一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
LOIS2018-11,IE2018-31,EMM2018-50 (2018-09)

次元削減を考慮した暗号化領域でのSVM学習法

河村　綾菜†　　前川　貴大†　　木下　裕磨†　　貴家　仁志†

† 首都大学東京大学院　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: †{kawamura-ayana,maekawa-takahiro,kinoshita-yuma}@ed.tmu.ac.jp, ††kiya@tmu.ac.jp

あらまし　本稿では，次元削減されたEtC画像を用いたサポートベクターマシン (SVM) 学習法を提案し，その性能を評価する．ここで，EtC(Encryption-then-Compression) 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SVM学習法を考察する．EtC画像の生成は，データに対する正規化処理の下で，ユニタリ性を持つ変換行列処理に帰着すること，またその結果，代表的なカーネル関数を使用した場合においても，その暗号化処理がSVMの性能に影響を及ぼさないことを示す．加えて，暗号化時に使用されたブロックサイズを考慮することによって，EtC画像から直接次元削減する方法を提案する．提案法では，非暗号化画像から同様に次元削減した場合のSVM計算結果と一致する結果を得ることができる．最後にSVMの学習法の一例として顔認証実験を行い，提案法の有効性を実験的にも確認している．

キーワード　SVM，Encryption-then-Compression，暗号化領域，JPEG

SVM Computing Considering Dimension Reduction in the Encrypted Domain

Ayana KAWAMURA†, Takahiro MAEKAWA†, Yuma KINOSHITA†, and Hitoshi KIYA†

† Faculity of System Design, Tokyo Metropolitan University　Asahigaoka 6–6, Hino-shi, Tokyo, 191–0065
E-mail: †{kawamura-ayana,maekawa-takahiro,kinoshita-yuma}@ed.tmu.ac.jp, ††kiya@tmu.ac.jp

Abstract　In this paper, we propose a SVM computing scheme with EtC images, and evaluate the effectiveness of the proposed scheme, where EtC images are images encrypted by the method, which has been proposed for Encryption-then-Systems with JPEG compression. Recently, 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 accidents. Because of such a situation, this paper considers privacy-preserving SVM computing. It is shown that generating EtC images is reduced to a generation scheme using an unitary transform matrix under the use of z-score normalization of the data, so it does not effect the accuracy of SVM computing, even when most of kernel fuctions are used. In addition, we propose a scheme for reducing the number of dimensions from EtC images directly by considering the block size used for encryption. The proposed scheme allows us to obtain the same results as those computed from unencrypted images with redued dimensions. Some face recognition experiments are carried out as a SVM classification scheme to experimentally confirm the effectiveness of the proposed scheme.

Key words　SVM，Encryption-then-Compression，encrypted domain，JPEG

1. ま え が き

近年，様々な分野において，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 [1]．今後の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をいかに解決するかが重要な課題となって いる．このような背景から，本稿では，プライバシーを考慮したサポートベクターマシン (SVM)

の学習法を考察する．

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，いわゆる秘匿計算が盛んに研究されている [2–6]．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，十分な普及には至っていない．さらに，秘匿計算では，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．秘匿計算とは独立に，エンドユーザーのプライバシーやデータの秘匿性を考慮した相関計算やデータ圧縮法が研究されている [7–9]．また SVM の計算に対しても、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可能で，かつユーザーのプライバシーの保護を考慮した SVM 学習法が検討されている [10]．その先行研究では，画像などから抽出されるテンプレート (特徴量) のテンプレートからランダムユニタリ行列を用いて保護テンプレートを生成する．この手法は，キャンセラブルバイオメトリックス法の一手法として研究されたものであるが [11, 12]，この方法が持つユニタリ性が SVM 学習を可能とする重要な性質であることが指摘された [13]．

本稿では，エンドユーザーのプライバシーやデータの秘匿性を考慮した SVM 計算が，EtC 画像を用いて実現できることを示す．本稿で対象とする EtC 画像とは，JPEG 圧縮の使用を前提とした EtC(Encryption-then-Compression) システムのために提案された暗号化処理が施された画像である．EtC 画像は，データ圧縮された形式で保存可能であり，かつ総当たり攻撃やジグソーパズル解放攻撃などに対して安全性がすでに評価されている [14, 15]．本稿では，EtC 画像生成に使用されるブロックベース暗号化法が，z-score 正規化処理を施したデータの下で，ユニタリ変換処理として表現され，先のユニタリ変換に基づく SVM 計算法と同様の性質を持つことが示される．このことは，SVM 計算において，代表的なカーネル関数を使用した場合においても，暗号化法が，SVM の認識性能を劣化させないことを意味する．また，本稿では EtC 画像のブロックサイズを考慮した次元削減法を提案する．EtC 画像から直接次元削減を行うことによって，原画像から同様に次元削減した場合の SVM の計算結果と一致する．最後に SVM の学習法の一例として顔認証実験を行い，提案法の有効性を評価する．

2. 準　　備

2.1 サポートベクターマシン

サポートベクターマシン (SVM) とは，機械学習の一つであり，非線形分類識別器として広く用いられている．SVM では，入力特徴ベクトル $\boldsymbol{x}$ に対し，識別関数

$$f(x) = sign(\boldsymbol{\omega}^{\mathrm{T}}\boldsymbol{x} + b) \tag{1}$$

により，2 値の出力値を計算する．ここで，$\boldsymbol{\omega}$ 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．T は転置を示す．また関数 $sign(u)$ は，$u > 1$ のとき 1 をとり，$u \leqq 0$ のとき-1 をとる符号関数である．

SVM にはカーネルトリックと呼ばれる技法がある．これは，

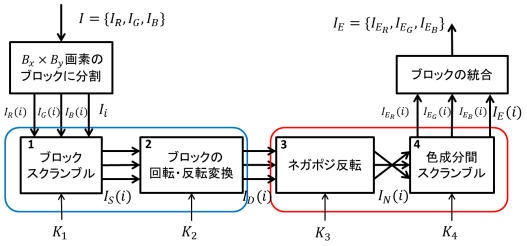


図 1　ブロックベース暗号化の手順

低次元の入力空間を，カーネル関数によって高次元の空間へ変換する方法である．ここで，次元とは，入力特徴ベクトル $\boldsymbol{x}$ に含まれる要素の個数のことである．カーネルトリックを式 (1) に適用すると，より高次元の特徴空間上に入力ベクトルを写像し，その空間上で以下のように分類することができる．

$$f(x) = sign(\boldsymbol{\omega}^{\mathrm{T}}\phi(\boldsymbol{x}) + b) \tag{2}$$

ここで $\phi(\boldsymbol{x}) : \mathbb{R}^d \longrightarrow \mathcal{F}$ は，入力ベクトル $\boldsymbol{x}$ を高次元の特徴空間 $\mathcal{F}$ へ写像する関数である．d は特徴空間の次元数である．この場合，パラメータ $\boldsymbol{\omega}$ も特徴空間 $\mathcal{F}$ 内の要素として定義される．2 つの入力ベクトルを $\boldsymbol{x}_i$，$\boldsymbol{x}_j$ とすると，そのカーネル関数は以下のように定義される．

$$K(\boldsymbol{x}_i, \boldsymbol{x}_j) = \langle \phi(\boldsymbol{x}_i), \phi(\boldsymbol{x}_j) \rangle \tag{3}$$

ここで，$\langle \cdot, \cdot \rangle$ は内積を表す．カーネル関数にはさまざまな種類がある．例えば，Radian Basis Function(RBF) カーネルは

$$K(\boldsymbol{x}_i, \boldsymbol{x}_j) = exp(-\gamma \|\boldsymbol{x}_i - \boldsymbol{x}_j\|^2) \tag{4}$$

また多項式カーネルは

$$K(\boldsymbol{x}_i, \boldsymbol{x}_j) = (1 + \langle \boldsymbol{x}_i, \boldsymbol{x}_j \rangle)^l \tag{5}$$

で与えられる．ここで γ は決定境界の複雑さを決めるハイパーパラメータ，l は多項式の次数を決めるパラメータである．

SVM の計算では，画像の画素値を直接入力特徴ベクトル $\boldsymbol{x}$ として使用すると，データ量が膨大なために，データの次元削減を行うことが一般的である．代表的な次元削減の方法として，ダウンサンプリング法 [16]，ランダム射影 [] などがある．

2.2 EtC 画像の生成

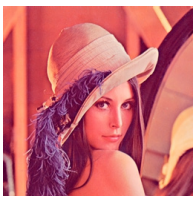
静止画像に対する暗号化法として，画像をブロックに分割して処理を行うブロックベース暗号化が研究されている [9]．この暗号化法は，EtC システムに適用可能であり，暗号化後に JPEG 圧縮を適用可能とする特徴を有する．この方法は図 1 に示すように，4 つのステップにより実行される．各ステップの詳細を以下に示す．

STEP1. ブロックスクランブル

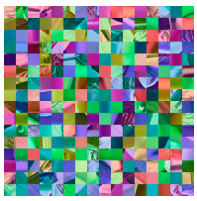
ブロックスクランブルは，分割されたブロックを乱数を用いてランダムに置換する方法である．ブロックスクランブルを行う前に，サイズ X × Y の画像を一定サイズ $B_x \times B_y$ のブロックに分割する．ただし，RGB の各ブロックは共通の鍵を使用して置換する．

STEP2. ブロックの回転，反転変換

ブロックの回転変換は，ブロックの位置関係を変更せずに，ブロックを 0°，90°，180°，270° のいずれかの角度だけ RGB 成分共通でランダムに回転させる方法である．ブロックの反転変換は，ブロックの位置関係を変更せずに，ブロックを水平・垂直方向に RGB 成分共通でランダムに反転させる方法



(a) 原画像 (256 × 256)



(b)EtC 画像 (B_x× B_y=16 × 16)

図 2　EtC 画像例

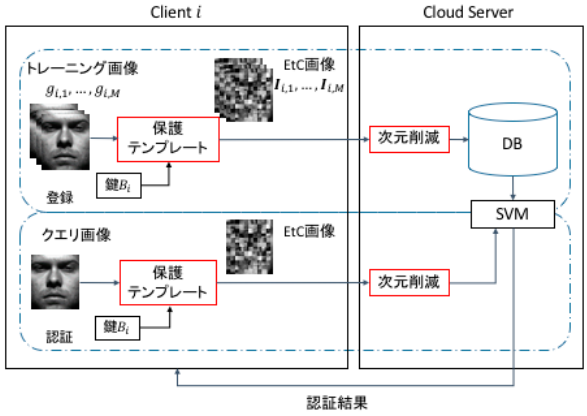


図 3　認証システム

であり，回転しない，もしくは水平・垂直方向どちらにも反転するといったことも起こりえる．

STEP3. ネガポジ反転

ネガポジ変換は，RGB 成分共通で，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すべての画素値を反転させる方法である．ブロック内の画素値を $p(0 \leqq p \leqq 255)$，鍵 K による乱数を $r(i)$ としたとき，次式によりブロックにネガポジ変換を行う．

$$\begin{cases} p' = p & (r(i) = 0) \\ p' = 255 - p & (r(i) = 1) \end{cases} \tag{6}$$

$r(i) = 0$ および $r(i) = 1$ の発生確率は一様に 0.5 が用いられる．

ネガポジ変換を行うことにより，画像の濃淡や色，およびヒストグラムが変化し，より原画像の特定が困難になる．

STEP4. 色成分間スクランブル

色成分間スクランブルは，乱数に応じてブロック内の R，G，B 成分の値を入れ替える方法である．

図 2 は，上述の手順で暗号化した画像例である．ブロックベース暗号化に対して，総当たり攻撃およびジグソーパズル解法による攻撃耐性に対する評価が行われている [14,15]．さらに安全性を向上させるために，グレースケールでのブロックベース暗号化がその拡張系として提案されている [17]．本稿では，このような方法で暗号化した画像を EtC 画像とよぶ．

3.　提　案　法

3.1　テンプレートの直交変換とその性質

本稿では，図 3 のような認証システムを想定する．Client $i, i = 1, ..., N$ は，顔画像などのトレーニングデータ $g_{i,j}, j = 1, ..., M$ を準備し，鍵 B_i を用いて M 個の暗号化されたテンプレート (保護テンプレート)$\boldsymbol{I}_{i,j}, j = 1, ..., M$ を作成する．この場合のテンプレートとは，EtC 画像に相当する．次にそれらを Cloud Server に送信する．その際 EtC 画像は，JPEG によって圧縮を施すことができる．Cloud Server は，JPEG 画像を伸長し，それらに次元削減を施し，データベースに保管すると同時に，SVM での認証に必要な学習を次元削減された保護テンプレートを用いて実行する．認証時には，Client i はクエリから鍵 B_i を用いて保護テンプレートを作成し，Cloud Server へ送信する．Cloud Server は受信した保護テンプレートに次元削減を施し，構築した SVM 学習モデルを用いて認証を行い，認証結果を Client i に返す．

先行研究において，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 [11,12]．ここで，Client$i$ の j 番目のテンプレートを $\boldsymbol{I}_{i,j}$ とおく．ランダムユニタリ行列に基づくテンプレートの保護では，鍵 B_i によって生成されるランダムユニタリ行列 $\boldsymbol{Q}_{B_i}$ を用いた変換 $T(\cdot)$ によって，次式のように保護テンプレート $\hat{\boldsymbol{I}}_{i,j}$ が生成される．

$$\hat{\boldsymbol{I}}_{i,j} = T(\boldsymbol{I}_{i,j}, B_i) = \boldsymbol{Q}_{B_i}\boldsymbol{I}_{i,j} \tag{7}$$

ただし，$\boldsymbol{Q}_{B_i} \in \mathbb{C}^{N \times N}$，$\boldsymbol{I}_{i,j} \in \mathbb{R}^d$ である．ここで，$\boldsymbol{Q}_{B_i}$ はユニタリ行列なので以下の式を満たす．

$$\boldsymbol{Q}_{B_i}^{*}\boldsymbol{Q}_{B_i} = \boldsymbol{I} \tag{8}$$

$[\cdot]^*$ と $\boldsymbol{I}$ は，それぞれエルミート行列と単位行列を示す．

$B_i = B_s$ の下で，式 (7) によって生成された保護テンプレートは，$\boldsymbol{Q}_{B_i} = \boldsymbol{Q}_{B_s}$ の下で以下の性質を持っている．

性質 1: ユークリッド距離の保存

$$\|\boldsymbol{I}_{i,j} - \boldsymbol{I}_{s,t}\|^2 = \|\hat{\boldsymbol{I}}_{i,j} - \hat{\boldsymbol{I}}_{s,t}\|^2 \tag{9}$$

性質 2: 内積の保存

$$\langle \boldsymbol{I}_{i,j}, \boldsymbol{I}_{s,t} \rangle = \langle \hat{\boldsymbol{I}}_{i,j}, \hat{\boldsymbol{I}}_{s,t} \rangle \tag{10}$$

性質 3: 相関係数の保存

$$\frac{\langle \boldsymbol{I}_{i,j}, \boldsymbol{I}_{s,t} \rangle}{\sqrt{\langle \boldsymbol{I}_{i,j}, \boldsymbol{I}_{i,j} \rangle}\sqrt{\langle \boldsymbol{I}_{s,t}, \boldsymbol{I}_{s,t} \rangle}} = \frac{\langle \hat{\boldsymbol{I}}_{i,j}\hat{\boldsymbol{I}}_{s,t} \rangle}{\sqrt{\langle \hat{\boldsymbol{I}}_{i,j}, \hat{\boldsymbol{I}}_{i,j} \rangle}\sqrt{\langle \hat{\boldsymbol{I}}_{s,t}, \hat{\boldsymbol{I}}_{s,t} \rangle}} \tag{11}$$

3.2　EtC 画像の性質

次に EtC 画像の性質について考察する．暗号化を行う行列を $\boldsymbol{E}_{B_i}$ とすると，EtC 画像のテンプレート $\hat{\boldsymbol{I}}_{i,j}$ は，一般に次式により表現される．

$$\hat{\boldsymbol{I}}_{i,j} = \boldsymbol{E}_{B_i}\boldsymbol{I}_{i,j} \tag{12}$$

以下では，$B_1 = B_2 = ... = B_i$ と仮定し，$\boldsymbol{I}_{i,j}$ と $\hat{\boldsymbol{I}}_{i,j}$ の関係を考察する．

A. 正規化なし

まず，ブロックスクランブルはブロック単位での画素の置換であり，ブロックの回転・反転変換，色成分間スクランブルはブロック内での画素の置換と考えられるため，$\boldsymbol{E}_{B_i}$ は置換行列になる．置換行列は

$$\boldsymbol{E}_{B_i} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \tag{13}$$

のように，各行各列に一つだけ 1 の要素を持ち，それ以外は全て 0 となる行列により表され，単位行列を $\boldsymbol{I}$ とすると，

$$\boldsymbol{I} = \boldsymbol{E}_{B_i}^{\mathrm{T}}\boldsymbol{E}_{B_i} \tag{14}$$

が成立する．したがって，$\hat{\boldsymbol{I}}_{i,j}$ は式 (9)，(10)，(11) の性質を持つ．そのため，4 ステップのうち 3 つ，すなわちブロックスク

ランブル，回転・反転変換，色成分間スクランブルの操作は，直交変換されたテンプレートの性質を維持できる．

一方，ネガポジ変換では，$\boldsymbol{I}_{i,j}$ の要素の k 番目の値を $p_{i,j}(k)$ とすると，$\hat{\boldsymbol{I}}_{i,j}$ の k 番目の要素は $255 - p_{i,j}(k)$ と表せ，

$$\begin{aligned} & \|(255 - p_{i,j}(k)) - (255 - p_{s,t}(k))\|^2 \\ = & \| - p_{i,j}(k) + p_{s,t}(k)\|^2 \\ = & \|p_{i,j}(k) - p_{s,t}(k)\|^2 \end{aligned} \tag{15}$$

となる．したがって，式 (9) が成り立ち，ユークリッド距離が保存される．

しかし，内積については，

$$\begin{aligned} & (255 - p_{i,j}(k)) \times (255 - p_{s,t}(k)) \\ = & \ 255^2 - 255(p_{i,j}(k) + p_{s,t}(k)) + p_{i,j}(k) \times p_{s,t}(k)) \\ \neq & \ p_{i,j}(k) \times p_{s,t}(k) \end{aligned} \tag{16}$$

となるため，式 (10) は成立しない．

従って，EtC 画像と原画像の間で，一般にブロックスクランブル，回転・反転，色成分間スクランブルの操作では内積が保存されるが，ネガポジ変換ではユークリッド距離のみが保存され，内積は保存されない．

B. 正規化あり

次に，データに対して正規化を行った場合について考える．今回想定する正規化は，広く用いられている z-score 正規化 [18] であり，データ $x_i, i = 1, 2, ..., N$ を次式によって z_i に置き換える操作である．

$$z_i = \frac{(x_i - \bar{X})}{S} \tag{17}$$

ただし，$\bar{X}$ は各データの平均値である．また，標準偏差 S は

$$S = \sqrt{\frac{\sum_{i=1}^{N}(x_i - \bar{X})^2}{N}} \tag{18}$$

で与えられる．

ネガポジ変換では，式 (17) に対応する表現として

$$\begin{aligned} \hat{z}_{i,j}(k) &= \frac{(255 - p_{i,j}(k)) - (255 - \bar{P}_k)}{S'} \\ &= -\frac{p_{i,j}(k) - \bar{P}_k}{S} \\ &= -z_{i,j}(k) \end{aligned} \tag{19}$$

ただし，

$$\bar{P}_k = \frac{1}{N \times M}\sum_{i=1}^{N}\sum_{j=1}^{M} p_{i,j}(k) \tag{20}$$

$$\begin{aligned} S' &= \sqrt{\frac{\sum_{i=1}^{N}\sum_{j=1}^{M}((255 - p_{i,j}(k)) - (255 - \bar{P}_k))^2}{N \times M}} \\ &= \sqrt{\frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(-p_{i,j}(k) + \bar{P}_k)^2}{N \times M}} \\ &= S \end{aligned} \tag{21}$$

である．ネガポジ変換を行った値を正規化した値 $\hat{z}_{i,j}(k)$ は元の画像を正規化した値 $z_{i,j}(k)$ を符号反転した値になる．符号反転行列は直交行列であるため，式 (9)，(10)，(11) が成り立ち，内積が保存される．したがって，EtC 画像のテンプレートに正規化を施した場合，ネガポジ変換を施しても内積が保存される．

表 1　カーネル関数と EtC 画像の関係

	EtC 画像の性質	
	距離保存 (正規化なし)	内積保存 (正規化あり)
線形カーネル		○
RBF カーネル	○	○
多項式カーネル		○
WAVE カーネル	○	○

3.3　カーネル関数の適用

ここで，EtC 画像を入力とした場合における，使用できるカーネル関数の制約を考察する．EtC 画像のテンプレート間のユークリッド距離が保存されているならば，カーネル関数が RBF カーネルの時，次式が成立する．

$$\begin{aligned} K(\hat{\boldsymbol{I}}_{i,j}, \hat{\boldsymbol{I}}_{s,t}) &= exp(-\gamma\|\hat{\boldsymbol{I}}_{i,j} - \hat{\boldsymbol{I}}_{s,t}\|^2) \\ &= exp(-\gamma\|\boldsymbol{I}_{i,j} - \boldsymbol{I}_{s,t}\|^2) \\ &= K(\boldsymbol{I}_{i,j}, \boldsymbol{I}_{s,t}) \end{aligned} \tag{22}$$

RBF カーネルは，次式を満たす isotropic stationay kernel [19] のクラスに属する．

$$K(\boldsymbol{x}_i, \boldsymbol{x}_j) = K_I(\|\boldsymbol{x}_i - \boldsymbol{x}_j\|) \tag{23}$$

また，テンプレートの内積が保存されているならば，次式が成立する．

$$\begin{aligned} K(\hat{\boldsymbol{I}}_{i,j}, \hat{\boldsymbol{I}}_{s,t}) &= \langle\hat{\boldsymbol{I}}_{i,j}, \hat{\boldsymbol{I}}_{s,t}\rangle \\ &= \langle\boldsymbol{I}_{i,j}, \boldsymbol{I}_{s,t}\rangle \\ &= K(\boldsymbol{I}_{i,j}, \boldsymbol{I}_{s,t}) \end{aligned} \tag{24}$$

線形カーネルや多項式カーネルは，

$$K(\boldsymbol{x}_i, \boldsymbol{x}_j) = K_{In}(\langle\boldsymbol{x}_i, \boldsymbol{x}_j\rangle) \tag{25}$$

を満たす，二つのベクトルの内積のみに依存するカーネルのクラスに属する．

以上のカーネル関数と暗号化画像の関係を表 1 に示す．○は暗号化しても原画像の計算結果と一致するカーネル関数である．

以下では，カーネル関数の計算結果が変化しない場合を想定する．

与えられた EtC 画像を SVM に基づき 2 値分類する問題を設定する．これは，SVM の学習に対する双対問題

$$\begin{aligned} & \max_{\alpha} -\frac{1}{2}\sum_{\substack{i,s\in N \\ j,t\in M}} \alpha_{i,j}\alpha_{s,t}y_{i,j}y_{s,t}\langle\phi(\hat{\boldsymbol{I}}_{i,j}), \phi(\hat{\boldsymbol{I}}_{s,t})\rangle + \sum_{i\in N}\alpha_i \\ & s.t. \sum_{i\in N}\alpha_i y_i = 0 \\ & 0 \leqq \alpha_i \leqq C, i \in N \end{aligned} \tag{26}$$

として与えられる．ここで，$y_{i,j}, y_{s,t} \in \{+1, -1\}$ は各トレーニングデータに対する正解ラベルであり，$\alpha_{i,j}, \alpha_{s,t}$ は双対変数，C は正則化係数である．ここで，内積 $\langle\phi(\hat{\boldsymbol{I}}_{i,j}), \phi(\hat{\boldsymbol{I}}_{s,t})\rangle$ がカーネル関数 $K(\boldsymbol{I}_{i,j}, \boldsymbol{I}_{s,t})$ と等しくなるとき，暗号化を施した場合

でも，双対問題は原画像を用いた場合と同じ問題に帰着することになる．したがって，正規化された EtC 画像と原画像では SVM の計算結果は一致する．

3.4 EtC 画像の次元削減

2.1 で述べたように，SVM の計算では，データの次元削減を行うことが一般的である．そのため，保護テンプレートを直接次元削減することを考える．本稿では，EtC 画像のブロックサイズを考慮したダウンサンプリング法を次元削減法として提案する．保護テンプレートから直接次元削減を行う提案法は，非暗号化画像から同様に次元削減した場合の SVM 計算結果と一致する特徴を持つ．

A．ブロックスクランブル，回転・反転，色成分間スクランブル

EtC 画像 $\hat{\boldsymbol{I}}_{i,j}$ において，$B_x \times B_y$ のブロック内の画素値の平均をブロックごとに計算し新しい画素値とすることで，削減率 $\frac{1}{B_x \times B_y}$ で次元削減された EtC 画像 $\hat{\boldsymbol{I}}_{i,j}$ を得る．ブロックスクランブルおよび回転・反転変換，色成分間スクランブルは画素の置換であるので，ブロック内で画素値の平均を取っても直交変換されたテンプレートの性質を維持できる．従って，次元削減された EtC 画像と，原画像から同様の条件で次元削減されたものとの間で, ブロックスクランブル, 回転・反転, 色成分間スクランブルの操作では内積が保存される．

B．ネガポジ変換

ブロックの平均を取った画素を $\hat{p}_{i,j}(k)$ とすると，ネガポジ変換では式 (19) と同様に，

$$\begin{aligned}\hat{z}_{i,j}(k) &= \frac{(255-\hat{p}_{i,j}(k))-(255-\bar{P}_k)}{S'} \\ &= -\frac{\hat{p}_{i,j}(k)-\bar{P}_k}{S} \\ &= -z_{i,j}(k) \end{aligned} \tag{27}$$

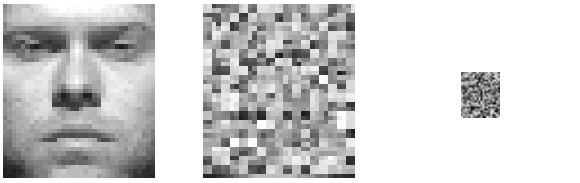
が成立する．従って，次元削減された EtC 画像と，原画像から同様の条件で次元削減されたものとの間では，3.2.A，3.2.B のときと同様の性質を持つことがわかる．よって，ネガポジ変換では，正規化を施した場合内積が保存される．

C．次元削減率の自由度

上述では，ブロックサイズ $B_x \times B_y$ に対して，$\frac{1}{B_x \times B_y}$ に次元削減できることを述べた．ここでは，より一般的な場合について考える．

2.2 で述べた EtC 画像の生成では，全てのステップで同一のブロックサイズ $B_x \times B_y$ を用いて暗号化を行った．JPEG 圧縮を考慮したうえでの最小のブロックサイズは $B_x = B_y = 8$ である．したがって，$\frac{1}{64}$ の削減率になる．

さらに大きな次元削減を行う場合を考察する．3.4 で述べた理由から，ブロックスクランブル，回転・反転変換，色成分間スクランブルでは，ブロックサイズに限らず，ブロックサイズの整数倍のもとで次元削減を行うことができる．しかし，ネガポジ変換に関しては，ブロックサイズと一致した次元削減のみが，暗号化の影響を回避する．この制約を緩和するために，ネガポジ変換処理のためのブロックサイズのみを $B_x \times B_y$ ではなく，それらの整数倍に選択することを提案する．このことによって，次元削減率は $\frac{1}{B_x \times B_y}$ のみならず，$\frac{1}{2 \times B_x \times B_y}$ あるいは $\frac{1}{3 \times B_x \times B_y}$ のように，さらに整数分の 1 に削減することが可能となる．



(a) 原画像 (192 × 160)　(b)EtC 画像 (192 × 160)　(c) 次元削減された EtC 画像 (24 × 20)

図 4　実験画像とその暗号化例

4. 実　　験

提案法の有効性を顔認証実験によって評価する．

4.1 実験準備

本実験では，代表的な顔画像データベースである Extended Yale Database B [20] を用いた．38 人の顔画像が 64 枚ずつ，計 2432 枚で構成され，すべて 192 × 160 のサイズに統一されている．各被験者に対する 64 枚の画像を，トレーニング 32 枚とクエリ 32 枚に分けて実験を行った．実験では，線形カーネルと RBF カーネルを使用した．RBF カーネルでは，ハイパーパラメータ γ を 83 とした．

また，特徴量を抽出する際には $B_x \times B_y = 8 \times 8$ 画素の画素値の平均値を新しい画素値とし，削減率 1/64 で次元削減を行った．192 × 160 の画像を 24 × 20 に次元削減して，480 次元のベクトルを生成した．図 4 には，原画像，EtC 画像，次元削減された EtC 画像を示す．暗号化を施したことによって，視覚的な情報が保護されていることがわかる．暗号化に使用する鍵 B_i は $B_1 = B_2 = ... = B_i$ である．

4.2 実験結果

SVM による顔認識では，DB の各登録者に対して 1 つの分類器が作成される．分類器は，各クエリテンプレート $\hat{\boldsymbol{I}}_q$ に対する予測ラベルおよび分類スコアを出力する．$\hat{\boldsymbol{I}}_q$ は，クエリテンプレート $\boldsymbol{I}_q$ から生成された EtC 画像のテンプレートである．分類スコアは，クエリから分類境界までの距離である．$\hat{\boldsymbol{I}}_q$ の正のラベルに対する分類スコア S_q と閾値 τ との間の関係は以下のように与えられる．

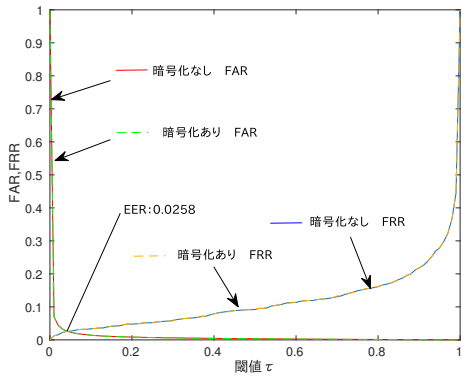
$$if\ S_q \leqq \tau\ then\ accept;\ else\ reject. \tag{28}$$

実験での評価尺度には，本人棄却率 (False Reject Rate：FRR) と他人受理率 (False Accept Rate：FAR)，それらが等しくなる点である等価エラー率 (Equal Error Rate：EER) を用いた．

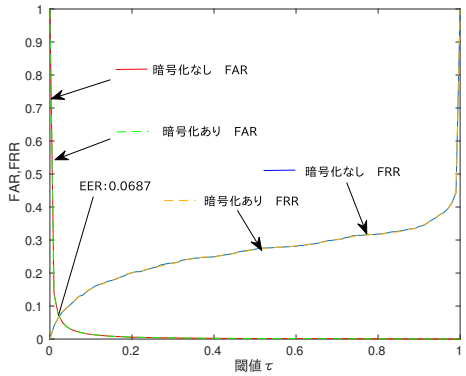
正規化を行ったときの FAR,FRR, および EER を図 5 に示す．これより，線形カーネル，RBF カーネルの両方で，次元削減された EtC 画像 (暗号化あり) と，原画像から同様に次元削減されたもの (暗号化なし) を用いたときの計算結果が一致していることがわかる．先の理論的検証に加え，この実験結果からも，提案法は SVM によるクラス分類に影響を与えないことがわかる．

5. ま と め

本稿では，次元削減を考慮した暗号化領域での SVM の学習



(a) 線形カーネル



(b)RBF カーネル

図 5　FRR と FAR(正規化あり)

法を提案した．EtC 画像のブロックサイズを考慮した次元削減を行うことで，原画像から同様に次元削減した場合の計算結果と一致することを理論的に示した．また，SVM を用いた顔認証実験によって理論の正当性を確認した．

謝　　辞

本研究の一部は，首都大学東京傾斜的研究費 (全学分) 学長裁量枠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)「プライバシー保護のための画像圧縮を可能とする知覚暗号化とその攻撃耐性」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, pp. e7, 2014.

[2] R. Lazzeretti and M. Barni, “Private computing with garbled circuits [applications corner],” *IEEE Signal Processing Magazine*, vol. 30, no. 2, pp. 123–127, 2013.

[3] 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. 66–67, 2015.

[4] R. 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.

[5] T. Araki, A. Barak, J. Furukawa, T. Lichter, Y. Lindell, A. Nof, K. Ohara, A. Watzman, and O. Weinstein, “Optimized honest-majority mpc for malicious adversaries - breaking the 1 billion-gate per second barrier,” in *IEEE Symposium on Security and Privacy (SP)*, 2017, pp. 843–862.

[6] Y. Aono, T. Hayashi, L. Phong, and L. Wang, “Privacy-preserving logistic regression with distributed data sources via homomorphic encryption,” *IEICE Transactions on Information and Systems*, vol. E99.D, no. 8, pp. 2079–2089, 2016.

[7] I. Ito and H. Kiya, “One-time key based phase scrambling for phase-only correlation between visually protected images,” *EURASIP Journal on Information Security*, vol. 2009, no. 841045, pp. 1–11, 2010.

[8] J. Zhou, X. Liu, O. C. Au, and Y. Y. Tang, “Designing an efficient image encryption-then-compression system via prediction error clustering and random permutation,” *IEEE transactions on information forensics and security*, vol. 9, no. 1, pp. 39–50, 2014.

[9] 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.

[10] 前川 貴大, 木下 裕磨, 塩田 さやか, and 貴家 仁志, “ランダムユニタリ変換を用いたプライバシー保護を考慮した svm 学習法,” vol. 117, no. 200, pp. 13–18, 2017.

[11] 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.

[12] 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, 2016.

[13] 河村 綾菜, 前川 貴大, 木下 裕磨, and 貴家 仁志, “ランダムユニタリ変換を用いたプライバシー保護を考慮した svm 学習法,” vol. 118, no. 73, pp. 1–6, 2018.

[14] T. Chuman, K. Kurihara, and H. Kiya, “On the security of block scrambling-based etc systems against jigsaw puzzle solver attacks,” in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2017, pp. 2157–2161.

[15] T. Chuman, K. Kurihara, and H. Kiya, “Security evaluation for block scrambling-based etc systems against extended jigsaw puzzle solver attacks,” in *IEEE International Conference on Multimedia and Expo (ICME)*, 2017, pp. 229–234.

[16] J. Wright, A. Yang, A. Ganesh, S. Sastry, and Y. Ma, “Robust face recognition via sparse representation,” *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 31, no. 2, 2009.

[17] Warit Sirichotedumrong, Tatsuya Chuman, Shoko Imaizumi, and Hitoshi Kiya, “Grayscale-based block scrambling image encryption for social networking services,” in *Proc. IEEE International Conference on Multimedia and Expo(ICME)*, 2018.

[18] S. Theodoridis, A. Pikrakis, K. Koutroumbas, and D. Cavouras, *Introduction to Pattern Recognition A MATLAB Approach*, Elsevier, 2010.

[19] M. G. Genton, “Classes of kernels for machine learning: A statistics perspective,” *J. Mach. Learn. Res.*, vol. 2, pp. 299–312, 2002.

[20] A.S. Georghiades, P.N. Belhumeur, and D.J. Kriegman, “From few to many: Illumination cone models for face recognition under variable lighting and pose,” *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 23, no. 6, pp. 643–660, 2001.