

# スパースコーディングを用いた暗号化領域での画像モデリング

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 〒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。多数の分野に応用されており、画像処理の分野においてもノイズ除去、超解像、顔画像の圧縮・分類などその有効性が認められている。一方、画像処理をはじめとする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、スパースコーディングを用いた画像処理について、プライバシー保護を考慮した暗号化領域での画像モデリングを提案する。暗号化画像に対するスパースコーディングの秘匿演算法を提案するとともに、暗号化画像が視覚的に秘匿されていること並びに暗号をかけない場合と比較して性能劣化がないことをシミュレーションにより確認する。

キーワード スパースコーディング、画像処理、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

## Image Patch Modeling in Encrypted Domain using Sparse Coding

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

<sup>†</sup> NTT Network Innovation Laboratories, Nippon Telegraph and Telephone Corp. 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. The effectiveness of sparse coding for image processing has been confirmed in the areas of image compression, image denoising, and image separation. 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, Image Processing, 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]-[23] 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多数

の分野に応用 [4] されており、画像処理の分野においてもノイズ除去 [10]、インペインティング [11]、超解像 [12]、顔画像の圧縮 [13]・分類 [14] などその有効性が認められている。

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画像処理、音響処理、生体信号の解析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 [15]。今後のクラウドコンピュー

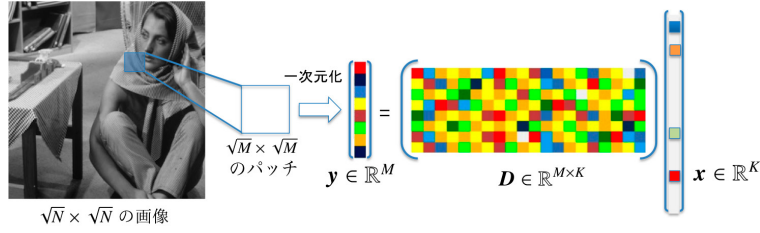


図1 画像パッチのスパースモデル：画像パッチを少数の基底ベクトルの重み付き線形和で表現する線形システム.

ティングの普及にとって、データの不正利用や流失、エンドユーザーのプライバシーの問題をいかに解決するかが重要な課題となっている。

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 [16]- [18]。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、スパースコーディングを用いた暗号化領域での画像モデリングを提案する。具体的には、画像パッチと呼ばれる小領域の画像がスパースコーディングによりモデル化できると仮定し、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) を画像を暗号化したまま演算する。提案法は、スパースコーディングで有効性が報告されているノイズ除去、インペインティング、超解像、顔画像の圧縮・分類などへの応用や、画像を暗号化した後に圧縮する Encryption-then-Compression (EtC) システム [19] への適用が期待できる。

本稿の構成は、以下の通りである。2. 節で画像モデリングの概要を説明し、3. 節で暗号化領域での画像モデリングを提案する。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. 画像モデリング

本節では、スパースコーディングを用いた画像モデリングについて述べる。

### 2.1 画像パッチモデル

図1の左に示すように、 $\sqrt{N} \times \sqrt{N}$ のサイズの画像を  $\sqrt{M} \times \sqrt{M}$ の画像パッチ (小領域のブロック) に分割し、一次元化した  $i$  番目の画像パッチ  $y_i = \{y_{i1}, \dots, y_{iM}\}^T \in \mathbb{R}^M$  を考える。この時、画像パッチ  $y_i$  が  $K$  個の基底の線形結合で表せると仮定する。

$$y_i = D x_i \quad (1)$$

ただし、 $D = \{d_1, \dots, d_K\} \in \mathbb{R}^{M \times K}$  は基底  $d_k$  (列ベクトル) を要素とする辞書行列であり、 $x_i = \{x_{i1}, \dots, x_{iK}\}^T \in \mathbb{R}^K$  はスパース係数

である。スパース係数は少数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  $D$  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  $y_i = D x_i$  では  $x_i$  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  $y_i$  の表現に利用される基底を  $D$  のうちの一部に制限する。つまり、 $\|x_i\|_0$  で  $x_i$  の  $l_0$  ノルム、すなわちベクトル  $x_i$  の非ゼロ成分の数を表すとして、スパースコーディングは典型的には最適化問題

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

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

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

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  $y_i$  と辞書  $D$  が与えられた時、 $y_i$  を  $D x_i$  で近似するような係数  $x_i$  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

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

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

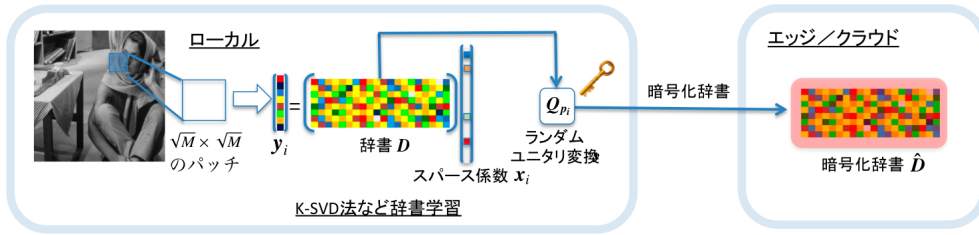


図2 事前準備：ローカルでの辞書学習と秘匿.

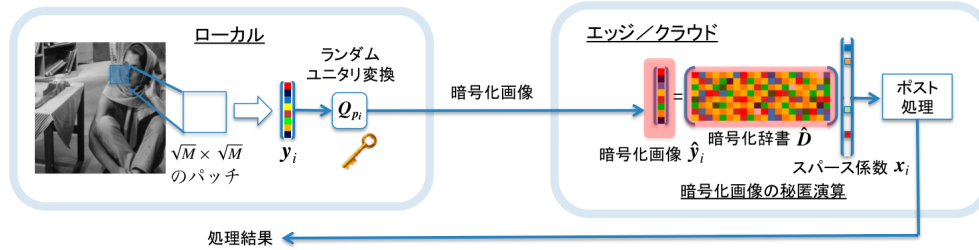


図3 実行：エッジ/クラウドでの暗号化画像の秘匿演算.

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。

### 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 [25] あるいはカーブレット変換 [26] 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  $y$  と  $Dx$  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. 暗号化領域での画像モデリング

本節ではエッジ/クラウドでの利用を想定した暗号化領域で画像モデリングを行う方法を提案する。

### 3.1 システム構成

エッジ/クラウドの計算資源を利用して、暗号化領域でスパースコーディングによる画像モデリング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  $D$  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  $D$  を鍵  $p_i$  を持つランダムユニタリ行列  $Q_{p_i}$  により暗号化辞書行列  $\hat{D}_i$  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暗号化領域の実行では、最初にローカルにおいて画像パッチ  $y_i$  を暗号化画像  $\hat{y}_i$  へ変換しクラウドへ伝送する。次にクラウドでは、事前に転送された暗号化辞書行列  $\hat{D}_i$  と暗号化画像  $\hat{y}_i$  を用いて OMP のア

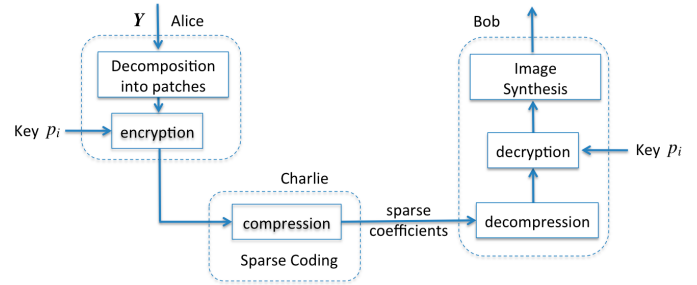


図4 Encryption-then-Compression (EtC) システムへの適用例.

ルゴリズムを実行してスパース係数  $x_i$  を推定する。

提案法は、スパースコーディングで有効性が報告されているノイズ除去、インペインティング、超解像、顔画像の圧縮・分類などへの応用や、画像を暗号化した後に圧縮する Encryption-then-Compression (EtC) システム [19] への適用が期待できる。

一例として、図4に EtC システムの構成例を示した。一般に SNS を利用した通信では、画像などのコンテンツはプロバイダが受信した信号を再圧縮 (CtE: Compression-then-Encryption) することが知られている。CtE システムでは、画像を再圧縮するために一旦伸張する必要があり、画像をプロバイダに開示しなければならない問題が発生する。プロバイダの人為的なミスや事故に対しては、無防備な現状である。このような問題に対して EtC システムでは、暗号化領域での圧縮が可能のため伸張の必要がなく、画像が流出した際にもその影響を小さくすることができる。図4の Alice (エンドユーザー) は画像を暗号化して、エッジ/クラウドへ送信する。Charlie (プロバイダ) は暗号化画像を受信し、圧縮を行う。Bob (エンドユーザー) は画像の閲覧を許可されたエンドユーザーである。画像伸張の後、公開鍵暗号などを用いて取得した鍵  $p_i$  を用いて暗号化画像を復号することができる。

### 3.2 ランダムユニタリ行列に基づく秘匿演算

提案法では、ランダムユニタリ変換を用いて、画像を暗号化

画像へ変換する。ランダムユニタリ変換を用いた秘匿演算の先行研究として、キャンセルラブルバイオメトリクスのための方法としてテンプレート保護法が研究されている [20]- [22]。また、先に著者らはランダムユニタリ変換を用いた OMP の秘匿演算法 [23] と、空間注意 BMI (Brain Machine Interface) デコーディングへの適用法 [24] を提案し、その有効性を検証した。

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  $p_i$  によって生成されるランダムユニタリ行列  $\mathbf{Q}_{p_i}$  を用いた変換  $T(\cdot)$  により、信号  $\mathbf{f}_{i,j}$  ( $j = 1, \dots, N$ ) を秘匿信号  $\hat{\mathbf{f}}_{i,j}$  へ変換する。

$$\hat{\mathbf{f}}_{i,j} = T(\mathbf{f}_{i,j}, p_i) = \mathbf{Q}_{p_i} \mathbf{f}_{i,j} \quad (5)$$

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

$$\mathbf{Q}_{p_i}^* \mathbf{Q}_{p_i} = \mathbf{I} \quad (6)$$

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  $\mathbf{Q}_{p_i}$  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によって  $\mathbf{Q}_{p_i}$  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秘匿信号は、 $\mathbf{Q}_{p_i} = \mathbf{Q}_{p_s}$  の場合、以下の特徴を持つ (多くの特徴が持つが、ここでは OMP の秘匿演算に関連する特徴のみ記載)。

特徴 1: ノルム不変

$$\|\mathbf{Q}_{p_i} \mathbf{f}_{i,j}\|_2^2 = \|\mathbf{f}_{i,j}\|_2^2 \quad (7)$$

特徴 2: ユークリッド距離の保存

$$\|\mathbf{f}_{i,j} - \mathbf{f}_{s,t}\|_2^2 = \|\hat{\mathbf{f}}_{i,j} - \hat{\mathbf{f}}_{s,t}\|_2^2 \quad (8)$$

特徴 3: 内積の保存

$$\mathbf{f}_{i,j}^* \mathbf{f}_{s,t} = \hat{\mathbf{f}}_{i,j}^* \hat{\mathbf{f}}_{s,t} \quad (9)$$

提案する暗号化領域での画像モデリングでは、 $i$  番目の画像パッチ  $\mathbf{y}_i$  について鍵  $p_i$  のランダムユニタリ行列  $\hat{\mathbf{Q}}_{p_i}$  を用いて、次式のように暗号化辞書行列  $\hat{\mathbf{D}}_i$  ならびに暗号化画像  $\hat{\mathbf{y}}_i$  を生成する。

$$\hat{\mathbf{D}}_i = T(\mathbf{D}, p_i) = \mathbf{Q}_{p_i} \mathbf{D} \quad (10)$$

$$\hat{\mathbf{y}}_i = T(\mathbf{y}_i, p_i) = \mathbf{Q}_{p_i} \mathbf{y}_i \quad (11)$$

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

$$\hat{\mathbf{x}}_i = \arg \min_{\mathbf{x}_i} \|\hat{\mathbf{y}}_i - \hat{\mathbf{D}}_i \mathbf{x}_i\|_2^2 \quad \text{subject to} \quad \|\mathbf{x}_i\|_0 < \epsilon \quad (12)$$

先に著者らは、上式を直交マッチング追跡法 (OMP) によって解き、スパース係数  $\hat{\mathbf{x}}_i$  が入力信号  $\mathbf{y}_i$  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  $\mathbf{x}_i$  と等しくなることを証明した [23]。これはランダムユニタリ変換が、内積の保存など式 (7)-(9) に示す持つために成立する。以下に、 $\hat{\mathbf{y}}_i$  と  $\hat{\mathbf{D}}_i$  が与えられた時の直交マッチング追跡法 (OMP) アルゴリズムを示す。ここでは煩雑さを避けるために、時間に関する添え字  $i$  の表記を省略した。

1) 初期化:  $k = 0$

$$\text{初期解 } \hat{\mathbf{x}}^0 = \mathbf{0}$$

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

$$\text{解の初期サポート } S^0 = \emptyset$$

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:

$$\begin{aligned} \hat{\epsilon}(j) &= \min_{\hat{\mathbf{x}}_j} \|\hat{\mathbf{x}}_j \hat{\mathbf{d}}_j - \hat{\mathbf{r}}^{k-1}\|_2^2 \\ &= \|\hat{\mathbf{r}}^{k-1}\|_2^2 - \frac{(\hat{\mathbf{d}}_j \cdot \hat{\mathbf{r}}^{k-1})^2}{\|\hat{\mathbf{d}}_j\|_2^2} \end{aligned} \quad (13)$$

2. サポートの更新:

$$j_0 = \arg \min_{j \in S^{k-1}} \{\hat{\epsilon}(j)\}, S^k = S^{k-1} \cup \{j_0\} \quad (14)$$

3. サポート内での最良解の探索:

$$\begin{aligned} \hat{\mathbf{x}}^k &= \arg \min_{\hat{\mathbf{x}}_{S^k}} \|\hat{\mathbf{y}} - \hat{\mathbf{D}}_{S^k} \hat{\mathbf{x}}_{S^k}\|_2^2 \\ &= (\hat{\mathbf{D}}_{S^k}^* \hat{\mathbf{D}}_{S^k})^{-1} (\hat{\mathbf{D}}_{S^k}^* \hat{\mathbf{y}}) \end{aligned} \quad (15)$$

4. 残差の更新:

$$\hat{\mathbf{r}}^k = \hat{\mathbf{y}} - \hat{\mathbf{D}}_{S^k} \hat{\mathbf{x}}^k \quad (16)$$

5. 停止条件:

$$\|\hat{\mathbf{r}}^k\|_2 < \epsilon \quad (17)$$

### 3.3 各画像パッチの鍵の選択

式 (11) に示すように、画像パッチ  $\mathbf{y}_i$  ( $i = 1, 2, \dots, L$ ) は鍵  $p_i$  のランダムユニタリ行列  $\mathbf{Q}_{p_i}$  を用いて暗号化画像  $\hat{\mathbf{y}}_i$  へ変換される。但し、 $L$  は画像パッチの総数 ( $L = N/M$ ) である。

1) 選択法 1 (鍵固定):  $p_1 = p_2 = \dots = p_L$

すべての画像パッチに対して、同じ鍵を用いて暗号化画像を生成する。鍵の管理が容易である。

2) 選択法 2 (鍵変動):  $p_1 \neq p_2 \neq \dots \neq p_L$

各画像パッチ毎に、異なる鍵を用いて暗号化画像を生成する。視認性ならびに復号確率の観点から、暗号化の強度が強くなる。

## 4. シミュレーション結果

有効性を検証するために、自然画像に対する画像モデリングを行った。

### 4.1 シミュレーション条件

評価画像として、図 5 に示す標準画像データベース SIDBA (Standard Image Data-BAsE) の  $512 \times 512$  画素のグレー画像 (Barbara, Mandril) を用いた。辞書  $\mathbf{D}$  は K-SVD 法により評価画像以外の複数の自然画像を入力として  $M = 64$  ( $8 \times 8$ ) の大きさの基底を  $K = 256$  個生成した。ランダムユニタリ行列は、 $M \times M = 64 \times 64$  の大きさでグラムシュミットの直交化に

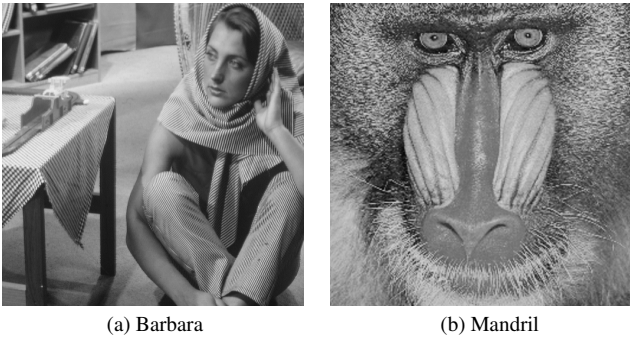


図5 原画像.

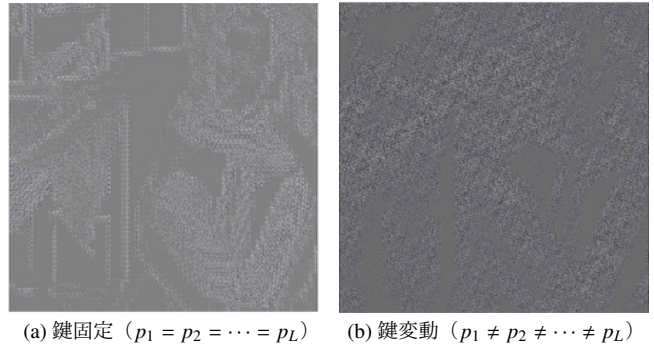


図7 Barbaraの暗号化画像.

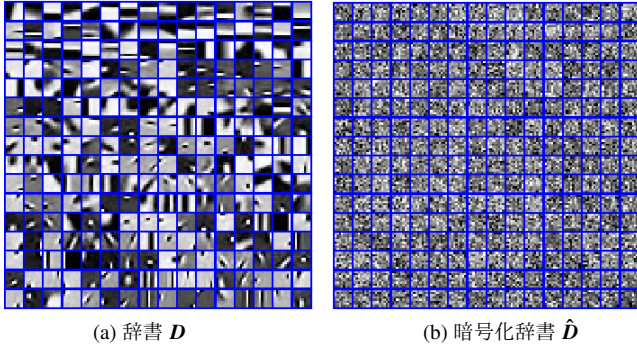


図6 K-SVD法により学習した辞書と暗号化辞書.

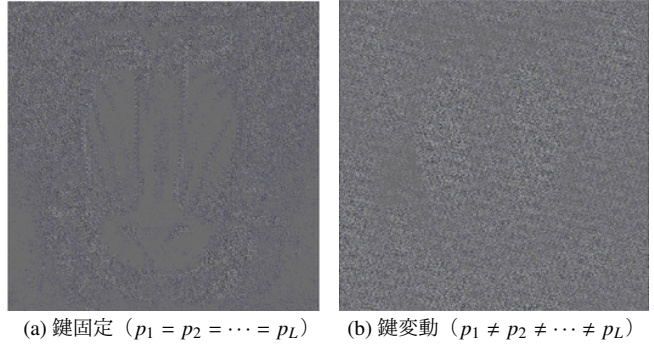


図8 Mandril画像の暗号化画像.

より生成した。

#### 4.2 結果と考察

図6に辞書  $D$  と式 (10) により変換した暗号化辞書  $\hat{D}$  を示す。秘匿信号に変換されていることが確認できる。図7ならびに図8に各画像パッチの鍵を固定ならびに変動させた場合の Barbara ならびに Mandril の暗号化画像を示す。鍵固定の場合には、若干半開示画像の特性を示している。画像パッチ内の画像は十分に暗号化されているものの、画像パッチの特性が同じ場合には視覚的に似た暗号化画像となる。鍵変動の場合には、視覚的秘匿性は十分高い。

表1には、式 (17) に示す残差の  $L_2$  ノルムに関する停止条件の  $\epsilon$  を変化させた時の平均スパース率  $\bar{S}_i$  と復号画像品質 (PSNR) を示した。平均スパース率は  $\bar{S}_i = \sum_{i=1}^L S_i / L$  で定義される。 $S_i$  は次式に示す画像パッチ  $y_i$  におけるスパース率である。

$$\text{スパース率 } S_i = \frac{\text{スパース係数の非ゼロ成分の個数}}{\text{スパース係数の次元 } K} \quad (18)$$

表1を見ると、 $\epsilon$  が大きくなるにつれスパース率が小さくなり復号画像品質が低下している。また、図9には  $\epsilon$  を変化させた時の Barbara の復号画像を示した。以上より、 $\epsilon$  により画像品質の制御が可能であることがわかる。なお、暗号化しない従来法の OMP も全く同じ特性を示した。

図10に従来法の OMP と提案法について、 $\epsilon=10.000$  の時の Barbara のスパース係数を示す。また、図11には対応する復号画像を示す。図10ならびに図11より、暗号化画像に対する画像モデリングでも、暗号化しない従来の OMP の場合と同じスパース係数が推定され、同じ復号画像が得られていることが確認できる。

表1 平均スパース率  $\bar{S}_i$  と復号画像品質 (PSNR).

(a) Barbara					
$\epsilon$	3.162	5.477	7.071	10.000	14.142
平均スパース率 $\bar{S}_i$	0.183	0.118	0.092	0.061	0.036
PSNR [dB]	37.57	34.52	32.88	30.52	28.12

(b) Mandril					
$\epsilon$	3.162	5.477	7.071	10.000	14.142
平均スパース率 $\bar{S}_i$	0.192	0.110	0.081	0.050	0.027
PSNR [dB]	38.60	34.09	32.08	29.47	27.05

## 5. まとめと今後の予定

本稿では、OMPの秘匿演算を用いた暗号化領域での画像モデリングを提案した。暗号化画像の視覚的秘匿性能について確認するとともに、画像モデリングの性能が、暗号をかけない場合と比較して劣化がないことをシミュレーションにより検証した。

### 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 directions 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",

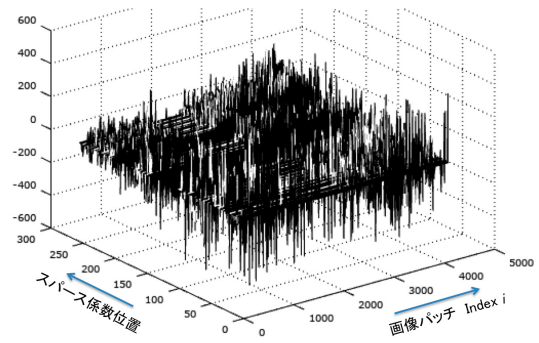


(a)  $\epsilon = 3.162$  (PSNR=37.57 [dB]) (b)  $\epsilon = 5.477$  (PSNR=34.52 [dB])

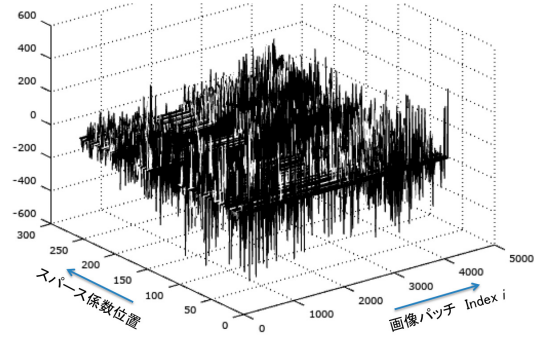


(c)  $\epsilon = 7.071$  (PSNR=32.88 [dB]) (d)  $\epsilon = 14.142$  (PSNR=28.12 [dB])

図9 停止条件  $\epsilon$  を変化させた時の Barbara の復号画像.



(a) OMP (平均スパース率  $\bar{S}_i = 0.061$ )



(b) 提案法 (平均  $\bar{S}_i = 0.061$ )

図10  $\epsilon=10.000$  の時の Barbara のスパース係数.



(a) OMP (PSNR=30.52 [dB]) (b) 提案法 (PSNR=30.52 [dB])

図11  $\epsilon=10.000$  の時の Barbara の復号画像.

- 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] J. Yang, J. Wright, T. S. Huang and Y. Ma, "Image super-resolution via sparse representation," IEEE Transactions on Image Processing, vol. 19, no. 11, pp. 2861-2873, Nov. 2010.
- [13] O. Bryt, M. Elad, "Compression of facial images using the K-SVD algorithm," Journal of Visual Communication and Image Representation, vol. 19, Issue 4, pp. 270-282, 2008.
- [14] Wright, J., Yang, A., Ganesh, A., Sastry, S. and Ma, Y., "Robust face recognition via sparse representation," IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 31, no. 2, pp. 210-227, 2009.
- [15] 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.
- [16] R. Lazerretti and M. Barni, "Private computing with garbled circuits [applications corner]," IEEE Signal Processing Magazine, vol. 30, no. 2, pp. 123-127, March 2013.
- [17] 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.
- [18] 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.
- [19] T. Chuman, K. Kurihara, H. Kiya, "On the security of block scrambling-based EtC systems against extended jigsaw puzzle solver attacks," IEICE Transactions on Information and Systems, vol. E101.D, no. 1, pp. 37-44, 2018.
- [20] 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.
- [21] I. Nakamura, Y. Tonomura, and H. Kiya, "Unitary transform-based template protection and its application to l2-norm minimization problems," IEICE Trans. Inf. & Sys., vol. E99-D, no.1, pp. 60-68, Jan. 2016.
- [22] 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.
- [23] 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, SIS2018-2, no.73, pp. 7-12, 2018年6月.
- [24] 仲地孝之, 石原裕之, 貴家仁志, "プライバシー保護を考慮した空間注意 BMI デコーディング," 信学技報, NC2018-8, no. 80, pp. 15-20, 2018年6月.
- [25] T. S. Lee: "Image representation using 2D Gabor wavelets", IEEE Trans. Pattern Anal. Mach. Intell., 18, 10, pp. 959-971 (1996).
- [26] 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).