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.

生体認証のためのユニタリ変換に基づくテンプレート保護法の拡張とその応用

斉藤　裕子† 　中村　維吹†† 　塩田さやか† 　外村　喜秀††† 　貴家　仁志†

† 首都大学東京システムデザイン学部　〒 191-0065 東京都日野市旭が丘 6-6
†† 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: †{saito-yuko,nakamura-ibuki}@ed.tmu.ac.jp, ††{sayaka,kiya}@tmu.ac.jp,
†††tonomura.yoshihide@lab.ntt.co.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．テンプレート保護法は，異なる鍵を用いて保護されたテンプレート間でクロスマッチングが生じない，という条件を満たす必要がある．本稿では，ユニタリ変換に基づくテンプレート保護法を拡張することによって，クロスマッチング特性を改善する手法を提案する．提案法では，N 次のオリジナルテンプレートから，L 次 $(L \geqq N)$ の保護テンプレートが生成される．ユニタリ変換に基づくテンプレート保護法は，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共通にした場合，テンプレート間の内積が保存されるため，認証精度を低下することなく線形結合に基づく生体認証法を実行可能とする，という特徴を有する．提案法は，この特徴を保持し，さらにクロスマッチング性能の向上を可能とする．顔認証実験を行い，提案法のクロスマッチング特性に対する有効性を実験的に評価する．

キーワード　生体認証　テンプレート保護　キャンセラブルバイオメトリクス　クロスマッチング

An extension of the unitary transformation-based template protection method for biometrics and its application

Yuko SAITO†, Ibuki NAKAMURA††, Sayaka SHIOTA†, Yoshihide TONOMURA†††, and Hitoshi KIYA†

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

Abstract　Since biometric features are personal and irrevocable data, some schemes to protect the features (templates) extracted from biometric information are indispensable. In the template protection, it is required that the cross-matching between templates protected by different keys is avoidable. This paper proposes a scheme to improve cross-matching performance by extending the unitary transformation-based template protection method. The proposed scheme can generate L-dimensional $(L \geqq N)$ protected templates from N-dimensional original templates. When a common key among all templates is used, the convensional unitary transformation-based template protection method has the same recognition performance as that of non-protected method, under the linear combination approach. In this paper, it is shown that the proposed scheme keeps this property and, furthermore, can enhance the cross-matching performance. By doing some face recognition experiments, the effectiveness of the proposed scheme is evaluated.

Key words　Biometrics Template protection Cancelable biometrics Cross-matching

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. [1]

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 [2] 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，保護テンプレートを生成し，かつその状態で認証を可能とする技術である．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再度変換を行い，異なる保護テンプレートに変更することが可能である．

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生成法の先行研究に，ユニタリ変換に基づく保護法 [3]，ランダム射影を用いた方法 [4] などがある．テンプレート保護法の要求条件の 1 つに，異なる鍵を用いて保護されたテンプレート間でクロスマッチング生じないこと，がある．本稿では，ユニタリ変換に基づくテンプレート保護法 [3] を拡張することによって，クロスマッチング特性を改善する手法を提案する．提案法は，N 次のオリジナルテンプレートから，L 次（$L \geqq N$) の保護テンプレートを作成することを可能にし，L の選択と特徴ベクトルのスクランブリングによって，クロスマッチング特性を制御する．最後に，顔認証の実験を行い，提案法のクロスマッチング特性に対する有効性を評価する．

2. 準　　備

本節では、本稿で対象とする認証システムの概要，テンプレートの保護に必要とされる要件，対象とするクロスマッチングおよび，ユニタリ変換による保護テンプレートの生成 [3] について説明する．

2.1 認証システムの概要

指紋や顔などの生体情報は個人情報かつ変更不可能な情報であるため，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である．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 (鍵）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，鍵によって変換されたテンプレートを保護テンプレートという．鍵を変更することによって，一つのテンプレートから生成される保護テンプレートの更新や変更が可能となる．

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

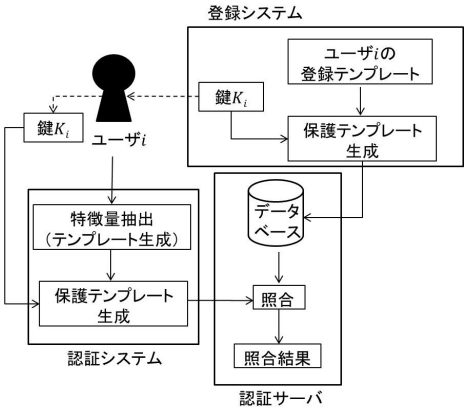


図 1: 認証システム

i 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．まず，ユーザ i は登録システムにおいて，生体情報からデータベース用にテンプレートを作成される．その後テンプレートは鍵 K_i によって保護テンプレートに変換され，認証サーバのデータベースに保存される．同時に，鍵 K_i はユーザ i に受け渡される．

認証時においては，ユーザ i は生体情報と自身の鍵 K_i を申請する．認証システムでは，登録システムと同様にテンプレートを生成し，鍵 K_i により保護テンプレートが作成される．その後保護テンプレートのみが認証サーバに送信され，事前に登録された保護テンプレートと照合される．

このシステムでは，ユーザ i の鍵 K_i が流出した場合でも，保護する際の鍵が一人一人異なるため，データベース上の他人の保護テンプレートには影響がない．さらに，鍵 K_i は鍵 $K_{i,1}, K_{i,2}$... と更新可能であるため，登録テンプレートを変更することができる．

2.2 テンプレート保護に必要とされる要件

生体認証では，生体情報から抽出された特徴量をテンプレートとし，それに基づいて認証を行う．そのため，テンプレートはプライバシー保護やセキュリティの観点から保護されていなければならない．テンプレートの保護は以下の 4 つの特性を満たすべきである [5].

（1） 多様性：異なる認証システム間において，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，認証サーバごとに異なる鍵でテンプレートが適切に変換される必要がある．

（2） 非可逆性：保護されたテンプレートから，オリジナルテンプレートを復元することが計算上困難であること．

（3） 精度：テンプレートの保護によって認証精度が下がらないこと．

（4） 破棄・更新：テンプレートが漏洩した場合に，登録されたテンプレートを消去でき，異なる鍵を使用することによって新たな保護テンプレートを同じ元画像から生成可能であること．

ユニタリ変換に基づくテンプレート保護法 [3] において，(2), (3), (4) の検討は十分になされており，特に (3) に関しては理

論的にも示されている．しかし，(1) に関しては十分評価されていない．

2.3 クロスマッチング

本稿において，異なる鍵で保護されたテンプレート間でマッチングすること，としてクロスマッチングを定義する．本研究では，先のユニタリ変換に基づくテンプレート保護法を拡張することによって，このクロスマッチング特性を改善する手法を提案する．この提案によって，同じ人物が異なる鍵によって保護された場合はもちろん，異なる人物が異なる鍵によって保護された場合においても特性が改善されることが期待される．

2.4 ユニタリ変換による保護テンプレートの生成

まず，2 つの生体情報のテンプレートにあたる特徴ベクトルを，$\mathbf{f}_i = [f_i(0), f_i(1), ..., f_i(N-1)]^T$，$\mathbf{f}_j = [f_j(0), f_j(1), ..., f_j(N-1)]^T$，ユニタリ行列を $\mathbf{A} = \{A(i,j), 0 \leqq i, j \leqq N-1\}$ とすると，$\mathbf{f}_i$，$\mathbf{f}_j$ をユニタリ変換したベクトル $\mathbf{F}_i$，$\mathbf{F}_j$ は

$$\mathbf{F}_i = \mathbf{A}\mathbf{f}_i,\ \mathbf{F}_j = \mathbf{A}\mathbf{f}_j \tag{1}$$

と与えられる．ここでは議論を簡単にするため，2 つのテンプレートを共通の鍵で保護すると仮定する．そこで，ある鍵 K を用いて生成される複素対角行列 $\mathbf{H}_K = \{H_K(p,p), 0 \leqq p \leqq N-1\}$ を用いて，

$$\hat{\mathbf{F}}_i = \mathbf{H}_K\mathbf{F}_i = \mathbf{H}_K\mathbf{A}\mathbf{f}_i \tag{2}$$

$$\hat{\mathbf{F}}_j = \mathbf{H}_K\mathbf{F}_j = \mathbf{H}_K\mathbf{A}\mathbf{f}_j \tag{3}$$

という新たなベクトルを生成する．ただし，$\mathbf{H}_K$ はエルミート転置 $\mathbf{H}_K^*$ を用いて $\mathbf{H}_K^*\mathbf{H}_K = \mathbf{I}$ ($|H_K(p,p)|^2 = 1$) であると仮定する．このとき，$\hat{\mathbf{F}}_i$，$\hat{\mathbf{F}}_j$ の逆変換 $\hat{\mathbf{f}}_i$，$\hat{\mathbf{f}}_j$ は，

$$\hat{\mathbf{f}}_i = \mathbf{A}^{-1}\hat{\mathbf{F}}_i = \mathbf{A}^{-1}\mathbf{H}_K\mathbf{A}\mathbf{f}_i \tag{4}$$

$$\hat{\mathbf{f}}_j = \mathbf{A}^{-1}\hat{\mathbf{F}}_j = \mathbf{A}^{-1}\mathbf{H}_K\mathbf{A}\mathbf{f}_j \tag{5}$$

と与えられる．以上より，

$$\begin{aligned}\hat{\mathbf{f}}_i \cdot \hat{\mathbf{f}}_j = \hat{\mathbf{f}}_i^*\hat{\mathbf{f}}_j &= (\mathbf{A}^{-1}\mathbf{H}_K\mathbf{A}\mathbf{f}_i)^*(\mathbf{A}^{-1}\mathbf{H}_K\mathbf{A}\mathbf{f_j}) \\ &= \mathbf{f}_i^*\mathbf{A}^{-1}\mathbf{H}_K^*\mathbf{A}\mathbf{A}^{-1}\mathbf{H}_K\mathbf{A}\mathbf{f}_j \\ &= \mathbf{f}_i^*\mathbf{f}_j = \mathbf{f}_i \cdot \mathbf{f}_j \end{aligned} \tag{6}$$

が成り立つ．また，このとき $\hat{\mathbf{f}}_\mathbf{i}$，$\hat{\mathbf{f}}_\mathbf{j}$ 間のユークリッド距離は，(6) より

$$|\hat{\mathbf{f}}_i - \hat{\mathbf{f}}_j|^2 = |\mathbf{f}_i - \mathbf{f}_j|^2 \tag{7}$$

となる．式 (6) および式 (7) より，$\hat{\mathbf{f}}_i$，$\hat{\mathbf{f}}_j$ は，$\mathbf{f}_i$，$\mathbf{f}_j$ 間の内積およびユークリッド距離を保存していることがわかる．

従って，$\mathbf{H}^*{}_K\mathbf{H}_K = \mathbf{I}$ となるような対角行列 $\mathbf{H}_K = \{H_K(p,p), 0 \leqq p \leqq N-1\}$ を鍵 K を用いて生成することによって，$\mathbf{f}_i$，$\mathbf{f}_j$ 間の内積および距離を保持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である．

3. 提 案 法

3.1 DFT による保護テンプレートの生成 ($L = N$ の場合)

2.4 で示した保護テンプレートの生成法に基づき，ユニタリ変換である DFT 変換を用いた保護テンプレートの生成法を説明する．本稿では特に，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する方法を提案する．まず，ここで，$N = L$ の場合について述べる．

まず，N 次元のテンプレート $\mathbf{f}_i = [f_i(0), f_i(1), ..., f_i(N-1)]^T$ に対して DFT を施す．

$$F_i(k) = \frac{1}{\sqrt{N}}\sum_{n=0}^{N-1} f_i(n)W_N^{nk},\ \ k = 0, 1, ..., N-1 \tag{8}$$

ただし，$W_N^{nk} = \mathrm{e}^{j\frac{2\pi}{N}}$ である．次に，鍵 K によってランダムに生成した $\theta_K(k)$ を用いて，

$$H_K(k) = \mathrm{e}^{j\theta_K(k)},\ \ k = 0, 1, ..., N-1 \tag{9}$$

と定義する．このとき，$|H_K(k)|^2 = 1$ であることは自明である．すなわち，$H_K(p,p) = H_K(k)$ とおくことによって，$|H_K(p,p)|^2 = 1$ が成立する．ここで，(9) を使って，

$$\hat{F}_i(k) = H_K(k) \cdot F_i(k),\ \ k = 0, 1, ..., N-1 \tag{10}$$

を求める．さらに逆 DFT を施し，

$$\hat{f}_i(n) = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} \hat{F}_i(k) \cdot W_N^{-nk} \tag{11}$$

とし，$\hat{\mathbf{f}}_i = [\hat{f}_i(0), \hat{f}_i(1), ..., \hat{f}_i(N-1)]^T$ を N 次元の保護テンプレートとする．本稿では，この DFT による保護手順を位相スクランブルと呼ぶ．

(a) 原画像 (テンプレート)　　(b) 保護テンプレート

図 2: 保護テンプレートの生成例

保護テンプレートの生成例として，図 2(a) に原画像 (テンプレート)，図 2(b) に DFT によって変換された保護テンプレートの例を示す．DFT を施すことによって，視覚的に保護できることがわかる．また，視覚的情報に限らず任意の特徴量を DFT によって保護することができる．

3.2 線形結合表現を用いた生体認証

ここでは，本実験に用いた生体認証法である，線形結合表現に基づく方法 [6] を説明する．

今，データベースの登録者を R 人と仮定し，各登録者に M_i 枚画像が準備される．M_i 枚の画像から特徴抽出を行い登録者 i のトレーニングテンプレートとして登録する．i 番目 ($i = 1, 2, ..., R$) の登録者における q 枚目 ($q \in \{1, 2, ..., M_i\}$) の画像のテンプレートを $\mathbf{f}_{i,q}$ としたとき，i 番目の登録者の M_i 個のテンプレートを，$\mathbf{D}_i = [\mathbf{f}_{i,1}, \mathbf{f}_{i,2}, ..., \mathbf{f}_{i,M_i}]$ と表現する．いま，i 番目の登録者に属するクエリ画像から特徴抽出を行い，クエリテンプレート $\mathbf{y}$ とする．さらに，$\mathbf{y}$ は i 番目のトレーニングテンプレートで線形近似されると仮定すると，

$$\mathbf{y} = \mathbf{f}_{i,1}x_{i,1} + \mathbf{f}_{i,2}x_{i,2} + ... + \mathbf{f}_{i,M_i}x_{i,Mi} = \mathbf{D}_i\mathbf{x}_i \quad (12)$$

と表される．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，R 人のすべてのトレーニングテンプレートを用いて，$\mathbf{y}$ は次のように表現される．

$$\mathbf{y} = \mathbf{D}_1\mathbf{0} + \mathbf{D}_2\mathbf{0} + ... + \mathbf{D}_i\mathbf{x}_i + ... + \mathbf{D}_R\mathbf{0} = \mathbf{D}\mathbf{x}_0 \quad (13)$$

ただし

$$\mathbf{D} = [\mathbf{D}_1, \mathbf{D}_2, ..., \mathbf{D}_R] \quad (14)$$

$$\mathbf{x}_0 = [\mathbf{0}, ..., \mathbf{0}, \mathbf{x}_i, \mathbf{0}, ..., \mathbf{0}] \quad (15)$$

であり，係数行列 $\mathbf{x}_0$ の i 番目の登録者以外の要素はすべて 0 になる．$\mathbf{x}_0$ を以下の式に基づいて推定する．

$$\tilde{\mathbf{x}}_0 = \arg\min_{\mathbf{x}} \|\mathbf{x}\|_2 \quad subject\ to\ \ \mathbf{y} = \mathbf{D}\mathbf{x} \quad (16)$$

従って，$\tilde{\mathbf{x}}_0$ と式 (13) に基づいて $\mathbf{y}$ を再近似する．最後に i 番目の人物に対して再構成されたテンプレート $\mathbf{D}\delta_i(\tilde{\mathbf{x}}_0)$ とテンプレート $\mathbf{y}$ と，の誤差を最小にする人物 C を識別結果とする．すなわち，

$$r_i = \|\mathbf{y} - \mathbf{D}\delta_i(\tilde{\mathbf{x}}_2)\|_2 \quad (17)$$

$$C = \arg\min_i r_i \quad (18)$$

ここで，$\delta_i(\tilde{\mathbf{x}}_0)$ は i 番目の登録者に無関係な登録テンプレートに対する係数をゼロに置き換える関数である．すなわち，

$$\delta_i(\tilde{\mathbf{x}}_0) = [\mathbf{0}, ..., \mathbf{0}, \tilde{\mathbf{x}}_{0,i}, \mathbf{0}, ..., \mathbf{0}] \quad (19)$$

と定義される．式 (17) の r_i を，登録者 i の推定二乗誤差と呼ぶ．

ここから，上述の認証法において保護テンプレートを用いた場合について説明する．式 (16) は，保護クエリテンプレート $\hat{\mathbf{y}}$ と保護トレーニングテンプレート $\hat{\mathbf{D}}$ の場合に拡張すると，

$$\tilde{\mathbf{x}}'_0 = \arg\min_{\mathbf{x}} \|\mathbf{x}\|_2 \quad subject\ to\ \ \hat{\mathbf{y}} = \hat{\mathbf{D}}\mathbf{x} \quad (20)$$

と表せる．保護クエリテンプレート $\hat{\mathbf{y}}$ と，保護トレーニングテンプレート $\hat{\mathbf{D}}\mathbf{x}$ との最小平均二乗誤差に着目し，$\tilde{\mathbf{x}}'_0$ について解くと，

$$\tilde{\mathbf{x}}'_0 = (\hat{\mathbf{D}}^*\hat{\mathbf{D}})^{-1}\hat{\mathbf{D}}^*\hat{\mathbf{y}} \quad (21)$$

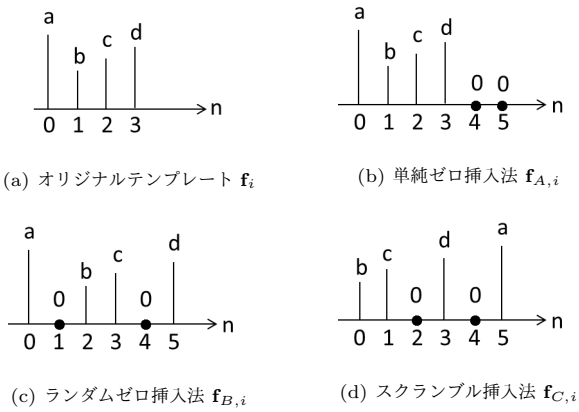
となる．このとき，式 (6) より，

$$\hat{\mathbf{D}}^*\hat{\mathbf{D}} = \mathbf{D}^*\mathbf{D},\ \hat{\mathbf{D}}^*\hat{\mathbf{y}} = \mathbf{D}^*\mathbf{y} \quad (22)$$

となる．よって，$\tilde{\mathbf{x}}'_0 = \tilde{\mathbf{x}}_0$ である．これは，内積が保存される場合式 (6) において，オリジナルテンプレートを用いた場合と，保護テンプレート場合の認証結果が同じになることを示している．

3.3 DFT による保護テンプレートの生成 ($L \geqq N$ の場合)

N 次のテンプレートより，L 次 ($L \geq N$) の保護テンプレートを生成する方法を提案する．提案法の例を図 3 に示す．



(a) オリジナルテンプレート $\mathbf{f}_i$　(b) 単純ゼロ挿入法 $\mathbf{f}_{A,i}$

(c) ランダムゼロ挿入法 $\mathbf{f}_{B,i}$　(d) スクランブル挿入法 $\mathbf{f}_{C,i}$

図 3: 提案法の例 ($N = 4, L = 6$)

A　単純ゼロ挿入法

いま，N 次のテンプレート $\mathbf{f}_i$ の末尾に，値 0 の要素を Z 個追加し，$L = N + Z$ 次のテンプレート $\mathbf{f}_{A,i}$ として再定義する (図 3(b))．このとき，$f_{A,i}(n)$ についての L 点 DFT，$F_{A,i}(k)$ を求め，さらに式 (10) と同様に

$$\hat{F}_{A,i}(k) = F_{A,i}(k)\mathrm{e}^{j\theta_K(k)} \quad (23)$$

を生成する．このとき，この $\hat{F}_{A,i}(k)$ の L 点逆 DFT，$\hat{f}_{A,i}(n)$ が以下の性質を持つことを確認することができる．

$$\sum_{n=0}^{N-1} f_i(n)f_j(n) = \sum_{n=0}^{L-1} \hat{f}_{A,i}(n)\hat{f}_{A,j}(n) \quad (24)$$

以上のように，内積を保存した，L 次の保護テンプレート $\hat{\mathbf{f}}_{A,i}, \hat{\mathbf{f}}_{A,j}$ が生成されることがわかる．

B　ランダムゼロ挿入法

N 次のテンプレート $\mathbf{f}_i$ の要素間のランダムな位置に，値 0 を Z 個挿入し，$L = N + Z$ 次のテンプレート $\mathbf{f}_{B,i}$ として再定義する (図 3(c))．このとき，A と同様に，内積を保存した L 次の保護テンプレート $\hat{\mathbf{f}}_{B,i}, \hat{\mathbf{f}}_{B,j}$ が生成される．

C　スクランブル挿入法

まず，N 次のテンプレート $\mathbf{f}_i$ の各要素の位置をランダムに入れ換える．その後，B と同様に値 0 の要素をランダムに Z 個挿入し，$L = N + Z$ 次のテンプレート $\mathbf{f}_{C,i}$ として再定義する (図 3(d))．このとき，A，B と同様に，内積を保存した L 次の保護テンプレート $\hat{\mathbf{f}}_{C,i}, \hat{\mathbf{f}}_{C,j}$ が生成される．

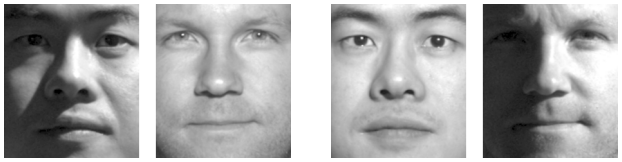
本稿では，これら 3 つの提案法を考察する．すべて，鍵を共通にした場合 ($K_i = K_j$)，オリジナルテンプレートを用いた場合と同じ認証結果を与える．すなわち，認証特性に影響を与えない保護テンプレートとなっている．しかし，鍵が異なる場合には，4 節で示すようにクロスマッチングの性能に違いがある．

4. 実　　験

本節では，顔画像を用いて，提案法のクロスマッチング特性に対する有効性を実験的に評価する．

4.1 設 定 条 件

実験においては，顔画像のデータベースである The Extended



(a) クエリ画像　　(b) データベース画像

図 4: データベースの画像例

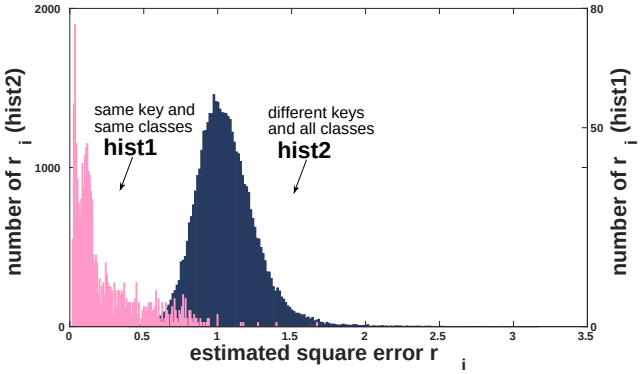


図 5: クロスマッチング特性の評価 ($L = N$)

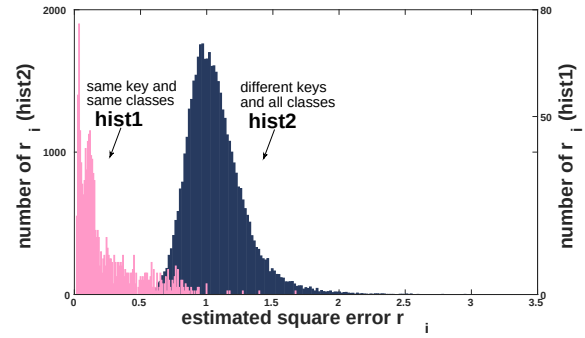
Yale Face Database B [7] を用いた．38 人を様々な照明条件下で撮影した顔画像が，1 人 64 枚ずつ計 2432 枚で構成されている．画像サイズはすべて 192×168 である．1 人につき 32 枚をデータベース画像，残り半分の 32 枚をクエリにわけて実験を行った．図 4 にこのデータベースの画像例を示す．

保護テンプレートの生成には 3.1 で述べた DFT による生成法を用い，パラメータ $\theta_K(k)$ には 4 値 $(0, \frac{\pi}{2}, -\frac{\pi}{2}, \pi)$ をランダムに使用した．一方，特徴抽出にはダウンサンプリング法を用いた．ダウンサンプリング法は，画像をダウンサンプリングすることにより，次元を低減し，それをテンプレートとする方法である．今回の実験では，198×168 の画像を 48×42 にダウンサンプリングし，それをテンプレートとした．

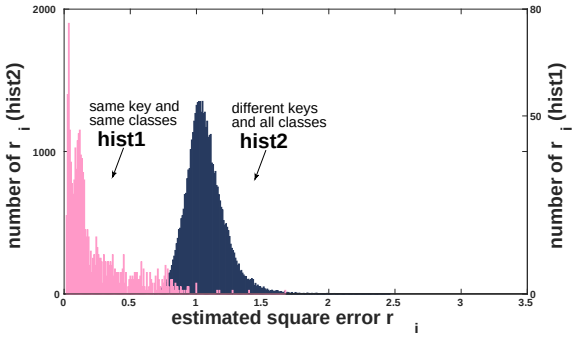
4.2 クロスマッチングの評価

オリジナルテンプレートの次元 N と，保護テンプレートの次元 L が等しい場合 ($L = N$) のクロスマッチングの関係を図 5 に示す．トレーニングテンプレートとクエリテンプレートに共通の鍵 $\theta_K(k)$ を施し，かつ両テンプレートの人物が同じときの推定二乗誤差 r_i の度数をヒストグラム 1(hist1) に示した．また，両テンプレートに対して異なる鍵を用いて保護したときの，クエリと全ての登録者間の推定二乗誤差の度数がヒストグラム 2(hist2) である．この時，この 2 つのヒストグラムのオーバーラップ数は，クロスマッチングの発生度合に対応する．図 5 では，オーバーラップした推定二乗誤差 r_i の数は 242 であり，これは hist1 の度数の総和を分母とすると，20.0%に相当する．

次に，クエリテンプレートから $L = N + Z$ 次元の保護テンプレートを作成する．一方，トレーニングテンプレートは N 次元の保護テンプレートとして作成される．ただし，認証計算を可能にするため，トレーニングテンプレートの末尾に値 0 の要素を Z 個追加し，次元を合わせている．単純ゼロ挿入法を用いたときの結果を図 6 に示す．ヒストグラム 1 は図 5 のヒストグラム 1 と同じであり，ヒストグラム 2 は単純ゼロ挿入法を用いた場合の認証結果である．同様に，ランダムゼロ挿入法の結果を図 7 に，スクランブル挿入法の結果を図 8 に示す．また，それぞれの提案法における，両ヒストグラム間においてオーバーラップした推定二乗誤差 r_i の度数とそのパーセンテージを表 1 に示す．



(a) 値 0 の要素を 100 追加



(b) 値 0 の要素を 1000 追加

図 6: 単純ゼロ挿入法のクロスマッチングの評価 ($L \geqq N$)

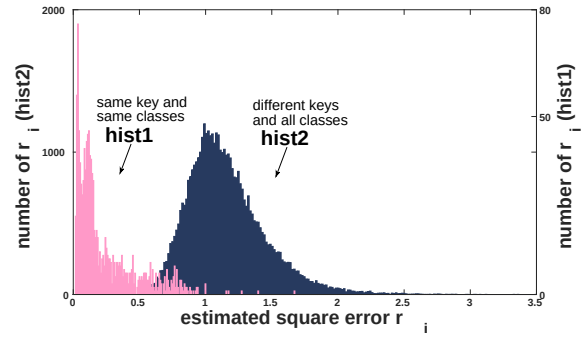
表 1: ヒストグラム間のオーバーラップ r_i の度数とそのパーセンテージ

追加したゼロの数	単純ゼロ挿入	ランダムゼロ挿入	スクランブル挿入
100	178 (14.6%)	189 (15.5%)	158 (13.0%)
500	119 (9.79%)	88 (7.24%)	75 (6.17%)
1000	88 (7.23%)	27 (2.22%)	18 (1.48%)
1500	106 (8.72%)	19 (1.56%)	14 (1.15%)

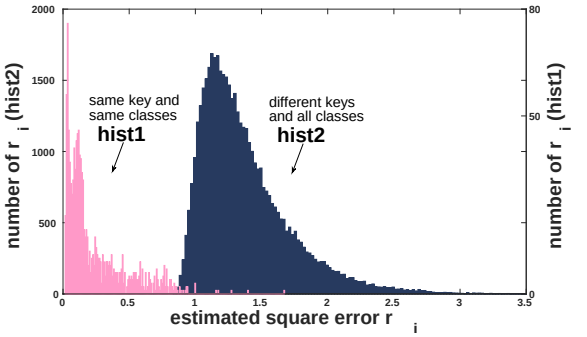
これらの実験結果より，N 次のオリジナルテンプレートから，L 次 ($L \geqq N$) の保護テンプレートを生成することで，クロスマッチング特性の改善効果があることがわかる．どの提案法においても次元数を増やすほど，クロスマッチング性能が向上している．提案法の中で特に，スクランブル挿入法が一番有効な結果を与えている．

5. おわりに

本稿では，ユニタリ変換に基づくテンプレート保護法 [3] を拡張することによって，クロスマッチング特性が改善される手

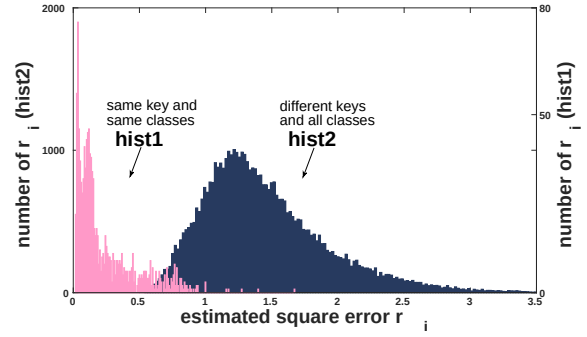


(a) 値 0 の要素を 100 追加

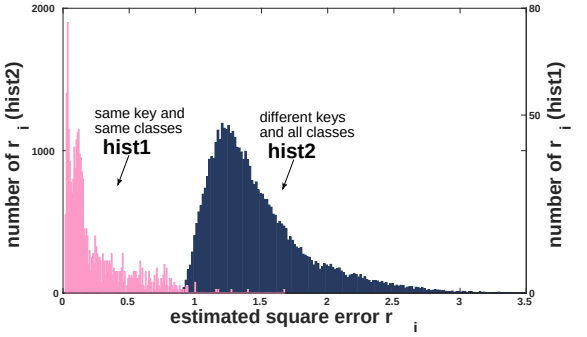


(b) 値 0 の要素を 1000 追加

図 7: ランダムゼロ挿入法のクロスマッチング評価 ($L \geqq N$)



(a) 値 0 の要素を 100 追加



(b) 値 0 の要素を 1000 追加

図 8: スクランブル挿入法のクロスマッチング評価 ($L \geqq N$)

法を提案した．まず，この提案法が，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共通にした場合，テンプレート間の内積が保存され，認証特性を劣化させないことを示した．さらに，この性質を保持したまま提案法がクロスマッチング性能の向上を可能であることを示すために，顔認証実験を行い，クロスマッチング特性に対する有効性を評価した．その結果，提案法がクロスマッチング特性に有効であることが確認された．

文　　献

[1] C.Rathgeb，and A. Uhl，”A survey on biometric cryptosystems and cancelable biometrics，” EURASIP Journal on Information Security，vol.2011，no.1，pp 1-25，2011.

[2] 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.

[3] 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 ,” 信学技報, vol. 114, no. 205, SIS2014-52, pp. 7-12, Sep.2014.

[4] 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.

[5] A.K.Jain，K.Nandakumar，and A.Nagar，”Biometric template security，” EURASIP Journal on Advances in Signal Processing 2008.

[6] 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.

[7] 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.