ランダムユニタリ変換を用いた
プライバシーを考慮した
機械学習法に関する研究

Privacy-preserving Machine Learning by using random unitary transformation

首都大学東京大学院
システムデザイン研究科　情報通信システムコース
17890536　前川 貴大

目次

あらまし

本稿では，ランダムユニタリ変換に基づき生成された保護画像を用いた，サポートベクターマシーン（SVM）学習法を提案し，その性能を評価する．近年，クラウドサービスを利用し，プロバイー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，プライバシー保護を考慮したSVM学習法を考察する．ユニタリ性を持つ変換行列を用いた画像保護法は，テンプレートを保護すると同時に，SVMの認識性能を劣化させないことを示す．また，鍵の更新や利用形態を考察し，保護なしの画像を用いた場合の性能を向上できる利用例について述べる．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．

Summary

A privacy-preserving Support Vector Machine (SVM) computing scheme is proposed in this paper. 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. Accordingly, we consider privacy-preserving SVM-computing. We focus on protecting visual imformation of images by using a random unitary transformation. Some properties of the protected images are discussed. The proposed scheme enables us not only to protect images, but also to have the same performance as that of unprotected images even when using typical kernel functions such as linear kernel, Radial Basis Function(RBF) kernel and polynomial kernel. Moreover, it can be directly carried out by using well-known SVM algorithms, without preparing any algorithms specialized for secure SVM computing. In an experiment, the proposed scheme is applied to a face-based authentication algorithm with SVM classifiers to confirm the effectiveness.

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が急速に普及してきている．SaaS(Software-as-a-Service) はクラウドコンピューティングサービスの一つであり，モバイルデバイスやウェブブラウザなどのクライアントが用途に応じて外部のソフトウェアを使用することを可能としている．商用の SaaS も多く存在し，そのアプリケーションの領域は画像処理を含め，多岐にわたっている．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 [1–3]．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機械学習の計算法を考察する．

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，いわゆる秘密計算が盛んに研究されている．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 [4–7]．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．また秘密計算とは独立に，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 [8–16]．しかし，それらの手法では，機械学習への適用は検討されていない．

以上の背景から，本論文では，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

保護を考慮した機械学習法を提案する．特に, 本論文では, 機械学習法として, 幅広いアプリケーション・ソフトウェアにて用いられているサポートベクターマシーン（SVM）に着目し, プライバシー保護を考慮したSVM学習法を提案する. 提案法では，画像などから抽出される画像 (特徴量) の画像からランダムユニタリ行列を用いて保護画像を生成する．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 [17–23]，本稿では，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を指摘する．特定の条件を満たすカーネル関数の下では, 画像保護法が持つ性質により, 保護画像を用いた場合においてもSVMの最適化問題がオリジナルの画像を用いた場合と同じ問題に帰着できることを示す. また画像と秘密鍵による二重認証性を実行することも可能であり，どちらかが流出した場合においても，認識性能を維持できる特徴を提案法は持つ．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 研究の背景と目的

2.1 サポートベクターマシン

SVMとは，機械学習の一つであり，カーネルトリックを適用した非線形分離識別機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

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

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$\mathrm{sign}(u)$は，$u > 1$のとき1をとり，$u \leq 0$のとき-1をとる符号関数である．

本質的に非線形な問題に対応するための方法として，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カーネル法が知られている．そこで入力$\boldsymbol{x}$を高次元の特徴空間$\mathcal{F}$へ写像する関数を$\phi(\boldsymbol{x}) : \mathbb{R}^d \to \mathcal{F}$を考える．この$\phi(\boldsymbol{x})$を新たな特徴ベクトルだと解釈すると式(1)は以下のように書き換えることができる．

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

この場合，パラメータωも特徴空間$\mathcal{F}$内の要素として定義される($\omega \in \mathcal{F}$)．二つのベクトル$\boldsymbol{x}_i$，$\boldsymbol{x}_j$のカーネル関数は以下のように定義される．

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

カーネル関数には代表的なカーネル関数として，Radial Basis Function(RBF)カーネル，

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

多項式カーネル

$$K(\boldsymbol{x}_i, \boldsymbol{x}_j) = (1 + \boldsymbol{x}_i^T \boldsymbol{x}_j)^d \tag{5}$$

などがある．ここでΥは決定境界の複雑さを決めるハイパーパラメータであり，dは多項式の次数を決定するパラメータである．

2.2 プライバシー保護を考慮したSVM学習

本稿では，図1のようなプライバシーを考慮した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 p_i を用いてM個の保護テンプレートを作成する．次にそれらをCloud Serverに送信する．Cloud Serverは，それらをデータベースに保管すると同時に，SVM認証に必要な学習を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 p_i を用いて保護テンプレートを作成し，Cloud Serverに送る．Cloud Serverは事前に構築した学習モデルを用いて顔認証を行い，認証結果をClient i に返す．ここで，Serverが保持するテンプレートはすべて保護されているため，データが持つプライバシー情報を保護した形式で，このSVMシステムは実行される．

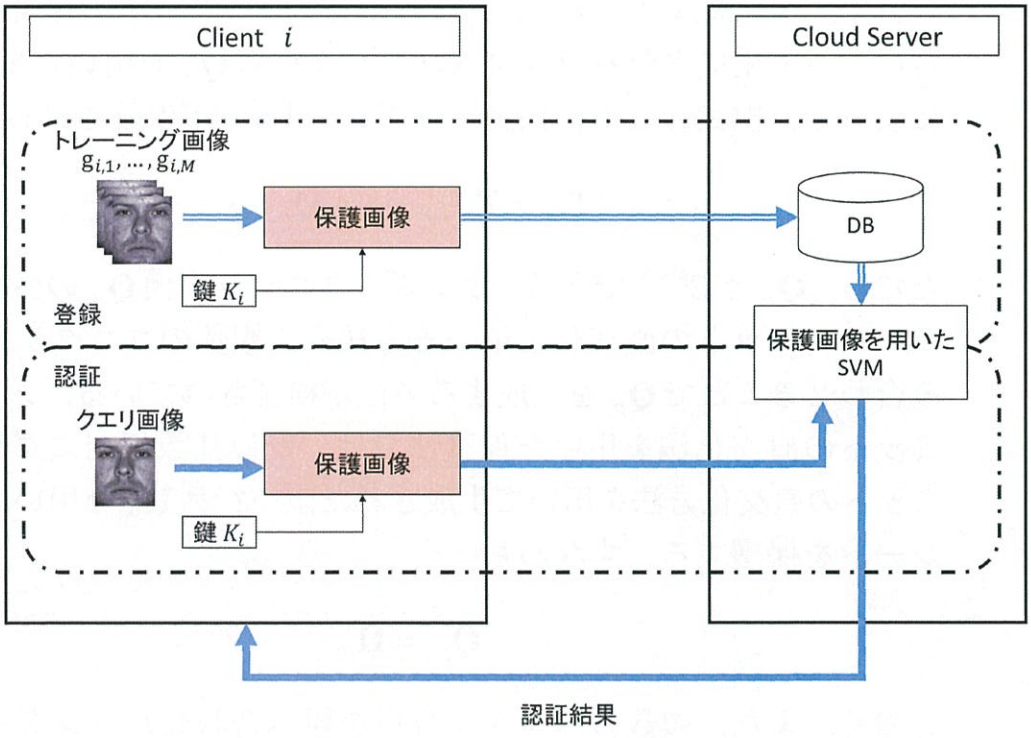


図 1: プライバシーを保護を考慮したアーキテクチャ

3 提案法

3.1 ユニタリ変換に基づくテンプレート保護

先行研究において，キャンセラブルバイオメトリクスのための一方法として，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 [17–22].

いま，Client i の j 番目の画像 $\mathrm{g}_{i.j}$ から生成されるテンプレートを $\mathbf{f}_{i,j}$ 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 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 $\mathrm{T}(\cdot)$ によって，次式のように保護テンプレート $\hat{\mathbf{f}}_{i,j}$ が生成される．

$$\hat{\mathbf{f}}_{i,j} = T(\mathbf{f}_{i,j}, p_i) = \mathbf{Q}_{p_i}\mathbf{f}_{i,j} \tag{6}$$

ただし，$\mathbf{Q}_{p_i} \in \mathbb{C}^{N\times N}$ である．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で $\mathbf{Q}_{p_i}$ を生成する方法が検証されている．グラムシュミットの直交化法を用いた保護法では，疑似乱数行列にグラムシュミットの直交化方法を用いて生成された直交行列 $\mathbf{H}_{p_i}$ を用いてテンプレートを保護する．すなわち

$$\mathbf{Q}_{p_i} = \mathbf{H}_{p_i} \tag{7}$$

とおく．また，複数のユニタリ行列を組み合わせたランダムユニタリ行列 $\mathbf{Q}$ を生成する方法の一例を以下に示す．

$$\mathbf{Q}_{p_i} = \mathbf{H}_{p_i}\mathbf{A}\mathbf{L}_{p_i} \tag{8}$$

ただし，$\mathbf{A}$ は離散フーリエ変換やアダマール変換等のランダム性を有しないユニタリ変換の行列であり，$\mathbf{H}_{p_i}$ および $\mathbf{L}_{p_i}$ はそれぞれ疑似乱数生成器によって，生成されたランダム性を持つユニタリ行列である．ここで $\mathbf{H}_{p_i}\mathbf{A}\mathbf{L}_{p_i}$ は次式を満たす．

$$(\mathbf{H}_{p_i}\mathbf{A}\mathbf{L}_{p_i})^*(\mathbf{H}_{p_i}\mathbf{A}\mathbf{L}_{p_i}) = \mathbf{I} \tag{9}$$

ただし，$[\cdot]^*$ と $\mathbf{I}$ はそれぞれエルミート転置と単位行列である．$\mathbf{H}_{p_i}$，$\mathbf{L}_{p_i}$ にはベクトルの要素の順番ランダムに入れ替える random permutation matrix や位相をランダムに変更する random phase matrix などがある [21,22].

3.1.1 ランダムユニタリ行列の持つ性質

ランダムユニタリ行列に基づくテンプレート保護法により，生成された保護テンプレートは以下の特徴を持っている [22]．ただし，以下では $p_1 = p_2 = ... = p_N$ を仮定する．

特徴1 ： ユークリッド距離の保存

$$\|\mathbf{f}_{i,j} - \mathbf{f}_{s,t}\|_2 = \|\hat{\mathbf{f}}_{i,j} - \hat{\mathbf{f}}_{s,t}\|_2 \tag{10}$$

特徴2 ： 内積の保存

$$\mathbf{f}_{i,j}^* \mathbf{f}_{s,t} = \hat{\mathbf{f}}_{i,j}^* \hat{\mathbf{f}}_{s,t} \tag{11}$$

特徴3 ： 相関係数の保存

$$\frac{\mathbf{f}_{i,j} \cdot \mathbf{f}_{s,t}}{\sqrt{\mathbf{f}_{i,j} \cdot \mathbf{f}_{i,j}} \sqrt{\mathbf{f}_{s,t} \cdot \mathbf{f}_{s,t}}} = \frac{\hat{\mathbf{f}}_{i,j} \cdot \hat{\mathbf{f}}_{s,t}}{\sqrt{\hat{\mathbf{f}}_{i,j} \cdot \hat{\mathbf{f}}_{i,j}} \sqrt{\hat{\mathbf{f}}_{s,t} \cdot \hat{\mathbf{f}}_{s,t}}} \tag{12}$$

3.1.2 ランダムユニタリ行列の鍵空間

ここでランダムユニタリ行列を用いた場合における鍵空間について考察する．

グラムシュミットの直交化による生成

この場合，擬似乱数生成器より生成された乱数を要素とする $N \times N$ の行列に対してグラムシュミットの直交化により、ランダムユニタリ行列を生成する．ここで擬似乱数生成器が u bit の乱数を生成する場合，このランダムユニタリ行列の鍵空間を N_G は，

$$N_G \fallingdotseq 2^u \quad \cdot N^2 \tag{13}$$

となる．

複数のユニタリ行列から生成

この生成法では, 式 (8) に示される通り, 複数のユニタリ行列を組み合わせることで, 変換行列を作成する. ここでユニタリ行列である離散コサイン変換行列 $\mathbf{A}_{DCT}$ と random permutation matrix $\mathbf{H}_{p_i}$ の 2 つの行列変換行列 $\mathbf{Q}$ について考える. この時 $\mathbf{Q}$ は,

$$\mathbf{Q} = \mathbf{A}_{DCT}\mathbf{H}_{p_i} \tag{14}$$

として与えられる. 離散コサイン変換行列の各要素は定数であるため, この変換行列の鍵空間 N_Q は randam permutation matrix に依存する. $\mathbf{H}_{p_i}$ はベクトルの各要素の順番をランダムに入れ替える変換であるため, 鍵空間は

$$N_Q = N^2 \tag{15}$$

となる.

3.2 ブロックベース画像暗号化

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 [11,24–26]．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．ブロックベースア暗号化では,$X \times Y$ の画素を持つ画像をオーバーラップすることなくブロックサイズ $B_x \times B_y$ に分割する. その後この方法は図 2 に示す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 $X \times Y$ の画像を一定サイズ $B_x \times B_y$ のブロックに分割する．ブロックの分割とスクランブルの例を図 3 に示 す. ただし，RGB の各ブロックは共通の鍵 K_1 を使用して置換する. ブロック毎の位置関係を原画像のそれとは変更することに より, 原画像の視認性を制御することが可能となる.

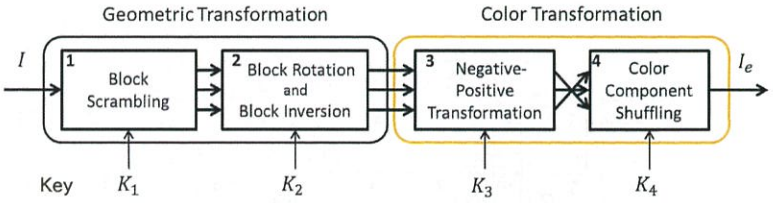


図 2: ブロックベース暗号化の手順

Step2 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，図 4a に示すようにブロックを 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，図 4b に示すようにブロックを水平・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 $p(0 \leq p \leq 255)$，鍵 K_3 による乱数を $r(i), P(r(i) = 0.5)$ としたとき，次式によりブロックにネガポジ変換を行う．

$$p' = \begin{cases} p & (r(i) = 0) \\ 255 - p & (r(i) = 1) \end{cases} \tag{16}$$

Step4: 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．各乱数に応じた色成分の置換を表 1 に示す．

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 [24]．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 [13, 14, 27].

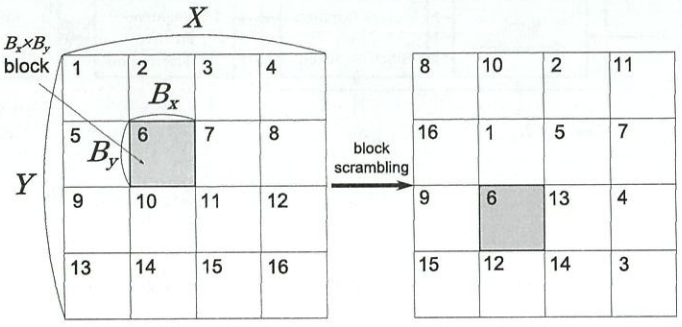
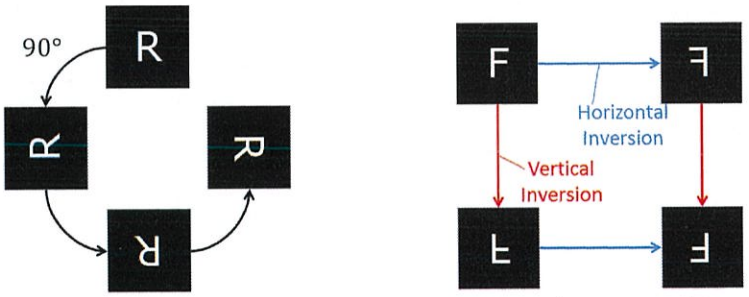


図 3: $B_x \times B_y$ 画素のブロックへの分割とブロックスクランブルの例



(a) ブロックの回転　(b) ブロックの反転

図 4: ブロックの回転・反転のイメージ

表 1: ブロックごとの乱数に対する置換の割り当て方法

乱数	R	G	B
0	R	B	G
1	R	G	B
2	G	R	B
3	G	B	R
4	B	R	G
5	B	G	R

3.2.1 ブロックベース暗号化の性質

次にブロックベース暗号化の特徴について考察する.暗号化を行う行列を$\mathbf{E}_{B_i}$とすると，保護画像$\hat{\mathbf{f}}_{i,j}$は，一般に次式により表現される.

$$\hat{\mathbf{f}}_{i,j} = \mathbf{E}_{B_i}\mathbf{f}_{i,j} \tag{17}$$

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，$\mathbf{E}_{B_i}$は置換行列になる.置換行列は

$$\mathbf{E}_{B_i} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \tag{18}$$

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$\mathbf{I}$とすると，

$$\mathbf{I} = {\mathbf{E}_{B_i}}^T\mathbf{E}_{B_i} \tag{19}$$

したがって，$\hat{\mathbf{f}}_{i,j}$は式(10),(11),(12)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，$\mathbf{f}_{i,j}$のk番目の値を$p_{i,j}(k)$とすると,$\hat{\mathbf{f}}_{i,j}$のk番目の要素は$255 - p_{i.j}$と表わせ,

$$\begin{aligned} & \|(255 - p_{i,j}(k)) - (255 - p_{s,t}(k))\|^2 \\ = \ & \| - p_{i,j}(k) + p_{s,t}\|^2 \\ = \ & \|p_{i,j}(k) - p_{s,t}(k)\|^2. \end{aligned} \tag{20}$$

となる.したがって式10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

$$\begin{aligned}
& (255 - p_{i,j}(k)) * (255 - p_{s,t}(k)) \\
= \; & 255^2 - 255(p_{i,j}(k) + p_{s,t}(k)) + p_{i,j}(k) \times p_{s,t}(k) \\
\neq \; & p_{i,j}(k) * p_{s,t}(k)
\end{aligned} \tag{21}$$

となるため, 式 11 は成立しない.

従って，保護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.

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 [28] であり，データ $x_i, i = 1, 2, \ldots, N$ を次式によって z_i に置き換える操作である.

$$z_i = \frac{(x_i - \bar{X})}{S}, \tag{22}$$

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

$$S = \sqrt{\frac{\sum_{i=1}^{N}(x_i - \bar{X})^2}{N}}. \tag{23}$$

で与えられる.

ネガポジ変換では, 式 (22) に対応する表現として

$$\begin{aligned}
\hat{z}_{i,j}(k) &= \frac{(255 - p_{i,j}(k)) - (255 - \bar{P}_k)}{S'} \\
&= -\frac{p_{i.j}(k) - \bar{P}_k}{S} \\
&= -z_{i,j}(k)
\end{aligned} \tag{24}$$

ただし,

$$\bar{P}_k = \frac{1}{N \times M} \sum_{i=1}^{N} \sum_{j=1}^{M} p_{i,j}(k) \tag{25}$$

$$
\begin{aligned}
S' &= \sqrt{\frac{\sum_{i=1}^{N}\sum_{j=1}^{M}((255-p_{i,j}(k))-(255-\bar{P}_k))^2}{N\times M}} \\
&= \sqrt{\frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(-p_{i,j}(k)+\bar{P}_k)^2}{N\times M}} \\
&= S. \qquad (26)
\end{aligned}
$$

である. ネガポジ変換を行った値を正規化した値 $\hat{z}_{i,j}$ は元の画像を正規化した値 $z_{i,j}$ 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 (10),(11),(12) が成り立ち，内積が保存される．したがって，保護画像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．

3.2.2 ブロックベース暗号化の鍵空間

ここでは，鍵空間の観点からブロックスクランブル画像暗号化法の安全性について要約する. ブロックスクランブル画像暗号化法は，元画像をブロックに分割してブロックベースの暗号化を施しているため，ブロックの総数 L が鍵空間に関係するパラメータである．すべての通りの鍵を用いて総当り攻撃が行われる場合を想定し，ブロックスクランブル画像暗号化法の評価が行われてきた.

ブロックスクランブルで暗号化を施す場合，ブロックの置換の総数がブロックスクランブルにおける鍵空間の大きさ N_B となる．これは総ブロック数 L を用いて $L!$ と表すことができるため,

$$N_B = L! \qquad (27)$$

となる．サイズ 672×504 の画像をサイズ 28×28 のブロックに分割した場合を考える．総ブロック数 L は $\lfloor\frac{672}{28}\rfloor\times\lfloor\frac{504}{28}\rfloor = 432$ となるため，鍵空間の大きさは 432! となる．$2^256 < 432!$ であることから，256 ビットの鍵を使用する暗号よりも大きい鍵空間を持つことがわかる．ブロックの回転変換を施す場合，各ブロックの回転方向は，回転しない場合を含む 4 通りから選ぶことができる．また，ブロックの反転変

換においても，各ブロックにつき水平・垂直方向それぞれに反転するか選ぶことができる．回転変換，反転変換 をそれぞれ施した場合の鍵空間の大きさを N_R, N_I とすると，

$$N_R = 4^L, N_I = 4^L \tag{28}$$

となる，回転，反転変換を両方施した場合の鍵空間の大きさを N_D とすると，270 回転したブロックと水平・垂直方向に反転したブロックは等しいので

$$N_D = 8^L \tag{29}$$

となる．ネガポジ反転を施した場合，RGB 成分共通，かつブロック単位でネガポジ反転を行うので，鍵空間の大きさを N_N とすると，

$$N_N = 2^L \tag{30}$$

となる．同様に色成分間スクランブルを施した場合は，表 1 から分かるように 6 通りの RGB 成分間の入れ替えが考えられるので，鍵空間の大きさを N_E とすると，

$$N_E = 6^L \tag{31}$$

となる．上記の暗号化法はそれぞれ独立な処理であることから，組み合わせて用いた場合に生成され得る暗号化画像の総数は，各暗号化により生成され得る暗号化画像の総数の積で表される．すなわち，暗号化画像の総数 N_A は，

$$NA = L! \cdot 8^L \cdot 2^L \cdot 6^L \tag{32}$$

により計算されることとなる．サイズ 672×504 の画像をサイズ 28×28 のブロックに分割し全ての暗号化を施した場合，総ブロック数 $L = 432$ なので，暗号化画像は $N_A = 432! \times 8^4 32 \times 2^4 32 \times 6^4 32$ の鍵空間を有する．$2^2 56 \ll N_A$ であるから，鍵空間の観点からすると総当り攻撃に対しては安全であると言える．

3.3 カーネル関数の適用

ここで，保護テンプレート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．保護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，提案法の特徴1により次式が成立する．

$$K(\hat{\mathbf{f}}_{i,j}, \hat{\mathbf{f}}_{s,t}) = \exp(-\frac{\|\hat{\mathbf{f}}_{i,j} - \hat{\mathbf{f}}_{s,t}\|_2}{\sigma^2}) \tag{33}$$

$$= \exp(-\frac{\|\mathbf{f}_{i,j} - \mathbf{f}_{s,t}\|_2}{\sigma^2}) = K(\mathbf{f}_{i,j}, \mathbf{f}_{s,t}) \tag{34}$$

A stationary カーネル $K_S(\boldsymbol{x}_i - \boldsymbol{x}_j)$ は不変カーネルであり，式35のように2つの入力ベクトルの差に依存したカーネルを示す．

$$K(\boldsymbol{x}_i, \boldsymbol{x}_j) = K_S(\boldsymbol{x}_i - \boldsymbol{x}_j), \tag{35}$$

さらに,stationary カーネルが2つの入力ベクトルの差のノルムに依存する場合，それらのカーネル $K_I(\|\boldsymbol{x}_i - \boldsymbol{x}_j\|)$ はisotropic カーネルと呼ばれ，以下のように示される．

RBFカーネルに限らず，代表的なカーネルの多くは，同様に，

$$K(\hat{\mathbf{f}}_{i,j}, \hat{\mathbf{f}}_{s,t}) = K(\mathbf{f}_{i,j}, \mathbf{f}_{s,t}) \tag{36}$$

が成立する．ただし成立しないカーネルも存在する．以下では，式(36)の下で議論を展開する．

次に，ある保護テンプレート $\hat{\mathbf{f}}_{i,j}$ が特定のものであるかどうかを判別するSVMについて考える．このSVMの学習に対する双対問題は

$$\begin{aligned} &\max_{\alpha} \ -\frac{1}{2} \sum_{\substack{i,s \in N \\ j,t \in M}} \alpha_{i,j}\alpha_{s,t}y_{i,j}y_{s,t}\phi(\hat{\mathbf{f}}_{i,j})^T\phi(\hat{\mathbf{f}}_{s,t}) + \sum_{\substack{i \in N \\ j \in M}} \alpha_{i,j} \\ &s.t. \sum_{\substack{i \in N \\ j \in M}} \alpha_{i,j}y_{i,j} = 0 \\ &0 \le \alpha_{i,j} \le C, \ i \in N \end{aligned} \tag{37}$$

として与えられる．ここで，$y_{i,j}$，$y_{s,t}$ は各トレーニングデータに対する正解ラベル $(y_{i,j}, y_{s,t} \in \{+1, -1\})$ であり，$\alpha_{i,j}$，$\alpha_{s,t}$ は双対変数，C は正則係数である．このとき，内積 $\phi(\hat{\mathbf{f}}_{i,j})^T \phi(\hat{\mathbf{f}}_{s,t})$ はカーネル関数 $K(\hat{\mathbf{f}}_{i,j}, \hat{\mathbf{f}}_{s,t})$ に相当する．従って，保護テンプレートを用いた場合の双対問題は，以下のように与えられる．

$$
\begin{aligned}
&\max_{\alpha} \; -\frac{1}{2} \sum_{\substack{i,s \in N \\ j,t \in M}} \alpha_{i,j} \alpha_{s,t} y_{i,j} y_{s,t} \phi(\hat{\mathbf{f}}_{i,j})^T \phi(\hat{\mathbf{f}}_{s,t}) + \sum_{\substack{i \in N \\ j \in M}} \alpha_{i,j} \\
&= \max_{\alpha} \; -\frac{1}{2} \sum_{\substack{i,s \in N \\ j,t \in M}} \alpha_{i,j} \alpha_{s,t} y_{i,j} y_{s,t} K(\mathbf{f}_{i,j}, \mathbf{f}_{s,t}) + \sum_{\substack{i \in N \\ j \in M}} \alpha_{i,j} \\
&s.t. \sum_{\substack{i \in N \\ j \in M}} \alpha_{i,j} y_{i,j} = 0 \\
&0 \le \alpha_{i,j} \le C, \; i \in N
\end{aligned}
\tag{38}
$$

この結論は，保護テンプレートを用いた場合においても，最適化問題はオリジナルのテンプレートを用いた場合と同じ問題に帰着することを示している．従って，ユニタリ変換に基づく保護テンプレートは SVM システムの認証率に影響を及ぼさないことがわかる．

3.4 鍵の選択と更新

図 1 に示したように，トレーニングデータ $\mathrm{g}_{i,j}$ は，鍵 p_i を用いて保護テンプレートに変換される．ここでは，鍵 p_i の 2 つの選択法について述べる．

3.4.1 Key condition 1: $p_1 = p_2 = ... = p_N$

第 1 の選択は，すべての i において共通の鍵を使用する，すなわち $p_1 = p_2 = ... = p_N$ とする方法である．このときは，3.1 での結論が直接成立する．従って，SVM による認証性能は，テンプレートを保護しない場合と一致する．

3.4.2 Key condition 2: $p_1 \neq p_2 \neq ... \neq p_N$

第2の選択は，すべてのiにおいて異なる鍵を使用する，すなわち$p_1 \neq p_2 \neq ... \neq p_N$とする方法である．このとき，3.1での結論は，共通のp_iによって生成された保護テンプレート間のみに成立する．この選択は，テンプレートと鍵による認証を同時に行うことに相当し，同時に2つが認証されたときのみに，認証が成立したと判断する処理に相当する．この鍵の条件の下では，2つのなりすまし攻撃が想定できる．1つは暗号化に用いる鍵が流出した場合である．この場合攻撃者は，その流出した鍵を用いてなりすまし攻撃を実行することが可能である．そしては，もうひとつはクライアントの画像が流出した場合である．この場合，攻撃者は流失した画像を任意の鍵により変換し，流出したクライアントになりすますことが考えられる．本稿では実験において，これらの場合においても安全であることを確認し，なりすまし攻撃に対して頑健であることを示す．

保護テンプレート生成に使用される鍵やランダム行列を，定期的に更新することが，安全性の観点から望まれる．保護テンプレート$\hat{\mathbf{f}}_{i,j}$を新しいランダム行列$\mathbf{Q}_{p_i'}$を用いて更新する操作は，

$$\hat{\mathbf{f}}'_{i,j} = \mathbf{Q}_{p_i'}\hat{\mathbf{f}}_{i,j} \tag{39}$$

と与えられる。新たに生成された保護テンプレートは、テンプレート$\mathbf{f}_{i,j}$からランダムユニタリ行列$\mathbf{Q}_{p_i''} = \mathbf{Q}_{p_i'}\mathbf{Q}_{p_i}$を用いて

$$\hat{\mathbf{f}}'_{i,j} = \mathbf{Q}_{p_i''}\mathbf{f}_{i,j} \tag{40}$$

と生成したものに一致する．以上のように，提案法は，オリジナルのテンプレート$\mathbf{f}_{i,j}$の保存なしに，保護テンプレートの更新が可能である．

4 シミュレーション

4.1 実験条件

本実験では，代表的な顔画像データベースであるExtended Yale Face Database B [23] を用いた．$N = 38$ 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，すべて 192×168 のサイズに統一されてる(図5参照)．各被験者に対する64枚の顔画像を，トレーニング32枚 ($M = 32$) とクエリ32枚分けて実験を行った．保護テンプレートの生成には，random permutation matrixによる生成法を用いた．また，実験では線形カーネルとRBFカーネルを，正則化係数 $C = 1$，$C = 34$ の元でそれぞれ使用した．またRBFカーネルでは，ハイパラメータ γ を81とした．

また特徴量の抽出方法としては，ダウンサンプリング法を使用した．ここでダウンサンプリングとは，画像を重複の無いブロックに分割し，各ブロックの平均値を計算することで，特徴を抽出する方法である [20]．192×168 の画像を複数のランダムユニタリ行列を組み合わせによる保護法の場合 38×32, ブロックベース暗号化による保護法の場合 32×32 にダウンサンプリングして，各1254次元,1024次元のテンプレートベクトルを生成した．図6には，それぞれランダムユニタリ行列を用いた保護法を適用しない場合と，適用した場合のテンプレートを示す．保護法を適用しな場合には視覚的情報が残っているが，適用した場合には視覚的情報が保護されていることがわかる．

4.2 結果と考察

SVMを用いた顔認証では，DBの登録者1人に対して一つの分類器が生成される。あるクエリーのテンプレート $\mathbf{f}_q$ を受け取った分類器は、正もしくは負の予測ラベルおよび各クラスに対する分類スコアを出力する．ここで分類スコアとは分類の信頼度に相当する．$\mathbf{f}_q$ の

(a)person1

(a)person2

図 5: Extended Yale Face Database B の例

正ラベルに対する分類スコア S_q と閾値 τ の関係性を以下のように定める．

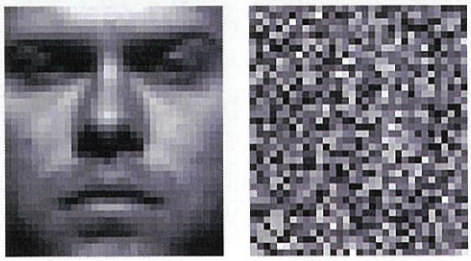
$$if\ S_q \geq \tau\ then\ accept;\ else\ reject \tag{41}$$

ユニタリ行列変換に基づく保護法の評価尺度には，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 Erroe Rate : EER) を用いた．

4.2.1 ランダムユニタリ行列による保護法

A. $p_1 = p_2 = ... = p_N$

すべての Client において同一の鍵を用いて保護テンプレートを生成した場合の結果を図 7 に示す．線形カーネルおよび RBF カーネルのどちらにおいても保護テンプレート (protected) から得られた結果が，オリジナルテンプレート (non-protected) から得た結果と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，ラ



(a) 原画像 (b) 保護画像

図 6: 保護画像の生成例

ンダムユニタリ行列を用いた保護法はSVMによるクラス分類に影響を与えないことがわかる．

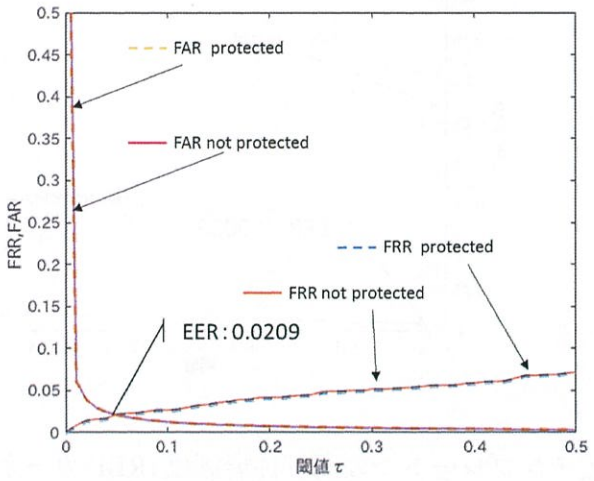
B. $p_1 \neq p_2 \neq ... \neq p_N$

図8は，保護テンプレートをClient毎に異なる鍵p_iによって生成した場合の結果である．3.4で述べたように，この条件は，テンプレートの保護なしの場合と異なり，テンプレートによる認証と鍵による認証を同時に行うことを想定している，図8及び図9から，図7に比べ認証性能が向上することがわかる．

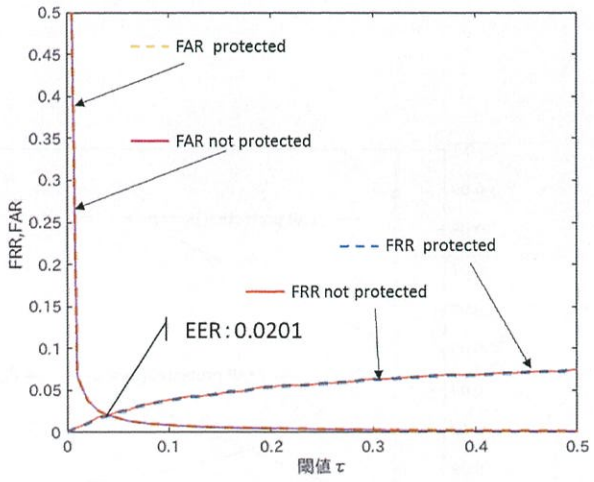
C. 鍵の流出

次に，秘密鍵が流出した場合の認識性能（FAR）を図10に示す．この特性は，鍵p_iが，クライアントiからテンプレート$g_{s,j}, s \neq i$を持つ他のクライアントsに流出した場合を想定した実験である．クライアントsが，鍵p_iとテンプレート$g_{s,j}$を用いて保護テンプレートを作成し，$g_{i,j}$の保護テンプレートに成りすます認証攻撃である．図10に示したように，図8に比べ少しFARは上昇するが，低い値を維持することがわかる．

一方，図11はテンプレート$g_{i,j}$が流出した場合の結果である．クライアントsが，鍵p_sとテンプレート$g_{i,j}$を用いて保護テンプレートを作成し，$g_{i,j}$の保護テンプレートに成りすます認証攻撃である．図10の場合と同様に，図8に比べFARは上昇するが，低い値を維持している．



(a) 線形カーネル ($C = 1$)



(b) RBF カーネル ($C = 34, \Upsilon = 81$)

図 7: 保護テンプレートでの認証性能評価 ($p_1 = p_2 = ... = p_N$)

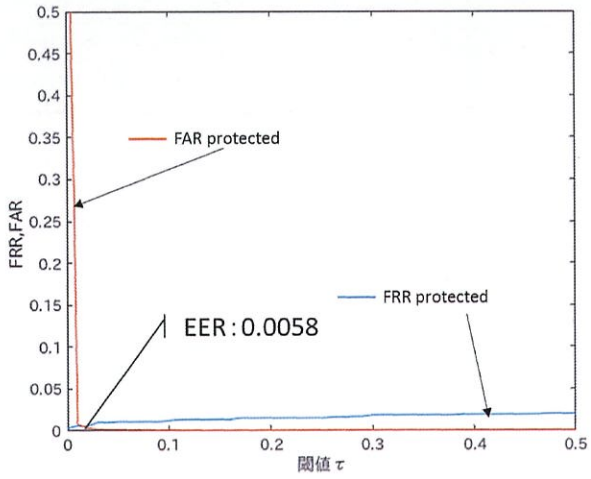


図 8: 保護テンプレートでの認証性能評価 (RBF カーネル，$p_1 \neq p_2 \neq ... \neq p_N$)

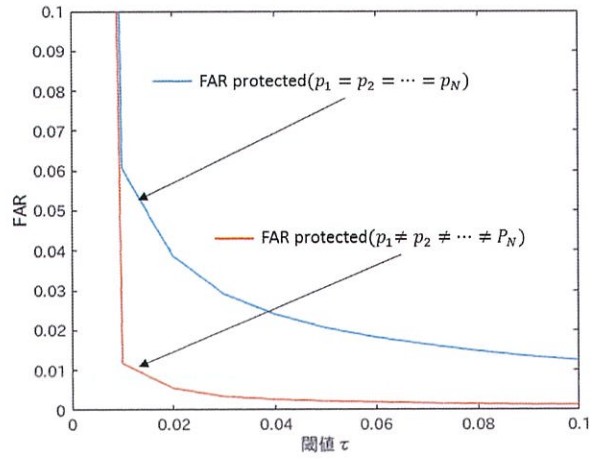


図 9: FAR の比較 (RBF カーネル)

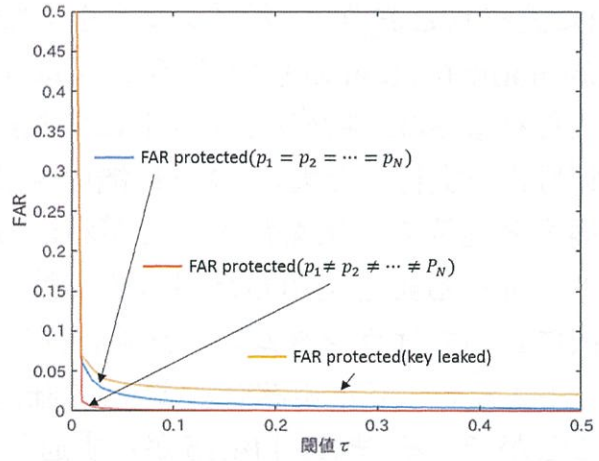


図 10: 鍵の流出を想定した場合の FAR (RBF カーネル)

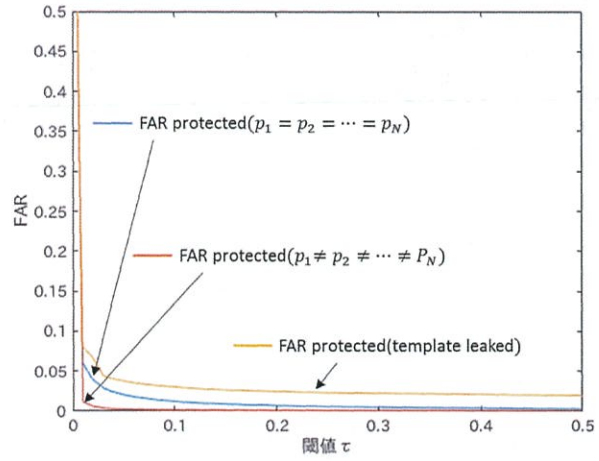
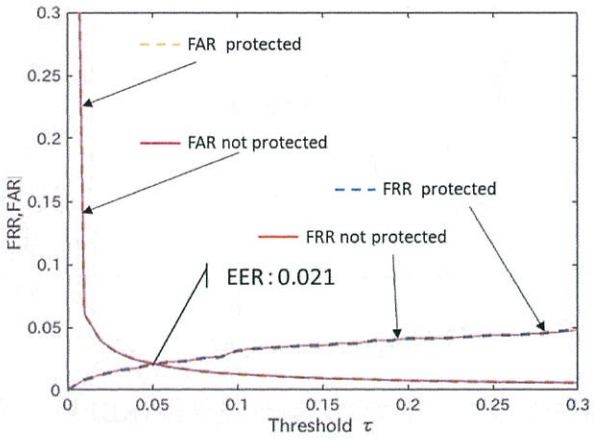


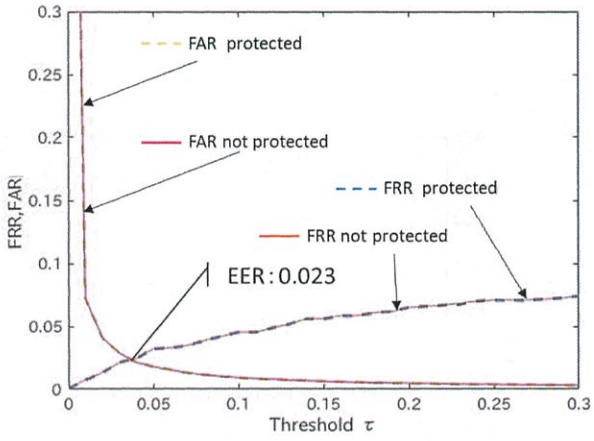
図 11: テンプレートが流出した場合の FAR (RBF カーネル)

4.2.2 ブロックベース暗号化による保護法

次にブロックベース暗号化によって画像を保護した場合の実験結果を示す. 先に述べたとおり, ネガポジ変換を含むブロックベース暗号化は z-score normalization の基では, ランダムユニタリ行列の一つであると考えられる. 故に各クライアントにて共通の鍵を用いてブロックベース暗号化を実行した場合, 認証性能は保護されていない元画像を用いた場合と同等の結果を得ることがわかる. (図 12) . 次に各クライアントで異なる鍵を利用した場合の実験結果を図 13 に示す. この鍵の選択においてはランダムユニタリ行列による保護法と同様に, テンプレートと鍵による 2 重認証により, 認証性能が向上する傾向を確認することができる. また図 14,15 が示す通り, ブロックベース暗号化による保護法も複数の先の実験結果と同様に, この鍵の選択の下では, 暗号化鍵や原画像が流出した場合においても, 低い FAR を維持することが確認できる.



(a) 線形カーネル ($C = 1$)



(b) RBF カーネル ($C = 34, \Upsilon = 81$)

図 12: 保護テンプレートでの認証性能評価 ($p_1 = p_2 = ... = p_N$)

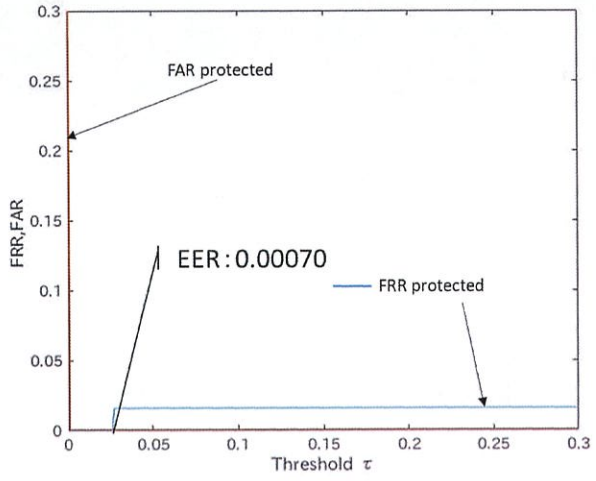


図 13: 保護テンプレートでの認証性能評価 (RBF カーネル，$p_1 \neq p_2 \neq ... \neq p_N$)

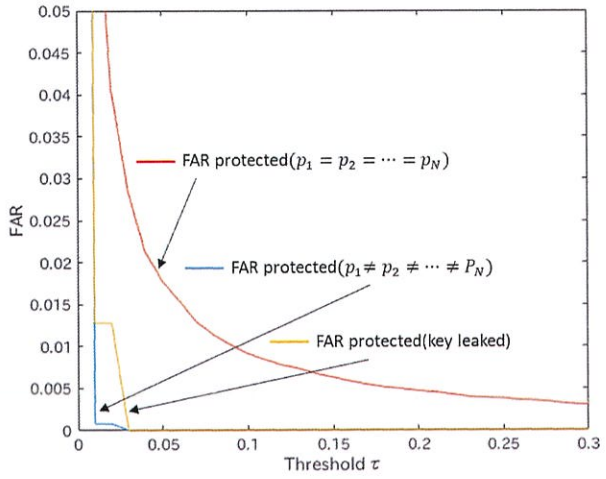


図 14: 鍵の流出を想定した場合の FAR (RBF カーネル)

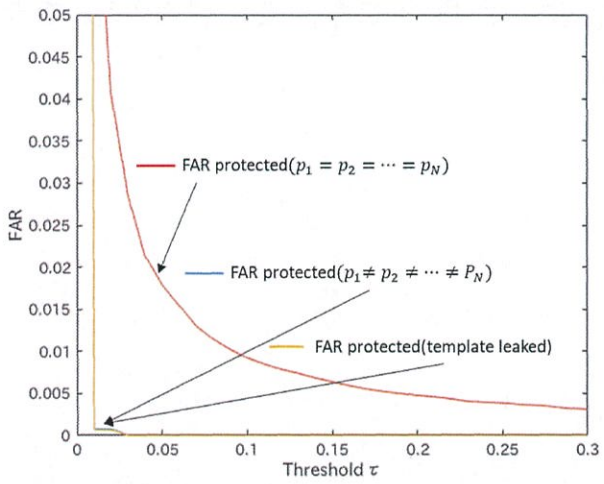


図 15: テンプレートが流出した場合の FAR (RBF カーネル)

5 おわりに

本稿では，プライバシー保護を考慮したSVMの学習法を提案した．ランダムユニタリ行列を用いたテンプレート保護法がSVMの認証性能に理論的に影響を及ぼさないことを示した． また鍵の更新の利用形態について考察し，トレーニングテンプレートとクエリテンプレートを保護する鍵をすべて共通にした場合，認証性能は，保護なしの場合と一致する．さらに登録者ごとに異なる鍵を使用した場合，認識性能は向上し，テンプレートと鍵による2重認証に相当することを述べた．また，そのような使用条件では，鍵またはテンプレートが流出した場合でも，安全性が確保できることが実験的に確認された．

6 謝辞

本研究は，著者が首都大学東京大学院システムデザイン研究科システムデザイン専攻情報通信システム学域において，多くの方々の御指導，御協力の元に進めたものであります．はじめに，指導教員である貴家仁志教授には，本研究の全般にわたり，進行，執筆，発表に関する熱心な御指導，御助言を賜りました．ここに心より厚く御礼申し上げます．また，小野 順貴教授，藤吉正明准教授には，本論文の審査を通して貴重な御助言と御指導を賜り．深く感謝の意を表します．藤吉正明准教授には，本論文の審査のみならず，研究全般に渡り，大変貴重な御助言，御指導を頂きました．また，塩田さやか助教にも，本研究のみならず，各種機器の使用法，会議の手続きなどをはじめとする各方面において大変貴重な御助言，御指導を頂きました．ここに深く感謝致します．研究を後ろから支えてくださった福島君子様，著者が在学中にお世話になった先輩，公私にわたり良き相談相手となってくれた同輩，後輩に感謝致します．最後に，これまでの学生生活を理解し，暖かい御支援を頂いた家族に心から感謝致します．

[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, 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. 66–76, 2015.

[4] 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.

[5] T. Araki, J. Furukawa, Y. Lindell, A. Nof, and K. Ohara, "High-throughput semi-honest secure three-party computation with an honest majority," in *Proceedings of ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 805–817.

[6] W. Lu, S. Kawasaki, and J. Sakuma, "Using fully homomorphic encryption for statistical analysis of categorical, ordinal and numerical data," in *IACR Cryptology ePrint Archive*, vol. 2016, 2016, p. 1163.

[7] Y. Aono and T. Hayashi and L. Phong and L. Wang, "Privacy-preserving logistic regression with distributed data sources via ho-

momorphic encryption," *IEICE Transactions on Information and Systems*, vol. E99.D, no. 8, pp. 2079–2089, 2016.

[8] 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.

[9] I. Ito and H. Kiya, "One-time key based phase scrambling for phaseonly correlation between visually protected images," in *EURASIP J. Information Security*, vol. 2009, no. 841045, 2010.

[10] J. Zhou, X. Liu, O. C. Au, and Y. Y. Tang, "Designing an efficient image encryption-then-compression system viapredictionerrorclusteringandrandompermutation," in *IEEE transactions on information forensics and security*, vol. 9, no. 1, 2014, pp. 39–50.

[11] K. Kurihara, S. Shiota, and H. Kiya, "2015 an encryption-then-compression system for jpeg standard," in *Picture Coding Symposium (PCS)*, 2015, pp. 119–123.

[12] K. Kurihara, M. Kikuchi, S. Imaizumi, S. Shiota, and H. Kiya, "An encryption-then-compression system for jpeg/motion jpeg standard," in *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 98, no. 11, 2015, pp. 2238–2245.

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

[14] T. Chuman, K. Kurihara, and H. Kiya, "Security evaluation for block scrambling-based etc systems against extended jigsaw puzzle

solver attacks," in *2017 IEEE International Conference on Multimedia and Expo (ICME)*, 2017, pp. 229–234.

[15] T. Chuman, K. Iida, and H. Kiya, "Image manipulation on social media for encryption-then-compression systems," in *2017 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*, 2017.

[16] 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. E101.D, no. 1, pp. 37–44, 2018.

[17] C. Rathgeb, and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," in *EURASIP J. Information Security*, vol. 2011, no. 1, 2011, pp. 1–25.

[18] K. Nandakumar, A. K. Jain, "Biometric template protection: Bridging the performance gap between theory and practice," in *Signal Processing Magazine, IEEE*, vol. 32, no. 5, 2015, pp. 88–100.

[19] S. Rane, "Standardization of biometric template protection," in *Signal Processing Magazine, IEEE*, vol. 21, no. 4, 2014.

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

[21] I. Nakamura, Y. Tonomura, and H. Kiya, "Unitary transform-based template protection and its properties," in *European Signal Processing Conference*, vol. SIPA-P3.4, 2015, pp. 2466–2470.

[22] I. Nakamura, Y. Tonomura, and H. Kiya, "Unitary transform-based template protection and its application to l2-norm minimization

problems," in *IEICE Transactions on Information and Systems*, vol. E99-D, no. 1, 2016, pp. 60–68.

[23] 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," in *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 23, no. 6, 2001, pp. 643–660.

[24] 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. E98.A, no. 11, pp. 2238–2245, 2015.

[25] K. Kurihara, O. Watanabe, and H. Kiya, "An encryption-then-compression system for jpeg xr standard," in *2016 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)*, 2016, pp. 1–5.

[26] 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. E100.D, no. 1, pp. 52–56, 2017.

[27] W. Sirichotedumrong, T. Chuman, S. Imaizumi, and H. Kiya, "Grayscale-based block scrambling image encryption for social networking services," in *2018 IEEE International Conference on Multimedia and Expo (ICME)*, 2018.

[28] A. Jain, K. Nandakumar, and A. Ross, "Score normalization in multimodal biometric systems," *Pattern Recognition*, vol. 38, no. 12, pp. 2270 – 2285, 2005.

著者紹介　前川 貴大

平 6 (1994) 年 4 月 長崎県生まれ.
平 22 (2010) 年 3 月 市立桜が原中学校卒業.
平 25 (2013) 年 3 月 県立大村高等学校卒業.
平 29 (2017) 年 3 月 首都大学東京 システムデザイン学部 卒業.
平 31 (2019) 年 3 月 首都大学東京大学院 システムデザイン研究科
情報通信システム学域 博士前期課程 修了見込.

発表論文

[1] 前川貴大, 栗原健太, 貴家仁志, "JPEG 画像の Encryption-then-Compression システムに基づくソーシャルネットワーキングサービスにおけるプライバシー保護," 画像工学研究会, vol.116, no.464, pp.7-12, 2017

[2] 前川貴大, 木下裕磨, 塩田さやか, 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," 電子情報通信学会 画像工学研究会, vol.117, no.200, pp.13-18, 2017

[3] Takahiro MAEKAWA, Ayana KAWAMURA, Yuma KINOSHITA, Hitoshi KIYA, "Privacy-Preserving SVM Computing in the Encrypted Domain," Proc. APSIPA Annual Summit and Conference, Honolulu, Hawaii, USA, 13th November, 2018.

[4] Takahiro MAEKAWA, Takayuki NAKACHI, Sayaka SHIOTA, Hitoshi KIYA, "Privacy-Preserving SVM Computing by Using Random Unitary Transformation," Proc. IEEE International Symposium on Intelligent Signal Processing and Communication Systems, Ishigaki Island, Okinawa, Japan, 28th November, 2018.