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.

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

中村　維吹†　倉上　高史†　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,kurakami-takashi}@ed.tmu.ac.jp, ††tonomura.yoshihide@lab.ntt.co.jp,
†††kiya@tmu.ac.jp

あらまし　生体情報は個人情報でありかつ変更不可な情報であるため，生体情報から抽出された特徴量（テンプレート）を保護する技術が必須となる．本稿では，直交変換のエネルギー保存則に基づく新しい保護テンプレートの生成法を提案する．提案法は，発生された乱数列に応じて保護テンプレートを生成・変更可能である．さらに，テンプレート間のユークリッド距離を完全に保存できるという特徴を持つ．この特徴から，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生体認証法に対して，l^2 ノルム最小問題を認証精度低下の影響なく実行することが可能となる．代表的なテンプレート生成である，ダウンサンプル法とランダム射影法に対して提案法を適用し顔認証実験を行い，提案法の有効性及び理論の正当性を検証する．

キーワード　生体認証　テンプレート保護法　キャンセラブルバイオメトリクス

A Generation Scheme of Protected Templates Based on Orthogonal Transforms for Biometrics

Ibuki NAKAMURA†, Takashi KURAKAMI†, 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,kurakami-takashi}@ed.tmu.ac.jp, ††tonomura.yoshihide@lab.ntt.co.jp,
†††kiya@tmu.ac.jp

Abstract　Since biometric features are personal and irrevocable data, some schemes which protect the features (templates) extracted from biometric information are indispensable. This paper proposes a new scheme to generate protected templates based on the energy conservation law of orthogonal transforms for biometrics authentification.The proposed scheme can generate cancelable templates protected by a random number sequence.Furthermore, the Euclid distance between protected templates is exactly the same as that between original ones. From this feature, there is no degradation of recognition performance in any solving problem of l^2 norm minimization, for biometrics authentification methods based on linear combination of training templates and query ones. The proposed method is also applied to some face recognition experiments by using the down-sampling method and the random projection method respectively, which are typical template generation methods, to verify the effectiveness of the proposed method.

Key words　Biometrics Template protection Cancelable biometrics

1. ま え が き

近年，様々なサービスにおいて，安全性のためユーザ認証が行われている．その中でも，ID とパスワードを用いた方法は，特別な機器を使用する必要が無いため，多くのサービスにおいて用いられている．しかし，この方法は，ユーザが ID やパスワードを記憶をしなければならないため，ユーザが利用するサービス数の増加とともに，ユーザの負担が大きくなってしまう．この問題に対して，指紋や虹彩，顔などの生体情報を用いて認証を行う，生体認証システムが注目を集めている．生体認

証は，生体情報から抽出された特徴量 (テンプレート) の比較によって認証を行うため，携帯や記憶が必要ない．しかし，生体情報は変更不可な情報なため，パスワードのように漏洩時に変更することができない．したがって，生体認証システムにおいて，テンプレートの保護が必須となる．

テンプレートの保護を行う一つの枠組みとして，キャンセラブルバイオメトリクス [1] がある．キャンセラブルバイオメトリクスは，ある変換によってテンプレートを意図的に歪ませることで，生体情報の復元が困難な保護テンプレートを生成し，変換したままの状態で認証が可能な技術である．また，漏洩時には，テンプレートに，以前と異なるパラメータを用いて変換を行い生成された，新たな異なる保護テンプレートに変更することが可能である．

従来のキャンセラブルバイオメトリクスにおける保護テンプレートの生成法には，次元低減と同時に保護を行う，ランダム射影を用いた方法 [2] や，故意にノイズを乗せ保護を行う方法 [3]，画素スクランブルを用いて保護を行う方法 [4] など，特徴変換による方法がある．しかし，これらの方法は，保護法の適用が起因する認証精度の低下を原理的に回避できないという課題があった．一方，準同型暗号を用い，暗号化されたまま計算を行う方法 [5] も提案されている．しかし，準同型暗号で行うことのできる演算には制限があるため，扱える認証法が限られてしまう．

本稿では，直交変換のエネルギー保存則に基づく，ユークリッド距離を保存した，新しい保護テンプレートの生成法を提案する．まず，提案法がユークリッド距離を完全に保存することについて理論的に述べる．また，ユークリッド距離を保存する特徴を用いて，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生体認証法に対して，認証精度を低下させることなく実現可能であることを理論的に示す．最後に，代表的なテンプレート生成である，ダウンサンプル法とランダム射影法に対して提案法を適用し，顔認証の実験を行い，提案法の有効性および理論の正当性を検証する．

2. 準　　備

本節では，対象とする生体認証システムとテンプレート保護法について述べ，直交変換の性質を要約する．

2.1 認証システムの概要

生体情報は変更不可な情報であるため，生体情報から抽出された特徴量 (テンプレート) を保護する技術が必須となる．テンプレート保護技術とは，テンプレートをあるパラメータで変換し，変換したままの状態で照合を可能にする技術である．また，パラメータ変換されたテンプレートを保護テンプレートという．パラメータの変更によって，一つのテンプレートからテンプレートの変更や更新が可能となる．

図 1 は本稿で想定する認証システムの概要である．ユーザは自身の生体情報を申請することによって，既登録者かどうか，さらにどの登録者かをシステムによって認証される．その際，生体情報に何らかの処理を施すことによって，まずテンプレートが生成され，さらにパラメータ p によってテンプレートが変換される．その変換されたテンプレート (保護テンプレート) は，認証サーバに送信され，事前にパラメータ p を用いて生成された登録テンプレートと照合される．

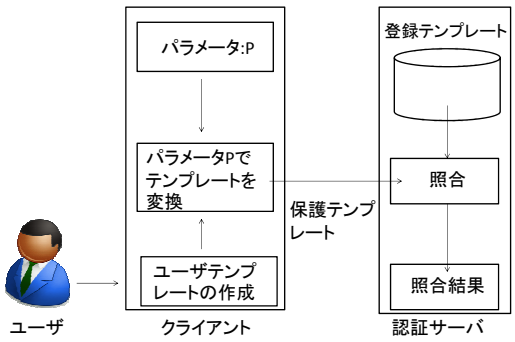


図 1　認証システム

このシステムでは，認証サーバにパラメータ p の情報は存在せず，登録テンプレートが漏洩した場合でも，生体情報の生の特徴量が閲覧されることはない．また，漏洩の危険があった場合には，他のパラメータを用いて登録テンプレートを変更することができる．ただし，パラメータ p と登録テンプレートが同時には漏洩しないことを仮定している．

2.2 保護テンプレート

生体認証において保護テンプレートは，以下の 4 つの特徴を持つことが要求される [6]．

（1） 多様性：異なる認証サーバ間において，登録されたテンプレートを用いたクロスマッチングが起こらないこと．そのためには，認証サーバ毎に異なるパラメータで適切な変換がなされる必要がある．

（2） 取消可能：テンプレートが漏洩した場合，登録されたテンプレートを消去できること．さらに，異なるパラメータによって新たな保護テンプレートを生成できなければならない．

（3） 安全性：保護テンプレートから，元のテンプレートを復元することが計算上困難であること．

（4） 性能：テンプレート保護により，認証精度が下がらないこと．

2.3 直行変換のエネルギー保存則

ベクトル $\mathbf{f} = [f(0), f(1), ..., f(N-1)]^T$ と N 行 N 列の正規直交行列 $\mathbf{A} = \{A(i,j)\}, (0 \leq i, j \leq N-1)$ により，直交変換されたベクトルの $\mathbf{F} = [F(0), F(1), ..., F(N-1)]^T$ は，

$$\begin{bmatrix} F(0) \\ F(1) \\ \vdots \\ F(N-1) \end{bmatrix} = \begin{bmatrix} A(0,0) & A(0,1) & \cdots & A(0,N-1) \\ A(1,0) & A(1,1) & \cdots & A(1,N-1) \\ \vdots & \vdots & \ddots & \vdots \\ A(N-1,0) & A(N-1,1) & \cdots & A(N-1,N-1) \end{bmatrix} \begin{bmatrix} f(0) \\ f(1) \\ \vdots \\ f(N-1) \end{bmatrix}$$

と与えられる．この時エネルギー保存則により $\mathbf{f}$ と $\mathbf{F}$ の間に，

$$\sum_{n=0}^{N-1} |f(n)|^2 = \sum_{k=0}^{N-1} |F(k)|^2 \qquad (1)$$

が成り立つ．本稿では，この性質を用いて新しい保護テンプレート生成法を考察する．

3. 提 案 法

3.1 直交変換による保護テンプレートの生成

生体認証では，まず，生体情報からある特徴量を抽出してテンプレートを生成する．次に，その特徴量に基づいて認証を実行する．代表的な認証の方法として，テンプレート間の距離に基づく方法がある．

2 つのテンプレートに対応するベクトル $\mathbf{f}_i$ と $\mathbf{f}_j$ の差を $\mathbf{f}_{i,j}$ と置く．すなわち，

$$\mathbf{f}_{i,j} = \mathbf{f}_i - \mathbf{f}_j \tag{2}$$

とする．また，$\mathbf{f}_i$，$\mathbf{f}_j$ と直交変換値，$\mathbf{F}_i$，$\mathbf{F}_j$ の差を，

$$\mathbf{F}_{i,j} = \mathbf{F}_i - \mathbf{F}_j \tag{3}$$

と置く．直交変換の線形性から，$\mathbf{F}_{i,j}$ は $\mathbf{f}_{i,j}$ の直交変換値に対応する．従って，次式が成立する．

$$\sum_{n=0}^{N-1} |f_i(n) - f_j(n)|^2 = \sum_{k=0}^{N-1} |F_i(k) - F_j(k)|^2 \tag{4}$$

ここで，$\mathbf{F}_i$，$\mathbf{F}_j$ 以外にも式 (4) の左辺と等式の関係が成立する変換値が無数に存在することに注意してほしい．すなわち，

$$\sum_{n=0}^{N-1} |f_i(n) - f_j(n)|^2 = \sum_{k=0}^{N-1} |\hat{F}_i(k) - \hat{F}_j(k)|^2 \tag{5}$$

となる $\hat{\mathbf{F}}_i$，$\hat{\mathbf{F}}_j$ が存在する．

例えば，いま，共通の $H_p(k)$ を用いて，

$$\hat{F}_i(k) = H_p(k)F_i(k) \qquad (0 \leqq k \leqq N-1) \tag{6}$$

$$\hat{F}_j(k) = H_p(k)F_j(k) \qquad (0 \leqq k \leqq N-1) \tag{7}$$

と各変換値を関係付ける．このとき式 (5) は，

$$\sum_{k=0}^{N-1} |F_i(k) - F_j(k)|^2 = \sum_{k=0}^{N-1} |H_p(k)|^2 |F_i(k) - F_j(k)|^2 \tag{8}$$

と表される．等式は，$|H_p(k)|^2 = 1$ $(0 \leqq k \leqq N-1)$ の条件下で成り立つ．このとき，$\hat{\mathbf{F}}_i$，$\hat{\mathbf{F}}_j$ の逆変換 $\hat{\mathbf{f}}_i$，$\hat{\mathbf{f}}_j$ においても，

$$\sum_{n=0}^{N-1} |f_i(n) - f_j(n)|^2 = \sum_{k=0}^{N-1} |\hat{f}_i(k) - \hat{f}_j(k)|^2 \tag{9}$$

が成立する．従って，$\hat{\mathbf{f}}_i$，$\hat{\mathbf{f}}_j$ は，$\mathbf{f}_i$，$\mathbf{f}_j$ 間の 2 乗誤差和および，ユークリッド距離を保存していることがわかる．

以上の特徴より，パラメータ p を用いて，$|H_p(k)|^2 = 1$ $(0 \leqq k \leqq N-1)$ となる $H_p(k)$ の導入によって，$\mathbf{f}_i$ と $\mathbf{f}_j$ のユークリッド距離を保存した新たなベクトル $\hat{\mathbf{f}}_i$，$\hat{\mathbf{f}}_j$ を保護テンプレートとして生成可能となる．

また，次式のように展開することもできる．

$$\begin{aligned}&\sum_{n=0}^{N-1} \{|f_i(n)|^2 - 2f_i(n)f_j(n) + |f_j(n)|^2\} \\ &= \sum_{n=0}^{N-1} \{|\hat{f}_i(n)|^2 - 2\hat{f}_i(n)\hat{f}_j(n) + |\hat{f}_j(n)|^2\}\end{aligned} \tag{10}$$

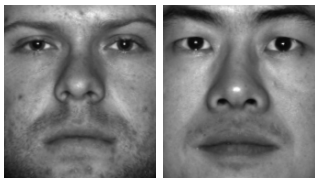


図 2 原 画 像

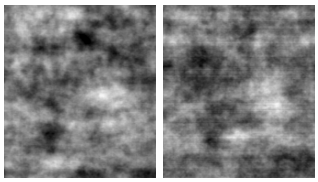


図 3 位相スクランブル画像

さらに，式 (1)，(6) および (7) の関係から，

$$\sum_{n=0}^{N-1} |f_i(n)|^2 = \sum_{n=0}^{N-1} |\hat{f}_i(n)|^2 \tag{11}$$

$$\sum_{n=0}^{N-1} |f_j(n)|^2 = \sum_{n=0}^{N-1} |\hat{f}_j(n)|^2 \tag{12}$$

が成立することに注意すると，式 (10) から，

$$\sum_{n=0}^{N-1} f_i(n)f_j(n) = \sum_{n=0}^{N-1} \hat{f}_i(n)\hat{f}_j(n) \tag{13}$$

を得る．後述するように，この結論は，保護テンプレートを用いた l^2 ノルム最小化問題の解法において重要な役割を果たす．

3.2 DFT による保護テンプレートの生成

3.1 の議論に基づき，直交変換を用いた保護テンプレートの一例として，DFT を用いた保護テンプレートの生成法を述べる．

まずテンプレートのベクトル $\mathbf{f}_i$ に対して DFT を施す．

$$F_i(k) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} f_i(n) \cdot W_N^{nk} \tag{14}$$

ただし，$W_N = e^{-j\frac{2\pi}{N}}$ とする．次に，パラメータ p(シード p) によりランダムに生成された位相 $\theta_p(k)$ を用いて，

$$H_p(k) = e^{j\theta_p(k)} \tag{15}$$

を定義する．ここで，明らかに $|H_p(k)|^2 = 1$ が成立する．さらに，

$$\hat{F}_i(k) = H_p(k) \cdot F_i(k) \tag{16}$$

を求め，その逆 DFT

$$\hat{f}_i(n) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \hat{F}_i(k) \cdot W_N^{-nk} \tag{17}$$

を保護テンプレートとする．本稿では，式 (16) に基づくこの手順を特に位相スクランブル [7] と呼ぶ．

図 2 の 2 枚の画像をテンプレートとすると，上記の手順によって位相スクランブルされた 2 枚の保護テンプレートが，2 次元 DFT の実行によって得られる．図 3 は，それらに対応する．図 2 の 2 枚のテンプレート間における，各画素間の 2 乗誤差和と，図 3 の画素間の 2 乗誤差和は一致する．また図 3 からわかるように位相スクランブルによって，視覚的情報を保護することもが可能となる．

次に，N 次のテンプレートより，L 次 $(L \geqq N)$ の保護テンプレートを生成できることを述べる．いま，N 次のテンプレー

ト $\mathbf{f}_i$ を

$$g_i(n) = \begin{cases} f_i(n) & (0 \leqq n \leqq N-1) \\ 0 & (N \leqq n \leqq L-1) \end{cases} \tag{18}$$

と L 次のテンプレートとして再定義する．このとき，この $g_i(n)$ についての L 点 DFT，$G_i(k)$ を求め，

$$\hat{G}_i(k) = G(k)e^{j\theta_p(k)} \tag{19}$$

を生成する．この $\hat{G}_i(k)$ の L 点逆 DFT，$\hat{g}_i(n)$ は以下の性質を持つ．

$$\sum_{n=0}^{N-1} |f_i(n) - f_j(n)|^2 = \sum_{n=0}^{L-1} |\hat{g}_i(n) - \hat{g}_j(n)|^2 \tag{20}$$

以上のように，提案法によって，ユークリッド距離を保存した，次数の異なる保護テンプレート $\hat{\mathbf{g}}_i$,$\hat{\mathbf{g}}_j$ が生成されることがわかる．これは，図 2 を例にすると，画素数の異なる位相スクランブル画像を生成できることを意味する．

3.3 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 [8] がある．提案法が有効な一例として述べる．

K 人をトレーニングテンプレートとして登録し，その i 番目 (i=1,2,...,K) の人に対して，M_i 個のテンプレート $\mathbf{D}_i$ を，

$$\mathbf{D}_i = [\mathbf{f}_{i,1}, \mathbf{f}_{i,2}, ..., \mathbf{f}_{i,M_i}] \tag{21}$$

$$M = \sum_{i=1}^{K} M_i \tag{22}$$

と準備する．また，トレーニングテンプレート全体を行列 $\mathbf{D}$,

$$\mathbf{D} = [\mathbf{D}_1, \mathbf{D}_2, ..., \mathbf{D}_K] \tag{23}$$

とする．いま，クエリテンプレートを $\mathbf{f}_{i,q}$ とする．ただし，i(i 番目の人) は未知である．$\mathbf{f}_{i,q}$ は i 番目のトレーニングテンプレート $\mathbf{D}_i$ の線形結合により近似されると仮定する．すなわち，

$$\mathbf{f}_{i,q} = \mathbf{f}_{i,1}x_{i,1} + \mathbf{f}_{i,2}x_{i,2} + ... + \mathbf{f}_{i,M_i}x_{i,M_i} = \mathbf{D}_i\mathbf{x}_i \tag{24}$$

と表現する．ただし $\mathbf{x}_i$ は，線形近似の係数ベクトルである．このとき，K 人のトレーニングテンプレート全体を用いると，クエリテンプレートは，

$$\mathbf{f}_{i,q} = \mathbf{D}_1\mathbf{0} + \mathbf{D}_2\mathbf{0} + ... + \mathbf{D}_i\mathbf{x}_i + ... + \mathbf{D}_K\mathbf{0} = \mathbf{D}\mathbf{X}_0 \tag{25}$$

で表される．ただし，

$$\mathbf{X}_0 = [\mathbf{0}, ..., \mathbf{0}, \mathbf{x}_i, \mathbf{0}, ..., \mathbf{0}] \tag{26}$$

である．係数行列 $\mathbf{X}_0$ は，スパースな性質を持つことがわかる．テンプレートの次元 N に対して $N \geqq M$ のとき，式 (25) から例えば，l^2 ノルム最小化問題を解くことで $\mathbf{X}_0$ を一意に決めることができる．また，一般に $N < M$ では $\mathbf{X}_0$ は一意に定まらないが，$\mathbf{X}_0$ がスパースならば l^0 ノルム最小化問題を解いて得た解 $\tilde{\mathbf{X}}_{l^0}$ に一致する．すなわち，

$$\tilde{\mathbf{X}}_{l^0} = \arg\min_{\mathbf{X}} ||\mathbf{X}||_0 \ \ subject\ to\ \ \mathbf{f}_{i,q} = \mathbf{D}\mathbf{X} \tag{27}$$

と与えられる．ここで，l^0 ノルム最小化問題は NP 困難であるが，$\mathbf{X}_0$ が十分にスパースである場合，l^1 ノルム最小化問題を解いて得た解 $\tilde{\mathbf{X}}_{l^1}$ に一致する．

$$\tilde{\mathbf{X}}_{l^1} = \arg\min_{\mathbf{X}} ||\mathbf{X}||_1 \ \ subject\ to\ \mathbf{f}_{i,q} = \mathbf{D}\mathbf{X} \tag{28}$$

この問題は多項式時間で解くことができる．従って，$\tilde{\mathbf{X}}_{l^1}$ における i 番目の人の係数ベクトル $\mathbf{x}_i$ とトレーニングテンプレートの行列 $\mathbf{D}$ の線形結合を用いて $\mathbf{f}_{i,q}$ を再近似し，テンプレート $\mathbf{f}_{i,q}$ と最も誤差の小さい i 番目の人物 C を識別結果とする．すなわち，

$$r_i = ||\mathbf{f}_{i,q} - \mathbf{D}\delta(\tilde{\mathbf{X}}_{l^1})_i||_2 \tag{29}$$

$$C = \arg\min_i r_i \tag{30}$$

ただし，

$$\delta(\tilde{\mathbf{X}}_{l^1})_i = [\mathbf{0}, ..., \mathbf{0}, \mathbf{x_i}, \mathbf{0}, ..., \mathbf{0}] \tag{31}$$

とする．

次に，上述の議論を保護テンプレートを用いた場合について拡張する．l^2 ノルム最小化問題の解は，

$$\tilde{\mathbf{X}}_{l^2} = \arg\min_{\mathbf{X}} ||\mathbf{X}||_2 \ \ subject\ to\ \ \mathbf{f}_{i,q} = \mathbf{D}\mathbf{X} \tag{32}$$

と記述される．保護テンプレート $\hat{\mathbf{f}}_{i,q}$ と保護されたトレーニングテンプレート $\hat{\mathbf{D}}$ との二乗誤差，

$$|\hat{\mathbf{f}}_{i,q} - \hat{\mathbf{D}}\tilde{\mathbf{X}}_{l^2}|^2 = 0 \tag{33}$$

に着目し，$\tilde{\mathbf{X}}_{l^2}$ について解くと，

$$\tilde{\mathbf{X}}_{l^2} = (\hat{\mathbf{D}}^T\hat{\mathbf{D}})^{-1}\hat{\mathbf{D}}^T\hat{\mathbf{f}}_{i,q} \tag{34}$$

となる．このとき，式 (13) を用いると，$\hat{\mathbf{D}}^T\hat{\mathbf{D}}$ は，

$$\begin{aligned} \hat{\mathbf{D}}^T\hat{\mathbf{D}} &= [\hat{\mathbf{f}}_{1,1}, \hat{\mathbf{f}}_{1,2}, ..., \hat{\mathbf{f}}_{K,M}]^T[\hat{\mathbf{f}}_{1,1}, \hat{\mathbf{f}}_{1,2}, ..., \hat{\mathbf{f}}_{K,M}] \\ &= \{\sum_{n=0}^{N-1} \hat{f}_{i,j}(n)\hat{f}_{l,o}(n)\}, \qquad (1 \leqq i,l \leqq K, 1 \leqq j,o \leqq M) \\ &= \{\sum_{n=0}^{N-1} f_{i,j}(n)f_{l,o}(n)\} = \mathbf{D}^T\mathbf{D} \end{aligned} \tag{35}$$

と表現される．また，$\hat{\mathbf{D}}^T\hat{\mathbf{f}}_{i,q}$ も同様に変換によって，

$$\begin{aligned} \hat{\mathbf{D}}^T\hat{\mathbf{f}}_{i,q} &= [\hat{\mathbf{f}}_{1,1}, \hat{\mathbf{f}}_{1,2}, ..., \hat{\mathbf{f}}_{K,M}]^T\hat{\mathbf{f}}_{i,q} \\ &= \{\sum_{n=0}^{N-1} \hat{f}_{i,j}(n)\hat{f}_{i,q}(n)\}, \qquad (1 \leqq i,j \leqq K) \\ &= \{\sum_{n=0}^{N-1} f_{i,j}(n)f_{i,q}(n)\} = \mathbf{D}^T\mathbf{f}_{i,q} \end{aligned} \tag{36}$$

を得る．このことより，$\hat{\mathbf{X}}_{l^2}$ を求める行列計算において，保護テンプレートを用いた場合にも，テンプレートを用いた場合と

(a) 原画像　(b) テンプレート　(c) 保護テンプレート

図 4　ダウンサンプリング法により次元低減されたテンプレート例

同じ結果を得ることができることがわかる．式 (29) の場合においても同様に保護法の影響受けない．以上より，保護テンプレートによる認証は，l^2 ノルムにおいてテンプレートを直接用いた場合と同じ結果となる．

4. 実　　験

代表的な顔認証法に提案法を適用し，その有効性を評価する．

4.1 データベース

顔認証においては，代表的な顔画像データベースである The Extended Yale Face Database B [9] 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 32 枚，クエリに 32 枚に分けて実験を行った．すなわち，トレーニングテンプレートの数は M=1216 となる．クエリテンプレートの次元 N は，画像の特徴量の抽出条件に依存して決定される．

保護テンプレートの生成には，3.2 で述べた DFT による生成法を用い，$H_p(k)$ の決定に用いる $\theta_p(k)$ を，共役複素数と直流値の関係に注意し，ランダムな $\frac{\pi}{2}$ と $-\frac{\pi}{2}$ を用いた．

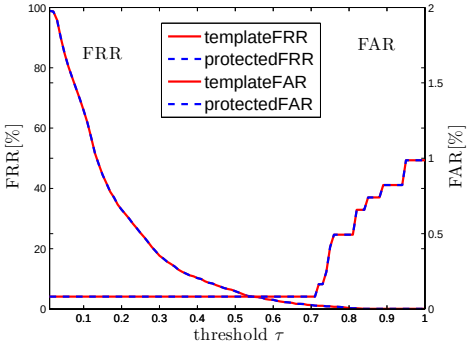
4.2 顔認証実験 (ダウンサンプリング法)

ダウンサンプリング法は，画像をダウンサンプリングにより，次元を低減し，それをテンプレートとする方法である．まず，192×168 の画像を，w×h($w < 192, h < 168$) にダウンサンプリングし，それをテンプレートとする．テンプレートへの提案法の適応例を図 4 に示す．ダウンサンプリング法による特徴抽出では，視覚的情報が残っているが，提案法によって視覚的情報の保護が可能となる．

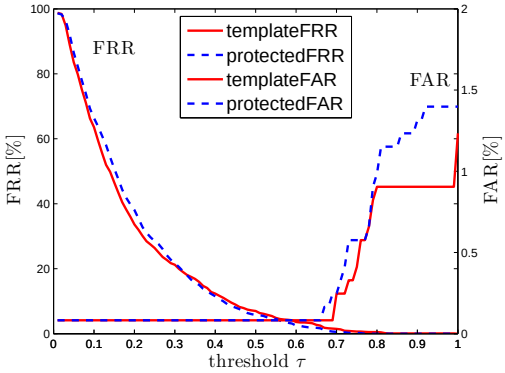
提案法により生成された保護テンプレートによる認証結果と，テンプレートを直接用いた認証結果を比較した．式 (29) の $\min r_i$ に対し，閾値 $\tau(0 \leqq \tau \leqq 1)$ を定め，$\min r_i \leqq \tau$ では受け入れ，$minr_i > \tau$ では拒否の判断をし，FRR（本人拒否率：False Rejection Rate）と FAR（他人受入率：False Acceptance Rate）をそれぞれ求めた．テンプレートの次元数 N(=w×h) がトレーニングテンプレートの数 M=1216 以上の場合 l^2 ノルム，$N < M$ の場合は l^1 ノルムの最小化問題を解き認証を行った．

図 5(a) は，N=48×42=2016，M=1216($N \geqq M$) の場合の結果である．提案法の特性とテンプレートを直接用いた特性が一致していることがわかる．すなわち，3.3 で述べた，保護テンプレートを用いてもテンプレートを直接用いた場合と同じ結果になることが実験的にも確認される．

図 5(b) は，N=16×14=224，M=1216($N < M$) の場合の結果である．l^1 ノルムを用いた場合，結果は完全一致はしないが，



(a) l^2 ノルム最小化 (N=2016，M=1216)



(b)l^1 ノルム最小化 (N=224，M=1216)

図 5　ダウンサンプリング法による FAR と FRR

識別性能は十分に維持している事がわかる．

4.3 顔認証実験 (ランダム射影法)

ランダム射影法は，元画像にランダム射影を施すことによって，次元を低減したテンプレートを生成する方法で，ダウンサンプリング法よりも高い認証率を持つ事が知られている．また，テンプレートは視覚的情報を持っておらず，保護テンプレートとなっている．しかし，視覚的情報を復元可能であるという脆弱性も指摘されている．ここでは，192×168=32256 画素の画像から得た 32256 次元のベクトルを，平均 0，分散 1 の正規分布に従う N 行 32256 列の行列との積としてランダム射影を行い，N 次元のベクトルを生成する．このテンプレートに提案法を適用した．その適応例を図 6 に示す．ランダム射影法による特徴抽出では，視覚的情報は失われている事がわかる．提案法の適用によって，認証精度を悪化させる事なく，保護テンプレートの安全性向上が期待される．本実験におけるその他の条件は，4.2 と同じである．

図 7(a) は，N=48×42=2016，M=1216($N \geqq M$) の場合の結果である．l^2 ノルムを用いた場合は，ランダム射影法においても，認証制度に影響しないことがわかる．

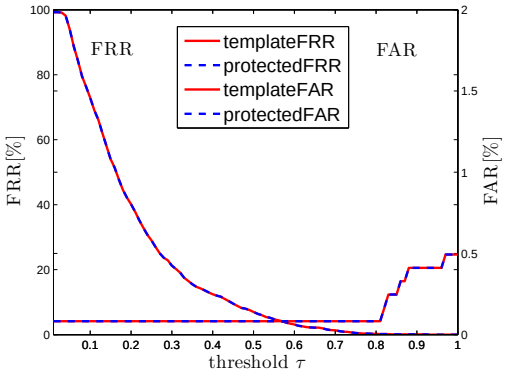
図 7(b) は，N=16×14=224，M=1216($N < M$) の場合の結果である．l^1 ノルムを用いた場合は，わずかに結果が一致しないが，ほぼ同じ結果が得られることがわかる．

4.4 クロスマッチング

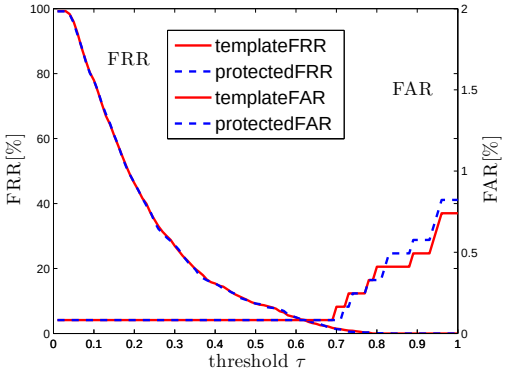
提案法のパラメータ $\theta_p(k)$ の違いとクロスマッチングの関係

(a) 原画像　　(b) テンプレート　　(c) 保護テンプレート

図 6　ランダム射影法により次元低減されたテンプレート例



(a) l^2 ノルム最小化 (N=2016，M=1216)



(b)l^1 ノルム最小化 (N=224，M=1216)

図 7　ランダム射影法による FAR と FRR

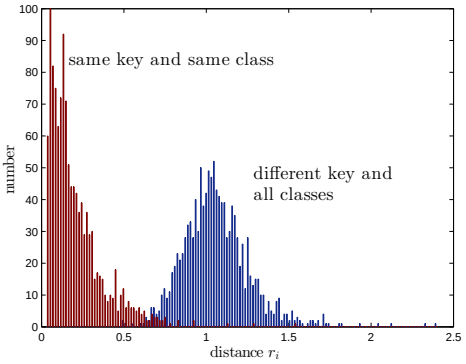


図 8　クロスマッチングについての検証

を検証した．図 8 は，ダウンサンプリング法にて特徴抽出して得たトレーニングテンプレートとクエリテンプレートに対して，式 (29) の距離 r_i を比較している．一方は，トレーニングとクエリに対して，異なる乱数列を用いて提案法を適用し，認証を行った結果であり，他方は，同じ人物のトレーニングとクエリに対して，同一の乱数列を用いて提案法を適用したものである．異なる乱数列を用いた際の r_i と，同一の乱数列を用いた際の r_i のヒストグラムが殆ど重なり合わないことが確認される．

5. おわりに

本稿では，直交変換と乱数列を用いた，テンプレート間のユークリッド距離を保存する方法を提案し，その保護テンプレートへの応用について述べた．ユークリッド距離の相対関係が保存されたテンプレートの使用により，l^2 ノルム最小化問題に対して影響を与えないことを理論的に示した．さらに，その妥当性を，顔認証において，ダウンサンプリング法とランダム射影法の条件で確認した．また，l^1 ノルム最小化問題の解に対しては，保護テンプレートの認証精度への影響はあるものの，その値が十分に保たれていることが確認された．

文　献

[1] N.K. Ratha, J.H. Connell, and R.M. Bolle, “Enhancing security and privacy in biometrics-based authentication systems,” IBM Syst. J. vol.40, no.3, pp.614-634, 2001.

[2] 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.

[3] 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.

[4] 古川 昌和, 村木 雄一, 藤吉 正明, 外村 喜秀, 貴家 仁志, “スパース表現に基づく顔識別のための保護テンプレート生成法,” 信学技報, vol.113, no.433, (no.IE2013-107), pp.73-78, Feb 2014.

[5] T. Izu, Y. Sakemi, M. Takenaka, N. Torii, ”キャンセラブル生体認証方式の安全性について (その 1),”第 3 回バイオメトリクスと認識・認証シンポジウム, Nov. 2013.

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

[7] 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.

[8] 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.

[9] 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.

[10] 奥井 宣広, 太田 陽基, 渡辺 龍, 三宅 優,”SIM カードを用いたテンプレート保護型リモート生体認証システムの提案,” 信学技法,vol.114, no.83, (no.BioX2014-3), pp.13-18, Jun 2014.

[11] 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.

[12] 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.