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

信学技報
TECHNICAL REPORT OF IEICE.

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

前川　貴大† 　木下裕磨† 　塩田さやか† 　貴家　仁志†

† 首都大学東京　〒 191-0065 東京都日野市旭ヶ丘 6-6

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テンプレートを用いた，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．ここで，テンプレートとは，画像や生体情報などから抽出された特徴量を意味する．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テンプレート保護法は，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，保護なしのテンプレート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．

キーワード　ユニタリ変換，カーネル法，SVM，テンプレート保護法，生体認証

Privacy-preserving SVM processing by using random unitary transformation

Takahiro MAEKAWA†, yuma KINOSHITA†, sayaka SHIOTA†, and Hitoshi KIYA†

† Faculty of System Design．Tokyo Metropolitan University 6-6，Asahigaoka，Hino-shi，191-0065 Japan

Abstract　In this paper,we propose a privacy-preserving SVM processing method with templates protected by using a random unitary transformation, and evaluate the effectiveness of the proposed scheme, where templates mean features extracted from images or biometric traits. 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 accident. Because of such a situation, this paper considers privacy-preserving SVM processing. It is shown that the unitary transformation-based template protection method enables us to not only protect templates, but also have the same classification performance as that of SVM processing with unprotected templates. Moreover, we consider how to update/assign secret keys, and then describe that it is possible to provide a higher performance than with unprotected templates. Some face recognition experiments are carried out as a SVM classification sheme to experimentally confirm the effectiveness of the method.

Key words　unitary transform，kernel method，SVM，template protection method，biometrics

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]．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ーン（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，いわゆる秘密計算が盛んに研究されている [2]- [4]．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 [5]- [10]．しかし，それらの手法では，SVM への適用は検討されていない．

以上の背景から，本稿では，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 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]- [14]，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．提案法は，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．またテンプレート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がある．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

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

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

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．また関数 $\mathrm{sign}(u)$ 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．

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．

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

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 ($\boldsymbol{\omega} \in \mathcal{F}$)．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，

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

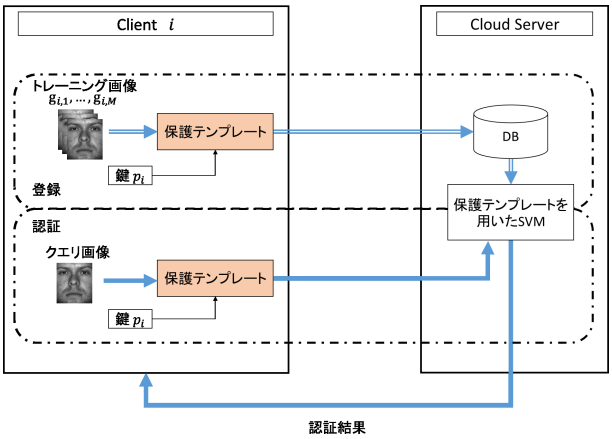


図 1　プライバシーを保護を考慮したアーキテクチャ

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 $\mathrm{g}_{i,j}, j = 1, ..., M$ 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．

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 [13] [14]．

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 [15]- [17].

3.2 保護テンプレートのカーネル法への適用

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 [13]. 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

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

特徴 2　：　内積の保存

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

特徴 3　：　相関係数の保存

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

カーネル関数にランダムユニタリ行列を用いたテンプレート保護を適用する場合を考える．RBF カーネルの場合、提案法の特徴 1 により次式が成立する．

$$K(\hat{\mathbf{f}}_{i,j}, \hat{\mathbf{f}}_{s,t}) = \exp(-\frac{\|\hat{\mathbf{f}}_{i,j} - \hat{\mathbf{f}}_{s,t}\|_2}{\sigma^2}) \tag{10}$$

$$= \exp(-\frac{\|\mathbf{f}_{i,j} - \mathbf{f}_{s,t}\|_2}{\sigma^2}) = K(\mathbf{f}_{i,j}, \mathbf{f}_{s,t}) \tag{11}$$

RBF カーネルに限らず，代表的なカーネルの多くは，同様に，

$$K(\hat{\mathbf{f}}_{i,j}, \hat{\mathbf{f}}_{s,t}) = K(\mathbf{f}_{i,j}, \mathbf{f}_{s,t}) \tag{12}$$

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 (12) 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

$$\begin{aligned} &\max_{\alpha} \ -\frac{1}{2}\sum_{\substack{i,s\in N\\ j,t\in M}} \alpha_{i,j}\alpha_{s,t}y_{i,j}y_{s,t}\phi(\hat{\mathbf{f}}_{i,j})^T\phi(\hat{\mathbf{f}}_{s,t}) + \sum_{\substack{i\in N\\ j\in M}}\alpha_{i,j} \\ &s.t. \ \sum_{\substack{i\in N\\ j\in M}} \alpha_{i,j}y_{i,j} = 0 \\ &0 \leqq \alpha_{i,j} \leqq C, \ i \in N \end{aligned} \tag{13}$$

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．

$$\begin{aligned} &\max_{\alpha} \ -\frac{1}{2}\sum_{\substack{i,s\in N\\ j,t\in M}} \alpha_{i,j}\alpha_{s,t}y_{i,j}y_{s,t}\phi(\hat{\mathbf{f}}_{i,j})^T\phi(\hat{\mathbf{f}}_{s,t}) + \sum_{\substack{i\in N\\ j\in M}}\alpha_{i,j} \\ &= \max_{\alpha} \ -\frac{1}{2}\sum_{\substack{i,s\in N\\ j,t\in M}} \alpha_{i,j}\alpha_{s,t}y_{i,j}y_{s,t}K(\mathbf{f}_{i,j}, \mathbf{f}_{s,t}) + \sum_{\substack{i\in N\\ j\in M}}\alpha_{i,j} \\ &s.t. \ \sum_{\substack{i\in N\\ j\in M}} \alpha_{i,j}y_{i,j} = 0 \\ &0 \leqq \alpha_{i,j} \leqq C, \ i \in N \end{aligned} \tag{14}$$

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．

3.3 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．

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．

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．また，テンプレート間での異なる鍵の使用は，保護テンプレートの安全性の向上にも貢献する．

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，

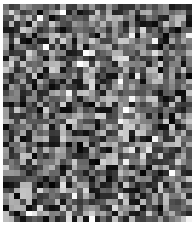
$$\hat{\mathbf{f}}^{'}_{i,j} = \mathbf{Q}_{p'_i}\hat{\mathbf{f}}_{i,j} \tag{15}$$

(a)person1

(a)person2

図 2　Extended Yale Face Database B の例

(a) 原画像 (テンプレート)



(b) 保護テンプレート

図 3　保護テンプレートの生成例

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

$$\hat{\mathbf{f}}_{i,j}^{'} = \mathbf{Q}_{p_i''}\mathbf{f}_{i,j} \tag{16}$$

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 [18] 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 2 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 Υ 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 [19]．192×168 の画像を 38×32 にダウンサンプリングして，1254 次元のテンプレートベクトルを生成した．図 3 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

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

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．

$$if\ S_q \leqq \tau\ then\ accept;\ else\ reject \tag{17}$$

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．

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 4 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 5 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．3.3 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 5 及び図 6 から，図 4 に比べ認証性能が向上することがわかる．

C. 鍵の流出

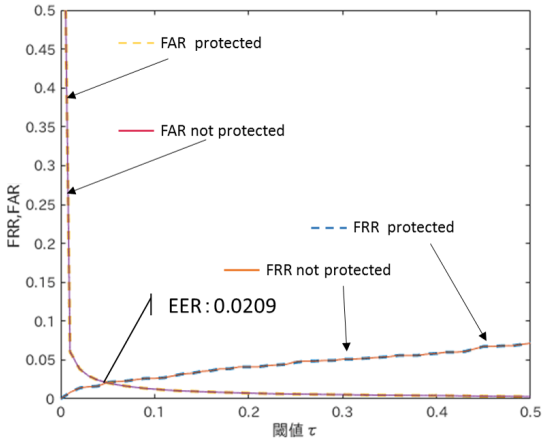
次に，秘密鍵が流出した場合の認識性能（FAR）を図 7 に示す．この特性は，鍵 p_i が，クライアント i からテンプレート $\mathrm{g}_{s,j}, s \neq i$ を持つ他のクライアント s に流出した場合を想定した実験である．クライアント s が，鍵 p_i とテンプレート $\mathrm{g}_{s,j}$ を用いて保護テンプレートを作成し，$\mathrm{g}_{i,j}$ の保護テンプレートに成りすます認証攻撃である．図 7 に示したように，図 5 に比べ少し FAR は上昇するが，低い値を維持することがわかる．

一方，図 8 はテンプレート $\mathrm{g}_{i,j}$ 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 $\mathrm{g}_{i,j}$ を用いて保護テンプレートを作成し，$\mathrm{g}_{i,j}$ の保護テンプレートに成りすます認証攻撃である．図 7 の場合と同様に，図 5 に比べ FAR は上昇するが，低い値を維持している．

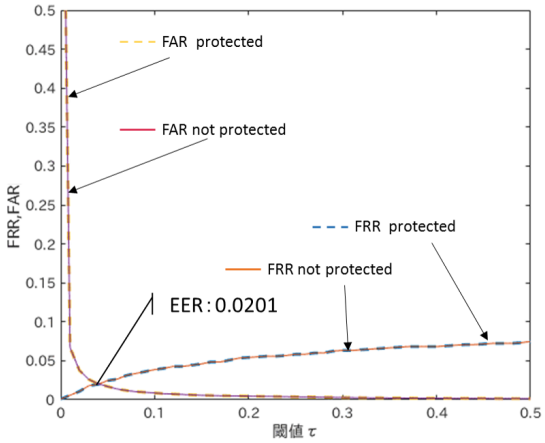
以上の傾向は，使用するランダム行列に依存することが予想され，今後種々のランダム行列のもとで追加実験を行う予定である．

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



(a) 線形カーネル



(b) RBF カーネル

図 4　保護テンプレートでの認証性能評価
$(p_1 = p_2 = ... = p_N)$

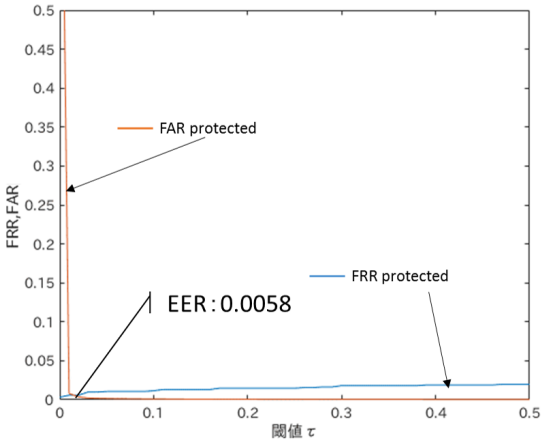


図 5　保護テンプレートでの認証性能評価
(RBF カーネル，$p_1 \neq p_2 \neq ... \neq p_N$)

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

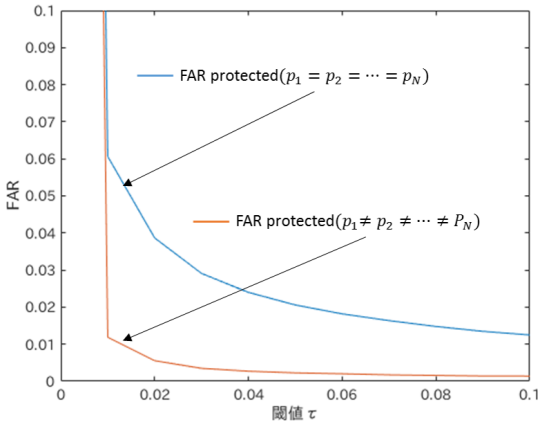


図 6　FAR の比較 (RBF カーネル)

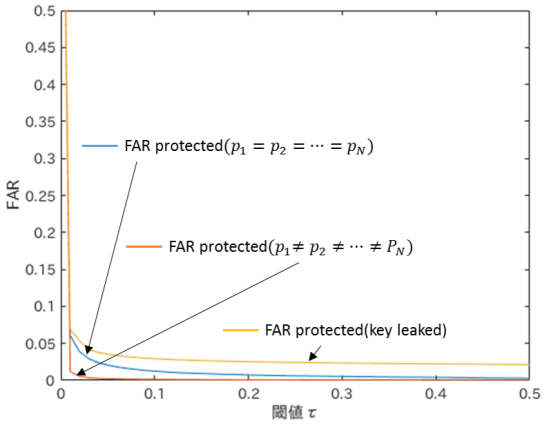


図 7　鍵の流出を想定した場合の FAR (RBF カーネル)

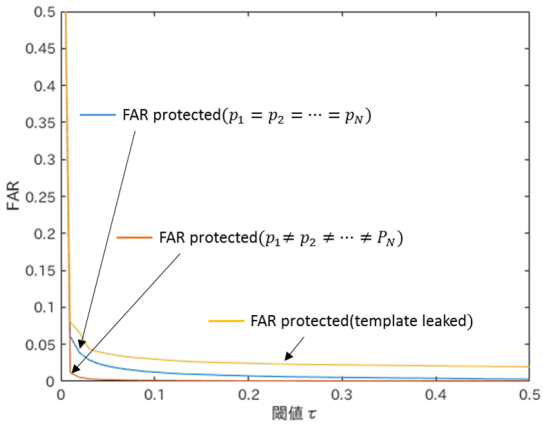


図 8　テンプレートが流出した場合の FAR (RBF カーネル)

でも，安全性が確保できることが実験的に確認された．

今後は，ランダムユニタリ行列の持つ自由度に着目し，最適なランダム行列の生成を考察する予定である．

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, e7, 2014.

[2] R. Lazzeretti and M. Barni, "Private Computing with Gar-

bled Circuits [Applications Corner]," in IEEE Signal Processing Magazine, vol. 30, no. 2, pp. 123-127, March 2013.
[3] M. Barni, G. Droandi and R. Lazzeretti, "Privacy Protection in Biometric-Based Recognition Systems: A marriage between cryptography and signal processing," in IEEE Signal Processing Magazine, vol. 32, no. 5, pp. 66-76, Sept. 2015.
[4] R. L. Lagendijk, Z. Erkin and M. Barni, "Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation," in IEEE Signal Processing Magazine, vol. 30, no. 1, pp. 82-105, Jan. 2013.
[5] I. Ito and H. Kiya, “One-Time Key Based Phase Scrambling for PhaseOnly Correlation between Visually Protected Images,” EURASIP J. Information Security, vol.2009, no.841045, Jan. 2010.
[6] I Ito and H Kiya,“Phase-only correlation based matching in scrambled domain for preventing illegal matching,” Transactions on data hiding and multimedia security V, pp.51-69,2010.
[7] J. Zhou, X. Liu, O. C. Au, and Y. Y. Tang, “Designing an efficient image encryption-then-compression system viapredictionerrorclusteringandrandompermutation,” IEEE transactions on information forensics and security, vol. 9, no. 1, pp. 39-50, 2014.
[8] 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.
[9] K. Kurihara, S. Imaizumi, S. Shiota, and H. Kiya, “An encryption-then-compression system for lossless image compressionstandards,” IEEEtransactionsoninformation and systems, vol. E100-D, no. 1, pp. 52-56, 2017.
[10] T. Chuman, K. Kurihara, and H. Kiya,“On the Security of Block Scrambling-based ETC Systems against Jigsaw Puzzle Solver Attacks,”Proc. IEEE International Conference on Acoustics, Speech and Signal Processing, pp.2157-2161, New Orleans, LA, USA, 5th March, 2017.
[11] K. Nandakumar, A. K. Jain, “Biometric Template Protection: Bridging the Performance Gap Between Theory and Practice.” Signal Processing Magazine, IEEE, vol.32, no.5, pp.88-100, 2015.
[12] C. Rathgeb, and A. Uhl,“A survey on biometric cryptosystems and cancelable biometrics,” EURASIP J. Information Security, vol.2011, no.1, pp.1-25, 2011.
[13] 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.
[14] I. Nakamura, Y. Tonomura, and H. Kiya, “Unitary Transform-Based Template Protection and Its Application to l2-norm Minimization Problems,” IEICE Trans. Inf. & Sys., vol.E99-D, no.1, pp.60-68, Jan.2016.
[15] 斉藤 裕子, 塩田 さやか, 貴家 仁志,“テンプレート保護のためのランダム・ユニタリ行列の生成法,”電子情報通信学会 信号処理研究会, vol.116, no.95, (no. SIP2016-48), pp.73-78, Jun.2016.
[16] Y. Saito, I. Nakamura, S. Shiota, and H. Kiya, “An Efficient Random Unitary Matrix for Biometric Template Protection,”Proc. International Conference on Soft Computing and Intelligent Systems and International Symposium on Advanced Intelligent Systems, Sapporo, Hokkaido, Japan, 27th August, 2016.
[17] 中村 維吹, 斉藤 裕子, 塩田 さやか, 貴家 仁志,“ユニタリ変換を用いたセキュアなカーネル法に基づくクラス分類,”電子情報通信学会 画像工学研究会,vol.115, no.458, (no.ITS2015-59), pp.17-22, Feb.2016.
[18] 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, Jun. 2001.
[19] 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, Feb. 2009.