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固有顔特徴量の生成法

中村　維吹†　　外村　喜秀††　　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 東京都日野市旭が丘 6-6
†† 日本電信電話株式会社　未来ねっと研究所
E-mail: †nakamura-ibuki@ed.tmu.ac.jp, ††tonomura.yoshihide@lab.ntt.co.jp, †††kiya@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，ユニタリ変換を用いたセキュアな固有顔特徴量の生成法を提案し、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，ユニタリ変換によって保護された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が等しくなること，l^2 ノルム最小化問題に対して認証性能劣化が生じないことが示されている．しかし、l^1 ノルムなど他の誤差基準に対しては，認証性能への影響を回避可能な保護テンプレートの生成法は示されていない．提案される固有顔に対するユニタリ変換に基づく保護テンプレート法は，オリジナルテンプレートから求められる固有顔の重みと同じ重みを，誤差基準の制約なしで与えることができる．これは，l^1 ノルムなど任意の誤差基準のもとで，テンプレート保護による認識性能の劣化が生じないことを意味する．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　生体認証，テンプレート保護法，ユニタリ変換，固有顔，l^1 ノルム最小化

Generating Protected Eigenface Templates Using an Unitary Transformaion

Ibuki NAKAMURA†, Yoshihide TONOMURA††, and Hitoshi KIYA†

† Tokyo Metropolitan University Information and Communication Systems　6-6 Asahigaoka , Hino-shi, Tokyo, 191-0065 Japan
†† NTT Network Innovation Laboratories, Nippon Telegraph and Telephone Corp.
E-mail: †nakamura-ibuki@ed.tmu.ac.jp, ††tonomura.yoshihide@lab.ntt.co.jp, †††kiya@tmu.ac.jp

Abstract　This paper considers a template protection scheme based on an unitary transformation, where the template consists of the features extracted from the biometric trait. In this paper, a generation method of secure eigenface features, i.e. protected templates using an unitary transformation is proposed and the recognition performance is theoretically considered. Previous studies showed that the Euclidean distance between the templates protected by a unitary transform is the same as that between original ones, and there is no degradation of the recognition performances against l^2-norm minimization. However, any generation method of protected templates that can provide no degradation of the authentication performance against other error criteria such as l^1-norm has not been shown. The proposed template protection method for eigenface features can give same weights as those of eigenface obtained from original templates without any error criterion constraint. That is, the proposed method enables that there is no degradation of the recognition performance under any error criterion such as l^1-norm. We perform some face recognition experiments experimentally to confirm the validity of the theory.
Key words　biometrics, template protection method, unitary transform, eigenface, l^1-norm minimization

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．

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 [1] [2]．前者 [3] - [12] は，後者 [13] - [17] に比べて，保護された領域において，行える信号処理の自由度が高い．特徴変換に基づく方法は，さらに，可逆方式 [3] - [7] と非可逆方式 [8] - [12] に分類される．

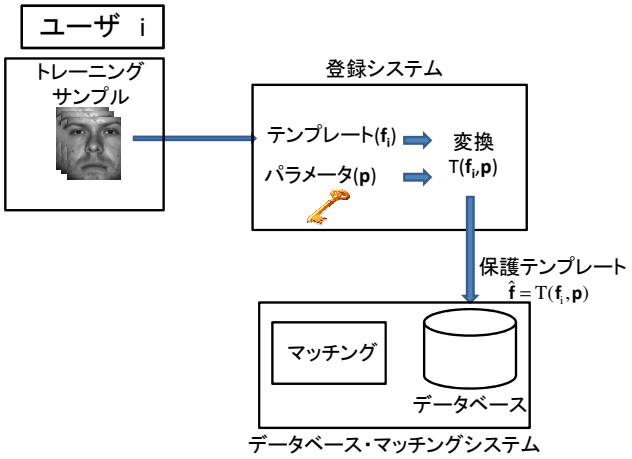
本稿のユニタリ変換に基づく保護法は，特徴変換に基づく方法における，可逆方式に分類される．一般に，非可逆方式が，鍵の配送が必要無く，セキュリティの観点で良い特徴を持つとされるが，決定論的に認証性能が低下しないと保証することは困難である．加えて，圧縮センシングや，非線形フィルタリングなどの技術を用いることで，保護テンプレートから，オリジナルテンプレートを推定されるリスクがあることが指摘されている [10] [18]．一方，可逆方式に分類される，ユニタリ変換に基づくテンプレート保護法は，変換のパラメータを秘密鍵として，安全に保護する必要があるが，いくつかの優れた特徴を持っている．たとえば，オリジナル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．

本稿では，ユニタリ変換を用いたセキュアな固有顔特徴量の生成法を提案し，保護による認証性能の低下が無いことを理論的に示す．ユニタリ変換に基づくテンプレート保護法は，保護された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が等しくなり，l^2 ノルム最小化問題においても，性能の劣化無しに解けることが示されている．しかし、l^1 ノルムなど他の誤差基準に対しては，認証性能への影響を回避可能な保護テンプレートの生成法は示されていない．提案法は，テンプレートをユニタリ変換に基づく保護法によって保護し，その保護テンプレートから固有顔 [19] を用いて重みを算出することで，固有顔などの特徴を保護しながらも，オリジナルテンプレートから求められる固有顔の重みと同じ重みを得ることが出来る．これは，l^1 ノルムなど任意の誤差基準のもとで，テンプレート保護による認識性能の劣化が生じないことを意味する．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．

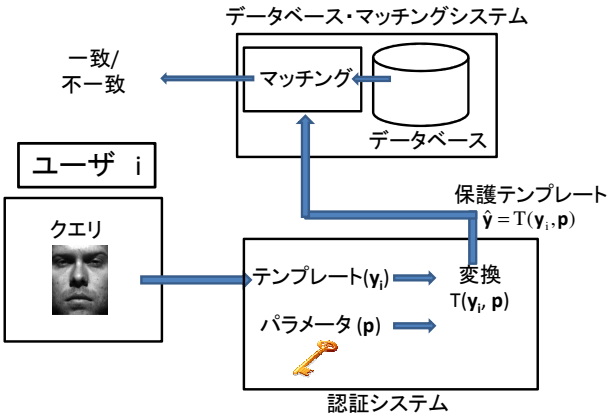
2. 準　　備

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 $\mathbf{f}_i$ 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 $\hat{\mathbf{f}}_i$=$\mathrm{T}(\mathbf{f}_i, \mathbf{p})$ 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，



(a) 登録システム



(b) 認証システム

図 1　生体認証システム

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．

2.2 固　有　顔

本節では、代表的な固有顔の重みの計算方法 [19] を要約する．まず、トレーニングサンプルの画像 $\mathbf{g}_i$ から，トレーニングテンプレート $\mathbf{f}_i \in \mathbb{R}^N, i = 1, 2, ..., M$ を抽出し、その平均 $\mathbf{\Psi}$ を計算する．

$$\mathbf{\Psi} = \frac{1}{M}\sum_{i=1}^{M}\mathbf{f}_i \tag{1}$$

ここで、$\mathbf{\Psi}$ 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，

$$\mathbf{\Phi}_i = \mathbf{f}_i - \mathbf{\Psi} \tag{2}$$

次に，このベクトル $\mathbf{\Phi}_i$ の集合から主成分分析によって，最適な正規直行ベクトル $\mathbf{u}_n \in \mathbb{R}^N$ と，それに関連する固有値 λ_n を導出する．以下の関係のもとで，k 番目のベクトル $\mathbf{u}_k$ は，λ_k を最大にするように選ばれる．

$$\lambda_k = \frac{1}{M}\sum_{n=1}^{M}(\mathbf{u}_k^T\mathbf{\Phi}_n)^2 \tag{3}$$

このとき、$\mathbf{u}_k$ と λ_k はそれぞれ，以下の共分散行列 $\mathbf{C}$ の固有ベクトルと固有値となる．

$$\begin{aligned}\mathbf{C} &= \frac{1}{M}\sum_{n=1}^{M}\mathbf{\Phi}_n\mathbf{\Phi}_n^T \\ &= \mathbf{A}\mathbf{A}^T \end{aligned} \tag{4}$$

ただし，$\mathbf{A} = [\mathbf{\Phi}_1, \mathbf{\Phi}_2, ..., \mathbf{\Phi}_M]$ である．ここで行列 $\mathbf{C}$ のサイズは $N \times N$ であり，テンプレートの次元 N によって決定される．このため，$\mathbf{C}$ から直接，固有ベクトルと固有値を求めるための演算量は，一般的に，非常に大きなものとなってしまう．ここで，行列 $\mathbf{L} = \mathbf{A}^T\mathbf{A}$ の固有ベクトル $\mathbf{v}_k$ について考える．まず，$\mathbf{v}_k$ を求める．

$$\mathbf{A}^T\mathbf{A}\mathbf{v}_k = \mu\mathbf{v}_k \tag{5}$$

次に，この式に左から $\mathbf{A}$ をかけると，

$$\mathbf{A}\mathbf{A}^T\mathbf{A}\mathbf{v}_k = \mu\mathbf{A}\mathbf{v}_k, \tag{6}$$

となり，$\mathbf{u}_k = \mathbf{A}\mathbf{v}_k$ とおくと，

$$\mathbf{A}\mathbf{A}^T\mathbf{u}_k = \mu\mathbf{u}_k. \tag{7}$$

$\mathbf{A}\mathbf{v}_k$ は $\mathbf{C} = \mathbf{A}\mathbf{A}^T$ の固有ベクトルと見なすことが出来る．また，行列 $\mathbf{L}$ のサイズは $M \times M$ で，登録テンプレート数 M によって決定する．従って $M \ll N$ なので，$\mathbf{C}$ の固有ベクトルを，$\mathbf{L}$ によって，より少ない演算量で求めることができる．$\mathbf{L}$ の固有ベクトル $\mathbf{v}_k$ と $\mathbf{\Phi}_n$ より，$\mathbf{u}_k$ は，

$$\mathbf{u}_k = \sum_{n=1}^{M}\mathbf{v}_{kn}\mathbf{\Phi_n} \tag{8}$$

と得られる．この $\mathbf{u}_k$ を固有顔といい，固有顔を用いて認証を行う．実際の認証には，M' 個 ($M' < M$) の固有顔が用いられる．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．

$$\omega_k = \mathbf{u}_k^T(\mathbf{y} - \mathbf{\Psi}) \tag{9}$$

ただし，$k = 1, ..., M'$ である．重みベクトル $\mathbf{\Omega}^T = [\omega_1, \omega_2, ..., \omega_{M'}]$ 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．

2.3 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 [9] がある．本稿では，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 $\mathbf{\Omega}_{i,m_i}$ を，i 番目の人の m_i 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，$m_i = 1, 2, ..., M_i$．K 人の登録者の中の，i 番目の人 M_i 個のトレーニングテンプレートは，$\mathbf{D}_i = [\mathbf{\Omega}_{i,1}, \mathbf{\Omega}_{i,2}, ..., \mathbf{\Omega}_{i,M_i}], i = 1, 2, ..., K$，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．

$$\mathbf{y} = \mathbf{\Omega}_{i,1}x_{i,1} + \mathbf{\Omega}_{i,2}x_{i,2} + ... + \mathbf{\Omega}_{i,M_i}x_{i,M_i} = \mathbf{D}_i\mathbf{x}_i, \tag{10}$$

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

$$\mathbf{y} = \mathbf{D}_1\mathbf{0} + ... + \mathbf{D}_{i-1}\mathbf{0} + \mathbf{D}_i\mathbf{x}_i + \mathbf{D}_{i+1}\mathbf{0} + ... + \mathbf{D}_K\mathbf{0} = \mathbf{D}\mathbf{x}_0, \tag{11}$$

ここで，$\mathbf{D} = [\mathbf{D}_1, \mathbf{D}_2, ..., \mathbf{D}_K]$,$\mathbf{x}_0 = [\mathbf{0}^T, ..., \mathbf{0}^T, \mathbf{x}_i^T, \mathbf{0}^T, ..., \mathbf{0}^T]^T$. である．ここで，$M' < M$ の関係より，$\mathbf{D}$ はランク M 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 (11) の l^1 ノルム最小化問題を解く．

$$\tilde{\mathbf{x}}_0 = \arg\min_{\mathbf{x}} ||\mathbf{x}||_1 \ \ subject\ to\ \ \mathbf{y} = \mathbf{D}\mathbf{x}. \tag{12}$$

式 (12) 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．

$$\delta_i(\tilde{\mathbf{x}}_0) = [\mathbf{0}^T, ..., \mathbf{0}^T, \tilde{\mathbf{x}}_i^T, \mathbf{0}^T, ..., \mathbf{0}^T]^T. \tag{13}$$

$\delta_i(\tilde{\mathbf{x}}_0)$ を式 (10) 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．

$$r_i = ||\mathbf{y} - \mathbf{D}\delta_i(\tilde{\mathbf{x}}_0)||_2, \tag{14}$$

$$C = \arg\min_i r_i, \tag{15}$$

ここで，r_i は i 番目の人の推定二乗誤差と言う．

2.4 ユニタリ変換に基づくテンプレート保護法

ユニタリ変換に基づくテンプレート保護法では，テンプレート $\mathbf{f}_i$ を，パラメータ $\mathbf{p}$ によってランダム性を持ったユニタリ行列 $\mathbf{Q}_p \in \mathbb{C}^{N\times N}$ によって，以下のように保護する．

$$\hat{\mathbf{F}}_i = T(\mathbf{f}_i, \mathbf{p}) = \mathbf{Q}_p\mathbf{f}_i, \tag{16}$$

ここで，$\hat{\mathbf{F}}_i$ は，保護テンプレートである．本稿では，その中でも，DFT に基づくテンプレート保護法を用いる [20].

DFT に基づくテンプレート保護法は，以下の手順でテンプレートの保護を行う．まず，テンプレート $\mathbf{f}_i = [f_i(0), f_i(1)..., f_i(N-1)]^T, i = 1, 2, ..., K$ に DFT を適用する

$$F_i(k) = \frac{1}{\sqrt{N}}\sum_{n=0}^{N-1} f_i(n)\cdot W_N^{nk},\ k = 0, 1, ..., N-1 \tag{17}$$

ここで，$W_N = e^{-j\frac{2\pi}{N}}$，$[\cdot]^T$ は行列の転置を表す．DFT 行列は $\mathbf{A} \in \mathbb{C}^{N\times N}$ と表現出来るので，式 (17) は以下の様に表す事ができる．

$$\mathbf{F}_i = \mathbf{A}\mathbf{f}_i, \tag{18}$$

ここで，$\mathbf{F}_i = [F_i(0), F_i(1)..., F_i(N-1)]$．次に，$N$ 個の位相値 $\theta_p(k) \in \{\frac{2\pi l}{L} + \alpha | l = 0, 1, ..., L-1, \alpha \in \mathbb{R}\}$, $k = 0, 1, ..., N-1$ が，擬似乱数生成器によって，ランダムに生成される [21] [22]. そして，この位相ベクトル $\boldsymbol{\theta}_p$ によって，対角行列 $\mathbf{H}_p$ を定義する．

$$H_p(k,k) = e^{j\theta_p(k)},\ k = 0, 1, ..., N-1. \tag{19}$$

ここで，$\mathbf{H}_p$ は以下の式を満たす．

$$\mathbf{H}_p^* \mathbf{H}_p = \mathbf{I}, \tag{20}$$

ここで，$[\cdot]^*$ と I は，それぞれ，エルミート行列と単位行列を示す．$\boldsymbol{\theta}_p$ は，図 1 における $\mathbf{p}$ である．このとき，$\mathbf{H}_p$ と，$\mathbf{F}_i$ との積を計算すると以下のようになる．

$$\hat{\mathbf{F}}_i = \mathbf{H}_p \mathbf{F}_i = \mathbf{H}_p \mathbf{A} \mathbf{f}_i. \tag{21}$$

式 (21) と式 (16) を比較すると，

$$\mathbf{Q}_p = \mathbf{H}_p \mathbf{A}, \tag{22}$$

の関係が成り立つ．ここで，$\mathbf{H}_p\mathbf{A}$ は，$\mathbf{A}$ と同様に，ユニタリ行列である．保護テンプレートとして実数値を得るために，逆 DFT を用いる．

$$\hat{\mathbf{f}}_i = \mathbf{A}^{-1} \hat{\mathbf{F}}_i = \mathbf{A}^{-1} \mathbf{H}_p \mathbf{A} \mathbf{f}_i, \tag{23}$$

この時，$\mathbf{A}^{-1}\mathbf{H}_p\mathbf{A}$ もユニタリ行列である．ここで，実数の保護テンプレート $\hat{\mathbf{f}}_i \in \mathbb{R}^N$ を得るには，$\boldsymbol{\theta}_p$ が，$\theta_p(k) = 2\pi - \theta_p(N-k)$, $k = 1, ..., \lfloor \frac{N-1}{2} \rfloor$ の関係を満たす必要がある．また，式 (16) と同様に，式 (23) も以下のように表すことが出来る．

$$\hat{\mathbf{f}}_i = T(\mathbf{f}_i, \mathbf{p}). \tag{24}$$

ユニタリ変換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 [7].

特徴 1 ：ユークリッド距離の保存
$||\mathbf{f}_i - \mathbf{f}_j||^2 = ||\hat{\mathbf{f}}_i - \hat{\mathbf{f}}_j||^2$

特徴 2 ：内積の保存
$\mathbf{f}_i^* \mathbf{f}_j = \hat{\mathbf{f}}_i^* \hat{\mathbf{f}}_j$

特徴 3 ：相関係数の保存
$\frac{||\mathbf{f}_i - \bar{\mathbf{f}}_i|| ||\mathbf{f}_j - \bar{\mathbf{f}}_j||}{\sqrt{||\mathbf{f}_j - \bar{\mathbf{f}}_j||^2} \sqrt{||\mathbf{f}_j - \bar{\mathbf{f}}_j||^2}} = \frac{||\hat{\mathbf{f}}_i - \bar{\hat{\mathbf{f}}}_i|| ||\hat{\mathbf{f}}_j - \bar{\hat{\mathbf{f}}}_j||}{\sqrt{||\hat{\mathbf{f}}_j - \bar{\hat{\mathbf{f}}}_j||^2} \sqrt{||\hat{\mathbf{f}}_j - \bar{\hat{\mathbf{f}}}_j||^2}}$

3. 提 案 法

3.1 ユニタリ変換に基づく保護法の固有顔への適用

ユニタリ変換に基づく保護法を固有顔へ適用する．

トレーニングサンプルの画像 $\mathbf{g}_i$ から，抽出したテンプレート $\mathbf{f}_i$ に，ユニタリ変換を用いて生成された保護テンプレート $\hat{\mathbf{f}}_i$ をトレーニングセットとして用いた場合について考察する．ただし，$i = 1, 2, ..., M$．平均顔を以下のように求める．

$$\hat{\boldsymbol{\Psi}} = \frac{1}{M} \sum_{i=1}^{M} \hat{\mathbf{f}}_i \tag{25}$$

平均顔を用いて，各テンプレートと平均との差を求める．

$$\hat{\boldsymbol{\Phi}}_i = \hat{\mathbf{f}}_i - \hat{\boldsymbol{\Psi}} \tag{26}$$

ただし，$k = 1, 2, ..., M$．ここで，固有ベクトルを求めるために $\hat{\mathbf{L}} = \hat{\mathbf{A}}^T \hat{\mathbf{A}}$ を求める．

$$\begin{aligned} \hat{\mathbf{A}}^T \hat{\mathbf{A}} &= [\hat{\boldsymbol{\Phi}}_1, \hat{\boldsymbol{\Phi}}_2, ..., \hat{\boldsymbol{\Phi}}_M]^T [\hat{\boldsymbol{\Phi}}_1, \hat{\boldsymbol{\Phi}}_2, ..., \hat{\boldsymbol{\Phi}}_M] \\ &= \sum_n \sum_m \hat{\boldsymbol{\Phi}}_n^T \hat{\boldsymbol{\Phi}}_m \end{aligned} \tag{27}$$

ここで，$\hat{\boldsymbol{\Phi}}_n^T \hat{\boldsymbol{\Phi}}_m$ は，以下のように展開できる．

$$\begin{aligned} \hat{\boldsymbol{\Phi}}_n^T \hat{\boldsymbol{\Phi}}_m &= (\hat{\mathbf{f}}_n - \hat{\boldsymbol{\Psi}})^T (\hat{\mathbf{f}}_m - \hat{\boldsymbol{\Psi}}) \\ &= (\hat{\mathbf{f}}_n - \frac{1}{M} \sum_{k=1}^{M} \hat{\mathbf{f}}_k)^T (\hat{\mathbf{f}}_m - \frac{1}{M} \sum_{l=1}^{M} \hat{\mathbf{f}}_l) \\ &= \hat{\mathbf{f}}_n^T \hat{\mathbf{f}}_m - \frac{1}{M} \sum_{l=1}^{M} \hat{\mathbf{f}}_n^T \hat{\mathbf{f}}_l + \frac{1}{M} \sum_{k=1}^{M} \hat{\mathbf{f}}_k^T \hat{\mathbf{f}}_m \\ &\quad - \frac{1}{M^2} \sum_{k=1}^{M} \sum_{l=1}^{M} \hat{\mathbf{f}}_k^T \hat{\mathbf{f}}_l \end{aligned} \tag{28}$$

この時，式 (28) の各項は保護テンプレートの内積計算となるため，特徴 2 の内積保存の性質より，以下の式が成り立つ．

$$\hat{\boldsymbol{\Phi}}_n^T \hat{\boldsymbol{\Phi}}_m = \boldsymbol{\Phi}_n^T \boldsymbol{\Phi}_m \tag{29}$$

すなわち，

$$\hat{\mathbf{A}}^T \hat{\mathbf{A}} = \mathbf{A}^T \mathbf{A}. \tag{30}$$

これは，固有ベクトル $\mathbf{v}_k$ は，保護の影響なく求めることができることを示している．この時，固有顔は，以下の式で与えられる．

$$\hat{\mathbf{u}}_k = \sum_{l=1}^{M} \mathbf{v}_{kl} \hat{\boldsymbol{\Phi}}_l \qquad k = 1, 2, ..., M. \tag{31}$$

認証時，保護されたクエリ $\hat{\mathbf{y}}$ と固有顔と平均顔を用いて重みを計算する．この時重みは，

$$\begin{aligned} \hat{\omega}_k &= \hat{\mathbf{u}}_k^T (\hat{\mathbf{y}} - \boldsymbol{\Psi}) \\ &= (\sum_{l=1}^{M} \mathbf{v}_{kl} \hat{\boldsymbol{\Phi}}_k)^T (\hat{\mathbf{y}} - \boldsymbol{\Psi}) \\ &= (\sum_{l=1}^{M} \mathbf{v}_{kl} (\hat{\mathbf{f}}_l - \boldsymbol{\Psi}))^T (\hat{\mathbf{y}} - \boldsymbol{\Psi}) \\ &= (\sum_{l=1}^{M} \mathbf{v}_{kl} (\hat{\mathbf{f}}_l - \frac{1}{M} \sum_{n=1}^{M} \hat{\mathbf{f}}_n))^T (\hat{\mathbf{y}} - \frac{1}{M} \sum_{m=1}^{M} \hat{\mathbf{f}}_m) \\ &= \sum_{l=1}^{M} \mathbf{v}_{kl}^T (\hat{\mathbf{f}}_l^T \hat{\mathbf{y}} - \frac{1}{M} \sum_{m=1}^{M} \hat{\mathbf{f}}_l^T \hat{\mathbf{f}}_m \\ &\quad - \frac{1}{M} \sum_{n=1}^{M} \hat{\mathbf{f}}_n^T \hat{\mathbf{y}} + \frac{1}{M^2} \sum_{n=1}^{M} \sum_{m=1}^{M} \hat{\mathbf{f}}_n^T \hat{\mathbf{f}}_m) \end{aligned} \tag{32}$$

となる．式 (28) と同様に保護テンプレートの内積計算によって表すことができるため，特徴 2 より，

$$\hat{\omega}_k = \omega_k \qquad k = 1, 2, ..., M \tag{33}$$

となることがわかる．これにより，生成される重みベクトルが，保護の影響を受けない事が示された．これは，式 (12) の l^1 ノルム最小化問題において，保護処理の影響をその解が受けないことを意味する．

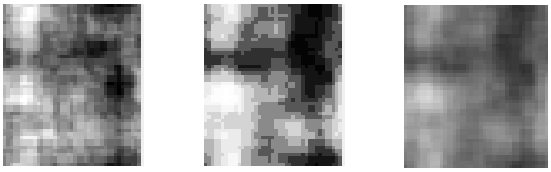
4. 実　　験

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 The Extended Yale Face Database B [23] を用いた．38 人の様々な照

(a) テンプレート　(b) 固有顔　(c) 平均顔

図 2　オリジナルテンプレート



(a) テンプレート　(b) 固有顔　(c) 平均顔

図 3　保護テンプレート

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 32 枚，クエリに 32 枚に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た，ここで，$\boldsymbol{\theta}_{p_i} \in \{\frac{\pi}{2}, -\frac{\pi}{2}\}$．また，本実験では，固有値 $\lambda_i > 1.0 \times 10^{-4}$ を満たす，固有顔 $\mathbf{u}_k$ のみを用いた．

4.2　顔認証実験

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，DFT に基づく保護法を適用して，その後，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，192×168 の画像を 38×33 にダウンサンプリングして，テンプレートを生成した．

図 2 と図 3 には，それぞれ，DFT に基づく保護法を，適用しない場合と，適用した場合の，テンプレートと固有顔と平均顔を示す．保護法を適用しない場合には，テンプレート，固有顔，平均顔，どれをとっても視覚的情報が残っているが，適用した場合には，いずれの場合も，それらの特徴が保護されていることがわかる．

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．

$$if\ r_i \leqq \tau\ then\ 受け入れ;\ else\ 拒否. \qquad (34)$$

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 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算出される重みを用いた結果が，オリジナルテンプレートから算出した重みによる結果と，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，ユニタリ変換に基づく保護法は，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．

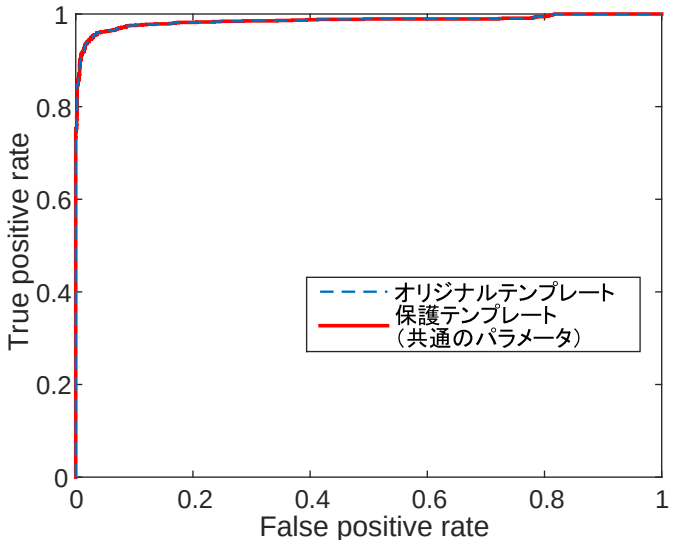


図 4　ROC カーブ

5.　お わ り に

本稿では，ユニタリ変換を用いたセキュアな固有顔特徴量の生成法を提案し，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．ユニタリ変換に基づくテンプレート保護法は，固有顔へ適用することで，ユークリッド距離や，l^2 ノルム最小化問題の解が保存されるだけでなく，l^1 ノルム最小化問題に対しても保護の影響を与えないことが示された．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] A.K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," EURASIP J. Adv. Signal Processing, vol.2008, no.579416, Jan. 2008.

[2] 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.

[3] 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.

[4] S. Marios, B. V. K. Vijaya Kumar, and P. K. Khosla, "Cancelable biometric filters for face recognition,"ICPR 2004. Proc. of the 17th International Conference on, vol.3, pp.922-925, 2004.

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

[6] S. Jassim, H.Al-assam, H.Sellahewa, "Improving performance and security of biometrics using efficient and stable random projection techniques," Proc. of the 6th International Symposium on Image and Signal Processing and Analysis, ISPA ' 09, pp. 556-561, 2009.

[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.K. Pillai, V.M. Patel, R. Chellappa, and N.K. Ratha, "Se-

cure 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.

[9] 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.

[10] Y. Muraki, M. Furukawa, M. Fujiyoshi, Y. Tonomura, and H. Kiya, "A Compressible Template Protection Scheme for Face Recognition Based on Sparse Representation," Proc. EURASIP, no.TH-P5, Sep. 2014.

[11] M. Furukawa, Y. Muraki, M. Fujiyoshi, and H. Kiya, "A Secure Face Recognition Scheme Using Noisy Images Based on Kernel Sparse Representation," Proc. APSIPA Annual Summit and Conference, no.OS.20-IVM.9-4, Kaohsiung, Taiwan, R.O.C., 30th October, 2013.

[12] A.B.J. Teoh and C.T. Yuang, "Cancelable biometrics realization with multispace random projections," IEEE Trans. Sys., Man, and Cybernetics Part B: Cybernetics, vol.37, pp.1096-1106, Mon. 2007.

[13] A. Juels, and M. Wattenberg, "A fuzzy commitment scheme,"Proc. of the 6th ACM conference on Computer and communications security, no.9, pp.28-36, 1999.

[14] Y.C. Feng, P.C. Yuen, and A.K. Jain, "A hybrid approach for generating secure and discriminating face template," IEEE Trans. Info. Forensic Security, vol.5, pp.103-117, Mar. 2010.

[15] U. ludag, S. Pankanti, S. Prabhakar, and K. Jain. "Biometric cryptosystems: issues and challenges," Proc. IEEE, vol.92, no.6, pp.948-960, Jun, 2004.

[16] E. Maiorana, P. Campisi, A. Neri, "Iris template protection using a digital modulation paradigm," Proc. IEEE International Conference on Acoustics, Speech and Signal Processing, pp.3787-3791, 2014

[17] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," IEEE Trans. Pattern Analysis and Machine Intelligence, vol.29, no.4, pp.561-572, Apr. 2011.

[18] Y. Muraki, M. Furukawa, M. Fujiyoshi, and H. Kiya, "Robustness Analysis of Cancelable Biometrics Systems in Terms of Visual Recognizability," Proc. International Workshop on Advanced Image Technology, no.A2-145, pp.24-27, Jan. 2014.

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

[20] 中村 維吹, 倉上 高史, 外村 喜秀, 貴家 仁志, "直交変換に基づく生体認証のためのテンプレート保護法," 電子情報通信学会 スマートインフォメディアシステム研究会, vol.114, no.205, (no.52), pp.7-12, 2014 年 9 月.]

[21] I. Ito and H. Kiya, "One-Time Key Based Phase Scrambling for Phase-Only Correlation between Visually Protected Images," EURASIP J. Information Security, vol.2009, no.841045, Jan. 2010.

[22] I. Ito and H. Kiya, "A new class of image registration for guaranteeing secure data management"Proc. IEEE International Conference on Image Processing, no.MA-PA.5, pp.269-272, Oct. , 2008.

[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," IEEE Trans. Pattern Analysis and Machine Intelligence, vol.23, no.6, pp.643-660, Jun. 2001.