Yu, J. P. Barbot, and A. Vlad, "Compressive sensing matrix designed by tent map, for secure data transmission," in *Signal Processing Algorithms, Architectures, Arrangements, and Applications Conference*, 2011, pp. 1–6.

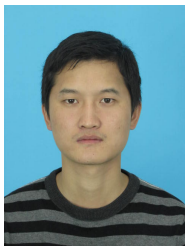
[27] H. Gan, Z. Li, J. Li, X. Wang, and Z. Cheng, "Compressive sensing using chaotic sequence based on Chebyshev map," *Nonlinear Dyn.*, vol. 78, no. 4, pp. 2429–2438, 2014.

[28] Z. Hua, Y. Zhou, C.-M. Pun, and C. P. Chen, "2D sine logistic modulation map for image encryption," *Inf. Sci.*, vol. 297, pp. 80–94, 2015.
[29] L. Gan, "Block compressed sensing of natural images," in *Proc. 15th Int. Conf. Digital Signal Process.*, 1-4 July 2007, Cardiff, United Kingdom, pp. 403–406.
[30] J. E. Fowler, S. Mun, E. W. Tramel *et al.*, "Block-based compressed sensing of images and video," *Foundations Trends Signal Process.*, vol. 4, no. 4, pp. 297–416, 2012.
[31] A. Kulkarni, A. Jafari, C. Shea, and T. Mohsenin, "CS-based secured big data processing on FPGA," in *Proc. IEEE 24th Annual Int. Symp. Field-Programmable Custom Comput. Machines (FCCM)*, 2016, Washington, DC, USA, p. 16247505.
[32] R. Baraniuk, M. Davenport, R. DeVore, and M. Wakin, "A simple proof of the restricted isometry property for random matrices," *Constr. Approx.*, vol. 28, no. 3, pp. 253–263, Dec 2008.
[33] C. Pak and L. Huang, "A new color image encryption using combination of the 1D chaotic map," *Signal Process.*, vol. 138, pp. 129–137, 2017.
[34] 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, 2015.
[35] Y. Zhang, Y. Xiang, L. Y. Zhang, Y. Rong, and S. Guo, "Secure wireless communications based on compressive sensing: a survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1093–1111, 2018.

Yushu Zhang (M'17) received the Ph.D. degree from the College of Computer Science, Chongqing University, Chongqing, China, in Dec. 2014. He held various research positions at the City University of Hong Kong, Southwest University, University of Macau, and Deakin University. He is now a Professor with College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, China. His research interests include multimedia security, artificial intelligence, cloud computing security, big data security, Internet of Things security, and blockchain. He is an Editor of Signal Processing.

Ping Wang is currently pursuing the Ph.D. degree in the College of Cybersecurity, Sichuan University, Chengdu, China. His research interests include multimedia security, cloud computing security, Internet of Things security security, and artificial intelligence security.

Hui Huang is currently pursuing the Ph.D. degree in the College of Computer Science, Chongqing University, Chongqing, China. His research interests include multimedia security, cloud computing security, big data security, Internet of Things security, and compressive sensing security.



Youwen Zhu received his B.E. degree and Ph.D. degree in Computer Science from University of Science and Technology of China, Hefei, China, in 2007 and 2012, respectively. From 2012 to 2014, he is a JSPS postdoc in Kyushu University, Japan. He is currently an Associate Professor at the College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, China. He has published more than 40 papers in refereed international conferences and journals, and has served as program committee member in several international conferences. His research interests include identity authentication, information security and data privacy.

Di Xiao (M'10) received the B.S. degree from Sichuan University, Chengdu, China, and the M.S. and Ph.D. degrees from Chongqing University, Chongqing, China. From 2006 to 2008, he accomplished the postdoctoral research in Chongqing University. From 2008 to 2009, he visited the Department of Computer Science, New Jersey Institute of Technology, USA, as a visiting scholar. In 2019, he visited the School of Information Technology, Deakin University, Australia, as a senior visiting fellow. He is currently a Full Professor at the College of Computer Science, Chongqing University, Chongqing, China. His research interests cover signal processing in encrypted domain, compressive sensing, security and privacy in Internet of things, etc. So far, he has published more than 90 academic journal papers and be selected as "2014-2019 Elsevier Most Cited Chinese Researchers".

Yong Xiang (SM'12) received the Ph.D. degree in the Electrical and Electronic Engineering from The University of Melbourne, Australia. He is a Professor at the School of Information Technology, Deakin University, Australia. His research interests include information security and privacy, signal and image processing, data analytics and machine intelligence, Internet of Things, and blockchain. He has published 5 monographs, over 150 refereed journal articles, and numerous conference papers in these areas. He is the Senior Area Editor of IEEE Signal Processing Letters and the Associate Editor of IEEE Communications Surveys and Tutorials. He has served as Honorary Chair, General Chair, Program Chair, TPC Chair, Symposium Chair, and Track Chair for a number of international conferences.