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.

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

中村　維吹†　　斉藤　裕子†　　塩田さやか†　　貴家　仁志†

† 首都大学東京システムデザイン研究科　〒 191–0065 東京都日野市旭が丘 6–6
E-mail: †{nakamura-ibuki,saito-yuko}@ed.tmu.ac.jp, ††sayaka@tmu.ac.jp, †††kiya@sd.tmu.ac.jp

あらまし　本稿では，テンプレート保護法の一つである，ユニタリ変換に基づく保護法を考察する．ここで，テンプレートとは，生体情報から抽出された特徴量を意味する．本稿では，カーネル法に対してランダムユニタリ変換に基づく保護法による保護テンプレートを適用し，その認証性能について理論的に検証を行う．先の研究によって，ランダムユニタリ変換が保護テンプレート間のユークリッド距離と，オリジナルテンプレート間のユークリッド距離とが等しくなる特徴や，l^2 ノルム最小化問題に対して認証性能の劣化を生じさせない特徴を持つことが示されている．本稿では，ランダムユニタリ変換に基づく保護法がカーネル法を用いた認証に対して，認証性能の劣化を生じさせない新たな特徴を示す．提案法は，保護テンプレートに対してオリジナルテンプレートによる認証と同一の手順を適用可能であり，かつその場合もオリジナルテンプレートと同一の認証結果を得ることが可能である．最後にカーネル法の一例として，カーネル固有顔を用いた顔認証実験を行い，本稿における理論検証の正当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，カーネル固有顔，テンプレート保護法，生体認証

Secure classification based on kernel method using unitary transformation

Ibuki NAKAMURA†, Yuko SAITOU†, Sayaka SHIOTA†, and Hitoshi KIYA†

† Tokyo Metropolitan University Information and Communication Systems　6-6 Asahigaoka , Hino-shi, Tokyo, 191-0065 Japan
E-mail: †{nakamura-ibuki,saito-yuko}@ed.tmu.ac.jp, ††sayaka@tmu.ac.jp, †††kiya@sd.tmu.ac.jp

Abstract　This study considers a template protection scheme based on an random unitary transformation, where the template consists of the features extracted from the biometric trait. In this paper, we apply the template protection scheme based on an unitary transformation to a kernel-based classification, and the recognition performance is theoretically considered. Previous studies showed that the Euclidean distance between templates protected by a unitary transform is the same as that between original ones, and there is no degradation of the recognition performances of using l^2-norm minimization. In this study, we show a new property that there is no degradation of the recognition performances of using a kernel-based classification. The proposed method can obtain the same recognition performance as authentication with original templates even though protected templates are applied to the same procedure as the authentication with original templates. We perform some face recognition experiments of using a kernel eigenface as one of the kernel-based classification schemes experimentally to confirm the validity of the theory.
Key words　unitary transform, kernel method, kernel eigenface, template protection method, biometrics

1. ま え が き

ユーザー認証は，様々なシステムにとって，重要な作業である．パスワードや IC カードによる認証は，それらの共有や置き忘れ，盗難等が容易である点から，十分に信頼できるシステムであるとはいえない．それに比べて，生体認証は，その様々な優れた特徴により，システムのユーザー認証において，信頼性の高い方法であるといえる．しかし，生体情報は，個人情報であり，かつ原理的に再発行が困難であるなど，セキュリティに関する幾つかの問題を抱えている．本稿では，その中でも，最も重要な課題の一つである，テンプレートのセキュリティに着目している．テンプレートのセキュリティに関する研究は，

認証性能を向上させる研究に並んで，多数行われている [1,2]．加えて，テンプレート保護法のセキュリティやプライバシーの評価基準は，ISO/IEC WD 30136 として標準化が進んでいる [3]．

様々な論文で提案されている，テンプレートの保護法は，大別すると，特徴変換に基づく方法と，暗号化に基づく方法とに分けられる [4,5]．ユニタリ変換に基づくテンプレート保護法は特徴変換に基づく方法における，可逆方式 [6,7] に分類される．一般に，非可逆方式が，鍵の配送が必要無く，セキュリティの観点で良い特徴を持つとされるが，決定論的に認証性能が低下しないと保証することは困難である [8,9]．また，特徴変換に基づく保護法には完全秘匿性を持ったテンプレート保護法がある [10,11]．しかしこの保護法の認証は相関に基づく方法に限定されている．一方，可逆方式に分類されるユニタリ変換に基づくテンプレート保護法は，変換のパラメータを秘密鍵として安全に保護する必要があるが，いくつかの優れた特徴を持っている．たとえば，オリジナルテンプレート間のユークリッド距離と保護テンプレート間のユークリッド距離が一致することが挙げられる．[12–14]

本稿では，カーネル法に対してランダムユニタリ変換に基づく保護法による保護テンプレートを適用し，その認証性能について理論的に検証を行う．カーネル法は，サポートベクターマシンやスパース表現に基づく認証法等のクラス分類手法や主成分分析やフィッシャーの線形判別等の特徴量生成法の性能を向上させるために広く用いられている方法である [15–17]．まず，オリジナルテンプレートから求められるカーネル関数の結果を，ランダムユニタリ変換に基づく保護法による保護テンプレートを用いて得ることが出来ることを示す．次にカーネル法への適用の一例として，カーネル固有顔 [17] の重みを保護による劣化なしに求められることを示す．提案法は，オリジナルテンプレートを用いた場合と同じ認証の手順によって同じ結果を得られるため，既存のカーネル法を用いた認証のテンプレートを保護テンプレートに置き換えることが可能である．最後に，線形結合表現を用いた生体認証法における l^1 ノルム最小化問題の解を用いた顔認証実験によって，本稿における理論検証の正当性を確認する．

2. 準　　備

2.1 生体認証システム

本稿では，図 1 のような，共通のパラメータ $\mathbf{p}$ によって保護を行う，生体認証システムについて考察する．登録時には，まず，トレーニングサンプルから，テンプレートと呼ばれる特徴量 $\mathbf{f}_{i,j}$ を抽出をする．さらに，テンプレートに特徴変換 $\mathrm{T}(\cdot)$ を適用して，保護テンプレート $\hat{\mathbf{f}}_{i,j}$=$\mathrm{T}(\mathbf{f}_{i,j},\mathbf{p})$ の生成を行い，データベースへ，保護テンプレートのみを登録する．また，認証時，ユーザー i は，パラメータ $\mathbf{p}$ を認証システムに渡し，クエリの特徴量 $\mathbf{y}_i$ に，登録時と同じ特徴変換 $\mathrm{T}(\cdot)$ を適用する．最後に，変換されたクエリ $\mathrm{T}(\mathbf{y}_i,\mathbf{p})$ と，データベースとを用いて，認証を行う．

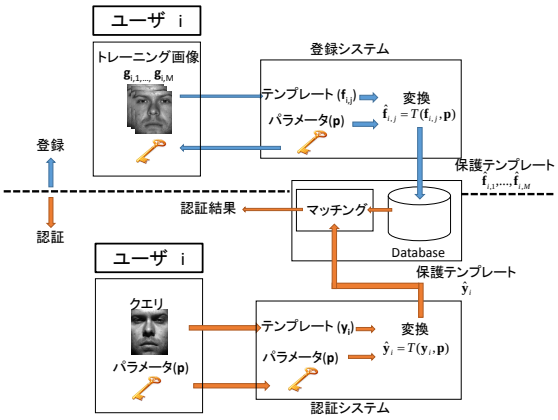


図 1　生体認証システム

2.2 カーネル法

カーネル法と、カーネル固有顔を用いた認証法について示す．

カーネル法は，特徴ベクトルを高次元の特徴空間上に写像し，その特徴空間上でパターン認識を行う．次元 N の特徴ベクトル $\mathbf{f}_{i,j}$ を高次元 S の特徴空間上へ写像する関数 $\mathbf{\Gamma}$ を考える．

$$\mathbf{\Gamma}:\mathbf{f}_{i,j}\in\mathbb{R}^N\rightarrow\mathbf{\Gamma}(\mathbf{f}_{i,j})=[\gamma_1(\mathbf{f}_{i,j}),...,\gamma_S(\mathbf{f}_{i,j})]^T\in\mathbb{R}^S \tag{1}$$

ただし，$S>N$ とする．このとき高次元特徴空間上での内積は以下のように，カーネル関数 $k(\cdot,\cdot)$ によって低次元特徴空間上の計算で求めることができる．

$$\langle\mathbf{\Gamma}(\mathbf{f_{i,j}}),\mathbf{\Gamma}(\mathbf{f_{s,t}})\rangle=k(\mathbf{f_{i,j}},\mathbf{f_{s,t}}) \tag{2}$$

ただし，$\langle\mathbf{x},\mathbf{y}\rangle$ は $\mathbf{x}$ と $\mathbf{y}$ との内積である．カーネル関数には Radial Basis Function(RBF) カーネルや多項式カーネルがある．それらのカーネル関数を以下に示す

$$k(\mathbf{f}_{i,j},\mathbf{f}_{s,t})=exp(-\frac{||\mathbf{f}_{i,j}-\mathbf{f}_{s,t}||_2}{\sigma^2}) \tag{3}$$

$$k(\mathbf{f}_{i,j},\mathbf{f}_{s,t})=(l+\mathbf{f}_{i,j}^*\mathbf{f}_{s,t})^d \tag{4}$$

ただし，σ,l,d はそれぞれ関数のパラメータである．

2.3 固　有　顔

固有顔の求め方を実行する [18]．まず、E 人の登録者の中の i 番目の人の，M 枚あるトレーニングトレーニングサンプルの j 番目の画像 $\mathbf{g}_{i,j}$ から，トレーニングテンプレート $\mathbf{f}_{i,j}\in\mathbb{R}^N, i=1,...,E, j=1,...,M$ を抽出し、その平均が以下のように計算される．

$$\mathbf{\Psi}=\frac{1}{EM}\sum_{i=1}^{E}\sum_{j=1}^{M}\mathbf{f}_{i,j} \tag{5}$$

ここで、$\mathbf{\Psi}\in\mathbb{R}^N$ を平均顔と呼ぶ．次に，各トレーニングテンプレートと平均顔との差を求める．すなわち，

$$\mathbf{\Phi}_{i,j}=\mathbf{f}_{i,j}-\mathbf{\Psi}. \tag{6}$$

固有顔は，$\mathbf{\Phi}_{i,j}$ から求められる共分散行列 $\mathbf{C}=\frac{1}{EM}\sum_{i=1}^{E}\sum_{j=1}^{M}\mathbf{\Phi_{i,j}}\mathbf{\Phi_{i,j}}^T$ から以下のように与えられる．

$$\lambda\mathbf{v}=\mathbf{C}\mathbf{v} \tag{7}$$

ただし，$\mathbf{v}$ は固有顔，μ はその固有値である．

2.4 カーネル固有顔

カーネル固有顔では，各特徴量ベクトル $\mathbf{\Phi}_{i,j}$ は $\mathbb{R}^n$ から高次元特徴空間 $\mathbb{R}^S$ に非線形写像関数 $\Gamma : \mathbb{R}^N \rightarrow \mathbb{R}^S$ によって写像され，高次元特徴空間上で固有顔が求められる [19]．$\Gamma(\mathbf{\Phi}_{i,j})$ の共分散行列 $\mathbf{C}^\Gamma$ の固有ベクトルは以下の固有値問題を解くことで得られる．

$$\lambda^\Gamma \mathbf{v}^\Gamma = \mathbf{C}^\Gamma \mathbf{v}^\Gamma \tag{8}$$

ただし，$\mu \geqq 0$，$\mathbf{v} \in S \setminus \{\mathbf{0}\}$．ここで，$\mathbf{C}^\Gamma \mathbf{v}^\Gamma$ は以下のように変形することができる．

$$\begin{aligned}\mathbf{C}^\Gamma \mathbf{v}^\Gamma &= (\frac{1}{EM}\sum_{i=1}^{E}\sum_{j=1}^{M}\mathbf{\Gamma}(\mathbf{\Phi_{i,j}})\mathbf{\Gamma}(\mathbf{\Phi_{i,j}})^T)\mathbf{v}^\Gamma \\ &= \frac{1}{EM}\sum_{i=1}^{E}\sum_{j=1}^{M}\langle\mathbf{\Gamma}(\mathbf{\Phi_{i,j}}), \mathbf{v}^\Gamma\rangle\mathbf{\Gamma}(\mathbf{\Phi_{i,j}})\end{aligned} \tag{9}$$

全ての $\mu \neq 0$ である解 $\mathbf{v}^\Gamma$ は，$\mathbf{\Gamma}(\mathbf{\Phi_{1,1}})$,...,$\mathbf{\Gamma}(\mathbf{\Phi_{E,M}})$ の張る空間に存在する．よって，式 (8) は次式と同等である．

$$\lambda\langle\mathbf{\Gamma}(\mathbf{\Phi_{i,j}}), \mathbf{v}\rangle = \langle\mathbf{\Gamma}(\mathbf{\Phi_{i,j}}), \mathbf{C}^\Gamma\mathbf{v}\rangle. \tag{10}$$

また，以下の関係を満たす係数 $\alpha_{i,j}$ が存在する．

$$\mathbf{v}^\Gamma = \sum_{i=1}^{E}\sum_{j=1}^{M}\alpha_{i,j}\Gamma(\mathbf{\Phi}_{i,j}) \tag{11}$$

式 (9), (10)，(11) より，次式の関係を得る．

$$\begin{aligned}&\lambda \sum_{i=1}^{E}\sum_{j=1}^{M}\alpha_{i,j}\langle\mathbf{\Gamma}(\mathbf{\Phi_{k,l}}), \mathbf{\Gamma}(\mathbf{\Phi_{i,j}})\rangle \\ &= \frac{1}{EM}\sum_{i=1}^{E}\sum_{j=1}^{M}\alpha_{i,j}\langle\mathbf{\Gamma}(\mathbf{\Phi_{k,l}}), \sum_{t=1}^{E}\sum_{s=1}^{M}\mathbf{\Gamma}(\mathbf{\Phi_{t,s}})\rangle \\ &\qquad \cdot\langle\mathbf{\Gamma}(\mathbf{\Phi_{t,s}}), \mathbf{\Gamma}(\mathbf{\Phi_{i,j}})\rangle\end{aligned} \tag{12}$$

式 (12) の固有値問題は高次元特徴空間に射影した特徴量ベクトルの内積計算のみによって与えられる．これは，カーネル関数によって低次元空間の特徴量を用いて計算できることを意味している．ここで $\mathbf{K} \in \mathbb{R}^{EM\times EM}$ を定義する，ただし $[K]_{(i,j),(s,t)} = k(\mathbf{\Phi_{i,j}}, \mathbf{\Phi_{s,t}})$．$\mathbf{K}$ を用いて，式 (12) は次のように表せる．

$$\lambda EM\mathbf{K}\alpha = \mathbf{K}^2\alpha, \tag{13}$$

ただし，$\alpha = [\alpha_{1,1}, ..., \alpha_{E,M}]^T$,$\alpha_{i,j} = [\alpha_{i,j}^{(1)}, ..., \alpha_{i,j}^{(EM)}]^T$ ．式 (13) の解を得るためには，次式の固有値問題を解けばよい．

$$\lambda EM\alpha = \mathbf{K}\alpha, \tag{14}$$

実際の認証には，固有値が上位 $(EM)'$ 個 ($(EM)' < EM$) の固有ベクトルが用いられる．入力されたクエリテンプレート $\mathbf{y}$ を用い，以下の手順で各固有顔とクエリテンプレート間の重み ω_k を計算する．

$$\begin{aligned}\omega_k &= \langle\mathbf{v}_k^T, \Gamma(\mathbf{\Phi}_y)\rangle \\ &= \sum_{i=1}^{E}\sum_{j=1}^{M}\alpha_{i,j}^{(k)}k(\mathbf{\Phi}_{i,j}, \mathbf{\Phi}_y)\end{aligned} \tag{15}$$

ただし，$k = 1, ..., (EM)'$ である．重みベクトル $\mathbf{\Omega}_y = [\omega_1, ..., \omega_{(EM')}]^T$ は，各固有顔とクエリテンプレートとの関係を表している．

2.5 線形結合表現を用いた生体認証

生体認証の代表的な方法の一つに，トレーニングテンプレートとクエリテンプレートの線形結合に基づく方法 [20] がある．本稿では，カーネル固有顔の重みベクトルを用い，この方法によって認証を行う．

まず $\mathbf{\Omega}_{i,j}$ を，i 番目の人の j 番目のテンプレートから生成された重みとして定義する．ただし，$j = 1, 2, ..., M$．E 人の登録者の中の，i 番目の人の M 個のトレーニングテンプレートは，$\mathbf{D}_i = [\mathbf{\Omega}_{i,1}, \mathbf{\Omega}_{i,2}, ..., \mathbf{\Omega}_{i,M}], i = 1, 2, ..., E$，と与えられる．$i$ 番目の人に属するテンプレートから得た重み $\mathbf{y}$ は，i 番目の人の重みの線形近似できると以下のように仮定する．

$$\mathbf{y} = \mathbf{\Omega}_{i,1}x_{i,1} + \mathbf{\Omega}_{i,2}x_{i,2} + ... + \mathbf{\Omega}_{i,M}x_{i,M} = \mathbf{D}_i\mathbf{x}_i, \tag{16}$$

ここで，$x_{i,j}$ は係数値である．また，E 人全ての重みを用いて，y は以下のように表現される．

$$\mathbf{y} = \mathbf{D}_1\mathbf{0} + ... + \mathbf{D}_{i-1}\mathbf{0} + \mathbf{D}_i\mathbf{x}_i + \mathbf{D}_{i+1}\mathbf{0} + ... + \mathbf{D}_E\mathbf{0} = \mathbf{D}\mathbf{x}_0, \tag{17}$$

ここで，$\mathbf{D} = [\mathbf{D}_1, \mathbf{D}_2, ..., \mathbf{D}_E]$,$\mathbf{x}_0 = [\mathbf{0}^T, ..., \mathbf{0}^T, \mathbf{x}_i^T, \mathbf{0}^T, ..., \mathbf{0}^T]^T$. である．ここで，$(EM)' < EM$ の関係より，$\mathbf{D}$ はランク EM を持たない事に注意する．従って，i が誰かを特定するために，式 (17) の l^1 ノルム最小化問題を解く．

$$\tilde{\mathbf{x}}_0 = \arg\min_{\mathbf{x}} ||\mathbf{x}||_1 \ \ subject\ to\ \ \mathbf{y} = \mathbf{D}\mathbf{x}. \tag{18}$$

式 (18) を解くために，近似解 $\tilde{\mathbf{x}}_0$ は，$\tilde{\mathbf{x}}_0 = [\tilde{\mathbf{x}}_1^T, \tilde{\mathbf{x}}_2^T, ..., \tilde{\mathbf{x}}_i^T, ..., \tilde{\mathbf{x}}_K^T]^T$ のように得られる．$\tilde{\mathbf{x}}_0$ は，認証結果 C を得るために用いられる．i 番目の人以外の係数をゼロにする関数 $\delta_i(\cdot)$ を，以下のように定義する．

$$\delta_i(\tilde{\mathbf{x}}_0) = [\mathbf{0}^T, ..., \mathbf{0}^T, \tilde{\mathbf{x}}_i^T, \mathbf{0}^T, ..., \mathbf{0}^T]^T. \tag{19}$$

$\delta_i(\tilde{\mathbf{x}}_0)$ を式 (16) の $\mathbf{x}_i$ に代入することで，認証結果 C は以下のように推定される．

$$r_i = ||\mathbf{y} - \mathbf{D}\delta_i(\tilde{\mathbf{x}}_0)||_2, \tag{20}$$

$$C = \arg\min_i r_i, \tag{21}$$

ここで，r_i は i 番目の人の推定二乗誤差と言う．

3. 提 案 法

3.1 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の保護は，パラメータ $\mathbf{p}$ のランダムユニタリ行列 $\mathbf{Q}_p$ による変換 T(·) よって次式のように行われる．

$$\hat{\mathbf{f}}_{i,j} = T(\mathbf{f}_{i,j}, \mathbf{p}) = \mathbf{Q}_p\mathbf{f}_{i,j} \tag{22}$$

ただし，$\mathbf{Q}_p \in \mathbb{C}^{N\times N}$ である．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]．

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保護テンプレート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 より以下の式が成り立つ．

$$\begin{aligned}k(\hat{\mathbf{f}}_{i,j},\hat{\mathbf{f}}_{s,t}) &= exp(-\frac{||\hat{\mathbf{f}}_{i,j}-\hat{\mathbf{f}}_{s,t}||_2}{\sigma^2})\\ &= exp(-\frac{||\mathbf{f}_{i,j}-\mathbf{f}_{s,t}||_2}{\sigma^2})=k(\mathbf{f}_{i,j},\mathbf{f}_{s,t})\end{aligned}\tag{23}$$

多項式カーネルの場合，提案法の特徴 2 より以下の式が成り立つ．

$$k(\hat{\mathbf{f}}_{i,j},\hat{\mathbf{f}}_{s,t})=(l+\hat{\mathbf{f}}_{i,j}^{*}\hat{\mathbf{f}}_{s,t})^{d}=(l+\mathbf{f}_{i,j}^{*}\mathbf{f}_{s,t})^{d}=k(\mathbf{f}_{i,j},\mathbf{f}_{s,t})\tag{24}$$

このことによって，以下の特徴を持つことができる．

・ 保護テンプレートを用いた場合の結果が，保護していないテンプレートを用いた場合の結果と等しくなる．

・ 保護していない場合と同じ計算手順で，等しい結果を得ることができる．

カーネル固有顔を例に，保護していない場合と同じ計算手順で等しい結果を得られることを示す．

保護テンプレート $\hat{\mathbf{f}}_{i,j}$ の平均顔が以下のように求められる．

$$\hat{\mathbf{\Psi}}=\frac{1}{EM}\sum_{i=1}^{E}\sum_{j=1}^{M}\hat{\mathbf{f}}_{i,j}\tag{25}$$

次に，各トレーニングテンプレートと平均顔との差を求める．すなわち，

$$\hat{\mathbf{\Phi}}_{i,j}=\hat{\mathbf{f}}_{i,j}-\hat{\mathbf{\Psi}}.\tag{26}$$

次に，式 (27) に保護テンプレートを適用し固有値問題を解く．

$$\hat{\lambda}EM\hat{\alpha}=\hat{\mathbf{K}}\hat{\alpha},\tag{27}$$

このとき，$\hat{\mathbf{K}}$ の要素はカーネル関数によって与えられる．すなわち，

$$\hat{K}_{(i,j),(s,t)}=k(\hat{\mathbf{\Phi}}_{i,j},\hat{\mathbf{\Phi}}_{s,t})=k(\mathbf{\Phi}_{i,j},\mathbf{\Phi}_{s,t})=K_{(i,j),(s,t)}.\tag{28}$$

よって，保護テンプレートを適用した場合の固有値問題の解，および固有値は $\hat{\alpha}=\alpha,\hat{\lambda}=\lambda$ となる．また，重み ω_k もカーネル関数によって与えられるため，以下の式が成り立つ．

$$\begin{aligned}\hat{\omega}_k &= \sum_{i=1}^{E}\sum_{j=1}^{M}\alpha_{i,j}^{(k)}k(\hat{\mathbf{\Phi}}_{i,j},\hat{\mathbf{\Phi}}_{y})\\ &= \sum_{i=1}^{E}\sum_{j=1}^{M}\alpha_{i,j}^{(k)}k(\mathbf{\Phi}_{i,j},\mathbf{\Phi}_{y})=\omega_k\end{aligned}\tag{29}$$

これにより，生成される重みベクトルが保護テンプレートの影響を受けないことが示された．

3.2 ユニタリ変換に基づく保護テンプレートの生成法

ランダムユニタリ変換 $\mathbf{Q}_p$ の生成は，グラムシュミットの直交化を用いて $\mathbf{Q}_p$ を生成する方法が一般的である [12]．しかし，グラムシュミットの直交化を用いた保護法は計算量が大きいという課題がある [13,14,21]．本稿では，複数のユニタリ行列を組み合わせることで，ランダムユニタリ行列 $\mathbf{Q}_p$ を生成する方法を用いる [13,14]．

提案するランダムユニタリ行列の生成法を以下に示す．

$$\mathbf{Q}_p=\mathbf{H}_p\mathbf{A},\tag{30}$$

ただし，$\mathbf{A}$ は離散フーリエ変換やアダマール変換等の一般的に用いられるユニタリ変換の行列であり，$\mathbf{H}_p$ は疑似乱数生成器を用い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，$\mathbf{H}_p\mathbf{A}$ は以下の式を満たす．

$$(\mathbf{H}_p\mathbf{A})^{*}(\mathbf{H}_p\mathbf{A})=\mathbf{I},\tag{31}$$

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．$\mathbf{H}_p$ にはベクトルの要素の順番を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 がある．ここで，random permutation matrix, random phase matrix の例として 4×4 行列を以下に示す．

$$\mathbf{Q}_p=\begin{pmatrix}1&0&0&0\\0&0&0&1\\0&0&1&0\\0&1&0&0\end{pmatrix}\tag{32}$$

$$\mathbf{Q}_p=\begin{pmatrix}e^{j\theta_1}&0&0&0\\0&e^{j\theta_2}&0&0\\0&0&e^{j\theta_3}&0\\0&0&0&e^{j\theta_4}\end{pmatrix}\tag{33}$$

これらの行列はユニタリ性（直交性）を持つ．グラムシュミットの直交化を用いた方法に比べて，$\mathbf{Q}_p$ の設計が容易である．加えて高速フーリエ変換 (FFT) のような高速アルゴリズムを $\mathbf{A}$ の行列計算に用いることができる．

4. シミュレーション

4.1 データベース

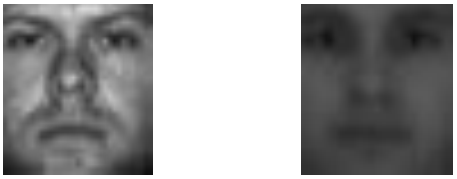
本実験では，代表的な顔画像データベースである Extended Yale Face Database B [22] を用いた．38 人の様々な照明条件で撮影された顔画像が 64 枚ずつ，計 2432 枚で構成され，すべて 192×168 のサイズに統一されている．各被験者に対する 64 枚の顔画像をトレーニングに 16 枚，クエリに 48 枚分けて実験を行った．

保護テンプレートの生成には，DFT による生成法を用い，ランダムユニタリ行列は random permutation matrix を使用した．また，本実験では，固有値の上位 $(EM)'=\{20,40,60,80\}$ 個の固有ベクトル α のみを用いた．

4.2 結果と考察

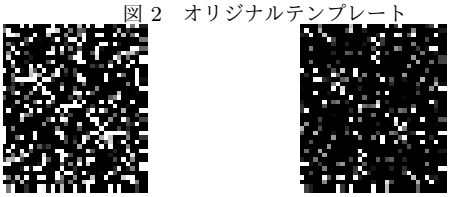
A. 特徴量の抽出法

本実験では，ダウンサンプリングにより抽出されたテンプレートに，ランダムユニタリ行列を用いた保護法を適用して，その後，カーネル固有顔により認証に用いる重みを算出する．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り [20]，192×168 の画像を 38×33 にダウンサンプリ



(a) テンプレート　　(b) 平均顔

図 2　オリジナルテンプレート



(a) テンプレート　　(b) 平均顔

図 3　保護テンプレート

ングして，1254 次元のテンプレートベクトルを生成した．図 2 と図 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と平均顔を示す．保護法を適用しない場合には，テンプレート，平均顔，のいずれも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．

B. 顔認証実験

ユニタリ変換に基づく保護法の評価を行うために，ROC(受信者操作特性) 曲線を図 4 に示す．推定二乗誤差 r_i と閾値 τ の関係を以下のように定め，ROC 曲線を得る．

$$if\ r_i \leqq \tau\ then\ 受け入れ;\ else\ 拒否. \tag{34}$$

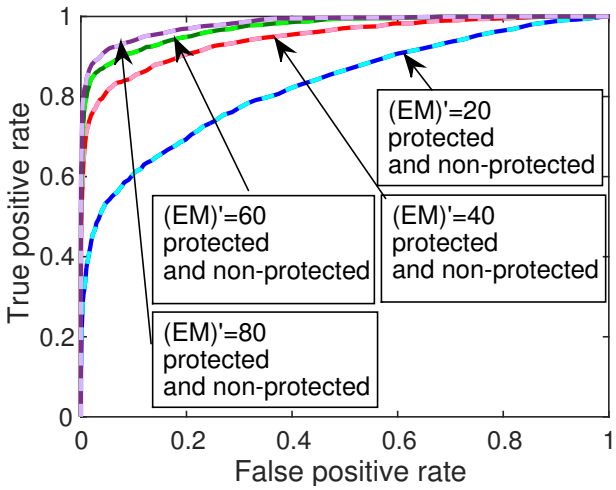
図 4 において，true positive rate は，本人受け入れ率を示し，false positive rate は，他人受け入れ率を示す．図 4(a)，(b) はそれぞれ，提案法に RBF カーネルを用いた場合，提案法に多項式カーネルを用いた場合の ROC カーブを示す．図 4(a)，(b) より，クエリとトレーニングに共通のパラメータを用いた保護テンプレートから得た結果 (protected) が，オリジナルテンプレートから得た結果 (non-protected) と完全に一致していることがわかる．理論的検証に加えこの実験結果からも，ランダムユニタリ行列を用いた保護法はカーネル固有顔を用いた認証結果に影響を与えないことがわかる．

C. ランダム射影との比較

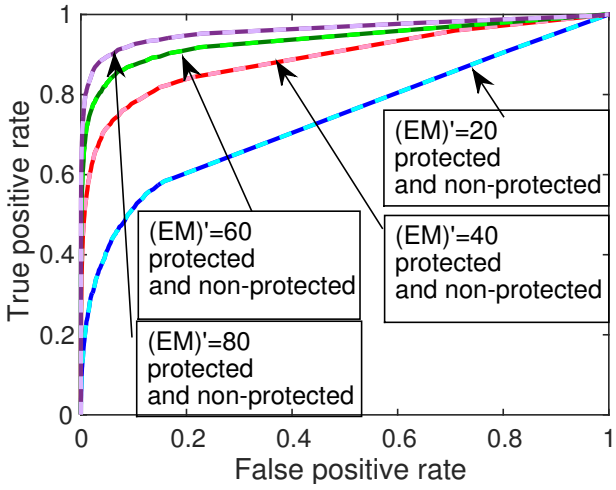
図 5 に，ランダム射影による保護テンプレート [23] と提案法に対して多項式カーネルを用いた場合の ROC カーブを示す．ただし，ランダム射影とは，1254×1254 の各列のユークリッド距離が正規化されたランダム行列をテンプレートベクトルにかけ保護を行う，ユニタリ性を持たない保護法である．ランダム射影によって保護を行った場合の結果は，提案法の結果に比べて大きく認証性能が劣化していることがわかる．

D. グラムシュミットの直交化法を用いた保護法との比較

次に，提案法とグラムシュミットの直交化法を用いた保護法 [12] とを $\mathbf{Q}_p$ を生成する計算量の観点で比較する．グラムシュミットの直交化法を用いた保護法は，擬似乱数行列にグラムシュミットの直交化法を用いて生成された直交行列によってテンプレートを保護する方法である．ここで，$N \times N$ の擬似乱数行列からランダム直交行列をグラムシュミットの直交化法を用いて生成する場合の計算量は，少なくとも $\mathcal{O}(N^3)$ である．

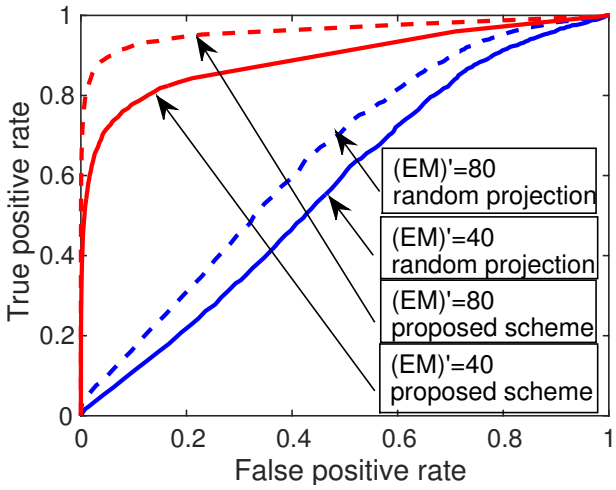


(a)RBF カーネル ($\sigma = 1$)



(b) 多項式カーネル ($l = 0, d = 2$)

図 4　ROC カーブ



多項式カーネル ($l = 0, d = 2$)

図 5　ROC カーブ (ランダム射影と提案法との比較)

また，特徴ベクトルを直交行列を用いて変換する際の計算量は $\mathcal{O}(N^2)$ である．よって，グラムシュミットの直交化法を用いた保護テンプレート生成法の計算量は $\mathcal{O}(N^3)$ である．対して，提案法の保護の手順は，FFT(IFFT) と，行列 $\mathbf{H}_p$ と FFT された特徴ベクトルの積とで構成される．N 点 FFT(IFFT) の計算量は $\mathcal{O}(NlogN)$ であり，H_p と特徴ベクトルの積の計算量は $\mathcal{O}(N)$ である．よって，提案法による保護の計算量は $\mathcal{O}(NlogN)$ である．以上より，提案法による保護はグラムシュミットの直交化法を用いた保護法に比べて高速であることが示される．シミュレーションによる計算時間を表 1 に，シミュレーションの環境を表 2 に示す．ただし，固有ベクトルの数は $(EM)' = 80$，カーネル関数は RBF カーネルで，$\sigma = 1$ であり，直交化と FFT にはそれぞれ Matlab R2015a の orth 関数と fft 関数を用いた．このとき，認証にかかる時間は認証法やテンプレートの次元が同一であるため，ほとんど同じである．しかし，特徴量の変換とランダムユニタリ行列の生成時間は提案法がより高速であることがわかる．

表 1　計 算 時 間

	提案法	グラムシュミット
変換及び生成時間	0.0007 [sec/template]	1.5153 [sec/template]
認証時間	0.1138 [sec/query]	0.1161 [sec/query]

表 2　シミュレーション条件

ソフトウェア	プロセッサ	RAM
MATLAB R2015a	Intel Core i7-3540M 3.00GHz	8.0GB

5. おわりに

本稿では，ランダムユニタリ行列を用いたテンプレート保護法をカーネル法に適用し，カーネル関数及びカーネル固有顔において保護による認証性能の低下が無いことを理論的に示した．また，線形結合表現を用いた生体認証法における，l^1 ノルム最小化問題の解を用いた認証実験によって，保護法は認証性能に影響を与えないことを実験的にも示した．

文　献

[1] 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.

[2] Y. Wang, S. Rane, S. C. Draper, and P. Ishwar, "A Theoretical Analysis of Authentication, Privacy, and Reusability Across Secure Biometric Systems," IEEE Trans. Information Forensics and Security, vol. 7, no. 6, pp. 1825-1840, Dec, 2012.

[3] S. Rane., "Standardization of Biometric Template Protection, "IEEE Multimedia Magazine, Vol. 21, No. 4, pp. 94–99, Oct. 2014.

[4] A.K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," EURASIP J. Adv. Signal Processing, vol.2008, no.579416, Jan. 2008.

[5] 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.

[6] A. Goh, A. B. J. Teoh and D. C. L. Ngo, "Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs," IEEE Trans. Pattern Anal Mach Intell, vol.28 ,no.12, pp.1892-1901, Dec 2006.

[7] H.Al-Assam, H. Sellahewa, and S. Jassim, "A lightweight approach for biometric template protection," SPIE Defense, Security, and Sensing. International Society for Optics and Photonics, p.73510P-73510P-12, 2009.

[8] J. Zuo, NK. Ratha, JH. Connel, "Cancelable iris biometric." Proc. International Conference on Pattern Recognition, pp. 1-4, 2008.

[9] J.K. Pillai, V.M. Patel, R. Chellappa, and N.K. Ratha, "Secure and robust iris recognition using random projections and sparse representation," IEEE Trans. Pattern Analysis and Machine Intelligence, vol.33, no.9, pp.1877-1893, Sep. 2011.

[10] S. Hirata, K. Takahashi, "Cancelable Biometrics with Perfect Secrecy for Correlation-Based Matching," Advances in Biometrics, Lecture Notes in Computer Science, Vol.5558, pp.868-878, 2009.

[11] K. Takahashi., "Unconditionally provably secure cancelable biometrics based on a quotient polynomial ring," International Joint Conference on Biometrics (IJCB), 11-13 Oct. 2011

[12] Y. Wang and K. Plataniotis "Face based biometric authentication with changeable and privacy preservable templates," Proc. IEEE Biometrics Symposium pp.1-6 2007.

[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 Tempalte Protection and Its Application to l2-norm Minimization Problems," IEICE Trans. Inf. and Sys., vol.E99-D, no.1, pp.6068, 2016.

[15] Christopher J. C. Burges, "A tutorial on support vector machines for pattern recognition." Data mining and knowledge discovery vol.2, no.2, pp.121-167, 1998

[16] L. Zhang, W. D. Zhou, P. C. Chang, J. Liu, Z. Yan, T. Wang, and F. Z. Li, "kernel sparse representation-based classifier,"IEEE Trans. Signal Process., vol.60, no.4, pp.1684-1695, 2012.

[17] M.H. Yang, "Kernel Eigenfaces vs. Kernel Fisherfaces: Face Recognition Using Kernel Methods," Proc. Fifth IEEE Int'l Conf. Automatic Face and Gesture Recognition, pp. 215-220, May 2002.

[18] M. Turk and A. Pentland, "Eigenfaces for Recognition," J. Cognitive Neuroscience, vol. 3, no. 1, 1991.

[19] J. M. Lee, C. K. Yoo, S. W. Choi and P. A. Vanrolleghem"Nonlinear process monitoring using kernel principal component analysis," Chemical Engineering Science, vol. 59, no.1, pp.223-234, 2004

[20] 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.

[21] H. Al-Assam, H. Sellahewa, and S. Jassim, "A lightweight approach for biometric template protection," Proc of SPIE, vol. 7351, pp. 73510P.173510P.12, March 2009.

[22] 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.

[23] S. Kaski, "Dimensionality Reduction by Random Mapping," Proc. IEEE Int'l Joint Conf. Neural Networks, vol. 1, pp. 413-418, 1998.