IEICE TRANSACTIONS

on Fundamentals of Electronics, Communications and Computer Sciences

DOI:10.1587/transfun.2024SMP0006

Publicized:2024/08/21

A PUBLICATION OF THE ENGINEERING SCIENCES SOCIETY

The Institute of Electronics, Information and Communication Engineers

Kikai-Shinko-Kaikan Bldg., 5-8, Shibakoen 3 chome, Minato-ku, TOKYO, 105-0011 JAPAN

PAPER

Privacy Preserving Deep Unrolling Methods and Its Application to Image Reconstruction*

Nichika YUGE[†a)], ***Student Member***, **Hiroyuki ISHIHARA**[††b)], **Morikazu NAKAMURA**[†††c)], ***Members***, ***and*** **Takayuki NAKACHI**[††††d)], ***Senior Member***

SUMMARY This paper introduces novel privacy-preserving deep unrolling techniques for recovering sparse signals, integrating privacy-preserving methodologies grounded in random unitary transformation. This approach facilitates data analysis and signal processing while safeguarding privacy. Focusing on sparse signal recovery, we concentrate on LASSO solutions known as LISTA and TISTA. These LISTA and TISTA methods, based on deep unrolling, have been devised to achieve notably faster convergence compared to ISTA. Our contribution lies in proposing secure LISTA and secure TISTA algorithms that operate on encrypted observation signals. The efficacy of the proposed approach was validated through simulations using artificially generated data for sparse signal recovery. As an illustration of the proposed methodology's utility, we applied secure LISTA and secure TISTA to image reconstruction,to evaluate their performance.

key words: *ISTA, Deep Unrolling, LISTA, TISTA, Random Unitary Transform, Image Modeling*

1. Introduction

In recent years, the use of edge computing has become widespread. However, concerns about data leakage and privacy infringement have emerged in the context of edge computing. One approach to addressing this issue is the use of secure computation. Secure computation, based on multiparty protocols or homomorphic encryption, is actively researched [1]. However, challenges such as the computational load and the increase in data size after encryption have become problematic. This limits the applicability of secure computation to big data processing, advanced image and video processing, and real-time applications. Cancelable biometric authentication addresses these challenges by employing low computational load methods, such as random projection [2] and bio-hashing [3]. Both methods demonstrate irreversibility, meaning that original information cannot be recovered from the transformed data, thus maintaining strong security. Additionally, a secure computation method based on random unitary transformation has been proposed [4]. Secure computational methods based on random unitary transforms, like random projections and biohashing, have low computational complexity, but unlike them, it exhibits reversibility. The reversibility provides the following advantages: 1) The transformation matrix can be updated without requiring the original data. 2) There is no degradation in the performance of compression and recognition.

Secure computing methods for sparse modeling using random unitary transformations have also been proposed [5]–[7]. Sparse modeling is an information processing model for extracting valuable insights hidden in large amounts of data [8][9]. In contrast to deep learning, sparse modeling offers the advantage of being trainable with a small amount of data, low computational cost, and explainable AI. We proposed an Encryption-then-Compression (EtC) system using sparse modeling and random unitary transformation [5], [6]. In addition, a face recognition method using sparse modeling combined with ensemble learning has also been proposed [7]. It achieves high recognition performance and, compared to a method called SPCANet (Stacked PCA Network) that uses deep learning, it requires about three orders of magnitude less computation for learning and recognition, and has been confirmed to achieve higher recognition rates with fewer training images.

The above-mentioned EtC and secure face recognition utilize the l_0 norm optimization for sparse modeling. In this paper, we focus on the privacy-preserving sparse signal recovery based on the l_1 norm optimization [10]–[12]. LASSO (Least Absolute Shrinkage and Selection Operator) is an optimization method that employs l_1 regularization. ISTA (Iterative Shrinkage Thresholding Algorithm) is one of the iterative optimization algorithms used to solve the LASSO problem. Recently, LISTA (Learned ISTA) [13] and TISTA (Trainable ISTA) [14], [15], which apply the technique of deep unrolling to ISTA to enable high estimation performance with fast convergence to the solution, have been proposed.

In this paper, we propose secure LISTA and secure TISTA by combining these LISTA and TISTA with random unitary transformation [11], [12]. Secure LISTA and secure TISTA can estimate sparse coefficients while maintaining fast convergence performance even with encrypted observation signals. The original algorithms of LISTA and TISTA

[†]The author is with the Graduate school of engineering and science,University of the Ryukyus, Japan

[††]The author is with the Nippon Telegraph and Telephone Corporation (NTT)

[†††]The author is with the Faculty of Engineering, University of the Ryukyus, Japan

[††††]The author is with the Information Technology Center, University of the Ryukyus, Japan

*This research was partially supported by JSPS Grant-in-Aid for Scientific Research (22K04089).

a) E-mail: k238573@ie.u-ryukyu.ac.jp

b) E-mail: hiroyuki.ishihara@ntt.com

c) E-mail: morikazu@ie.u-ryukyu.ac.jp

d) E-mail: takayuki.nakachi@ieee.org

can be used without modification.

The organization of this paper is as follows. Section 2 explains the ISTA solution using deep unrolling, and Section 3 describes the proposed methods, secure LISTA and secure TISTA. Section 4 discusses the results of the Secure LISTA and Secure TISTA experiments, and finally, Section 5 summarizes and discusses future work.

2. Estimation of LASSO Solution using Deep Unrolling

Deep unrolling is a method of learning iterative algorithms using deep learning techniques such as error back propagation and stochastic gradient descent [16].

2.1 LASSO

LASSO is one of the optimization methods based on l_1 regularization for sparse modeling. Given an observation vector $\boldsymbol{y} \in \mathbb{R}^n$ and a dictionary matrix $\boldsymbol{A} \in \mathbb{R}^{n\times m}$. The general linear regression model is expressed as follows

$$\boldsymbol{y} = \boldsymbol{A}\boldsymbol{x}. \tag{1}$$

The sparse coefficient $\boldsymbol{x} \in \mathbb{R}^m$ is obtained by minimizing the following cost

$$\hat{\boldsymbol{x}} = \underset{\boldsymbol{x}\in\mathbb{R}^m}{\operatorname{argmin}} \left(\frac{1}{2}||\boldsymbol{y} - \boldsymbol{A}\boldsymbol{x}||_2^2 + \lambda||\boldsymbol{x}||_1 \right). \tag{2}$$

Algorithm 1 shows the ISTA algorithm, which is one of the LASSO solution estimation methods.

Algorithm 1 Iterative Shrinkage Thresholding Algorithm: ISTA

1: Initialization:$t = 0$
$\boldsymbol{x}_0 = \boldsymbol{A}^\top \boldsymbol{y}$, $\tau = \frac{1}{L}$ (L is the largest eigenvalue of $\boldsymbol{A}^\top \boldsymbol{A}$)
2: Main loop:Execute the following steps ($t = 0, 1, \ldots$) until the termination condition is met.
・Gradient descent step
$\boldsymbol{r}_t = \boldsymbol{x}_t + \tau \boldsymbol{A}^\top (\boldsymbol{y} - \boldsymbol{A}\boldsymbol{x}_t)$
・Shrinkage step
$\boldsymbol{x}_{t+1} = S_\tau(\boldsymbol{r}_t)$
where $S_\tau(\cdot)$ is a soft thresholding function, as shown in Fig. 1.

2.2 LISTA

Gregor and LeCun proposed a method called LISTA [13], which combines ISTA and deep expansion techniques for fast convergence to a solution. LISTA is an algorithm that adds $\boldsymbol{B}_t \in \mathbb{R}^{m\times m}$ and $\boldsymbol{S}_t \in \mathbb{R}^{m\times n}$ as learnable parameters in the gradient step of ISTA. The algorithm of LISTA is shown in Algorithm 2.

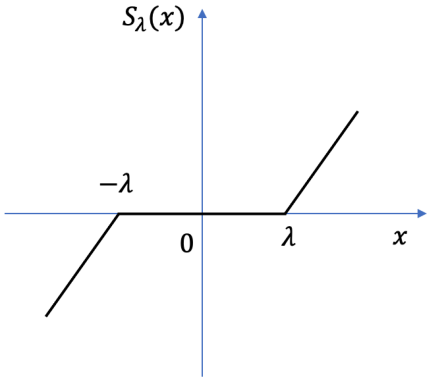

Fig. 1 Soft threshold function.

Algorithm 2 LISTA

Input: $\boldsymbol{y}$,$\boldsymbol{A}$
Output: $\boldsymbol{x}$

1: $t = 0$, Initial value of $\boldsymbol{x}$ is set to 0.
2: Compute $\boldsymbol{r}_t$ (the next value of $\boldsymbol{x}$).
$\boldsymbol{r}_t = \boldsymbol{B}_t \boldsymbol{x}_t + \boldsymbol{S}_t \boldsymbol{y}$
3: Update the value of $\boldsymbol{x}$ by applying a soft-thresholding function.
$\boldsymbol{x}_{t+1} = S_{\tau_t}(\boldsymbol{r}_t)$
4: Repeat steps 2-3 until the termination condition is met.

2.3 TISTA

Itoh et al. and others proposed TISTA [14], [15], a sparse signal reconstruction algorithm that applies deep unrolling to ISTA. TISTA is characterized by a small number of trainable parameters, fast convergence, and high interpretability of the algorithm. It adjusts the step size parameter appearing in the gradient descent step using a learning process. In most cases, TISTA has been confirmed to show faster convergence to the solution compared to ISTA and LISTA. The TISTA algorithm is shown in Algorithm 3.

Algorithm 3 TISTA

Input: $\boldsymbol{y}$, $\boldsymbol{A}$
Output: $\boldsymbol{x}$

1: $t = 0$, Initial value of $\boldsymbol{x}$ is set to 0.
2: Compute $\boldsymbol{r}_t$ (the next value of $\boldsymbol{x}$).
$\boldsymbol{r}_t = \boldsymbol{x}_t + \gamma_t \boldsymbol{W}(\boldsymbol{y} - \boldsymbol{A}\boldsymbol{x}_t)$
$v_t^2 = \max\left\{ \frac{||\boldsymbol{y} - \boldsymbol{A}\boldsymbol{x}_t||_2^2 - m\sigma^2}{\mathrm{tr}(\boldsymbol{A}^\top \boldsymbol{A})}, \epsilon \right\}$
$\tau_t^2 = \frac{v_t^2}{n}(n + (\gamma_t^2 - 2\gamma_t)m) + \frac{\gamma_t^2 \sigma^2}{n}\mathrm{tr}(\boldsymbol{W}\boldsymbol{W}^\top)$.
3: Update the value of $\boldsymbol{x}$ by applying a soft-thresholding function.
$\boldsymbol{x}_{t+1} = \eta_{MMSE}(\boldsymbol{r}_t; \tau_t^2)$
4: Repeat steps 2-3 until the termination condition is met.

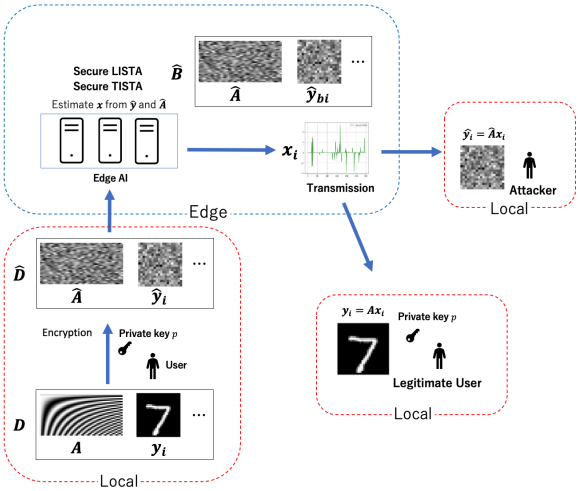

Fig. 2 Use case scenario for the proposed secure LISTA and secure TISTA.

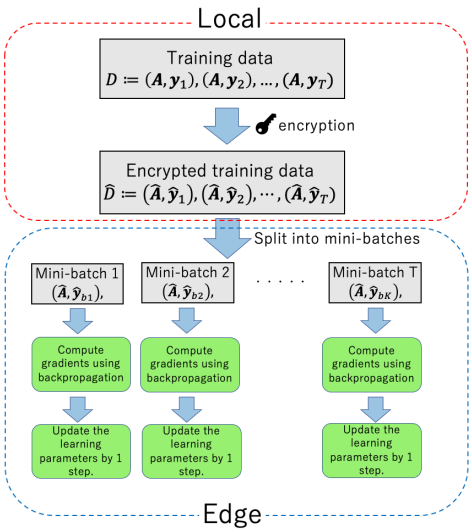

Fig. 3 A mini-batch learning method used for secure deep unrolling.

3. Proposed Method

In this section, we propose secure LISTA and secure TISTA, which are privacy-preserving versions of LISTA and TISTA.

3.1 Overview

Figure 2 shows use case scenario for the proposed secure LISTA and secure TISTA. At the local site, we have the following training data:

$$D := (\boldsymbol{A}, \boldsymbol{y}_1), (\boldsymbol{A}, \boldsymbol{y}_2), ..., (\boldsymbol{A}, \boldsymbol{y}_T), \tag{3}$$

where $\boldsymbol{y}_i \in \mathbb{R}^n$ represents the observed signal, where i denotes the sample number [†]. First, the generation of encrypted training data is performed locally. The encrypted training data is generated by using a random unitary matrix:

$$\hat{D} := (\hat{\boldsymbol{A}}, \hat{\boldsymbol{y}}_1), (\hat{\boldsymbol{A}}, \hat{\boldsymbol{y}}_2), ..., (\hat{\boldsymbol{A}}, \hat{\boldsymbol{y}}_T), \tag{4}$$

where $\hat{\boldsymbol{A}} \in \mathbb{R}^{n \times m}$ and $\hat{\boldsymbol{y}}_i \in \mathbb{R}^n$ are the encrypted versions of $\boldsymbol{A}$ and $\boldsymbol{y}_i$, respectively.

Then, the encrypted training data $\hat{D}$ is transmitted to the edge. At the edge, the encrypted training data $\hat{D}$ is split into mini-batches. The following equation represents the mini-batched training data:

$$\hat{B} := (\hat{\boldsymbol{A}}, \hat{\boldsymbol{y}}_{b1}), (\hat{\boldsymbol{A}}, \hat{\boldsymbol{y}}_{b2}), ..., (\hat{\boldsymbol{A}}, \hat{\boldsymbol{y}}_{bK}), \tag{5}$$

where, the size K denotes the mini-batch size. Figure 3 shows an overview of the mini-batch learning method used for secure deep unrolling. Secure LISTA and secure TISTA are executed while the training data $\hat{B}$ is still encrypted, and the sparse coefficient $\boldsymbol{x}_i$ is estimated. Even if the training data $\hat{B}$ and $\boldsymbol{x}_i$ are leaked, attackers cannot obtain the estimated value of $\boldsymbol{y}_i$. Since the legitimate users have the private key p, they can obtain the estimated value of $\boldsymbol{y}_i$ by using the known dictionary $\boldsymbol{A}$ and the estimated $\boldsymbol{x}_i$.

[†]Note that the subscript i is different from the subscript t in Algorithms 1-5, which denotes the iteration number.

3.2 Privacy Preserving Computation using Random Unitary Transformation

In secure computations based on random unitary transformation, the observed signal $\boldsymbol{y}_i$ and the dictionary $\boldsymbol{A}$ are transformed into encrypted signals $\hat{\boldsymbol{y}}_i$ and encrypted dictionary $\hat{\boldsymbol{A}}$ as shown in the following equation.

$$\hat{\boldsymbol{y}}_i = \boldsymbol{Q}_p \boldsymbol{y}_i, \tag{6}$$

$$\hat{\boldsymbol{A}} = \boldsymbol{Q}_p \boldsymbol{A}, \tag{7}$$

where $\boldsymbol{Q}_p \in \mathbb{R}^{n \times n}$ represents the random unitary matrix generated by the private key p. The random unitary matrices are originally defined as complex matrices, but in this section, they are treated as real matrices. The random unitary matrix $\boldsymbol{Q}_p$ has the following property

$$\boldsymbol{Q}_p^\top \boldsymbol{Q}_p = \boldsymbol{I}, \tag{8}$$

where $[\cdot]^\top$ denotes the transpose and I represents the identity matrix. The generation of random unitary transform $\boldsymbol{Q}_p$ has been investigated by methods such as the Gram-Schmidt orthogonalization method and combining multiple unitary matrices [4]. Signal transformations based on random unitary transforms generally have the following properties

- Property 1: Norm isometry ($||\boldsymbol{y}_i||_2^2 = ||\hat{\boldsymbol{y}}_i||_2^2$)
- Property 2: Conservation of Euclidean distance ($||\boldsymbol{y}_i - \boldsymbol{y}_j||_2^2 = ||\hat{\boldsymbol{y}}_i - \hat{\boldsymbol{y}}_j||_2^2$)
- Property 3: Conservation of inner product ($\boldsymbol{y}_i^T \boldsymbol{y}_j = \hat{\boldsymbol{y}}_i^T \hat{\boldsymbol{y}}_j$)

These properties allow the sparse modeling coefficient estimation algorithm [5] and the dictionary learning algorithm [6], [7] to be used in the secure domain without performance degradation.

In the encrypted domain, given an encrypted observation vector $\hat{\boldsymbol{y}}$ and a dictionary matrix $\hat{\boldsymbol{A}}$, the LASSO solution to estimate and sparse coefficients $\boldsymbol{x} \in \mathbb{R}^m$ is obtained by minimizing the following cost:

$$\hat{\boldsymbol{x}} = \underset{\boldsymbol{x}\in\mathbb{R}^m}{\operatorname{argmin}} \left(\frac{1}{2}||\hat{\boldsymbol{y}} - \hat{\boldsymbol{A}}\boldsymbol{x}||_2^2 + \lambda||\boldsymbol{x}||_1 \right). \tag{9}$$

In the next section, we will explain the proposed method that utilizes this characteristic.

3.3 Secure LISTA

We propose secure LISTA that can perform with the same accuracy regardless of whether it is encrypted using a random unitary transformation. Algorithm 4 shows an algorithm for estimating the LASSO solution $\boldsymbol{x}$ by secure LISTA. The algorithm estimates the sparse coefficients $\boldsymbol{x}$ using the encrypted observed signal $\hat{\boldsymbol{y}}$ and the encrypted dictionary matrix $\hat{\boldsymbol{A}}$, which are encrypted by a random unitary transformation.

Algorithm 4 Proposed method: Secure LISTA

Input: $\hat{\boldsymbol{y}} = \boldsymbol{Q}_P\boldsymbol{y}, \hat{\boldsymbol{A}} = \boldsymbol{Q}_P\boldsymbol{A}$
Output: $\boldsymbol{x}$

1: $t = 0$, Initial value of $\boldsymbol{x}$ is set to 0.
2: Compute $\boldsymbol{r}_t$ (the next value of $\boldsymbol{x}$)
$\boldsymbol{r}_t = \boldsymbol{B}_t\boldsymbol{x}_t + \boldsymbol{S}_t\hat{\boldsymbol{y}}$
3: Update the value of $\boldsymbol{x}$ by applying a soft-thresholding function.
$\boldsymbol{x}_{t+1} = S_{\tau_t}(\boldsymbol{r}_t)$
4: Repeat steps 2-3 until the termination condition is met.

The LASSO solution obtained from LISTA remains the same value, even when the observed signal $\boldsymbol{y}$ and dictionary $\boldsymbol{A}$ are encrypted using a random unitary transformation, as when they are not encrypted. This proof is shown in Appendix Appendix A.

3.4 Secure TISTA

In this section, we describe the secure TISTA algorithm. The estimation algorithm for the LASSO solution $\boldsymbol{x}$ using secure TISTA is shown in Algorithm 5. Similar to LISTA, the observed signal $\boldsymbol{y}$ and the dictionary matrix $\boldsymbol{A}$ are encrypted using a random unitary transformation.

Algorithm 5 Proposed method: Secure TISTA

Input: $\hat{\boldsymbol{y}} = \boldsymbol{Q}_P\boldsymbol{y}, \hat{\boldsymbol{A}} = \boldsymbol{Q}_P\boldsymbol{A}$
Output: $\boldsymbol{x}$

1: $t = 0$, Initial value of $\boldsymbol{x}$ is set to 0.
2: Compute $\boldsymbol{r}_t$ (the next value of $\boldsymbol{x}$)
$\boldsymbol{r}_t = \boldsymbol{x}_t + \gamma_t\boldsymbol{W}(\hat{\boldsymbol{y}} - \hat{\boldsymbol{A}}x_t)$
$v_t^2 = \max\left\{ \frac{||\hat{\boldsymbol{y}}-\hat{\boldsymbol{A}}\boldsymbol{x}_t||_2^2 - m\sigma^2}{\mathrm{tr}(\hat{\boldsymbol{A}}^\top\hat{\boldsymbol{A}})}, \epsilon \right\}$
$\tau_t^2 = \frac{v_t^2}{n}(n + (\gamma_t^2 - 2\gamma_t)m) + \frac{\gamma_t^2\sigma^2}{n}\mathrm{tr}(\boldsymbol{W}\boldsymbol{W}^\top)$.
3: Update the value of $\boldsymbol{x}$ by applying a soft-thresholding function.
$\boldsymbol{x}_{t+1} = \eta_{MMSE}(\boldsymbol{r}_t; \tau_t^2)$
4: Repeat steps 2-3 until the termination condition is met.

TISTA can also estimates the coefficients $\boldsymbol{x}$ without compromising the accuracy even when the data is encrypted. This proof is shown in Appendix Appendix B.

3.5 Security Strength

We evaluate the security strength of the random unitary transform in terms of the key space of $\boldsymbol{Q}_p \in \mathbb{R}^{n\times n}$. Elements of the unitary transform are limited to real numbers. The degree of freedom is n^2, which is equal to the number of matrix elements. However, the unitary matrix is subject to the following conditions:

1. The column vectors of the unitary matrix are orthogonal to each other. The number of conditional expressions is ${}_nC_2$, which is the number of combinations selecting 2 from n column vectors.
2. The norm of each column vector is 1. The number of conditions imposed is n from the condition.

Therefore, the random unitary transformation Q_p has $n(n-1)/2$ degrees of freedom. If each element is represented by an 8-bit fixed-point number, the size of the keyspace is expressed by the following equation.

$$8^{n(n-1)/2} \tag{10}$$

Therefore, the size of the keyspace depends on the dimension of n. Compared to the keyspace used in AES, when $n = 10$, it is wider than the 128-bit case and narrower than the 256-bit case. When n is 14 or more, it is wider than 256 bits.

4. Simulation Results

In this section, we demonstrated the accuracy of secure LISTA and secure TISTA on both synthetic data, and handwritten images assuming an image reconstruction application.

4.1 Synthetic Data

In this experiment, we created a dictionary $\boldsymbol{A} \in \mathbb{R}^{n\times m}$, where

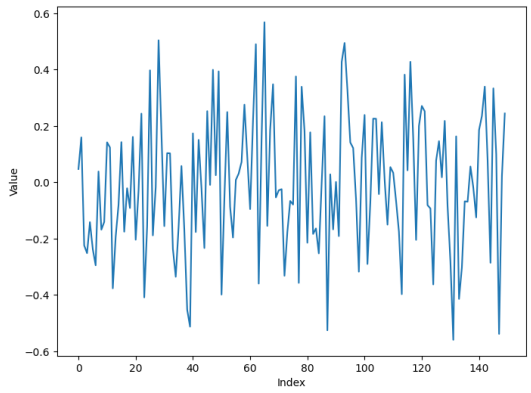

Fig. 4 An example of observed signal $\boldsymbol{y}$ used for LISTA.

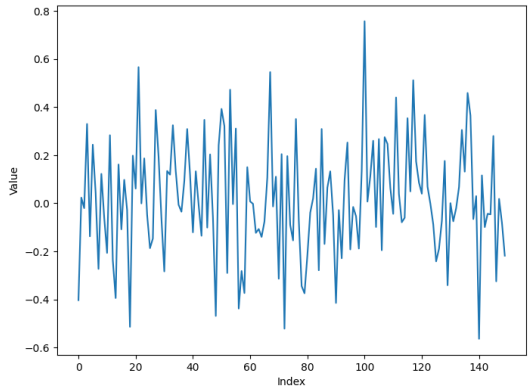

Fig. 5 An example of secure observed signal $\hat{\boldsymbol{y}}$ used for secure LISTA.

$n = 150$ and $m = 300$, that follows a normal distribution with a mean of 0 and a variance of 1. Subsequently, 2000 vectors $\boldsymbol{x}$ were generated, each with a small number of non-zero elements among the m coefficients. Then, using them, the observed signal $\boldsymbol{y} = \boldsymbol{A}\boldsymbol{x}$ is generated. The corresponding encrypted observed signal $\hat{\boldsymbol{y}}$ is generated by $\hat{\boldsymbol{y}} = \hat{\boldsymbol{A}}\boldsymbol{x} = \boldsymbol{Q}_p\boldsymbol{A}\boldsymbol{x}$, where the random unitary transformation $\boldsymbol{Q}_p$ is given by applying the Gram-Schmidt orthogonalization to a random matrix. We set the batch size to 100, dividing them into 20 batches to use as training data.

Figures 4 and 5 show examples of the observed signal$\boldsymbol{y}$ and the encrypted observation signal $\hat{\boldsymbol{y}}$ for LISTA and secure LISTA, respectively. LISTA takes an observed signal $\boldsymbol{y}$ and dictionary $\boldsymbol{A}$ as inputs, while secure LISTA uses the encrypted observation signal $\hat{\boldsymbol{y}}$ and dictionary $\hat{\boldsymbol{A}}$, both obtained using a random unitary transform, as inputs. Figure 6 shows sparse coefficients $\boldsymbol{x}$ estimated by LISTA and secure LISTA, alongside the ground truth. Secure LISTA takes the encrypted observation signal as input and estimates sparse coefficients that are nearly identical to the ground truth. Additionally, it has been confirmed that both LISTA and secure LISTA estimate the same coefficients. The correlation coefficient between the true sparse coefficients and that estimated by secure LISTA was 0.9963. These results suggest that there is no change in accuracy even when privacy is protected using the random unitary transformation.

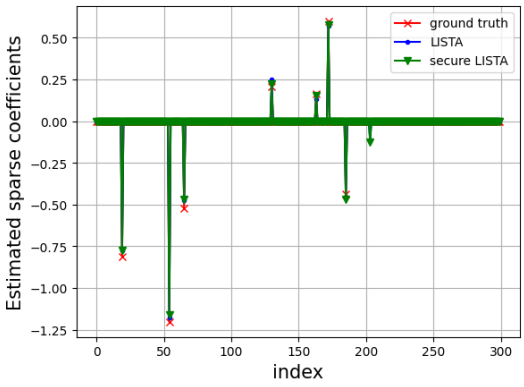

Fig. 6 Sparse coefficients estimated by secure LISTA.

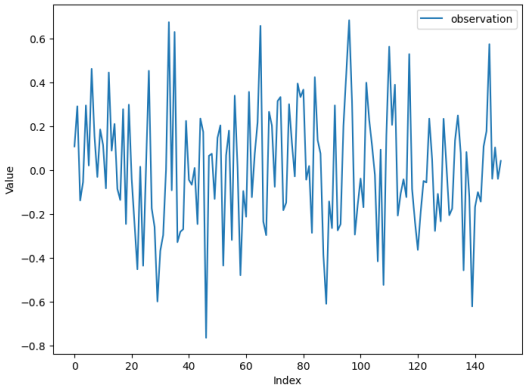

Fig. 7 An example of observed signal $\boldsymbol{y}$ used for TISTA.

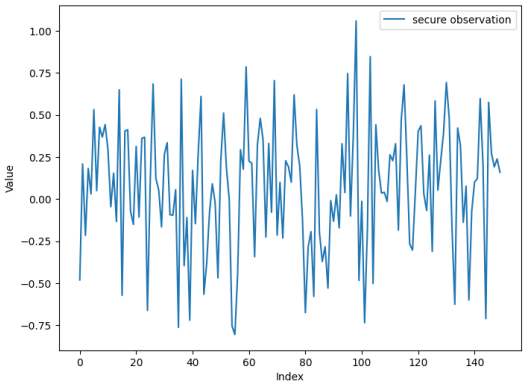

Fig. 8 An example of secure observed signal $\hat{\boldsymbol{y}}$ used for secure TISTA.

Next, we show the results of estimating sparse coefficients using TISTA and secure TISTA. Examples of the observation signal $\boldsymbol{y}$ and the corresponding encrypted observation signal $\hat{\boldsymbol{y}}$ are shown in Fig. 7 and 8, respectively. Figure 9 shows the sparse coefficients estimated by TISTA and secure TISTA, alongside the ground truth. TISTA also takes an observed signal $\boldsymbol{y}$ and dictionary $\boldsymbol{A}$ as inputs, while secure TISTA uses the encrypted observation signal $\hat{\boldsymbol{y}}$ and

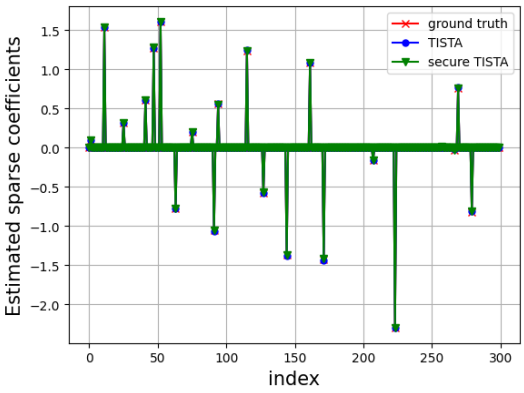

Fig. 9 Sparse Coefficients estimated by secure TISTA.

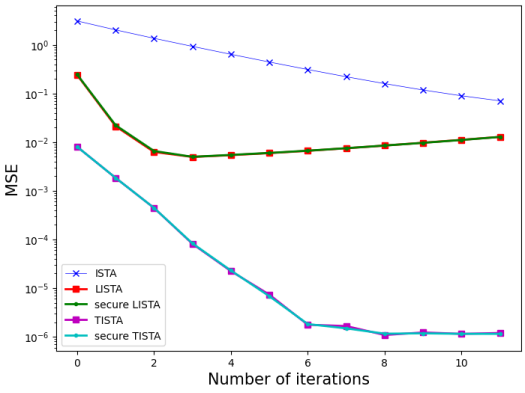

Fig. 10 MSE versus the number of iterations for secure LISTA.

dictionary $\hat{\boldsymbol{A}}$, both obtained using a random unitary transform, as inputs. Even when the data is encrypted, it is observed that secure TISTA can estimate sparse coefficients almost identical to the true values. The correlation coefficient between the true sparse coefficients and that estimated by secure TISTA was 0.9999. From these results, it can be concluded that secure TISTA can also estimate sparse coefficients almost identical to the true values. Additionally, it is observed that the coefficients estimated by TISTA and secure TISTA are also identical. These results show that there is almost no change in accuracy when combining the deep unrolling technique with the random unitary transform secrecy technique.

Figure 10 shows MSE (Mean Squared Error) during the training of ISTA, LISTA, TISTA, secure LISTA, and secure TISTA. From this figure, it can be observed that LISTA and secure LISTA, as well as TISTA and secure TISTA, exhibit nearly identical learning processes. This result suggests that secure LISTA and secure TISTA, which take encrypted signals as input, can undergo similar learning processes as their non-encrypted counterparts and estimate sparse coefficients with almost the same accuracy.

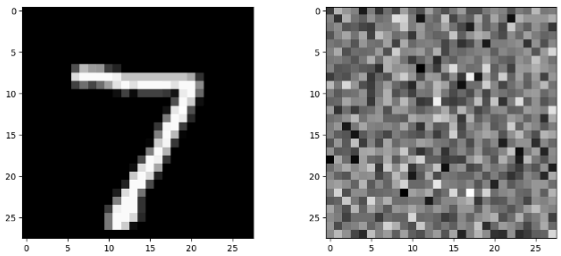

Fig. 11 Raw and encrypted images (left:raw, right:encrypted).

4.2 Image Reconstruction

We applied secure LISTA and secure TISTA to sparse image reconstruction as an example of Fig. 2. We made experiments of sparse image reconstruction using the MNIST database (Modified National Institute of Standards and Technology database) [17]. The MNIST dataset includes monochrome images of hand-written numerals and the corresponding labels. An MNIST image has $28 \times 28 = 784$ pixels where a pixel takes an integer value from 0 to 255. In this experiment, we normalize the pixel values of a MNIST image to [0, 1] and then create $\boldsymbol{y}$ by rasterizing the pixel values as 784-dimensional vectors. We set $n = 1024$ and $m = 784$, and generate an artificial dictionary $\boldsymbol{A}$ following a normal distribution with mean 0 and variance $1/m$. $\boldsymbol{y}$ and $\boldsymbol{A}$ are encrypted by applying a random unitary matrix $\boldsymbol{Q}_p$. Figure 11 shows the original image and encrypted image, respectively. It is difficult to see any visible information of the original image from the encrypted image.

In this experiment, we show that image reconstruction is feasible even from the encrypted observation signal $\hat{\boldsymbol{y}}$ and observation matrix $\hat{\boldsymbol{A}}$ using secure LISTA and secure TISTA. As shown in Figure 2, the user sends the encrypted training data $hatbmD$ to the edge device. The edge device performs a secure TISTA using the received $\hat{\boldsymbol{D}}$ to estimate the sparse coefficients $\boldsymbol{x}_i$. The edge device then sends the estimated sparse coefficients $\boldsymbol{x}_i$ to the user. The legitimate user receives the sparse coefficients $\boldsymbol{x}_i$ and can reconstruct image $\boldsymbol{A}\boldsymbol{x}_i$ using the private key p.

Figure 12 shows reconstructed images $\hat{\boldsymbol{A}}\boldsymbol{x}_i$(encrypted) and $\boldsymbol{A}\boldsymbol{x}_i$(decrypted) for sample number $i = 0, 1, \cdots, 7$. The image on the left shows the encrypted reconstruction image, and the image on the right shows the reconstructed image decrypted with the private key p. Where T is the number of iteration. Even when the input images are encrypted, it can be seen that LISTA and TISTA reconstruct MNIST images that are almost identical to the original images. The correlation coefficients between original MNIST images and reconstructed MNIST images from secure LISTA and secure TISTA were 0.9997 and 0.9996, respectively.

Figure 13 shows the image reconstruction by the non-encrypted variants of ISTA, LISTA and TISTA. Comparing Figure 12 and Figure 13, it is clear that almost the same

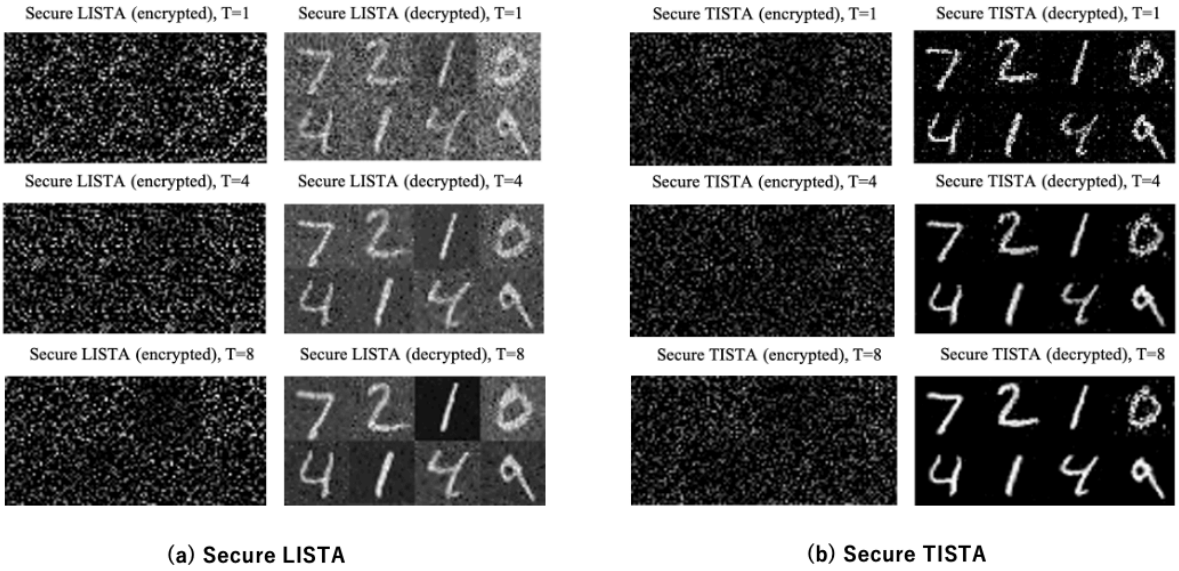

Fig. 12 Reconstructed images by the proposed Secure LISTA and Secure TISTA.

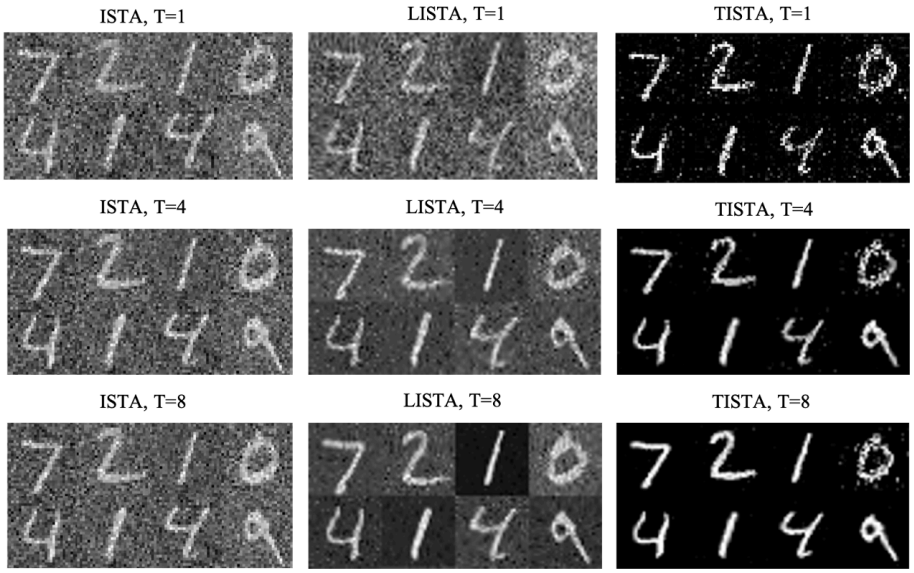

Fig. 13 Reconstructed images by the non-encrypted LISTA and the non-encrypted TISTA.

results are obtained as with the normal algorithm, even when secrecy is used. Normally, encryption would randomize the information that the data possesses, making machine learning processing impossible. From these results, it can be concluded that encrypted LISTA and TISTA can also reconstruct image that are almost identical to the true values. Figure 14 compares the change in MSE values of the MNIST image reconstruction. We compared the change in MSE between TISTA and secure TISTA and LISTA and secure LISTA during estimation. These results confirm that the same convergence acceleration is achieved with and without encryption.

As an application method of sparse modeling in the encrypted domain, its application to image processing has been proposed. Nakachi et al. proposed an Encryption-then-Compression (EtC) system for encrypted images using sparse modeling and random unitary transformation in their papers [5], [6]. In addition, a face recognition method using sparse

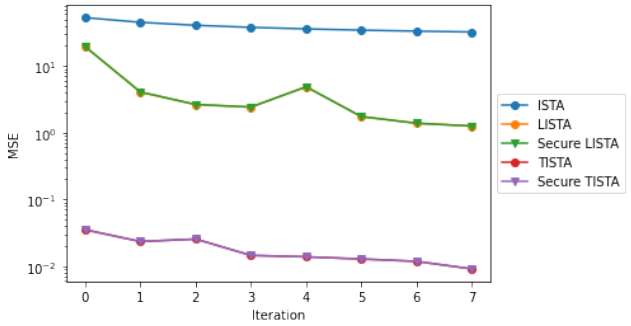

Fig. 14 MSE versus the number of iterations in MNIST image recovery.

modeling combined with ensemble learning has also been proposed [7]. We expect that applying the proposed method to these methods will further improve the performance of image compression and face recognition.

5. Conclusion and Future Work

In this paper, we proposed deep unrolling secure LISTA and secure TISTA for recovering sparse signals, integrating privacy-preserving methodologies grounded in random unitary transformation. The proposed methods are LASSO-based sparse modeling estimation methods and can be implemented in the encrypted domain. The effectiveness of these methods was validated through simulations of sparse signal recovery using artificially generated data and image reconstruction. The proposed methods achieved almost the same estimation accuracy and learning performance as the non-encrypted variants of LISTA and TISTA.

In the future, we plan to study algorithms to perform image denoising and single image super-resolution in the secure domain using secure LISTA and secure TISTA.

References

[1] K. Nuida, "Recent research topics fully homomorphic encryption", IEICE, vol.99, No.12, pp.1150-1183, 2016.
[2] E. Bingham and H. Mannila, "Random projection in dimensionality reduction:Applications to image and text data,"Proc. 7th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining (KDD), 2001, pp. 245-250.
[3] A. B. J. Teoh, A. Goh, and D. C. L. Ngo, " Random multispace quantization as an analytic mechanism for BioHashing of biometric and random identity inputs, " IEEE Trans. Pattern Anal. Mach. Intell., vol.28, no. 12, pp. 1892-1901, Dec. 2006.
[4] I. Nakamura, Y. Tonomura, and H. Kiya, "Unitary transform-based template protection and its application to l2-norm minimization problems," IEICE Transactions on Information and Systems, vol. E99-D, no.1, pp. 60-68, Jan. 2016.
[5] T. Nakachi, H. Kiya, "Secure OMP computation maintaining sparse representations and its application to EtC systems," IEICE Transactions on Information and Systems, vol. E103-D, no. 9, 2020.
[6] T. Nakachi, Y. Bandoh, H. Kiya, "Secure overcomplete dictionary learning for sparse representation," IEICE Transactions on Information and Systems, vol. E103.D(1) pp.50-58, 2020.
[7] Y. Wang and T. Nakachi, "A privacy-preserving learning framework for face recognition in edge and cloud networks," IEEE Access, vol. 8, pp. 136056-136070, 2020.
[8] M. Elad, " Sparse and redundant representations: from theory to applications in signal and mage processing, " Springer, 2010.
[9] I. Rish and G. Grabarnik, " Sparse modeling: Theory, algorithms, and applications, " CRC Press, 2014.
[10] H. Ishihara, and T. Nakachi, "Privacy preserving ISTA using random unitary transform", SIP Symposium, 2022.
[11] N. Yuge, T. Nakachi, and M. Nakamura, "Privacy preserving deep unrolling methods using random unitary transform", Technical Report of IEICE, May, 2023
[12] N. Yuge, T. Nakachi, and M. Nakamura, "Privacy preserving deep unrolling methods for sparse signal recovery", International Workshop on Smart Info-Media Systems in Asia (SISA 2023), Aug. 31-Sep.1, 2023
[13] K. Gregor, and Y. LeCun, "Learning fast approximations of sparse coding", Proc. 27th Int. Conf. Machine Learning, pp.399-406, 2010.
[14] D. Ito, S. Takabe, and T. Wadayama, "Trainable ISTA for sparse signal recovery", IEEE Transactions on Signal Processing, vol.67, no.12, June 15, 2019.
[15] D. Ito, S. Takabe, and T. Wadayama,"Trainable ISTA for sparse signal recovery", IEEE International Conference on Communications (ICC2019), Workshop on Promises and Challenges of Machine Learning in Communication Networks, Kansas city, May, 2018.
[16] T. Wadayama, "Fundamentals of deep learning for wireless communications", IEICE, https://github.com/wadayama/MIKA2019/blob/master/MIKA2019.pdf
[17] Y. LeCun, L.Bottou, Y. Bengio, and P. Haffner, "Gradient-based learning applied to document recognition," Proceedings of the IEEE, vol. 86. no. 11, pp. 2278-2324, 1998.

Appendix A: Secure LISTA

When $\boldsymbol{I}$ is the identity matrix, $\boldsymbol{B} = \boldsymbol{I} - \frac{1}{\mu}\boldsymbol{A}^\top\boldsymbol{A}$ and $\boldsymbol{S} = \frac{1}{\mu}\boldsymbol{A}^\top$. Therefore, when the data is encrypted, due to the properties of the random unitary matrix $\boldsymbol{Q}_p$, we have:

$$\begin{aligned}
\hat{\boldsymbol{r}}_t &= \boldsymbol{B}_t\boldsymbol{x}_t + \boldsymbol{S}_t\hat{\boldsymbol{y}} \\
&= (\boldsymbol{I} - \frac{1}{\mu}\hat{\boldsymbol{A}}^\top\hat{\boldsymbol{A}})\boldsymbol{x}_t + (\frac{1}{\mu}\hat{\boldsymbol{A}}^\top)\hat{\boldsymbol{y}} \\
&= (\boldsymbol{I} - \frac{1}{\mu}\boldsymbol{A}^\top\boldsymbol{Q}_p^\top\boldsymbol{Q}_p\boldsymbol{A})\boldsymbol{x}_t + (\frac{1}{\mu}\boldsymbol{A}^\top\boldsymbol{Q}_p^\top)\boldsymbol{Q}_p\boldsymbol{y} \\
&= (\boldsymbol{I} - \frac{1}{\mu}\boldsymbol{A}^\top\boldsymbol{A})\boldsymbol{x}_t + (\frac{1}{\mu}\boldsymbol{A}^\top)\boldsymbol{y} \\
&= \boldsymbol{B}\boldsymbol{x}_t + \boldsymbol{S}\boldsymbol{y} \\
&= \boldsymbol{r}_t
\end{aligned} \tag{A·1}$$

As $\boldsymbol{r}_t$ takes the same value before and after encryption, the soft thresholding function remains unchanged before and after encryption. Therefore, the LASSO solution obtained from LISTA will have the same value when the input is encrypted using a random unitary transformation as when it is not encrypted.

Appendix B: Secure TISTA

for $\boldsymbol{r}_t$, since $W = \boldsymbol{A}^\top(\boldsymbol{A}\boldsymbol{A}^\top)$, we have:

$$\begin{aligned}
\hat{\boldsymbol{r}}_t &= \boldsymbol{x}_t + \gamma_t\boldsymbol{W}(\hat{\boldsymbol{y}} - \hat{\boldsymbol{A}}\boldsymbol{x}_t) \\
&= \boldsymbol{x}_t + \gamma_t\boldsymbol{A}^\top\boldsymbol{Q}_p^\top(\boldsymbol{Q}_p\boldsymbol{A}\boldsymbol{A}^\top\boldsymbol{Q}_p^\top)(\boldsymbol{Q}_p\boldsymbol{y} - \boldsymbol{Q}_p\boldsymbol{A}\boldsymbol{x}_t) \\
&= \boldsymbol{x}_t + \gamma_t\boldsymbol{A}^\top(\boldsymbol{A}\boldsymbol{A}^\top)(\boldsymbol{y} - \boldsymbol{A}\boldsymbol{x}_t) \\
&= \boldsymbol{x}_t + \gamma_t\boldsymbol{W}(\boldsymbol{y} - \boldsymbol{A}\boldsymbol{x}_t)
\end{aligned}$$

$$= \boldsymbol{r}_t \tag{A· 2}$$

thus having the same value as when not encrypted. If v_t^2 is calculated in the same way,

$$\begin{aligned}
\hat{v}_t^2 &= \max\left\{\frac{||\boldsymbol{Q}_p(\boldsymbol{y}-\boldsymbol{A}\boldsymbol{x}_t)||_2^2 - m\sigma^2}{\mathrm{tr}(\boldsymbol{A}^\top\boldsymbol{Q}_p^\top\boldsymbol{Q}_p\boldsymbol{A})}, \epsilon\right\} \\
&= \max\left\{\frac{\{\boldsymbol{Q}_p(\boldsymbol{y}-\boldsymbol{A}\boldsymbol{x}_t)\}^\top\{\boldsymbol{Q}_p(\boldsymbol{y}-\boldsymbol{A}\boldsymbol{x}_t)\} - m\sigma^2}{\mathrm{tr}(\boldsymbol{A}^\top\boldsymbol{Q}_p^\top\boldsymbol{Q}_p\boldsymbol{A})}, \epsilon\right\} \\
&= \max\left\{\frac{(\boldsymbol{y}-\boldsymbol{A}\boldsymbol{x}_t)^\top(\boldsymbol{y}-\boldsymbol{A}\boldsymbol{x}_t) - m\sigma^2}{\mathrm{tr}(\boldsymbol{A}^\top\boldsymbol{A})}, \epsilon\right\} \\
&= \max\left\{\frac{||\boldsymbol{y}-\boldsymbol{A}\boldsymbol{x}_t||_2^2 - m\sigma^2}{\mathrm{tr}(\boldsymbol{A}^\top\boldsymbol{A})}, \epsilon\right\} \\
&= v_t^2
\end{aligned} \tag{A· 3}$$

As a result, v_t^2 becomes the same as the value obtained when no privacy is preserved. Finally, regarding $\mathrm{tr}(\boldsymbol{W}\boldsymbol{W}^\top)$ in τ_t^2, since $W = \boldsymbol{A}^\top(\boldsymbol{A}\boldsymbol{A}^\top)$, we can calculate:

$$\begin{aligned}
\mathrm{tr}(\hat{\boldsymbol{W}}\hat{\boldsymbol{W}}^\top) &= \mathrm{tr}(\{\hat{\boldsymbol{A}}^\top(\hat{\boldsymbol{A}}\hat{\boldsymbol{A}}^\top)\}\{\hat{\boldsymbol{A}}^\top(\hat{\boldsymbol{A}}\hat{\boldsymbol{A}}^\top)\}^\top) \\
&= \mathrm{tr}(\{\hat{\boldsymbol{A}}^\top(\hat{\boldsymbol{A}}\hat{\boldsymbol{A}}^\top)\}\{(\hat{\boldsymbol{A}}\hat{\boldsymbol{A}}^\top)^\top(\hat{\boldsymbol{A}}^\top)^\top\}) \\
&= \mathrm{tr}(\{\boldsymbol{A}^\top\boldsymbol{Q}_p^\top(\boldsymbol{Q}_p\boldsymbol{A}\boldsymbol{A}^\top\boldsymbol{Q}_p^\top)\} \\
&\qquad \{(\boldsymbol{Q}_p\boldsymbol{A}\boldsymbol{A}^\top\boldsymbol{Q}_p^\top)\boldsymbol{Q}_p\boldsymbol{A}\}) \\
&= \mathrm{tr}(\{\boldsymbol{A}^\top(\boldsymbol{A}\boldsymbol{A}^\top)\}\{(\boldsymbol{A}\boldsymbol{A}^\top)\boldsymbol{A}\}) \\
&= \mathrm{tr}(\boldsymbol{W}\boldsymbol{W}^\top)
\end{aligned} \tag{A· 4}$$

Therefore, the LASSO solution obtained from TISTA gives the same results whether the input signal is encrypted by a random unitary transformation or not.

Nichika Yuge received the B.E. degree from the Department of Engineering, Faculty of Engineering, University of the Ryukyus in 2023. Since then, he has been a master's degree student at the Graduate School of Engineering and Science, University of the Ryukyus. His research interests are in the area of information security.

Hiroyuki Ishihara received MS degree in informatics from Kyoto University, in 2016. He is currently a research engineer in NTT Network Innovation Labs. His research interests include image processing, computer vision, and multimodal signal processing for wireless communication. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan.

Morikazu Nakamura received the B.E. and M.E degrees from University of the Ryukyus in 1989 and 1991, respectively, and D.E degree from Osaka University in 1996. He was a Research Assistant from 1991 to 1996, and an associate professor from 1996 to 2006 with university of the Ryukyus, respectively. He was a visiting researcher from 1998 to 1999 at University of Zaragoza, Spain. He is currently a professor in Area of Computer Science and Intelligent Systems, Faculty of Engineering, University of the Ryukyus. His research interests include theory and applications on mathematical systems and optimization algorithms. He is a member of IEICE and IEEE.

Takayuki Nakachi received a Ph.D. degree in electrical engineering from Keio University in 1997. Since joining Nippon Telegraph and Telephone (NTT) Corporation in 1997, he has conducted 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 is currently a professor at the Information Technology Center, University of the Ryukyus. His current research interests include secure and light-weight AI technologies based on sparse modeling, and communication science. He received the 26th TELECOM System Technology Award, the 6th Paper Award of the Journal of Signal Processing, and the Best Paper Award at IEEE ISPACS2015. Dr. Nakachi is a member of the Institute of Electrical and Electronics Engineers (IEEE) and the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan.