

## 重心による位置補正を行うブロックスクランブル手法

武田明久<sup>†</sup> 岩村恵市<sup>††</sup>

生体情報は一度漏えいすると、他の認証システムでも悪用されることになり危険である。キャンセルラブルバイオメトリクス的一种であるブロックスクランブル方式は特徴点座標をブロックごとに分けて、ブロックをスクランブルすることで、元のテンプレートを特定できなくする。しかし位置ずれや回転ずれが発生した場合に特徴点が別のブロックに所属してしまい、認証スコアが落ちる場合がある。したがってブロックの大きさはあまり小さくできず、セキュリティ強度として強くない。これらの問題を解決するために本稿では重心を利用した位置補正を提案する。位置を補正することでブロックサイズを小さくした場合の認証スコアの向上を目的としている。重心からテンプレート情報を特定することは困難である。

### A block scramble technique of performing the position compensation by the center of gravity

AKIHISA TAKEDA<sup>†</sup> KEIICHI IWAMURA<sup>††</sup>

Once biometric data is exposed, it may be abused in other authentication systems, which is very dangerous. The brock scramble, a kind of cancelable biometrics, hides the original template data by scrambling brocks of coordinate of the minutia which are divided into brocks. However, in case a position gap or rotation gap occurs, minutia will move to another brocks, and verification score may fall. The Brock size must not be too small in order to keep the security intensity high. To solve this problem, we propose a scheme that use the center of gravity to compensate position gap. By using the position compensate scheme, we can improve verification score when block size small is smaller. It is very difficult to detect original template data from the center of gravity.

### 1. はじめに

近年ネットワークが普及し、オンライン情報における個人認証の重要性が高まっている。それに伴い個人情報不正アクセスや情報漏洩などが問題になっており、個人情報の漏洩に伴う悪用、偽造、なりすましなどの犯罪が増加している。シリコンで作成された偽造指紋でゲートを通過するなどの事件も起きている。そこで個人認証のセキュリティ向上と利便性の両立が求められている。一方で、生体情報は一生変更することができないことから、漏洩すると他の認証システムでも悪用されるという欠点がある。このようにパスワード認証などと同様にテンプレートが漏洩した場合には即座にそのテンプレートを失効・再登録を行う必要がある。この問題を解決するため、サーバに対して生体情報を秘匿しつつ認証を受けることが可能な、キャンセルラブルバイオメトリクスが提案されている。

キャンセルラブルバイオメトリクスにはモーフィング方式・ブロックスクランブル方式・画像マッチングなどがあるが、ブロックスクランブル方式は特徴点を格子状に区切ったブロックにそれぞれ配置させて、ブロックの位置をスクランブルさせる。ブロックをスクランブル化させる乱数がキャンセルラブルバイオメトリクスの関数に相当する。複数のブロックの特徴点が同じブロックで混ざることあるため一方関数の役割を果たしている。テンプレートが漏えいした際はスクランブル化の乱数を変更することでブロックの位置を変更する。ブロックの配置を変えるだけなので、他の方式に比べて計算コストが小さくなっている。またスクランブル化後の特徴点は元の特徴点とデータの形式が同様なので、保護を行っていない従来の方式からの移行が容易で、特徴点を扱う既存のテンプレート保護技術と組み合わせることもできると考えられる。ただし、問題点として認証時に特徴点の位置がずれた場合、特徴点が違うブロックに配置され、スクランブル化した後の認証スコアが低下する場合がある。特徴点の位置がずれる原因として特徴点個別の微小変化ノイズ・特徴点の消失と特徴点全体の位置ずれを挙げる。生体認証で用いる画像は毎回全く同じではなく、抽出する機器の状態や指表面の汚れなどでゆらぎが生じるので、画像処理の際に微小変化ノイズや特徴点の消失が発生してしまう。また登録時と全く同じ場所に指を置くことは不可能であり、位置ずれは必ず発生してしまう。よって、ブロック分割数を増やしていくとブロックサイズは小さくなっていくので、少しの位置ずれだけで別のブロックに配置されてしまう可能性が高くなる。したがってブロック数をあまり多くできず、組み合わせが限られてしまうのでセキュリティ強度として高くない。参考文献[1][2]は補正データを用いて特徴点をブロックの境界線から遠ざけるようなデータを作成し、別のブロックへ

\*<sup>†</sup> 東京理科大学大学院  
Tokyo University of Science Graduate School  
<sup>††</sup> 東京理科大学  
Tokyo University of Science

移動することを防いでいる。この方式の問題点として特徴点が2ブロック以上移動すると、元のブロックに戻れなくなることと、補正データ領域の割合が高くなると補正データが漏えいした際に元の特徴点の配置が特定されやすくなることがある。そこで本論文ではエリアごとの重心を求め、最もズレが少ないエリアを選択して位置ずれを補正し、スクランブル化した後に認証スコアを算出する。対象は位置ずれと特徴点の消失とする。これによって、認証スコアの向上を目的としている。

## 2. キャンセラブルバイオメトリクス

キャンセラブルバイオメトリクスとはテンプレート保護型の生体認証システムである。生体情報の特徴量をパラメータでテンプレートに変換し、元の生体情報を特定されないように認証を行う技術である。テンプレートは一方向性関数によって変換されるので、パラメータとテンプレートが同時に漏えいしない限り、元の生体情報に復元することは困難となっている。テンプレートが漏えいした場合はパラメータを変更することによってテンプレートを再登録する。この際に再登録するテンプレートは元のテンプレートと関連が薄いようなものにする。本論文で対象とするブロックスクランブルはスクランブル情報が変換のパラメータとなっている。

### 2.1 ブロックスクランブル方式

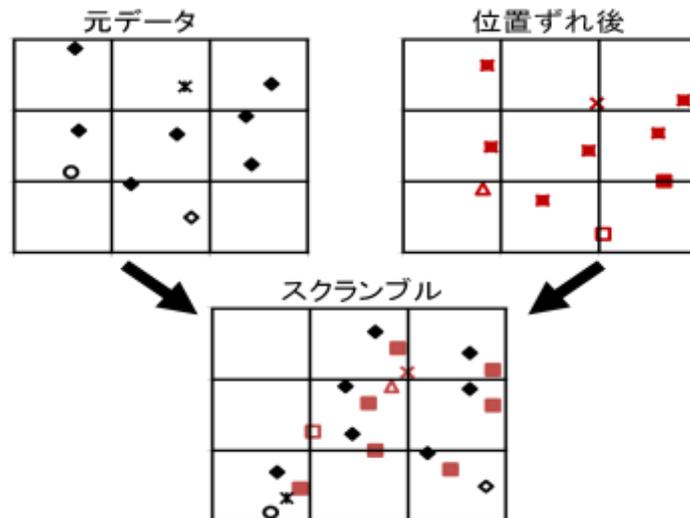


図1 位置ずれによる境界線問題

ブロックスクランブル方式とは特徴点を格子状に区切ったブロックにそれぞれ配置させて、ブロックの位置をスクランブルさせる方式である。複数のブロックの特徴点と同じブロックで混ざることによって一方向関数の役割を果たしている。テンプレートが漏えいした際はスクランブル化の乱数を変更することでブロックの位置を変更する。問題点として認証時に特徴点の位置が変わってしまう場合、特徴点が違うブロックに位置され、移動前は特徴点の差異が小さかったとしても、移動後は別のブロックに配置されるので差異が大きくなってしまふ。

図1に右下方向への位置ずれの例を示す。塗りつぶされていない点は、他の点に比べて大きくずれてしまっている。これは位置ずれにより別のブロックに位置されたためである。このように境界線を越えて別のブロックに位置してしまうことを境界線問題と言う。提案方式では位置ずれを重心により元の位置に戻してスコアの向上を行う。

### 2.2 既存方式・境界線問題解決手法

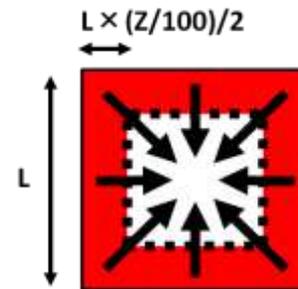


図2 補正データ領域

[1][2]の方式を説明する。この方式は境界線問題を解決するために、補正データを用いている。補正データとは特徴点をブロックの境界線から遠ざけるようなデータのことである。ブロック境界線付近の不安定な特徴点をノイズが入った後にブロックの中央へ移すことで特徴点が安定し、照合スコアも向上させることが可能となっている。図2に補正データについて示す。外側の色が塗られている領域が補正領域で、この部分に配置された特徴点は点線の枠内の領域部分に移動させるような補正データと関連付けられる。補正データは補正後のデータが枠内の領域内に収まるようなランダムな整数から選択される。最初から枠内の領域に配置された特徴点の補正データは0となる。

ブロックの一辺の長さをL、ブロックの面積に対する補正領域の割合をZ%とおくと、補正領域の幅は図2のように  $L \times (Z/100)/2$  となる。

この方式の問題点として特徴点が2ブロック以上移動すると、元のブロックに戻れ

なくなる点と、補正データ領域の割合が高くなると、補正データが漏えいした際に元の特徴点の配置が特定されやすくなる点と、X座標順に補正データを保存しているので、特徴点が消失した場合にどの補正データがどの特徴点に関連付けられているのかわからなくなる点がある。

### 3. 提案方式

既存方式は2ブロック以上特徴点が移動した場合元のブロックに戻せなくなるという問題点がある。位置ずれの場合は微小変化ノイズと違い、2ブロック以上移動する場合は考えられる。例として指紋画像が300×300pixelで30mm×30mmだった場合、ブロック分割数を10,20,30,40,50と増やしていくとブロックサイズは30×30,15×15,7×7,4×4,2×2pixelと小さくなっていく。したがって位置ずれの場合2ブロック以上移動することは十分想定されると言える。提案方式では特徴点の重心を登録情報と照合情報でそれぞれ計算しその差分の値を全ての特徴点に加えることで位置の補正を行う。指紋の渦の中心や三角州によって位置を合わせる方法もあるが、指紋によってはない場合もある。また安定して抽出できない可能性がある。セキュリティの面からも一点だけではあるが特徴点が漏洩する危険性がある。

重心は以下の式で表わされる。

$$X_G = \frac{\sum_{i=1}^n X_i}{n} \quad Y_G = \frac{\sum_{i=1}^n Y_i}{n}$$

$X_G$  : X座標の重心     $Y_G$  : Y座標の重心     $n$  : 特徴点の個数

しかし重心を補正に用いる場合、位置ずれには対応できるが、特徴点が消失した場合、重心がずれて元の座標に戻せなく可能性がある。したがって本論文ではエリアごとの重心を提案する。特徴点集合から重心を求めることはできるが、重心から特徴点集合を特定することはできない。

#### 3.1 登録

1. 元の特徴点集合  $A_0 = \{a_1^0, \dots, a_n^0\}$  から全体の重心  $a_g$  を保存する。

2. それぞれのエリアで重心を保存する。

元の特徴点集合を X 成分について昇順にソートし  $A_L = \{a_1^l, \dots, a_n^l\}$  とする。

先頭から m 個選択する。  $A_{L2} = \{a_1^{l2}, \dots, a_m^{l2}\}$  選んだ m 個の重心  $a_{gl}$  を求める。

同様に X 成分について降順にソートして m 個選んだものの重心を  $a_{gr}$  とする。

同様に Y 成分について昇順にソートして m 個選んだものの重心を  $a_{gt}$  とする。

同様に Y 成分について降順にソートして m 個選んだものの重心を  $a_{gb}$  とする。

それぞれのエリア重心をまとめて  $A_G = \{a_g, a_{gl}, a_{gr}, a_{gt}, a_{gb}\}$  とする。

3. ランダムなスクランブル情報  $S$  を生成し、元の特徴点集合  $A_0$  を  $S$  に従ってスクランブルし、  $A_1 = \{a_1^1, \dots, a_n^1\}$  とする。

4. 登録テンプレート  $T = \{A_1, s, A_G\}$  を個人の ID とともに登録する。

#### 3.2 認証

1. 照合用の特徴点集合  $B_0 = \{b_1^0, \dots, b_n^0\}$  から登録時と同様に重心

$$B_G = \{b_g, b_{gl}, b_{gr}, b_{gt}, b_{gb}\} \text{ を求める。}$$

登録テンプレートより  $A_G$  を参照し、補正值  $h_G = |a_g - b_g|$  を求め、それぞれの

$$\text{エリア重心に加えて } \{a_{gl}, a_{gr}, a_{gt}, a_{gb}\} + h_G = \{h_{gl}, h_{gr}, h_{gt}, h_{gb}\}$$

とする。全体の位置ずれが補正される。

$$\text{次に } C_{gl} = |a_{gl} - b_{gl}| = \sqrt{(X_{agl} - X_{bgl})^2 + (Y_{agl} - Y_{bgl})^2}$$

を求める。それぞれのエリアで  $\{C_{gl}, C_{gr}, C_{gt}, C_{gb}\}$  を求め、もつとも値が小さく、ズレの小さいエリアを選択する。

ズレの少なかったエリアの  $|a_{gl} - b_{gl}|$  を特徴点集合に加えて

$$B_{0h} = \{b_1^{0h}, \dots, b_n^{0h}\} \text{ とする。}$$

この方式では微小変化ノイズがなく、4つのエリアのうち1つでも先頭からの  $m$  個の特徴点が失われていない場合は完全に補正できる。また先頭から多く選ぶとセキュリティ強度が高くなり、多くの特徴点で平均を取ることで微小変化ノイズには強くなる。ただし特徴点の消失が増えた場合に先頭からの  $m$  個に消失点が含まれる確率が高くなる。

したがって消失点が X 座標の昇順・降順、Y 座標の昇順・降順の先頭  $m$  個に含まれなければ、元の位置に戻すことができる。

図3にエリアごとの重心のずれの例を示す。

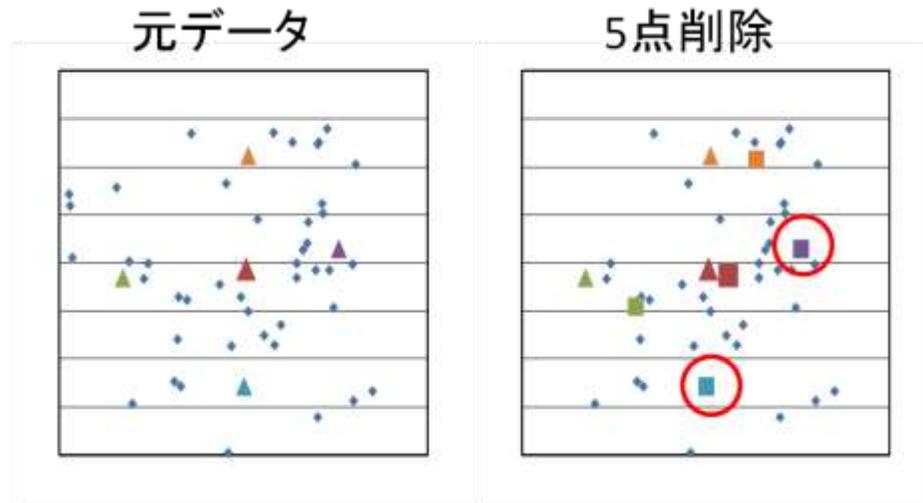


図3 エリアごとの重心のずれ

図3の左側が元データで、右側が X 成分について昇順にソートされた特徴点の先頭から5個を削除した図となっている。三角形のマーカーが元データのそれぞれのエリアの重心で、四角形のマーカーが5点を削除した後のエリアの重心となっている。左側にある特徴点が削除されているので、 $a_g$   $a_{gl}$   $a_{gt}$  はずれが生じているが、

$a_{gb}$   $a_{gr}$  はずれていない。位置補正を行うときは○を付けたいずれかを選択して補正を行うことができる。

2. 登録テンプレートから  $S$  を参照し、

元の特徴点集合  $B_{0h}$  を  $S$  に従ってスクランブルし、認証用の特徴点集合  $B_1 = \{b_1^1, \dots, b_n^1\}$  とする。

3.  $A_1$  と  $B_1$  から認証スコアを算出する。

#### 4. 実験

表1 シミュレーション諸元

|         |                                   |
|---------|-----------------------------------|
| 指紋データ   | FVC2004[6] DB2_の指紋画像 20 枚         |
| 特徴点抽出   | MINDTCT                           |
| 認証スコア   | BOZORTH3                          |
| 開発ソフト   | Microsoft Visual C++ 2010 Express |
| 画像サイズ   | 328 × 362                         |
| ブロック分割数 | 10 × 10, 20 × 20, 30 × 30         |
| ブロックサイズ | 32 × 36, 16 × 18, 10 × 12         |
| 特徴点の消失  | 0(消失点なし), 4(四隅)                   |
| 方式      | 既存, 境界線補正, 重心補正                   |

表1にシミュレーション諸元を示す。NISTが公開している指紋認証ソフトウェアであるNFIS2[5]を用いた。特徴点抽出ソフトウェアであるMINDTCTで元の特徴点集合を得て、認証スコア算出には特徴点同士を照合して類似度を算出するBOZORTH3を用いた。BOZORTH3を用いたことにより特徴点が消失した場合でもある程度のスコアを保つことができる。指紋の特徴量はX座標、Y座標、角度、信頼度を採用したが、スクランブル化したのはX座標、Y座標のみである。FVC2004の指紋画像について位置ずれを起こした時の本人-本人間照合と他の19枚との本人-他人間認証で比較を行った。位置ずれの移動値は1の時X座標を1、Y座標を1ずつ、30まで右下の方向にずらしていった。特徴点の消失は消失させなかった0と、X成分とY成分がそれぞれ最も小さいものと大きなものを選択して四隅を削除したものを対象とした。四隅を削除すると昇順・降順でソートした内の先頭の10個に含まれるので、4つのエリアが全てずれて完全に元の位置に戻すことはできなくなる。したがって重心で完全に補正できる消失0と、エリア補正では完全に補正できない四隅削除の場合で実験を行った。

図4～6に従来方式と提案方式の比較を示す。

0が消失点なし、四隅が四隅の点を削除した場合を示している。

既存は何も補正を行わずにスクランブルした方式。

境界線補正は補正データ領域を用いて補正を行った方式。

補正データ領域はZ=50とした。

重心は提案方式の重心補正を行った方式である。各エリアの重心は先頭から10個を選択して算出した。

設定するパラメータが多くなりすぎるため、前提条件として特徴点個別の微小変化ノイズはないものとした。

図の横軸は移動値で、縦軸はスコアを示している。図4はブロック分割数10、図5はブロック分割数20、図6はブロック分割数30の場合の比較を示した。

本人-本人間認証は20枚の画像それぞれについて、ブロック分割数、特徴点の消失、方式、移動値をそれぞれ変化させて、 $3 \times 2 \times 3 \times 31 = 558$ 通りのパラメータで実験を行い、平均をグラフに示した。

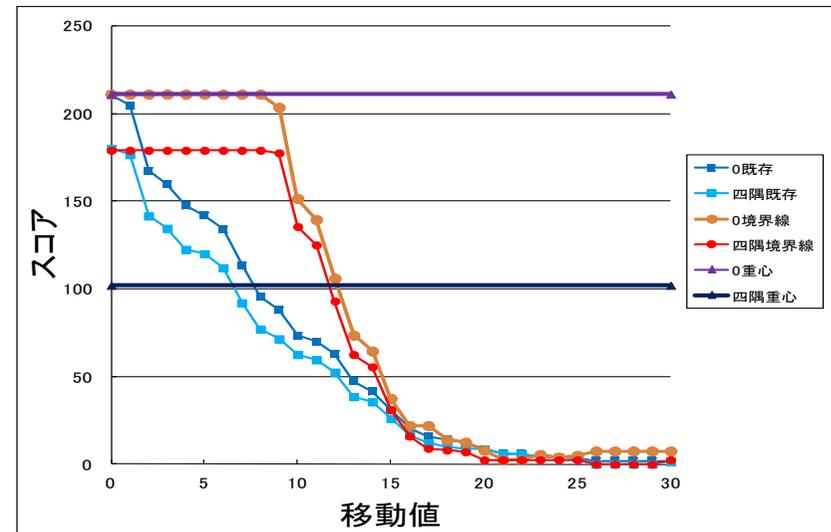


図4 移動値とスコアの関係・ブロック分割数10 (サイズ32×36)

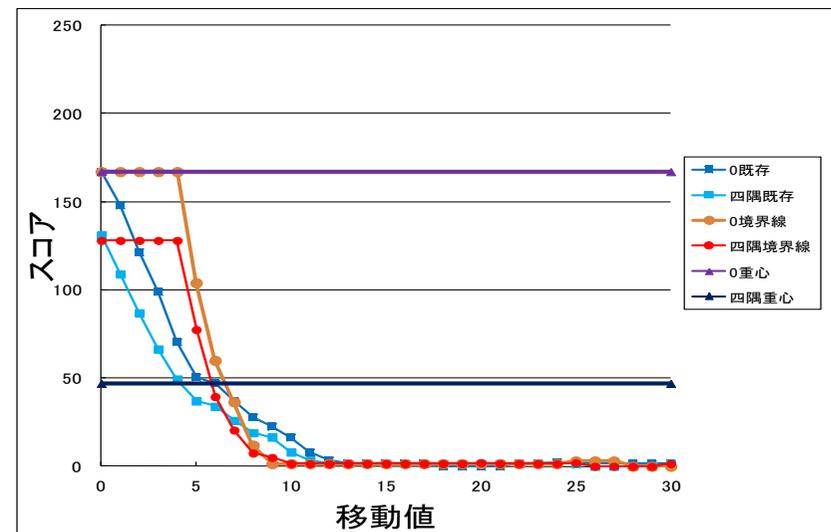


図5 ブロック分割数20 (サイズ16×18)

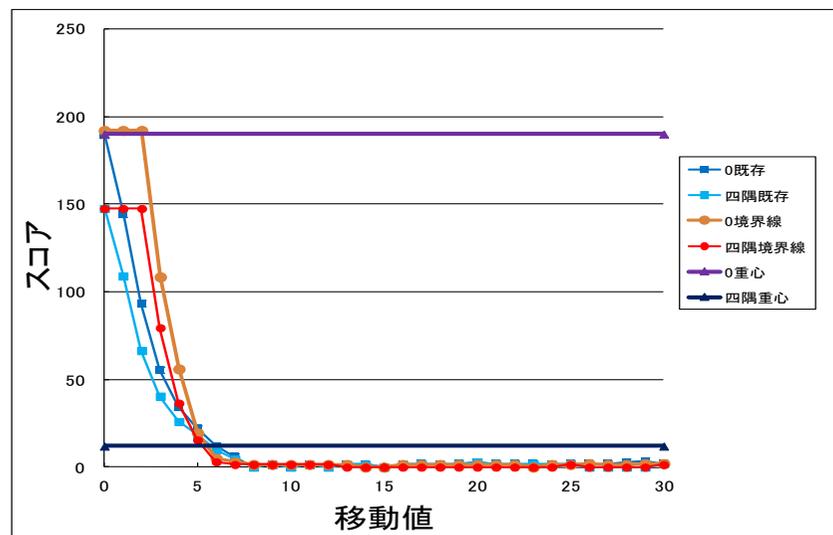


図6 ブロック分割数 30 (サイズ 10×12)

本人—他人間認証も同様に 20 枚の画像それぞれについて他の画像 19 枚との比較で 558 通りのパラメータで実験を行った. 0~30 までの移動値の平均スコアを表 2 に示す. 表 2 はブロック分割数と各方式のスコアを示している.

表 2 本人—人間認証におけるスコア

|    | 0 既存 | 四隅既存 | 0 境界線 | 四隅境界線 |
|----|------|------|-------|-------|
| 10 | 2.3  | 1.8  | 2.2   | 1.8   |
| 20 | 1.5  | 1.2  | 1.5   | 1.2   |
| 30 | 1.9  | 1.7  | 1.9   | 1.6   |

## 5. 考察

### ・本人—本人間認証

消失点が四隅の場合は 4 点特徴点を削除しているため、全体としてスコアが低くなっている. 既存方式と境界線補正方式はブロック数が増えるほど、少ない移動値で大きくスコアが落ちることがわかる. 図 4~6 より 10,20,30 の時でそれぞれ、移動値が 20,12,8 の時は既存・境界線補正方式でほぼスコアが 0 になっている. これは位置ずれによって多くの特徴点が違うブロックに位置されるためである. 境界線補正は特徴点が中央に特徴点が集まっているので既存方式と比較すると移動値に対して高いスコアを保っていることが分かる. またブロック数が増えるとブロックサイズが小さくなっていくので、早い段階でスコアが落ちている. 重心による補正は全ての特徴点と同じ値で移動しているため、スコアが一定になっている. 消失点が 0 の場合は重心により移動値が 0 の位置まで位置を戻しているため、高いスコアのまま一定になっている. 四隅削除の場合は 4 つのエリアの重心が全て影響を受けるため、0 の位置までは戻せずにスコアが低くなっている. ブロック数が増えた場合は移動値が小さい場合でも影響が出るため、四隅削除のスコアは大きく低下している.

提案方式の重心補正では 4 つのエリアの内 1 つでも消失がないエリアがあれば元の位置まで補正できるので 3 つの特徴点消失までなら確実に補正できるが、四隅を削除した場合など全てのエリアの重心がずれると完全には補正できなくなる. よって消失点が 4 個以上から増えていくと、認証スコアの低下とともに重心で元の位置に戻せる可能性が低くなっていく.

### ・本人—他人間認証

今回実験を行った 20 枚の画像の限りでは、本人—他人間認証の場合移動値によるスコアの変動はあまりなかった. 変化があった場合でも誤差の範囲内であった. ブロック数・方式の違いによるスコアの変動も本人—本人間認証と比較するとあまり変化はなかった.

## 6. まとめ

位置ずれに対して重心を補正する提案方式の実験を行い、既存方式と境界線補正方式との比較を行った. 既存方式と境界線補正方式は位置をずらしていくとスコアが下がったが、重心で元の位置に戻すことでスコアを一定に保つことができた.

今後の課題として消失点を増やしていったときに、エリアごとによる重心補正でどこまでスコアを保つことができるか、エリアごとの重心を選ぶときの先頭の数との関係はどう変化するかを実験する必要がある. 今回は位置ずれに対する実験しか行わなかったが、微小変化ノイズを考慮した場合の重心のズレ、スコアの変化も実験を行う必要がある. また対策として境界線補正との組み合わせなども考えられる.

**謝辞** 本報告作成のためにご協力頂いた岩村研究室の皆様、謹んで感謝の意を表する。

### 参考文献

- [1] 泉 昭年, 上繁 義史, 堀 良彰, 櫻井 幸一 “ブロックスクランブルに基づくキャンセラブルバイオメトリクス of 改善手法の評価” CSS2008 pp797-802
- [2] 泉 昭年, 上繁 義史, 堀 良彰, 櫻井 幸一” ブロックスクランブル方式に基づくキャンセラブルバイオメトリクスにおける境界線問題解決手法の実験・分析” SCIS 2009
- [3] 茂木優里, 吉田孝博, 和田直哉, 半谷精一郎 “指紋採取時の画像劣化要因と認証への影響に関する検討” SCIS2010
- [4] 清水 将吾, 瀬戸 洋一 “国際標準化に向けたテンプレート保護技術の体系化” 産業技術大学院大学紀要 No.1, pp.93-104 (2007)
- [5] NIST Fingerprint Image Software , 2010.“  
<http://fingerprint.nist.gov/NFIS/> ”
- [6] <http://bias.csr.unibo.it/fvc2004/download.asp>