

秘匿 OMP 演算を用いた暗号化画像のクラス分類

仲地 孝之[†] 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

^{††} 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: [†]nakachi.takayuki@lab.ntt.co.jp, ^{††}kiya@tmu.ac.jp

あらまし 近年、SNS などネット上の個人に関連する映像の爆発的な増加や公共の場における監視カメラ台数の増加に伴い、プライバシー保護が新たな課題として発生している。SNS や監視カメラなどの膨大な映像の処理は、特に急速に普及してきているエッジ/クラウド上での処理が増えることが予想される。しかしながら、その利用はサービス提供者の信頼性を前提にしている。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ランダムユニタリ変換に基づく暗号化画像のクラス分類法について提案する。提案法を人物を含む画像とそれ以外の画像で構成される INRIA Person Dataset に適用し、暗号化しない画像に対するクラス分類法と比較して、推定性能が劣化し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 画像のクラス分類、スパースコーディング、辞書学習、K-SVD 法、ランダムユニタリ変換、秘匿演算

Encrypted Image Classification by Using Secure OMP Computation

Takayuki NAKACHI[†] and Hitoshi KIYA^{††}

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

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

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

Abstract Currently, huge amounts of image/video are being recorded and uploaded every day by surveillance systems or SNS services etc. Recent popularized edge/cloud computing is widely used for handling and analysis such huge amount of image/video data. 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 an encrypted image classification method by using secure sparse coding based on a random unitary transform. We carry out experiments of detecting human in images on the INRIA person dataset. It is shown that the encrypted image classification method enables us to not only protects images, but also have the same classification performance as that of sparse coding with unprotected images.

Key words Image Classification, Sparse Coding, Dictionary Learning, K-SVD, Random Unitary Transform, Secure Computation

1. ま え が き

近年、インターネットの普及により SNS やネット上に画像や映像をアップロードする機会が増えている。また公共の場における安全の確保が重要な社会課題として認識される中、監視カメラのシステムは有効な解決手段として期待され、その設置台数は世界規模で増加傾向にある。

一方、これら SNS などネット上の個人に関連する映像の爆発的な増加や監視カメラ台数の増加に伴い、プライバシー保護が新たな課題として発生している [1]。また近年、様々な分野でエッジ/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。SNS や監視カメラなどの膨大な映像処理は、今後さらにエッジ/クラウド上で処理することが増えることが予想されるが、その利用はサービス提供者の信頼性を前提にしている。特にエッジ/クラウドコンピューティングでは、信頼性の欠如や事故によるデータの不正利用や流失が発生することで、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 [2]。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、エンドユーザーのプライバシーの問題の解決は重要な課題である。

エッジ/クラウドコンピューティングのプライバシー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

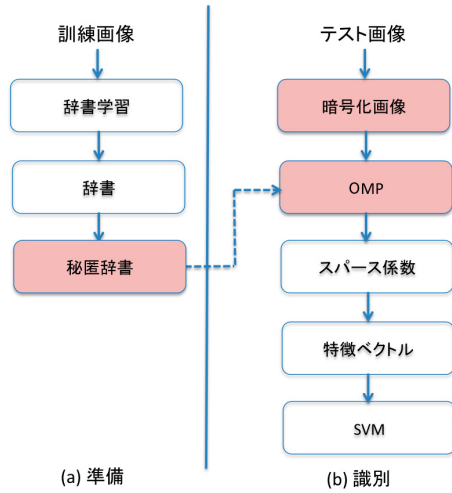


図1 暗号化画像のクラス分類の概要。

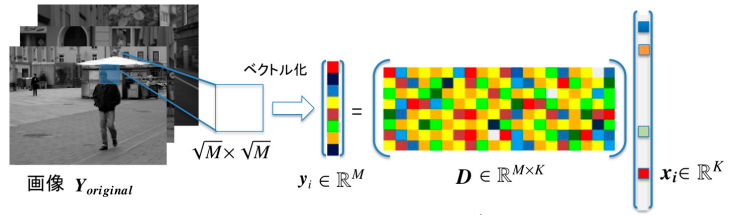


図2 画像パッチのスパースモデル。

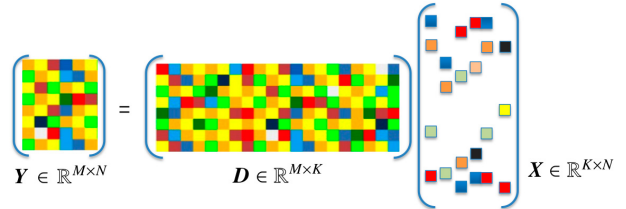


図3 スパース辞書学習。

ことが可能な秘密計算が盛んに研究されている [3]- [5]。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、秘密計算は除算の困難性、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。

そのような背景のもと、先に著者らはランダムユニタリ変換に基づくスパースコーディングの秘匿演算法を提案した [6]- [8]。ランダムユニタリ変換による秘匿演算は、マルチパーティプロトコルや準同型暗号と比較すると高速に演算が可能であり、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できる特徴がある。

スパースコーディング (Sparse Coding: SC) [9]- [16] 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の重み付き線形和で表現する手法である。ノイズ除去、インペインティング、超解像、顔画像の圧縮・分類などの分野で有効性が報告されている。近年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 [15]。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 [17] では代表的な辞書学習法である K-SVD (K-Singular Value Decomposition) [13] 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。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画像のクラス分類法について提案する。

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. 節でスパースコーディングを用いた暗号化画像のクラス分類法を提案する。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

図1に提案する暗号化画像のクラス分類法の概要を示す。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 K-SVD (K-Singular Value Decomposition) [13] について説明する。

2.1 定式化

図2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。観測信号 y_i (M 次元の列ベクトル) の集合を $Y = \{y_i\}_{i=1}^N$ とする。このとき、図3に示すように、 Y が K 個の基底の線形結合で表せると仮定する。

$$Y = DX \quad (1)$$

ただし、 $D = \{d_1, \dots, d_K\} \in \mathbb{R}^{M \times K}$ は基底 d_i (M 次元の列ベクトル) を要素とする辞書行列であり、 $X = \{x_i\}_{i=1}^N$ 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 $Y = DX$ では 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 Y の表現に利用される基底を 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、

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

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 $\|A\|_F = \sqrt{\sum_{ij} A_{ij}^2}$ 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 D を固定し、式 (2) の最適化問題を解く。各入力観測信号ベクトル 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。

$$\mathbf{x}_i = \arg \min_{\mathbf{x}_i} \|\mathbf{y}_i - \mathbf{D}\mathbf{x}_i\|_F^2 \quad \text{subject to} \quad \|\mathbf{x}_i\|_0 < T_0$$

$$i = 1, 2, \dots, N. \quad (3)$$

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で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 [18]。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) [14] 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 \mathbf{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 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。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 (あるいは fuzzy k-means 法) では各サンプルを多数のクラスに割り当てる。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 \mathbf{D} 全体ではなく、一つの基底 \mathbf{d}_k に着目し順次更新する。

$$\|\mathbf{Y} - \mathbf{D}\mathbf{X}\|_F^2 = \left\| \mathbf{Y} - \sum_{j=1}^K \mathbf{d}_j \mathbf{x}_T^j \right\|_F^2$$

$$= \left\| \left(\mathbf{Y} - \sum_{j \neq k} \mathbf{d}_j \mathbf{x}_T^j \right) - \mathbf{d}_k \mathbf{x}_T^k \right\|_F^2$$

$$= \|\mathbf{E}_k - \mathbf{d}_k \mathbf{x}_T^k\|_F^2. \quad (4)$$

ここで、 \mathbf{x}_T^k は図4に示すように \mathbf{X} の k 番目の行ベクトルを表し、 \mathbf{E}_k は観測信号の集合 \mathbf{Y} から基底 \mathbf{d}_k を除いた線形予測値との残差を示す。

K-SVD では \mathbf{E}_k を特異値分解 (Singular Value Decomposition: SVD) することで、 \mathbf{d}_k と \mathbf{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 \mathbf{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。 \mathbf{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。

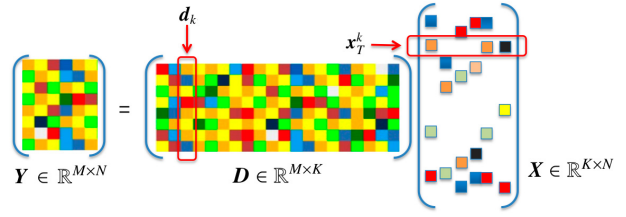


図4 基底 \mathbf{d}_k と \mathbf{X} の k 番目の行ベクトル \mathbf{x}_T^k .

$$\omega_k = \{i \mid 1 \leq i \leq K, \mathbf{x}_T^k(i) \neq 0\}. \quad (5)$$

但し、 $\mathbf{x}_T^k(i)$ は \mathbf{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 $\mathbf{\Omega}_k$ を定義する。 $\mathbf{\Omega}_k$ を用いると \mathbf{x}_T^k の非ゼロ要素のみで構成されるベクトル \mathbf{x}_R^k が、次式のように書き表せる。

$$\mathbf{x}_R^k = \mathbf{x}_T^k \mathbf{\Omega}_k. \quad (6)$$

同様に \mathbf{E}_k に対して、 $\mathbf{\Omega}_k$ を用いて $\mathbf{E}_k^R = \mathbf{E}_k \mathbf{\Omega}_k$ と変換する。

$$\|\mathbf{E}_k \mathbf{\Omega}_k - \mathbf{d}_k \mathbf{x}_T^k \mathbf{\Omega}_k\|_F^2 = \|\mathbf{E}_k^R - \mathbf{d}_k \mathbf{x}_R^k\|_F^2. \quad (7)$$

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

$$\mathbf{E}_k^R = \mathbf{U} \mathbf{\Delta} \mathbf{V}^T$$

$$= \mathbf{u}_1 \cdot \sigma_1 \mathbf{v}_1^T + \mathbf{u}_2 \cdot \sigma_2 \mathbf{v}_2^T + \dots + \mathbf{u}_n \cdot \sigma_n \mathbf{v}_n^T. \quad (8)$$

\mathbf{u}_i と \mathbf{v}_j は、それぞれ \mathbf{U} と \mathbf{V} の i 番目の列ベクトル、 σ_i は $\mathbf{\Delta}$ 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 \mathbf{u}_1 と $\sigma_1 \mathbf{v}_1^T$ を用いて、基底 $\mathbf{d}_k = \mathbf{u}_1$ ならびにスパース係数の行ベクトル $\mathbf{x}_T^k = \sigma_1 \mathbf{v}_1^T$ とし近似解を得る。

3. 秘匿 OMP 演算を用いた暗号化画像のクラス分類

本節ではランダムユニタリ行列に基づく秘匿 OMP 演算を用いた暗号化画像のクラス分類法を提案する。

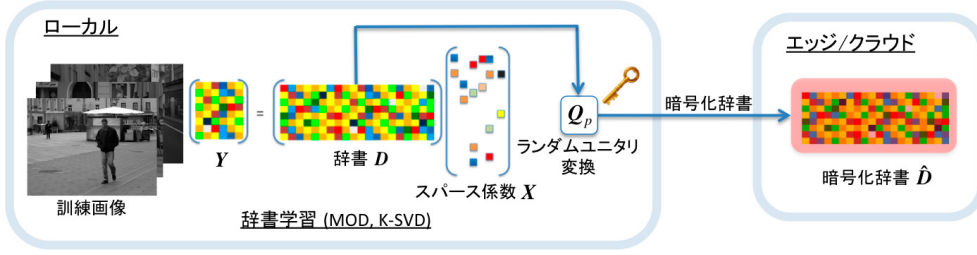
3.1 システム構成

図5にエッジ/クラウドの計算資源を利用して、スパースコーディングによる暗号化画像のクラス分類法のシステム構成を示す。図5(a)のステップでは、ローカルにおいて辞書行列 \mathbf{D} を K-SVD 法を用いて学習し生成する。その後、辞書行列 \mathbf{D} を鍵 p を持つランダムユニタリ行列 \mathbf{Q}_p により暗号化辞書行列 $\hat{\mathbf{D}}$ へ変換しエッジ/クラウドへ伝送する。

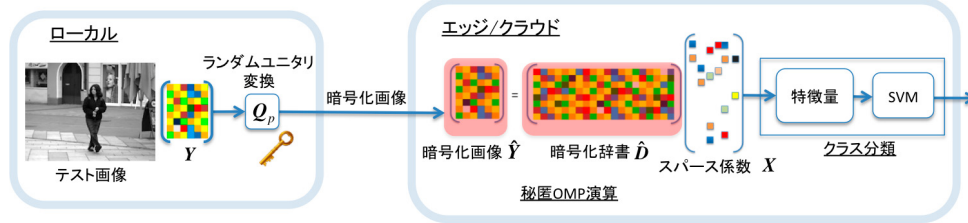
図5(b)のステップでは、秘匿 OMP 演算によりスパース係数を推定しクラス分類を行う。最初にローカルにおいて画像パッチ \mathbf{y}_i を暗号化画像 $\hat{\mathbf{y}}_i$ へ変換しエッジ/クラウドへ伝送する。次にエッジ/クラウドでは、暗号化画像 $\hat{\mathbf{y}}_i$ と事前に転送された暗号化辞書行列 $\hat{\mathbf{D}}$ を用いて OMP のアルゴリズムを実行してスパース係数 \mathbf{x}_i を推定する。その後スパース係数 \mathbf{x}_i から特徴量を生成し、サポートベクターマシン (SVM) によりクラス分類を行う。

3.2 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



(a) 辞書の学習と暗号化辞書の生成



(b) 秘匿 OMP 演算によるスパース係数の推定とクラス分類

図5 スパースコーディングによる暗号化画像のクラス分類法のシステム構成。

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。

$$\hat{f}_i = T(f_i, p) = Q_p f_i \quad (9)$$

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

$$Q_p^* Q_p = I \quad (10)$$

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。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

$$\|f_i\|_F^2 = \|\hat{f}_i\|_F^2 \quad (11)$$

特徴2: ユークリッド距離の保存

$$\|f_i - f_j\|_F^2 = \|\hat{f}_i - \hat{f}_j\|_F^2 \quad (12)$$

特徴3: 内積の保存

$$f_i^* f_j = \hat{f}_i^* \hat{f}_j \quad (13)$$

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。

3.3 直交マッチング追跡法 (OMP) の秘匿演算

秘匿 OMP 演算を用いた暗号化画像のクラス分類では、次式のように暗号化画像パッチ \hat{y}_i ならびに暗号化辞書 \hat{D} を生成する。

$$\hat{y}_i = T(y_i, p) = Q_p y_i \quad (14)$$

$$\hat{D} = T(D, p) = Q_p D \quad (15)$$

式(3)に代わり、次式に示す \hat{y}_i と \hat{D} が与えられた時の最適化問題を考える。

$$\hat{x}_i = \arg \min_{x_i} \|\hat{y}_i - \hat{D} x_i\|_2^2 \quad \text{subject to} \quad \|x_i\|_0 < \epsilon \quad (16)$$

先に著者らは、上式を OMP によって解き、スパース係数 \hat{x}_i が画像パッチ y_i と辞書 D を暗号化しない場合に得られたスパース係数 x_i と等しくなることを証明した [6]。以下に、 \hat{y}_i と \hat{D} が与えられた時の OMP アルゴリズムを示す。ここでは煩雑さを避けるために、添え字 i の表記を省略した。

直交マッチング追跡法 (OMP) アルゴリズム

1) 初期化: $k = 0$

初期解 $\hat{x}^0 = \mathbf{0}$

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

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:

$$\begin{aligned} \hat{\epsilon}(i) &= \min_{\hat{x}_i} \|\hat{x}_i \hat{d}_i - \hat{r}^{k-1}\|_2^2 \\ &= \|\hat{r}^{k-1}\|_2^2 - \frac{(\hat{d}_i^* \cdot \hat{r}^{k-1})^2}{\|\hat{d}_i\|_2^2} \end{aligned} \quad (17)$$

2. サポートの更新:

$$i_0 = \arg \min_{i \notin S^{k-1}} \{\hat{\epsilon}(i)\}, S^k = S^{k-1} \cup \{i_0\} \quad (18)$$

3. サポート内での最良解の探索:

$$\begin{aligned} \hat{x}^k &= \arg \min_{\hat{x}_{S^k}} \|\hat{y} - \hat{D}_{S^k} \hat{x}_{S^k}\|_2^2 \\ &= (\hat{D}_{S^k}^* \hat{D}_{S^k})^{-1} (\hat{D}_{S^k}^* \hat{y}) \end{aligned} \quad (19)$$

4. 残差の更新:

$$\hat{r}^k = \hat{y} - \hat{D}_{S^k} \hat{x}^k \quad (20)$$

5. 停止条件:

$$\|\hat{r}^k\|_2 < \epsilon \quad (21)$$

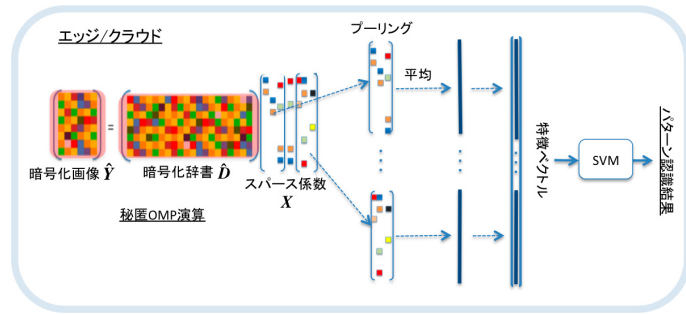


図6 特徴量抽出と SVM によるクラス分類.

3.4 特徴量抽出と SVM によるクラス分類

図6に特徴量抽出と SVM によるクラス分類について示す。最初に各画像パッチ y_i に対応するスパース係数 x_i を画像中の局所的な範囲でブロック化し、これを一つの局所的な特徴ベクトルとする。具体的にはブロックサイズを $B \times B$ としたとき、その範囲に該当する B^2 個の係数ベクトルを行方向に足しあわせて平均を計算し、局所的な特徴ベクトル $\bar{x}_j (j = 1, 2, \dots, N/B^2)$ とする。全てのブロックに対する局所的な特徴ベクトルを連結し特徴量

$$\bar{x} = [\bar{x}_1^T, \bar{x}_2^T, \dots, \bar{x}_{N/B^2}^T]^T \quad (22)$$

とする。

SVM は機械学習の一つであり、分離識別機器として広く用いられている。SVM では特徴ベクトル \bar{x} に対し、識別関数

$$y = \text{sign}(\omega^T \bar{x} + b) \quad (23)$$

により、2 値の出力値を計算する。ここで ω は重みに対応するパラメータであり、 b はバイアス項である。また関数 $\text{sign}(u)$ は、 $u > 0$ のとき 1 をとり、 $u \leq 0$ のとき -1 をとる符号関数である。カーネル法と呼ばれる手法により、非線形な問題に対応することも可能である。特徴ベクトルをより高次元の特徴空間へ写像し、その空間で線形の識別を行う。

4. シミュレーション結果

有効性を検証するために、人物を含む画像とそれ以外の画像を識別する課題に対して、シミュレーションを行った。

4.1 INRIA Person Dataset と実験条件

識別対象は INRIA Person Dataset [20] を用いた。INRIA Person Dataset は人物を含む画像とそれ以外の画像で構成されており、ベンチマークのデータセットとして幅広く使用されている。複数の大きさの画像が提供されているが、ここでは識別対象の画像は 480×640 に統一した。

1) K-SVD による辞書設計

人物が含まれる 20 枚の画像から 8×8 の大きさの画像パッチをランダムに取得し観測信号の集合 Y とし、基底の数は $K = 256$ と設定した。 64×256 の大きさの辞書となる。

2) ランダムユニタリ変換の生成

グラムシュミットの直交化を用いて 64×64 の大きさのランダムユニタリ行列を生成した。

表1 提案法の識別率 [%].

(a) 基底の数: $L = 1$											
試行	1	2	3	4	5	6	7	8	9	10	平均
識別率	100	70	80	70	90	90	80	60	90	70	80

(b) 基底の数: $L = 5$											
試行	1	2	3	4	5	6	7	8	9	10	平均
識別率	90	60	90	70	90	90	80	50	100	70	79

表2 非秘匿 OMP を用いた場合の識別率 [%].

(a) 基底の数: $L = 1$											
試行	1	2	3	4	5	6	7	8	9	10	平均
識別率	100	70	80	70	90	90	80	60	90	70	80

(b) 基底の数: $L = 5$											
試行	1	2	3	4	5	6	7	8	9	10	平均
識別率	90	60	90	70	90	90	80	50	100	70	79

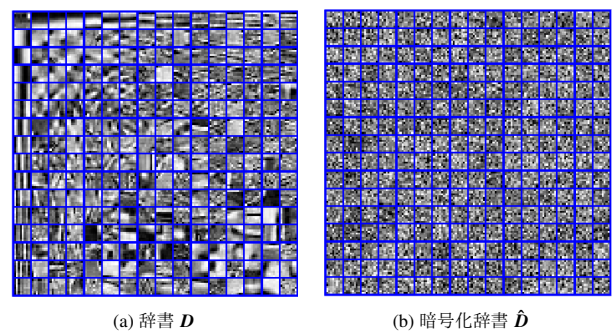


図7 人物が含まれる画像 (20 枚) から設計した辞書とその暗号化辞書.

3) SVM の学習と識別

局所的な特徴ベクトルを生成する際のブロックサイズを 20×20 とした。SVM の設計では 100 枚の画像 (人物を含む画像 50 枚、人物を含まない画像 50 枚) を対象として、線形 SVM の学習と識別を行った。評価方法として K-分割交差検証を用いた。100 枚の画像を 10 分割 (1 分割あたり人物を含む画像と含まない画像それぞれ 5 枚) し、1 つが識別のテスト用で残りの 9 つを学習に使用した。この試行をテストに使用する分割を順々に変えて行った。評価尺度として、以下の識別率を用いた。

$$\text{識別率} = \frac{\text{正しいクラスに分類された枚数}}{\text{識別に使用した画像の枚数}} \quad (24)$$

4.2 結果

図7に K-SVD により設計した辞書と対応する暗号化辞書を示す。図8と図9には、それぞれ人物が含まれる画像と人物が含まれない画像の任意のサンプルについて、原画像と暗号化画像を示した。

表1には基底の数が $L = 1$ と $L = 5$ の場合について、提案法の識別率を示した。識別率は 80% 程度となっている。基底の数の違いは、識別率にほとんど影響を与えていないことがわかる。

図10には基底の数 $L = 1$ の場合の特徴量 (行列形式で表記) と対応する復号画像を示した。図10より、人物を含む画像は含まない画像に対して、特徴量が比較的スパースに表されていることがわかる。スパースな特徴が識別率に寄与していると考えられる。なお復号画像は $\hat{y}_i = Q_p^* \hat{D} \hat{x}_i$ により得ることができる。

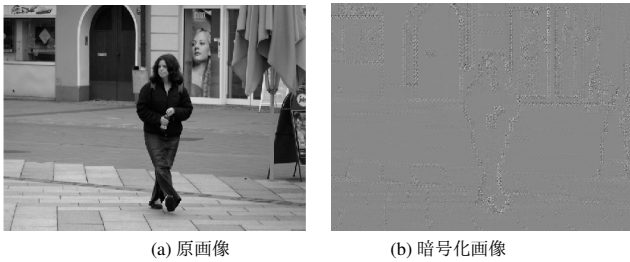


図8 人物が含まれる画像とその暗号化画像の例。

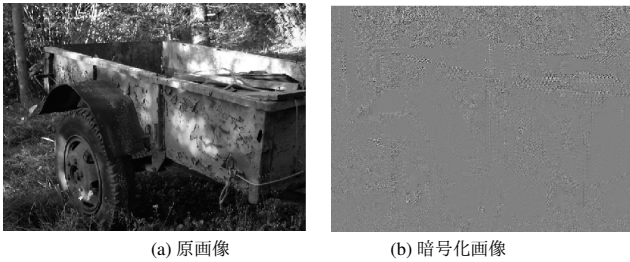


図9 人物が含まれない画像とその暗号化画像の例。

提案法は画像認識システムとして動作するとともに、画像を暗号化した後に圧縮する Encryption-then-Compression (EtC) システム [19] としても動作可能であると言える。

表2には、画像を暗号化しない場合に OMP でスパース係数を求めた際の識別率を示した。提案した暗号化画像に対するクラス分類法は、画像を暗号化しないで処理した場合と同じ識別率結果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、秘匿 OMP 演算を用いた暗号化画像のクラス分類法を提案した。提案法は暗号化画像から特徴となるスパース係数を推定し、そこから得られる特徴量と SVM と組み合わせて用いることでクラス識別を行う。INRIA Person Dataset を対象として、人物を含む画像を識別する課題を実行して、暗号化画像から人物を含む画像が識別可能であることを確認した。

今後は、スパース辞書学習の秘匿演算について検討するとともに、スパースコーディングを用いた暗号化画像の識別性能と復号画像品質の関係について検証する予定である。

文 献

[1] 小林 健人, 稲村勝樹, 金田北洋, 岩村恵市, "プライバシー保護と犯罪防止を両立させる監視カメラシステム," 情報処理学会論文誌 57(1), 172-183, 2016-01-15.

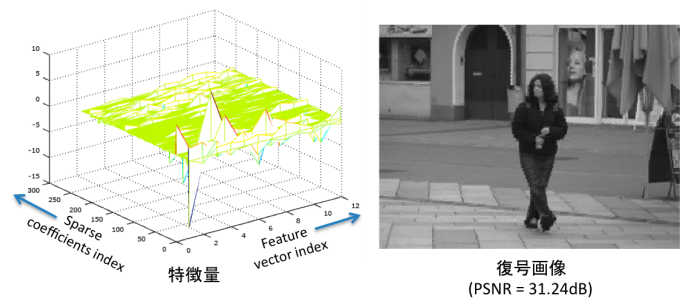
[2] C. T. Huang, L. Huang, Z. Qin, H. Yuan, L. Zhou, V. Varad-harajan, and C-C. J. Kuo, "Survey on securing data storage in the cloud," APSIPA Transactions on Signal and Information Processing, vol. 3, e7, 2014.

[3] 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.

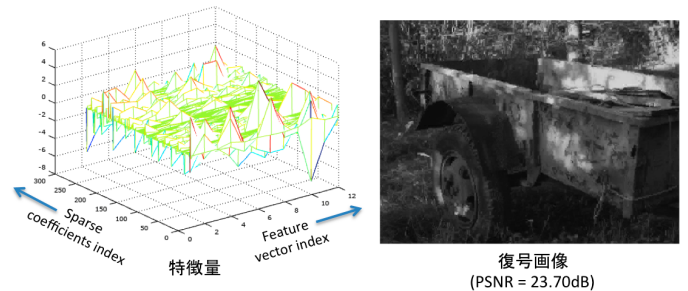
[4] R. L. Lagendijk, Z. Erkin and M. Barni, "Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation," IEEE Signal Processing Magazine, vol. 30, no. 1, pp. 82-105, Jan. 2013.

[5] 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.

[6] 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.



(a) 人物を含む画像



(b) 人物を含まない画像

図10 基底の数 $L = 1$ の場合の特徴量 (行列形式で表記) と対応する復号画像。

7-12, 2018年6月.

[7] Takayuki Nakachi, Hitoshi Kiya, "Practical secure OMP computation and its application to image modeling," IHIP2018, 2018.

[8] Takayuki Nakachi, Hiroyuki Ishihara, Hitoshi Kiya, "Privacy-preserving network BMI decoding of covert spatial attention," IEEE ICSPCS2018, p12, 2018.

[9] 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).

[10] Michael Elad, "Sparse and Redundant Representations: From Theory to Applications in Signal and Image Processing," Springer, 2010.

[11] 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.

[12] K. Egan, S. O. Aase and J. Hakon Husoy: "Method of optimal directions for frame design", ICASSP1999, pp. 2443-2446 (1999).

[13] 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).

[14] 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).

[15] 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.

[16] 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.

[17] 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.

[18] B. K. Natarajan: "Sparse approximate solutions to linear systems", SIAM J. Comput., 24, 2, pp. 227-234, 1995.

[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] "INRIA Person Dataset," <http://pascal.inrialpes.fr/data/human/>.