IEICE TRANS. INF. & SYST., VOL.E103–D, NO.1 JANUARY 2020

PAPER Special Section on Enriched Multimedia—Application of Multimedia Technology and Its Security—

Secure Overcomplete Dictionary Learning for Sparse Representation

Takayuki NAKACHI[†a)], ***Member***, **Yukihiro BANDOH**[†], ***Senior Member***, ***and*** **Hitoshi KIYA**[††], ***Fellow***

SUMMARY In this paper, we propose secure dictionary learning based on a random unitary transform for sparse representation. Currently, edge cloud computing is spreading to many application fields including services that use sparse coding. This situation raises many new privacy concerns. Edge cloud computing poses several serious issues for end users, such as unauthorized use and leak of data, and privacy failures. The proposed scheme provides practical MOD and K-SVD dictionary learning algorithms that allow computation on encrypted signals. We prove, theoretically, that the proposal has exactly the same dictionary learning estimation performance as the non-encrypted variant of MOD and K-SVD algorithms. We apply it to secure image modeling based on an image patch model. Finally, we demonstrate its performance on synthetic data and a secure image modeling application for natural images.

key words: *sparse representation, dictionary learning, random unitary transform, secure computation*

1. Introduction

With the advent of the big data era, the amount of digital data continues to grow. Sparse modeling [1]–[8] is drawing attention as an information processing model for extracting useful information hidden in large amounts of data. It represents observed signals effectively as a linear combination of a small number of bases chosen from the basis functions trained by a dictionary learning algorithm. Sparse modeling has yielded numerous processing applications for sources such as image/video, audio, biological signal, and seismic data [8].

Another trend is the spread of edge cloud computing, which includes big data analysis, to many fields. However, edge cloud computing confronts end users with several serious issues, such as unauthorized use and leak of data, and privacy failures, due to the unreliability of providers and accidents [9]. Most of the many studies that have examined the processing of encrypted data use homomorphic encryption (HE) and secure multiparty computation (MPC) [10]–[13]. Even though service providers cannot directly access the native content of the encrypted signals, they can still employ HE and MPC. In particular, fully homomorphic encryption (FHE) allows arbitrary computation on encrypted data. It imposes high computation complexity and large cipher text size, so further advances are needed for applications such as big data analysis and advanced image/video processing [13].

Our study focuses on the secure but practical computation of sparse modeling. The proposed scheme, based on the random unitary transform, has much lower computation complexity and small cipher text size than either HE or MPC. We have already proposed a secure Orthogonal Matching Pursuit (OMP) computation method for image modeling [14] and network BMI decoding [15]. OMP is one of the pursuit algorithms that choose the basis and calculate the sparse coefficients sequentially. Secure OMP can choose the basis and estimate the sparse coefficients from encrypted signals.

In this paper, we propose a secure sparse dictionary learning method [16]–[18]. Method of Optimal Direction (MOD) [4] and K-Singular Value Decomposition (K-SVD) [5] are well-known dictionary learning algorithms that seek dictionaries that fit the observed signals. MOD is known for its simple way of updating the dictionary. K-SVD is an adaptive learning algorithm that generalizes the K-means clustering algorithm. The proposed scheme yields practical MOD and K-SVD algorithms that allow computation on encrypted signals. The secure dictionary learning proposed here not only protects observed signals, but also attains the same estimation performance as that of sparse dictionary learning for non-encrypted signals. We apply the proposed secure dictionary learning to secure image modeling, which can be used for applications such as an Encryption-then-Compression (EtC) system [14], [19], and secure image pattern recognition [20]. Finally, we demonstrate its performance on both synthetic data and a secure image modeling application for a natural image. We show that secure MOD and secure K-SVD can represent the image with fewer sparse coefficients, even when processing is performed in the encrypted domain. We evaluate the security strength of the proposed method from the viewpoints of quality and visibility of decoded/decrypted images. It is shown that unauthorized users can only extract images of unusable quality and visibility. The organization of this paper is as follows. Section 2 overviews dictionary learning. In Sect. 3, we propose a secure MOD and K-SVD computation process. Section 4 illustrates its application to secure image modeling. Section 5 shows numerical assessment results. Conclusions are given in Sect. 6.

Manuscript received April 1, 2019.
Manuscript revised August 9, 2019.
Manuscript publicized October 9, 2019.

[†]The authors are with NTT Corporation, Yokosuka-shi, 239–0847 Japan.
[††]The author is with Tokyo Metropolitan University, Hino-shi, 191–0065 Japan.
a) E-mail: takayuki.nakachi.pu@hco.ntt.co.jp

DOI: 10.1587/transinf.2019MUP0009

2. Overview of Dictionary Learning

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

2.1 Sparse Representation

Given an 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 $\boldsymbol{D} = \{\boldsymbol{d}_1, \ldots, \boldsymbol{d}_K\} \in \mathbb{R}^{M\times K}$, whose columns contain K 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 set of sparse coefficients.

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

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

where $\|\cdot\|_0$ is the l_0-norm which counts the nonzero entries of the vector. The notation $\|\boldsymbol{A}\|_F$ stands for the Frobenius norm, defined as $\|\boldsymbol{A}\|_F = \sqrt{\sum_{ij} A_{ij}^2}$. Sparse dictionary learning solves the optimization problem of Eq. (2) by alternately repeating two steps: 1) sparse coding and 2) dictionary update. In the sparse coding step, fix the dictionary $\boldsymbol{D}$ and estimate the sparse coefficient set $\boldsymbol{X}$. In the dictionary update step, fix $\boldsymbol{X}$ and update the dictionary $\boldsymbol{D}$.

MOD and K-SVD are well known sparse dictionary learning algorithms. One key property of MOD is its simple way of updating the dictionary. K-SVD is the adaptive learning algorithm that generalizes the K-means clustering algorithm. When forced to have a unit coefficient for one atom, it exactly reproduces the K-means algorithm. MOD and K-SVD use the same sparse coding step, but employ different methods of updating the dictionary. The following overviews 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 Matching Pursuit (MP) [6], Orthogonal Matching Pursuit (OMP) [7], to approximate the solution of

$$\arg\min_{\boldsymbol{x}_i} \left\|\boldsymbol{y}_i - \boldsymbol{D}\boldsymbol{x}_i\right\|_2^2 \quad \text{subject to} \quad \|\boldsymbol{x}_i\|_0 \le T_0, \quad \text{for } i = 1, 2, \cdots, N. \tag{3}$$

· **Dictionary Update Step:** Update $\boldsymbol{D}$ by MOD or K-SVD. The dictionary update steps are shown in the following section.

2.2 MOD Dictionary Update

MOD uses a pseudo inverse to minimize the squared error between $\boldsymbol{Y}$ and $\boldsymbol{D}\boldsymbol{X}$. For the given $\boldsymbol{Y}$ and the fixed $\boldsymbol{X}$ approximated in the sparse coding step, update the dictionary by the formula:

$$\begin{aligned}\boldsymbol{D} &= \arg\min_{D} \|\boldsymbol{Y} - \boldsymbol{D}\boldsymbol{X}\|_F^2 \\ &= \boldsymbol{Y}\boldsymbol{X}^T(\boldsymbol{X}\boldsymbol{X}^T)^{-1}.\end{aligned} \tag{4}$$

2.3 K-SVD Dictionary Update Step

Unlike MOD, K-SVD updates one atom sequentially. Figure 2 shows the k-th atom $\boldsymbol{d}_k$ and the corresponding sparse coefficient vector $\boldsymbol{x}_T^k$. For each atom $\boldsymbol{d}_k$ ($k = 1, 2, \cdots, K$ in $\boldsymbol{D}$), update it by the following steps:

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

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

2) Define the group of indexes that satisfy the following:

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

Define $\boldsymbol{\Omega}_k$ as a matrix of size $N \times |\omega_k|$ with ones on the $(\omega_k(i), i)$th entries and zeros elsewhere. Multiplication $\boldsymbol{E}_k^R = \boldsymbol{E}_k\boldsymbol{\Omega}_k$ creates a matrix that includes a selection of error columns that use the atom $\boldsymbol{d}_k$.

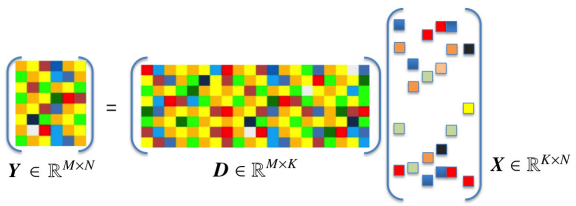


Fig. 1 Sparse coding: observed signals are effectively represented as a linear combination of a small number of bases.

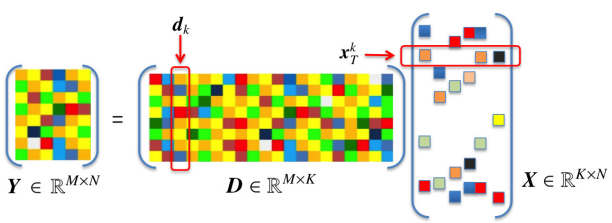


Fig. 2 One atom $\boldsymbol{d}_k$ and corresponding sparse coefficient vector $\boldsymbol{x}_T^k$.

3) Apply Singular Value Decomposition (SVD) to $\boldsymbol{E}_k^R$:

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

Choose the updated dictionary atom $\boldsymbol{d}_k$ to be the first column $\boldsymbol{u}_1$. Update coefficient vector $\boldsymbol{x}_{R_k}^k$ to be the first column multiplied by the first eigenvalue $\sigma_1 \boldsymbol{v}_1^T$.

3. Secure Dictionary Learning

In this section, we propose secure MOD and K-SVD dictionary learning algorithms that allow computations in the encrypted domain.

3.1 Overview of Secure Dictionary Learning

Figure 3 illustrates the architecture of secure dictionary learning. At the local site, a random unitary transform $\boldsymbol{Q}_p \in \mathbb{C}^{N\times N}$ with a private key p is applied to a given set of training signals $\boldsymbol{Y}$. The encrypted set $\hat{\boldsymbol{Y}} = \{\hat{\boldsymbol{y}}_i\}_{i=1}^N$ is sent to the edge and cloud site. By using just 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

$$\hat{\boldsymbol{Y}} = T(\boldsymbol{Y}, p) = \boldsymbol{Q}_p \boldsymbol{Y}. \tag{8}$$

Note that the random unitary matrix $\boldsymbol{Q}_p$ satisfies

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

where $[\cdot]^*$ and $\boldsymbol{I}$ mean 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. The following is an example of generating $\boldsymbol{Q}_p$ by using multiple unitary matrices.

$$\boldsymbol{Q}_p = \boldsymbol{H}_p \boldsymbol{A} \boldsymbol{L}_p \tag{10}$$

where $\boldsymbol{H}_p$ is an orthogonal matrix generated using Gram-Schmidt orthogonalization, $\boldsymbol{A}$ is a unitary transform having no randomness such as discrete Fourier transformation or Hadamard transformation, and $\boldsymbol{L}_p$ is a unitary matrix with randomness generated by a pseudorandom number generator. Note that $\boldsymbol{H}_p \boldsymbol{A} \boldsymbol{L}_p$ satisfies

$$(\boldsymbol{H}_p \boldsymbol{A} \boldsymbol{L}_p)^* (\boldsymbol{H}_p \boldsymbol{A} \boldsymbol{L}_p) = \boldsymbol{I}. \tag{11}$$

Security analyses of the protection schemes have been demonstrated from the aspects of brute-face attack, diversity and irreversibility [21]. The encrypted vector has the following properties:

· Property 1: Conservation of Euclidean distances

$$\left\|\boldsymbol{y}_i - \boldsymbol{y}_j\right\|_2^2 = \left\|\hat{\boldsymbol{y}}_i - \hat{\boldsymbol{y}}_j\right\|_2^2. \tag{12}$$

· Property 2: Norm isometry

$$\|\boldsymbol{y}_i\|_2^2 = \|\hat{\boldsymbol{y}}_i\|_2^2. \tag{13}$$

· Property 3: Conservation of inner products

$$\boldsymbol{y}_i^* \boldsymbol{y}_j = \hat{\boldsymbol{y}}_i^* \hat{\boldsymbol{y}}_j. \tag{14}$$

Here we consider the following optimization problem:

$$\min_{\hat{\boldsymbol{D}}, \boldsymbol{X}} \left\|\hat{\boldsymbol{Y}} - \hat{\boldsymbol{D}}\boldsymbol{X}\right\|_F^2 \quad \text{subject to } \forall i, \ \ \|\boldsymbol{x}_i\|_0 \le T_0, \tag{15}$$

where $\hat{\boldsymbol{D}} = \{\hat{\boldsymbol{d}}_1, \ldots, \hat{\boldsymbol{d}}_K\} \in \mathbb{R}^{M\times K}$ is an encrypted dictionary. The following is an overview of the secure dictionary learning algorithm:

Secure Dictionary Learning Algorithm

Task: Train an encrypted dictionary $\hat{\boldsymbol{D}}$ to sparsely represent data $\hat{\boldsymbol{Y}} = \{\hat{\boldsymbol{y}}_i\}_{i=1}^N$ by approximating the solution to the problem posed in Eq. (15).

Initialization: Set the encrypted dictionary matrix $\hat{\boldsymbol{D}} \in \mathbb{R}^{M\times K}$ with l_0 normalized columns.

Main Iteration: Repeat until convergence (stopping rule):

· **Sparse Coding Step:** Use OMP to approximate the solution of

$$\arg\min_{x_i} \left\|\hat{\boldsymbol{y}}_i - \hat{\boldsymbol{D}}\boldsymbol{x}_i\right\|_2^2 \quad \text{subject to} \quad \|\boldsymbol{x}_i\|_0 \le T_0, \quad \text{for } i = 1, 2, \cdots, N. \tag{16}$$

We have already proven that the solution obtained by solving Eq. (16) by OMP is equal to the solution yielded by the non-encrypted variant of the OMP algorithm [14], [15] under the condition $\hat{\boldsymbol{D}} = \boldsymbol{Q}_p \boldsymbol{D}$. We refer to the secure variant as secure OMP.

· **Dictionary Update Step:** Update $\hat{\boldsymbol{D}}$ by secure MOD or secure K-SVD. The dictionary update steps are shown in the following section.

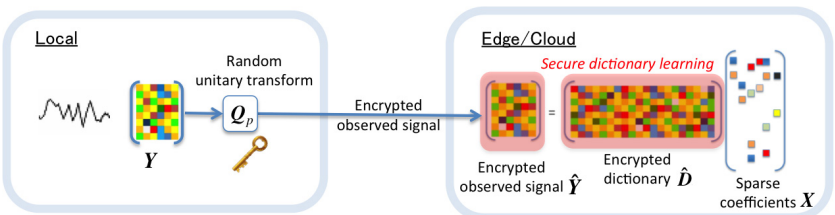


Fig. 3 Architecture of secure dictionary learning.

3.2 Secure MOD Dictionary Update

The derivation of Eq. (15) with respect to $\hat{\boldsymbol{D}}$ yields $(\hat{\boldsymbol{Y}} - \hat{\boldsymbol{D}}\boldsymbol{X})\boldsymbol{X}^T = 0$, which leads to

$$\begin{aligned}\hat{\boldsymbol{D}} &= \arg\min_{\hat{D}} \left\|\hat{\boldsymbol{Y}} - \hat{\boldsymbol{D}}\boldsymbol{X}\right\|_F^2 \\ &= \hat{\boldsymbol{Y}}\boldsymbol{X}^T(\boldsymbol{X}\boldsymbol{X}^T)^{-1}. \end{aligned} \tag{17}$$

The encrypted dictionary $\hat{\boldsymbol{D}}$ can be calculated by Eq. (17). The following shows the relationship between the non-encrypted dictionary $\boldsymbol{D}$ and the encrypted dictionary $\hat{\boldsymbol{D}}$. From the definition $\hat{\boldsymbol{Y}} = \boldsymbol{Q}_p\boldsymbol{Y}$, Eq. (17) can be rewritten as

$$\hat{\boldsymbol{D}} = \boldsymbol{Q}_p\boldsymbol{Y}\boldsymbol{X}^T(\boldsymbol{X}\boldsymbol{X}^T)^{-1}. \tag{18}$$

3.3 Secure K-SVD Dictionary Update Step

Similar to the derivation of the non-encrypted version of K-SVD, the overall representation error matrix $\hat{\boldsymbol{E}}_k$ is written as

$$\hat{\boldsymbol{E}}_k = \hat{\boldsymbol{Y}} - \sum_{j\neq k}^{K} \hat{\boldsymbol{d}}_j \boldsymbol{x}_T^j. \tag{19}$$

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

$$\hat{\boldsymbol{E}}_k^R = \hat{\boldsymbol{U}}\hat{\boldsymbol{\Delta}}\hat{\boldsymbol{V}}^{\boldsymbol{T}} = \sum_{i=1}^{n} \hat{\boldsymbol{u}}_i \cdot \hat{\sigma}_i \hat{\boldsymbol{v}}_i^T. \tag{20}$$

Choose the updated dictionary atom $\hat{\boldsymbol{d}}_k = \hat{\boldsymbol{u}}_1$. Updated 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 yielded 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 non-encrypted variant of K-SVD, the overall representation error matrix $\hat{\boldsymbol{E}}_k$ of Eq. (19) can be written as

$$\begin{aligned}\hat{\boldsymbol{E}}_k &= \hat{\boldsymbol{Y}} - \sum_{j\neq k}^{K} \hat{\boldsymbol{d}}_j \boldsymbol{x}_T^j \\ &= \boldsymbol{Q}_p\boldsymbol{E}_k, \end{aligned} \tag{21}$$

where we assume that $\hat{\boldsymbol{d}}_j = \boldsymbol{Q}_p\boldsymbol{d}_j$ which is derived from the condition $\hat{\boldsymbol{D}} = \boldsymbol{Q}_p\boldsymbol{D}$ [14], [15] in the sparse coding step. Multiplication $\hat{\boldsymbol{E}}_k^R = \hat{\boldsymbol{E}}_k\boldsymbol{\Omega}_k$ creates a matrix that includes a selection of error columns that use the atom $\boldsymbol{d}_k$. Using Eq. (21), $\hat{\boldsymbol{E}}_k^R$ can be written as

$$\begin{aligned}\hat{\boldsymbol{E}}_k^R &= \hat{\boldsymbol{E}}_k\boldsymbol{\Omega}_k \\ &= \boldsymbol{Q}_p\boldsymbol{E}_k\boldsymbol{\Omega}_k = \boldsymbol{Q}_p\boldsymbol{E}_k^R. \end{aligned} \tag{22}$$

Using Eq. (7), i.e. the result of applying SVD to the non-encrypted variant of overall representation error matrix $\boldsymbol{E}_k^R$, Eq. (22) can be decomposed as follows:

$$\begin{aligned}\hat{\boldsymbol{E}}_k^R &= \boldsymbol{Q}_p\boldsymbol{E}_k^R \\ &= \boldsymbol{Q}_p \sum_{i=1}^{n} \boldsymbol{u}_i \cdot \sigma_i \boldsymbol{v}_i^T. \end{aligned} \tag{23}$$

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

$$\cdot\text{Sparse coefficients}: \ \hat{\boldsymbol{x}}_R^k = \sigma_1\boldsymbol{v}_1^T \tag{24}$$

$$\cdot\text{Dictionary atom}: \ \hat{\boldsymbol{d}}_k = \boldsymbol{Q}_p\boldsymbol{u}_1 \tag{25}$$

Equations (24)–(25) can be shown as described in Appendix A and Appendix B, respectively.

4. Secure Image Modeling

In this section, we apply the secure dictionary learning proposal to secure image modeling.

4.1 Overview of Secure Image Modeling

Figures 4 and 5 show the architectures of 1) learning step and 2) encoding and decoding steps of secure image modeling, respectively. In the learning step, content owner Alice wants to securely transmit images for dictionary learning to public service provider Charlie. Alice wants Charlie to design the encrypted dictionary $\hat{\boldsymbol{D}}$. The details of the learning step are shown in Sect. 4.2.

At the encoding and decoding steps, content owner Alice wants to securely transmit images to recipient Bob, via a public service provider Charlie. Alice wants Charlie

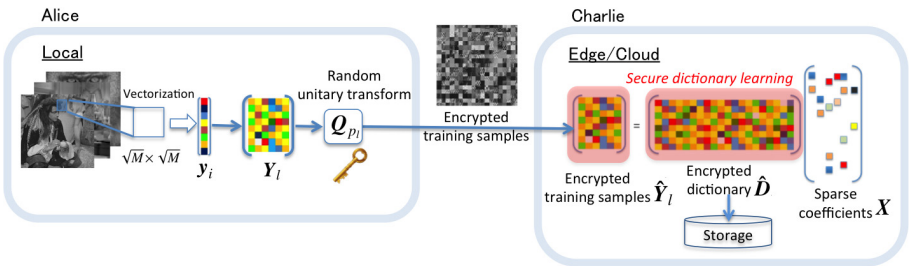


Fig. 4 Architecture of learning step for secure image modeling.

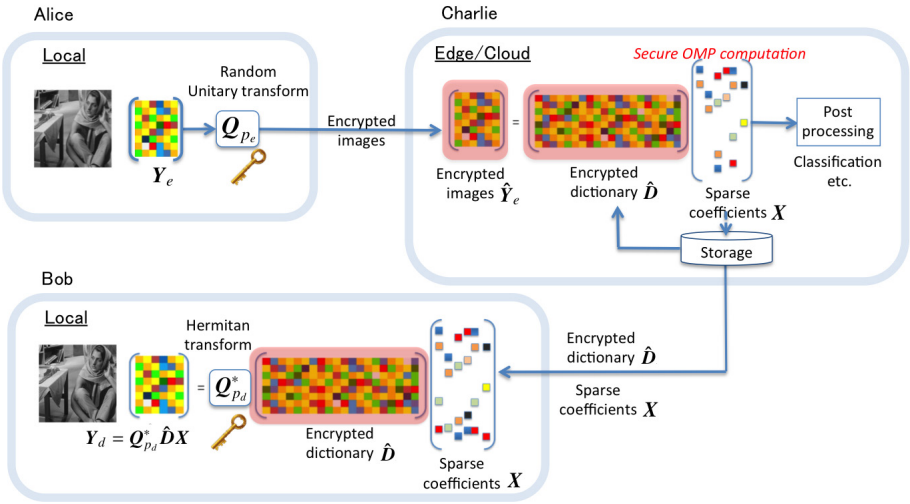


Fig. 5 Architecture of encoding (upper) and decoding (lower) steps for secure image modeling.

to store images or analysis images etc. The proposed system works as an EtC system [19]. In conventional secure image transmission systems, image compression has to be conducted prior to image encryption. On the other hand, as EtC systems are expected to provide privacy protection, they allow image encryption to be conducted prior to compression. Even if the transmitted data leaks, privacy can be maintained because the data remains encrypted. Furthermore, the proposed system can work as a secure image pattern recognition system by processing the estimated sparse coefficients as shown in Ref. [20]. The public service provider Charlie provides the pattern recognition results to Alice and Bob without viewing their image contents. This offers a surveillance camera system and an SNS photo service, etc. The details of the encoding and decoding step are shown in Sect. 4.3.

4.2 Secure Dictionary Learning for Image Patches

In secure image modeling, training and encoding sets are formulated around an image patch model. At the learning step, as shown in the left side of Fig. 4, we order image patches of size $\sqrt{M} \times \sqrt{M}$ pixels lexicographically as column vectors $\boldsymbol{y}_i \in \mathbb{R}^M$ $(i = 1, \cdots, N_l)$, where N_l is the number of image patches for dictionary learning. Each image patch is extracted lexicographically or randomly selected from an image or multiple images. Next, the image patch set $\boldsymbol{Y}_l = \{\boldsymbol{y}_i\}_{i=1}^{N_l}$ is transformed into an encrypted image patch set $\hat{\boldsymbol{Y}}_l = \{\hat{\boldsymbol{y}}_i\}_{i=1}^{N_l}$ by

$$\hat{\boldsymbol{Y}}_l = T(\boldsymbol{Y}_l, p_l) = \boldsymbol{Q}_{p_l} \boldsymbol{Y}_l, \tag{26}$$

where p_l and $\boldsymbol{Q}_{p_l}$ are the secret key and the random unitary transform in the learning step, respectively.

The secure dictionary learning proposed in the previous section is applied to the encrypted image patch set $\hat{\boldsymbol{Y}}_l$. We assume that encrypted image patch set $\hat{\boldsymbol{Y}}_l$ could be represented sparsely over the encrypted over-complete dictionary $\hat{\boldsymbol{D}} \in \mathbb{R}^{M \times K}$. By feeding the encrypted image patch set $\hat{\boldsymbol{Y}}_l$ to the secure dictionary learning algorithms, the encrypted dictionary $\hat{\boldsymbol{D}}$ is estimated and stored in the edge/cloud site.

4.3 Secure Encoding and Decoding

In the encoding step, we order image patches of size $\sqrt{M} \times \sqrt{M}$ pixels lexicographically as column vectors, which are then permuted randomly using a random integer generated with a secret key p_e. Each image patch is extracted from a $\sqrt{N} \times \sqrt{N}$ pixel encoded image without overlaps, which yields $N_e = N/M$. The resulting image patch set, $\boldsymbol{Y}_e = \{\boldsymbol{y}_i\}_{i=1}^{N_e}$, is transformed into an encrypted image patch set $\hat{\boldsymbol{Y}}_e = \{\hat{\boldsymbol{y}}_i\}_{i=1}^{N_e}$ by

$$\hat{\boldsymbol{Y}}_e = T(\boldsymbol{Y}_e, p_e) = \boldsymbol{Q}_{p_e} \boldsymbol{Y}_e, \tag{27}$$

where $\boldsymbol{Q}_{p_e}$ is a random unitary transform in the encoding step. Upon receiving the encrypted image patch set $\hat{\boldsymbol{Y}}_e$ and the encrypted dictionary $\hat{\boldsymbol{D}}$ designed at the learning step, secure OMP estimates the sparse coefficients. Since the encrypted dictionary $\hat{\boldsymbol{D}}$ is optimized for images owned by content owner Alice, sparse coefficients can be estimated efficiently when $\boldsymbol{Q}_{p_e} = \boldsymbol{Q}_{p_l}$.

In the decoding step, a decoded/decrypted image patch set $\boldsymbol{Y}_d = \{\dot{\boldsymbol{y}}_i\}_{i=1}^{N_e}$ can be calculated by $\boldsymbol{Y}_d = \boldsymbol{Q}^*_{p_d} \hat{\boldsymbol{D}} \boldsymbol{X}$, where p_d and $\boldsymbol{Q}_{p_d}$ are a secret key and a random unitary transform in the decoding step, respectively. When $\boldsymbol{Q}_{p_d} = \boldsymbol{Q}_{p_e} = \boldsymbol{Q}_{p_l}$, the proposal has exactly the same coding performance as the non-encrypted variant of image modeling. The image quality of decoded/decrypted 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 secure OMP, i.e. (l_2-norm of reconstruction error) $< \epsilon_i$. If we want to keep each image patch quality the same, the same threshold is set: $\epsilon_i = \text{constant}$ $(i = 1, \cdots, N)$.

5. Numerical Assessments

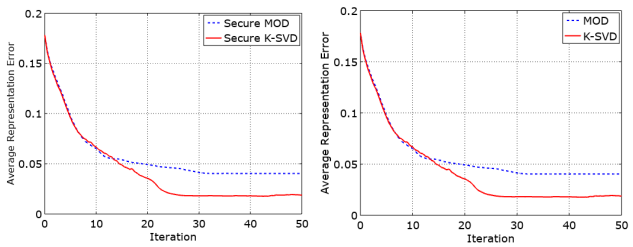
We demonstrated the performance of the proposed method both on synthetic data and in an image modeling application for natural images.

5.1 Synthetic Data

We created a random matrix $\boldsymbol{D}$ of size 30×60 and generated a training data set $\boldsymbol{X} = \{\boldsymbol{x}_i\}_{i=1}^{4000}$, with uniformly distributed iid sparse coefficients in random and independent locations. We set the target cardinality to $T_0 = 4$. Once $\boldsymbol{X}$ was generated, we computed $\boldsymbol{Y} = \boldsymbol{DX}$. Then we encrypted $\boldsymbol{Y}$ by using a random unitary transform $\boldsymbol{Q}_p$ based on Gram-Schmidt orthogonalization, i.e. $\hat{\boldsymbol{Y}} = \boldsymbol{Q}_p\boldsymbol{Y}$. We performed experiments on $\hat{\boldsymbol{Y}} = \{\hat{\boldsymbol{y}}_i\}_{i=1}^{4000}$, and present the average results. We present two measures: normalized l_2-norm error and recovery of support[†]. Normalized l_2-norm error was computed as the ratio $E(\|\boldsymbol{X} - \hat{\boldsymbol{X}}\|^2/\|\boldsymbol{X}\|^2)$, where $E(\cdot)$ is an ensemble average. Recovery of support indicates l_2 proximity of the two solutions. Denoting the two supports as $\hat{\boldsymbol{S}}$ and $\boldsymbol{S}$, we define this distance by

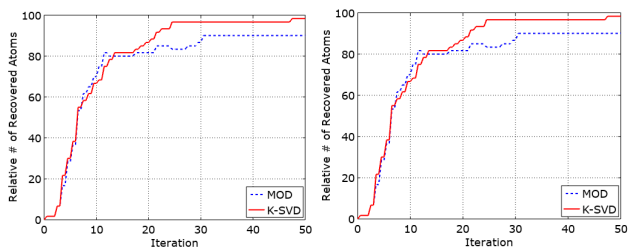
$$dist(\hat{\boldsymbol{S}}, \boldsymbol{S}) = \frac{max\{|\hat{\boldsymbol{S}}|, |\boldsymbol{S}|\} - |\hat{\boldsymbol{S}} \cap \boldsymbol{S}|}{max\{|\hat{\boldsymbol{S}}|, |\boldsymbol{S}|\}}. \tag{28}$$

It represents the relative number (in %) of correctly recovered atoms. The results are shown in Figs. 6 and 7. Horizontal axis shows iteration number. As can be seen, secure K-SVD gives better results than secure MOD in terms of both final outcome and speed of convergence. We compared the proposed method with the non-encrypted versions of MOD and K-SVD algorithms. Figures 6 and 7 show that the proposed method offers exactly the same performance as the non-encrypted versions of MOD and K-SVD algorithms with regard to both measures.



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

Fig. 6 Normalized l_2-norm error: $E(\|\boldsymbol{X} - \hat{\boldsymbol{X}}\|^2/\|\boldsymbol{X}\|^2)$.



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

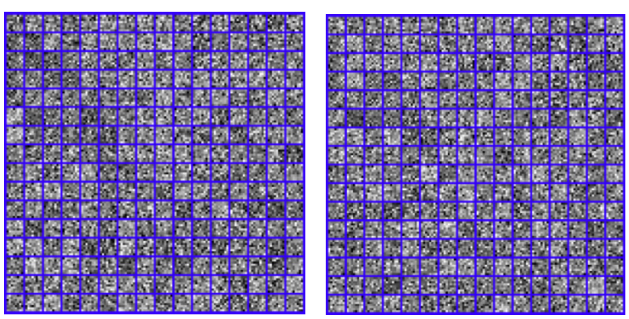
Fig. 7 Recovery of the support: dist$(\hat{\boldsymbol{S}}, \boldsymbol{S})$.

[†]Support is the set of indexes corresponding to non-zero elements of a sparse vector.

5.2 Secure Image Modeling

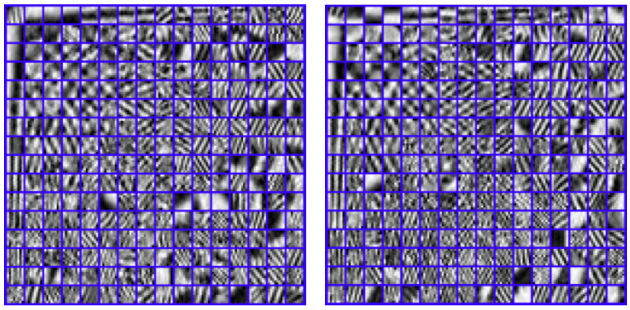
We confirmed the practicality of the proposed method by conducting secure image modeling experiments on natural images. We trained a dictionary $\hat{\boldsymbol{D}}$ to sparsely represent patches of 8×8 pixels extracted from a 512×512 Barbara image. We extracted one fifth of these image patches, i.e. the total number of image patches $N_l = 820$. Our choice $N_l = 820$ came from our attempt to seek the dictionary that fit the Barbara image with moderate computational cost. Each selected patch was transformed by a 64×64 random unitary transform $\boldsymbol{Q}_{p_l}$ to produce a training encrypted image patch $\hat{\boldsymbol{Y}}_l$. The random unitary transform $\boldsymbol{Q}_{p_l}$ was based on Gram-Schmidt orthogonalization. Feeding the encrypted image patch set $\hat{\boldsymbol{Y}}_l$ into secure MOD and secure K-SVD with 50 iteration yielded the encrypted dictionary $\hat{\boldsymbol{D}}$. We set the number of atoms to $K = 256$ and the l_0-norm constrains $T_0 = 5$. $T_0 = 5$ was set heuristically so as to minimize $\left\|\hat{\boldsymbol{Y}} - \hat{\boldsymbol{D}}\boldsymbol{X}\right\|_F^2$. Encrypted dictionaries designed by secure MOD and secure K-SVD are shown in Fig. 8. They provide no visible information. Corresponding decrypted dictionaries calculated by $\boldsymbol{Q}_{p_l}^* \hat{\boldsymbol{D}}$ are shown in Fig. 9. Figure 10 shows convergence properties of l_2-norm error $E\|\hat{\boldsymbol{Y}} - \hat{\boldsymbol{D}}\boldsymbol{X}\|^2$. Both secure algorithms have almost the same performance.

Then, we carried out secure image modeling using secure OMP [14] with the trained encrypted dictionaries $\hat{\boldsymbol{D}}$. The encoding image patch set $\boldsymbol{Y}_e$ consisted of 8×8 pixel images extracted from the 512×512 Barbara image without overlapping, i.e. the total number of image patches $N_e = 4096$. Each patch was permuted randomly using a random integer and transformed by a 64×64 random unitary transform $\boldsymbol{Q}_{p_e}$ with a secret key p_e. Figure 11 shows original Barbara and corresponding encrypted images. In the decoding step, a decoded/decrypted image patch set



(a) Secure MOD (b) Secure K-SVD

Fig. 8 Encrypted dictionaries designed by secure MOD and secure K-SVD.



(a) Secure MOD (b) Secure K-SVD

Fig. 9 Decrypted dictionaries $\boldsymbol{Q}_{p_l}^{*}\hat{\boldsymbol{D}}$.

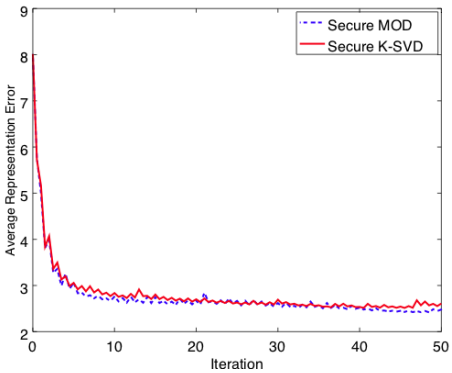


Fig. 10 Convergence property of secure MOD and secure K-SVD.

(a) Barbara (b) Encryped image

Fig. 11 Original and encrypted images.

$\boldsymbol{Y}_d = \{\dot{\boldsymbol{y}}_i\}_{i=1}^{N_e}$ was calculated by $\boldsymbol{Y}_d = \boldsymbol{Q}_{p_d}^{*}\hat{\boldsymbol{D}}\boldsymbol{X}$. Figure 12 plots coding efficiency (average sparsity ratio $\bar{S}$ vs. decoded/decrypted image quality PSNR [dB]) in comparison with over-complete DCT. We controlled the image quality of decoded/decrypted image at each patch by setting the threshold $\epsilon_i = \{3.0, 5.0, 7.0, 10.0, 15.0\}$. The random unitary transforms were set to $\boldsymbol{Q}_{p_d} = \boldsymbol{Q}_{p_e} = \boldsymbol{Q}_{p_l}$. Average sparsity ratio $\bar{S}$ is defined by $\bar{S}=\sum_{i=1}^{N} s_i/K$. It can be seen that secure MOD and secure K-SVD can represent the image with fewer sparse coefficients than over-complete DCT. The secure MOD and secure K-SVD have the same coding performance.

Finally, we evaluated the security strength of the proposed method from the viewpoints of quality and visibility

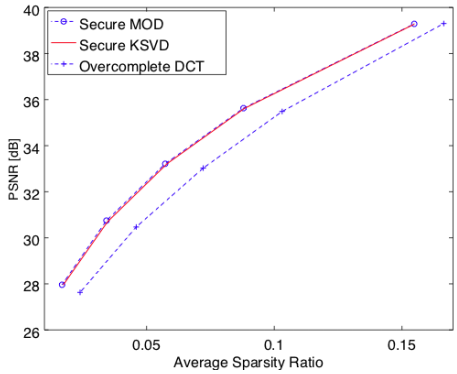


Fig. 12 Average sparsity ratio $\bar{S}_i$ vs. decoded image quality PSNR [dB].

Table 1 Decoded/decrypted image quality by secure K-SVD for authorized and unauthorized users.

(a) Authorized user ($\boldsymbol{Q}_{p_l} = \boldsymbol{Q}_{p_e} = \boldsymbol{Q}_{p_d}$)

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 ($\boldsymbol{Q}_{p_l} \neq \boldsymbol{Q}_{p_e} = \boldsymbol{Q}_{p_d}$)

ϵ	3.0	5.0	7.0	10.0	15.0
$\bar{S}$	0.370	0.308	0.261	0.202	0.123
PSNR [dB]	10.40	10.46	10.52	10.35	10.53

(c) Unauthorized user ($\boldsymbol{Q}_{p_l} = \boldsymbol{Q}_{p_e} \neq \boldsymbol{Q}_{p_d}$)

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]	10.42	10.37	10.38	10.31	10.39

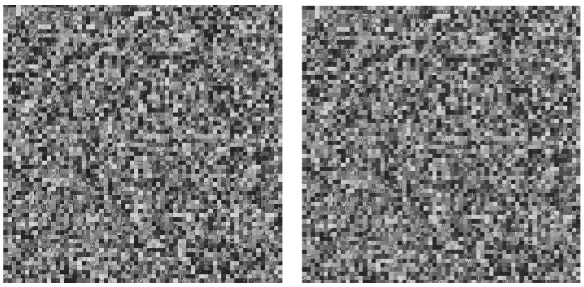
of decoded/decrypted images. We assumed the following three cases:

(*a*) Access by an authorized user ($\boldsymbol{Q}_{p_l} = \boldsymbol{Q}_{p_e} = \boldsymbol{Q}_{p_d}$)
(*b*) Access by an unauthorized user ($\boldsymbol{Q}_{p_l} \neq \boldsymbol{Q}_{p_e} = \boldsymbol{Q}_{p_d}$)
(*c*) Access by an unauthorized user ($\boldsymbol{Q}_{p_l} = \boldsymbol{Q}_{p_e} \neq \boldsymbol{Q}_{p_d}$)

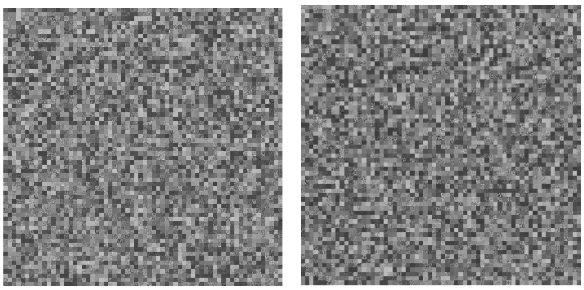
All the cases used the same random unitary transform $\boldsymbol{Q}_{p_l}$ in the learning step. In case (b), the random unitary matrix for encoding and decoding was different from that in the learning step. In case (c), the random unitary matrix for decoding was different from that in the learning and encoding steps. Table 1 shows decoded/decrypted image quality achieved by secure K-SVD with different stopping conditions (l_2 norm of reconstruction error ϵ). From Table 1, it can be seen that the unauthorized users attain only very low decoded/decrypted image quality regardless of ϵ. Figure 13 shows images decoded/decrypted by authorized and unauthorized users at $\epsilon = 3.0$ and 15.0. These results show that the encrypted images cannot be decrypted by unauthorized users.

The purpose of this paper is to provide a theoretical guarantee about secure dictionary learning and to demonstrate the theoretical guarantee through experiments. Regarding the hyperparameters in secure image modeling, they were set experimentally as described above. In the practical application of the system, the hyperparameters optimization is important and is considered as a future issue.

ϵ=3.0 (PSNR = 39.28 [dB]) ϵ = 15.0 (PSNR = 27.95 [dB])
(a) Authorized user ($\boldsymbol{Q}_{p_l} = \boldsymbol{Q}_{p_e} = \boldsymbol{Q}_{p_d}$)



ϵ=3.0 (PSNR = 10.43 [dB]) ϵ = 15.0 (PSNR = 10.45 [dB])
(b) Unauthorized user ($\boldsymbol{Q}_{p_l} \neq \boldsymbol{Q}_{p_e} = \boldsymbol{Q}_{p_d}$)



ϵ=3.0 (PSNR = 10.40 [dB]) ϵ = 15.0 (PSNR = 10.47 [dB])
(c) Unauthorized user ($\boldsymbol{Q}_{p_l} = \boldsymbol{Q}_{p_e} \neq \boldsymbol{Q}_{p_d}$)

Fig. 13 Decoded/decrypted images by secure K-SVD for authorized and unauthorized users.

6. Conclusions

In this paper, we proposed secure MOD and secure K-SVD algorithms for sparse representation. The proposed algorithms are practical as they realize efficient computation on encrypted signals. We proved, theoretically, that the proposal has exactly the same dictionary learning performance as their non-encrypted variants. Finally, we confirmed their performance on synthetic data and a secure image modeling application for natural images. The secure MOD and secure K-SVD proposals can represent images with fewer sparse coefficients than over-complete DCT.

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] M. Elad, "Sparse and Redundant Representations: From Theory to Applications in Signal and Image Processing," Springer, New York, NY, 2010.
[3] B.K. Natarajan, "Sparse approximate solutions to linear systems," SIAM J. Comput., vol.24, no.2, pp.227–234, 1995.
[4] K. Engan, S.O. Aase, and J.H. 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. Signal Process., vol.54, no.11, pp.4311–4322, 2006.
[6] S.G. Mallat and Z. Zhang, "Matching pursuits with time-frequency dictionary," IEEE Trans. Signal Process., vol.41, no.12, pp.3397–3415, 1993.
[7] Y.C. Pati, R. Rezaiifar, and P.S. Krishnaprasad, "Orthogonal matching pursuit: Recursive function approximation with applications to wavelet decomposition," Proc, 27th Asilomar Conference on Signals, Systems and Computers, pp.40–44, 1993.
[8] M. Elad, "Sparse and redundant representation modeling—What next?," IEEE Signal Process. Lett., vol.19, no.12, pp.922–928, Dec. 2012.
[9] C.-T. Huang, L. Huang, Z. Qin, H. Yuan, L. Zhou, V. Varadharajan, and C.-C.J. Kuo, "Survey on securing data storage in the cloud," APSIPA Trans. Signal and Information Processing, vol.3, e7, 2014.
[10] 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 Process. Mag., vol.30, no.1, pp.82–105, Jan. 2013.
[11] R. Lazzeretti and M. Barni, "Private computing with garbled circuits [applications corner]," IEEE Signal Process. Mag., vol.30, no.2, pp.123–127, March 2013.
[12] M. Barni, G. Droandi, and R. Lazzeretti, "Privacy protection in biometric-based recognition systems: A marriage between cryptography and signal processing," IEEE Signal Process. Mag., vol.32, no.5, pp.66–76, Sept. 2015.
[13] Z. Brakerski, "Fundamentals of fully homomorphic encryption—A survey," Electronic Colloquium on Computational Complexity, report no.125, 2018.
[14] T. Nakachi and H. Kiya, "Practical secure OMP computation and its application to image modeling," Proc. International Conference on Information Hiding and Image Processing, pp.25–29, 2018.
[15] T. Nakachi, H. Ishihara, and H. Kiya, "Privacy-preserving network BMI decoding of covert spatial attention," IEEE ICSPCS2018, p.12, 2018.
[16] T. Nakachi, Y. Bandoh, and H. Kiya, "Secure computation of sparse dictionary learning," IEICE Technical Report, vol.118, no.473, SIS2018-43, pp.35–40, March 2019.
[17] T. Nakachi and H. Kiya, "Image patch modeling in encrypted domain using sparse coding," IEICE Technical Report, vol.118, no.224, EMM2018-51, pp.13–18, March 2019.
[18] T. Nakachi, Y. Bandoh, and H. Kiya, "Secure dictionary learning for sparse representation," 2019 27th European Signal Processing Conference (EUSIPCO2019), TuAP1.7, pp.1–5, A Coruña, Spain, 3rd Sept. 2019.
[19] T. Chuman, K. Kurihara, and H. Kiya, "On the security of block scrambling-based EtC systems against extended jigsaw puzzle solver attacks," IEICE Trans. Inf. & Syst., vol.E101-D, no.1, pp.37–44, Jan. 2018.
[20] T. Nakachi and H. Kiya, "Privacy-preserving pattern recognition using secure sparse computation," International Conference on Frontiers of Image Processing, Florence, Italy, March 2019.
[21] 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), pp.366–370, Sapporo, 2016.

Appendix A: Derivation of Eq. (24)

From Eq. (20) and the general property of SVD, the eigen decomposition of $(\hat{\boldsymbol{E}}_k^R)^T \hat{\boldsymbol{E}}_k^R$ can be written as

$$(\hat{\boldsymbol{E}}_k^R)^T \hat{\boldsymbol{E}}_k^R \hat{\boldsymbol{v}}_i = \hat{\lambda}_i \hat{\boldsymbol{v}}_i \tag{A·1}$$

where $\hat{\lambda}_i$ is the i-th eigenvalue. By using the relationship $\hat{\boldsymbol{E}}_k^R = \boldsymbol{Q}_p \boldsymbol{E}_k^R$, the left side of Eq. (A·1) can be expressed as

$$\begin{aligned}(\hat{\boldsymbol{E}}_k^R)^T \hat{\boldsymbol{E}}_k^R &= (\boldsymbol{E}_k^R)^T \boldsymbol{Q}_p^T \boldsymbol{Q}_p \boldsymbol{E}_k^R \\ &= (\boldsymbol{E}_k^R)^T \boldsymbol{E}_k^R. \end{aligned} \tag{A·2}$$

Since $(\hat{\boldsymbol{E}}_k^R)^T \hat{\boldsymbol{E}}_k^R$ and $(\boldsymbol{E}_k^R)^T \boldsymbol{E}_k^R$ are equal, the eigenvector and the eigenvalue of these matrices are equal:

$$\hat{\boldsymbol{v}}_i = \boldsymbol{v}_i \tag{A·3}$$

$$\hat{\lambda}_i = \lambda_i. \tag{A·4}$$

From Eq. (A·4), and the relationship between $\hat{\lambda}_i$ and the singular value $\hat{\sigma}_i$ ($\hat{\sigma}_i = \sqrt{\hat{\lambda}_i}$), the singular value is also equal:

$$\hat{\sigma}_i = \sigma_i. \tag{A·5}$$

Equations (A·3) and (A·5) show that Eq. (24) is satisfied.

Appendix B: Derivation of Eq. (25)

In the SVD of $\hat{\boldsymbol{E}}_k^R$ shown in Eq. (20) and the general property of SVD, the eigenvectors on the left side $\hat{\boldsymbol{u}}_i$ and the eigenvectors on the right side $\hat{\boldsymbol{v}}_i$ have the relationship:

$$\hat{\boldsymbol{u}}_i = \pm \hat{\boldsymbol{E}}_k^R \hat{\boldsymbol{v}}_i / \sqrt{\hat{\lambda}_i}. \tag{A·6}$$

Using the relationship $\hat{\boldsymbol{E}}_k^R = \boldsymbol{Q}_p \boldsymbol{E}_k^R$, $\hat{\sigma}_i = \sqrt{\hat{\lambda}_i}$ and Eq. (A·3), the first term of Eq. (20) can be expressed as follows:

$$\begin{aligned}\hat{\boldsymbol{u}}_1 \cdot \hat{\sigma_1} \hat{\boldsymbol{v}}_1^T &= \frac{\pm \hat{\boldsymbol{E}}_k^R \hat{\boldsymbol{v}}_1 \cdot \hat{\sigma_1} \hat{\boldsymbol{v}}_1^T}{\sqrt{\hat{\lambda}_1}} \\ &= \pm \boldsymbol{Q}_p \boldsymbol{E}_k^R \boldsymbol{v}_1 \boldsymbol{v}_1^T. \end{aligned} \tag{A·7}$$

Similarly, the first term of Eq. (23) can be written as

$$\begin{aligned}\boldsymbol{Q}_p \boldsymbol{u}_1 \cdot \sigma_i \boldsymbol{v}_1^T &= \frac{\pm \boldsymbol{Q}_p \boldsymbol{E}_k^R \boldsymbol{v}_1 \cdot \sigma_1 \boldsymbol{v}_1^T}{\sqrt{\lambda_1}} \\ &= \pm \boldsymbol{Q}_p \boldsymbol{E}_k^R \boldsymbol{v}_1 \boldsymbol{v}_1^T. \end{aligned} \tag{A·8}$$

Therefore, Eq. (25) is satisfied.

Takayuki Nakachi received the Ph.D. degree in electrical engineering from Keio University, Tokyo, Japan, in 1997. Since joining Nippon Telegraph and Telephone Corporation (NTT) in 1997, he has been engaged in research on super-high-definition image/video coding and media transport technologies. From 2006 to 2007, he was a visiting scientist at Stanford University. He also actively participates in MPEG international standardization activities. His current research interests include communication science, information theory, and signal processing. He received the 26th TELECOM System Technology Award, the 6th Paper Award of Journal of Signal Processing and the Best Paper Award of IEEE ISPACS2015. Dr. Nakachi is a member of the Institute of Electrical and Electronics Engineers the Institute of Electronics (IEEE) and the Information and Communication Engineers (IEICE) of Japan.

Yukihiro Bandoh received the B.E., M.E., and Ph.D. degrees from Kyushu University, Japan, in 1996, 1998 and 2002, respectively. He granted JSPS Research Fellowship for Young Scientists from 2000 to 2002. In 2002, he joined Nippon Telegraph and Telephone (NTT) Corporation, where he has been engaged in research on efficient video coding for high realistic communication. He is currently a distinguished engineer at NTT Media intelligence Laboratories. He received IPSJ Nagao Special Researcher Award (2012), FFIT Funai Information Technology Award (2013), the TELECOM System Technology Award (2015), FIT Funai Best Paper Award (2008, 2016). Dr. Bandoh is a senior member of IEEE, IEICE, and IPSJ.

Hitoshi Kiya received his B.E and M.E. degrees from Nagaoka University of Technology, in 1980 and 1982, respectively, and his Dr. Eng. degree from Tokyo Metropolitan University in 1987. In 1982, he joined Tokyo Metropolitan University, where he became a Full Professor in 2000. From 1995 to 1996, he attended the University of Sydney, Australia as a Visiting Fellow. He is a Fellow of IEEE, IEICE and ITE. He currently serves as President-Elect of APSIPA, and he served as Inaugural Vice President (Technical Activities) of APSIPA from 2009 to 2013, and as Regional Director-at-Large for Region 10 of the IEEE Signal Processing Society from 2016 to 2017. He was also President of the IEICE Engineering Sciences Society from 2011 to 2012, and he served there as a Vice President and Editor-in-Chief for IEICE Society Magazine and Society Publications. He was Editorial Board Member of eight journals, including IEEE Trans. on Signal Processing, Image Processing, and Information Forensics and Security, Chair of two technical committees and Member of nine technical committees including APSIPA Image, Video, and Multimedia Technical Committee (TC), and IEEE Information Forensics and Security TC. He has organized many international conferences, in such roles as TPC Chair of IEEE ICASSP 2012 and as General Co-Chair of IEEE ISCAS 2019. He has received numerous awards, including nine best paper awards.