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.

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

斉藤　裕子†　塩田さやか††　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
†† 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
E-mail: †saito-yuko@ed.tmu.ac.jp, ††{sayaka,kiya}@tmu.ac.jp

あらまし　テンプレート保護法の一つとして，ランダム・ユニタリ行列に基づく保護法が研究されている．先行研究では，要素が固定値であるユニタリ行列と，要素値がランダム性を持つユニタリ行列を 1 つずつ組み合わせた変換が提案された．これは，グラムシュミットの直交化法に基づく生成法に比べ，計算量が少なく，かつ整数値の保護テンプレートが生成できる．しかし，それらの方法では，クロスマッチング性能および保護テンプレートのランダム性が，使用されるランダム行列に依存することが指摘されている．本稿では，この課題を解決するような新たなランダム・ユニタリ行列の生成法を提案する．提案法は，要素が固定値であるユニタリ行列を 1 つと，要素値がランダム性をもつユニタリ行列を 2 つ，計 3 つの行列を用いて保護を行う．ランダムな行列として，ランダムな正負符号を持つパーミュテーション行列を用いることを提案する．最後に顔認証実験に提案法を適用して，クロスマッチング性能，保護テンプレートのランダム性について評価を行い，提案法の有効性を示す．
キーワード　生体認証　保護テンプレート　ランダム・ユニタリ行列

A generation scheme of random unitary matrices for template protection

Yuko SAITO†, Sayaka SHIOTA††, 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
E-mail: †saito-yuko@ed.tmu.ac.jp, ††{sayaka,kiya}@tmu.ac.jp

Abstract　Random unitary matrices-based template protection methods have been proposed as one of biometric template protection schemes. In the prior studies, a template is protected by two matrices, i.e, an unitary matrix with fixed values and one with random values. These methods have lower calculation costs than these of the Gram-Schmidt orthogonalization, and can also generate integer protected templates. However, these methods have been pointed out that the cross matching performance and the randomness of a protected template depend on the combination of random unitary matrices. In this study,to overcome these problems, we propose a new generation method of a random unitary matrix. In the proposed method, a template is protected by three matrices, i.e, an unitary matrix with fixed values and two unitary matrix with random values. In addition, we propose to use a permutation matrix having plus or minus sign in a random order as a random matrix. We perform some face recognition experiments to evaluate the cross matching performance and the randomness of a protected template and show the effectiveness of the proposed scheme.
Key words　Biometrics, Template protection, random unitary matrices

1. ま え が き

近年，様々なシステムにおいて，安全性のためユーザ認証が行われている．パスワードや IC カードを用いた認証は，共有や置き忘れ，盗難などが容易である点から，十分に信頼できるものとはいえない．それに比べ，生体認証は，そのさまざま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]．ランダム・ユニタリ行列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．ランダム・ユニタリ行列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 [8]．さらに，この保護法はテンプレート保護を行う枠組みの一つである，キャンセラブルバイオメトリクスに分類される．この方法では，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，定期的に異なる保護テンプレートに更新することが求められる．そのため，保護テンプレートの生成および更新を少ない計算量で行うことが必要となる．

しかしながら，ランダム・ユニタリ行列の代表的な生成法である，グラムシュミットの直交化法に基づく保護法 [9] においては，ある鍵から初期生成した行列を直交化させるため，計算量が大きい．また，行列が実数値であるため，整数値の保護テンプレートの生成が困難である．そこで，少ない計算量で，かつ使用するユニタリ行列によっては整数値の保護テンプレートを生成可能な，ランダム・ユニタリ行列に基づく保護法が提案されている [8], [10]〜[12]．この方法では，要素が固定値であるユニタリ行列と要素値がランダム性をもつユニタリ行列を 1 つずつ組み合わせてテンプレートの保護を行う．しかし，この方法では，クロスマッチング性能および保護テンプレートのランダム性が使用するランダム行列に依存することが指摘されている [13]．

そこで本稿では，これらの問題を解決するような，新たなランダム・ユニタリ行列の生成法を提案する．提案法は，要素が固定値である行列を 1 つと，要素値がランダム性をもつユニタリ行列を 2 つ，計 3 つの行列を用いてテンプレートの保護を行う．ランダム性をもつ行列として，新たにランダムに正負符号をもつパーミュテーション行列を使用する．最後に，顔認証実験によって，クロスマッチング性能および保護テンプレートのランダム性が改善されていることを確認する．

2. 準　　備

本節では、本稿で対象とする生体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およびユニタリ変換の性質について説明する．

2.1 生体認証システムの概要

図 1 は，本稿で想定する，各ユーザ毎に個別のパラメータ $\mathbf{p}_i$，

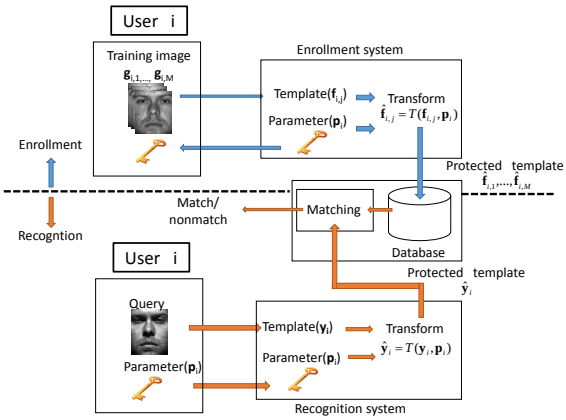


図 1: 認証システム

$i = 1, 2, ..., K$，によって保護を行う生体認証システムの概要である．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 $\mathbf{f}_{i,j}$ を抽出する．その後テンプレートに特徴変換 $T(\cdot)$ を適用して，保護テンプレート $\hat{\mathbf{f}}_{i,j} = T(\mathbf{f}_{i,j}, \mathbf{p}_i)$ の生成を行う．最後にデータベースへ，保護テンプレートのみを登録する．また，認証時には，ユーザ i は，パラメータ $\mathbf{p}_i$ 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 $T(\cdot)$ を適用する．最後に，変換されたクエリ $T(\mathbf{y}_{i,j}, \mathbf{p}_i)$ をデータベース内の特徴量と認証を行う．このように，パラメータ $\mathbf{p}_i$ を用いるシステムは，キャンセラブルバイオメトリクスシステムとして知られている [14]．

全てのユーザに同じパラメータ $\mathbf{p}_i$ を使用したとき，すなわち $\mathbf{p}_1 = \mathbf{p}_2 = ... = \mathbf{p}_k$ のときには，ユーザ分類を実行するシステムとなる．その際鍵は登録システムと認証システムに安全に保管されることとなる．

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 [4]．

（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．

ランダム・ユニタリ行列に基づくテンプレート保護法 [8], [10] は，(3) および (4) の要件を十分に満たすことができる．しか

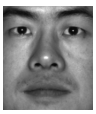


(a) template A (b) template B

図 2: オリジナルテンプレート



(a) template A (b) template B

図 3: 保護テンプレート

し，(1) および (2) の要件については，使用されるランダム行列に依存し，適切なランダム行列の設計が課題となっている．さらに，テンプレートが整数値である場合でも，保護テンプレートの値が実数値となってしまい，量子化誤差等の影響が指摘されている．そこで本稿では，これらの課題を解決するような新たなランダム・ユニタリ行列の生成法を提案する．

2.3 ランダム・ユニタリ行列によるテンプレート保護

$N \times N$ 行列のランダム・ユニタリ行列を $\mathbf{Q}_{\mathbf{p}_i} = \{Q_{\mathbf{p}_i}(i,j), 0 \leqq i,j \leqq N-1\}$ とする．さらに，$\mathbf{Q}_{\mathbf{p}_i}$ の要素 $Q_{\mathbf{p}_i}(i,j)$ はパラメータである鍵 $\mathbf{p}_i$ によってランダムに決定される．すなわち，行列の要素が鍵 $\mathbf{p}_i$ によってランダムに生成され，かつ $\mathbf{Q}_{\mathbf{p}_i}$ がユニタリ性を有する行列をランダム・ユニタリ行列と本稿では呼ぶ．

一般に，テンプレート $\mathbf{f}_{i,j} \in \mathbb{R}^N$ を，鍵 $\mathbf{p}_i$ の下で，ランダム・ユニタリ行列 $\mathbf{Q}_{\mathbf{p}_i} \in \mathbb{C}^{N\times N}$ によって変換 $(T(\mathbf{f}_{i,j}, \mathbf{p}_i))$ した保護テンプレート $\hat{\mathbf{f}}_{i,j}$ は，

$$\hat{\mathbf{f}}_{i,j} = T(\mathbf{f}_{i,j}, \mathbf{p}_i) = \mathbf{Q}_{\mathbf{p}_i}\mathbf{f}_{i,j} \tag{1}$$

と与えられる．

ここで，図 2 にテンプレート例，図 3 にそれらの保護テンプレート例を示す．図 3 からオリジナルテンプレートの視覚的情報が保護されていることがわかる．

また，ランダム・ユニタリ行列 $\mathbf{Q}_{\mathbf{p}_i}$ は以下を満たす．

$$\mathbf{Q}^*_{\mathbf{p}_i}\mathbf{Q}_{\mathbf{p}_i} = \mathbf{I} \tag{2}$$

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．

ここで，2 つのテンプレート $\mathbf{f}_{i,j} = [f_{i,j}(1), ..., f_{i,j}(N)]$, $\mathbf{f}_{s,t} = [f_{s,t}(1), ..., f_{s,t}(N)]$ を，共通のランダム・ユニタリ行列 $\mathbf{Q}_{p_i}$ で変換した場合の性質を以下に示す [8]．ここで，$\hat{\mathbf{f}}_{i,j} = \left[\hat{f}_{i,j}(1), ..., \hat{f}_{i,j}(N)\right]$, $\hat{\mathbf{f}}_{s,t} = \left[\hat{f}_{s,t}(1), ..., \hat{f}_{s,t}(N)\right]$ はそれぞれ $\mathbf{f}_{i,j}$,$\mathbf{f}_{s,t}$ の保護テンプレートを表す．

Property 1: ユークリッド距離の保存

$$\sqrt{\textstyle\sum_k (f_{i,j}(k) - f_{s,t}(k))^2} = \sqrt{\textstyle\sum_k (\hat{f}_{i,j}(k) - \hat{f}_{s,t}(k))^2}$$

Property 2: 内積の保存

$$\textstyle\sum_k f^*_{i,j}(k) f_{s,t}(k) = \sum_k \hat{f}^*_{i,j}(k)\hat{f}_{s,t}(k)$$

Property 3: 相関の保存

$$\frac{\sum_k (f_{i,j}(k)-\bar{f}_{i,j})(f_{s,t}(k)-\bar{f}_{s,t})}{\sqrt{\sum_k (f_{i,j}(k)-\bar{f}_{i,j})^2}\sqrt{\sum_k (f_{s,t}(k)-\bar{f}_{s,t})^2}} = \frac{\sum_k (\hat{f}_{i,j}(k)-\bar{\hat{f}}_{i,j})(\hat{f}_{s,t}(k)-\bar{\hat{f}}_{s,t})}{\sqrt{\sum_k (\hat{f}_{i,j}(k)-\bar{\hat{f}}_{i,j})^2}\sqrt{\sum_k (\hat{f}_{s,t}(k)-\bar{\hat{f}}_{s,t})^2}}$$

Property 4: l^2 ノルムに基づく認証結果の保存

全てのユニタリ変換に基づく保護法はこれらの性質を持つ．

保護テンプレートの生成において，$\mathbf{Q}_{\mathbf{p}_i}$ はユニタリ性に加え，ランダム性を有する必要がある．$\mathbf{Q}_{\mathbf{p}_i}$ を生成する一般的な方法として，グラムシュミットの直交化法によって，ある鍵から初期生成した行列を直交化させる方法がある [9]．しかしながら，グラムシュミットの直交化法は一般に $\mathcal{O}(N^3)$ の計算コストが必要である．また，行列が実数値であるため，テンプレートが整数値の場合においても，整数値の保護テンプレートの生成が困難である．

これらの問題を解決するような，ランダム・ユニタリ行列の生成法 [8], [10] が提案されている．この方法では，テンプレート $\mathbf{f}_i$ を，2 つのユニタリ行列 $\mathbf{A} = \{A(i,j), 0 \leqq i,j \leqq N-1\}$, $\mathbf{H}_{\mathbf{p}_i} = \{H_{\mathbf{p}_i}(i,j), 0 \leqq i,j \leqq N-1\}$ を用いて変換する．ただし，$\mathbf{A}$ は，単位行列，離散フーリエ変換（DFT），離散コサイン変換（DCT），アダマール変換などの固定行列である．$\mathbf{H}_{\mathbf{p}_i}$ はランダム性を持つユニタリ行列とする．このとき，保護テンプレート $\hat{\mathbf{f}}_i$ を，

$$\hat{\mathbf{f}}_i = \mathbf{Q}_{\mathbf{p}_i}\mathbf{f}_i = (\mathbf{H}_{\mathbf{p}_i}\mathbf{A})\mathbf{f}_i \tag{3}$$

のように生成することができる．この方法では，すでにユニタリ性をもつ行列を直接使用するため，グラムシュミットの直交化法のような，行列を直交化する操作を必要としない．しかし，上述の要件 (1) および (2) が使用する行列の種類によって依存することが指摘されている．

3. 提 案 法

本節では，クロスマッチングが生じにくく，かつ高いランダム性を有する保護テンプレートの生成を可能とするランダム・ユニタリ行列の生成法を提案する．

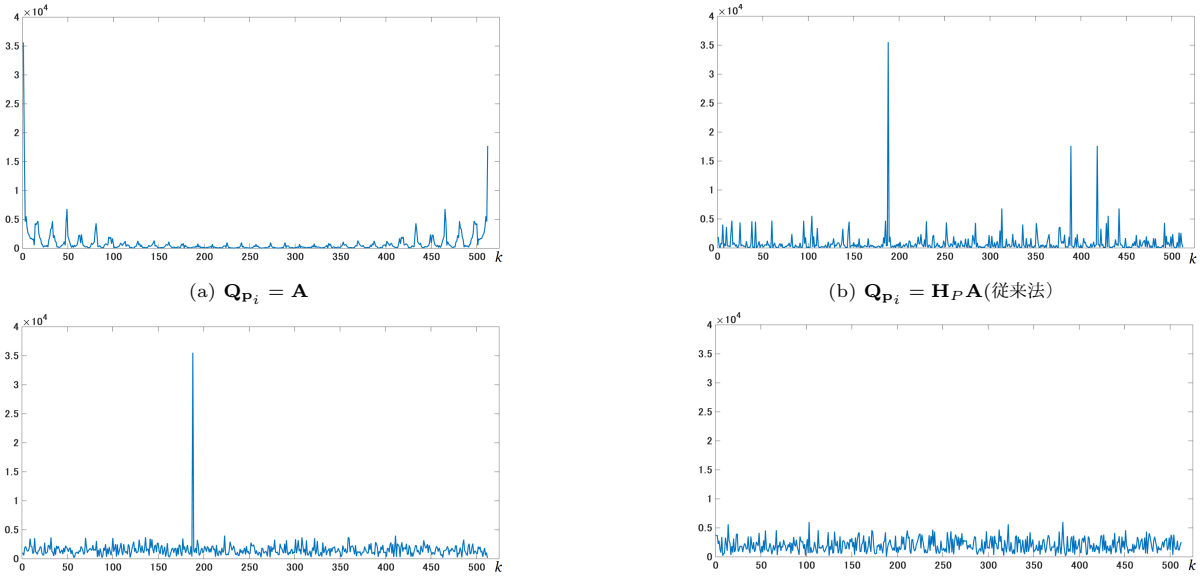
3.1 ランダム・ユニタリ行列の生成法

提案法では，ランダム・ユニタリ行列 $\mathbf{Q}_{\mathbf{p}_i}$ の生成に 3 つのユニタリ行列を組み合わせて使用する．いま，固定値を要素とするユニタリ行列 $\mathbf{A}$ とランダム性をもつ 2 つのユニタリ行列 $\mathbf{H}_{\mathbf{p}_i}$ を用いてランダム・ユニタリ行列 $\mathbf{Q}_{\mathbf{p}_i}$ を設計する．このとき，N 次元のテンプレート $\mathbf{f}_i$ から保護テンプレート $\hat{\mathbf{f}}_i$ は，

$$\hat{\mathbf{f}}_i = \mathbf{Q}_{\mathbf{p}_i}\mathbf{f}_i = (\mathbf{H}_{\mathbf{p}_i}\mathbf{A}\mathbf{H}_{\mathbf{p}_i})\mathbf{f}_i \tag{4}$$

のように生成される．本稿では $\mathbf{H}_{\mathbf{p}_i}$ として，ランダムパーミュテーション行列 $\mathbf{H}_P$ と，ランダムな正負符号を持つパーミュテーション行列（サインランダムパーミュテーション行列）$\mathbf{H}_{SP}$ を用いる．$\mathbf{H}_P$ は，テンプレートベクトルの要素をランダムに入れ替える行列，$\mathbf{H}_{SP}$ は，テンプレートベクトルの要素をランダムに入れ替え，かつ符号をランダムに反転させる行列である．ここで，$\mathbf{H}_P$，$\mathbf{H}_{SP}$ の例として，4×4 行列を以下に示す．

$$\mathbf{H}_P = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} \tag{5}$$



(a) $\mathbf{Q}_{\mathbf{p}_i} = \mathbf{A}$　(b) $\mathbf{Q}_{\mathbf{p}_i} = \mathbf{H}_P\mathbf{A}$(従来法)

(c) $\mathbf{Q}_{\mathbf{p}_i} = \mathbf{H}_P\mathbf{A}\mathbf{H}_P$（参考）　(d) $\mathbf{Q}_{\mathbf{p}_i} = \mathbf{H}_P\mathbf{A}\mathbf{H}_{SP}$（提案法）

図 4: 保護テンプレート $\hat{f}_{i,j}(k)$ の絶対値

$$\begin{aligned}\mathbf{H}_{SP} &= \mathbf{H}_S\mathbf{H}_P \\ &= \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} \\ &= \begin{bmatrix} 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \end{bmatrix} \end{aligned} \tag{6}$$

$\mathbf{H}_{SP}$ は，符号をランダムに反転させる行列であるランダムサイン行列（$\mathbf{H}_S$）と，$\mathbf{H}_P$ を組み合わせることで生成できる．

本稿では，特に，$\mathbf{Q}_{\mathbf{p}_i} = \mathbf{H}_P\mathbf{A}\mathbf{H}_{SP}$ を提案法とする．

3.2 提案法のランダム性

提案法の有効性を示すため，保護テンプレートのランダム性について例示する．図 4 に，保護テンプレートの絶対値を示す．ここで，$\mathbf{A}$ は DFT とする．

まず，図 4(a) は，ある顔画像から抽出した特徴量を DFT した値の絶対値であり，これは，保護を行う前の状態である．図 4(b) は従来法の一例である．これは，周波数領域で要素を入れ替えているだけであるため，横軸 k に対してはランダム性があるが，各値にはランダム性がなく，(a) と同じ値となる．図 4(c) では，ランダム性は増すが，パーミュテーションを DFT の前に行うだけでは，直流成分の値はそのまま残ってしまう．そこで，図 4(d) の提案法では，さらに，符号の反転も加えることにより，直流成分値も含めてランダム性を高めている．

以上のことから，提案法が最もランダム性が高くなっていることが期待される．

次節で，提案法の有効性を実験的にも確認する．

4. 実　　験

本節では，実験に用いた特徴抽出法について説明し，3 節で述べた提案法について性能を実験的に検証する．

表 1: 使用した $\mathbf{A}$ および $\mathbf{H}_{\mathbf{p}_i}$.

$\mathbf{A}$		$\mathbf{H}_{\mathbf{p}_i}$	
$\mathbf{A}_I$	単位行列	$\mathbf{H}_S$	ランダムサイン
$\mathbf{A}_D$	DFT	$\mathbf{H}_P$	ランダムパーミュテーション
$\mathbf{A}_C$	DCT	$\mathbf{H}_{SP}$	サインランダムパーミュテーション

表 2: ランダム・ユニタリ行列の種類.

生成法	ランダム・ユニタリ行列 $\mathbf{Q}_{\mathbf{p}_i}$
C_0（従来法）	$\mathbf{H}_S\mathbf{A}$
C_1（従来法）	$\mathbf{H}_P\mathbf{A}$
C_2（参考）	$\mathbf{H}_P\mathbf{A}\mathbf{H}_P$
C_3(提案法)	$\mathbf{H}_P\mathbf{A}\mathbf{H}_{SP}$

4.1 設 定 条 件

本実験では，代表的な顔画像のデータベースである The Extended Yale Face Database B [15] 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，画像サイズはすべて 192×168 で統一されている．1 人につき 4 枚をデータベース画像，残りの 60 枚をクエリにわけて実験を行った．また，特徴抽出には Local Binary Pattern を用い，認証法にはユークリッド距離に基づく最近傍法を使用した実験を行った．今回の実験では，特徴抽出において，認証に使う顔画像を 12×12 画素のブロックにわけ，そのブロックごとに LBP 処理を行い，各ヒストグラムを連結させてテンプレートとした．テンプレートは 2124 次元である．認証結果を出すために扱う，クエリと各登録者間のユークリッド距離を $r_{i,j}$ とする．

ここで，実験に用いたユニタリ行列 $\mathbf{A}$ および $\mathbf{H}_{\mathbf{p}_i}$ の種類を表 1 に示す．また，生成したランダム・ユニタリ行列の種類を表 2 に示す．このとき，$\mathbf{A}$ は表 1 で示した 4 種類すべてで実験を行った．これらのランダム・ユニタリ行列の生成において，

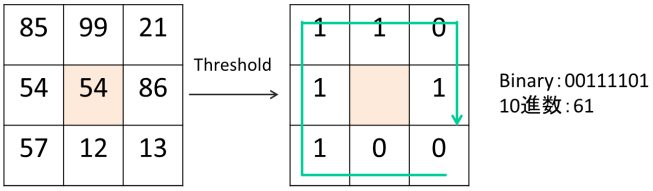


図 5: LBP の抽出方法

(a) 原画像　(b) LBP 画像

図 6: LBP 画像例

DFT の計算には，DFT の高速アルゴリズムである FFT を用いた．

4.2 Local Binary Pattern

ここでは，本実験に用いた代表的な特徴抽出法である Local Binary Pattern [16](LBP) について説明する．特徴抽出には，画像の全体的な特徴を抽出する holistic アプローチ [17] と，画像の局所的な特徴を抽出する local アプローチ [16] が存在する．local アプローチは，holistic アプローチよりも画像の照明変化に強く，かつ画像の細かい情報をより効果的に表現できる．LBP は local アプローチの一つであり，ある画素と，その近傍画素の画素値に基づいた特徴抽出法となっている．ここで，図 5 に基本的な LBP の抽出方法を示す．まず中心画素値とその周囲 8 画素でしきい値処理を行うことで，全ての画素にラベルを割り当て，割り当てた結果を二進数とみなす．その後，ラベルのヒストグラムを特徴量とする．

また，本実験では，UniformLBP [18] を用いて実験を行った．UniformLBP とは，“0 から 1 ”または“1 から 0 ”への遷移が 2 箇所以下の LBP に係る特徴量を用いる手法となっている．例えば，LBP の値が 01110000 は遷移 2，11001001 は遷移 4 とする．遷移が 2 箇所以下の各値はヒストグラムのビンにそれぞれ割り当てる．一方で，遷移が 3 以上の値は全て 1 つのビンにまとめる．

図 6 に，顔画像とその LBP 画像を示す．

4.3 クロスマッチングの評価

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．

保護テンプレートのクロスマッチングの関係を図 7 に例示する．同図は，$\mathbf{Q} = \mathbf{H}_P\mathbf{A}_I$ の場合についての結果である．ヒストグラム 1(hist1) は，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ランダム・ユニタリ行列による変換を施し，かつ両テンプレートの人物 i が同じときの，クエリと人物 i の j 枚目のトレーニングテンプレート間のユークリッド距離 $r_{i,j}$ の度数である．また，ヒストグラム 2(hist2) は，両テンプレートに対して異なるランダム・ユニタリ行列を用いて保護したときの，クエリと全ての登録者間のユークリッド距離の度数である．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．

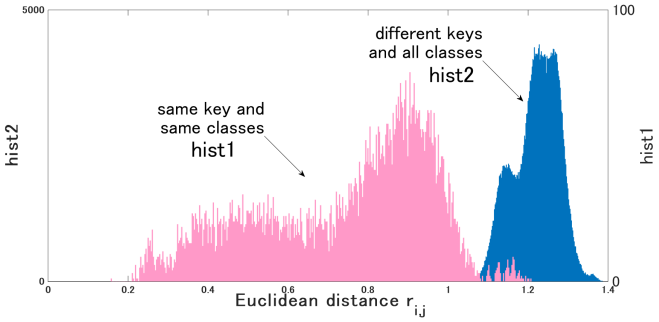


図 7: ユークリッド距離 $r_{i,j}$ のヒストグラム

表 3: ヒストグラム間のオーバーラップした $r_{i,j}$ の度数とそのパーセンテージ

	C_0(従来法)	C_1(従来法)	C_2(参考)	C_3(提案法)
$\mathbf{A}_I$	16(0.17%)	1058 (11.6%)	1184(12.9%)	0
$\mathbf{A}_D$	4285 (47.0%)	0	0	0
$\mathbf{A}_C$	1797 (20.0%)	0	0	0
グラムシュミット	0			

ここで，表 3 に，両ヒストグラム間においてオーバーラップしたユークリッド距離 $r_{i,j}$ の度数とそのパーセンテージをまとめたものを示す．

これらの実験結果より，クロスマッチング性能について，提案法は従来法を上回り，グラムシュミットと同等の高い性能を有することがわかる．また，$\mathbf{A}_I$ を使用した場合にも効果的であることがわかった．

4.4 エントロピーの評価

ここでは，保護テンプレートのランダム性について，エントロピーを用いて評価を行う．エントロピーは，ランダム性の評価尺度として広く使われている．エントロピーの式を以下に示す．

$$H = -\sum P_i \log 2P_i \qquad (7)$$

$$P_i = N_i/N$$

このとき，保護テンプレートの次元数を N，保護テンプレートの要素の値がレベル i である数を N_i とする．本実験では，保護テンプレートの値が $i = 0 \sim 255$ になるように量子化し，実験を行った．ここで，表 4 に，エントロピーの実験結果を示す．この結果は，152 枚の保護テンプレートからエントロピーをそれぞれ計算し，平均を取った値である．

実験結果より，提案法はグラムシュミットと同程度のランダム性をもつことが示されている．ただし，$\mathbf{A}_I$ を使用した場合にはどの方法でもエントロピーは低下する．

4.5 計算量の評価

提案法とグラムシュミットの直交化法を用いた保護法とを $\mathbf{Q}_{\mathbf{P}_i}$ を生成する計算量の観点で比較する．

表 4: 保護テンプレートのエントロピー（152 枚平均）

	C_0(従来法)	C_1(従来法)	C_2(参考)	C_3(提案法)
$\mathbf{A}_I$	2.791	2.791	2.791	2.791
$\mathbf{A}_D$	2.861	2.861	3.110	3.363
$\mathbf{A}_C$	2.942	2.942	3.147	3.515
グラムシュミット	3.515			

グラムシュミットの直交化法を用いた保護法は，疑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，$N \times N$ の疑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．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．

一方で，$\mathbf{A}$ に FFT を用いた場合を例にとると，提案法の保護の手順は，行列 $\mathbf{H}_{SP}$ と特徴ベクトルの積，そしてその特徴ベクトルを FFT し，最後にベクトル行列 $\mathbf{H}_P$ と FFT された特徴ベクトルの積とで構成される．$\mathbf{H}_{SP}$ と特徴ベクトルの積および $\mathbf{H}_P$ と特徴ベクトルの計算量は $\mathcal{O}(N)$ であり，N 点 FFT の計算量は $\mathcal{O}(N \log N)$ である．よって，提案法による保護の計算量は $\mathcal{O}(N \log N)$ である．同様に，DCT やアダマール変換にも高速アルゴリズムが存在するため，低い計算量で保護が可能である．よって，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．

キャンセラブルバイオメトリクスでは，保護テンプレートを一度生成してそれを使い続けるのではなく，定期的な保護テンプレートの更新が求められる．更新の際には，新たな $\mathbf{Q}_{\mathbf{P}_i}$ を生成する必要があるため，$\mathbf{Q}_{\mathbf{P}_i}$ の生成にかかる計算量は重要な課題となっている．

5. おわりに

本稿では，先行研究の課題であったクロスマッチング性能および保護テンプレートのランダム性を改善する新たなランダム・ユニタリ行列の生成法を提案し，性能を検証した．まず，要素が固定値であるユニタリ行列と，要素値がランダム性を持つユニタリ行列を 1 つずつ組み合わせて保護を行う先行研究について説明し，クロスマッチング性能および保護テンプレートのランダム性の課題を述べた．これらの課題を解決するような，固定値を要素とするユニタリ行列 1 つと，ランダム性を持つユニタリ行列を 2 つ，計 3 つのユニタリ行列を用いてランダム・ユニタリ行列を生成する方法を提案法とした．また，ランダムな行列として，サインランダムパーミュテーション行列の使用を提案した．最後に，顔認証実験を行い，クロスマッチング性能および保護テンプレートのランダム性への提案法の有効性を示した．

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] 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.

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

[10] I. Nakamura, Y. Tonomura, and H. Kiya, “Unitary Transform-Based Template Protection and Its Application to l_2-norm Minimization Problems,” IEICE Trans. Inf. & Sys., vol.E99-D, no.1, pp.60-68, Jan,2016.

[11] 中村 維吹, 外村 喜秀, 貴家 仁志, “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,” 電子情報通信学会 情報理論研究会, vol.115, no.37, pp.35-40, May,2015.

[12] 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, pp.17-22, Feb,2016.

[13] 斉藤 裕子, 中村 維吹, 塩田 さやか, 外村 喜秀, 貴家 仁志, “セキュアな生体認証のためのランダム・ユニタリ行列の検討,” 電子情報通信学会 画像工学研究会, vol.115, no.171, (no.IE2015-47), pp.7-12, Aug,2015.

[14] L. MengHui, A. Beng, J. Teoh and J. Kim, “Biometric Feature-Type Transformation: Making templates compatible for secret protection,” Signal Processing Magazine, IEEE, vol32, no.5, pp.77-87, 2015

[15] 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.

[16] T. Ahonen, A. Hadid, and M.Pietikainen, “Face Description with Local Binary Patterns: Application to Face Recognition,” IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 28, no. 12, pp. 2037-2041, 2006.

[17] M. Turk and A. Pentland, “Eigenfaces for recognition”,J. Cognitive Neuroscience, vol. 3, no.1, pp. 71-86, Jan. 1991.

[18] T. Ojala, M. Pietikainen, and T. Maenpaa, “Multiresolution Gray-Scale and Rotation Invariant Texture Classification with Local Binary Patterns,” IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 24, no. 7, pp. 971-987,July 2002.