IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 16, 2022, accepted February 10, 2022, date of publication February 14, 2022, date of current version February 18, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3151398

Privacy-Enhanced and Verifiable Compressed Sensing Reconstruction for Medical Image Processing on the Cloud

XIN SUN[1], CHENGLIANG TIAN[1,2], WEIZHONG TIAN[3], AND YAN ZHANG[4]

[1]College of Computer Science and Technology, Qingdao University, Qingdao 266071, China
[2]Business School, Qingdao University, Qingdao 266071, China
[3]College of Big Data and Internet, Shenzhen Technology University, Shenzhen, Guangdong 518118, China
[4]College of Electromechanical Engineering, Qingdao University of Science and Technology, Qingdao 266061, China

Corresponding author: Chengliang Tian (tcl0815@gmail.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61702294, and in part by the National Development Foundation of Cryptography under Grant MMJJ20170126.

ABSTRACT The well-known compressed sensing reconstruction ($\mathcal{CSR}$) uses the sparse characteristics of the signal to obtain discrete samples with the compression (*i.e.* measurement) algorithm, and then perfectly reconstructs the signal through the reconstruction algorithm. Benefiting from the storage savings, the $\mathcal{CSR}$ has been widely used in the field of large-scale image processing. However, the reconstruction process is computationally overloaded for resource-constrained clients. Therefore, designing a cloud-aided $\mathcal{CSR}$ algorithm becomes a hot topic. In this paper, we investigate the existing secure $\mathcal{CSR}$ algorithms within a cloud environment and propose a new privacy-enhanced and verifiable $\mathcal{CSR}$ outsourcing algorithm for online medical image processing services. Compared with previous work, our new design can efficiently achieve more extensive security. Precisely, (1) our algorithm realizes the privacy preservation of the original image, as well as the input/output information of the reconstruction process under the chosen-plaintext attack, (2) our design is based on a malicious cloud server model and can verify the correctness of the cloud returned result with a probability of approximating 1, and (3) our algorithm is highly efficient and can make the local client achieve decent computational savings. The main technique of our design is a combination of linear transformation, permutation and restricted random padding which is concise and high-efficiency. We analyze the above claims with rigorous theoretical arguments and comprehensive experimental analysis.

INDEX TERMS Client-server system, computation outsourcing, compressed sensing reconstruction, privacy preservation.

I. INTRODUCTION

In recent years, the COVID-19 pandemic has greatly boosted the development of online diagnosis and treatment, in which paradigm, potential patients with the new coronary disease can first take CT images of their lungs with the medical data acquisition device, and then send the images to the doctor. After that, the doctor can judge the disease and present the corresponding treatment planning based on the received images. In this case, the resolution of the image will greatly affect the doctor's judgment. Low-resolution images could make the doctor present wrong judgments, while high-resolution images will make the doctor's judgment more accurate. However, images with high qualities are usually too large to store. Generally, we can employ the compressed sensing reconstruction ($\mathcal{CSR}$) algorithm [4], [5], [11] to solve this problem. The $\mathcal{CSR}$ is an efficient signal sampling technique proposed by Donoho *et al.* [4], [5], [11]. For any compressible image, it can accurately reconstruct the original image from a set of far fewer samples than those required by the Shannon–Nyquist sampling theorem [14]. Therefore, the acquisition device can sample the medical image with $\mathcal{CSR}$ algorithm and send the compressed image (*i.e.* sample) to the doctor. Since the size of a sample is always smaller than that of the original image, this method can evidently reduce the storage overhead [10]. Yet there still exist many practical

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

concerns for $\mathcal{CSR}$-based image processing. On one hand, in the current big data era, the scale of the tackled medical images is usually very large, the storage savings with $\mathcal{CSR}$ may not be enough for local resource-constrained medical institutes. On the other hand, the reconstruction processing of $\mathcal{CSR}$ is time-consuming, it may be overloaded for most data acquisition devices. Fortunately, the promising cloud computing paradigm exactly solve these two problems [8], [12]. That is, the resource-constrained data acquisition device can upload the compressed images to a resource-abundant cloud server and, meanwhile, the cloud server can assist the doctor in realizing the images reconstruction.

Although cloud computing can provide a flexible storage and processing infrastructure, many security issues arise [17], [21], [22], [27], [31]. First, the image data is usually private, the leakage of these data may cause significant property losses to the outsourcer (e.g. individuals or enterprises). Second, the cloud server is remote and thus out of control. It may grab valuable information from the received information and the intermediate calculated result, or even deliberately send a forged result to fool the outsourcer. Finally, due to some unforeseeable reasons, hardware damage or software errors may encounter when computing or transmitting the data. Therefore, it is of great significance to design a secure cloud-assisted $\mathcal{CSR}$ algorithm, which, besides achieving considerable computational savings on the local side, should assure the privacy of the outsourcer's sensitive information and the verifiability of the server returned result [16], [30], [35]. Along this direction, many different methods have been developed to securely outsource the $\mathcal{CSR}$ task to a remote cloud server [13], [23], [24], [34]. However, there still exist many security and efficiency issues, which will be discussed in the following separate subsection, needing to be further investigated.

A. RELATED WORK

In recent years, many scholars have studied the $\mathcal{CSR}$ algorithm in the field of information security [15], [28], [29], [33]. In this section, we will review the closely related work towards two lines: the progress of $\mathcal{CSR}$ theory and the progress of privacy-preserving $\mathcal{CSR}$ within a cloud environment.

For $\mathcal{CSR}$ theory, since Donoho [11] proposed the theory of $\mathcal{CSR}$ which consists of a sampling sub-algorithm with some measurement matrix and a reconstruction sub-algorithm with some sensing matrix, many scholars have tried to improve the quality of the reconstructed image with a sample as small as possible. Divekar and Ersoy [10] utilized compressed sensing technology to reduce the storage space of large-scale data. That is, uploading the compressed sample to the cloud server instead of storing the complete image locally. According to their demonstration, compared with directly storing the original image, storing the compressed sample can save 50% of the storage space. But their work does not concern data security issues. Dai and Milenkovic [9] noticed the complexity of the reconstruction process and proposed a new method for reconstructing sparse signals with high reconstruction accuracy. Also, they did not consider achieving the computational task through cloud servers, and thus did not involve privacy issues. Another view is treating the $\mathcal{CSR}$ algorithm as a data encryption approach [19], [20]. They pointed out that if the measurement matrix was kept secret, the attacker was incapable of recovering the original data. For instances, Wang *et al.* [26] utilized the chaotic discrete wavelet transform basis and chaotic discrete cosine transform measurement matrix to specify the sampling and reconstruction sub-algorithms in $\mathcal{CSR}$ theory. Compared with the traditional measurement matrix method, this algorithm can improve the quality of reconstructed images with a small sample. At essentially the same time, Liu *et al.* [18] proposed an image visual privacy-preserving level evaluation method for the multilayer $\mathcal{CSR}$ model based on contrast and salient structural features, they used an improved Gaussian random measurement matrix to sample the images. Subsequently, Chai *et al.* [7] designed an efficient visually meaningful double color image sample algorithm with an optimized measurement matrix by SVD.

For the $\mathcal{CSR}$ within a cloud environment, many efficient and secure outsourcing $\mathcal{CSR}$ algorithms have been proposed. Firstly, Wang *et al.* [23], [24] considered two application scenarios about the outsourcing of $\mathcal{CSR}$, one is to privacy-preserving store and reconstruct large-scale images on the cloud, and the other is outsourcing the storage and reconstruction of healthcare diagnostic signals to a cloud server. The encryption methods of their algorithms are similar and on basis of affine mapping technology. Although the security of their algorithms is robust, due to the multiple operations of dense matrix multiplications, the efficiency is poor, especially for large-scale applications. In addition, the cloud server in their designs is assumed to be semi-honest, so their schemes fail to fulfill the verifiability of the results returned from the cloud. Later, Zhang *et al.* [34] studied a new scenario that multiple non-colluding and semi-honest cloud servers parallelly sample and reconstruct the original signal, and designed a privacy-preserving method based on random permutations. However, the non-colluding assumption among multiple clouds is too strong in practice, and the verifiability is also missed. Subsequently, Hu *et al.* [13] presented an outsourcing scheme for image storage and reconstruction with a non-standard $\mathcal{CSR}$ algorithm. They designed a sparse ℓ_1 norm-preserving matrix transformation to realize the preservation of the measurement matrix and the sparse coefficient vector during the reconstruction process. However, their scheme does not consider the privacy of the sample. Also, it is designed under a semi-honest cloud and thus without verifiability. Under the assumption of a malicious cloud server, Zhang *et al.* [32] proposed a verifiable outsourcing algorithm for $\mathcal{CSR}$. Their algorithm realizes the privacy of the original signal by keeping the employed orthogonal sparse base secret and achieves the verifiability of the server returned result by outsourcing the task twice. Essentially, their algorithm is an adaptation of the standard $\mathcal{CSR}$ algorithm without

any encryption operation. The measurement matrix is public and the sparse coefficient vector in the reconstruction process is also not protected. More importantly, the outsourcer must perform the outsourcing algorithm twice to verify the correctness of the results returned from the cloud, which greatly reduces the efficiency of their algorithm. Recently, Wang *et al.* [25] proposed a low-complexity p-tensor product $\mathcal{CSR}$ outsourcing algorithm under the assumption of an honest cloud. They mainly consider the threats from outside attackers. For data security and user authentication, the cloud server uses asymmetric encryption to encrypt the sample and share the private key with the user for identity authentication. After the user is authenticated, the cloud performs a $\mathcal{CSR}$ service and returns the result to the user.

B. MOTIVATION AND OUR CONTRIBUTION

Based on our above investigation, most of the existing $\mathcal{CSR}$ outsourcing algorithms are designed without verifiability. Meanwhile, the verifiable outsourcing algorithm [32] does not concern the privacy of the sample and the key coefficient vector in the reconstruction process, and the employed verifiability method is low efficiency. These unsatisfactory facts motivate us to design a highly efficient, privacy-enhanced, and verifiable outsourcing algorithm for medical image processing within a fully malicious cloud environment.

In this paper, we focus on the setting that the medical institute aims to rent a resource-powerful cloud server to securely store and reconstruct the large-scale medical images with $\mathcal{CSR}$ technique, and design a new efficient and secure cloud-aided diagnosis algorithm. Precisely, compared with prior arts, our main contribution can be reflected as the following three aspects:

1) Our design is privacy-enhanced. Our design can not only protect the privacy of the original image, but also blind the sampled signal, the sensing matrix and the solution vector of the convex optimization problem. We argue the one-way privacy of the above information under the chosen-plaintext attack with rigorous theoretical analysis.
2) Our algorithm is designed under a malicious cloud server. With an intentionally designed random padding technique, our design enables the doctor to detect dishonest behaviors of the cloud with a probability of approximating 1.
3) Our algorithm is high-efficiency. Our privacy preservation approach is on basis of linear transformation, permutation and restricted random padding techniques, which can be efficiently implemented. We theoretically argue the computational savings achieved on the local side and experimentally evaluate the practical performance of our outsourcing algorithm by (1) comparing our design with Wang et al's algorithm [24] and (2) contrasting the time cost of outsourcing with the time cost without outsourcing. Theoretical and experimental analysis shows the high efficiency of our algorithm.

C. LAYOUT OF OUR PAPER

The rest of this article is arranged as follows: Section II briefly reviews the $\mathcal{CSR}$ theory and introduces the system model, the threat model and our design goals. In section III, we introduced some notations and mathematical concepts used in our design. Our outsourcing design of $\mathcal{CSR}$ for medical images is provided with a detailed description in section IV, and the correctness and security of the design are analyzed in section V. Section VI evaluates the efficiency of the proposed algorithm with rigorous theoretical argument and extensive experimental analysis. Finally, we conclude our paper in section VII.

II. PROBLEM STATEMENT

Before presenting our design, we introduce some preliminaries about $\mathcal{CSR}$.

A. COMPRESSED SENSING RECONSTRUCTION

Compressed sensing is a non-adaptive linear measurement process, which improves the shortcomings of traditional sampling that discards part of the data [6], [11]. Suppose there is a signal (e.g., a medical image) $\mathbf{x} \in \mathbb{R}^n$ which is usually not sparse. The signal $\mathbf{x}$ is called compressible, if there exists some orthogonal basis $\mathbf{D} \in \mathbb{R}^{n\times n}$ (the classic orthogonal basis includes discrete cosine transform, Fourier transform, discrete wavelet transform [1]) such that $\mathbf{x}$ can be expressed as

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

where $\mathbf{s} \in \mathbb{R}^n$ is a sparse projection coefficient vector. Obviously, $\mathbf{x}$ and $\mathbf{s}$ are equivalent representations of the same signal.

Sampling process: Choose a measurement matrix $\mathbf{A} \in \mathbb{R}^{m\times n}$ ($m \ll n$) satisfying the restricted isometry property (RIP) [3], and then calculate the compressed sample $\mathbf{y} \in \mathbb{R}^m$ as below:

$$\mathbf{y} = \mathbf{A}\mathbf{x}. \tag{2}$$

Generally, the most commonly used measurement matrices are independent and identically distributed Gaussian random matrices, as well as random Bernoulli matrices and Toplitz matrices [1].

Reconstruction process: This step reconstructs the sparse coefficient vector $\mathbf{s}$ from the measurement sample $\mathbf{y}$ by solving an ℓ_1 minimization problem:

$$\min \|\mathbf{s}\|_1 \quad \text{subject to } \mathbf{y} = \mathbf{H}\mathbf{s}, \tag{3}$$

where $\mathbf{H} = \mathbf{A}\mathbf{D} \in \mathbb{R}^{m\times n}$ is the sensing matrix. Finally, the original signal $\mathbf{x}$ can be recovered via (1)

B. SYSTEM ARCHITECTURE AND THREAT MODEL

1) SYSTEM MODEL

As shown in Fig.1, our medical image compression and reconstruction outsourcing algorithm (MIOA$_{\mathcal{CSR}}$) model includes three participants: the medical image acquisition

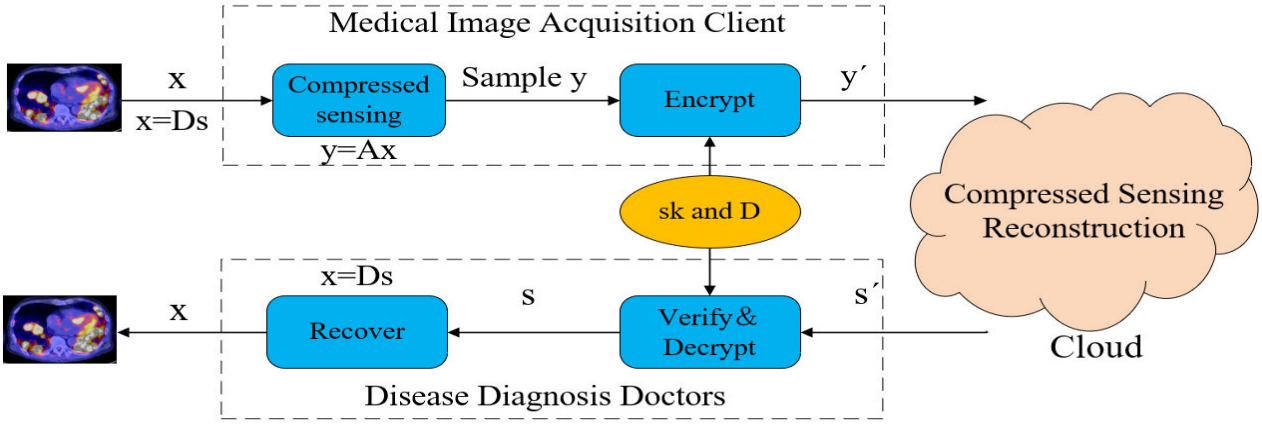


FIGURE 1. The system model.

client C, the disease diagnosis doctor D and the cloud server S. Limited by the storage and computing capabilities, the medical image acquisition device and disease diagnosis doctor use compressed sensing technology to reduce storage, and at the same time leverage resource-rich cloud servers to achieve reconstruction tasks. However, due to the potential untrustworthiness of cloud servers, a tailored encryption technology must be designed to ensure the privacy of information. First, the medical image acquisition client C adopts compressed sensing technology to obtain the patient's image sample data. That is, C samples the medical image $\mathbf{x} \in \mathbb{R}^n$ with an $m \times n$ ($m \ll n$) measurement matrix $\mathbf{A}$ and obtains the sample $\mathbf{y} = \mathbf{Ax}$. Simultaneously, it calculates the sensing matrix $\mathbf{H} = \mathbf{AD}$, where $\mathbf{D} \in \mathbb{R}^{n\times n}$ is some orthogonal sparse matrix. In order to protect the patient's data privacy, the medical image acquisition client C generates a secret key sk and encrypts the information $z = (\mathbf{H}, \mathbf{y})$ to $z' = (\mathbf{H}', \mathbf{y}')$. Then it uploads z' to the cloud S for storage and image reconstruction. After receiving the image query request from the disease diagnosis doctor D, the cloud S performs the medical image reconstruction task. That is, it calculates $\mathbf{s}' = \mathcal{CSR}'(z')$, and sends $\mathbf{s}'$ to the doctor D. Finally, after receiving $\mathbf{s}'$, D employs the key sk shared with the client C to decrypt $\mathbf{s}'$ and gets $\mathbf{s} = \mathcal{CSR}(z)$. Followed by the verification of its correctness, D further restores the original medical image $\mathbf{x} = \mathbf{Ds}$.

Precisely, our secure medical image compression and reconstruction outsourcing algorithm can be formalized as a six-tuple $\text{MIOA}_{\mathcal{CSR}}$ = (**Sample**, **KeyGen**, **ProbEnc**, **Compute**, **ProbVer&Dec**, **Recover**) consisting of the following six probabilistic polynomial-time (PPT) algorithms:

1) **Sample**$(\mathbf{x}, \mathbf{A}, \mathbf{D}) \rightarrow \{\mathbf{y}, \mathbf{H}\}$: For the medical image $\mathbf{x} \in \mathbb{R}^{n\times n}$, the medical image acquisition client C employs an $m \times n$ matrix $\mathbf{A}$ to measure $\mathbf{x}$ and obtains a sample $\mathbf{y}$. Simultaneously, C selects an $n \times n$ orthogonal matrix $\mathbf{D}$ and calculates the sensing matrix $\mathbf{H} = \mathbf{AD}$.
2) **KeyGen**$(\mathcal{CSR}, z, 1^\kappa) \rightarrow \{sk\}$: For the computation task $\mathcal{CSR}$ with an input $z = (\mathbf{y}, \mathbf{H})$, and a security parameter κ, medical image acquisition client C invokes the algorithm **KeyGen** to generate a secret key sk.
3) **ProbEnc**$(\mathcal{CSR}, z, sk) \rightarrow \{\mathcal{CSR}', z'\}$: With the input sk, the algorithm **ProbEnc** encrypts the original computation task ($\mathcal{CSR}$,z) into a blinded task ($\mathcal{CSR}'$, z'). Medical image acquisition client C performs this algorithm and sends the output ($\mathcal{CSR}'$, z') to the cloud S.
4) **Compute**$(\mathcal{CSR}', z') \rightarrow \{\mathbf{s}'\}$: After receiving the computation task ($\mathcal{CSR}'$, z'), the cloud server S performs this algorithm to compute $\mathbf{s}' = \mathcal{CSR}'(z')$, and then sends s' to the disease diagnosis doctor D.
5) **ProbVer&Dec**$(\mathcal{CSR}, \mathbf{s}', sk) \rightarrow \{\delta\}$: After receiving the cloud returned result $\mathbf{s}'$, the disease diagnosis doctor D utilizes the secret key sk shared by the client C to verify and decrypt the result $\mathbf{s}'$. If $\mathbf{s}'$ passes the verification, the algorithm decrypts it and outputs $\delta = \mathbf{s}$. Otherwise, it outputs $\delta = \perp$.
6) **Recover**$(\delta, \mathbf{D}) \rightarrow \{\gamma\}$: If $\delta = \mathbf{s}$, D carries out this algorithm to recover the original medical image $\gamma = \mathbf{x} = \mathbf{Ds}$. Else, this algorithm outputs $\gamma = \delta = \perp$.

2) THREAT MODEL

In the above system, threats mainly come from the untrusted cloud server. Generally, based on the different behaviors of cloud servers, untrusted cloud servers can be divided into three categories: lazy, honest and curious (*i.e.* semi-honest), and malicious (dishonest and curious). After receiving the assigned computation task, to save the expensive computational resource, a 'lazy' server may not perform the specified operations completely and return an intermediate result or even a random result to the doctor. An honest and curious server will perform the specified task honestly. However, it may be curious about the patient's private data and try to recover the valuable part from the input and output of the computation task. For a malicious server, it not only is curious about the patient's sensitive information, but also may arbitrarily deviate from the specifications. For example, it could falsify a result to deceive the doctor.

Furthermore, according to the different abilities of cloud servers, there are mainly three attack models:

1) **Ciphertext-only attack (*COA*) Model.** In *COA* model, the cloud server only knows the encryption algorithm and the ciphertext to be decrypted, and tries to recover the corresponding plaintext.
2) **Known-plaintext attack (*KPA*) Model.** In *KPA* model, except the encryption algorithm and the ciphertext to be decrypted, the cloud server also owns several plaintexts and their corresponding ciphertexts.
3) **Chosen-plaintext attack (*CPA*) Model.** In *CPA* model, the cloud server can adaptively choose several plaintexts and obtain their corresponding ciphertexts. It tries to recover the plaintext of the ciphertext to be decrypted.

Overall, there are nine possible combined threat models according to different behaviors and attack abilities of cloud servers. Clearly, an outsourcing algorithm designed under the malicious cloud with a *CPA* model is also secure under other threat models, but not vice versa. Therefore, in terms of security, it is more meaningful to design the outsourcing algorithm under the 'malicious server + *CPA*' threat model.

C. DESIGN GOALS

Our goal is to design a correct, high-efficiency and secure medical image compression and reconstruction outsourcing algorithm $\text{MIOA}_{\mathcal{CSR}}$ under the 'malicious server + *CPA*' threat model. We formalize their strict definitions as follows.

1) CORRECTNESS

Roughly, for the computation task $\mathcal{CSR}$, correctness means that the algorithm $\text{MIOA}_{\mathcal{CSR}}$ can assure the doctor D to obtain the correct result if the cloud performs the assigned computation task honestly.

Definition 1 (Correctness): A medical image compression and reconstruction outsourcing algorithm $\text{MIOA}_{\mathcal{CSR}}$ *is correct if, for any input* z, $\{sk\} \leftarrow \textbf{KeyGen}(\mathcal{CSR}, z, 1^\kappa)$, $\{\mathcal{CSR}', \mathbf{y}'\} \leftarrow \textbf{ProbEnc}(\mathcal{CSR}, z, sk)$, $\{\mathbf{s}'\} \leftarrow \textbf{Compute}(\mathcal{CSR}', z')$ *and* $\mathbf{s}' = \mathcal{CSR}'(z')$, *the algorithm* **ProbVer&Dec**$(\mathcal{CSR}, \mathbf{s}', sk)$ *outputs* $\mathbf{s} = \mathcal{CSR}(z)$.

2) INPUT/OUTPUT PRIVACY

Informally, input privacy represents that the outsourcing algorithm $\text{MIOA}_{\mathcal{CSR}}$ should protect the privacy of the client's information z, and output privacy means $\text{MIOA}_{\mathcal{CSR}}$ should protect the privacy of the doctor's information $s = \mathcal{CSR}(z)$ under decent threat model. Here, we mainly argue the input (resp. output) privacy with one-way notion under the *CPA* model. Strictly, we formalize the description of *CPA* model with the following two experiments $Exp_{\mathcal{A}}^{input}[\mathcal{CSR}, 1^\kappa]$ and $Exp_{\mathcal{A}}^{output}[\mathcal{CSR}, 1^\kappa]$.

Experiment $Exp_{\mathcal{A}}^{input}[\mathcal{CSR}, 1^\kappa]$

Query and response :

$z_0 = \sigma_{z_0} = \perp$.
For $i = 1, \cdots, t = \text{poly}(\kappa)$
$z_i \leftarrow \mathcal{A}(\mathcal{CSR}, (z_j, \sigma_{z_j})_{0 \le j \le i-1})$.
$sk_i \leftarrow \textbf{KeyGen}(\mathcal{CSR}, z_i, 1^\kappa)$.
$\sigma_{z_i} = (\mathcal{CSR}', z_i') \leftarrow \textbf{ProbEnc}(\mathcal{CSR}, sk_i, z_i)$.

Challenge :

$\hat{z} \leftarrow \text{Domain}(\mathcal{CSR})$.
$\hat{sk} \leftarrow \textbf{KeyGen}(\mathcal{CSR}, \hat{z}, 1^\kappa)$.
$\sigma_{\hat{z}} = (\mathcal{CSR}', \hat{z}') \leftarrow \textbf{ProbEnc}(\mathcal{CSR}, \hat{sk}, \hat{z})$.
$\bar{z} \leftarrow \mathcal{A}(\mathcal{CSR}, (z_j, \sigma_{z_j})_{0 \le j \le t}, \sigma_{\hat{z}})$.
if $\bar{z} = \hat{z}$ output $'1'$;
else output $'0'$.

In the *query and response* phase of the above experiment, the adversary $\mathcal{A}$ can adaptively choose $t = \text{poly}(\kappa)$ inputs $\{z_i\}_{1 \le i \le t}$ and capture their corresponding ciphertext $\{\sigma_{z_i}\}_{1 \le i \le t}$ by repeatedly invoking the oracle algorithm **ProbEnc**. Subsequently, in the *challenge* phase, the adversary $\mathcal{A}$ receives the ciphertext $\sigma_{\hat{z}}$ of some challenge plaintext $\hat{z}$. Then, $\mathcal{A}$ tries to calculate a result $\bar{z}$ on basis of its collected information in the *query and response* phase. If $\bar{z} = \hat{z}$, the experiment outputs 1, otherwise, it outputs 0.

Experiment $Exp_{\mathcal{A}}^{output}[\mathcal{CSR}, 1^\kappa]$

Query and response :

$z_0 = \sigma_{z_0} = \delta_0 = \perp$.
For $i = 1, \cdots, t = \text{poly}(\kappa)$
$z_i \leftarrow \mathcal{A}(\mathcal{CSR}, (z_j, \sigma_{z_j}, \delta_j)_{0 \le j \le i-1})$.
$sk_i \leftarrow \textbf{KeyGen}(\mathcal{CSR}, z_i, 1^\kappa)$.
$\sigma_{z_i} \leftarrow \textbf{ProbEnc}(\mathcal{CSR}, sk_i, z_i)$.
$s_i' \leftarrow \mathcal{A}(\mathcal{CSR}, (z_j, \sigma_{z_j}, \delta_j)_{0 \le j \le i-1}, \sigma_{z_i})$.
$\delta_i \leftarrow \textbf{ProbVer\&Dec}(\mathcal{CSR}, sk_i, s_i')$.

Challenge :

$\hat{z} \leftarrow \text{Domain}(\mathcal{CSR})$.
$\hat{sk} \leftarrow \textbf{KeyGen}(\mathcal{CSR}, \hat{z}, 1^\kappa)$.
$\sigma_{\hat{z}} = (\mathcal{CSR}', \hat{z}') \leftarrow \textbf{ProbEnc}(\mathcal{CSR}, \hat{sk}, \hat{z})$.
$\hat{s}' \leftarrow \textbf{Compute}(\sigma_{\hat{z}})$.
$\hat{s} \leftarrow \mathcal{A}(\mathcal{CSR}, (z_j, \sigma_{z_j}, \delta_j)_{0 \le j \le t}, \sigma_{\hat{z}}, \hat{s}')$.
if $\hat{s} = \mathcal{CSR}(\hat{z})$, output $'1'$;
else output $'0'$.

Similarly, in the *query and response* phase, the adversary $\mathcal{A}$ can adaptively choose $t = \text{poly}(\kappa)$ inputs $\{z_i\}_{1 \le i \le t}$, and obtain their corresponding t three-tuples of $(z_i, \sigma_{z_i}, \delta_i)_{1 \le i \le t}$ with the oracle access to the algorithms **ProbEnc** and **ProbVer&Dec**. In the *challenge* phase, given a challenge plaintext $\hat{z}$, the adversary $\mathcal{A}$ captures $\sigma_{\hat{z}}$ and $\hat{s}'$ output by the algorithms **ProbEnc** and **Compute**. Then, according to the collected information in the previous stage, $\mathcal{A}$ tries to calculate a value $\hat{s}$. If $\hat{s} = \mathcal{CSR}(\hat{z})$, the experiment outputs 1. Otherwise, the experiment outputs 0.

Definition 2 (Input and Output Privacy): An outsourcing algorithm $\text{MIOA}_{\mathcal{CSR}}(\cdot)$ *satisfies input (resp. output) privacy if, for any probabilistic polynomial time (PPT) adversary* $\mathcal{A}$*, the probability of the* $Exp_{\mathcal{A}}^{input}[\mathcal{CSR}, 1^{\kappa}]$ *(resp.* $Exp_{\mathcal{A}}^{output}[\mathcal{CSR}, 1^{\kappa}]$ *) output* 1 *is negligible, i.e.*

$$Pr[Exp_{\mathcal{A}}^{input}[\mathcal{CSR}, 1^{\kappa}] = 1] \leq \texttt{negl}(\kappa)$$
$$(resp. Pr[Exp_{\mathcal{A}}^{output}[\mathcal{CSR}, 1^{\kappa}] = 1] \leq \texttt{negl}(\kappa)),$$

where $\texttt{negl}(\kappa)$ *is a negligible function in the parameter* κ.

3) VERIFIABILITY

Verifiability points to that the doctor D can detect the dishonest behaviors of the cloud with a non-negligible probability. Precisely,

Definition 3 (α-Verifiable): A medical image compression and reconstruction outsourcing algorithm $\text{MIOA}_{\mathcal{CSR}}$ *is α-verifiable, if, for any input z,* $\{sk\} \leftarrow \textbf{KeyGen}(\mathcal{CSR}, z, 1^{\kappa})$, $\{\mathcal{CSR}', z'\} \leftarrow \textbf{ProbEnc}(\mathcal{CSR}, z, sk)$, *and* $\mathbf{s}' \leftarrow \textbf{Compute}(\mathcal{CSR}', z')$, *then the probability of* $\textbf{ProbVer\&Dec}(\mathcal{CSR}', \mathbf{s}', sk) \rightarrow \{\mathbf{s}\}$ *is no less than α in case that if* $\mathbf{s}' = \mathcal{CSR}'(z')$, *and the probability of* $\textbf{ProbVer\&Dec}(\mathbf{s}') \rightarrow \{\mathbf{s}\}$ *is less than* $1 - \alpha$ *in case that* $\mathbf{s}' \neq \mathcal{CSR}'(z')$. *I.e.,*

$$\Pr[\{\mathbf{s}\} \leftarrow \textbf{ProbVer\&Dec}(\mathcal{CSR}', \mathbf{s}', sk) \mid \mathbf{s}' = \mathcal{CSR}'(z')] \geq \alpha,$$
$$\Pr[\{\mathbf{s}\} \leftarrow \textbf{ProbVer\&Dec}(\mathcal{CSR}', \mathbf{s}', sk) \mid \mathbf{s}' \neq \mathcal{CSR}'(z')] < 1 - \alpha.$$

4) EFFICIENCY

Without outsourcing, the client must reconstruct the sparse transformation coefficient vector by itself. We denote the time cost is t_o. With the algorithm $\text{MIOA}_{\mathcal{CSR}}$, the time-consuming reconstruction task is outsourced to the cloud server S. However, the outsourcing process causes additional encryption and decryption operations, the time cost of which we denote as t_c. Intuitively, an efficient outsourcing algorithm should assure that t_o is substantially larger than t_c.

Definition 4 (β-Efficient): A medical image compression and reconstruction outsourcing algorithm $\text{MIOA}_{\mathcal{CSR}}$ *is β-efficient if* $\frac{t_o}{t_c} \geq \beta$, *where t_o is the time cost of the client performing the image reconstruction task by itself, and t_c represents the overall time consumption of the client and the doctor realizing the encryption and decryption operations through employing the outsourcing algorithm* $\text{MIOA}_{\mathcal{CSR}}$.

III. PREPARATORY KNOWLEDGE

In this section, we will introduce the terms and some basic mathematical tools that used in the rest of our paper.

A. NOTATIONS

In our paper, without instruction, the uppercase bold letters (e.g. $\mathbf{H}$) represent various matrices and the lowercase bold letters (e.g. $\mathbf{x}$) represent column vectors. Assume $h(x)$ and $l(x)$ are two non-decreasing functions, $h(x) = O(l(x))$ means $\lim_{n\to\infty} \frac{h(x)}{l(x)} = 0$. Finally, Table 1 lists other commonly used notations and their corresponding explanations in this paper.

TABLE 1. Notations.

Notations	Descriptions
$\mathbf{A}$	the $m \times n$ measurement matrix
$\mathbf{D}$	the $n \times n$ orthogonal matrix
$\mathbf{H}$	the $m \times n$ sensing matrix
$\mathbf{P}$	an $(n+k) \times (n+k)$ permutation matrix
$\mathbf{B}$	a $k \times k$ random matrix
$\mathbf{M}$	an $(m+k) \times (m+k)$ random matrix
λ	the security parameter
$\|\cdot\|_1$	the l_1 norm function
k	the verifiability parameter
$\mathbf{x}$	the n-dimensional medical image
$\mathbf{y}$	the m-dimensional sample vector of $\mathbf{x}$
$\mathbf{s}$	the sparse projection coefficient vector
$\mathbf{r}$	a random k-dimensional vector
$\mathbf{y}'$	the ciphertext vector of $\mathbf{y}$
$\mathbf{H}'$	the ciphertext matrix of $\mathbf{H}$
$\mathbf{s}'$	the ciphertext vector of $\mathbf{s}$
a	a random real number
C	the medical image acquisition client
D	the disease diagnosis doctor
S	the cloud server

B. PERMUTATION MATRIX

Definition 5 (Permutation [2]): Each n-ary permutation corresponds to a unique permutation matrix. Let π be an n-ary permutation:

$$\pi : \{1, 2, \cdots, n\} \rightarrow \{1, 2, \cdots, n\}.$$

Give its mapping diagram:

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \pi(1) & \pi(2) & \pi(3) & \cdots & \pi(n) \end{pmatrix}.$$

Its corresponding $n \times n$ permutation matrix $\mathbf{P}_{\pi}$ is expressed as:

$$\mathbf{P}_{\pi} = \begin{bmatrix} \mathbf{e}_{\pi(1)} \\ \mathbf{e}_{\pi(2)} \\ \vdots \\ \mathbf{e}_{\pi(n)} \end{bmatrix},$$

where $\mathbf{e}_{\pi(i)} (i = 1, 2 \cdots n)$ *is a row vector, only the entry of* $\pi(i)$ *is* 1, *and the rest are* 0.

Example 1: Given a permutation π,

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

the corresponding permutation matrix $\mathbf{P}_{\pi}$ is

$$\mathbf{P}_{\pi} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

IV. SECURELY OUTSOURCING IMAGE COMPRESSION AND RECONSTRUCTION

A. DESIGN RATIONALE

Clearly, the key of our design is to come up with an efficient and secure blind technique to outsource the convex optimization problem (3). To avoid the cloud server obtaining any useful sensitive information, the designed technique should simultaneously ensure the privacy of the input ($\mathbf{y}$, $\mathbf{H}$) and the output $\mathbf{s}$.

Naturally, we can construct an equivalent convex optimization problem with a decent encryption approach

$$\min \left\|\mathbf{s}'\right\|_1 \quad \text{subject to } \mathbf{y}' = \mathbf{H}'\mathbf{s}'. \tag{4}$$

where $\mathbf{y}'$, $\mathbf{H}'$ and $\mathbf{s}'$ refer to the ciphertext of $\mathbf{y}$, the ciphertext of $\mathbf{H}$ and the ciphertext of $\mathbf{s}$ respectively. Naturally, to protect the information in $\mathbf{y}$ and $\mathbf{H}$, we can employ the technique in [23], [24] by simultaneously left-multiplying the two sides of the equation in (3) by an invertible matrix $\mathbf{M}$. However, this simple operation can not be directly applied to blind the output $\mathbf{s}$ and needs to be adapted according to the technique used to protect $\mathbf{s}$. For the privacy of $\mathbf{s}$, since $\mathbf{s}$ is sparse, we need to conceal the number, the position, and the value information of the non-zero entries in $\mathbf{s}$. Meanwhile, our encryption approach should ensure the plaintext objective function and the ciphertext objective function to achieve the optimal value for the same value of $\mathbf{s}$. First, we confuse the number of the non-zero entries by adding a random vector $\mathbf{r}$ at the end of $\mathbf{s}$. Then, we perform a permutation $\mathbf{P}$ on $\mathbf{s}'$ to hide the position information of the entries in the actual output $\mathbf{s}$. Finally, we multiply $\mathbf{s}'$ by a random real a to protect the value information of each entry in the actual output $\mathbf{s}$. Correspondingly, we adapt the dimensions of $\mathbf{y}$ and $\mathbf{H}$ with a random matrix $\mathbf{B}$ to make the equation in (3) hold. In this way, the problem (3) can be equivalently transformed into

$$\begin{aligned}&\min \left\| a\mathbf{P}\begin{bmatrix}\mathbf{s}\\ \mathbf{r}\end{bmatrix}\right\|_1\\ &\text{subject to } a\mathbf{M}\begin{bmatrix}\mathbf{y}\\ \mathbf{Br}\end{bmatrix} = \mathbf{M}\begin{bmatrix}\mathbf{H} & \mathbf{0}\\ \mathbf{0} & \mathbf{B}\end{bmatrix}\mathbf{P}^{-1}a\mathbf{P}\begin{bmatrix}\mathbf{s}\\ \mathbf{r}\end{bmatrix}.\end{aligned}$$

That is, corresponding to the blinded convex optimization problem (4), we have

$$\begin{cases}\mathbf{s}' = a\mathbf{P}\begin{bmatrix}\mathbf{s}\\ \mathbf{r}\end{bmatrix}\\ \mathbf{y}' = a\mathbf{M}\begin{bmatrix}\mathbf{y}\\ \mathbf{Br}\end{bmatrix}\\ \mathbf{H}' = \mathbf{M}\begin{bmatrix}\mathbf{H} & \mathbf{0}\\ \mathbf{0} & \mathbf{B}\end{bmatrix}\mathbf{P}^{-1}.\end{cases}$$

With this method, the medical image acquisition client C can outsource the blinded convex optimization problem (4) instead of the problem (3) to the cloud server.

B. THE DETAILS OF OUTSOURCING ALGORITHM

In detail, our algorithm $\text{MIOA}_{\mathcal{CSR}}$ = (**Sample**, **KeyGen**, **ProbEnc**, **Compute**, **ProbVer&Dec**, **Recover**) consists of six sub-algorithms.

1) SAMPLE ALGORITHM: **SAMPLE**

The medical image acquisition client C selects a measurement matrix $\mathbf{A} \in \mathbb{R}^{m\times n}$ ($m \ll n$) and an orthogonal matrix $\mathbf{D}$. For any given medical image signal $\mathbf{x} \in \mathbb{R}^n$, C samples $\mathbf{x}$ and calculates the sensing matrix $\mathbf{H}$ with $\mathbf{A}$ and $\mathbf{D}$. *I.e.* the sample $\mathbf{y} = \mathbf{Ax}$ and the sensing matrix $\mathbf{H} = \mathbf{AD}$.

2) KEY GENERATION ALGORITHM: **KeyGen**

For any given input matrix $\mathbf{H} = (h_{ij})_{1\le i\le m, 1\le j\le n} \in \mathbb{R}^{m\times n}$ and vector $\mathbf{y} = (y_i)_{1\le i\le m} \in \mathbb{R}^m$, denote $\lambda = \max\{\log\|\mathbf{H}\|, \log\|\mathbf{y}\|, \log\|\mathbf{D}\|, \log\|\mathbf{x}\|\}$, where $\log\|\mathbf{H}\| = \max_{1\le i\le m, 1\le j\le n}(\lfloor\log|h_{ij}|\rfloor + 1)$ (resp. $\log\|\mathbf{y}\| = \max_{1\le i\le m}(\lfloor\log|y_i|\rfloor + 1)$, $\log\|\mathbf{D}\| = \max_{1\le i\le n, 1\le j\le n}(\lfloor\log|d_{ij}|\rfloor + 1)$, $\log\|\mathbf{x}\| = \max_{1\le i\le n}(\lfloor\log|x_i|\rfloor + 1)$) represents the maximum bit size of the entries in $\mathbf{H}$ (resp. $\mathbf{y}$, $\mathbf{D}$, $\mathbf{x}$). Given a positive constant (*i.e.*, verifiability parameter) k, the key generation algorithm **KeyGen** performs as follows:

1) Choose a random real number $a \neq 0$ with the bit size of its integer part and its decimal part being equal to λ.
2) Generate two random matrices $\mathbf{B} = (b_{ij})_{1\le i,j\le k} \in \mathbb{R}^{k\times k}$ and $\mathbf{M} = (m_{ij})_{1\le i,j\le m+k} \in \mathbb{R}^{(m+k)\times(m+k)}$ and a vector $\mathbf{r} \in \mathbb{R}^k$, out of which, each non-zero entry is with λ bits that is chosen randomly and uniformly.
3) Randomly and uniformly generate a permutation matrix $\mathbf{P} \in \{0, 1\}^{(n+k)\times(n+k)}$.
4) Output the encryption key $sk = (\mathbf{B}, \mathbf{M}, \mathbf{P}, \mathbf{r}, a)$.

3) CLIENT ENCRYPTION ALGORITHM: **ProbEnc**

With the secret key $sk = (\mathbf{B}, \mathbf{M}, \mathbf{P}, \mathbf{r}, a)$, the medical image acquisition client C encrypts the sensing matrix $\mathbf{H}$ and the sample vector $\mathbf{y}$ into

$$\begin{cases}\mathbf{H}' = \mathbf{M}\begin{bmatrix}\mathbf{H} & \mathbf{0}\\ \mathbf{0} & \mathbf{B}\end{bmatrix}\mathbf{P}^{-1}\\ \mathbf{y}' = a\mathbf{M}\begin{bmatrix}\mathbf{y}\\ \mathbf{Br}\end{bmatrix},\end{cases} \tag{5}$$

and sends $(\mathbf{H}', \mathbf{y}')$ to the cloud server S. Meanwhile, C sends $\mathbf{D}$ and part of secret key $(\mathbf{P}, \mathbf{r}, a)$ to the disease diagnosis doctor D with a secure channel.

4) SERVER COMPUTING ALGORITHM: **COMPUTE**

After receiving $(\mathbf{H}', \mathbf{y}')$, the cloud server S performs the specified computation task of solving the blinded convex optimization problem, *i.e.*,

$$\min \left\|\mathbf{s}'\right\|_1 \quad \text{subject to } \mathbf{y}' = \mathbf{H}'\mathbf{s}'.$$

Then, it returns the solution vector $\mathbf{s}'$ with the minimum ℓ_1 norm to the disease diagnosis doctor D.

5) VERIFICATION AND DECRYPTION ALGORITHM: **ProbVer&Dec**

After receiving $\mathbf{s}'$, the disease diagnosis doctor D calculates

$$\mathbf{s}^{\star} = \frac{1}{a}\mathbf{P}^{-1}\mathbf{s}' = \begin{bmatrix} \mathbf{s} \\ \mathbf{r} \end{bmatrix}. \tag{6}$$

Then, D verifies whether the vector formed by the last k entries of $\mathbf{s}^{\star}$ equals to $\mathbf{r}$. If they are same, D accepts the result $\mathbf{s}'$ and takes the vector formed by the first n entries of $\mathbf{s}^{\star}$ as the actual $\mathbf{s}$. Otherwise, it rejects.

6) RECOVER ALGORITHM: **RECOVER**

After obtaining $\mathbf{s}$, the disease diagnosis doctor D uses the matrix $\mathbf{D}$ shared by the medical image acquisition client C to recover

$$\mathbf{x} = \mathbf{D}\mathbf{s}.$$

Here, $\mathbf{x}$ is the actual high-resolution medical image that the disease diagnosis doctor D wanted.

V. CORRECTNESS AND SECURITY ANALYSIS

In this section, we will theoretically analyze the correctness, input/output privacy, verifiability of the proposed algorithm $\mathrm{MIOA}_{\mathcal{CSR}}$.

A. CORRECTNESS

Theorem 1: According to Definition 1, our outsourcing algorithm $\mathrm{MIOA}_{\mathcal{CSR}}$ *is correct for any input matrix* $\mathbf{H} \in \mathbb{R}^{m\times n}$ *and vector* $\mathbf{y} \in \mathbb{R}^m$.

Proof: Assume $\hat{\mathbf{s}}'$ is the output of the algorithm **Compute**, if the cloud server S is honest, $\hat{\mathbf{s}}'$ satisfies the problem (4). That is, $\hat{\mathbf{s}}' = a\mathbf{P}\begin{bmatrix} \hat{\mathbf{s}} \\ \mathbf{r} \end{bmatrix}$. Then $\frac{1}{a}\mathbf{P}^{-1}\hat{\mathbf{s}}' = \begin{bmatrix} \hat{\mathbf{s}} \\ \mathbf{r} \end{bmatrix}$, and the verification and decryption algorithm **ProbVer&Dec** will output $\hat{\mathbf{s}}$. Hence, substitute $(\mathbf{y}', \mathbf{H}')$ in problem (4) with equation (5), we get

$$\begin{cases} \|\hat{\mathbf{s}}'\|_1 = \min \|\mathbf{s}'\|_1 \\ a\mathbf{M}\begin{bmatrix} \mathbf{y} \\ \mathbf{B}\mathbf{r} \end{bmatrix} = \mathbf{M}\begin{bmatrix} \mathbf{H} & \mathbf{0} \\ \mathbf{0} & \mathbf{B} \end{bmatrix}\mathbf{P}^{-1}\hat{\mathbf{s}}'. \end{cases} \tag{7}$$

Since $\hat{\mathbf{s}}' = a\mathbf{P}\begin{bmatrix} \hat{\mathbf{s}} \\ \mathbf{r} \end{bmatrix}$, the equation (7) is equivalent to

$$\begin{cases} \left\| a\mathbf{P}\begin{bmatrix} \hat{\mathbf{s}} \\ \mathbf{r} \end{bmatrix} \right\|_1 = \min \left\| a\mathbf{P}\begin{bmatrix} \mathbf{s} \\ \mathbf{r} \end{bmatrix} \right\|_1 \\ \mathbf{y} = \mathbf{H}\hat{\mathbf{s}}. \end{cases} \tag{8}$$

Due to that $\mathbf{P}$ is a permutation matrix and a is a non-zero real, the equation (8) is further equivalent to

$$\begin{cases} \|\hat{\mathbf{s}}\|_1 = \min \|\mathbf{s}\|_1 \\ \mathbf{y} = \mathbf{H}\hat{\mathbf{s}}, \end{cases} \tag{9}$$

which shows that $\hat{\mathbf{s}}$ is the solution of problem (3). □

B. INPUT AND OUTPUT PRIVACY

In this section, we will prove that our algorithm $\mathrm{MIOA}_{\mathcal{CSR}}$ satisfies input and output privacy. Precisely, we will argue the one-way privacy of the input information $(\mathbf{H}, \mathbf{y})$ and the output vector $\mathbf{s}$ under the *CPA* model

Theorem 2: According to Definition 2, for any input matrix $\mathbf{H} \in \mathbb{R}^{m\times n}$ *and vector* $\mathbf{y} \in \mathbb{R}^m$, *our outsourcing algorithm* $\mathrm{MIOA}_{\mathcal{CSR}}$ *satisfies the input and output privacy.*

Proof: (1) Input privacy. In the experiment $Exp_{\mathcal{A}}^{input}[\mathcal{CSR}, 1^{\kappa}]$, $\mathcal{CSR}$ represents the computation task of compressed sensing reconstruction, and $\kappa = mn\lambda$. In the *Query and response* phase, the adversary $\mathcal{A}$ can adaptively choose $(z_i, \sigma_{z_i}) = ((\mathbf{H}_i, \mathbf{y}_i), (\mathbf{H}_i', \mathbf{y}_i'))$ for $1 \le i \le t$. With each new input, the **KenGen** algorithm will generate different sk randomly and independently, so the adversary will not get any useful information at this phase. In the *Challenge* phase, the adversary tries to recover the challenge target $(\mathbf{H}, \mathbf{y})$ after receiving its ciphertexts $(\mathbf{H}', \mathbf{y}')$.

Next, we analyze the probability that the $\mathbf{H}$ (resp.$\mathbf{y}$) can be successfully recovered by the adversary. Through the **ProbEnc** algorithm, we have

$$\begin{bmatrix} \mathbf{H} & \mathbf{0} \\ \mathbf{0} & \mathbf{B} \end{bmatrix} = \mathbf{M}^{-1}\mathbf{H}'\mathbf{P}, \tag{10}$$

$$\begin{bmatrix} \mathbf{y} \\ \mathbf{B}\mathbf{r} \end{bmatrix} = \frac{1}{a}\mathbf{M}^{-1}\mathbf{y}'. \tag{11}$$

Clearly, the adversary can recover $\mathbf{H}$ (resp. $\mathbf{y}$) after obtaining $\begin{bmatrix} \mathbf{H} & \mathbf{0} \\ \mathbf{0} & \mathbf{B} \end{bmatrix}$ (resp.$\begin{bmatrix} \mathbf{y} \\ \mathbf{B}\mathbf{r} \end{bmatrix}$).

If the adversary wants to recover $\mathbf{H}$, then the adversary must know the correct product $\mathbf{M}^{-1}\mathbf{H}'\mathbf{P}$. So the probability $\mathrm{Pr}_{\mathbf{H}}$ of the adversary successfully recovering $\mathbf{H}$ is

$$\begin{aligned} \mathrm{Pr}_{\mathbf{H}} &= \frac{1}{\left|\left\{\mathbf{H} \mid \begin{bmatrix} \mathbf{H} & \mathbf{0} \\ \mathbf{0} & \mathbf{B} \end{bmatrix} = \mathbf{M}^{-1}\mathbf{H}'\mathbf{P}\right\}\right|} \\ &\le \frac{1}{|\{\mathbf{M}^{-1} \mid \mathbf{M} \text{ is constructed as in sec. IV-B2}\}|} \\ &\le \frac{1}{|\{\mathbf{M} \mid \mathbf{M} \text{ is constructed as in sec.IV-B2}\}|} \\ &\le \frac{1}{2^{\lambda(m+k)^2}}. \end{aligned}$$

Obviously, the probability is negligible.

Similarly, to recover $\mathbf{y}$, the adversary must know the correct $\mathbf{M}$. Then, the probability $\mathrm{Pr}_{\mathbf{y}}$ that the adversary successfully recovers $\mathbf{y}$ is

$$\begin{aligned} \mathrm{Pr}_{\mathbf{y}} &= \frac{1}{\left|\left\{\mathbf{y} \mid \begin{bmatrix} \mathbf{y} \\ \mathbf{B}\mathbf{r} \end{bmatrix} = \frac{1}{a}\mathbf{M}^{-1}\mathbf{y}'\right\}\right|} \\ &\le \frac{1}{|\{\mathbf{M}^{-1} \mid \mathbf{M} \text{ is constructed as in sec.IV-B2}\}|} \\ &\le \frac{1}{|\{\mathbf{M} \mid \mathbf{M} \text{ is constructed as in sec.IV-B2}\}|} \\ &\le \frac{1}{2^{\lambda(m+k)^2}}, \end{aligned}$$

which is also negligible.

(2) Output privacy. We need to argue our algorithm protects the positions, the values and the number of non-zero entries of the output $\mathbf{s}$. In the experiment $Exp_{\mathcal{A}}^{output}[\mathcal{CSR}, 1^{\kappa}]$, the adversary $\mathcal{A}$ can adaptively obtain t three-tuples $(z_i, \sigma_{z_i}, \delta_i) = ((\mathbf{H}_i, \mathbf{y}_i), (\mathbf{H}_i', \mathbf{y}_i'), \hat{\mathbf{s}}_i)$ or $((\mathbf{H}_i, \mathbf{y}_i), (\mathbf{H}_i', \mathbf{y}_i'), \perp)$ for $i = 1, \cdots, t$. In the *Challenge* phase, given a ciphertext $(\mathbf{H}', \mathbf{y}')$ encrypted from some plaintext information $(\mathbf{H}, \mathbf{y})$, and the adversary can get the output result $\hat{\mathbf{s}}'$ from **Compute** algorithm, and attempts to recover $\hat{\mathbf{s}}$ from the information inferred in the first phase. Since, for different inputs, the **KenGen** algorithm will re-generate new keys randomly and independently, the adversary will not get any useful information at the *Query and response* phase. According to the decryption algorithm, we have

$$\begin{bmatrix} \mathbf{s} \\ \mathbf{r} \end{bmatrix} = \frac{1}{a}\mathbf{P}^{-1}\mathbf{s}'. \tag{12}$$

That is, the adversary needs to know the $(a, \mathbf{P})$ to recover the correct $\mathbf{s}$. Thus, the success probability $\Pr_{\mathbf{s}}$ that the adversary recovers the correct $\mathbf{s}$ is

$$\begin{aligned}\Pr_{\mathbf{s}} &= \frac{1}{\left|\left\{\mathbf{s} \mid \begin{bmatrix} \mathbf{s} \\ \mathbf{r} \end{bmatrix} = \frac{1}{a}\mathbf{P}^{-1}\mathbf{s}'\right\}\right|} \\ &\leq \frac{1}{|\{(a, \mathbf{P^{-1}}) \mid a \text{ and } \mathbf{P} \text{ is constructed as in sec.IV-B2}\}|} \\ &= \frac{1}{|\{(a, \mathbf{P}) \mid a \text{ and } \mathbf{P} \text{ is constructed as in sec.IV-B2}\}|} \\ &\leq \frac{k!}{(n+k)!},\end{aligned}$$

which is negligible. □

C. VERIFIABILITY

In this section, we will prove that our verification algorithm can detect that the cloud server returns an incorrect result with a probability approximate to 1.

Theorem 3: According to Definition 3, for any input matrix $\mathbf{H} \in \mathbb{R}^{m\times n}$ *and vector* $\mathbf{y} \in \mathbb{R}^m$*, our outsourcing algorithm* $\text{MIOA}_{\mathcal{CSR}}$ *is* $(1 - \frac{1}{2^{\lambda k}})$*-verifiable.*

Proof: According to Definition 3, we need to prove

$$\begin{aligned}&\Pr[\{\mathbf{s}\} \leftarrow \textbf{ProbVer\&Dec}(\mathcal{CSR}', s', sk) \mid \\ &\ s' = \mathcal{CSR}'(z')] \geq 1, \end{aligned} \tag{13}$$

$$\begin{aligned}&\Pr[\{\mathbf{s}\} \leftarrow \textbf{ProbVer\&Dec}(\mathcal{CSR}', s', sk) \mid \\ &\ s' \neq \mathcal{CSR}'(z')] < \frac{1}{2^{\lambda k}}. \end{aligned} \tag{14}$$

For the equation (13), it can be directly obtained by the correctness of our algorithm. If $s' \neq \mathcal{CSR}'(z')$, $\mathbf{s}'$ is not the solution of the blinded convex optimization problem (4). According to the **ProbVer&Dec** algorithm, if and only if the vector formed of the last k entries of the decrypted $\mathbf{s}^{\star}$ in equation (6) exactly equals to $\mathbf{r}$, $\mathbf{s}'$ can pass the verification. Thus, the probability that the cloud server can forge $\mathbf{r}$ is less than $\frac{1}{2^{\lambda k}}$, which proves the equation (14). □

VI. EFFICIENCY ANALYSIS

In this section, we will argue the efficiency of the proposed algorithm from theoretical and experimental perspectives.

A. THEORETICAL ANALYSIS

For the first step, we present a strict theoretical analysis.

Theorem 4: According to Definition 4, for any input matrix $\mathbf{H} \in \mathbb{R}^{m\times n}$ $(m < n)$ *and vector* $\mathbf{y} \in \mathbb{R}^m$*, our outsourcing algorithm* $\text{MIOA}_{\mathcal{CSR}}$ *is* β*-Efficient with*

$$\beta = O\left(n^2/m^2\right).$$

Proof: For any input matrix $\mathbf{H} \in \mathbb{R}^{m\times n}$ with $m < n$, without outsourcing, the convex optimization problem of compressed sensing reconstruction algorithm needs more than $O(n^3)$ multiplications [13], [23].

Next, we calculate the local client's added cost t_{total} with our outsourcing algorithm. On the local side, compared with non-outsourcing, the time-consuming convex optimization problem is avoidable yet the additional cost t_{client} incurs during the outsourcing process which mainly consists of three parts: the cost $t_{\textbf{KeyGen}}$ of Algorithm **KeyGen**, the cost $t_{\textbf{ProbEnc}}$ of Algorithm **ProbEnc**, and the cost $t_{\textbf{VeDec}}$ of Algorithm **ProbVer&Dec**. Therefore, the total cost $t_{\text{total}} = t_{\textbf{KeyGen}} + t_{\textbf{ProbEnc}} + t_{\textbf{VeDec}}$.

1) Estimation of $t_{\textbf{KeyGen}}$. In the key generation stage, the medical image acquisition client C need to generate two random matrices $\mathbf{B}$ and $\mathbf{M}$, a vector $\mathbf{r}$, a permutation matrix $\mathbf{P}$ and a real number a. Therefore $t_{\textbf{KeyGen}} = O(n + (m+k)^2 + k^2)$ random generation operations.
2) Estimation of $t_{\textbf{ProbEnc}}$. In the encryption stage, the medical image acquisition client C calculating $\mathbf{H}' = \mathbf{M}\begin{bmatrix} \mathbf{H} & \mathbf{0} \\ \mathbf{0} & \mathbf{B} \end{bmatrix}\mathbf{P}^{-1}$ needs $O(m(m+k)n + k(m+k)k) = O((m+k)(mn+k^2))$ multiplications, and calculating $\mathbf{y}' = a\mathbf{M}\begin{bmatrix} \mathbf{y} \\ \mathbf{Br} \end{bmatrix}$ needs $O((m+k)^2+k^2)$ multiplications. Thus, the total cost is $t_{\textbf{ProbEnc}} = O((m+k)(mn+k^2))$ multiplications.
3) Estimation of $t_{\textbf{VeDec}}$. In the verification and decryption stage, the dominant step is to calculate $\mathbf{s}^{\star} = \frac{1}{a}\mathbf{P}^{-1}\mathbf{s}'$, which requires $O(n+k)$ swap operations. Thus, the total cost is $t_{\textbf{VeDec}} = O(n+k)$ swaps.

Overall, the local time cost is $t_{\text{total}} = t_{\textbf{KeyGen}} + t_{\textbf{ProbEnc}} + t_{\textbf{VeDec}} = O((m+k)(mn+k^2))$ multiplications. Since k is some given constant, the efficiency factor is

$$\beta = \frac{t_{\text{original}}}{t_{\text{total}}} = \frac{O(n^3)}{O((m+k)(mn+k^2))} = O\left(\frac{n^2}{m^2}\right).$$

□

Next, we analyze the storage savings achieved by the algorithm for the local client. Assuming that there are ℓ medical images $\mathbf{x}_1, \cdots, \mathbf{x}_\ell$, without $\mathcal{CSR}$ and outsourcing algorithm, the local client only needs to store these original medical images $\mathbf{x}_i \in \mathbb{R}^n$ $(i = 1, \cdots, \ell)$, which are about $\ell n\lambda$ bits. With $\mathcal{CSR}$ and outsourcing algorithm, the local client needs to store ℓ verification and decryption secret keys

$(a_i, \mathbf{P}_i, \mathbf{r}_i)(i = 1, \cdots, \ell)$ which are about $\ell(\lambda+(n+k)\log(n+k)+k\lambda)$ bits, and the orthogonal matrix $\mathbf{D} \in \mathbb{R}^{n\times n}$ which are about $n^2\lambda$ bits. Hence, in this case, the storage complexity is $\ell(\lambda+(n+k)\log(n+k)+k\lambda)+n^2\lambda$. By solving the equation $\ell n\lambda \geq \ell(\lambda+(n+k)\log(n+k)+k\lambda)+n^2\lambda$, we have that, if

$$\ell \geq \frac{n^2}{n-1-k-(n+k)\log(n+k)/\lambda},$$

the proposed $\mathcal{CSR}$ outsourcing algorithm can save storage space. It must be pointed out that, in practice, the scale ℓ of medical images is usually very large. Consequently, the local client can achieve considerable storage savings in practical applications.

B. THEORETICAL COMPARISON WITH PREVIOUS ALGORITHMS

In this following subsection, we will compare our algorithm with existing $\mathcal{CSR}$ outsourcing algorithms in both security and efficiency. Currently, there mainly exist four outsourcing algorithms for $\mathcal{CSR}$, Wang *et al.*'s algorithms [23], [24], Hu et al's algorithm [13], and Zhang *et al.*'s algorithm [32].

In terms of security, Hu *et al.*'s algorithm [13] is designed for a non-standard $\mathcal{CSR}$ algorithm under the semi-honest cloud server model and doesn't consider the privacy of the measurement sample $\mathbf{y}$. Zhang *et al.*'s algorithm [32] just employs the standard $\mathcal{CSR}$ algorithm to realize the protection of $\mathbf{x}$ under the malicious cloud server model. As they stated, the $\mathcal{CSR}$ algorithm inherently protects the privacy of $\mathbf{x}$ without any encryption operation in an outsourcing setting. That is, the local client can directly send $(\mathbf{y}, \mathbf{H})$ to the cloud S and keep the matrices $\mathbf{A}$ and $\mathbf{D}$ secret. Therefore, Zhang *et al.* [32] don't care about the input privacy of $(\mathbf{y}, \mathbf{H})$ and the output privacy of $\mathbf{s}$. Wang *et al.* [23], [24] subsequently proposed two outsourcing $\mathcal{CSR}$ algorithms for image reconstruction and healthcare services under the semi-honest cloud server model. Their algorithms are designed for general signals and are closely related to our work. These two outsourcing algorithms utilize similar encryption techniques and simultaneously realize the privacy preservation of $\mathbf{y}$, $\mathbf{H}$, $\mathbf{s}$ and $\mathbf{x}$. As a summary, we compare the security of the above algorithms with that of our algorithm in Table 2.

In terms of efficiency, it is unfair and meaningless to compare two algorithms towards to different privacy preservation goals. From Table 2, the security intentions of Hu *et al.*'s and Zhang *et al.*'s algorithms [13], [32] are evidently different from those of ours, so we only compare our algorithm with Wang's algorithms [23], [24]. As mentioned above, Wang *et al.*'s two algorithms utilize similar encryption techniques. Without loss of generality, Table 3 shows the theoretical efficiency comparison between our algorithm and Wang's latest version [24], where $t_{\mathbf{KenGen}}, t_{\mathbf{ProbEnc}}, t_{\mathbf{VeDec}}$ and $t_{\mathbf{total}}$ denote the time cost of the key generation stage, the time cost of the problem encryption stage, the time cost of the result verification and decryption stage, and the total cost of these three stages on the local side, respectively. Since the verifiability parameter k is a constant independent of m, n, it can be seen that, for each stage, our algorithm is more theoretically efficient than Wang's algorithm [24].

C. EXPERIMENTAL ANALYSIS AND COMPARISON

Finally, we evaluate the actual performance of our algorithm with extensive experiments and the comparison with Wang *et al.*'s algorithm [24].

1) EXPERIMENTAL ENVIRONMENT AND METHODOLOGY

In our experiments, we simulate the operations of medical image acquisition client C, disease diagnosis doctor D and cloud server S on a Windows 10 machine with Intel(R) Core(TM) i5-8500T 2.11GHz CPU and 8GB RAM by using Matlab R2019b.

Our experiments are proceeded as two parts: In the first part, we mainly focus on the efficiency of our algorithm. We compare the local client's time cost of our outsourcing algorithm with that of the original algorithm without outsourcing. In the second part, we mainly compare the local client's time cost of our algorithm with that of Wang *et al.*'s algorithm [24].

2) EXPERIMENTAL RESULTS AND ANALYSIS

In our experiments, we choose the size n of the medical images $\mathbf{x}$ to be 500, 1000, 1500, 2000, and 2500 respectively, and set $m = \frac{2}{5}n$, $k = 50$. Table 4 lists the time cost of each stage and several important ratios that are used to measure the performance of the algorithm, out of which, t_{original} represents the time cost of solving the original convex optimization problem, $t_{\mathbf{KeyGen}}$ and $t_{\mathbf{ProbEnc}}$ refer to the client C's time cost of key generation stage and the cost of encryption stage respectively, $t_{\mathbf{VeDec}}$ denotes the doctor D's time cost in the verification and decryption stage, $t_{\text{total}} = t_{\mathbf{KeyGen}}+t_{\mathbf{ProbEnc}}+t_{\mathbf{VeDec}}$ is the total time cost of C and D induced by our outsourcing design, and t_{cloud} represents the time for the cloud server S to solve the encrypted convex optimization problem.

As reflected in the table, the total time cost t_{total} on the local side is always far less than t_{original} that refers to the time cost of directly solving the convex optimization problem without outsourcing, and the ratio $t_{\text{original}}/t_{\text{total}}$ becomes larger and larger, which indicate that, as the enlargement of the image size n, the local client can achieve more computational savings and our outsourcing algorithm becomes more efficient. At the same time, the ratio $t_{\text{cloud}}/t_{\text{original}}$ is close to 1, which means that the time cost t_{cloud} of solving the encrypted convex optimization problem is approximate to that of solving the original convex optimization problem. This shows that our outsourcing algorithm with encryption does not cause too much additional lease fee to rent the cloud server compared with the algorithm of directly outsourcing without encryption.

In addition, we experimentally compare our algorithm with Wang *et al.*'s algorithm [24]. We also choose the size n of the medical images $\mathbf{x}$ to be 500, 1000, 1500, 2000, and 2500, and record the time costs of the two algorithms on the local side. Visually, we plot the comparison results in Fig.2 and Fig.3.

TABLE 2. Comparison on the security of existing algorithms.

Existing algorithms	$\mathbf{H}$	$\mathbf{y}$	$\mathbf{s}$	$\mathbf{x}$	Cloud	Verifiability
Wang et al.'s algorithm [23, 24]	Protected	Protected	Protected	Protected	Semi-honest	No
Hu et al.'s algorithm [13]	Protected	Unprotected	Protected	Protected	Semi-honest	No
Zhang et al.'s algorithm [32]	Unprotected	Unprotected	Unprotected	Protected	Malicious	Yes
Our algorithm	Protected	Protected	Protected	Protected	Malicious	Yes

TABLE 3. Comparison on the efficiency between Wang et al's algorithm and ours.

Existing algorithms	$t_{\mathbf{KenGen}}$	$t_{\mathbf{ProbEnc}}$	$t_{\mathbf{VeDec}}$	$t_{\mathbf{total}}$
Wang et al.'s algorithm [24]	$O(n^2+mn+m^2+n)$	$O(n^3+mn^2+m^2n+m^2+mn)$	$O(n^2)$	$O(n^3+mn^2)$
Our algorithm	$O(n+(m+k)^2+k^2)$	$O((m+k)(mn+k^2))$	$O(n+k)$	$O(m^2n+n)$

TABLE 4. Experimental results (unit: second).

image size (n)	$t_{\mathbf{KeyGen}}$	$t_{\mathbf{ProbEnc}}$	$t_{\mathbf{VeDec}}$	t_{total}	t_{original}	t_{cloud}	$t_{\text{original}}/t_{\text{total}}$	$t_{\text{cloud}}/t_{\text{original}}$
500	0.00106	0.00424	0.00016	0.00546	1.08572	1.63968	198.84981	1.51022
1000	0.00254	0.01038	0.00028	0.01320	6.15940	8.74478	466.62121	1.41975
1500	0.00456	0.02332	0.00003	0.02818	23.18452	28.63022	822.72959	1.23489
2000	0.00700	0.04952	0.00026	0.05678	53.65018	63.41148	944.87813	1.18194
2500	0.01028	0.08950	0.00034	0.10012	107.16556	129.24888	1070.37115	1.20606

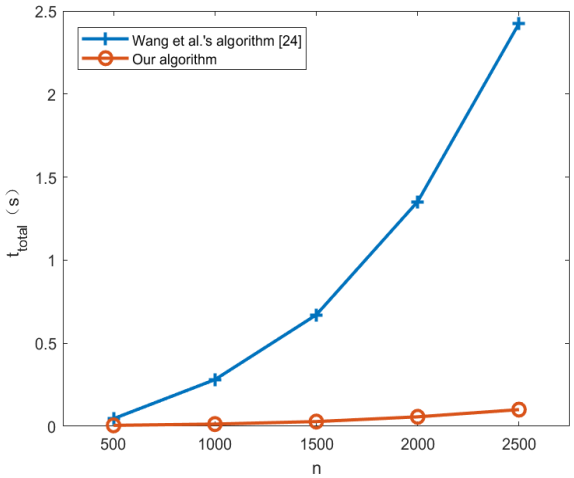


FIGURE 2. The comparison of local client's time cost of the algorithms.

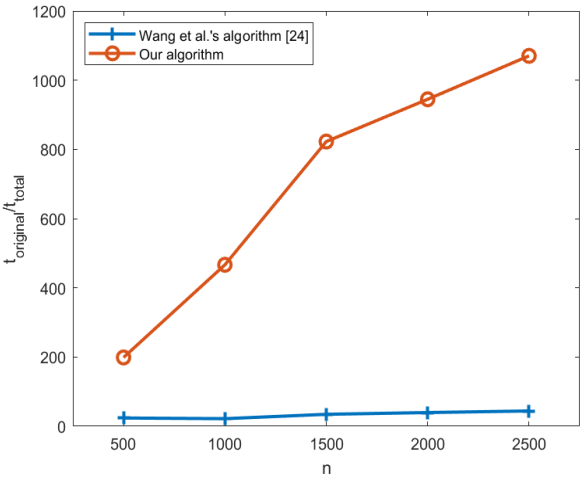


FIGURE 3. The comparison of the efficiency of the algorithms.

Fig.2 depicts the variance of the local client's total time cost t_{total} with the enlargement of the size n of the medical images, which shows that the local client's time cost of our algorithm is far less than that of Wang's algorithm. Fig.3 compares the speedup ratio $t_{\text{original}}/t_{\text{client}}$ of the two algorithms under the same experimental settings, which shows that our algorithm can achieve more computational savings than Wang *et al.*'s algorithm.

VII. CONCLUSION

In this paper, we design a secure outsourcing algorithm for $\mathcal{CSR}$ of medical images. This algorithm enables the medical institute and the doctor to securely store and reconstruct the medical images with the help of a cloud server. In addition to keeping the privacy of the original image and the input/output information of the reconstruction process, our design also can enable the doctor to detect the correctness of the result sent from the cloud with a probability of approximating 1. Finally, we theoretically and experimentally analyze the efficiency of the proposed outsourcing algorithm.

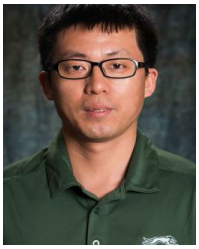
REFERENCES

[1] R. G. Baraniuk, "Compressive sensing [lecture notes]," *IEEE Signal Process. Mag.*, vol. 24, no. 4, pp. 118–121, Jul. 2007.
[2] M. Bóna, *Combinatorics Permutations*. Boca Raton, FL, USA: CRC Press, 2012.
[3] E. J. Candès, "The restricted isometry property and its implications for compressed sensing," *Comp. Rendus Math.*, vol. 346, nos. 9–10, pp. 589–592, May 2008.
[4] 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.
[5] 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.
[6] 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.
[7] X. Chai, H. Wu, Z. Gan, D. Han, Y. Zhang, and Y. Chen, "An efficient approach for encrypting double color images into a visually meaningful cipher image using 2D compressive sensing," *Inf. Sci.*, vol. 556, pp. 305–340, May 2021.
[8] F. Chen, T. Xiang, and Y. Yang, "Privacy-preserving and verifiable protocols for scientific computation outsourcing to the cloud," *J. Parallel Distrib. Comput.*, vol. 74, no. 3, pp. 2141–2151, 2014.

[9] W. Dai and O. Milenkovic, "Subspace pursuit for compressive sensing signal reconstruction," *IEEE Trans. Inf. Theory*, vol. 55, no. 5, pp. 2230–2249, May 2009.
[10] A. Divekar and O. Ersoy, "Compact storage of correlated data for content based retrieval," in *Proc. Conf. Rec. 43rd Asilomar Conf. Signals, Syst. Comput.*, Nov. 2009, pp. 109–112.
[11] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.
[12] F. Emekci, A. Methwally, D. Agrawal, and A. E. Abbadi, "Dividing secrets to secure data outsourcing," *Inf. Sci.*, vol. 263, pp. 198–210, Apr. 2014.
[13] G. Hu, D. Xiao, T. Xiang, S. Bai, and Y. Zhang, "A compressive sensing based privacy preserving outsourcing of image storage and identity authentication service in cloud," *Inf. Sci.*, vol. 387, pp. 132–145, May 2017.
[14] A. J. Jerri, "The Shannon sampling theorem—Its various extensions and applications: A tutorial review," *Proc. IEEE*, vol. 65, no. 11, pp. 1565–1596, Nov. 1977.
[15] G. Kuldeep and Q. Zhang, "Compressive sensing based multi-class privacy-preserving cloud computing," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2020, pp. 1–6.
[16] X. Lei, X. Liao, T. Huang, and F. Heriniaina, "Achieving security, robust cheating resistance, and high-efficiency for outsourcing large matrix multiplication computation to a malicious cloud," *Inf. Sci.*, vol. 280, pp. 205–217, Oct. 2014.
[17] H. Liu, H. Zhang, L. Guo, J. Yu, and J. Lin, "Privacy-preserving cloud-aided broad learning system," *Comput. Secur.*, vol. 112, Jan. 2022, Art. no. 102503.
[18] J. Liu, Z. Tang, N. Sun, G. Han, and S. Kwong, "Visual privacy-preserving level evaluation for multilayer compressed sensing model using contrast and salient structural features," *Signal Process., Image Commun.*, vol. 89, Nov. 2020, Art. no. 115996.
[19] A. Orsdemir, H. O. Altun, G. Sharma, and M. F. Bocko, "On the security and robustness of encryption via compressed sensing," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Nov. 2008, pp. 1–7.
[20] Y. Rachlin and D. Baron, "The secrecy of compressed sensing measurements," in *Proc. 46th Annu. Allerton Conf. Commun., Control, Comput.*, Sep. 2008, pp. 813–817.
[21] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," *IEEE Internet Comput.*, vol. 16, no. 1, pp. 69–73, Jan./Feb. 2012.
[22] C. Tian, J. Yu, H. Zhang, H. Xue, C. Wang, and K. Ren, "Novel secure outsourcing of modular inversion for arbitrary and variable modulus," *IEEE Trans. Services Comput.*, vol. 15, no. 1, pp. 241–253, Jan. 2022.
[23] 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.
[24] 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. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2014, pp. 2130–2138.
[25] M. Wang, D. Xiao, and J. Liang, "Low complexity secure P-tensor product compressed sensing reconstruction outsourcing and identity authentication in cloud," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Jun. 2021, pp. 2630–2634.
[26] Z. Wang, Z. S. Hussein, and X. Wang, "Secure compressive sensing of images based on combined chaotic DWT sparse basis and chaotic DCT measurement matrix," *Opt. Lasers Eng.*, vol. 134, Nov. 2020, Art. no. 106246.
[27] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, "Edge computing security: State of the art and challenges," *Proc. IEEE*, vol. 107, no. 8, pp. 1608–1631, Aug. 2019.
[28] W. Xue, C. Luo, Y. Shen, R. Rana, G. Lan, S. Jha, A. Seneviratne, and W. Hu, "Towards a compressive-sensing-based lightweight encryption scheme for the Internet of Things," *IEEE Trans. Mobile Comput.*, vol. 20, no. 10, pp. 3049–3065, Oct. 2021.
[29] X. Yuan, X. Wang, C. Wang, J. Weng, and K. Ren, "Enabling secure and fast indexing for privacy-assured healthcare monitoring via compressive sensing," *IEEE Trans. Multimedia*, vol. 18, no. 10, pp. 2002–2014, Oct. 2016.
[30] F. Zhang, X. Ma, and S. Liu, "Efficient computation outsourcing for inverting a class of homomorphic functions," *Inf. Sci.*, vol. 286, pp. 19–28, Dec. 2014.
[31] H. Zhang, P. Gao, J. Yu, J. Lin, and N. Xiong, "Machine learning on cloud with blockchain: A secure, verifiable and fair approach to outsource the linear regression for data analysis," *IEEE Trans. Netw. Sci. Eng.*, early access, Sep. 3, 2021, doi: 10.1109/TNSE.2021.3110101.
[32] Y. Zhang, Y. Xiang, L. Y. Zhang, L.-X. Yang, and J. Zhou, "Efficiently and securely outsourcing compressed sensing reconstruction to a cloud," *Inf. Sci.*, vol. 496, pp. 150–160, Sep. 2019.
[33] Y. Zhang, L. Y. Zhang, J. Zhou, L. Liu, F. Chen, and X. He, "A review of compressive sensing in information security field," *IEEE Access*, vol. 4, pp. 2507–2519, 2016.
[34] 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)*, Nov. 2015, pp. 1–6.
[35] Y. Zheng, C. Tian, H. Zhang, J. Yu, and F. Li, "Lattice-based weak-key analysis on single-server outsourcing protocols of modular exponentiations and basic countermeasures," *J. Comput. Syst. Sci.*, vol. 121, pp. 18–33, Nov. 2021.

XIN SUN received the B.E. degree in information security from Qingdao University, in 2019, where he is currently pursuing the M.S. degree with the College of Computer Science and Technology. His research interests include cloud computing security and cryptography.

CHENGLIANG TIAN received the B.S. and M.S. degrees in mathematics from Northwest University, Xi'an, China, in 2006 and 2009, respectively, and the Ph.D. degree in information security from Shandong University, Ji'nan, China, in 2013. He held a postdoctoral position with the State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing. He is currently an Associate Professor with the College of Computer Science and Technology, Qingdao University. His research interests include lattice-based cryptography and cloud computing security.



WEIZHONG TIAN received the B.S. degree in information and computing science from Northwest A&F University, Yangling, China, in 2006, the M.S. degree in computational mathematics from Northwest University, Xi'an, China, in 2009, and the M.S. and Ph.D. degrees in statistics from New Mexico State University, Las Cruces, NM, USA, in 2012 and 2015, respectively. He has been working as an Assistant Professor with the Department of Mathematical Sciences, Eastern New Mexico University, since 2016. He is currently working as an Associate Professor with the College of Big Data and Internet, Shenzhen Technology University. His research interests include the family of skew slash distribution, matrix variate distribution, tail dependence, and change point detection.

YAN ZHANG received the B.S. degree in computer science and technology from Northwestern Polytechnical University, Xi'an, China, in 2004, and the M.S. and Ph.D. degrees in automatic control from the Qingdao University of Science and Technology, Qingdao, China, in 2009 and 2014, respectively. He was a Visiting Scholar with the Research Group on Electrical Engineering and Automatic Control (GREAH), Faculty of Sciences, Normandy University, Le Havre, France, from 2014 to 2015. He is currently an Associate Professor of electrical and computer engineering with Qingdao University of Science and Technology. His research interests include digital image processing, pattern recognition, and nondestructive testing.