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.

# 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

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
††† 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**　テンプレート保護法の一つとして，ランダム・ユニタリ変換に基づく保護法が提案されている．この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共通のユニタリ行列で保護した場合，テンプレート間の内積が保存され，認証精度を低下することなく $l^2$ ノルムや $l^1$ ノルムに基づく生体認証法を実行できる．本稿では，これらの特徴を有するランダム・ユニタリ行列の様々な生成法を考察し，それらの性能を検証する．顔認証実験を行い，クロスマッチング特性，処理時間，安全性の観点から種々のランダム・ユニタリ行列を比較して，有効なランダム・ユニタリ行列の生成法を考察する．

**キーワード**　生体認証　保護テンプレート　ユニタリ行列

# A study of random unitary matrices for secure biometric authentication

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**　Random unitary transformation-based template protection methods have been proposed as one of biometric template protection schemes. When a common unitary matrix among all templates is used, it is known that the template protection methods can provide the same recognition performance as for the use of non-protected ones, in $l^2$-norm and $l^1$-norm minimization problems. This article considers how to generate random unitary matrices that have the above characteristic, and verifies the difference among the matrices . By doing some face recognition experiments, various randam unitary matrixes are compared in terms of cross-matching performance, processing time and security, and then effective generation methods of random unitary matrices are considered.

**Key words**　Biometrics, Template protection, unitary matrices

## 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] - [3]

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 [4] - [7]，ランダム射影を用いた方法 [8] などに代表される，ランダム行列によってテンプレートを変換する手法がある．

本稿では，ユニタリ変換に基づく保護法に使用される，ランダム・ユニタリ行列の様々な生成法を考察し，それらの性能を検証する．本稿で用いるランダム・ユニタリ行列は，ランダム性を持たないユニタリ行列とランダム性を持つユニタリ行列を組み合わせたものである．これにより，ユニタリ変換の性質を保ったまま，DFT や DCT などの代表的なユニタリ変換をランダム行列の生成に利用することが可能となる．最後に顔認証実験を行い，クロスマッチング特性，処理時間，安全性の観点から種々のランダム・ユニタリ行列の生成法を，グラムシュミットの正規直交化法も含め比較して，有効な生成法を考察する．

## 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およびユニタリ変換の性質 [4] 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 $i$ 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．

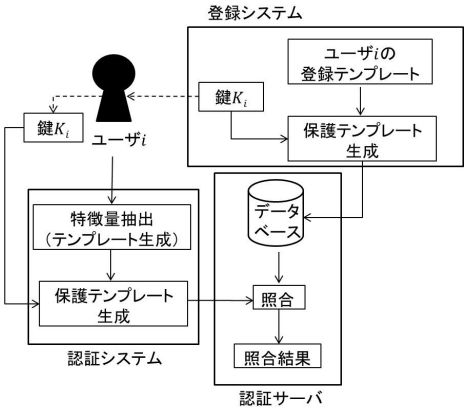



図 1: 認証システム

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 [9].

（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．

### 2.3 ユニタリ変換の性質

まず，生体情報のテンプレートに相当する特徴ベクトルを，$\mathbf{f}_i = [f_i(0), f_i(1), ..., f_i(N-1)]^T$，ユニタリ行列を，$\mathbf{Q} = \{Q(i,j), 0 \leqq i,j \leqq N-1\}$，ユニタリ変換を施す関数を $T$，パラメータを $a$ をとすると，$\mathbf{f}_i$ をユニタリ変換した保護ベクトル $\hat{\mathbf{f}}_i$ は

$$\hat{\mathbf{f}}_i = T(\mathbf{f}_i, a) = \mathbf{Q}\mathbf{f}_i \tag{1}$$

と与えられる．保護テンプレート生成においては，$\mathbf{Q}$ はユニタリ性に加え，ランダム性を有する必要がある．直接この性質を持つ $\mathbf{Q}$ を生成する方法に，グラム・シュミットの直行化法によって，ある鍵から初期生成した行列を直行化させる方法がある．

ここで，$N$ 次元の 2 つのテンプレート $\mathbf{f}_i$，$\mathbf{f}_j$ を，共通のユニタリ行列 $\mathbf{Q}$ で変換した場合のユニタリ変換の性質を以下に示す．

（1） 内積の保存：変換前のテンプレート間および変換後の保護テンプレート間の内積が等しい

（2） ユークリッド距離の保存：変換前のテンプレート間および変換後の保護テンプレート間のユークリッド距離が等しい

（3） 相関の保存：変換前のテンプレート間および変換後の保護テンプレート間の相関が等しい

（4） $l^2$ ノルムに基づく認証結果の保存：$l^2$ ノルムに基づく認証方法 [7] [10] において，変換前のテンプレートを直接用いた場合の結果と，保護テンプレートによる認証結果が等しい

（5） 固有顔を用いた認証可能 [6]：変換前に生成した固有顔を用いた認証における重みと，保護テンプレートから生成した固有顔の重みが等しい

ユニタリ変換の性質の (1)，(2) の証明を以下に示す．$\mathbf{Q}$ がエルミート転置 $\mathbf{Q}^*$ を用いて $\mathbf{Q}^*\mathbf{Q} = \mathbf{I}$ を満たす性質より，$\hat{\mathbf{f}}_i$，$\hat{\mathbf{f}}_j$ 間の内積は，

$$\begin{aligned}\hat{\mathbf{f}}_i \cdot \hat{\mathbf{f}}_j = \hat{\mathbf{f}}_i^* \hat{\mathbf{f}}_j &= (\mathbf{Q}\mathbf{f}_i)^*(\mathbf{Q}\mathbf{f}_j) \\ &= \mathbf{f}_i^* \mathbf{Q}^* \mathbf{Q} \mathbf{f}_j \\ &= \mathbf{f}_i^* \mathbf{f}_j = \mathbf{f}_i \cdot \mathbf{f}_j \end{aligned} \tag{2}$$

と求められる．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，(2) より

$$|\hat{\mathbf{f}}_i - \hat{\mathbf{f}}_j|^2 = |\mathbf{f}_i - \mathbf{f}_j|^2 \tag{3}$$

となる．式 (2) および式 (3) 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，ユニタリ変換は，共通のユニタリ行列を用いることで $\mathbf{f}_i$，$\mathbf{f}_j$ 間の内積およびユークリッド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という性質を持つ．また，内積が保存されるという性質から，保護前のテンプレート間と，保護テンプレート間の相関が等しくなり，さらに保護テンプレートによる認証が，$l^2$ ノルムにおいて保護前のテンプレートを直接用いた場合と同じ結果になる [7]．保護テンプレートから生成した固有顔を用いた認証においても，その固有顔の重みが，保護される前に生成した固有顔の重みと等しくなるため，保護テンプレートでの固有顔を用いた $l^1$ ノルムに基づく認証が可能となる [6]．

これらの性質は，ユニタリ変換であれば有するものである．そこで本稿では，これらの性質を共通に有する代表的なランダム・ユニタリ行列について比較する．

## 3. ランダム・ユニタリ行列の評価

### 3.1 ランダム・ユニタリ行列

$N \times N$ 行列のランダム・ユニタリ行列を $\mathbf{Q} = \{Q(i,j), 0 \leqq i,j \leqq N-1\}$ とする．さらに，$\mathbf{Q}$ の要素 $Q(i,j)$ はパラメータである鍵 $a$ 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 $a$ によって保護され，かつ $\mathbf{Q}$ 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．

### 3.2 保護テンプレートの生成法

ユニタリ行列の性質から，ユニタリ変換を施したテンプレートにさらにユニタリ変換を施しても，テンプレートはユニタリ変換の性質を保つことができる．

いま，$N$ 次元のテンプレート $\mathbf{f}_i = [f_i(0), f_i(1), ..., f_i(N-1)]^T$ を，2 つのユニタリ行列 $\mathbf{A} = \{A(i,j), 0 \leqq i,j \leqq N-1\}$，$\mathbf{H} = \{H(i,j), 0 \leqq i,j \leqq N-1\}$ を用いてユニタリ変換する．ただし，$\mathbf{H}$ 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，

$$\hat{\mathbf{f}}_i = \mathbf{Q}\mathbf{f}_i = \mathbf{H}\mathbf{A}\mathbf{f}_i \tag{4}$$

もしくは

$$\hat{\mathbf{f}}_i = \mathbf{Q}\mathbf{f}_i = \mathbf{A}^{-1}\mathbf{H}\mathbf{A}\mathbf{f}_i \tag{5}$$

のように生成することができる．このとき，$\mathbf{Q}$ はランダム・ユニタリ行列となる．すなわち，ランダム性を持たない DFT や DCT などをランダム行列の生成に利用することが可能である．

### 3.3 ランダム・ユニタリ行列の種類

本稿で保護テンプレートの生成に用いるランダム・ユニタリ行列を以下に示す．$\mathbf{A}$ で施すユニタリ変換は

$\mathbf{A}_0$　単位行列
$\mathbf{A}_1$　DFT
$\mathbf{A}_2$　DCT
$\mathbf{A}_3$　アダマール変換

を用い，ランダム性をもつユニタリ行列 $\mathbf{H}$ には

$\mathbf{H}_1$　ランダムにベクトル要素を入れ替える行列
$\mathbf{H}_2$　ランダムにベクトル要素の符号を反転する行列
$\mathbf{H}_3$　ランダムにベクトル要素の位相を変換する行列

を用いる．本稿では以降，これらの変換行列を以上の記号で表すものとする．ここで，上記の $\mathbf{H}_1$，$\mathbf{H}_3$ の例として，$4 \times 4$ 行列を以下に示す．

$$\mathbf{H}_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \tag{6}$$

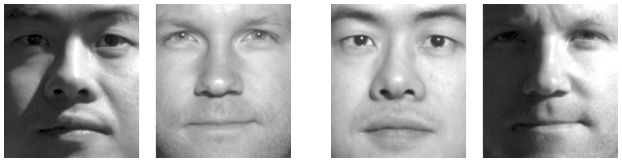
$$\mathbf{H}_3 = \begin{bmatrix} \mathrm{e}^{j\theta_1} & 0 & 0 & 0 \\ 0 & \mathrm{e}^{j\theta_2} & 0 & 0 \\ 0 & 0 & \mathrm{e}^{j\theta_3} & 0 \\ 0 & 0 & 0 & \mathrm{e}^{j\theta_4} \end{bmatrix} \tag{7}$$

$\mathbf{H_2}$ は，式 (7) の $\mathrm{e}^{j\theta_i}$ を 1 または $-1$ で置換したものとなる．

先行研究 [4] [7] では，DFT とランダムに位相を変換する行列の組み合わせのみ使用されていたが，本稿では，これらのユニタリ変換およびランダム性をもつユニタリ行列を様々に組み合わせ生成される保護テンプレートを評価する．上述以外の生成法に，グラム・シュミットの直行化法によって，ある鍵から初期生成した行列を直行化させる方法がある [11]．

## 4. 実　　験

本節では，顔画像を用いて，3 節で述べたランダム・ユニタ



(a) クエリ画像　　(b) データベース画像

図 2: データベースの画像例

リ行列について，それらの性能を実験的に検証する．

### 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 Yale Face Database B [12] 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 2 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先に述べたランダム・ユニタリ行列を用い，特徴抽出にはダウンサンプリング法 [10] 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 64×32= 2048 にダウンサンプリングし，それを 2048 次元のテンプレートとした．さらに，認証法には $l^2$ ノルムに基づく認証方法 [10] を使用した．このとき，識別結果として使用されるクエリとトレーニングデータ間の誤差を推定二乗誤差 $r_i$ と呼ぶ．実験において，ランダム・ユニタリ行列の組み合わせ条件は，$\mathbf{Q} = \mathbf{A}^{-1}\mathbf{HA}$ および $\mathbf{Q} = \mathbf{HA}$ の各々の場合において，

条件 $C_1$　: $\mathbf{A} = \mathbf{A}_0, \mathbf{A}_1, \mathbf{A}_2$ or $\mathbf{A}_3$, $\mathbf{H} = \mathbf{H}_1$
条件 $C_2$　: $\mathbf{A} = \mathbf{A}_1, \mathbf{A}_2$ or $\mathbf{A}_3$, $\mathbf{H} = \mathbf{H}_2$
条件 $C_3$　: $\mathbf{A} = \mathbf{A}_1, \mathbf{A}_2$ or $\mathbf{A}_3$, $\mathbf{H} = \mathbf{H}_2\mathbf{H}_1$
条件 $C_4$　: $\mathbf{A} = \mathbf{A}_1$, $\mathbf{H} = \hat{\mathbf{H}}_3$(複素共役を維持)
条件 $C_5$　: $\mathbf{A} = \mathbf{A}_1$, $\mathbf{H} = \mathbf{H}_3$
条件 $C_6$　: $\mathbf{A} = \mathbf{A}_1$, $\mathbf{H} = \mathbf{H}_1\mathbf{H}_3$
条件 $C_7$　: $\mathbf{A} = \mathbf{A}_1$, $\mathbf{H} = \mathbf{H}_2\mathbf{H}_3$

とした．条件 $C_4$ は，$\mathbf{f}_i$ が実ベクトルの時，$\mathbf{Q} = \mathbf{A}^{-1}\mathbf{HA}$ による変換値が実数になるような条件（$\mathbf{HAf}_i$ が複素共役性を維持する）を $\mathbf{H}_3$ に課している．これらのランダム・ユニタリ行列の生成において，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 認証精度の確認

まず，クエリテンプレートとトレーニングテンプレートを，同じ鍵で生成されたランダム・ユニタリ行列で保護した場合の認証精度について確認する．図 3 に，保護前のテンプレートを直接用いて認証したときと，ランダム・ユニタリ変換により生成された保護テンプレートを用いて認証したときの ROC（Receiver Operating Characteristic）特性を示す．両者の ROC は，図に示すように同じ結果となる．すなわち，ユニタリ性を持つどの変換を用いても，保護テンプレートを使用することによる，特性劣化は生じない．

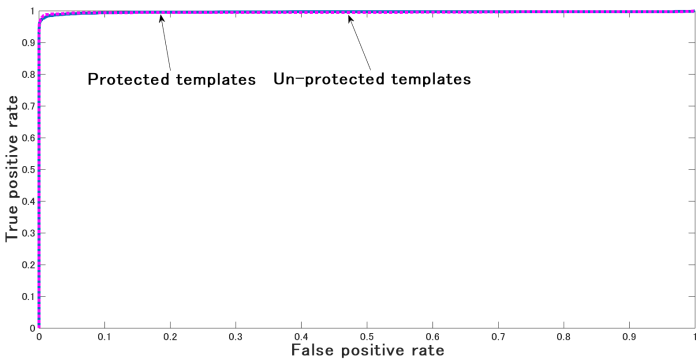



図 3: ROC 特性

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

| | $C_1$ | $C_2$ | $C_3$ |
|---|---|---|---|
| $\mathbf{A}_0$ | 1052 (51.0%) | | |
| $\mathbf{A}_1$ | 3 (0.25%) | 168 (13.8%) | 3 (0.25%) |
| $\mathbf{A}_2$ | 5 (0.41%) | 206 (16.9%) | 5 (0.41%) |
| $\mathbf{A}_3$ | 5 (0.41%) | 195 (16.0%) | 4 (0.33%) |

| | $C_4$ | $C_5$ | $C_6$ | $C_7$ |
|---|---|---|---|---|
| $\mathbf{A_1}$ | 204 (16.8%) | 189 (15.5%) | 3 (0.25%) | 189 (15.5%) |

| | |
|---|---|
| グラムシュミット | 4 (0.33%) |

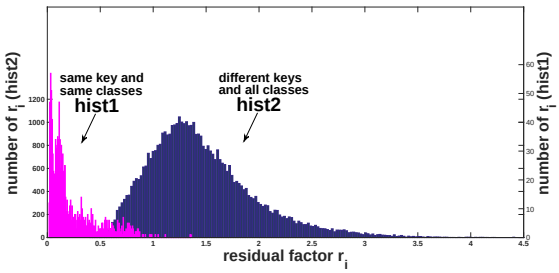
### 4.3 クロスマッチングの評価

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．

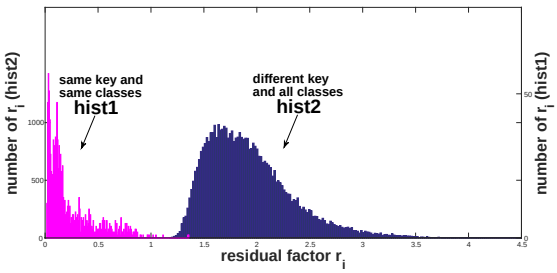
保護テンプレートのクロスマッチングの関係を図 4 に示す．同図は，$\mathbf{Q} = \mathbf{HA}$ の場合についての，条件 $C_1$，条件 $C_4$ およびグラムシュミットによる各結果である．ヒストグラム 1(hist1) は，トレーニングテンプレートとクエリテンプレートに共通のランダム・ユニタリ行列による変換を施し，かつ両テンプレートの人物が同じときの推定二乗誤差 $r_i$ の度数である．また，ヒストグラム 2(hist2) は，両テンプレートに対して異なるランダム・ユニタリ行列を用いて保護したときの，クエリと全ての登録者間の推定二乗誤差の度数である．この時，この 2 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．

表 1 は，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にまとめたものである．なお，$\mathbf{Q} = \mathbf{A}^{-1}\mathbf{HA}$ の結果は $\mathbf{Q} = \mathbf{HA}$ の結果とほぼ等しくなった．

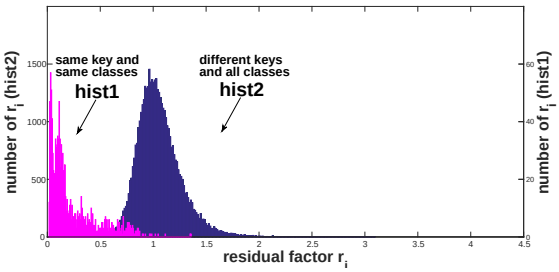
これらの実験結果より，クロスマッチング性能については，効果的なランダム・ユニタリ行列の生成法は，ランダムにベクトル要素を入れ替える行列 $\mathbf{H}_1$ の使用時であることがわかる．ただし，$\mathbf{A}_0$ を用いたとき，つまりテンプレートを $\mathbf{H}_1$ のみで変換したときは，クロスマッチング特性の改善に効果がない．また，多少ではあるが，ユニタリ変換には DFT を用いた場合が最も効果的であった．



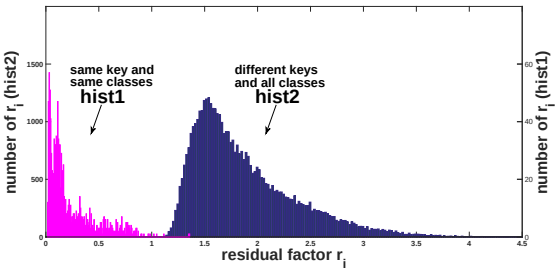

(a) 条件 $C_1$ : $\mathbf{A} = \mathbf{A}_0$ (51.0%)




(b) 条件 $C_1$ : $\mathbf{A} = \mathbf{A}_1$ (0.25%)




(c) 条件 $C_4$ (15.5%)




(d) グラムシュミット (0.33%)

図 4: 推定二乗誤差 $r_i$ のヒストグラム
( ) 内はオーバーラップした $r_i$ のパーセンテージを示す

表 2: 実験環境

| | |
|---|---|
| CPU | Intel(R)Core(TM) i7-4810MQ CPU 2.80GHz |
| メモリ | 16.0GB |
| OS | Windows7 |
| 使用ソフト | MATLAB |

表 3: 処理時間 [s]

| | FFT $C_1$ | DCT $C_1$ | アダマール $C_1$ | FFT $C_2$ | グラムシュミット |
|---|---|---|---|---|---|
| 生成時間 | 0.12 | 0.57 | 24.0 | 0.08 | 7.12 |

### 4.4 処理時間の評価

ここでは，4.1 で示したランダム・ユニタリ行列の生成時間について評価する．

今回は，DFT 変換，DCT 変換，アダマール変換それぞれを使用した条件 $C_1$ および条件 $C_4$ の処理時間と，グラムシュミットの直行化法を使用して作成したユニタリ行列を用いた場合の処理時間を比較する．このとき，DFT の計算には高速アルゴリズム FFT を用いた．また，グラムシュミットの直行化法を用いて作成した行列は，$2048 \times 2048$ である．また，実験を行った PC の環境を表 2 に示す．

処理時間として，テンプレートから保護テンプレートを作り出すまでにかかった時間である生成時間を測定した．テンプレート 1216 個に対する保護テンプレートの生成時間を表 3 に示す．生成時間においては，高速アルゴリズムである FFT が最も短くなった．特に，アダマール変換，グラムシュミットを用いた場合と比較すると生成の速さは明確である．さらに，グラムシュミットにおいては行列の次元数が増加すると，生成時間も増加する（原理的には次元数 $N \times N$ の行列において $O(N^3)$ で増加）．これら処理時間の違いは，テンプレートの更新時などにおいて重要となる．

続いて，保護テンプレートを用いて，認証結果が出力されるまでの時間である認証時間を計測した．認証時間においては，条件 $C_1$ 時の FFT は複素数での認証計算になるため，他の変換と比較すると 3 倍ほど遅くなった．FFT 以外の変換は，認証時間に差はみられなかった．しかし，実数で認証計算を行えるように変換した $C_4$ の場合の認証時間は他の変換を使用した場合と同程度の速度になった．従って FFT でも保護テンプレートの要素が実数になるようにすれば，認証時間は改善される．

### 4.5 安全性の評価

提案法の非可逆性について評価を行う．まず，文献 [13] における，パーフェクトセキュリティの要件を満たすか検証する．以下の 2 つの定義を満たすものがパーフェクトセキュリティと定義される．

定義 1： 暗号システムは以下の性質を満たす組 $(\mathbf{M}, \mathbf{C}, \mathbf{K}, \mathbf{E}, \mathbf{D})$ である．

1. $\mathbf{M}$ は平文の集合である
2. $\mathbf{C}$ は暗号文の集合である
3. $\mathbf{K}$ は鍵空間の集合である
4. $\mathbf{E} = \{E_k; k \in \mathbf{K}\}$ は関数である $\quad (E_k; \mathbf{M} \to \mathbf{C})$
5. $\mathbf{D} = \{D_k; k \in \mathbf{K}\}$ は関数である $\quad (D_k; \mathbf{C} \to \mathbf{M})$
6. 全ての $m \in \mathbf{M}$ に対して $Dd(Ee(m)) = m$ となるような鍵 $d \in \mathbf{K}$ が各 $e \in \mathbf{K}$ に対して存在する．

定義 2： 特定の暗号文の生成と特定の平文の暗号化の事象が独立である場合，暗号システム $(\mathbf{M}, \mathbf{C}, \mathbf{K}, \mathbf{E}, \mathbf{D})$ は，パーフェクトセキュリティを持つ

また，パーフェクトセキュリティを持つには，以下の Shanon の定理を満たさなければならない．

定理： すべての平文に対して，$|\mathbf{M}| = |\mathbf{K}| = |\mathbf{C}| < \infty$,

$Pr(m) > 0$ とする

暗号システム（$\mathbf{M}, \mathbf{C}, \mathbf{K}, \mathbf{E}, \mathbf{D}$) は，鍵空間の確率分布が一様分布であり，すべての平文とすべての暗号文に対して，$E_k(m) = c$ となる鍵 $k$ が一つだけ存在する．

本研究では，実数を用いた演算を行い，$|\mathbf{M}|$ と $|\mathbf{K}|$ と $|\mathbf{C}|$ がそれぞれ異なり，以上の定理を満たさないため，パーフェクトセキュリティには分類されない．そのため，暗号文がどの程度の非可逆性を有しているかを評価するために，暗号文から総当たり攻撃で復元する場合を想定し，鍵空間を求めた．$\mathbf{H}_1$ の鍵空間は，ベクトルの要素の入れ替えなので，テンプレートベクトルの次元数 $N$ により決定し，$N!$ になる．次に，$\mathbf{H}_2$ の鍵空間は，$+$ と $-$ の 2 種類の符号とテンプレートベクトルの次元数 $N$ により決定し，$2^N$ となる．$\mathbf{H}_3$ の鍵空間は，位相ベクトル $\theta$ の要素数 $L$ とテンプレートベクトルの次元数 $N$ により決定し，$L^N$ となる．複素共役を維持した場合である $\hat{\mathbf{H}}_3$ の鍵空間は $L^{\lfloor \frac{N-1}{2} \rfloor}$ となる．

今回実験では，次元数 $N = 2048$，$L = 4$ であるため，各鍵空間の広さは，$\mathbf{H}_1 : 2048!$，$\mathbf{H}_2 : 2^{2048}$，$\mathbf{H}_3 : 4^{2048}$，$\hat{\mathbf{H}}_3 : 4^{1023}$ となる．これらの鍵空間はどれも 256 ビットの鍵を使用する暗号よりも広い鍵空間を持つ．鍵を掛け合わせた，$\mathbf{H} = \mathbf{H}_1\mathbf{H}_2$ などの場合は，それぞれの鍵空間の積となるため，更に広い鍵空間となる．$\hat{\mathbf{H}}_3$ は鍵空間は $\mathbf{H}_3$ に比べて小さくなるものの，保護テンプレートが実数で生成される利点をもつ．

$\mathbf{H}_2$，$\mathbf{H}_3$ および $\hat{\mathbf{H}}_3$ の鍵を用いた場合，$|H(k,k)| = 1$ であるため，変換領域での振幅スペクトルを入手可能である．それに対して，$\mathbf{H}_1$ の鍵を用いた場合は，振幅スペクトルも保護することが可能であるため，$\mathbf{H}_1$ を鍵として用いる必要があることに注意する必要がある．

### 4.6 その他の評価

テンプレート $\mathbf{f}_i$ が整数ベクトルである場合，一般的に保護テンプレートも整数値を維持することが望まれる．このとき，グラムシュミットの使用では保護テンプレートは実数ベクトルとなってしまう．一方，アダマール変換を用いた場合には整数値を保つことが可能となる．また，$\mathbf{Q} = \mathbf{A}^{-1}\mathbf{H}\mathbf{A}$ のような逆変換 $\mathbf{A}^{-1}$ を含む変換は，テンプレート $\mathbf{f}_i$ の数値的制約を維持することがある程度可能である．このように，様々のランダム・ユニタリ行列を定義可能であり，認証性能という観点からは同一であるが，いくつかの異なる特性を持つことがわかる．

## 5. おわりに

本稿では，ユニタリ変換の特徴を有するランダム・ユニタリ行列の様々な生成法を考察し，それらの性能を検証した．まず，ユニタリ変換の性質を述べ，その後ランダム・ユニタリ行列の種類の生成法を提示した．さらに，顔認証実験を行い，クロスマッチング特性，処理時間，安全性などの観点からランダム・ユニタリ行列を比較した．その結果どの生成法も認証性能は同じであるが，様々な異なる特性を持つことが確認された．グラムシュミットの直交化法に比べ，優れた特徴を持つユニタリ行列を容易に生成可能であることが示された．

## 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] Rane.S, Standardization of Biometric Template Protection. MultiMedia, IEEE, 2014, 21.4: 94-99.

[4] 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.

[5] 斉藤 裕子，中村 維吹，塩田 さやか，外村 喜秀，貴家 仁志,“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,”電子情報通信学会 マルチメディア情報ハイディング・エンリッチメント研究会，vol.114, no.511, no.EMM2014-81, pp.25-30, Mar.2015.

[6] 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, no.IT2015-7, pp.35-40, 2015.

[7] I.Nakamura, Y.Tonomura, and H.Kiya,“Unitary Transform-Based Template Protection and Its Properties,”Proc. EURASIP European Signal Processing Conference, 4th September, 2015.(accepted)

[8] 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.

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

[10] 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.

[11] Y.Wang，and K. N. Plataniotis，”Face based biometric authentication with changeable and privacy preservable templates.，” IEEE Biometrics Symposium, pp1-6.2007.

[12] 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.

[13] Shinji Hirata, Kenta Takahashi., ”Cancelable Biometrics with Perfect Secrecy for Correlation-Based Matching,” Advances in Biometrics, Lecture Notes in Computer Science, Vol.5558, pp.868-878, 2009.