

## 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

古川昌和<sup>†</sup> 村木雄一<sup>†</sup> 藤吉正明<sup>†</sup> 外村喜秀<sup>††</sup> 貴家仁志<sup>†</sup>

<sup>†</sup> 首都大学東京大学院システムデザイン研究科情報通信システム学域 〒191-0065 東京都日野市旭が丘 6-6

<sup>††</sup> 日本電信電話株式会社 未来ねっと研究所

E-mail: <sup>†</sup>{furukawa-masakazu,muraki-yuichi}@ed.tmu.ac.jp, mfujiyoshi@m.ieice.org, kiya@tmu.ac.jp

<sup>††</sup>tonomura.yoshihide@lab.ntt.co.jp

あらまし 顔識別を用いたシステムでは、顔画像から抽出された特徴量(テンプレート)を比較して識別を行う。本稿では、テンプレートの漏えいに対して耐性を有する保護テンプレートの新たな生成法を提案し、スパース表現に基づく顔識別法を例にそれを適用する。テンプレートの漏えいは利用者の個人情報の流出を意味し、プライバシー保護やセキュリティの観点からテンプレートは保護される必要がある。提案される保護テンプレート生成法は画素スクランブルとダウンサンプリングとから構成される。スクランブルとダウンサンプリングの変換パラメータが公知の場合においても、提案法による保護テンプレートから顔画像の視覚的情報を復元することは困難である。更に、従来のランダム射影による保護テンプレートに比べて、提案法による保護テンプレートは画素値の分布が集中するため、より効果的なデータ圧縮を可能とする。複数の顔画像データベースを用いた実験によって、識別性能、視覚的復元の困難性、データ圧縮の観点から提案法の有効性が確認された。

キーワード テンプレート保護, キャンセラブルバイオメトリクス, JPEG-LS, 生体認証, 画像圧縮,  $\ell^1$  ノルム

## A Generation Scheme of Protected Templates for Sparse Representation-based Face Recognition

Masakazu FURUKAWA<sup>†</sup>, Yuichi MURAKI<sup>†</sup>, Masaaki FUJIYOSHI<sup>†</sup>, Yoshihide TONOMURA<sup>††</sup>, and

Hitoshi KIYA<sup>†</sup>

<sup>†</sup> Dept. of Information and Communication Systems, Tokyo Metropolitan University

6-6 Asahigaoka, Hino-shi, Tokyo, 191-0065 JAPAN

<sup>††</sup> NTT Network Innovation Laboratories, Nippon Telegraph and Telephone Corp. 239-0847 JAPAN

E-mail: <sup>†</sup>{furukawa-masakazu,muraki-yuichi}@ed.tmu.ac.jp, mfujiyoshi@m.ieice.org, kiya@tmu.ac.jp

<sup>††</sup>tonomura.yoshihide@lab.ntt.co.jp

**Abstract** In face recognition systems, facial images are recognized by comparing features (template) extracted from them. This paper proposes a generation scheme of protected templates which are tolerant to template leakage and applies the scheme to the sparse representation-based face recognition. Template leakage leads to disclose users' personal information so that templates should be protected. The proposed scheme for template protection consists of random pixel permutation and down-sampling. It is difficult to reconstruct visual information of facial images from the templates protected with the proposed scheme even though parameters for random pixel permutation and down-sampling are disclosed to the public. Furthermore, the templates protected with the proposed scheme can be more effectively compressed in terms of the data size than those with the conventional scheme using random projection because the histogram of the templates protected with the proposed scheme is denser than that with the conventional scheme. Experimental results with two major database of facial images demonstrate the effectiveness of the proposed scheme in terms of recognition performance, difficulty of visual information reconstruction, and data compression.

**Key words** Template protection, cancelable biometrics, biometrics, JPEG-LS, image compression,  $\ell^1$ -norm

## 1. はじめに

顔識別はアミューズメントパークの入場システムから入国管理システムまで、幅広い分野で利用されている。これらのシステムでは、顔画像から抽出された特徴量(テンプレート)を比較して識別を行う。

顔識別技術はこれまで識別性能の向上を目的として、頑健な顔識別法と不変な特徴量との2つの観点から発展してきた。前者は、ノイズによるテンプレートの変動に影響されずに識別することを目的に発展してきた。その中でもスパース表現に基づく顔識別法 [1] が頑健さの観点から近年注目されており、多くの派生手法が提案されている。後者は、撮影条件に不変で、かつ、同一人物に対して同じ特徴量を与えることを目的に発展してきた。gabor 特徴量 [2] やローカルバイナリパターン [3] など顔の局所的な特徴に焦点を当てた特徴量が近年注目されているが、最も一般的な特徴量は顔全体の外見に基づくものであり、例えば eigenface [4], fisherface [5], laplacianface [6] などが知られている。このような特徴量は、局所特徴量に必要なパラメータの調整や注目領域の抽出を必要としないという利点がある一方、元画像の視覚的情報が含まれるため、テンプレートの漏えいは利用者の個人情報流出を意味する。また利用者情報の流出によってシステムの安全性が損なわれる可能性もある。以上のことから、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なければならない。

生体認証の分野において、テンプレート保護の枠組みの1つとしてキャンセルバイオメトリクス [7] が知られている。キャンセルバイオメトリクスでは、テンプレートのある変換によって意図的に歪ませることで保護する。クエリテンプレートとデータベース内の登録テンプレートとの両方に同一の変換が施され、テンプレート同士は変換領域で比較される。つまり、オリジナルテンプレートを復元することなく比較を行うため、利用者のプライバシーを保護できるという利点がある。変換方法は通常非可逆なものを用いるため、オリジナルテンプレートを復元することは困難である。もう1つの大きな利点は、漏えいによって保護テンプレートの信頼性が失われた場合、すべてのテンプレートを破棄し、パラメータの変更によって保護テンプレートを再発行できることである。これによって、漏えいした保護テンプレートを失効できるため、セキュリティの向上に繋がる。

これまでいくつかの研究でキャンセルバイオメトリクスの概念がスパース表現に基づく顔識別法 [1] に応用されてきた。代表的な保護テンプレート生成法として、ランダム射影と呼ばれる次元削減法がある [8]。ランダム射影はキャンセルバイオメトリクスのためにしばしば用いられてきた [9-11]。しかし、ランダム射影による保護テンプレートは信号の無相関化の影響に加え、一般に倍精度浮動小数点型で表現されるため、データサイズが大きくなってしまふ。一方で、スパース表現に基づく顔識別のためにノイズ画像を用いた保護テンプレート生成法が提案されている [12]。この手法による保護テンプレートは一般的な画像と同じ符号なし8ビット整数型で表現されるが、特

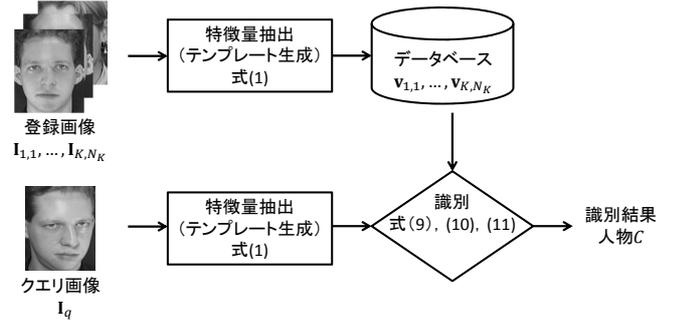


図 1: スパース表現に基づく顔識別法

定の処理とノイズ除去フィルタとを用いることで、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可能性がある。

本稿では、保護テンプレートの新たな生成法を提案し、スパース表現に基づく顔識別法を例にそれを適用する。提案する生成法は画素スクランブルとダウンサンプリングとから構成される。スクランブルとダウンサンプリングの変換パラメータが公知の場合においても、提案法による保護テンプレートから顔画像の視覚的情報を復元することは困難である。また従来のランダム射影による保護テンプレートに比べて、提案法による保護テンプレートは値の度数分布が集中し、また一般的な画像と同じ型で表現されるため、より効果的なデータ圧縮を可能とする。複数の顔画像データベースを用いた実験によって、識別性能、視覚的復元の困難性、データ圧縮の観点から提案法の有効性が確認する。

## 2. 準備

本節では、スパース表現に基づく顔識別法 [1] とテンプレート保護法における要件を記述する。

### 2.1 スパース表現に基づく顔識別法

図 1 はスパース表現に基づく顔識別法 [1] のブロック図を示す。 $i$  番目の人物における  $j$  枚目の登録画像  $\mathbf{I}_{i,j} \in \mathbb{R}^{H \times W}$  から特徴量抽出を行い、テンプレート  $\mathbf{v}_{i,j} \in \mathbb{R}^d$  を得る。ここで、 $i = 1, \dots, K$ ,  $j = 1, \dots, N_i$  とする。本稿では、 $\mathbf{I}_{i,j}$  をラスタスキャンすることによって得られたベクトル  $\mathbf{v}'_{i,j}$  をオリジナルテンプレートと呼び、行列  $\mathbf{B} \in \mathbb{R}^{d \times M}$  を用いてそれを線形変換することによって得られたベクトル  $\mathbf{v}_{i,j}$  をテンプレートとする。ここで、 $M = HW$  である。すなわち、

$$\mathbf{v}_{i,j} = \mathbf{B}\mathbf{v}'_{i,j} \quad (1)$$

となる。上式において、テンプレートは  $\mathbf{B}$  が単位行列 ( $d = M$ ) ならば画素値に、分散  $\frac{1}{d}$ 、平均 0 のガウス分布に従う行列ならばランダム射影による特徴量 [1] になる。

また、 $K$  人中  $i$  番目に登録された人物に対して、 $N_i$  個のテンプレート

$$\mathbf{A}_i = [\mathbf{v}_{i,1}, \dots, \mathbf{v}_{i,N_i}] \quad (2)$$

が予め登録されている。この識別法 [1] では、 $i$  番目の人物に属するクエリ画像  $\mathbf{I}_q \in \mathbb{R}^{H \times W}$  から特徴量抽出して得られたクエリテンプレート  $\mathbf{y} \in \mathbb{R}^d$  が  $i$  番目の人物の登録テンプレートで

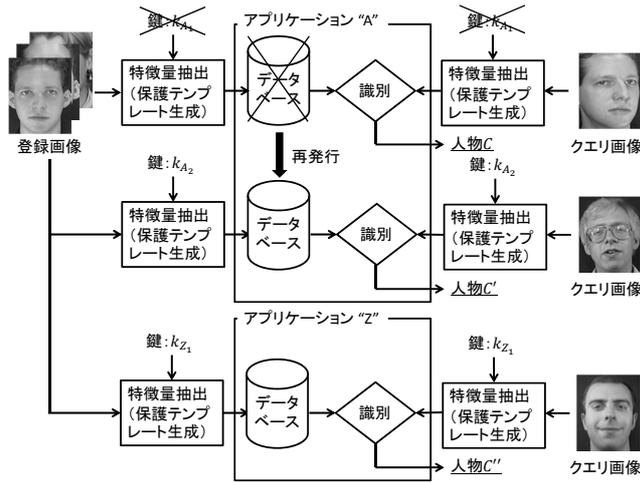


図2: キャンセラブルバイオメトリクスに基づく顔識別システム。×印は失効を表す。

線形近似されると仮定する。すなわち、

$$\mathbf{y} = \mathbf{v}_{i,1}x_{i,1} + \dots + \mathbf{v}_{i,N_i}x_{i,N_i} = \mathbf{A}_i\mathbf{x}_i \quad (3)$$

が成立する。それゆえ、 $K$  人の登録者に関する全ての登録テンプレートを用いて、 $\mathbf{y}$  は次のように表現される。

$$\begin{aligned} \mathbf{y} &= \mathbf{A}_1\mathbf{0} + \dots + \mathbf{A}_{i-1}\mathbf{0} + \mathbf{A}_i\mathbf{x}_i + \mathbf{A}_{i+1}\mathbf{0} + \dots + \mathbf{A}_K\mathbf{0} \\ &= \mathbf{A}\mathbf{x}_0 \end{aligned} \quad (4)$$

但し、

$$\mathbf{A} = [\mathbf{A}_1, \dots, \mathbf{A}_K] \in \mathbb{R}^{M \times N}, \quad (5)$$

$$\mathbf{x}_0 = [\mathbf{0}, \dots, \mathbf{0}, \mathbf{x}_i, \mathbf{0}, \dots, \mathbf{0}] \in \mathbb{R}^N, \quad (6)$$

$$N = \sum_{i=1}^K N_i. \quad (7)$$

ここで、係数ベクトル  $\mathbf{x}_0$  は  $i$  番目の人物に無関係な係数はゼロとなるためスパースとなる。この性質に基づき、式 (4) を解くことによって得られる解  $\mathbf{x}_0$  によって顔を識別する。

もし式 (4) が優決定問題、すなわち  $d \geq N$  ならば、解は最小二乗問題を解くことによって一意に決定される。しかし、劣決定問題、すなわち  $d < N$  ならば、解を一意に決定することはできない。しかし、最適解  $\mathbf{x}_0$  がスパースならば、 $l^0$  ノルム最小化問題を解くことによって決定される解  $\hat{\mathbf{x}}_0$  に一致する。

$$\hat{\mathbf{x}}_0 = \min_{\mathbf{x}} \|\mathbf{x}\|_0 \text{ subject to } \mathbf{y} = \mathbf{A}\mathbf{x}. \quad (8)$$

更に、もし最適解  $\mathbf{x}_0$  が十分にスパースならば、以下の  $l^1$  ノルム最小化問題の解  $\hat{\mathbf{x}}_1$  に一致する。

$$\hat{\mathbf{x}}_1 = \min_{\mathbf{x}} \|\mathbf{x}\|_1 \text{ subject to } \mathbf{y} = \mathbf{A}\mathbf{x}. \quad (9)$$

式 (9) は多項式時間で解くことができる。また、これらの問題を解くための高速アルゴリズムが研究されている [13]。

最後に、式 (9) を解いた後、クエリテンプレート  $\mathbf{y}$  が式 (4) と  $\hat{\mathbf{x}}_1$  に基づいて再構成される。 $\mathbf{y}$  と  $i$  番目の人物に対して再

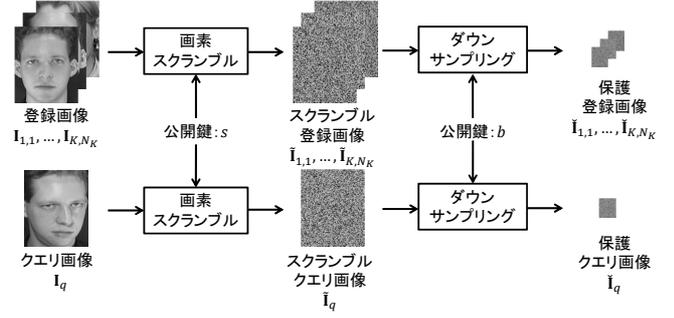


図3: 提案法

構成されたクエリテンプレート  $\mathbf{A}\delta_i(\hat{\mathbf{x}}_1)$  との誤差を最小とする人物  $C$  を識別結果とする。

$$r_i = \|\mathbf{y} - \mathbf{A}\delta_i(\hat{\mathbf{x}}_1)\|_2 \quad (10)$$

$$C = \arg \min_i r_i \quad (11)$$

ここで、 $\delta_i(\hat{\mathbf{x}}_1)$  は  $i$  番目の人物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。

$$\delta_i(\hat{\mathbf{x}}_1) = [0, \dots, 0, \hat{x}'_{i,1}, \dots, \hat{x}'_{i,N_i}, 0, \dots, 0]^T. \quad (12)$$

## 2.2 テンプレート保護法に対する要件

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なければならない。顔や指紋、虹彩などの生体情報に関するテンプレートを保護する方法は以下の4つの特性を満たすべきだとされている [14]。

(a) 多様性: テンプレート保護のための鍵 (パラメータ) はアプリケーションごとに異なるべきである。

(b) 失効可能: あるアプリケーションにおいて保護テンプレートの信頼性が失われた場合、そのアプリケーションにおける保護テンプレートを全て破棄し、鍵を変更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再発行することができる。

(c) 性能: テンプレート保護法は識別性能を低下させるべきではない。

(d) 安全性: 保護テンプレートからオリジナルテンプレートを得ることが計算上困難である。

生体認証の分野において、テンプレート保護の枠組みの1つとして知られるキャンセルバイオメトリクス [7] が挙げられる。図2はその枠組みに基づいた顔識別システムを示す。このシステムでは、要件 (a) と要件 (b) とを満たしていることが分かる。要件 (c) と要件 (d) とを満たすかどうかは保護テンプレート生成法によって決定される。

## 3. 提案法

本節では、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を提案する。図3は提案法のブロック図を示す。

### 3.1 手順

提案法は2つの手順から構成される。

(a) 画素スクランブル

(b) ダウンサンプリング

各手順の詳細は以下に記述される。

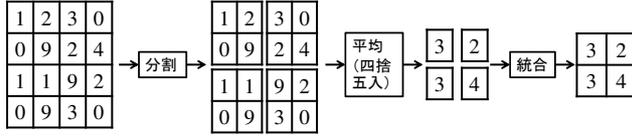


図 4: ダウンサンプリングの例 ( $H = W = 4$ ,  $b = 2$ )

### (a) 画素スクランブル

元画像  $\mathbf{I} \in \mathbb{R}^{H \times W}$  を視覚的に保護するために、 $\mathbf{I}$  の画素位置がランダムに並び替えられる。本稿では、これを画素スクランブルと呼ぶ。

$$\tilde{\mathbf{I}} = \text{PixScr}(\mathbf{I}, s) \quad (13)$$

ここで、 $\tilde{\mathbf{I}} \in \mathbb{R}^{H \times W}$  はスクランブル画像、 $\text{PixScr}()$  は画素位置を並び替える関数、 $s$  は並び替えのためのシードである。 $s$  は保護テンプレート生成法における第一の鍵である。

### (b) ダウンサンプリング

画素スクランブルは可逆変換なので、悪意ある者が  $s$  と  $\tilde{\mathbf{I}}$  を入手した場合、 $\tilde{\mathbf{I}}$  から逆スクランブルによって容易に元画像  $\mathbf{I}$  を復元されてしまう。このような不正な復元を防ぐために、 $\hat{\mathbf{I}}$  をサイズ  $\frac{H}{b} \times \frac{W}{b}$  の画像にダウンサンプリングする。

$$\hat{\mathbf{I}} = \text{DownSamp}(\tilde{\mathbf{I}}, b) \quad (14)$$

ここで、 $\hat{\mathbf{I}} \in \mathbb{R}^{\frac{H}{b} \times \frac{W}{b}}$  は保護画像であり、 $\text{DownSamp}(\tilde{\mathbf{I}}, b)$  は  $\tilde{\mathbf{I}}$  を  $b \times b$  のブロックに分割し、各ブロックでの画素平均を計算し、平均値を統合する関数である。図 4 は  $4 \times 4$  の画像に対して  $b = 2$  のダウンサンプリングを行う例を示す。 $b$  は保護テンプレート生成法における第二の鍵である。

## 3.2 提案法を適用したスパース表現に基づく顔識別

$K$  人 (各  $N_K$  枚) の保護登録画像  $\tilde{\mathbf{I}}_{1,1}, \dots, \tilde{\mathbf{I}}_{K,N_K}$  と保護クエリ画像  $\tilde{\mathbf{I}}_q$  をそれぞれラスタスキャンすることによって得られたベクトル  $\mathbf{v}'_{1,1}, \dots, \mathbf{v}'_{K,N_K}$  と  $\mathbf{y}'$  をそのまま保護テンプレートとする。つまり、式 (1) における変換行列  $\mathbf{B}$  を  $\frac{M}{b^2} \times \frac{M}{b^2}$  の単位行列として保護登録テンプレート  $\check{\mathbf{A}} = [\mathbf{v}'_{1,1}, \dots, \mathbf{v}'_{K,N_K}] \in \mathbb{R}^{\frac{M}{b^2}}$  と保護クエリテンプレート  $\check{\mathbf{y}} \in \mathbb{R}^{\frac{M}{b^2}}$  を生成する。

このとき、式 (9) は以下のように表現される。

$$\check{\mathbf{x}}_1 = \min_{\mathbf{x}'} \|\mathbf{x}'\|_1 \text{ subject to } \check{\mathbf{y}} = \check{\mathbf{A}}\mathbf{x}'. \quad (15)$$

最後に、式 (10)、式 (11) と同様に、人物  $C$  は以下によって同定される。

$$\check{r}_i = \|\check{\mathbf{y}} - \check{\mathbf{A}}\delta_i(\check{\mathbf{x}}_1)\|_2 \quad (16)$$

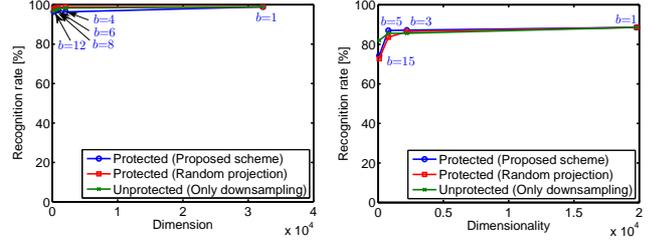
$$C = \arg \min_i \check{r}_i \quad (17)$$

## 3.3 特徴

本節では、提案法の特徴を記述する。

### (a) 鍵の管理が不要

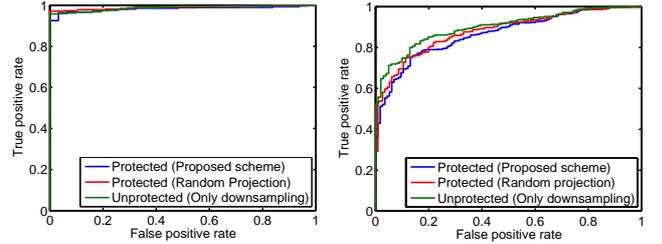
画素スクランブルとダウンサンプリングの変換パラメータ  $s$  と  $b$ 、つまり 2 つの鍵が公知の場合においても、ランダム射影と同等に、一般に提案法による保護テンプレートから顔画像の



(a) Extended Yale B database.

(b) AR database.

図 5: 非保護 (従来法 [1]) と保護 (提案法) されたスパース表現に基づく顔識別法におけるテンプレートの次元  $d$  に対する識別率



(a) Extended Yale B database.

(b) AR database.

図 6: 非保護 (従来法 [1]) と保護 (提案法) されたスパース表現に基づく顔識別法における ROC 曲線

視覚的情報を復元することは困難である。それゆえ、提案法は鍵の管理が不要であり、鍵を公開できるという利点がある。視覚的復元の困難性については次節で実験的にも確認される。

### (b) 効果的なデータ圧縮

提案法による保護画像の画素値分布 (ヒストグラム) は元画像よりも疎になる。このことはランダムにサンプリングされた画素の平均値が元画像のヒストグラムの平均値に近づくためである。ヒストグラムの疎性はデータ圧縮において効果的とされている [15, 16] ため、提案法による保護画像は効果的なデータ圧縮が期待される。

## 4. 実験

本節では、[1] と同様に、代表的な顔画像データベースである Extended Yale B database [17] と AR database [18] とを用いて、提案法がスパース表現に基づく顔識別法の識別性能を殆ど低下させない (要件 (c) を満たす) ことを実験的に示し、また提案法による保護テンプレートから元画像の視覚的情報を復元することが困難である (節 2.2 における要件 (d) を満たす) こと、そして提案による保護画像が効果的なデータ圧縮を実現することを実験的に示す。

### 4.1 Extended Yale B database に対する識別性能

Extended Yale B database [17] は 38 人分の顔画像 2414 枚で構成される。顔画像は実験室で制御された様々な照明条件にて撮影された。この実験では、図 8(a) のように、 $192 \times 168$  に切り取られたものを使用した。また、各被験者に対する約 64 枚の顔画像を 2 つのグループに分割し、1 つのグループを訓練のために、他のグループをクエリのために使用した。

図 5(a) と図 6(a) では、非保護なスパース表現に基づく顔識別



図 7: 非保護テンプレート (ダウンサンプリングのみ) と従来法 [8] による保護テンプレートとから復元された画像.

(ダウンサンプリングのみ), ランダム射影を適用したスパース表現に基づく顔識別, 提案法を適用したスパース表現に基づく顔識別における, テンプレートの次元  $d$  に対する識別率と ROC 曲線とをそれぞれ示す. なお, ROC 曲線は,  $b = 8$  として閾値  $\tau \in [0, 1]$  を変化させながら, 以下の式に従って求めた値をプロットしている.

$$\text{if } \min r_i \leq \tau \text{ then accepted; else rejected} \quad (18)$$

$$\text{if } \min \hat{r}_i \leq \tau \text{ then accepted; else rejected} \quad (19)$$

提案法はスパース表現に基づく顔識別 [1] の識別性能を殆ど低下させないこと, すなわち, 提案法が要件 (c) を満たすことが確認された.

#### 4.2 AR database に対する識別性能

AR database [18] は 126 人分の顔画像 4000 枚超で構成される. 顔画像は  $165 \times 120$  のサイズに切り取られたもの [19] を使用した. この実験では, 50 人の男性と 50 人の女性に対する一部のデータセットを使用した. 各被験者に対して, 顔の表情と実験室で制御された様々な照明条件をもつ 14 枚の画像 (撮影は 2 週間離れた 2 回のセッションで行われた) を選択した. 1 回目のセッションで撮影された 7 枚の画像を訓練のために, 2 回目のセッションで撮影された 7 枚の画像をクエリのために使用した. 図 5(b) と図 6(b) は, 節 4.1 と同様に, 非保護なスパース表現に基づく顔識別, ランダム射影を適用したスパース表現に基づく顔識別, 提案法を適用したスパース表現に基づく顔識別における, テンプレートの次元  $d$  に対する識別率と ROC 曲線とをそれぞれ示す. 但し, 図 6(b) において,  $b = 5$  とした. 提案法はスパース表現に基づく顔識別 [1] の識別性能を殆ど低下させないことが分かる. つまり, 提案法が要件 (c) を満たすことが確認された.

#### 4.3 安全性の検証

ここでは, 提案法による保護テンプレートから顔画像の視覚的情報を復元することが困難であることを示す. 図 7 は非保護テンプレート (ダウンサンプリングのみ) とランダム射影を用いた生成法 [8] による保護テンプレートとを, それぞれバイリニア補間と圧縮センシングの概念 [20] とを用いて復元された  $192 \times 168$  の元画像を示す. 但し, 図 7(c) では  $d = 504 (b = 8$  に相当) とした. 但し,  $b$  と  $d$  の関係は, 元画像の画素数を  $M$  として

$$d = \frac{M}{b^2} \quad (20)$$

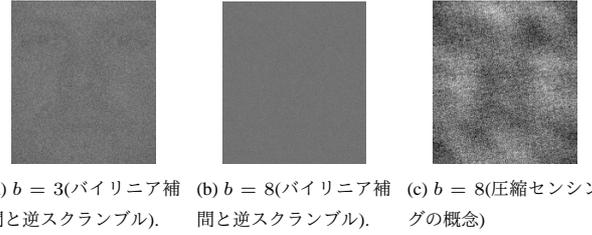


図 8: 提案法によって生成された保護テンプレートから復元された画像. () 内は復元方法を表す.

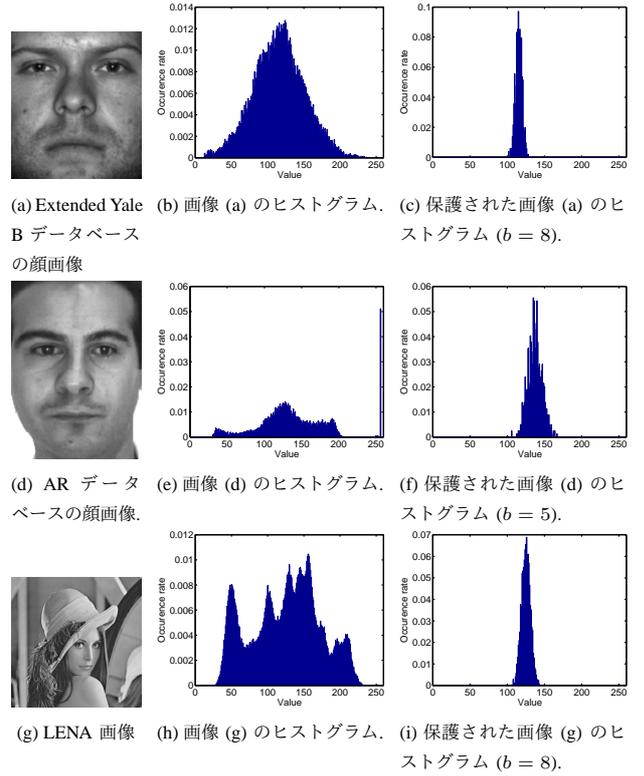


図 9: 提案法によって生成された保護テンプレートの値分布.

で与えられる.

一方で, 図 8(a) と図 8(b) はそれぞれ  $b = 3$ ,  $b = 8$  に対して, バイリニア補間と逆画素スクランブルとを用いて, 保護テンプレートから復元された元画像を示す. また図 8(c) は  $b = 8$  に対して, 圧縮センシングの概念を用いて, 保護テンプレートから復元された元画像を示す. 提案法による保護テンプレートから元画像の視覚的情報を復元できないことが分かる. 以上の結果から提案法による保護テンプレートは, ランダム射影による保護テンプレートと同程度の復元困難性を有すること, すなわち, 要件 (d) を満たすことが確認された.

#### 4.4 データ圧縮に関する検証

最後に, 提案法による保護テンプレートが効率的なデータ圧縮を実現できることを示す. 図 9 は Extended Yale B database の顔画像 ( $192 \times 168$ ), AR database の顔画像 ( $165 \times 120$ ), Lena 画像 ( $512 \times 512$ ) に対する, 元画像と保護画像の画素値分布 (ヒストグラム) をそれぞれ示す. 但し, 各画像に対して, それぞれ  $b = 8$ ,  $b = 5$ ,  $b = 8$  を用いた. 元画像のヒストグラムに比べて, 保護画像のヒストグラムが集中している. ヒストグラム

表 1: テンプレートの次元  $d$  に対するテンプレートのデータ量 [bpp]

(a) Extended Yale B database

テンプレートの次元 $d$ (ブロックサイズ $b$ )	192 × 168 ( $b = 1$ )	48 × 42 ( $b = 4$ )	32 × 42 ( $b = 6$ )	24 × 21 ( $b = 8$ )	16 × 14 ( $b = 12$ )
保護+JPEG-LS	7.79	6.13	<b>5.70</b>	<b>5.35</b>	<b>5.46</b>
非保護+JPEG-LS	<b>3.90</b>	<b>5.70</b>	6.67	7.56	9.29
保護 (ランダム射影)	64	64	64	64	64

(b) AR database

テンプレートの次元 $d$ (ブロックサイズ $b$ )	165 × 120 ( $b = 1$ )	55 × 40 ( $b = 3$ )	33 × 24 ( $b = 5$ )	11 × 8 ( $b = 15$ )
保護+JPEG-LS	8.20	7.38	6.91	<b>7.09</b>
非保護+JPEG-LS	<b>3.91</b>	<b>5.28</b>	<b>6.51</b>	13.27
保護 (ランダム射影)	64	64	64	64

(c) Lena

テンプレートの次元 $d$ (ブロックサイズ $b$ )	512 × 512 ( $b = 1$ )	128 × 128 ( $b = 4$ )	64 × 64 ( $b = 8$ )	32 × 32 ( $b = 16$ )	16 × 16 ( $b = 32$ )
保護+JPEG-LS	8.01	6.09	5.19	<b>4.46</b>	<b>4.25</b>
非保護+JPEG-LS	<b>4.24</b>	<b>4.74</b>	<b>5.70</b>	7.39	10.34
保護 (ランダム射影)	64	64	64	64	64

の疎性は画像圧縮において有効とされている [15, 16]. 表 1 はロスレス画像圧縮方式である JPEG-LS [21] を用いて, 非保護画像 (ダウンサンプリングのみ) と提案法による保護画像とを圧縮した際のデータ量と, ランダム射影による保護テンプレートのデータ量をそれぞれ画素数あたりのデータ量 (bpp) 示す. ランダム射影による保護テンプレートは一般に倍精度浮動小数点型で表現されるため, JPEG-LS を適用することができない. それに対して, 提案法による保護画像は 8 ビットの符号なし整数型で表現されるためデータサイズを削減することができることが確認された.  $b$  が小さい場合において, 非保護なテンプレートは効果的なデータ圧縮を実現しているが, 図 7(b) で示したようにテンプレートから元画像の視覚的情報を復元されてしまう. それに対して,  $b$  が大きい場合において, 提案法による保護テンプレートはより集中したヒストグラムの分布を有するため, 非保護なテンプレートよりも効果的なデータ圧縮が可能であることが確認された.

## 5. おわりに

本稿では, 保護テンプレートの新たな生成法を提案し, スパース表現に基づく顔識別を例にそれを適用した. 提案法は画素スクランブルとダウンサンプリングとで構成される. スクランブルとダウンサンプリングの変換パラメータが公知の場合においても, 保護テンプレートから元画像の視覚的情報を復元することが困難となる. 提案法はスパース表現に基づく顔識別法 [1] の識別性能を殆ど低下させない. ダウンサンプリングのブロックサイズが小さい場合には, 非保護なテンプレートが効果的な圧縮を実現するが, 元画像の視覚的情報を復元できるため安全とは言えない. 一方で, ブロックサイズが大きい場合には, 提案法による保護テンプレートが非保護なテンプレートに比べて, より効果的なデータ圧縮が可能となる. これによって, データベース容量の削減が期待される.

## 文 献

[1] J. Wright, A.Y. Yang, A. Ganesh, S.S. Sastry, and Y. Ma, “Robust face recognition via sparse representation,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol.31, no.2, pp.210–227, Feb. 2009.  
 [2] L. Wiskott, J.M. Fellous, N. Krüger, C.v.d. Malsburg, “Face recognition by elastic bunch graph matching,” *IEEE Trans. Pattern Anal.*

*Mach. Intell.*, vol.19, no.7, pp.775–779, Jul. 1997.  
 [3] T. Ahonen, A. Hadid, and M. Pietikäinen, “Face description with local binary patterns: Application to face recognition,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol.28, no.12, pp.2037–2041, Dec. 2006.  
 [4] M. Turk and A. Pentland, “Eigenfaces for recognition,” *J. Cognitive Neuroscience*, vol.3, no.1, pp.71–86.  
 [5] P.N. Belhumeur, J.P. Hespanha, and D.J. Kriegman, “Eigenfaces versus fisherfaces: Recognition using class specific linear projection,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol.19, no.7, pp.711–720, Jul. 1997.  
 [6] X. He, S. Yan, Y. Hu, P. Niyogi, and H.J. Zhang, “Face recognition using laplacianfaces,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol.27, no.3 pp.328–340, Mar. 2005.  
 [7] 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.  
 [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 Anal. Mach. Intell.*, vol.33, no.9, pp.1877–1893, Sept. 2011.  
 [9] A.B.J. Teoh, A. Goh, and D.C.L. Ngo, “Random multispace quantization as analytic mechanism bihashing of biometric and random identity inputs,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol.28, no.12, pp.1892–1901, Dec. 2006.  
 [10] 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, no.5, pp.1096–1106, Oct. 2007.  
 [11] Y.C. Feng, P.C. Yuen, and A.K. Jain, “A hybrid approach for generating secure and discriminating face template,” *IEEE Trans. Info. Fore. Security*, vol.5, no.1, pp.103–117, Mar. 2010.  
 [12] M. Furukawa, Y. Muraki, M. Fujiyoshi, and H. Kiya, “A secure face recognition scheme using noisy images based on kernel sparse representation” in *Proc. APSIPA ASC*, no.OS.20–IVM.9–4, Kaohsiung, Taiwan, R.O.C., Oct. 2013.  
 [13] A.Y. Yang, Z. Zihan, A.G. Balasubramanian, S.S. Sastry, and Y. Ma, “Fast  $\ell_1$ -minimization algorithms for robust face recognition,” *IEEE Trans. Image Process.*, vol.22, no.8, pp.3234–3246, Aug. 2013.  
 [14] A.K. Jain, K. Nandakumar, and A. Nagar, “Biometric template security,” *EURASIP J. Adv. Signal Process.*, vol.2008, Jan. 2008.  
 [15] P.J.S.G. Ferreira, and A.J. Pinho, “Why does histogram packing improve lossless compression rates?,” *IEEE Signal Process. Letter*, vol.9, no.8, Aug. 2002.  
 [16] A.J. Pinho, “An online preprocessing technique for improving the lossless compression of images with sparse histogram,” *IEEE Signal Process. Letter*, vol.9, no.1, Jan. 2002.  
 [17] A. Georghiadis, P. Belhumeur, and D. Kriegman, “From few to many: Illumination cone models for face recognition under variable lightning and pose,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol.23, no.6, pp.643–660, June 2001.  
 [18] A. Martinez and R. Benavente, “The AR face database,” *CVC Technical Report #24*, June 1998.  
 [19] A.M. Martinez and A.C. Kak, “PCA versus LDA,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol.23, no.2, Feb. 2002.  
 [20] E.J. Candes and T. Tao, “Near-optimal signal recovery from random projections: Universal encoding strategies?,” *IEEE Trans. Info. Theory*, vol.52, no.12, pp.5406–5425, Dec. 2006.  
 [21] ISO/IEC 14495–1, Information technology — Lossless and near-lossless compression of continuous-tone still images: Baseline, Dec. 1999.  
 [22] M.J. Weinberger, G. Seroussi, and G. Sapiro, “The LOCO-I lossless image compression algorithm: principles and standardization into JPEG-LS,” *IEEE Trans. Image Process.*, vol.9, no.8, pp.1309–1324, Aug. 2000.