

# EtC画像を用いた固有顔のプライバシー保護を考慮した計算法

北山 昌希<sup>†</sup> 貴家 仁志<sup>†</sup>

<sup>†</sup> 首都大学東京

〒 191-0065 東京都日野市旭丘 6-6

あらまし 本稿では, EtC (Encryption-then-Compression) 画像を用いた固有顔およびカーネル固有顔による顔認証法を提案する. ここで, EtC 画像とは, JPEG 圧縮可能な暗号化処理が施された画像である. 近年, クラウドサービスを利用し, プロバイダーの提供する計算資源を利用する計算形態が急速に普及している. しかし, プロバイダー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, プライバシーを保護した固有顔およびカーネル固有顔による顔認証法を考察する. 本稿では, EtC 画像が, その中心化された画素ベクトル群においてベクトル間の内積およびユークリッド距離が保存することを示す. さらにその結果から, その暗号化処理が固有顔および代表的なカーネル関数を用いたカーネル固有顔による特徴ベクトル生成に影響を及ぼさないことを示す. 最後に, 固有顔およびカーネル固有顔の特徴ベクトルの視覚化と顔認証実験を行い, 提案法の有効性を確認している.

キーワード 固有顔, カーネル固有顔, Encryption-then-Compression, 暗号化領域, JPEG

## A privacy preserving calculation method of eigenface using EtC images

Masaki KITAYAMA<sup>†</sup> and Hitoshi KIYA<sup>†</sup>

<sup>†</sup> Tokyo Metropolitan University

Asahigaoka 6-6, Hino-shi, Tokyo, 191-0065

**Abstract** In this paper, we propose a face recognition scheme using eigenface and kernel eigenface with EtC (Encryption-then-Compression) images, where EtC images are images encrypted by the method which has been proposed for Encryption-then-Systems with JPEG compression. Recently, cloud computing has been 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. Because of such a situation, this paper considers a privacy-preserving face recognition method using eigenface and kernel eigenface. In this paper, we show inner products and euclidean distances between the centered vectors of pixels in EtC images are preserved, and the encryption steps do not affect feature vectors generated by eigenface and kernel eigenface. To evaluate the proposed method, we visually compare feature vectors generated from EtC images with ones generated from non-encrypted images. Moreover, a face recognition experiment is carried out under the use of a support vector machine algorithm.

**Key words** eigenface, kernel eigenface, Encryption-then-Compression, encrypted domain, JPEG

### 1. ま え が き

近年, 様々な計算分野において, プロバイダーの計算資源を利用するクラウドコンピューティングやエッジコンピューティングが急速に普及してきている. しかしクラウドコンピューティングの利用は, プロバイダー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出, 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 [1].

これらの問題を解決するためのアプローチの一つに, 準同型暗号で計算を行う方法がある [2]~[12]. これらは, 証明可能な高い安全性を有するが, 機械学習法に広く利用されるには至っていない. 単純な統計計算 [5], 暗号化画像からの特徴量の抽出 [7],[8], 深層学習における重みの統合 [10], 限定されたネットワークではあるが暗号化領域でのネットワークの学習などの報告がある [11]. しかし準同型暗号の機械学習への応用では, 損失関数が多項式に限定されること, 特別な計算形式をアルゴリ

ズム毎に準備する必要があることに加え、計算量が膨大になるなどの多くの課題が指摘されている [12].

このような背景から、本稿ではクラウドサービス上での標準的な機械学習アルゴリズムによる画像分類サービスを想定し、プライバシーを保護した EtC(Encryption-then-Compression) 画像を用いた固有顔およびカーネル固有顔による顔認証システムを考察する。本稿における EtC 画像とは、JPEG 圧縮の使用を前提として提案されたブロックベース暗号化処理が施された画像である [13]~[16]. EtC 画像は、JPEG 圧縮された形式で保存可能であり、安全性がすでに評価されている [17]~[19].

固有顔 [20] は顔認証システムで用いられる特徴ベクトル抽出および次元削減の手法であり、顔画像の画素ベクトル群を中心化し、ベクトル空間上の統計的主成分を表す正規直交基底列を求め、その基底列の表す部分空間上に各ベクトルを直交射影するものである。固有顔はその手法の単純さ、処理の軽さ、保持すべきデータ容量の少なさに対して良い認証性能を持つことが知られている。カーネル固有顔 [21] は、固有顔をカーネル法により拡張して非線形な主成分軸への射影を可能としたものであり、より一般化された固有顔として解釈される。

本稿では、教師画像データベースおよびクエリ画像に対して、同一鍵を用いて EtC 変換を施し、固有顔およびカーネル固有顔による顔認証を行うことを考える。この時、中心化された画素ベクトル群においてベクトル間の内積およびユークリッド距離が保存することを示し、またその結果から、その暗号化処理が固有顔および代表的なカーネル関数を用いたカーネル固有顔による特徴ベクトル生成に影響を及ぼさないことを示す。

最後に、固有顔およびカーネル固有顔の特徴ベクトルの視覚化と顔認証実験を行い、提案法の有効性を確認している。

## 2. 準備

### 2.1 固有顔を用いた顔画像認証システム

図 1 に固有顔を用いた顔画像認証システムの概略を示す。\$N\$ 枚の教師画像データベース \$\{L\_n \mid n = 1, 2, \dots, N\}\$ と、それに対応する正解ラベル \$\{y\_n\}\$、クエリ画像 \$Q\$ があり、これら全ての画像のサイズは \$W \times H\$ ピクセルとする。以下では、学習と認証の処理の流れを同時に説明する。

#### A. 教師データおよび新規データの中心化

画像 1 枚の画素数を \$D = W \times H\$ として、\$\{L\_n\}\$ および \$Q\$ から教師画素ベクトル (画素値のベクトル表現)

\$\{x\_n = (x\_{n,1}, x\_{n,2}, \dots, x\_{n,D})^T \mid n = 1, 2, \dots, N\}\$ およびクエリ画素ベクトル \$q = (q\_1, q\_2, \dots, q\_D)^T\$ をそれぞれ生成する。ただし、\$^T\$ はベクトルまたは行列の転置を表す。教師画素ベクトルの平均ベクトル \$m\$ を

$$m = \frac{1}{N} \sum_{n=1}^N x_n, \quad (1)$$

として求める。次に、\$\{x\_n\}\$ および \$q\$ から中心化されたベクトル \$\{\hat{x}\_n = (\hat{x}\_{n,1}, \hat{x}\_{n,2}, \dots, \hat{x}\_{n,D})^T \mid n = 1, 2, \dots, N\}\$,

\$\hat{q} = (\hat{q}\_1, \hat{q}\_2, \dots, \hat{q}\_D)^T\$ をそれぞれ

$$\hat{x}_n = x_n - m, \quad (2)$$

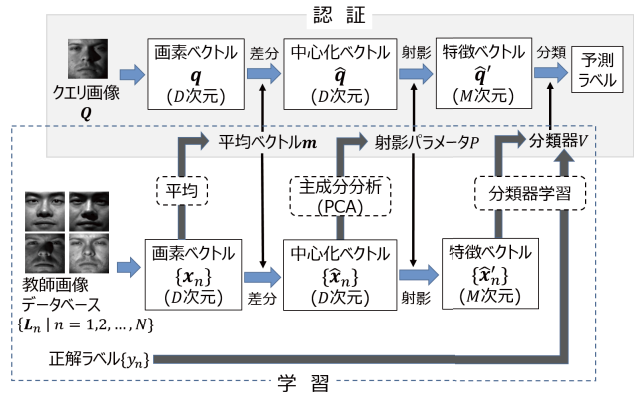


図 1 固有顔を用いた顔画像認証システム。

$$\hat{q} = q - m, \quad (3)$$

のように求める。ベクトル集合の変換 \$\{x\_n, q\} \rightarrow \{\hat{x}\_n, \hat{q}\}\$ はベクトル空間上の平行移動に相当し、ベクトル間のパターンとしての相対的な情報は保持する。

#### B. データの主成分分析と射影・分類

\$\{\hat{x}\_n\}\$ を用いて主成分分析 (PCA) を行い、\$D\$ 次元空間上の \$M (< D)\$ 個の正規直交基底列 \$U = [u\_1, u\_2, \dots, u\_M]\$ を得る。ここで、\$u\_1\$ は \$\{\hat{x}\_n\}\$ の分散が最大となるような基底であり、\$u\_m\$ は \$u\_1, u\_2, \dots, u\_{m-1}\$ に直交する制約化で分散が \$m\$ 位となる基底である。\$U = [u\_1, u\_2, \dots, u\_M]\$ は、以下に示す行列 \$S\$ についての固有方程式を解き、固有値 \$\lambda\_i\$ の大きい順 \$\lambda\_1, \lambda\_2, \dots, \lambda\_M\$ に対応する固有ベクトル \$u\_i\$ の列 \$u\_1, u\_2, \dots, u\_M\$ として求められる。

$$S u_i = \lambda_i u_i \quad (4)$$

ただし \$S\$ は \$\{\hat{x}\_n\}\$ の共分散行列であり、

$$S = \frac{1}{N} \sum_{n=1}^N \hat{x}_n \hat{x}_n^T \quad (5)$$

として与えられる。

得られた \$U\$ を用いて、\$\{\hat{x}\_n\}\$ および \$\hat{q}\$ をそれぞれ次式により \$M\$ 次元の部分空間へと直交射影し、\$M\$ 次元特徴ベクトル \$\{\hat{x}'\_n = (\hat{x}'\_{n,1}, \hat{x}'\_{n,2}, \dots, \hat{x}'\_{n,M})^T \mid n = 1, 2, \dots, N\}\$ および \$\hat{q}' = (\hat{q}'\_1, \hat{q}'\_2, \dots, \hat{q}'\_M)^T\$ を得る。

$$\hat{x}'_{n,m} = u_m^T \hat{x}_n, \quad \hat{q}'_m = u_m^T \hat{q}, \quad m = 1, 2, \dots, M \quad (6)$$

このとき、図 1 の射影パラメータは \$P = U\$ である。

得られた \$\{\hat{x}'\_n\}\$ と正解ラベル \$\{y\_n\}\$ を用いてサポートベクターマシン等の分類器 \$V\$ を学習し、\$\hat{q}'\$ を分類する。

### 2.2 カーネル固有顔

カーネル固有顔 [21] は、カーネル PCA [22] を用いることにより射影 \$\{\hat{x}\_n, \hat{q}\} \rightarrow \{\hat{x}'\_n, \hat{q}'\}\$ を非線形な関係で実現する固有顔である。カーネル PCA を行うためには、非線形射影関数 \$\phi(\cdot)\$ によって \$\{\hat{x}\_n\}\$ および \$\hat{q}\$ を高次元空間に射影した \$\{\phi(\hat{x}\_n)\}\$, \$\phi(\hat{q})\$ に対して、カーネル PCA を実行する必要がある。しかし、低次元ベクトル \$\{\hat{x}\_n\}\$, \$\hat{q}\$ を直接 \$\phi(\cdot)\$ で高次元に射影して計算

することは一般的に困難である。

そこで、カーネル PCA では、カーネル法を用いることにより、低次元ベクトルの計算のみで高次元ベクトル空間の PCA を表現する。ここで、カーネル法とは、ある低次元ベクトルの組  $\mathbf{v}_1, \mathbf{v}_2 \in \mathbb{R}^{N'}$  に対して、高次元に射影されたベクトル同士の内積  $\phi(\mathbf{v}_1)^\top \phi(\mathbf{v}_2)$  を、カーネル関数  $k(\mathbf{v}_1, \mathbf{v}_2)$  を用いて低次元ベクトルの計算で求めるものである。カーネル関数には例えば以下のような種類がある。

$$\text{線形カーネル } k_i(\mathbf{v}_1, \mathbf{v}_2) = \mathbf{v}_1^\top \mathbf{v}_2 \quad (7)$$

$$\text{多項式カーネル } k_g(\mathbf{v}_1, \mathbf{v}_2) = (\mathbf{v}_1^\top \mathbf{v}_2 + p_r)^{p_d} \quad (8)$$

$$\text{ガウスカーネル } k_p(\mathbf{v}_1, \mathbf{v}_2) = \exp(-p_\gamma \|\mathbf{v}_1 - \mathbf{v}_2\|^2) \quad (9)$$

ただし、 $p_r, p_d, p_\gamma$  はハイパーパラメータである。式 (7) は、 $\mathbf{v}_1, \mathbf{v}_2$  を  $\phi(\cdot)$  で高次元に射影しなかった場合の、通常の内積に対応する。

今、中心化ベクトル  $\{\hat{\mathbf{x}}_n\}$ 、 $\hat{\mathbf{q}}$  は  $\phi(\cdot)$  によって高次元ベクトル  $\{\phi(\hat{\mathbf{x}}_n)\}$ 、 $\phi(\hat{\mathbf{q}})$  に射影されているものとする。以下に、これらの高次元ベクトルを通常の PCA の式 (式 (4)~(6)) に当てはめて変形することによって、カーネル PCA を導出する過程を簡単に示す。

まず、式 (5) を式 (4) に代入すると、

$$\frac{1}{N} \sum_{n=1}^N \phi(\hat{\mathbf{x}}_n) \{\phi(\hat{\mathbf{x}}_n)^\top \mathbf{u}_i\} = \lambda_i \mathbf{u}_i \quad (10)$$

よって、 $\mathbf{u}_i$  は  $\phi(\hat{\mathbf{x}}_n)$  の線形結合として与えられ、

$$\mathbf{u}_i = \sum_{n=1}^N a_{i,n} \phi(\hat{\mathbf{x}}_n) \quad (11)$$

として表される。式 (11) を式 (10) に代入すると、

$$\begin{aligned} \frac{1}{N} \sum_{n=1}^N \phi(\hat{\mathbf{x}}_n) \phi(\hat{\mathbf{x}}_n)^\top \sum_{k=1}^N a_{i,k} \phi(\hat{\mathbf{x}}_k) \\ = \lambda_i \sum_{n=1}^N a_{i,n} \phi(\hat{\mathbf{x}}_n) \end{aligned} \quad (12)$$

両辺に  $\phi(\hat{\mathbf{x}}_l)^\top$  を左から掛けて、

$$\begin{aligned} \frac{1}{N} \sum_{n=1}^N \phi(\hat{\mathbf{x}}_l)^\top \phi(\hat{\mathbf{x}}_n) \sum_{k=1}^N a_{i,k} \phi(\hat{\mathbf{x}}_n)^\top \phi(\hat{\mathbf{x}}_k) \\ = \lambda_i \sum_{n=1}^N a_{i,n} \phi(\hat{\mathbf{x}}_l)^\top \phi(\hat{\mathbf{x}}_n) \end{aligned} \quad (13)$$

を得る。ここで、行列  $\mathbf{K} \in \mathbb{R}^{N \times N}$  を以下のように定義する。

$$\mathbf{K} = \begin{pmatrix} \phi(\hat{\mathbf{x}}_1)^\top \phi(\hat{\mathbf{x}}_1) & \phi(\hat{\mathbf{x}}_1)^\top \phi(\hat{\mathbf{x}}_2) & \dots & \phi(\hat{\mathbf{x}}_1)^\top \phi(\hat{\mathbf{x}}_N) \\ \phi(\hat{\mathbf{x}}_2)^\top \phi(\hat{\mathbf{x}}_1) & \phi(\hat{\mathbf{x}}_2)^\top \phi(\hat{\mathbf{x}}_2) & \dots & \phi(\hat{\mathbf{x}}_2)^\top \phi(\hat{\mathbf{x}}_N) \\ \vdots & \vdots & \ddots & \vdots \\ \phi(\hat{\mathbf{x}}_N)^\top \phi(\hat{\mathbf{x}}_1) & \dots & \dots & \phi(\hat{\mathbf{x}}_N)^\top \phi(\hat{\mathbf{x}}_N) \end{pmatrix} \quad (14)$$

式 (13) は、式 (14) および  $\mathbf{a}_i = (a_{i,1}, a_{i,2}, \dots, a_{i,N})^\top$  を用いて、以下のように表される。

$$\mathbf{K}^2 \mathbf{a}_i = \lambda_i N \mathbf{K} \mathbf{a}_i \quad (15)$$

この式の両辺に左から  $\mathbf{K}^{-1}$  を掛けて

$$\mathbf{K} \mathbf{a}_i = \lambda_i N \mathbf{a}_i \quad (16)$$

を得る。上式を行列  $\mathbf{K}$  についての固有値問題として解き、 $M$  個の固有値  $\lambda_i N$  の大きい順  $\lambda_1 N, \lambda_2 N, \dots, \lambda_M N$  に対応する固有ベクトル  $\mathbf{a}_i$  の列  $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_M$  を得る。このとき、 $\{\phi(\hat{\mathbf{x}}_n)\}$  および  $\phi(\hat{\mathbf{q}})$  の、それぞれ  $\{\hat{\mathbf{x}}'_n\}$  および  $\hat{\mathbf{q}}'$  への射影は、式 (11) を式 (6) に代入して、

$$\begin{aligned} \hat{\mathbf{x}}'_{n,m} &= \mathbf{u}_m^\top \phi(\hat{\mathbf{x}}_n) = \sum_{l=1}^N a_{m,l} \phi(\hat{\mathbf{x}}_l)^\top \phi(\hat{\mathbf{x}}_n) , \\ \hat{\mathbf{q}}'_m &= \mathbf{u}_m^\top \phi(\hat{\mathbf{q}}) = \sum_{l=1}^N a_{m,l} \phi(\hat{\mathbf{x}}_l)^\top \phi(\hat{\mathbf{q}}) , \end{aligned} \quad (17)$$

$$m = 1, 2, \dots, M$$

として得られる。

ここで、 $\{\hat{\mathbf{x}}_n, \hat{\mathbf{q}}\}$  に含まれる任意の 2 つのベクトルを  $\hat{\mathbf{x}}_e, \hat{\mathbf{x}}_{e'}$  とすると、式 (14)(16)(17) より、高次元空間における PCA の計算は全て、高次元ベクトル同士の内積計算  $\phi(\hat{\mathbf{x}}_e)^\top \phi(\hat{\mathbf{x}}_{e'})$  のみによって与えられる。これは、カーネル法により、低次元ベクトル  $\hat{\mathbf{x}}_e, \hat{\mathbf{x}}_{e'}$  を用いて、 $k(\hat{\mathbf{x}}_e, \hat{\mathbf{x}}_{e'}) = \phi(\hat{\mathbf{x}}_e)^\top \phi(\hat{\mathbf{x}}_{e'})$  として計算できることを意味している。式 (14)(17) に現れる高次元ベクトル同士の内積計算部を、これらのカーネル関数に置き換える。例えば、 $\mathbf{K}$  の  $(i, j)$  要素は  $\phi(\hat{\mathbf{x}}_i)^\top \phi(\hat{\mathbf{x}}_j) = k(\hat{\mathbf{x}}_i, \hat{\mathbf{x}}_j)$  と置き換えられる。これにより、高次元に射影された  $\{\phi(\hat{\mathbf{x}}_n)\}, \phi(\hat{\mathbf{q}})$  の PCA アルゴリズムは、カーネル関数  $k(\cdot, \cdot)$  による低次元ベクトル  $\{\hat{\mathbf{x}}_n\}, \hat{\mathbf{q}}$  の計算で実現できることが示され、カーネル PCA の導出が完了した。

ここで、通常 PCA は、式 (7) に表される線形カーネル関数を用いたカーネル PCA と等価であることに注意する。すなわち、固有顔はカーネル固有顔の特殊な例であると解釈される。カーネル固有顔を図 1 に組み込んだ場合、射影パラメータは  $P \in \{\mathbf{A}, \hat{\mathbf{x}}_n\}$  となる。ただし、 $\mathbf{A} = [\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_M]$  である。

### 3. 提案法

本稿では、グレースケール顔画像に対してブロックベース暗号化を施し、教師画像およびクエリ画像に対して同一鍵による暗号化が施された場合、暗号化が固有顔およびカーネル固有顔による特徴ベクトル生成に影響を与えないことを理論的に示す。次に、その理論に基づき、暗号化画像を用いた固有顔およびカーネル固有顔による顔画像認証法を提案する。

#### 3.1 画像のブロックベース暗号化 (EtC)

静止画像の暗号化法として、画像をブロックに分割して処理を行うブロックベース暗号化が研究されている [13]~[16]。この暗号化法は、暗号化画像を JPEG 圧縮できるという特徴を有す。この暗号化が施された画像を EtC (Encryption then Compression) 画像と呼ぶ。図 2 に白黒画像からの EtC 画像生成フローを示す。

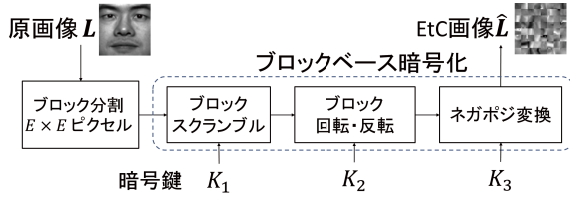


図2 画像のブロックベース暗号化.

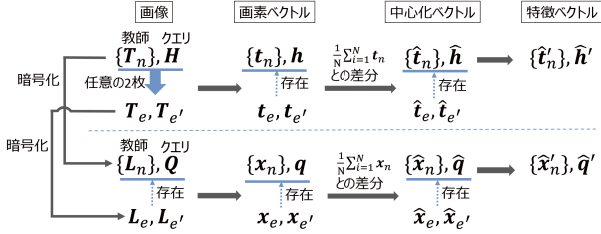


図3 原画像  $\{T_n\}, H$  および EtC 画像  $\{L_n\}, Q$  の、顔認証システム (図1) における特徴ベクトル取得フロー.

### 1) ブロックスクランブル

まず、サイズ  $W \times H$  の画像を一定サイズ  $E \times E$  のブロックに分割する。ブロックスクランブルは、このブロックを鍵  $K_1$  を用いてランダムに置換する操作である。

### 2) ブロック回転・反転

ブロックスクランブルの後に、鍵  $K_2$  各ブロックに対しランダムに回転および反転変換を施す。ブロックの回転変換は、各ブロックを  $0^\circ, 90^\circ, 180^\circ, 270^\circ$  の4つのいずれかの角度だけランダムに回転させる操作である。ブロックの反転変換は、ブロック内の画素を水平または垂直方向にランダムで反転させる方法である。反転しない、水平方向のみ反転、垂直方向のみ反転、水平・垂直両方向の反転の4つのパターンがある。ただし、水平・垂直両方向の反転変換は  $180^\circ$  の回転変換と等しい。よって、回転・反転変換を合わせた変換の総パターンは12通りである。

### 3) ネガポジ変換

ネガポジ変換は、ランダムにブロックを選択して、選択されたブロック内の全ての画素値を反転させる方法である。ブロック  $i$  内の画素値を  $p (0 \leq p \leq 255)$ 、鍵  $K_3$  により生成された2値の乱数を  $r(i)$  としたとき、次式によりネガポジ変換が実行される。

$$\begin{cases} p' = p & (r(i) = 0) \\ p' = 255 - p & (r(i) = 1) \end{cases} \quad (18)$$

ただし  $r(i)$  の発生確率は  $p(r(i)) = 0.5$  である。ネガポジ変換を行うことにより、画像の濃淡やヒストグラムが変化し、より原画像の特定が困難になる。

## 3.2 EtC 画像の固有顔・カーネル固有顔

図3は、EtC画像からカーネル固有顔により特徴ベクトルを取得する手順である。教師画像データベース  $\{T_n\}$ 、クエリ画像  $H$ 、それらを暗号化したものをそれぞれ  $\{L_n\}$ 、 $Q$  と表す。また、同図では、 $\{T_n, H\}$  の中から任意に選択された2枚の画像を  $T_e, T_{e'}$ 、それらを暗号化した画像を  $L_e, L_{e'}$  として記

述している。本稿では、 $T_e, T_{e'}, L_e, L_{e'}$  それぞれから生成される特徴ベクトル  $\hat{t}'_e, \hat{t}'_{e'}, \hat{x}'_e, \hat{x}'_{e'}$  に対して、カーネル関数  $k(\hat{t}_e, \hat{t}_{e'})$  と  $k(\hat{x}_e, \hat{x}_{e'})$  が

$$k(\hat{t}_e, \hat{t}_{e'}) = k(\hat{x}_e, \hat{x}_{e'}) \quad (19)$$

として一致することを証明する。

カーネル固有顔の計算式(式(14)(16)(17))より、式(19)は、特徴ベクトル  $\{\hat{t}'_n\}, \hat{h}', \{\hat{x}'_n\}$  および  $\hat{q}'$  が、

$$\hat{t}'_n = \hat{x}'_n, \quad n = 1, 2, \dots, N \quad (20)$$

$$\hat{h}' = \hat{q}' \quad (21)$$

を満たすための十分条件である。

3種類のカーネル関数(式(7)(8)(9))の使用の下で、式(19)を満たすための条件は、次のA, Bである。

A. 内積の保存:  $\hat{t}_e^T \hat{t}_{e'} = \hat{x}_e^T \hat{x}_{e'}$

B. ユークリッド距離の保存:  $\|\hat{t}_e - \hat{t}_{e'}\| = \|\hat{x}_e - \hat{x}_{e'}\|$

EtC画像が条件A, Bを満たすことを、図2の暗号化手順を2つのステップに分けて示す。

#### Step1. ブロックスクランブル・ブロックの回転・反転

ブロックスクランブル、ブロックの回転・反転は、いずれも画素ベクトルの要素の入れ替えに相当する。式(1)(2)(3)より、平均ベクトルと中心化ベクトルそれぞれにおいても同様にベクトル要素の入れ替えに相当する。よって、暗号化の鍵が共通であれば、条件A, Bが満たされることは自明である。

#### Step2. ネガポジ変換

$t_e = (t_{e,1}, t_{e,2}, \dots, t_{e,D})^T$  にネガポジ変換を適用し  $x_e = (x_{e,1}, x_{e,2}, \dots, x_{e,D})^T$  を生成することを考える。このとき、式(18)が適用された要素(ネガティブ要素)の個数を  $D' (< D)$  として、その要素を  $x_{e,d'_i}, i = 1, 2, \dots, D'$  として表す。また、式(18)が適用されなかった要素(非ネガティブ要素)を  $x_{e,d_j}, j = 1, 2, \dots, D - D'$  として表す。このとき、 $x_{e,d'_i}, x_{e,d_j}$  はそれぞれ、

$$x_{e,d'_i} = 255 - t_{e,d'_i}, \quad x_{e,d_j} = t_{e,d_j} \quad (22)$$

として与えられる。よって  $\hat{x}_e = (\hat{x}_{e,1}, \hat{x}_{e,2}, \dots, \hat{x}_{e,D})^T$  は、

$$\begin{aligned} \hat{x}_{e,d'_i} &= x_{e,d'_i} - \frac{1}{N} \sum_{n=1}^N x_{n,d'_i} \\ &= (255 - t_{e,d'_i}) - \frac{1}{N} \sum_{n=1}^N (255 - t_{n,d'_i}) \\ &= 255 - 255 - (t_{e,d'_i} - \frac{1}{N} \sum_{n=1}^N t_{n,d'_i}) = -\hat{t}_{e,d'_i}, \end{aligned} \quad (23)$$

$$\begin{aligned} \hat{x}_{e,d_j} &= x_{e,d_j} - \frac{1}{N} \sum_{n=1}^N x_{n,d_j} \\ &= t_{e,d_j} - \frac{1}{N} \sum_{n=1}^N t_{n,d_j} = \hat{t}_{e,d_j} \end{aligned} \quad (24)$$

である。よって、条件 A は、

$$\begin{aligned}\hat{\mathbf{x}}_e^T \hat{\mathbf{x}}_{e'} &= \sum_{i=1}^{D'} \hat{x}_{e,d'_i} \hat{x}_{e',d'_i} + \sum_{j=1}^{D-D'} \hat{x}_{e,d_j} \hat{x}_{e',d_j} \\ &= \sum_{i=1}^{D'} (-\hat{t}_{e,d'_i})(-\hat{t}_{e',d'_i}) + \sum_{j=1}^{D-D'} \hat{t}_{e,d_j} \hat{t}_{e',d_j} \\ &= \hat{\mathbf{t}}_e^T \hat{\mathbf{t}}_{e'}\end{aligned}\quad (25)$$

として成り立つことが示される。条件 B についても、

$$\begin{aligned}\|\hat{\mathbf{x}}_e - \hat{\mathbf{x}}_{e'}\| &= \sqrt{\sum_{i=1}^{D'} (\hat{x}_{e,d'_i} - \hat{x}_{e',d'_i})^2 + \sum_{j=1}^{D-D'} (\hat{x}_{e,d_j} - \hat{x}_{e',d_j})^2} \\ &= \sqrt{\sum_{i=1}^{D'} (\hat{t}_{e,d'_i} - \hat{t}_{e',d'_i})^2 + \sum_{j=1}^{D-D'} (\hat{t}_{e,d_j} - \hat{t}_{e',d_j})^2} \\ &= \|\hat{\mathbf{t}}_e - \hat{\mathbf{t}}_{e'}\|\end{aligned}\quad (26)$$

として成り立つことが示される。

以上の議論により、式 (7)(8)(9) のカーネル関数の仮定の下で、EtC 画像は、 $k(\hat{\mathbf{x}}_e, \hat{\mathbf{x}}_{e'}) = k(\hat{\mathbf{t}}_e, \hat{\mathbf{t}}_{e'})$  の成立を保証する。従って、原画像を入力とした認証システムの特徴ベクトルと、EtC 画像を入力とした特徴ベクトルが一致する。

## 4. 実験

提案法の妥当性を評価するため、顔画像データベース Extended Yale Face Database B [23] を用いて実験を行った。このデータベースは、38 人の様々な照明条件で撮影された顔画像が 64 枚ずつ、計 2432 枚で構成されている。本実験ではすべて 64×64 ピクセルに正規化して使用した。また、各被験者に対する 64 枚の顔画像を、教師画像に 50 枚、クエリ画像に 14 枚に分けて実験を行った。暗号化のブロックサイズは 8×8 ピクセルとした。特徴ベクトルは、固有顔、多項式カーネル (式 (8)) 固有顔、ガウスカーネル (式 (9)) 固有顔の 3 種類を用いた。

### 実験 A

得られた特徴ベクトルの第 1 成分、第 2 成分のプロットによる可視化を行った。図 4 に、教師特徴ベクトルおよびクエリ特徴ベクトルの第 1 成分、第 2 成分のプロットを示す。原画像から得られた特徴ベクトルが、各条件下で EtC 画像から得られたものと一致することが視覚的に確認できる。

### 実験 B

次元  $M \in \{40, 60, 80, 100, 120\}$  に射影して得られた特徴ベクトルを用いた線形 SVM による分類実験を行った。図 5 に、線形 SVM による分類実験の結果を示す。分類性能評価には等価エラー率 (Equal Error Rate: EER) を用いた。これは、本人棄却率 (False Reject Rate: FRR) と他人受理率 (False Accept Rate: FAR) の値が等しくなる時の値であり、分類器が新規データを本人と分類する分類スコアの閾値を操作することにより得られる。EER が低いほど分類器が良い分類性能を持つことを示す。図 5 より、固有顔、多項式カーネル固有顔、ガウスカーネル固有顔それぞれについて、特徴ベクトルの次元に関わらず

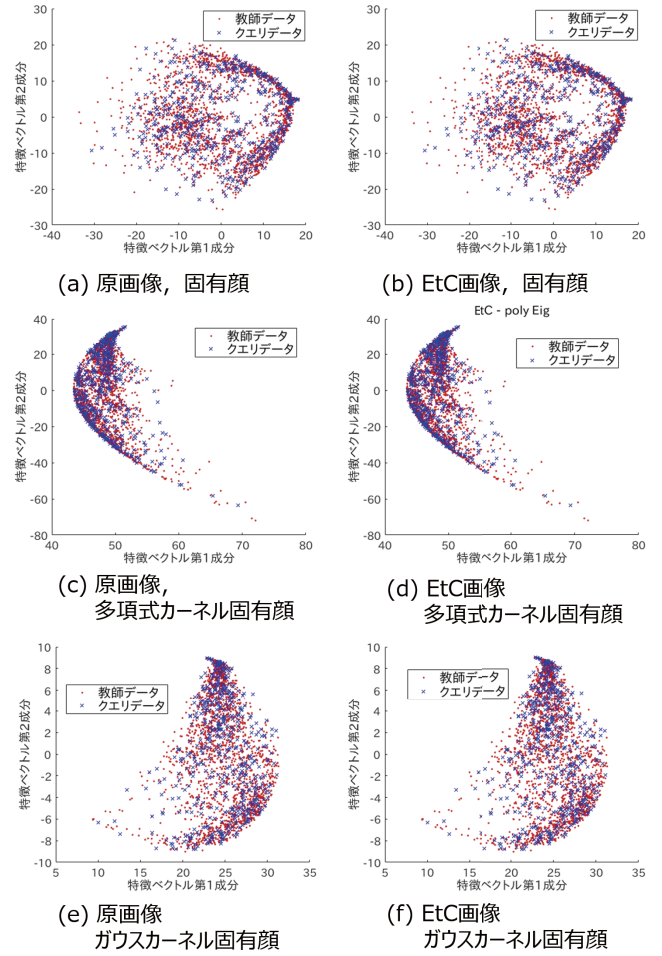


図 4 教師データとクエリデータから得られた特徴ベクトルの第 1 成分、第 2 成分のプロット。

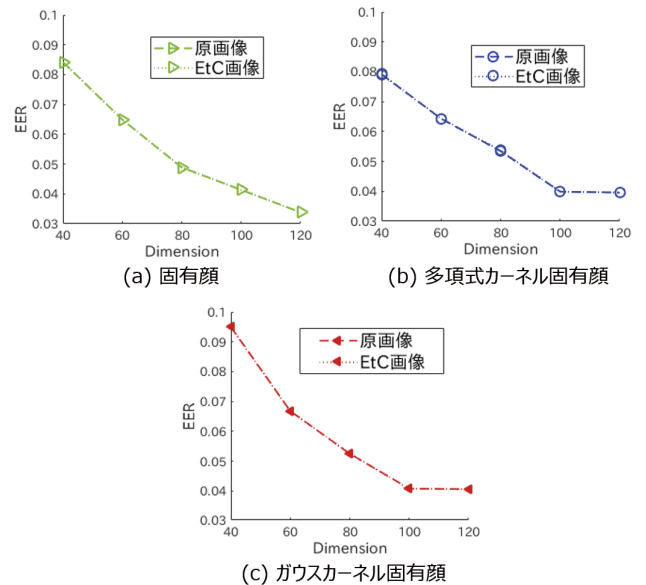


図 5 線形 SVM による分類実験。

原画像と EtC 画像で等しい EER を示していることが分かる。以上の実験より提案法の妥当性が示された。

## 5. ま と め

本稿では、ブロックベース暗号化が施された EtC 画像を、固有顔およびカーネル固有顔による顔認証システムに適用することを提案した。原画像、EtC 画像それぞれの中心化ベクトルは内積とユークリッド距離が保存することを示し、固有顔、多項式カーネル固有顔、ガウスカーネル固有顔による特徴ベクトル生成に影響がないことを理論的に証明した。最後に、顔画像認証実験により理論の妥当性を評価した。

謝辞 本研究の一部は、首都大学東京戦略的研究プロジェクト戦略的研究支援枠「ソーシャルビッグデータの分析・応用のための学術基盤の研究」、及び JSPS 科研費 JP17H03267(基盤研究 (B) 一般) の助成を受けたものである。

### 文 献

- [1] C.-T. Huang, L. Huang, Z. Qin, H. Yuan, L. Zhou, V. Varadharajan, and C.-C.J. Kuo, "Survey on securing data storage in the cloud," *APSIPA Transactions on Signal and Information Processing*, vol.3, no.e7, pp.1–17, 2014.
- [2] M. Barni, G. Droandi, and R. Lazzeretti, "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, 2015.
- [3] 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, 2013.
- [4] R. Lazzeretti and M. Barni, "Private computing with garbled circuits [applications corner]," *IEEE Signal Processing Magazine*, vol.30, no.2, pp.123–127, 2013.
- [5] W. Lu, S. Kawasaki, and J. Sakuma, "Using fully homomorphic encryption for statistical analysis of categorical, ordinal and numerical data.," *IACR Cryptology ePrint Archive*, vol.2016, p.1163, 2016.
- [6] Y. Aono, T. Hayashi, L.T. Phong, and L. Wang, "Privacy-preserving logistic regression with distributed data sources via homomorphic encryption," *IEICE TRANSACTIONS on Information and Systems*, vol.99, no.8, pp.2079–2089, 2016.
- [7] H. Yang, Y. Huang, Y. Yu, M. Yao, and X. Zhang, "Privacy-preserving extraction of hog features based on integer vector homomorphic encryption," *International Conference on Information Security Practice and Experience-Springer*, pp.102–117 2017.
- [8] Q. Wang, J. Wang, S. Hu, Q. Zou, and K. Ren, "Sechog: Privacy-preserving outsourcing computation of histogram of oriented gradients in the cloud," *Proceedings of the 11th ACM on Asia Conference on Computer and Communications SecurityACM*, pp.257–268 2016.
- [9] R. Shokri and V. Shmatikov, "Privacy-preserving deep learning," *Proceedings of the 22nd ACM SIGSAC conference on computer and communications securityACM*, pp.1310–1321 2015.
- [10] Y. Aono, T. Hayashi, L. Wang, S. Moriai, et al., "Privacy-preserving deep learning via additively homomorphic encryption," *IEEE Transactions on Information Forensics and Security*, vol.13, no.5, pp.1333–1345, 2018.
- [11] R. Gilad-Bachrach, N. Dowlin, K. Laine, K. Lauter, M. Naehrig, and J. Wernsing, "Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy," *International Conference on Machine Learning*, pp.201–210, 2016.
- [12] Y. Wang, J. Lin, and Z. Wang, "An efficient convolution core architecture for privacy-preserving deep learning," *Circuits and Systems (ISCAS)*, 2018 IEEE International Symposium onIEEE, pp.1–5 2018.
- [13] O. Watanabe, A. Uchida, T. Fukuhara, and H. Kiya, "An encryption-then-compression system for jpeg 2000 standard," *Acoustics, Speech and Signal Processing (ICASSP)*, 2015 IEEE International Conference onIEEE, pp.1226–1230 2015.
- [14] K. Kurihara, S. Shiota, and H. Kiya, "An encryption-then-compression system for jpeg standard," *Picture Coding Symposium (PCS)*, 2015IEEE, pp.119–123 2015.
- [15] K. Kurihara, M. Kikuchi, S. Imaizumi, S. Shiota, and H. Kiya, "An encryption-then-compression system for jpeg/motion jpeg standard," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol.98, no.11, pp.2238–2245, 2015.
- [16] K. Kurihara, S. Imaizumi, S. Shiota, and H. Kiya, "An encryption-then-compression system for lossless image compression standards," *IEICE transactions on information and systems*, vol.100, no.1, pp.52–56, 2017.
- [17] T. Chuman, K. Kurihara, and H. Kiya, "On the security of block scrambling-based etc systems against jigsaw puzzle solver attacks," *Acoustics, Speech and Signal Processing (ICASSP)*, 2017 IEEE International Conference onIEEE, pp.2157–2161 2017.
- [18] T. Chuman, K. Kurihara, and H. Kiya, "On the security of block scrambling-based etc systems against extended jigsaw puzzle solver attacks," *IEICE TRANSACTIONS on Information and Systems*, vol.101, no.1, pp.37–44, 2018.
- [19] T. Chuman, K. Kurihara, and H. Kiya, "Security evaluation for block scrambling-based etc systems against extended jigsaw puzzle solver attacks," *Multimedia and Expo (ICME)*, 2017 IEEE International Conference on IEEE, pp.229–234, 2017.
- [20] J. Zhang, Y. Yan, and M. Lades, "Face recognition: eigenface, elastic matching, and neural nets," *Proceedings of the IEEE*, vol.85, no.9, pp.1423–1435, 1997.
- [21] M.-H. Yang, N. Ahuja, and D. Kriegman, "Face recognition using kernel eigenfaces," *Image processing, 2000. proceedings. 2000 international conference on*, vol.1IEEE, pp.37–40 2000.
- [22] B. Schölkopf, A. Smola, and K.-R. Müller, "Kernel principal component analysis," *International Conference on Artificial Neural NetworksSpringer*, pp.583–588 1997.
- [23] A.S. Georghiadis, P.N. Belhumeur, and D.J. Kriegman, "From few to many: Illumination cone models for face recognition under variable lighting and pose," *IEEE transactions on pattern analysis and machine intelligence*, vol.23, no.6, pp.643–660, 2001.