Secure Dictionary Learning for Sparse Representation

Takayuki Nakachi
NTT Network Innovation Laboratories
Nippon Telegraph and Telephone Corp.
Yokosuka-city Kanagawa, Japan
takayuki.nakachi.pu@hco.ntt.co.jp

Yukihiro Bandoh
NTT Media Intelligence Laboratories
Nippon Telegraph and Telephone Corp.
Yokosuka-city Kanagawa, Japan
yukihiro.bandoh.pe@hco.ntt.co.jp

Hitoshi Kiya
Information and Communication Systems
Tokyo Metropolitan University
Hino-city Tokyo, Japan
kiya@tmu.ac.jp

***Abstract*—In this paper, we propose secure dictionary learning for sparse representation based on a random unitary transform. Edge cloud computing is now spreading to many application fields including services that use sparse coding. This situation raises many new privacy concerns. The proposed scheme provides practical MOD and K-SVD schemes that allow computation on encrypted signals. We prove, theoretically, that the proposal has exactly the same dictionary and sparse coefficient estimation performance as sparse dictionary learning for unencrypted signals. It can be directly carried out by using MOD and K-SVD algorithms. Moreover, we apply it to image modeling based on an image patch model. Finally, we demonstrate its excellent performance on synthetic data and natural images.**

***Index Terms*—Sparse Representation, Dictionary Learning, Random Unitary Transform, Secure Computation**

I. Introduction

With the advent of the big data era, digital contents continue to explode. Sparse modeling [1]- [6] is drawing attention as an information processing model for extracting useful information hidden in a large amount of data. It represents observed signals effectively as a linear combination of a small number of bases chosen from the basis functions trained by the dictionary learning algorithm. The sparse coding model has found numerous processing applications such as image/video, audio, biological signal, seismic data and more [2].

In another trend, edge cloud computing including big data analysis is spreading in many fields. However, edge cloud computing has some serious issues for end users, such as unauthorized use, leak of data, and privacy compromisation, due to the unreliability of providers and some accident [7]. Many studies have examined the processing of encrypted data; most proposals use homomorphic encryption (HE) and secure multiparty computation (MPC) [8]. Even though service providers cannot directly access the native content of the encrypted signals, they can still employ HE and MPC. However, these schemes can not be applied yet to sparse coding algorithms. Moreover, it imposes high computation complexity and large cipher text size, so further advances are needed for some applications such as big data analysis, advanced image/video processing.

Our study focuses on secure computation that is practical. The proposed scheme, based on a random unitary transform, has much lower computation complexity than either HE or MPC. We have already proposed a secure Orthogonal Matching Pursuit (OMP) computation method for image modeling [9] and network BMI decoding [10]. Secure OMP can estimate the sparse coefficients from encrypted signals.

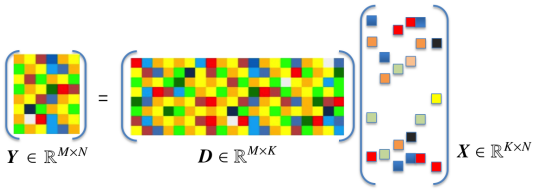


Fig. 1. Sparse coding: observed signals effectively are represented as a linear combination of a small number of bases.

In this paper, we propose a secure sparse dictionary learning method. Method of Optimal Direction (MOD) [4] and K-Singular Value Decomposition (K-SVD) [5] are well-known dictionary learning algorithms which seek to create dictionaries that fit the observed signals. The proposed scheme provides practical MOD and K-SVD schemes that allow computation on encrypted signals. It is shown that secure dictionary learning can not only protect observed signals, but also match the estimation performance of sparse dictionary learning for unencrypted signals. It can be directly carried out by using MOD and K-SVD algorithms, without preparing any algorithms specialized for secure MOD and K-SVD computing. Moreover, we apply it to image modeling based on an image patch model. Finally, we demonstrate its performance on both synthetic data and natural images.

The organization of this paper is as follows. Section II overviews dictionary learning. In Sec. III, we propose a secure MOD and K-SVD computation process. Section IV introduces its application to image modeling. Section V shows simulation results. Conclusions are given in Sec. VI.

II. Overview of Dictionary Learning

In this section, we overview dictionary learning and two representative algorithms (MOD and K-SVD).

A. Sparse Representation

Given observed signal set $\boldsymbol{Y} = \{\boldsymbol{y}_i\}_{i=1}^{N} \in \mathbb{R}^{M\times N}$, we assume that there exists an over-complete dictionary matrix $\boldsymbol{D} = \{\boldsymbol{d}_1, ..., \boldsymbol{d}_K\} \in \mathbb{R}^{M\times K}$, whose columns contain K

978-9-0827-9703-9/19/$31.00 ©2019 IEEE

prototype signal-atoms $\boldsymbol{d}_k$. As shown in Fig. 1, $\boldsymbol{Y}$ can be represented as a sparse linear combination of these atoms:

$$\boldsymbol{Y} = \boldsymbol{D}\boldsymbol{X}, \tag{1}$$

where $\boldsymbol{X} = \{\boldsymbol{x}_i\}_{i=1}^N \in \mathbb{R}^{K\times N}$ is a sparse coefficients set.

If $M < K$ and $\boldsymbol{D}$ is a full-rank matrix, an infinite number of solutions to the representation problem are available. The solution with the fewest number of nonzero coefficients is certainly an appealing representation. This sparsest representation is the solution given by

$$\min_{\boldsymbol{D},\boldsymbol{X}} ||\boldsymbol{Y} - \boldsymbol{D}\boldsymbol{X}||_F^2 \quad \text{subject to } \forall i, \quad ||\boldsymbol{x}_i||_0 \le T_0, \tag{2}$$

where $||\cdot||_0$ is the l_0-norm which counts the nonzero entries of the vector, $||\boldsymbol{A}||_F = \sqrt{\sum_{ij} A_{ij}^2}$.

Sparse dictionary learning solves the optimization problem of Eq. (2) by alternately repeating two steps: 1) Sparse Coding and 2) Dictionary Update. The Sparse Coding step fixes dictionary $\boldsymbol{D}$ and estimates sparse coefficients set $\boldsymbol{X}$. Dictionary Update step fixes $\boldsymbol{X}$ and updates dictionary $\boldsymbol{D}$. MOD and K-SVD are well known sparse dictionary learning algorithms. MOD and K-SVD use the same Sparse Coding step, the method of updating the dictionary is different. The following is an overview of the dictionary learning algorithm:

Dictionary Learning Algorithm

Task: Train a dictionary $\boldsymbol{D}$ to sparsely represent the data $\boldsymbol{Y} = \{\boldsymbol{y}_i\}_{i=1}^N$ by approximating the solution to the problem posed in Eq. (2).

Initialization: Set the dictionary matrix $\boldsymbol{D} \in \mathbb{R}^{M\times K}$ with l^0 normalized columns.

Main Iteration: Repeat until convergence (stopping rule):

· **Sparse Coding Step:** Use a pursuit algorithm such as Orthogonal Matching Pursuit (OMP) [6], to approximate the solution of

$$\boldsymbol{x}_i = \arg\min_x ||\boldsymbol{y}_i - \boldsymbol{D}\boldsymbol{x}_i||_2^2 \quad \text{subject to} \quad ||\boldsymbol{x}_i||_0 \le T_0. \tag{3}$$

· **Dictionary Update Step:** Update $\boldsymbol{D}$ by MOD or K-SVD. Each dictionary update step is below.

B. MOD Dictionary Update Step

MOD uses a pseudo inverse to minimize the squared error between $\boldsymbol{Y}$ and $\boldsymbol{D}\boldsymbol{X}$. Update the dictionary by the formula:

$$\boldsymbol{D} = \arg\min_D ||\boldsymbol{Y} - \boldsymbol{D}\boldsymbol{X}||_F^2 = \boldsymbol{Y}\boldsymbol{X}^T(\boldsymbol{X}\boldsymbol{X}^T)^{-1}. \tag{4}$$

C. K-SVD Dictionary Update Step

Unlike MOD, K-SVD updates one atom sequentially. Each atom $\boldsymbol{d}_k$ ($k = 1, 2, \cdots, K$ in $\boldsymbol{D}$) is updated by the following steps:

1) Compute the overall representation error matrix $\boldsymbol{E}_k$ by

$$\boldsymbol{E}_k = \boldsymbol{Y} - \sum_{j\neq k}^{K} \boldsymbol{d}_j \boldsymbol{x}_T^j, \tag{5}$$

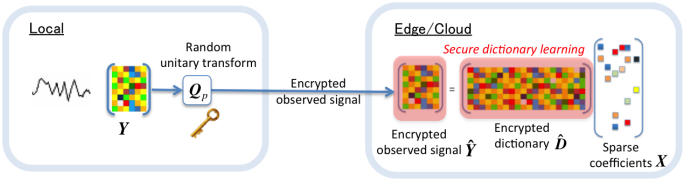


Fig. 2. Secure dictionary learning architecture.

where $\boldsymbol{x}_T^j$ is the jth row in $\boldsymbol{X}$.

2) Define the group of examples that use this atom:

$$\omega_k = \{i \mid 1 \le i \le K, \quad \boldsymbol{x}_T^k(i) \neq 0\}. \tag{6}$$

Restrict $\boldsymbol{E}_k$ by choosing only the columns corresponding to ω_k, and obtain $\boldsymbol{E}_k^R$.

3) Apply Singular Value Decomposition (SVD):

$$\boldsymbol{E}_k^R = \boldsymbol{U}\boldsymbol{\Delta}\boldsymbol{V}^T = \sum_{i=1}^{n} \boldsymbol{u}_i \cdot \sigma_i \boldsymbol{v}_i^T. \tag{7}$$

Choose the updated dictionary atom $\boldsymbol{d}_k$ to be the first column $\boldsymbol{u}_1$. Updated coefficient vector $\boldsymbol{x}_R^k$, taken as the first column, is multiplied by the first eigenvalue: $\sigma_1 \boldsymbol{v}_1^T$.

III. Secure Dictionary Learning

In this section, we propose secure dictionary learning (MOD and K-SVD) that allows computation in the encrypted domain.

A. Random Unitary Transform

Vector $\boldsymbol{f}_i$ $(i = 1, \cdots, L) \in \mathbb{R}^N$ is encrypted by random unitary matrix $\boldsymbol{Q}_p \in \mathbb{C}^{N\times N}$ with private key p as follows:

$$\hat{\boldsymbol{f}}_i = T(\boldsymbol{f_i}, p) = \boldsymbol{Q}_p \boldsymbol{f_i}, \tag{8}$$

where $\hat{\boldsymbol{f}}_{\boldsymbol{i}}$ is an encrypted vector; L is the number of vectors. Note that the unitary matrix that $\boldsymbol{Q}_p$ satisfies is encrypted by unitary matrix $\boldsymbol{Q}_p \in \mathbb{C}^{N\times N}$ with parameter p as

$$\boldsymbol{Q}_p^* \boldsymbol{Q}_p = \boldsymbol{I}, \tag{9}$$

where $[\cdot]^*$ and $\boldsymbol{I}$ represent the Hermitian transpose operation and the identity matrix, respectively. Gram-Schmidt orthogonalization is a typical method for generating $\boldsymbol{Q}_p$. In addition to unitarity, $\boldsymbol{Q}_p$ must offer randomness when generating the encrypted signal. Security analyses of the protection schemes have been considered in terms of brute-face attack, diversity and irreversibility [12]. The encrypted vector has the key properties of conservation of the Euclidean distances ($||\boldsymbol{f_i} - \boldsymbol{f_j}||_2^2 = ||\hat{\boldsymbol{f}}_{\boldsymbol{i}} - \hat{\boldsymbol{f}}_{\boldsymbol{j}}||_2^2$), norm isometry ($||\boldsymbol{f_i}||_2^2 = ||\hat{\boldsymbol{f}}_{\boldsymbol{i}}||_2^2$), and conservation of inner products ($\boldsymbol{f}_i^* \boldsymbol{f}_j = \hat{\boldsymbol{f}}_i^* \hat{\boldsymbol{f}}_j$).

B. Secure MOD and secure K-SVD

Figure 2 illustrates the architecture of secure dictionary learning. At the local site, the random unitary transform $\boldsymbol{Q}_p$ with private key p is applied to a given set of training signals $\boldsymbol{Y}$. The encrypted set, $\hat{\boldsymbol{Y}}$, is sent to the edge or cloud site. By using only the encrypted set $\hat{\boldsymbol{Y}}$, the secure dictionary learning method designs the encrypted dictionary $\hat{\boldsymbol{D}}$ in the encrypted domain. The encrypted set $\hat{\boldsymbol{Y}}$ is generated by

$$\hat{\boldsymbol{Y}} = T(\boldsymbol{Y}, p) = \boldsymbol{Q}_p \boldsymbol{Y}. \tag{10}$$

Here we consider the following optimization problem:

$$\min_{\hat{\boldsymbol{D}},\boldsymbol{X}} \left|\left|\hat{\boldsymbol{Y}} - \hat{\boldsymbol{D}}\boldsymbol{X}\right|\right|_F^2 \quad \text{subject to } \forall i, \quad ||\boldsymbol{x}_i||_0 \leq T_0, \tag{11}$$

where $\hat{\boldsymbol{D}} = \{\hat{\boldsymbol{d}}_1, ..., \hat{\boldsymbol{d}}_K\} \in \mathbb{R}^{M\times K}$ is an encrypted dictionary.

1) Sparse Coding Step: In Sparse Coding step, fix dictionary $\hat{\boldsymbol{D}}$ and estimate sparse coefficients set $\boldsymbol{X}$ by solving Eq.(11). We use OMP to approximate the solution of

$$\boldsymbol{x}_i = \arg\min_{\boldsymbol{x}_i} \left|\left|\hat{\boldsymbol{y}}_i - \hat{\boldsymbol{D}}\boldsymbol{x}_i\right|\right|_F^2 \quad \text{subject to} \quad ||\boldsymbol{x}_i||_0 \leq T_0. \tag{12}$$

Previously, we proved that the solution obtained by solving Eq. (12) by OMP is equal to the solution yielded by the unencrypted variant of the OMP algorithm [9]- [10] under the condition $\hat{\boldsymbol{D}} = \boldsymbol{Q}_p\boldsymbol{D}$.

2) Secure MOD Dictionary Update Step: Update the encrypted dictionary $\hat{\boldsymbol{D}}$ by the formula:

$$\hat{\boldsymbol{D}} = \arg\min_{\hat{D}} \left|\left|\hat{\boldsymbol{Y}} - \hat{\boldsymbol{D}}\boldsymbol{X}\right|\right|_F^2 = \hat{\boldsymbol{Y}}\boldsymbol{X}^T(\boldsymbol{X}\boldsymbol{X}^T)^{-1}. \tag{13}$$

From the definition $\hat{\boldsymbol{Y}} = \boldsymbol{Q}_p\boldsymbol{Y}$, Eq. (13) can be rewritten as

$$\hat{\boldsymbol{D}} = \boldsymbol{Q}_p\boldsymbol{Y}\boldsymbol{X}^T(\boldsymbol{X}\boldsymbol{X}^T)^{-1}. \tag{14}$$

3) Secure K-SVD Dictionary Update Step: Similar to the derivation of the unencrypted version of K-SVD, the overall representation error matrix $\hat{\boldsymbol{E}}_k$ is written by

$$\hat{\boldsymbol{E}}_k = \hat{\boldsymbol{Y}} - \sum_{j\neq k}^{K} \hat{\boldsymbol{d}}_j \boldsymbol{x}_T^j. \tag{15}$$

Restrict $\hat{\boldsymbol{E}}_k$ by choosing only the columns corresponding to ω_k, and obtain $\hat{\boldsymbol{E}}_k^R$. Apply SVD:

$$\hat{\boldsymbol{E}}_k^R = \hat{\boldsymbol{U}}\hat{\boldsymbol{\Delta}}\hat{\boldsymbol{V}}^{\boldsymbol{T}} = \sum_{i=1}^{n} \hat{\boldsymbol{u}}_i \cdot \hat{\sigma}_i \hat{\boldsymbol{v}}_i^T. \tag{16}$$

Choose the updated dictionary atom $\hat{\boldsymbol{d}}_k$=$\hat{\boldsymbol{u}}_1$. Update coefficient vector $\boldsymbol{x}_R^k$ = $\hat{\sigma}_1\hat{\boldsymbol{v}}_1^T$.

Next, we show the relationship between the solution obtained by K-SVD (i.e. $\boldsymbol{d}_k$=$\boldsymbol{u}_1$, $\boldsymbol{x}_R^k$ = $\sigma_1\boldsymbol{v}_1^T$) and the solution obtained by secure K-SVD (i.e. $\hat{\boldsymbol{d}}_k$=$\hat{\boldsymbol{u}}_1$, $\hat{\boldsymbol{x}}_R^k$ = $\hat{\sigma}_1\hat{\boldsymbol{v}}_1^T$) . Similar to the derivation of the unencrypted version of K-SVD, the overall representation error matrix $\hat{\boldsymbol{E}}_k$ of Eq. (15) can be written as

$$\hat{\boldsymbol{E}}_k \quad = \quad \hat{\boldsymbol{Y}} - \sum_{j\neq k}^{K} \hat{\boldsymbol{d}}_j \boldsymbol{x}_T^j = \boldsymbol{Q}_p\boldsymbol{E}_k, \tag{17}$$

where we assume that $\hat{\boldsymbol{d}}_j$=$\boldsymbol{Q}_p\boldsymbol{d}_j$, which is derived from the condition $\hat{\boldsymbol{D}} = \boldsymbol{Q}_p\boldsymbol{D}$ [9]- [10] in the Sparse Coding step. From Eq. (17), $\hat{\boldsymbol{E}}_k^R$ can be written as

$$\hat{\boldsymbol{E}}_k^R \quad = \quad \hat{\boldsymbol{E}}_k\boldsymbol{\Omega}_K = \boldsymbol{Q}_p\boldsymbol{E}_k\boldsymbol{\Omega}_K = \boldsymbol{Q}_p\boldsymbol{E}_k^R. \tag{18}$$

Furthermore, by using Eq. (7), Eq. (18) can be rewritten as follows:

$$\hat{\boldsymbol{E}}_k^R = \boldsymbol{Q}_p\boldsymbol{E}_k^R = \boldsymbol{Q}_p \sum_{i=1}^{n} \boldsymbol{u}_i \cdot \sigma_i \boldsymbol{v}_i^T. \tag{19}$$

Therefore, the dictionary atom and the sparse coefficients of the encrypted version of K-SVD can be expressed by using that of the non-encrypted version of K-SVD as follows:

$$\cdot\text{Sparse coefficients}: \quad \hat{\boldsymbol{x}}_R^k = \sigma_1\boldsymbol{v}_1^T \tag{20}$$

$$\cdot\text{Dictionary atom}: \quad \hat{\boldsymbol{d}}_k = \boldsymbol{Q}_p\boldsymbol{u}_1 \tag{21}$$

4) Proof of Eq. (20): From Eq. (16), $\hat{\boldsymbol{v}}_i$ is the i-th eigenvector of $\left(\hat{\boldsymbol{E}}_k^R\right)^T\hat{\boldsymbol{E}}_k^R$ and can be written as:

$$\left(\hat{\boldsymbol{E}}_k^R\right)^T\hat{\boldsymbol{E}}_k^R\hat{\boldsymbol{v}}_i \quad = \quad \hat{\lambda}_i\hat{\boldsymbol{v}}_i, \tag{22}$$

where $\hat{\lambda}_i$ is the i-th eigenvalue. $\hat{\lambda}_i$ and the singular value $\hat{\sigma}_i$ have the relationship of $\hat{\sigma}_i = \sqrt{\hat{\lambda}_i}$. By using relationship $\hat{\boldsymbol{E}}_k^R = \boldsymbol{Q}_p\boldsymbol{E}_k^R$, the left side of Eq. (22) can be expressed as

$$\left(\hat{\boldsymbol{E}}_k^R\right)^T \hat{\boldsymbol{E}}_k^R = \left(\boldsymbol{E}_k^R\right)^T\boldsymbol{Q}_p^T\boldsymbol{Q}_p\boldsymbol{E}_k^R = \left(\boldsymbol{E}_k^R\right)^T\boldsymbol{E}_k^R. \tag{23}$$

Since $\left(\hat{\boldsymbol{E}}_k^R\right)^T\hat{\boldsymbol{E}}_k^R$ and $\left(\boldsymbol{E}_k^R\right)^T\boldsymbol{E}_k^R$ are equal, each eigenvector is also equal:

$$\hat{\boldsymbol{v}}_i = \boldsymbol{v}_i. \tag{24}$$

Therefore, Eq. (20) is satisfied.

5) Proof of Eq. (21): In SVD of $\hat{\boldsymbol{E}}_k^R$ shown in Eq. (16), the eigenvectors on the left side $\hat{\boldsymbol{u}}_i$ and the eigenvectors on the right side $\hat{\boldsymbol{v}}_i$ have the relationship: $\hat{\boldsymbol{u}}_i = \pm\hat{\boldsymbol{E}}_k^R\hat{\boldsymbol{v}}_i/\sqrt{\hat{\lambda}_i}$ (From the general property of SVD). Using this relationship, $\hat{\boldsymbol{E}}_k^R = \boldsymbol{Q}_p\boldsymbol{E}_k^R$ and Eq. (24), the first term of Eq. (16) can be expressed as follows:

$$\hat{\boldsymbol{u}}_1 \cdot \hat{\sigma_1}\hat{\boldsymbol{v}}_1^T = \frac{\pm\hat{\boldsymbol{E}}_k^R\hat{\boldsymbol{v}}_1 \cdot \hat{\sigma_1}\hat{\boldsymbol{v}}_1^T}{\sqrt{\hat{\lambda_1}}} = \pm\boldsymbol{Q}_p\boldsymbol{E}_k^R\boldsymbol{v}_1\boldsymbol{v}_1^T. \tag{25}$$

Similarly, the first term of Eq. (19) can be written as

$$\boldsymbol{Q}_p\boldsymbol{u}_1 \cdot \sigma_i\boldsymbol{v}_1^T = \frac{\pm\boldsymbol{Q}_p\boldsymbol{E}_k^R\boldsymbol{v}_1 \cdot \sigma_1\boldsymbol{v}_1^T}{\sqrt{\lambda_1}} = \pm\boldsymbol{Q}_p\boldsymbol{E}_k^R\boldsymbol{v}_1\boldsymbol{v}_1^T. \tag{26}$$

Therefore, Eq. (21) is satisfied.

IV. Application to Image Modeling

In this section, we apply the secure dictionary learning proposed in the previous section to image modeling.

A. Sparse Coding for Image Patches

We consider image patches of size $\sqrt{M}\times\sqrt{M}$ pixels that are ordered lexicographically as column vectors $\hat{\boldsymbol{y}}_i \in \mathbb{R}^M$ $(i = 1, \cdots, N)$. The patches are extracted from image $\boldsymbol{Y}$ as shown in Fig. 3. Next, each image patch $\boldsymbol{y}_i$ is transformed into encrypted image patch $\hat{\boldsymbol{y}}_i$ by random unitary transform $\boldsymbol{Q}_p$. Given the set $\hat{\boldsymbol{Y}} = \{\hat{\boldsymbol{y}}_i\}_{i=1}^N$, we assume that an encrypted image patch set $\hat{\boldsymbol{Y}}$ can be represented sparsely over the encrypted over-complete dictionary $\hat{\boldsymbol{D}} \in \mathbb{R}^{M\times K}$.

The encrypted image patch model can be used for applications such as secure image compression [9] and secure image pattern recognition [11]. Here we apply it the Encryption-then-Compression (EtC) system [13] for image compression. In conventional secure image transmission systems, image

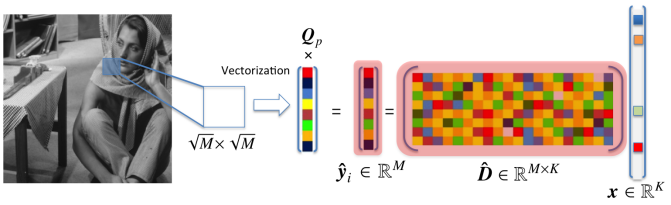


Fig. 3. Secure sparse coding of image patches.

compression has to be conducted prior to image encryption. On the other hand, EtC systems are expected to offer privacy protection as they allow image encryption to be conducted prior to compression. This approach can compress images on the edge cloud while keeping the image data secure.

B. Generation of Random Unitary Matrices

The secure dictionary learning proposed in the previous section is applied to each encrypted image patch $\hat{\boldsymbol{y}}_i$. We generate the encrypted image set $\hat{\boldsymbol{Y}}$ by the following transforms:

$$\hat{\boldsymbol{Y}} \quad = T(\boldsymbol{Y}, p) = \boldsymbol{Q}_p \boldsymbol{Y}, \tag{27}$$

where p and $\boldsymbol{Q}_p$ are a secret key and a random unitary transform, respectively. For each encrypted image patch $\hat{\boldsymbol{y}}_i$, the sparse coefficient $\boldsymbol{x}_i$ is estimated. The decoded image $\dot{\boldsymbol{y}}_i$ can be calculated by $\dot{\boldsymbol{y}}_i = \boldsymbol{Q}_p^* \hat{\boldsymbol{D}} \boldsymbol{x}_i$, where $[\cdot]^*$ means the Hermitian transpose operation.

The image quality of decoded image $\dot{\boldsymbol{y}}_i$ at each patch can be controlled by using sparsity ratio s_i or threshold ϵ_i. Sparsity ratio s_i is the ratio of the number of nonzero sparse coefficients to the total number of elements of the dictionary $\hat{\boldsymbol{D}}$. Threshold ϵ_i determines the stopping condition of the secure OMP algorithm, i.e. (l_2-norm of reconstruction error) $< \epsilon_i$. In order to keep the image quality of each image patch, the same threshold is set: ϵ_i = constant ($i = 1, \cdots, N$).

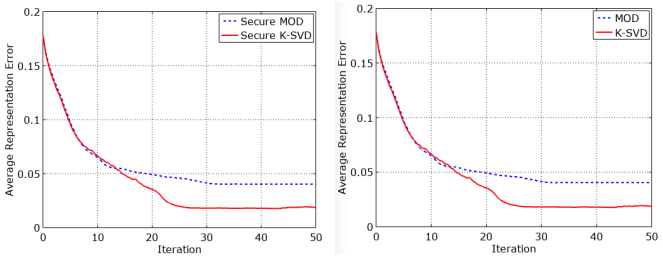
V. Numerical Demonstrations

We demonstrate the performance of the proposed method both on synthetic data and in an image modeling application involving natural images.

A. Synthetic Data

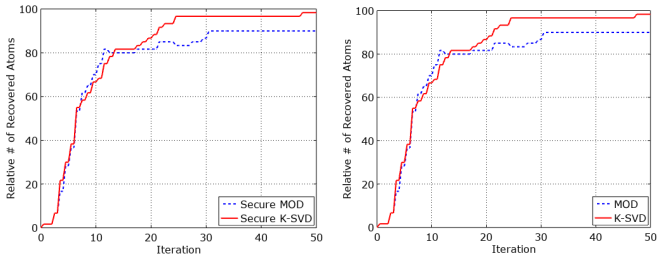
We create random matrix $\boldsymbol{D}$ of size 30×60. We generate sparse vectors $\boldsymbol{x}$. We set the target cardinality to $T_0 = 4$. Once $\boldsymbol{x}$ is generated, we compute $\boldsymbol{y} = \boldsymbol{D}\boldsymbol{x}$. We then encrypt $\boldsymbol{y}$ by using random unitary transform $\boldsymbol{Q}_p$ by designing by Gram-Schmidt orthogonalization, i.e. $\hat{\boldsymbol{y}} = \boldsymbol{Q}_p \boldsymbol{y}$. We perform 4000 such tests and present average results. We present two measures - normalized l_2-norm error and recovery of the support. Normalized l_2-norm error is computed as the ratio $||\boldsymbol{x} - \hat{\boldsymbol{x}}||^2/||\boldsymbol{x}||^2$. Recovery of the support indicates l_2 proximity between the two solutions. Denoting the two supports as $\hat{\boldsymbol{S}}$ and $\boldsymbol{S}$, we define this distance by

$$dist(\hat{\boldsymbol{S}}, \boldsymbol{S}) = \frac{max\{|\hat{\boldsymbol{S}}|, |\boldsymbol{S}|\} - |\hat{\boldsymbol{S}} \cap \boldsymbol{S}|\}}{max\{|\hat{\boldsymbol{S}}|, |\boldsymbol{S}|\}}. \tag{28}$$



(a) Secure K-SVD and MOD (b) Non-secure K-SVD and MOD

Fig. 4. Normalized l_2-norm error: $||\boldsymbol{x} - \hat{\boldsymbol{x}}||^2/||\boldsymbol{x}||^2$.



(a) Secure K-SVD and MOD (b) Non-secure K-SVD and MOD

Fig. 5. Recovery of the support: dist($\hat{\boldsymbol{S}}, \boldsymbol{S}$) .

(a) Barbara (b) Encryped image

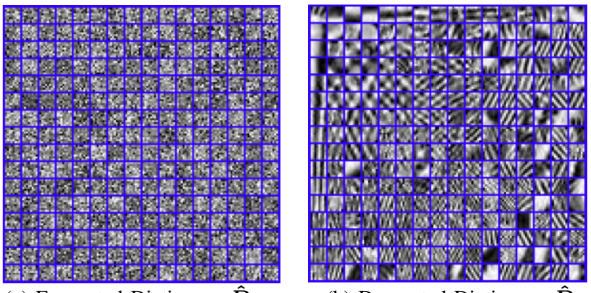
Fig. 6. Original and encrypted images.

The results are shown in Figs. 4 and 5. Horizontal axis shows iteration number. As can be seen, secure K-SVD gives better results than secure MOD, both in final outcome and speed of convergence. We compare the proposed method with the MOD and K-SVD algorithms as applied to non-encrypted signals. Figures 4 and 5 show that the proposed precisely matches the performance of the MOD and K-SVD algorithms for non-encrypted signals with regard to both measures.

B. Image Modeling

We show the practicality of the proposed algorithm by conducting image modeling experiments on natural images. We train a dictionary for sparsely representing 8×8 patches extracted from the 512×512 Barbara image. Each extracted patch is permuted randomly using a random integer generated by a secret key p. Then each patch is transformed by a 64×64 random unitary transform $\boldsymbol{Q}_p$ which is designed by Gram-Schmidt orthogonalization. Figure 6 shows the original Barbara and corresponding encrypted images.

We extract one fifth of these encrypted patches. Feeding the encrypted patch set into the secure K-SVD and secure MOD with 50 iterations yields encrypted dictionary $\hat{\boldsymbol{D}}$. In



(a) Encrypted Dictionary $\hat{\boldsymbol{D}}$ (b) Decrypted Dictionary $\hat{\boldsymbol{D}}$

Fig. 7. Dictionary designed by secure K-SVD.

TABLE I
DECODED/DECRYPTED IMAGE QUALITY BY USING SECURE K-SVD FOR AUTHORIZED AND UNAUTHORIZED USERS.

(a) Authorized user

ϵ	3.0	5.0	7.0	10.0	15.0
$\bar{S}$	0.155	0.088	0.058	0.035	0.017
PSNR [dB]	39.28	35.61	33.21	30.70	27.95

(b) Unauthorized user

ϵ	3.0	5.0	7.0	10.0	15.0
$\bar{S}$	0.155	0.088	0.058	0.035	0.017
PSNR [dB]	10.40	10.54	10.39	10.40	10.47

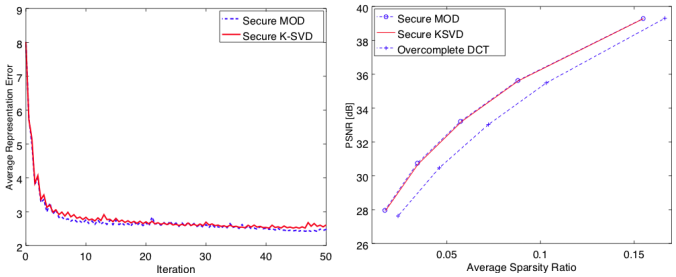
both cases, we set the number of atoms to $K = 256$ and the l_0-norm constraint T_0 to 5 atoms per patch. For example, an encrypted dictionary designed by the secure K-SVD and a corresponding decrypted dictionary are shown in Fig. 7. No visible information is present in the encrypted dictionary.

Figure 8(a) shows average convergence properties of l_2-norm error $||\hat{\boldsymbol{y}}_i - \hat{\boldsymbol{D}}\boldsymbol{x}_i||^2$. Both secure algorithms have almost the same performance. Then, by using the trained encrypted dictionaries, we use the secure OMP algorithm to carry out image modeling [9]. Figure 8(b) shows coding efficiency (the average sparsity ratio $\bar{S}$ vs. decoded/decrypted image quality PSNR [dB]) when compared with over-complete DCT. Average sparsity ratio $\bar{S}$ is defined by $\bar{S}$=$\sum_{i=1}^{N} s_i/N$. It can be seen that secure K-SVD can represent the image with fewer sparse coefficients than over-complete DCT.

Finally, we evaluate the security strength of the proposed method. Table I shows decoded/decrypted image quality attained by secure K-SVD for authorized and unauthorized (a decryption key $d_j \neq$ an encryption key d_i) users. Figure 9 shows samples of the decoded/decrypted images for authorized and unauthorized users. These results show that the encrypted images can't be decrypted by unauthorized users.

VI. CONCLUSIONS

In this paper, we proposed secure MOD and secure K-SVD computations for sparse representation. The proposed scheme provides practical MOD and K-SVD schemes that allow computation on encrypted signals. We prove, theoretically, that the proposal has exactly the same dictionary learning performance as the unencrypted variants of the MOD and K-SVD schemes. Finally, we confirmed its performance on synthetic data and natural images.



(a) Convergence (b) Coding efficiency

Fig. 8. Properties of secure MOD and secure K-SVD.

(a) ϵ = 3.0 (PSNR = 39.28 [dB]) (b) ϵ = 3.0 (PSNR = 10.40 [dB])

Fig. 9. Decoded/decrypted images by authorized (left) and unauthorized (right) users.

REFERENCES

[1] B. A. Olshausen and D. J. Field, " Emergence of simple-cell receptive-field properties by learning a sparse code for natural images, " Nature, vol. 381, pp. 607-609, 1996.

[2] Michael Elad, " Sparse and redundant representation modeling - what next?, " IEEE Signal Processing Letters, vol. 19, no. 12, pp. 922-928, Dec. 2012.

[3] B. K. Natarajan: " Sparse approximate solutions to linear systems, " SIAM J. Comput., 24, 2, pp. 227-234, 1995.

[4] K. Engan, S. O. Aase and J. Hakon Husoy: " Method of optimal directions for frame design ", ICASSP1999, pp. 2443-2446, 1999.

[5] M. Aharon, M. Elad and A. Bruckstein: " K-SVD: An algorithm for designing overcomplete dictionaries for sparse representation ", IEEE Trans. Sig. Proc., 54, 11, pp. 4311-4322, 2006.

[6] Y. C. Pati, R. Rezaiifar, Y. C. P. R. Rezaiifar and P. S. Krishnaprasad, " Orthogonal matching pursuit: Recursive function approximation with applications to wavelet decomposition", Asilomar1993, pp. 40-44, 1993.

[7] C. T. Huang, L. Huang, Z. Qin, H. Yuan, L. Zhou, V. Varad-harajan, and C-C. J. Kuo, " Survey on securing data storage in the cloud, " APSIPA Transactions on Signal and Information Processing, vol. 3, e7, 2014.

[8] R. L. Lagendijk, Z. Erkin and M. Barni, "Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation," IEEE Signal Processing Magazine, vol. 30, no. 1, pp. 82-105, Jan. 2013.

[9] Takayuki Nakachi, Hitoshi Kiya, "Practical secure OMP computation and its application to image modeling," IHIP2018, 2018.

[10] Takayuki Nakachi, Hiroyuki Ishihara, Hitoshi Kiya, "Privacy-preserving network BMI decoding of covert spatial attention," IEEE ICSPCS2018, p12, 2018.

[11] Takayuki Nakachi, Hitoshi Kiya, "Privacy-preserving Pattern Recognition using Secure Sparse Computation," ICFIP, 2019.

[12] Y. Saito, I. Nakamura, S. Shiota and H. Kiya, " An Efficient Random Unitary Matrix for Biometric Template Protection," 2016 Joint 8th International Conference on Soft Computing and Intelligent Systems (SCIS) and 17th International Symposium on Advanced Intelligent Systems (ISIS), Sapporo, 2016, pp. 366-370, 2016.

[13] T. Chuman, K. Kurihara, H. Kiya, "On the security of block scrambling-based EtC systems against extended jigsaw puzzle solver attacks," IEICE Transactions on Information and Systems, vol. E101.D, no. 1, pp. 37-44, 2018.