

# プライバシー保護を考慮したスパースコーディングの秘匿演算

仲地 孝之<sup>†</sup> 貴家 仁志<sup>††</sup>

<sup>†</sup> 日本電信電話株式会社 未来ねっと研究所 〒239-0847 神奈川県横須賀市光の丘 1-1

<sup>††</sup> 首都大学東京 システムデザイン研究科 〒191-0065 東京都日野市旭ヶ丘 6-6

E-mail: <sup>†</sup>nakachi.takayuki@lab.ntt.co.jp, <sup>††</sup>kiya@tmu.ac.jp

**あらまし** スパースコーディングは生物の一次視覚野の情報処理を数学的にモデル化したものであり、観測信号を少数の基底の線型結合で表現する手法である。画像・音響信号などのメディア信号処理、脳波など生体信号の解析、機械学習など多数の分野に応用されており、その有効性が認められている。一方、メディア信号処理・生体信号の解析や機械学習などの情報処理をネットワーク上で行うエッジ/クラウドコンピューティングが急速に進んでいく。しかし、サービス提供者の信頼性欠如や事故によってデータの不正利用、流出、プライバシー侵害などの問題が危惧されている。本稿ではそのような背景から、プライバシー保護を考慮したスパースコーディングの秘匿演算法を提案する。演算を秘匿しない場合と比較して、理論的に推定性能が劣化しないことを示すとともに、シミュレーションにより有効性を確認した。

**キーワード** スパースコーディング、直交マッチング追跡法 (OMP)、ランダムユニタリ変換、秘匿演算

## Secure Computation of Sparse Coding for Privacy Protection

Takayuki NAKACHI<sup>†</sup> and Hitoshi KIYA<sup>††</sup>

<sup>†</sup> NTT Network Innovation Laboratories, Nippon Telegraph and Telephone Corp. Yokosuka, 239-0847 JAPAN

<sup>††</sup> Information and Communication Systems, Tokyo Metropolitan University, Tokyo, 191-0065, Japan

E-mail: <sup>†</sup>nakachi.takayuki@lab.ntt.co.jp, <sup>††</sup>kiya@tmu.ac.jp

**Abstract** Sparse coding represents observed signals effectively as a linear combination of a small number of bases which are chosen from the basis functions trained by the algorithm. On the other hand, cloud computing is spreading in many fields. However, the cloud computing has some serious issues for end users, such as unauthorized use and leak of data, and privacy compromise, due to unreliability of providers and some accident. In this manuscript, we propose a secure sparse coding computation. It is shown that the secure sparse coding computation enables us to not only protect observed signals, but also have the same estimation performance as that of sparse coding with unprotected observed signals.

**Key words** Sparse Coding, Orthogonal Matching Pursuit (OMP), Random Unitary Transform, Secure Computation

### 1. まえがき

スパースコーディング (Sparse Coding: SC) [1]-[12] は、元々生物の一次視覚野の計算モデルとして提案されたものであり、観測信号を少数の基底ベクトルの重み付き線形和で表現する手法である。生物の一次視覚野における受容細胞は、空間周波数成分が網膜上の特定の領域に出現すると、選択的に反応する性質を持つ。Olshausen らはこの性質を、自然画像の統計的構造を積極的に利用することによって自然画像を効率的に符号化(コーディング)するための仕組みとして獲得した [1] とする考えを提案し脚光を浴びた。現在、スパースコーディングは画像・音響信号などのメディア信号処理 [4]、脳波など生体信号の解析 [12]、機械学習など多数の分野に応用されており、その

有効性が認められている。例えば、画像処理の分野では雑音除去 [10] や画像修復 [11]、深層学習では要素技術の一つとして利用され画像識別の分野で最先端の性能を示している。

一方、近年様々な分野においてエッジ/クラウドコンピューティングが急速に普及してきている。そのアプリケーションの領域はスパースコーディングの有効性が確認されているメディア信号処理、生体信号の解析、機械学習などを含め多岐にわたる。しかしエッジ/クラウドコンピューティングの利用は、サービス提供者の信頼性を前提にしており、その信頼性の欠如や事故によって、データの不正利用や流失、プライバシーの侵害といった問題の発生が危惧されている [13]。今後のエッジ/クラウドコンピューティングの普及にとって、データの不正利用や流失、プライバシーの問題の解決は重要な課題である。

データを公開することなく、暗号化したデータを第三者に渡し計算を依頼する方法、いわゆる秘密計算が盛んに研究されている [14]-[17]。秘密計算は一般にマルチパーティプロトコルや準同型暗号に基づき実行される。しかし、除算の困難性、計算効率及び計算精度などに課題があり、ソーティング処理や幾つかの統計解析に限定されるなど、十分な普及には至っていない。さらに秘密計算では、暗号化領域での計算実行のために特別な手順を必要とし、広く普及した多くのアプリケーションソフトウェアを直接利用することは一般に困難である。

本稿では、エッジ/クラウドでの利用を想定し広く普及した多くのアプリケーションソフトウェアが直接利用可能で、かつユーザーのプライバシーの保護を考慮したスパースコーディングの秘匿演算法を提案する。具体的には、係数選択のアルゴリズムとして広く用いられている直交マッチング追跡法 (Orthogonal Matching Pursuit: OMP) の秘匿演算法を検討した。秘匿演算としてランダムユニタリ行列を用い、観測信号と辞書行列の変換を行う。ランダムユニタリ変換を用いた秘匿演算に関する先行研究として、キャンセルラビオメトリクスのためのテンプレート保護法が研究されている [19]-[20]。本稿では、この方法が持つユニタリ性が OMP の秘匿演算を可能とする重要な性質であることを証明する。シミュレーションにより、演算を秘匿しない場合と比較して、係数選択の推定性能が劣化しないことを検証した。

本稿の構成は、以下の通りである。2. 節でスパースコーディングの概要を説明し、3. 節でスパースコーディングの秘匿演算法を提案する。4. 節でシミュレーション結果、最後にまとめと今後の課題について述べる。

## 2. スパースコーディング

本節ではスパースコーディングの定式化を行うとともに、代表的なアルゴリズムである直交マッチング追跡法 (Orthogonal Matching Pursuit: OMP) について説明する。

### 2.1 定式化

図 1 に示すように、 $M$  次元の観測信号ベクトル  $\mathbf{y} \in \mathbb{R}^M$  が、 $K$  個の基底の線形結合で表せると仮定する。

$$\mathbf{y} = \mathbf{D}\mathbf{x} \quad (1)$$

ただし、 $\mathbf{D} = \{\mathbf{d}_1, \dots, \mathbf{d}_K\} \in \mathbb{R}^{M \times K}$  は基底  $\mathbf{d}_i$  (列ベクトル) を要素とする辞書行列であり、 $\mathbf{x} = \{x_1, \dots, x_K\} \in \mathbb{R}^K$  はスパース係数である。スパース係数は少数の  $k$  個の係数のみが非ゼロの値を取り、残りの大部分の係数はゼロの値を取る。このように、非ゼロ要素が全体に対して少数である状態をスパース (Sparse: 疎) と呼ぶ。辞書行列  $\mathbf{D}$  は事前に与えられるか、または観測データに基づき学習により適応的に推定される。

一般的に  $K > M$  (基底の数が、観測信号の次元よりも大きい) であり、過完備な辞書行列を用いる。信号の次元より多い基底による表現  $\mathbf{y} = \mathbf{D}\mathbf{x}$  では  $\mathbf{x}$  の一意性を保証することが出来ないため、通常は観測信号  $\mathbf{y}$  の表現に利用される基底を  $\mathbf{D}$  のうちの一部に制限する。つまり、 $\|\mathbf{x}\|_0$  で  $\mathbf{x}$  の  $l_0$  ノルム、すなわちベクトル  $\mathbf{x}$  の非ゼロ成分の数を表すとして、スパースコーディ

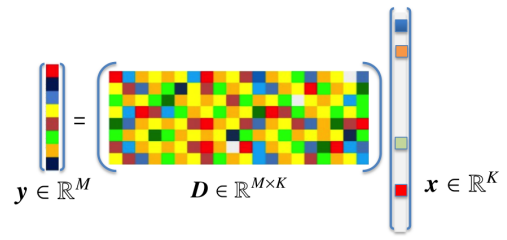


図 1 スパースコーディング: 少数の基底ベクトルの重み付き線形和で表現する線形システム。

ングは典型的には最適化問題

$$\min_{\mathbf{x}} \|\mathbf{y} - \mathbf{D}\mathbf{x}\|_2^2 + \lambda \|\mathbf{x}\|_0, \quad \lambda > 0 \quad (2)$$

として定式化される。しかしながら、この問題は全ての基底の組み合わせを試さないと最適解が得られない組合せ最適化問題であり、NP 困難であることが知られている [5]。そこで、 $l_1$  ノルムへの緩和問題

$$\min_{\mathbf{x}} \|\mathbf{y} - \mathbf{D}\mathbf{x}\|_2^2 + \lambda \|\mathbf{x}\|_1, \quad \lambda > 0 \quad (3)$$

を考えることが多い。この  $l_1$  ノルム正則化問題は線型計画問題として表現することが可能である。

### 2.2 係数選択の方法

観測信号  $\mathbf{y}$  と辞書  $\mathbf{D}$  が与えられた時、 $\mathbf{y}$  を  $\mathbf{D}\mathbf{x}$  で近似するような係数  $\mathbf{x}$  を求める問題を、(狭義の) スパースコーディング問題と呼ぶ。ここでは式 (2) の最適化問題を、再構成誤差を一定の閾値以下に抑えた上で出来るだけ少ない数の基底の線型結合で信号を近似する問題

$$\mathbf{x} = \arg \min_{\mathbf{x}} \|\mathbf{y} - \mathbf{D}\mathbf{x}\|_2^2 \quad \text{subject to} \quad \|\mathbf{x}\|_0 < \epsilon \quad (4)$$

として考える。この問題に対する解法として、貪欲法に基づく方法や  $l_0$  制約を  $l_1$  制約で緩和した上で解く方法など、数多くのアルゴリズムが提案されている。スパースコーディングのアルゴリズムとして直交マッチング追跡法 (OMP) [8] と反復再重み付け最小二乗法 (Iterative. Reweighted Least Squares: IRLS) [9] はよく知られている。

本稿では、直交マッチング追跡法の秘匿演算について検討する。直交マッチング追跡法は  $l_0$  制約に基づく近似解法であり、観測信号の近似に利用する係数の添字集合の中から「サポート」、すなわち非ゼロ係数の添字集合  $S$  を見つけ出すアルゴリズムである。初めはサポートは空集合であるとして、観測信号  $\mathbf{y}$  を基底の線型結合で近似した時の残差を最小にするように新たな基底をサポート集合に一つ一つ追加していき、サポートに含まれる基底のみで信号を近似した時の残差が  $\epsilon$  以下になったら停止する。残差の低減に寄与する基底を順次選択していく貪欲法であり、解の最適性は保証されないが、多くの場合優れた近似を与えることが知られている。以下に、直交マッチング追跡法のアルゴリズムを示す。

---

直交マッチング追跡法 (OMP) アルゴリズム

---

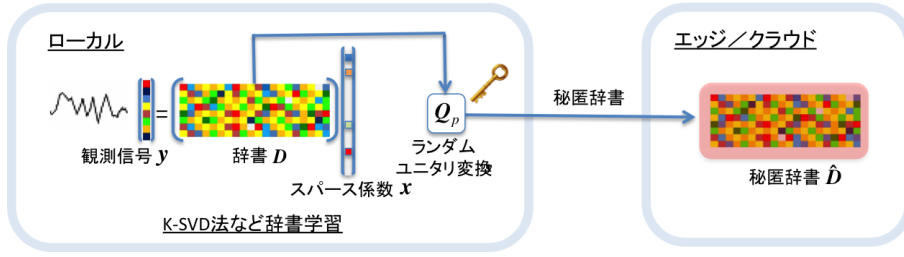


図2 事前準備：ローカルでの辞書学習と秘匿.

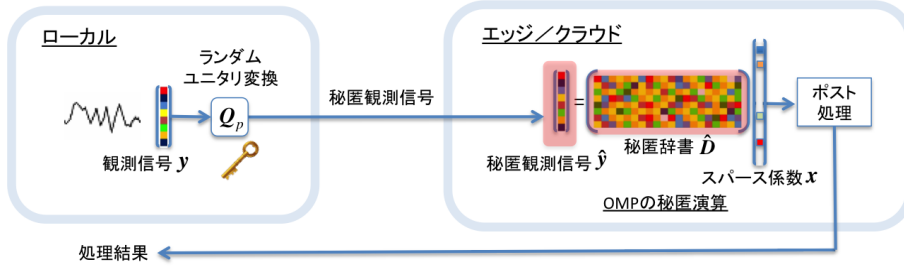


図3 実行：エッジ/クラウドでのスパースコーディングの秘匿演算.

1) 初期化： $k = 0$

初期解  $\mathbf{x}^0 = \mathbf{0}$

初期残差  $\mathbf{r}^0 = \mathbf{y} - \mathbf{D}\mathbf{x}^0 = \mathbf{y}$

解の初期サポート  $S^0 = \emptyset$

2) メインループ

$k \rightarrow k+1$  とし、以下のステップを実行する。

1. 近似誤差：

$$\epsilon(i) = \min_{x_i} \|x_i \mathbf{d}_i - \mathbf{r}^{k-1}\|_2^2 = \|\mathbf{r}^{k-1}\|_2^2 - \frac{(\mathbf{d}_i \cdot \mathbf{r}^{k-1})^2}{\|\mathbf{d}_i\|_2^2} \quad (5)$$

2. サポートの更新：

$$i_0 = \arg \min_{i \in S^{k-1}} \{\epsilon(i)\}, S^k = S^{k-1} \cup \{i_0\} \quad (6)$$

3. サポート内での最良解の探索：

$$\tilde{\mathbf{x}}^k = \arg \min_{\mathbf{x}_{S^k}} \|\mathbf{y} - \mathbf{D}_{S^k} \mathbf{x}_{S^k}\|_2^2 = (\mathbf{D}_{S^k}^* \mathbf{D}_{S^k})^{-1} (\mathbf{D}_{S^k}^* \mathbf{y}) \quad (7)$$

4. 残差の更新：

$$\mathbf{r}^k = \mathbf{y} - \mathbf{D}_{S^k} \tilde{\mathbf{x}}^k \quad (8)$$

5. 停止条件：

$$\|\mathbf{r}^k\|_2 < \epsilon$$

## 2.3 辞書学習

辞書行列は離散コサイン変換やフーリエ変換、ウェーブレット変換 [21] あるいはカーブレット変換 [22] のように予め基底を用意しておく方法と、信号から基底を学習する方法がある。スパースコーディングのための辞書学習の代表的な手法が MOD (Method of Optimal Direction) [6] と K-SVD (K-Singular Value Decomposition) [7] である。MOD は  $\mathbf{y}$  と  $\mathbf{D}\mathbf{x}$  の間の二乗誤差の最小化に疑似逆行列を使用する。K-SVD は k-means 法を一般化したものと位置づけられ、MOD より高速な反復的アルゴリズムとして提案された。

## 3. スパースコーディングの秘匿演算

本節では 3.1 節でランダムユニタリ行列に基づく秘匿演算の基本性質について述べ、3.2 節で直交マッチング追跡法 (OMP) の秘匿演算について提案する。

### 3.1 ランダムユニタリ行列に基づく秘匿演算

先行研究において、キャンセラブルバイオメトリクスのための一方法として、ランダムユニタリ変換に基づくテンプレート保護法が研究されている [19]-[20]。

一般的にランダムユニタリ行列に基づく秘匿演算では、鍵  $p$  によって生成されるランダムユニタリ行列  $\mathbf{Q}_p$  を用いた変換  $T(\cdot)$  により、信号  $\mathbf{f}_i$  ( $i = 1, \dots, L$ ) が秘匿信号  $\hat{\mathbf{f}}_i$  へ変換される。

$$\hat{\mathbf{f}}_i = T(\mathbf{f}_i, p) = \mathbf{Q}_p \mathbf{f}_i \quad (10)$$

但し  $\mathbf{Q}_p \in \mathbb{C}^{N \times N}$  であり、

$$\mathbf{Q}_p^* \mathbf{Q}_p = \mathbf{I} \quad (11)$$

を満たす。ここで  $[\cdot]^*$  はエルミート転置、 $\mathbf{I}$  は単位行列を表す。

ランダムユニタリ変換  $\mathbf{Q}_p$  の生成は、グラムシュミットの直交化を用いる方法や、複数のユニタリ行列を組み合わせることで  $\mathbf{Q}_p$  を生成する方法が検証されている。ランダムユニタリ行列に基づき変換された信号は、一般的に以下の特徴を持つ。

引き続き解析を容易にするために、ここで基底ベクトル  $\mathbf{d}_i$  を

$$\mathbf{d}_i = \mathbf{D} \boldsymbol{\delta}_i \quad (9)$$

で定義する。但し  $\boldsymbol{\delta}_i$  は  $\boldsymbol{\delta}_i = [(0, \dots, 0, \delta(i), 0, \dots, 0)]^T$  の  $i$  番目の要素が 1 でそれ以外の要素はゼロの列ベクトルである。 $\boldsymbol{\delta}_i$  を用いて、式 (5) の近似誤差を以下のように表現する。

$$\epsilon(i) = \min_{x_i} \|x_i \mathbf{D} \boldsymbol{\delta}_i - \mathbf{r}^{k-1}\|_2^2 = \|\mathbf{r}^{k-1}\|_2^2 - \frac{(\mathbf{D} \boldsymbol{\delta}_i \cdot \mathbf{r}^{k-1})^2}{\|\mathbf{D} \boldsymbol{\delta}_i\|_2^2} \quad (5')$$

特徴 1: ノルム不変

$$\|\mathbf{Q}_p \mathbf{a}\|_2^2 = \|\mathbf{a}\|_2^2 \quad (12)$$

特徴 2: ユークリッド距離の保存

$$\|\mathbf{a} - \mathbf{b}\|_2^2 = \|\hat{\mathbf{a}} - \hat{\mathbf{b}}\|_2^2 \quad (13)$$

特徴 3: 内積の保存

$$\mathbf{a}^* \mathbf{b} = \hat{\mathbf{a}}^* \hat{\mathbf{b}} \quad (14)$$

ただし、 $\mathbf{a}$  と  $\mathbf{b}$  は大きさが等しい任意のベクトルであり、 $\hat{\mathbf{a}}$  と  $\hat{\mathbf{b}}$  はそれぞれランダムユニタリ行列  $\mathbf{Q}_p$  により変換された信号である。

### 3.2 直交マッチング追跡法 (OMP) の秘匿演算

エッジ/クラウドでスパースコーディングの秘匿演算を行うアーキテクチャを図 2 ならびに図 3 に示す。図 2 の事前準備では、ローカルにおいて辞書行列  $\mathbf{D}$  を予め用意または K-SVD 法などを用い学習して生成する。その後、辞書行列  $\mathbf{D}$  を秘匿辞書行列  $\hat{\mathbf{D}}$  へ変換しクラウドへ伝送する。図 3 のスパースコーディングの秘匿演算の実行では、最初にローカルにおいて観測信号  $\mathbf{y}$  を秘匿観測信号  $\hat{\mathbf{y}}$  へ変換しクラウドへ伝送する。次にクラウドでは、事前に転送された秘匿辞書行列  $\hat{\mathbf{D}}$  と秘匿観測信号  $\hat{\mathbf{y}}$  を用いて OMP のアルゴリズムを実行してスパース係数を推定する。

提案するスパースコーディングの秘匿演算では、次式のように秘匿された観測信号  $\hat{\mathbf{y}}$  ならびに辞書行列  $\hat{\mathbf{D}}$  を生成する。

$$\hat{\mathbf{y}} = T(\mathbf{y}, p) = \mathbf{Q}_p \mathbf{y} \quad (15)$$

$$\hat{\mathbf{D}} = T(\mathbf{D}, p) = \mathbf{Q}_p \mathbf{D} \quad (16)$$

このとき式 (4) に代わり、次式に示す  $\hat{\mathbf{y}}$  と  $\hat{\mathbf{D}}$  が与えられた時の最適化問題を考える。

$$\hat{\mathbf{x}} = \arg \min_{\mathbf{x}} \|\hat{\mathbf{y}} - \hat{\mathbf{D}} \mathbf{x}\|_2^2 \quad \text{subject to} \quad \|\mathbf{x}\|_0 < \epsilon \quad (17)$$

上式を直交マッチング追跡法によって解き、得られたスパース係数  $\hat{\mathbf{x}}$  が、観測信号  $\mathbf{y}$  と辞書行列  $\mathbf{D}$  を秘匿しない場合に得られたスパース係数  $\mathbf{x}$  と等しくなることを証明する。なお、ランダムユニタリ行列に基づき変換された秘匿信号ではユークリッド距離の保存の性質が成立するものの、これらのスパース係数が一致することは自明ではない。直交マッチング追跡法は  $l_0$  制約に基づく近似解法であり、解が一致するかアルゴリズムを検証する必要がある。

#### 直交マッチング追跡法 (OMP) の秘匿演算アルゴリズム

1) 初期化:  $k = 0$

初期解  $\mathbf{x}^0 = \mathbf{0}$

初期残差  $\hat{\mathbf{r}}^0 = \hat{\mathbf{y}} - \hat{\mathbf{D}} \mathbf{x}^0 = \hat{\mathbf{y}} = \mathbf{Q}_p \mathbf{y}$

解の初期サポート  $S^0 = \emptyset$

2) メインループ

$k \rightarrow k+1$  とし、以下の 1-5 のステップを実行する。

1. 近似誤差:

式 (5') で辞書行列  $\mathbf{D}$  と残差  $\mathbf{r}^{k-1}$  を秘匿した  $\hat{\mathbf{D}}$  ならびに  $\hat{\mathbf{r}}^{k-1}$  で置き換え、式 (15)(16) の関係式を用いると、近似誤差は次式で表される。

$$\begin{aligned} \hat{\epsilon}(i) &= \min_{\hat{\mathbf{x}}_i} \|\hat{\mathbf{x}}_i \hat{\mathbf{D}} \delta_i - \hat{\mathbf{r}}^{k-1}\|_2^2 \\ &= \|\hat{\mathbf{r}}^{k-1}\|_2^2 - \frac{(\hat{\mathbf{D}} \delta_i \cdot \hat{\mathbf{r}}^{k-1})^2}{\|\hat{\mathbf{D}} \delta_i\|_2^2} \\ &= \|\mathbf{Q}_p \mathbf{r}^{k-1}\|_2^2 - \frac{(\mathbf{Q}_p \mathbf{D} \delta_i \cdot \mathbf{Q}_p \mathbf{r}^{k-1})^2}{\delta_i^* \hat{\mathbf{D}}^* \hat{\mathbf{D}} \delta_i} \end{aligned} \quad (18)$$

ユニタリ行列の性質より、 $\|\mathbf{Q}_p \mathbf{r}^{k-1}\|_2^2 = \|\mathbf{r}^{k-1}\|_2^2$  (ノルム不変)、 $\mathbf{Q}_p \mathbf{D} \delta_i \cdot \mathbf{Q}_p \mathbf{r}^{k-1} = \mathbf{D} \delta_i \cdot \mathbf{r}^{k-1}$  (内積の保存)、 $\hat{\mathbf{D}}^* \hat{\mathbf{D}} = \mathbf{D}^* \mathbf{D}$  (内積の保存) が成立することから、式 (18) は以下のように書き換えることができる。

$$\hat{\epsilon}(i) = \|\mathbf{r}^{k-1}\|_2^2 - \frac{(\mathbf{D} \delta_i \cdot \mathbf{r}^{k-1})^2}{\|\mathbf{D} \delta_i\|_2^2} \quad (19)$$

上式は式 (5') と等しく、秘匿信号を用いて計算される近似誤差  $\hat{\epsilon}(i)$  は原信号 (秘匿前の信号) を用いて計算される近似誤差  $\epsilon(i)$  と等しいことがわかる。

2. サポートの更新:

$\hat{\epsilon}(i) = \epsilon(i)$  より、次式が成立する。

$$\begin{aligned} i_0 &= \arg \min_{i \in S^{k-1}} \{\hat{\epsilon}(i)\} \\ &= \arg \min_{i \in S^{k-1}} \{\epsilon(i)\}, S^k = S^{k-1} \cup \{i_0\} \end{aligned} \quad (20)$$

3. サポート内での最良解の探索:

サポート内での最良解  $\hat{\mathbf{x}}^k$  は

$$E_2 = \|\hat{\mathbf{y}} - \hat{\mathbf{D}}_{S^k} \mathbf{x}_{S^k}\|_2^2 \quad (21)$$

の  $\mathbf{x}_{S^k}$  に関する最小化  $\frac{\partial E_2}{\partial \mathbf{x}_{S^k}} = 0$  を解くことにより、次式の通り得られる。

$$\begin{aligned} \hat{\mathbf{x}}^k &= \arg \min_{\mathbf{x}_{S^k}} \|\hat{\mathbf{y}} - \hat{\mathbf{D}}_{S^k} \mathbf{x}_{S^k}\|_2^2 \\ &= (\hat{\mathbf{D}}_{S^k}^* \hat{\mathbf{D}}_{S^k})^{-1} (\hat{\mathbf{D}}_{S^k}^* \hat{\mathbf{y}}) \end{aligned} \quad (22)$$

式 (14) の内積の保存の関係より  $\hat{\mathbf{D}}_{S^k}^* \hat{\mathbf{D}}_{S^k} = \mathbf{D}_{S^k}^* \mathbf{D}_{S^k}$ 、 $\hat{\mathbf{D}}_{S^k}^* \hat{\mathbf{y}} = \mathbf{D}_{S^k}^* \mathbf{y}$  が成立することから、式 (22) は次式のように書き換えることができる。

$$\hat{\mathbf{x}}^k = (\mathbf{D}_{S^k}^* \mathbf{D}_{S^k})^{-1} (\mathbf{D}_{S^k}^* \mathbf{y}) \quad (23)$$

上式は式 (7) と等しく、秘匿信号を用いて得られるサポート内での最良解  $\hat{\mathbf{x}}^k$  は、原信号を用いた場合の最良解  $\bar{\mathbf{x}}^k$  と一致することがわかる。

4. 残差の更新:

式 (8) を秘匿信号に置き換えると次式となる。

$$\hat{\mathbf{r}}^k = \hat{\mathbf{y}} - \hat{\mathbf{D}}_{S^k} \hat{\mathbf{x}}^k \quad (24)$$

式 (15)(16) の定義式ならびにサポート内での最良解  $\hat{\mathbf{x}}^k = \bar{\mathbf{x}}^k$  より、次式が得られる。

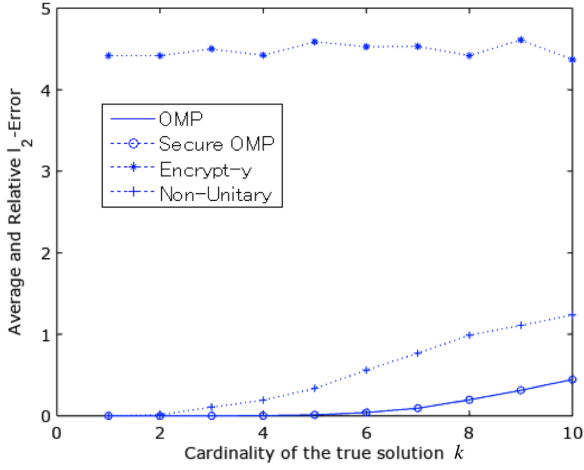


図4 非ゼロの係数の個数  $k$  と平均  $l_2$  誤差.

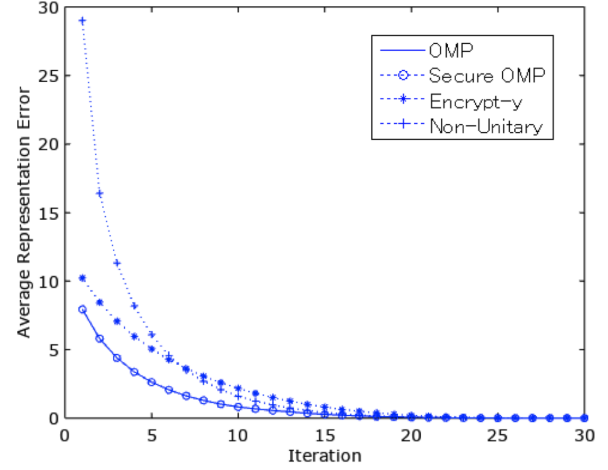


図6 平均  $\|r^k\|_2$  の収束状況 (停止条件:  $\|r^k\|_2 < \epsilon = 10^{-4}$ ).

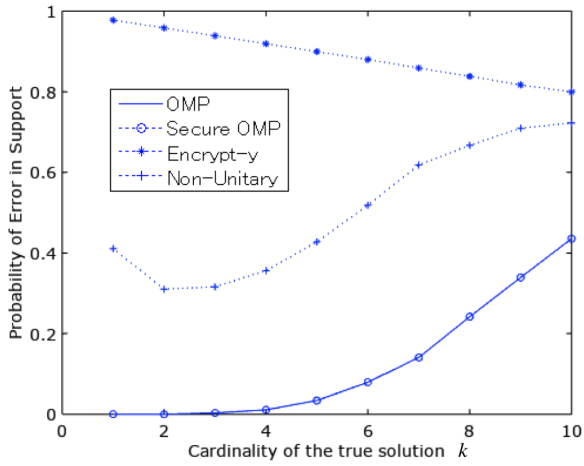


図5 非ゼロの係数の個数  $k$  とサポート間距離  $dist(\hat{S}, S)$ .

$$\hat{r}^k = Q_p(y - D_{S^k} \hat{x}^k) \quad (25)$$

ここで式 (8) の関係より、上式の  $\hat{r}^k$  は原信号を用いた場合の誤差  $r^k$  を用いて次式のように表すことができる。

$$\hat{r}^k = Q_p r^k \quad (26)$$

5. 停止条件:

$\|\hat{r}^k\|_2 < \epsilon$  を満たすとき終了となるが、式 (26) ならびにノルム不変の性質より、

$$\begin{aligned} \|\hat{r}^k\|_2 &= \|Q_p r^k\|_2 \\ &= \|r^k\|_2 < \epsilon \end{aligned} \quad (27)$$

が成立する。原信号を用いた場合の停止条件と一致する。

以上のステップ 1-5 より、秘匿信号を用いて計算されるスパース係数は、原信号を用いて計算されるスパース係数と等しいことが証明された。

## 4. シミュレーション結果

有効性を検証するために、人工データに対してスパース係数の推定を行った。

### 4.1 人工データの生成

過完備なランダム辞書行列  $D$  にスパース係数  $x$  を入力して、 $y = Dx$  により観測データ  $y$  を生成した。以下に、具体的な設定条件を示す。

- ・ 観測データ  $y \in \mathbb{R}^M$ :  $M=30$  次元の列ベクトル
- ・ 辞書行列  $D \in \mathbb{R}^{M \times K}$ :  $M \times K = 30 \times 50$  のランダム行列
- ・ スパース係数  $x \in \mathbb{R}^K$ :  $K = 50$  次元のベクトル  
非ゼロの係数の個数  $k = (1, 2, \dots, 10)$  の 10 種類  
正規分布に従うランダム変数
- ・ サンプル数: それぞれの  $k$  について 1000 サンプル

### 4.2 評価

最初に、直交マッチング追跡法と提案法によりスパース係数の推定を行い、推定精度の比較を行った。

- ・ 手法 1: 直交マッチング追跡法 (OMP)
- ・ 手法 2: 提案法 (Secure OMP)

両手法ともに辞書  $D$  は既知として、スパース係数を推定した。図 4 にスパース係数の非ゼロ要素の個数  $k$  とスパース係数の推定値  $\hat{x}$  の平均  $l_2$  誤差 ( $\|x - \hat{x}\|_2 / \|x\|_2$ ) との関係を示す。図 4 より、提案法により推定される平均  $l_2$  誤差は、直交マッチング追跡法により推定した平均  $l_2$  誤差と一致していることが確認できる。図 5 にスパース係数の非ゼロ要素の個数  $k$  とサポート間距離

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

を示す。図 5 よりサポート間距離に関しても、提案法と直交マッチング追跡法により推定したサポート間距離は一致していることが確認できる。図 6 には平均 2 乗誤差  $\|r^k\|_2$  の収束状況を示した。両手法ともに、停止条件は  $\|r^k\|_2 < \epsilon = 10^{-4}$  とした。提案法ならびに直交マッチング追跡法ともに 20 回程度の繰り返しでほぼ収束していることがわかる。

次に、提案法の秘匿性能ならびにランダムユニタリ行列  $Q_p$  の妥当性を検証するために、同じく図 4-6 の 3 つの評価量について、以下の 2 つの手法との比較を行った。

- ・ 手法 3: 観測信号のみ秘匿 (Encrypt-y)
- ・ 手法 4: 非ユニタリ行列 (Non-Unitary)

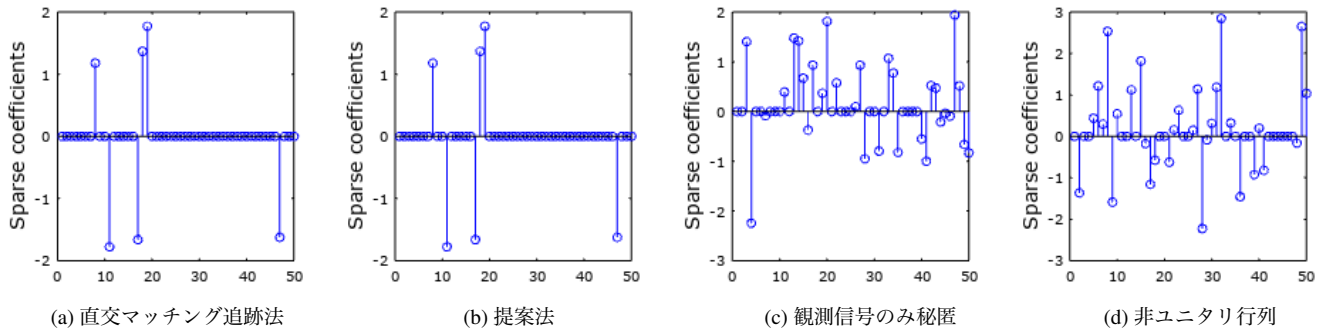


図7 スパース係数  $\mathbf{x}$  の推定値 ( $k=6$  の場合の任意の 1 サンプル) .

手法3では辞書  $\mathbf{D}$  は秘匿せずに、観測信号のみ秘匿した後に、直交マッチング追跡法を適用した。図4-6より平均  $\|\mathbf{r}^k\|_2$  は十分収束しているものの、平均  $l_2$  誤差とサポート間距離は大幅に増加している。スパース係数の推定精度が大幅に低下しており、観測信号が十分秘匿できていると考えられる。

手法4では、観測信号ならびに辞書ともに秘匿信号を生成する際にランダムユニタリ行列  $\mathbf{Q}_p$  に代わってユニタリ性を有しないランダム行列により観測信号と辞書行列を生成し、直交マッチング追跡法を適用した。図4-6より平均  $\|\mathbf{r}^k\|_2$  は十分収束しているものの、平均  $l_2$  誤差とサポート間距離が増加していることが確認できる。秘匿信号の生成にユニタリ性は重要な性質であることがわかる。

図7には、 $k=6$  の場合の任意の 1 サンプルについて、スパース係数  $\mathbf{x}$  の推定値を示した。図7より、観測信号のみ秘匿した場合と非ユニタリ行列で変換した場合には推定誤差が発生している一方、提案法は直交マッチング追跡法と同じスパース係数を推定できていることが確認できる。

## 5. まとめと今後の予定

本稿ではランダムユニタリ行列を用いたスパースコーディングの秘匿演算法を提案した。スパースコーディングの代表的な係数選択アルゴリズムである直交マッチング追跡法において、観測信号  $\mathbf{y}$  と辞書  $\mathbf{D}$  を秘匿したまま演算し、秘匿しない場合と比較して理論的に同じ結果となることを証明するとともに、シミュレーションにより性能を確認した。

今後は、プライバシー保護の観点から秘匿演算が必要とされる画像や脳活動を計測した生体信号などへ適用し、具体的な応用事例について検討する予定である。

## 文 献

- [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 Representations: From Theory to Applications in Signal and Image Processing," Springer, 2010.
- [3] 日野英逸, 村田 昇, "スパース表現の数理とその応用," *信学技報* vol. 112(198), pp. 133-142, 2012.
- [4] 笠井 裕之, "スパースコーディングの研究動向," *研究報告オーディオビジュアル複合情報処理 (AVM)*, vol. 2014-AVM-84(8), pp. 1-10, 2014.
- [5] B. K. Natarajan: "Sparse approximate solutions to linear systems", *SIAM J. Comput.*, 24, 2, pp. 227-234 (1995).
- [6] K. Engan, S. O. Aase and J. Hakon Husoy: "Method of optimal di-

- rections for frame design", *ICASSP1999*, pp. 2443-2446 (1999).
- [7] 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).
- [8] Y. C. Pati, R. Rezaifar, Y. C. P. R. Rezaifar and P. S. Krishnaprasad, "Orthogonal matching pursuit: Recursive function approximation with applications to wavelet decomposition", *Asilomar1993*, pp. 40-44 (1993).
- [9] R. Chartrand and W. Yin: "Iteratively reweighted algorithms for compressive sensing", *IEEE ICASSP2008*, pp. 3869-3872 (2008).
- [10] M. Elad and M. Aharon, "Image denoising via sparse and redundant representations over learned dictionaries," *IEEE Transactions on Image Processing*, vol. 15, no. 12, pp. 3736-3745, Dec. 2006.
- [11] J. Mairal, M. Elad and G. Sapiro, "Sparse representation for color image restoration," *IEEE Transactions on Image Processing*, vol. 17, no. 1, pp. 53-69, Jan. 2008.
- [12] H. Morioka, A. Kanemura, J. Hirayama, M. Shikachi, T. Ogawa, S. Ikeda, M. Kawanabe, and S. Ishii, "Learning a common dictionary for subject-transfer decoding with resting calibration", *NeuroImage*, vol. 111, pp. 167-178, 2015.
- [13] 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.
- [14] R. Lazzaretto and M. Barni, "Private Computing with Garbled Circuits [Applications Corner]," *IEEE Signal Processing Magazine*, vol. 30, no. 2, pp. 123-127, March 2013.
- [15] M. Barni, G. Droandi and R. Lazzaretto, "Privacy Protection in Biometric-Based Recognition Systems: A marriage between cryptography and signal processing," *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 66-76, Sept. 2015.
- [16] 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.
- [17] 電子情報通信学会誌, "小特集 完全準同形暗号の研究動向," vol. 99, no.12, pp. 1150-1183, 2016.
- [18] M. A. Lebedev, and M. A. L. Nicolelis. Brain-machine interfaces: past, present and future. *Trends in Neuroscience*, 29(9), 536-546, 2006.
- [19] I. Nakamura, Y. Tonomura, and H. Kiya, "Unitary Transform-Based Template Protection and Its Properties," *Proc. European Signal Processing Conference*, vol. SIPA- P3.4, pp. 2466-2470, 2015.
- [20] I. Nakamura, Y. Tonomura, and H. Kiya, "Unitary Transform-Based Template Protection and Its Application to  $l_2$ -norm Minimization Problems," *IEICE Trans. Inf. & Sys.*, vol. E99-D, no.1, pp. 60-68, Jan. 2016.
- [21] T. S. Lee: "Image representation using 2D Gabor wavelets", *IEEE Trans. Pattern Anal. Mach. Intell.*, 18, 10, pp. 959-971 (1996).
- [22] E. Candès and D. Donoho: "Curvelets: A surprisingly effective non-adaptive representation for objects with edges", *Curves and Surfaces* (Ed. by L. L. Schumaker et al.), Vanderbilt University Press (1999).