

スパース辞書学習の秘匿演算

秘匿データからパターンや法則性を見つける

仲地 孝之[†] 坂東 幸浩^{††} 貴家 仁志^{†††}

[†] 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

^{††} 日本電信電話株式会社 メディアインテリジェンス研究所 〒239-0847 神奈川県横須賀市光の丘 1-1

^{†††} 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: [†]{takayuki.nakachi.pu,yukihiro.bandoh}@hco.ntt.co.jp, ^{††}kiya@tmu.ac.jp

あらまし ビックデータ時代の到来とともに、あらゆるデジタルコンテンツが質量ともに増え続けている。その中でスパースモデリングは大量のデータの中に隠れている有為な情報を抽出する情報処理モデルとして注目されている。一方、近年ビックデータの解析をはじめ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の利用が急速に普及してきている。しかし、サービス提供者の信頼性欠如や事故によるデータの不正利用や流失によって、プライバシーを侵害する問題の発生が危惧されている。本稿ではそのような背景から、プライバシーを保護しつつデータ解析・信号処理を行う手法として、秘匿したデータからスパース辞書学習を行う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同時に、シミュレーションにより有効性を確認する。
キーワード スパース辞書学習、スパースモデリング、MOD、K-SVD、ランダムユニタリ変換、秘匿演算

Secure Computation of Sparse Dictionary Learning

Takayuki NAKACHI[†], Yukihiro BANDO^{††}, and Hitoshi KIYA^{†††}

[†] NTT Network Innovation Laboratories, Nippon Telegraph and Telephone Corp. Yokosuka, 239-0847 JAPAN

^{††} NTT Media Intelligence Laboratories, Nippon Telegraph and Telephone Corp. Yokosuka, 239-0847 JAPAN

^{†††} Information and Communication Systems, Tokyo Metropolitan University, Tokyo, 191-0065, Japan

E-mail: [†]{takayuki.nakachi.pu,yukihiro.bandoh}@hco.ntt.co.jp, ^{††}kiya@tmu.ac.jp

Abstract With the advent of the big data era, all digital contents continue to increase. Sparse modeling is drawing attention as an information processing model for extracting useful information hidden in a large amount of data. On the other hand, cloud computing including big data analysis 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 dictionary learning method for encrypted observed signals. It is shown that the secure dictionary learning enables us to not only protects observed signals, but also have the same estimation performance as that of sparse dictionary learning for unencrypted observed signals.

Key words Sparse Coding, MOD, K-SVD, Random Unitary Transform, Secure Computation

1. ま え が き

ビックデータ時代の到来とともに、テキスト、映像・画像、音声・音響などのあらゆるデジタルコンテンツが質量ともに肥大化し続けている。ビックデータは膨大であるものの不必要なデータも多く、活用するためにはデータを解析する必要がある。現在注目を集めている数理手法の一つがスパースコーディング (Sparse Coding: SC) [1]-[9] に代表されるスパースモデリングである。スパースモデリングは大量のデータの中に隠れている有

為な情報を抽出する情報処理モデルである。また、法則性を導き、断片的なデータを補完して実態を忠実に再現することも可能である。

スパースモデリングは、観測信号を少数の基底の重み付き線形和で表現する。基底から構成される辞書は、予め基底を用意しておく方法と、観測信号から基底を学習する辞書学習があるが、辞書学習によって得られる辞書はデータ依存である。辞書学習自体がひとつのパターン発見手法となっていると言える。文献 [8] では代表的な辞書学習法である K-SVD (K-Singular

Value Decomposition) [5] を特徴抽出機構に用いたパターン認識システムを提案している。

一方、近年ビックデータの解析をはじめ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の利用が急速に普及してきている。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るデータの不正利用や流失によって、プライバシーを侵害する問題の発生が危惧されている [10]。その問題を解決する一つの方法として、データを暗号化したまま計算する方法、いわゆる秘密計算が盛んに研究されている [11]-[12]。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。

本稿では、エッジ/クラウドでの利用を想定し、ランダムユニタリ変換を用いたスパース辞書学習 (スパースモデリングの辞書学習) の秘匿演算法を提案する。具体的には、スパース辞書学習のアルゴリズムとして知られている MOD (Method of Optimal Direction) [4] と K-SVD [5] の秘匿演算法を提案する。暗号化領域で MOD と K-SVD の演算が可能であることを証明するとともに、シミュレーションにより観測信号を秘匿しない場合と比較して推定性能が劣化しないことを検証する。

本稿の構成は、以下の通りである。2. 節でスパース辞書学習の概要を説明し、3. 節でスパース辞書学習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. スパース辞書学習

本節ではスパース辞書学習の定式化を行うとともに、代表的なアルゴリズムである MOD [4] と K-SVD [5] について説明する。

2.1 定式化

観測信号 y_i (M 次元の列ベクトル) の集合を $\mathbf{Y} = \{y_i\}_{i=1}^N$ とする。このとき、図 1 に示すように、 \mathbf{Y} 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 (M 次元の列ベクトル) を要素とする辞書行列であり、 $\mathbf{X} = \{\mathbf{x}_i\}_{i=1}^N$ はスパース係数 x_i (K 次元の列ベクトル) を要素とする行列である。

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。すなわち、少数の T_0 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制約を設ける。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。スパースの制約を持つ最適化問題は、

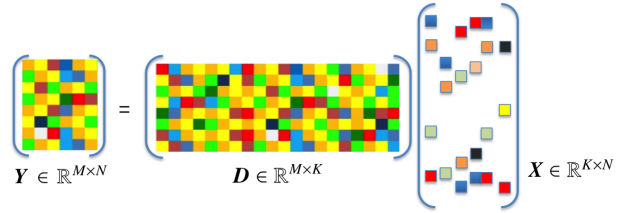


図 1 スパース辞書学習：少数の基底ベクトルの重み付き線形和で表現する線形システム。

$$\min_{\mathbf{D}, \mathbf{X}} \|\mathbf{Y} - \mathbf{D}\mathbf{X}\|_F^2 \quad \text{subject to } \forall i, \|\mathbf{x}_i\|_0 < T_0. \quad (2)$$

として定式化される。ただし、 $\|\cdot\|_0$ は L_0 ノルム (ベクトル中の非ゼロ要素の個数) を表し、 $\|\cdot\|_F$ はフロベニウスのノルムを表し $\|\mathbf{A}\|_F = \sqrt{\sum_{ij} A_{ij}^2}$ で定義される。

一般的に辞書学習は、二つのステップを交互に繰り返すことによって、式 (2) の最適化問題を解く。ステップ 1 はスパース係数の計算、ステップ 2 では辞書の更新を行う。

2.2 ステップ 1：スパース係数の計算

ステップ 1 では辞書 \mathbf{D} を固定し、式 (2) の最適化問題を解く。各入力 i の観測信号ベクトル y_i に対して、スパース係数 \mathbf{x}_i を求める問題であり、次式のように書き換えることができる。

$$\mathbf{x}_i = \arg \min_{\mathbf{x}_i} \|y_i - \mathbf{D}\mathbf{x}_i\|_F^2 \quad \text{subject to } \|\mathbf{x}_i\|_0 < T_0 \quad i = 1, 2, \dots, N. \quad (3)$$

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 [3]。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。

本稿では、 l_0 制約に基づく近似解法である直交マッチング追跡法 (OMP) [6] を用いる。直交マッチング追跡法は、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 y_i を基底の線形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 ϵ 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。

2.3 ステップ 2：辞書の更新

ステップ 2 ではステップ 1 で求めた \mathbf{X} を固定し、辞書 \mathbf{D} の更新を行う。スパース辞書学習の代表的な手法が MOD と K-SVD である。MOD と K-SVD とともにステップ 1 は同じ処理で、ステップ 2 の辞書の更新方法が異なる。

A. MOD

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。辞書 \mathbf{D} について解くと、 $\partial \|\mathbf{Y} - \mathbf{D}\mathbf{X}\|_F^2 / \partial \mathbf{D} = 0$ より、

$$\mathbf{D} = \arg \min_{\mathbf{D}} \|\mathbf{Y} - \mathbf{D}\mathbf{X}\|_F^2 = \mathbf{Y}\mathbf{X}^T(\mathbf{X}\mathbf{X}^T)^{-1} \quad (4)$$

が得られる。

B. K-SVD

K-SVD は、k-means 法を一般化したものと位置づけられる。k-means 法では各サンプルをクラスタに割り当てるステップと、クラスタの重心を移動させるステップが交互に繰り返される。クラスタ重心は特徴量の空間におけるベクトルであり、そのクラスタに割り当てられたサンプルの平均的な特徴と捉えられる k-means 法の拡張である。soft k-means 法では各サンプルを多数のクラスタに割り当てる。これはクラスタ重心の一次結合としてサンプルが表されることを意味し、クラスタ重心を基底に置き換えることで、辞書学習と対応する。

K-SVD では MOD とは異なり D 全体ではなく、一つの基底 d_k に着目し順次更新する。

$$\begin{aligned} \|Y - DX\|_F^2 &= \left\| Y - \sum_{j=1}^K d_j x_T^j \right\|_F^2 \\ &= \left\| \left(Y - \sum_{j \neq k} d_j x_T^j \right) - d_k x_T^k \right\|_F^2 \\ &= \|E_k - d_k x_T^k\|_F^2. \end{aligned} \quad (5)$$

ここで E_k は観測信号の集合 Y から基底 d_k を除いた線形予測値との残差を示す。

$$E_k = Y - \sum_{j \neq k} d_j x_T^j \quad (6)$$

K-SVD では E_k を特異値分解 (Singular Value Decomposition : SVD) することで、 d_k と x_T^k を求める。しかしながら、得られる解はスパースの制約を満たすとは限らないため、K-SVD ではステップ 1 で求めた x_T^k における非ゼロ要素のみを更新する。これによって、ステップ 1 で得られたスパース性を維持することができる。 x_T^k における非ゼロ要素のインデックス集合 ω_k を以下のように定義する。

$$\omega_k = \{i \mid 1 \leq i \leq K, x_T^k(i) \neq 0\}. \quad (7)$$

但し、 $x_T^k(i)$ は x_T^k の i 番目の要素を表す。ここで $(\omega_k(i), i)$ の位置の要素のみが 1 である大きさ $N \times |\omega_k|$ の行列 Ω_k を定義する。 Ω_k を用いると x_T^k の非ゼロ要素のみで構成されるベクトル x_R^k が、次式のように書き表せる。

$$x_R^k = x_T^k \Omega_k. \quad (8)$$

同様に E_k に対して、 Ω_k を用いて $E_k^R = E_k \Omega_k$ と変換する。

$$\|E_k \Omega_k - d_k x_T^k \Omega_k\|_F^2 = \|E_k^R - d_k x_R^k\|_F^2. \quad (9)$$

E_k^R に対して SVD を適用し、直行行列 U, V と対角行列 Σ に分解すると次式が得られる。

$$\begin{aligned} E_k^R &= U \Delta V^T \\ &= u_1 \cdot \sigma_1 v_1^T + u_2 \cdot \sigma_2 v_2^T + \cdots + u_n \cdot \sigma_n v_n^T. \end{aligned} \quad (10)$$

u_i と v_j は、それぞれ U と V の i 番目の列ベクトル、 σ_i は Δ の i 番目の対角成分である。K-SVD では第一特異値に関する成分

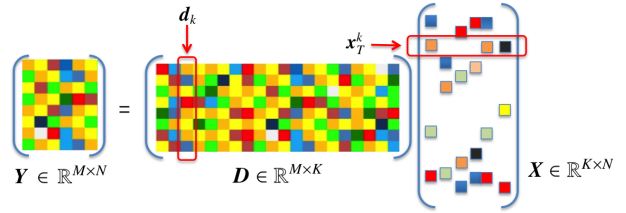


図2 基底 d_k と X の k 番目の行ベクトル x_T^k .

u_1 と $\sigma_1 v_1^T$ を用いて、次式のように基底ならびにスパース係数の行ベクトルの近似解を得る。

$$\cdot \text{基底: } d_k = u_1 \quad (11)$$

$$\cdot \text{スパース係数: } x_R^k = \sigma_1 v_1^T \quad (12)$$

3. スパース辞書学習の秘匿演算

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 MOD と K-SVD の秘匿演算法を提案する。

3.1 ランダムユニタリ行列に基づく秘匿演算

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 Q_p を用いた変換 $T(\cdot)$ により、信号 f_i ($i = 1, \dots, L$) が秘匿信号 \hat{f}_i へ変換される。

$$\hat{f}_i = T(f_i, p) = Q_p f_i \quad (13)$$

但し $Q_p \in \mathbb{C}^{N \times N}$ であり、

$$Q_p^* Q_p = I \quad (14)$$

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

ランダムユニタリ変換 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 Q_p を生成する方法が検証されている [13]。

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。

特徴 1: ノルム不変

$$\|f_i\|_F^2 = \|\hat{f}_i\|_F^2 \quad (15)$$

特徴 2: ユークリッド距離の保存

$$\|f_i - f_j\|_F^2 = \|\hat{f}_i - \hat{f}_j\|_F^2 \quad (16)$$

特徴 3: 内積の保存

$$f_i^* f_j = \hat{f}_i^* \hat{f}_j \quad (17)$$

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

3.2 スパース辞書学習の秘匿演算

エッジ/クラウドでスパース辞書学習の秘匿演算を行うアーキテクチャを図 3 に示す。最初にローカルにおいて、鍵 p により生成したランダムユニタリ行列 Q_p を用いて、観測信号 Y を秘匿観測信号 \hat{Y} へ変換する。その後、秘匿観測信号 \hat{Y} をエッ

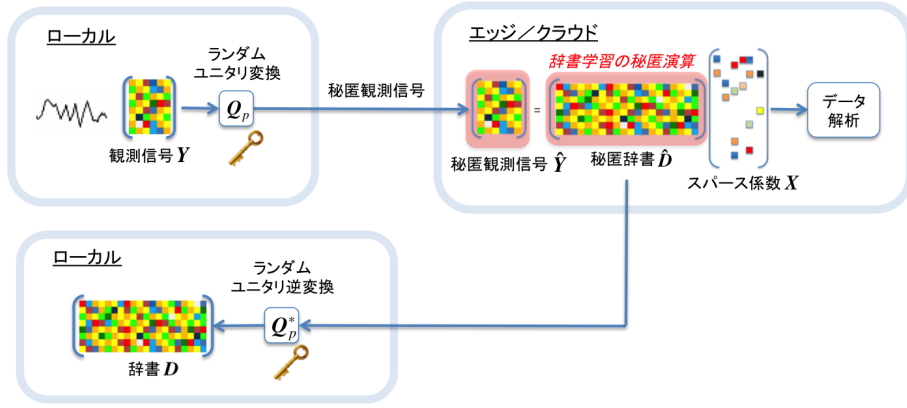


図3 エッジ/クラウドでのスパース辞書学習の秘匿演算。

ジ/クラウドへ転送する。エッジ/クラウドでは、秘匿観測信号 \hat{Y} を入力として、MOD または K-SVD のアルゴリズムを実行して秘匿辞書 \hat{D} を推定する。エッジ/クラウドでは秘匿領域での辞書すなわち秘匿辞書 \hat{D} が随時更新される。鍵 p を持つユーザはランダムユニタリ逆変換 Q_p^* を秘匿辞書 \hat{D} へ掛け合わせることで、辞書 D を得ることができる。

スパース係数 X は、エッジ/クラウドにおいて MOD または K-SVD のステップ1の段階で随時更新され求められる。スパース係数 X をデータ解析することで観測信号のパターンや法則性を見つけることが可能となる。提案するスパース辞書学習の秘匿演算では、次式のように秘匿観測信号 \hat{Y} を生成する。

$$\hat{Y} = T(y, p) = Q_p Y \quad (18)$$

このとき式 (2) に代わり、次式に示す最適化問題を考える。

$$\min_{\hat{D}, X} \|\hat{Y} - \hat{D}X\|_F^2 \quad \text{subject to } \forall i, \|x_i\|_0 < T_0. \quad (19)$$

ただし、 $\hat{D} = \{\hat{d}_1, \dots, \hat{d}_K\} \in \mathbb{R}^{M \times K}$ は基底 \hat{d}_i (M 次元の列ベクトル) を要素とする秘匿辞書行列である。

3.3 ステップ1：スパース係数の計算

ステップ1では辞書 \hat{D} を固定し、式 (19) の最適化問題を解く。各入力の観測信号ベクトル \hat{y}_i に対して、スパース係数 x_i を求める問題であり、次式のように書き換えることができる。

$$x_i = \arg \min_{x_i} \|\hat{y}_i - \hat{D}x_i\|_F^2 \quad \text{subject to } \|x_i\|_0 < T_0 \\ i = 1, 2, \dots, N. \quad (20)$$

先に著者らは、辞書を $\hat{D} = Q_p D$ と秘匿した後に、上式を OMP で解いて得られる解 x_i が、観測 y_i と辞書行列 D を秘匿しない場合に OMP を解いて得られるスパース係数 x_i と等しくなることを示した [14]-[16]。

3.4 ステップ2：秘匿辞書の更新

ステップ2ではステップ1で求めた X を固定し、秘匿辞書 \hat{D} の更新を行う。以下、それぞれ MOD と K-SVD の場合を示す。

A. 秘匿 MOD

秘匿 MOD では \hat{Y} と $\hat{D}X$ の間の二乗誤差の最小化に疑似逆行列を使用する。 $\partial \|\hat{Y} - \hat{D}X\|_F^2 / \partial \hat{D} = 0$ より、秘匿領域での辞書

$$\hat{D} = \arg \min_{\hat{D}} \|\hat{Y} - \hat{D}X\|_F^2 = \hat{Y}X^T(XX^T)^{-1} \quad (21)$$

が得られる。すなわち秘匿辞書 \hat{D} が更新される。

次に、秘匿辞書 \hat{D} と観測信号を秘匿しない場合に MOD を解いて得られる辞書 D との関係を示す。式 (18) で定義の $\hat{Y} = Q_p Y$ より、式 (21) は次式の通り書き換えることができる。

$$\hat{D} = Q_p YX^T(XX^T)^{-1} \quad (22)$$

式 (4) に示す観測信号を秘匿しない場合に MOD を解いて得られる $D = YX^T(XX^T)^{-1}$ の関係式を用いると、秘匿辞書 \hat{D} と辞書 D の関係は、

$$\hat{D} = Q_p D \quad (23)$$

となる。鍵 p を持つユーザは、 $D = Q_p^* \hat{D}$ より辞書 D を得ることができる。

B. 秘匿 K-SVD

秘匿 K-SVD では秘匿 MOD とは異なり \hat{D} 全体ではなく、一つの基底 \hat{d}_k に着目し順次更新する。2.3 節の観測信号を秘匿しない場合の K-SVD の辞書更新の手法を用いて、同様に求める。

$$\|\hat{Y} - \hat{D}X\|_F^2 = \left\| \hat{Y} - \sum_{j=1}^K \hat{d}_j x_j^T \right\|_F^2 \\ = \left\| \left(\hat{Y} - \sum_{j \neq k} \hat{d}_j x_j^T \right) - \hat{d}_k x_k^T \right\|_F^2 \\ = \|\hat{E}_k - \hat{d}_k x_k^T\|_F^2. \quad (24)$$

ここで、 \hat{E}_k は秘匿観測信号の集合 \hat{Y} から基底 \hat{d}_k を除いた線形予測値との残差を示す。

解のスパース性を維持するために、 x_k^T の非ゼロ要素のみで構成されるベクトル x_R^k のみ更新する。 \hat{E}_k に対して、 Ω_K を用いて $\hat{E}_k^R = \hat{E}_k \Omega_K$ と変換する。

$$\|\hat{E}_k \Omega_K - \hat{d}_k x_k^T \Omega_K\|_F^2 = \|\hat{E}_k^R - \hat{d}_k x_R^k\|_F^2. \quad (25)$$

\hat{E}_k^R に対して SVD を適用し、直行列 \hat{U} 、 \hat{V} と対角行列 $\hat{\Sigma}$ に分解すると次式が得られる。

$$\hat{E}_k^R = \hat{U} \hat{\Lambda} \hat{V}^T \\ = \hat{u}_1 \cdot \hat{\sigma}_1 \hat{v}_1^T + \hat{u}_2 \cdot \hat{\sigma}_2 \hat{v}_2^T + \dots + \hat{u}_n \cdot \hat{\sigma}_n \hat{v}_n^T. \quad (26)$$

第一特異値に関する成分 \hat{u}_1 と $\hat{\sigma}_1 \hat{v}_1^T$ を用いて、次式のように基

底ならびにスパース係数の行ベクトルの近似解を得る。

$$\cdot \text{基底: } \hat{\mathbf{d}}_k = \hat{\mathbf{u}}_1 \quad (27)$$

$$\cdot \text{スパース係数: } \hat{\mathbf{x}}_R^k = \hat{\sigma}_1 \hat{\mathbf{v}}_1^T \quad (28)$$

次に、観測信号を秘匿しない場合に解いて得られる解と、秘匿しない場合に得られる解との関係を示す。ここで式 (24) における $\hat{\mathbf{E}}_k$ の第 2 項 $\hat{\mathbf{d}}_j$ を $\hat{\mathbf{d}}_j = \mathbf{Q}_p \mathbf{d}_j$ と分解し、式 (18) の関係を用いて整理すると、

$$\begin{aligned} \hat{\mathbf{E}}_k &= \hat{\mathbf{Y}} - \sum_{j \neq k} \hat{\mathbf{d}}_j \mathbf{x}_T^j \\ &= \mathbf{Q}_p \left(\mathbf{Y} - \sum_{j \neq k} \mathbf{d}_j \mathbf{x}_T^j \right) = \mathbf{Q}_p \mathbf{E}_k \end{aligned} \quad (29)$$

が得られる。なお $\hat{\mathbf{d}}_j = \mathbf{Q}_p \mathbf{d}_j$ の分解は、ステップ 1 において秘匿信号に対するスパース係数を求める際の前提条件 $\hat{\mathbf{D}} = \mathbf{Q}_p \mathbf{D}$ [14]-[16] から導出される。次に解のスパース性を維持するために、 $\hat{\mathbf{E}}_k$ に対して $\mathbf{\Omega}_K$ を用いて $\hat{\mathbf{E}}_k^R = \hat{\mathbf{E}}_k \mathbf{\Omega}_K$ と変換して、式 (29) の関係を用いると、

$$\hat{\mathbf{E}}_k^R = \hat{\mathbf{E}}_k \mathbf{\Omega}_K = \mathbf{Q}_p \mathbf{E}_k \mathbf{\Omega}_K = \mathbf{Q}_p \mathbf{E}_k^R \quad (30)$$

と書き表すことができる。さらに、式 (10) の関係式 (観測信号を秘匿しない場合の \mathbf{E}_k^R に対する SVD の結果) を用いると、式 (30) は次のように分解できる。

$$\begin{aligned} \hat{\mathbf{E}}_k^R &= \mathbf{Q}_p \mathbf{E}_k^R \\ &= \mathbf{Q}_p \mathbf{u}_1 \cdot \sigma_1 \mathbf{v}_1^T + \mathbf{Q}_p \mathbf{u}_2 \cdot \sigma_2 \mathbf{v}_2^T + \cdots + \mathbf{Q}_p \mathbf{u}_n \cdot \sigma_n \mathbf{v}_n^T. \end{aligned} \quad (31)$$

式 (31) より基底ならびにスパース係数は、観測信号を秘匿しない場合の値を用いて $\hat{\mathbf{d}}_k = \hat{\mathbf{u}}_1 = \mathbf{Q}_p \mathbf{u}_1$ ならびに $\hat{\mathbf{x}}_R^k = \sigma_1 \mathbf{v}_1^T$ と表現できることがわかる。

$$\cdot \text{基底: } \hat{\mathbf{d}}_k = \mathbf{Q}_p \mathbf{u}_1 \quad (32)$$

$$\cdot \text{スパース係数: } \hat{\mathbf{x}}_R^k = \sigma_1 \mathbf{v}_1^T \quad (33)$$

しかしながら、 $\hat{\mathbf{E}}_k^R = \mathbf{Q}_p \mathbf{E}_k^R$ の SVD の結果が、式 (31) と等しいことは自明ではない。以下に、 $\hat{\mathbf{E}}_k^R = \mathbf{Q}_p \mathbf{E}_k^R$ の SVD の結果が、式 (31) と等しいことを証明する。

[スパース係数の関係式]

式 (26) より $\hat{\mathbf{v}}_i$ は $(\hat{\mathbf{E}}_k^R)^T \hat{\mathbf{E}}_k^R$ の i 番目の固有ベクトルであり、次式のように書き表すことができる。

$$(\hat{\mathbf{E}}_k^R)^T \hat{\mathbf{E}}_k^R \hat{\mathbf{v}}_i = \hat{\lambda}_i \hat{\mathbf{v}}_i \quad (34)$$

但し $\hat{\lambda}_i$ は i 番目の固有値であり、特異値 $\hat{\sigma}_i$ と $\hat{\sigma}_i = \sqrt{\hat{\lambda}_i}$ の関係にある。ここで $\hat{\mathbf{E}}_k^R = \mathbf{Q}_p \mathbf{E}_k^R$ の関係を用いると式 (34) の左辺は

$$(\hat{\mathbf{E}}_k^R)^T \hat{\mathbf{E}}_k^R = (\mathbf{E}_k^R)^T \mathbf{Q}_p^T \mathbf{Q}_p \mathbf{E}_k^R = (\mathbf{E}_k^R)^T \mathbf{E}_k^R \quad (35)$$

と表すことができる。式 (35) より、 $(\hat{\mathbf{E}}_k^R)^T \hat{\mathbf{E}}_k^R$ と $(\mathbf{E}_k^R)^T \mathbf{E}_k^R$ は等しいことから、それぞれの固有ベクトル $\hat{\mathbf{v}}_i$ ならびに \mathbf{v}_i も等しい。

$$\hat{\mathbf{v}}_i = \mathbf{v}_i \quad (36)$$

したがって対応する固有値ならびに特異値も等しく、式 (33)

($\hat{\mathbf{x}}_R^k = \sigma_1 \mathbf{v}_1^T$) は妥当であることがわかる。

[基底の関係式]

式 (26) に示す行列 $\hat{\mathbf{E}}_k^R$ の特異値分解において、左側の固有ベクトル $\hat{\mathbf{u}}_i$ と右側の固有ベクトル $\hat{\mathbf{v}}_i$ には $\hat{\mathbf{u}}_i = \pm \hat{\mathbf{E}}_k^R \hat{\mathbf{v}}_i / \sqrt{\hat{\lambda}_i}$ (一般的な特異値分解の性質より) の関係がある。この関係と $\hat{\mathbf{E}}_k^R = \mathbf{Q}_p \mathbf{E}_k^R$ の関係より、式 (26) の第 1 番目の項は、

$$\hat{\mathbf{u}}_1 \cdot \hat{\sigma}_1 \hat{\mathbf{v}}_1^T = \frac{\pm \hat{\mathbf{E}}_k^R \hat{\mathbf{v}}_1 \cdot \hat{\sigma}_1 \hat{\mathbf{v}}_1^T}{\sqrt{\hat{\lambda}_1}} = \pm \mathbf{Q}_p \mathbf{E}_k^R \mathbf{v}_1 \mathbf{v}_1^T \quad (37)$$

と表せる。同様に式 (31) の第 1 番目の項は、

$$\mathbf{Q}_p \mathbf{u}_1 \cdot \sigma_1 \mathbf{v}_1^T = \frac{\pm \mathbf{Q}_p \mathbf{E}_k^R \mathbf{v}_1 \cdot \sigma_1 \mathbf{v}_1^T}{\sqrt{\lambda_1}} = \pm \mathbf{Q}_p \mathbf{E}_k^R \mathbf{v}_1 \mathbf{v}_1^T \quad (38)$$

と表せる。式 (32) ($\hat{\mathbf{d}}_k = \mathbf{Q}_p \mathbf{u}_1$) は妥当であることがわかる。

4. シミュレーション結果

有効性を検証するために、人工的に生成した秘匿観測信号に対して、スパース係数ならびに辞書の推定を行った。

4.1 秘匿観測信号の生成と評価指標

過完備な辞書 \mathbf{D}_{true} にスパース係数の行列 \mathbf{X} を入力して、 $\mathbf{Y} = \mathbf{D}_{true} \mathbf{X} + \epsilon$ により観測データ \mathbf{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 $\mathbf{Y} \in \mathbb{R}^{M \times N}$: 30×4000 次元の行列
- ・辞書 $\mathbf{D}_{true} \in \mathbb{R}^{M \times K}$: 30×60 次元の Overcomplete DCT
- ・スパース係数 $\mathbf{X} \in \mathbb{R}^{K \times N}$: 60×4000 次元の行列で非ゼロの係数の個数 $L = 4$ (位置・大きさを一様ランダムに生成)
- ・付加雑音 : $\epsilon = 0.02$

観測データ \mathbf{Y} にランダムユニタリ行列 \mathbf{Q}_p を掛け、秘匿観測信号 $\hat{\mathbf{Y}}$ を生成した。

評価指標として、以下の 2 つを用いた。

- (1) サポート間距離

$$\text{dist}(\hat{S}, S) = \frac{\max\{|\hat{S}|, |S|\} - |\hat{S} \cap S|}{\max\{|\hat{S}|, |S|\}} \quad (39)$$

ここで \hat{S} は、秘匿領域で求めた辞書を非秘匿領域へ逆変換することにより求めた。

- (2) スパース係数の推定値 $\hat{\mathbf{x}}$ の平均 l_2 誤差

$$J = \|\mathbf{x} - \hat{\mathbf{x}}\|^2 / \|\mathbf{x}\|^2 \quad (40)$$

4.2 評価

観測信号を秘匿した場合の推定精度を検証するため、観測信号を秘匿しない場合の MOD ならびに K-SVD との比較を行った。

- 1) 提案法 : 秘匿 MOD ならびに秘匿 K-SVD
- 2) 従来法 : MOD ならびに K-SVD

図 7 に秘匿 MOD ならびに秘匿 K-SVD により得られたサポート間距離 $\text{dist}(\hat{S}, S)$ と平均 l_2 誤差を示す。横軸は学習の更新回数を示す。更新回数 50 回において、サポート間距離は 80% を超え平均 l_2 誤差も 0.05 以下の値となっており、十分学習ができていくことがわかる。また図 8 に、観測信号を秘匿しない場合の MOD と KSVD により得られたサポート間距離 $\text{dist}(\hat{S}, S)$ と平均 l_2 誤差を示す。図 7 と図 8 を比較すると、同じ挙動を示

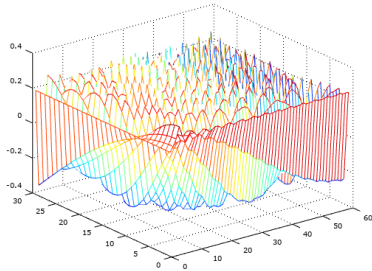


図4 辞書 $D_{true} \in \mathbb{R}^{30 \times 50}$: overcomplete DCT.

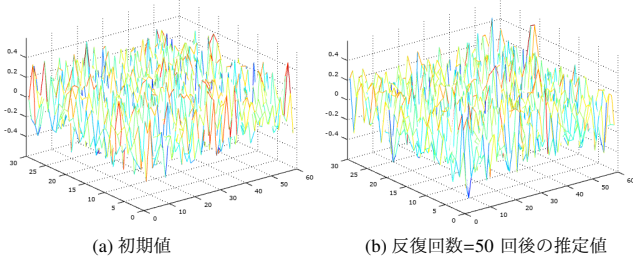


図5 秘匿領域の辞書 \hat{D} .

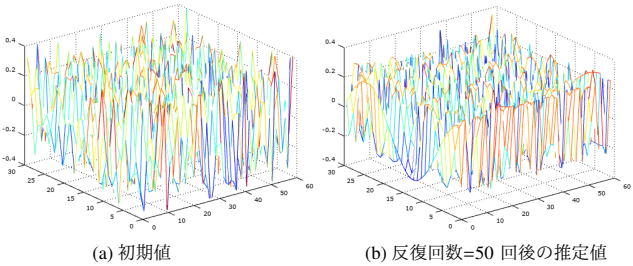


図6 秘匿領域の辞書 \hat{D} から復号した辞書 $D = Q_p^* \hat{D}$.

しており、観測信号を秘匿した場合にも推定精度の劣化がなく辞書ならびにスパース係数が推定できていることがわかる。

図4に観測データ生成に用いた overcomplete DCT の辞書 D_{true} を示す。図5には秘匿領域の辞書 \hat{D} の (a) 初期値、(b) 反復回数 50 回の後の推定値を示した。 \hat{D} は秘匿領域で更新されるため、反復回数 50 回の後もランダム信号として視認されることがわかる。図6には図5の秘匿辞書 \hat{D} に対応する復号した辞書 $D = Q_p^* \hat{D}$ を示した。反復回数 50 回後は、初期値よりも図4に示す辞書 D_{true} に近い値を示していることがわかる。

5. まとめと今後の予定

本稿ではスパース辞書学習アルゴリズムである MOD と K-SVD の秘匿演算法を提案した。観測信号を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。辞書学習は OMP などの係数選択アルゴリズムと比較して演算負荷も高い。セキュリティを保持しつつ、エッジ/クラウドの計算資源を利用して学習が可能となる利点は大きいと言える。今後は、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 The-

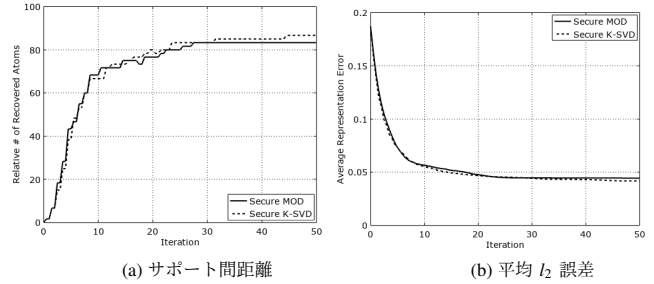


図7 秘匿 MOD ならびに秘匿 K-SVD のサポート間距離と平均 l_2 誤差.

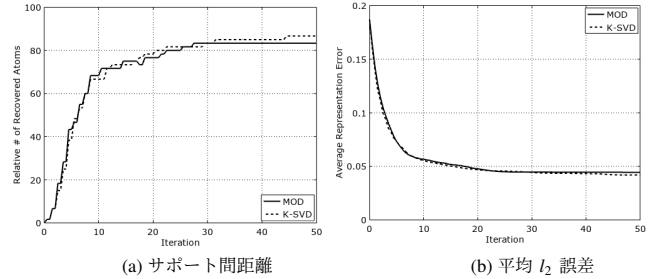


図8 MOD ならびに K-SVD のサポート間距離と平均 l_2 誤差.

- ory to Applications in Signal and Image Processing," Springer, 2010.
- [3] B. K. Natarajan: "Sparse approximate solutions to linear systems," *SIAM J. Comput.*, 24, 2, pp. 227-234, 1995.
- [4] K. Engan, S. O. Aase and J. Hakon Husoy: "Method of optimal directions for frame design", *ICASSP1999*, pp. 2443-2446, 1999.
- [5] M. Aharon, M. Elad and A. Bruckstein: "K-SVD: An algorithm for designing overcomplete dictionaries for sparse representation", *IEEE Trans. Sig. Proc.*, 54, 11, pp. 4311-4322, 2006.
- [6] Y. C. Pati, R. 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.
- [7] 手塚 太郎, "辞書学習によるビッグデータからのパターン発見," *日本化学会情報化学部会誌*, 32 巻, 4 号, p.76-79, 2014.
- [8] 杉田寛樹, 佐々木博昭, 庄野逸, "K-SVD を特徴抽出機構に用いたパターン認識," *信学技報*, vol. 114, no. 105, pp. 101-106, 2014.
- [9] 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.
- [10] 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.
- [11] R. L. Legendijk, 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.
- [12] 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.
- [13] Y. Saito, I. Nakamura, S. Shiota and H. Kiya, "An Efficient Random Unitary Matrix for Biometric Template Protection," *2016 Joint 8th International Conference on Soft Computing and Intelligent Systems (SCIS) and 17th International Symposium on Advanced Intelligent Systems (ISIS)*, Sapporo, 2016, pp. 366-370, 2016.
- [14] 仲地孝之, 貴家仁志, "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," *信学技報*, vol. 118, no. 73, SIS2018-2, pp. 7-12, 2018 年 6 月.
- [15] Takayuki Nakachi, Hitoshi Kiya, "Practical secure OMP computation and its application to image modeling," *IHIP2018*, 2018.
- [16] Takayuki Nakachi, Hiroyuki Ishihara, Hitoshi Kiya, "Privacy-preserving network BMI decoding of covert spatial attention," *IEEE ICSPCS2018*, p12, 2018.