

バイオメトリクス教科書

—原理からプログラミングまで—

映像情報メディア学会 編

工学博士 半谷 精一郎 編著

コロナ社

編著者・執筆者一覧

編著者

半谷精一郎（東京理科大学）

執筆者（執筆順）

半谷精一郎（東京理科大学，1，2章，5.1節）

瀬戸 洋一（産業技術大学院大学，3，7章）

吉田 孝博（東京理科大学，4.1節）

清水 孝一（北海道大学，4.2節）

鷺見 和彦（青山学院大学，4.3節）

市野 将嗣（電気通信大学，5.2節，6章）

（2012年5月現在）

ま え が き

近年、ネットワークを利用するビジネスが拡大し、セキュアな情報交換が普及しつつあるが、その前提となる本人認証のために、生体認証を意味する「バイオメトリクス」という言葉がキーワードとして用いられるようになってきた。バイオメトリクスとは、本来、生物学（biology）と尺度（metrics）という二つの言葉の合成語であり、本人しか持ちえない物理的な情報あるいは特徴のことである。したがって、こうした特徴を積極的に利用する生体認証は、今後、印鑑や暗証番号の代替情報として、現実世界で活動するうえでも、サイバー世界で活動するうえでも、必要不可欠な技術になることが予想される。

生体認証によるセキュリティシステムを導入するうえで、公共の利益を優先するのか、個人のプライバシーを優先するのかといった議論が聞かれる。しかし、少なくとも社会の安全が確保されなければ、個人のプライバシーも危うくなることは明らかである。このことは、わが国で発生した地下鉄サリン事件や米国で発生した同時多発テロのことを思い起こせば、十分理解できるであろう。以来、世界各国はバイオメトリクスに大きな注目と期待を寄せ、2002年に、ISOとIECの合同委員会であるJTC1（Joint Technical Committee 1）により関連技術の開発と標準化を担うSC（Subcommittee）が設置され、グローバルな生体認証セキュリティシステムの構築を目指して活動が開始されている。

この世界共通な生体認証セキュリティシステムは、同システムに準拠していると認定された機器であれば、すべての情報を標準化されたデータ形式で情報交換でき、容易にシステムを構築できるというもので、実世界あるいはサイバー世界の犯罪者が、国を越えネットワークを越えて活動することを抑制できる。そのため、世界各国においてバイオメトリクスに関する豊富な知識と経験を有する研究者や技術者の拡大が、安全な国家あるいは世界を構築するうえで

重要課題になってきている。

本書では、バイオメトリクス全般にわたる知識を平易に解説し、どのような原理によって身体情報が収集され、認証にまで至るのかを十分理解できるようにそれぞれのご専門の方々に執筆していただくこととした。特に、指紋、静脈、顔、署名、音声といったモダリティごとの特徴量がどのように抽出され利用されているかについては詳しく記述し、MATLAB に準拠したプログラム例も付録に付すことでアルゴリズムの理解を助けるように配慮したつもりである。したがって、初学者や学生のみならず、実際に生体認証に関わる技術者にとっても体系的に学べるものと自負している。

本書の構成は半谷が担当して決めたが、瀬戸洋一先生（産業技術大学院大学）にも多くのご助言をいただいた。もちろん、内容に関する責めは半谷が負うべきものであり、ご無理を申し上げたにも関わらず出版までこぎつけられたのは、各先生のご協力とご努力によるところが大きい。

なお、大学の15回の授業で本書を利用されるのであれば、基礎編の1章のモダリティの話を一回で、2章は信号処理とアルゴリズムなので実習を行いながら3回で、3章の精度評価に関しては2回程度に分けるとよい。また、応用・実践編の4章で指紋、静脈、顔を用いる具体的な認証系を3回で、5章の署名と音声による認証系を2回で、6章のマルチモーダルの考え方を1回で、7章のセキュリティに関わる考え方を2回で教授し、最後の1回でバイオメトリクスに関してまとめることで体系的に学べると考えている。各章末にある演習問題の解答は下記のホームページをご参照いただきたい。

最後に、本書の出版に際し、多くの労をとっていただいた映像情報メディア学会ならびにコロナ社の方々に心から謝意を表する次第である。

2012年4月

著者を代表して 半谷精一郎

付録のプログラムおよび演習問題の解答は以下のホームページに掲載した。

<http://www.ee.kagu.tus.ac.jp/lbu/profs/hangai/biometrics.html>

MATLAB を利用できる環境をお持ちの方は是非ともお試しいただきたい。

目 次

第 I 部 基 礎 編

1 ——— バイオメトリック認証 のためのモダリティ

1.1 身体的特徴の概要	3
1.2 行動的特徴の概要	4
1.3 市場規模	5

2 ——— バイオメトリック認証 のための信号処理

2.1 身体情報の採取から認証まで	7
2.2 代表的なセンサと動作原理	11
2.3 代表的な前処理	15
2.3.1 雑音除去処理	16
2.3.2 変換処理	19
2.4 特徴量間の距離と整合処理	25
2.4.1 特徴量間の距離	25
2.4.2 整合のための処理	30
2.5 判定処理	35
2.5.1 隠れマルコフモデルによる判定	36
2.5.2 ニューラルネットワーク	38
演習問題	39

3 — バイオメトリック認証システム における精度評価の方法

3.1 認証モデルと精度評価	40
3.1.1 認証モデル	40
3.1.2 精度の表現	41
3.1.3 Receiver Operating Curve	44
3.1.4 信頼度と対応率	45
3.2 精度評価ガイドライン	47
3.2.1 基本方針	47
3.2.2 評価対象の機能構成	47
3.2.3 被験者の構成と数	49
3.2.4 指紋収集条件	51
3.2.5 未対応	52
3.2.6 精度の表記	52
3.2.7 評価結果	52
3.3 精度評価ガイドラインと Best Practice	54
3.3.1 Best Practice の概要	54
3.3.2 精度評価ガイドラインと Best Practice の関係	55
演習問題	57

第Ⅱ部 応用・実践編

4 — 静的バイオメトリック認証系の実例

4.1 指紋認証	58
4.1.1 指紋認証の歴史	59
4.1.2 指紋と指紋特徴	60
4.1.3 指紋認証の形態	61

4.1.4	指紋認証システムの原理	62
4.1.5	指紋認証の脆弱性	77
4.1.6	指紋認証の応用事例	78
4.2	静脈認証	79
4.2.1	静脈認証の原理	79
4.2.2	各種静脈像の利用	85
4.2.3	静脈認証の技術	88
4.3	顔認証	96
4.3.1	顔認証技術の発展	96
4.3.2	顔画像認証の基本構成	101
4.3.3	顔画像認証における技術系統分類	103
4.3.4	顔画像認証における注意点	105
4.3.5	国家プロジェクトと商品化動向	106
	演習問題	108

5 — 動的バイOMETリック認証系の実例

5.1	署名認証	109
5.1.1	署名時に取得できる時系列データ	109
5.1.2	時系列データどうしの誤差量による認証方法	111
5.1.3	偽筆に対する耐性	116
5.1.4	今後の署名認証技術	118
5.2	話者認識	119
5.2.1	話者認識の歴史	120
5.2.2	話者認識方法の概要	120
5.2.3	話者認識の特微量	124
5.2.4	話者認識の認証方法	131
5.2.5	話者認識の認識アルゴリズム	132
5.2.6	まとめ	136
	演習問題	137

6——マルチモーダル生体認証

6.1 複数の身体情報の統合方法	138
6.2 マルチモーダル生体認証の特徴	140
6.3 マルチモーダル生体認証の統合手法	140
6.3.1 結果レベル統合—論理的手法	141
6.3.2 スコアレベル統合—統計的手法	143
6.3.3 スコアレベル統合—識別的手法	144
6.4 マルチモーダル生体認証の検討方針	145
6.5 マルチモーダル生体認証の例	146
6.5.1 使用するモダリティの選択	146
6.5.2 認証システム	147
6.6 マルチモーダル生体認証の課題	150
演習問題	151

7——セキュリティとプライバシー

7.1 バイオメトリクスとセキュリティ	152
7.2 バイオメトリック認証システムにおけるセキュリティ要件	155
7.2.1 バイオメトリックセキュリティとは	155
7.2.2 バイオメトリック認証システムの不正防止技術	160
7.2.3 セキュリティ強度	163
7.3 バイオメトリクスとプライバシー	165
7.3.1 バイオメトリック技術の受容性	165
7.3.2 プライバシー保護および影響評価	165
演習問題	167
付 録	169
引用・参考文献	178
索 引	188

第I部 基礎編

1 バイOMETリック認証 のためのモダリティ

人間のどのような特徴がどこまで一致していたら、その特徴は登録されている人間のものと同じであると認証できるのであろうか。少なくとも私たちの社会生活の中では、見覚えのある「顔」や聞いたことのある「声」だけで判断することがほとんどである。しかし、よく考えてみるとこんな曖昧な特徴だけで、相手を本人であると認め、話をし、金品の授受を行って大丈夫なのであろうか。そこには、記憶というもともと曖昧な情報だけで、短時間に本人認証するための知恵が働いている。つまり、最初は曖昧な状態で相手を本人と認めているが、相手との会話や断片的だった相手の顔の記憶をつなぎ合わせていくうちに推論を行い、最終的に確信に変えていく。言い換えれば、相手の顔の物理的な形状や音声の周波数成分の時間的な推移といった客観的な特徴の中で、主観的な特徴とみなした部分の記憶を利用することによって認証を行っているということである。

しかし、信用できない相手がたくさんいる世界を考えると、そうもいっていただけなくなる。例えば、見知らぬ土地に行き、写真を頼りに初対面の人と会ったならば、金品を渡したり、大切な情報を渡しても大丈夫なのだろうかと不安になる。ネットワークの向こう側にあるサイバー世界は、さらに危険な空間であり、このようなサイバー世界ではより厳密な客観的な尺度によって認証が行われるべきである。つまり、本人でなければ知りえないことや本人でなければ

2 1. バイオメトリック認証のためのモダリティ

持っていないもので紛失や忘却、盗難の危険性がより少ないものによって認証する必要がある。こうしたことから、記憶の中にある暗証番号やパスワード、そして本書で扱う生体の身体的特徴や行動的特徴を認証に用いることは、セキュリティ上、理にかなっている。

表 1.1 は、生体認証に用いられる特徴の大分類を意味するモダリティ (modality) とそのセンサ、抽出して認証に利用される特徴量 (feature)、認証に要するおおよその時間、認証誤差、人間にとっての受容性、導入経費、問題点などをまとめたものである。このうち、指紋、顔、虹彩、静脈、掌形、DNA といったモダリティは、個人を直接特定できる物理的な特徴であるために身体的特徴と呼ばれる。比較的認証誤差が小さく、経時変化が生じにくいことから、これらの特徴量を採取する多様なセンサや得られた特徴量を用いて認証するアルゴリズムが多数提案され、さまざまな分野で利用されている。これ

表 1.1 実用化されている生体認証技術

モダリティ	センサ	特徴量	認証時間	認証誤差	受容性	導入経費	問題点
指紋	静電容量形センサ 感圧式センサ 光学式センサ	画像そのもの マニキュア スケルトン	5秒以下	10^{-4}	中	安	異なる特徴量 間の互換性、 乾燥指、水濡 れの影響
顔	CCD カメラ	目鼻口の位置 髪の色、顔色	5秒以下	5~10% 程度	高	中	化粧、眼鏡、 照明の影響、 加齢、双生児
虹彩	CCD カメラ	瞳孔外側のア イリスコード	5秒以下	10^{-5}	中	高	まつ毛の影響 装置が大きい
静脈	赤外線を利用する CCD カメラ	手の平・指の 静脈パターン	5秒以下	10^{-5}	中	中	装置がやや大 きい
掌形	CCD カメラ	指の長さ、幅、 厚み、4本の 指の表面積	1秒以下	0.2% 程度	中	中	装置が大きい
DNA	DNA センサアレー	塩基配列	3時間	10^{-21}	低	高	コスト、時 間、倫理
音声	マイクロホン	フォルマント	5秒以下	2% 程度	高	安	体調、双生 児、経時変化
署名	タブレット	筆順、筆圧、 筆速	5秒以下	2% 程度	高	安	筋肉疲労 経時変化

に対し、音声や署名のようなモダリティは、何らかの行動に伴って現れる生成物から抽出した特徴であるために行動的特徴と呼ぶ。

例えば、音声は呼気で声帯を振動させた音という生成物であり、署名も筆記具を手に持ち複数の運動系を動かすことによって得られる生成物である。行動的特徴は、われわれ人間にとって採取されても心理的な負担が比較的少ない生体特徴ではあるが、採取時の環境の影響や生体固有の変化がつねに存在するために、身体的特徴を上回るほどの認証精度が得られず、実用化されている装置やシステムはかなり限定される。いずれにしても、どのモダリティも一長一短があり用途に応じた使い分けが必要である。

1.1 身体的特徴の概要

指紋は、当初はイギリスが中心となって犯罪捜査のために用いられてきたが、1980年ごろから米国でAFIS(Automatic Fingerprint Identification System)という自動化システムが利用されるようになり^{1)†}、その後、1985年頃から原子力発電施設などの重要施設の入退室管理システムとして利用されるようになった²⁾。現在では認証誤差が小さく導入経費も安くなったために、わが国をはじめ欧米でも幅広い分野で用いられている。例えば、携帯電話やコンピュータの使用開始時の認証³⁾、USBメモリ内の情報にアクセスするときの認証⁴⁾、マンションやビルへの住人の入退室管理⁵⁾、入出国管理のためのホームランドセキュリティシステム⁶⁾などがそれである。ただし、センサの特性上、皮膚の状態(水ぬれや乾燥)によって認証しにくいことがあり、センサを3次元に配置して指紋の測定精度を高める研究⁷⁾も行われている。

顔認証は、人にとって最も自然な個人認証方法で、空港などの防犯カメラからの画像を用いた監視⁸⁾や入国時のパスポートの顔画像データとの自動照合⁹⁾、入退室管理などに利用されている。ただし、化粧や眼鏡といった見掛けの変化や照明の当たり方の影響を受けやすいことから、近赤外光を使った顔画像取

† 肩付き数字は、巻末の引用・参考文献を表す。

得¹⁰⁾ や光源の位置を変えたときの顔画像取得によって認証精度を上げる試みもある¹¹⁾。

虹彩認証は、認証精度が高いことから高いセキュリティを必要とする入退室で利用されている。ただし、虹彩画像が低品質（まつげが入るなど）になると認証率が低下するため、特徴点の検出と特徴量の記述を行う SIFT (Scale-Invariant Feature Transform) を利用した研究が行われている¹²⁾。カメラの撮影能力を高めることで空港や路上といった公共の場所で認証し、施設や地域のセキュリティに役立てる試みもある¹³⁾。

静脈認証は、血液中のヘモグロビンが近赤外光を通しにくいことを利用して血管パターンを撮影し、その特徴量を用いて認証する方法で、手の平の中の静脈を用いる方式¹⁴⁾ と指の中の静脈を用いる方式¹⁵⁾ がある。2004 年から、ATM 利用時の本人認証手段として導入され²⁾、ほかにも製造系システム、データセンタなどの入退出管理システム¹⁶⁾、情報系の PC ログオンシステム¹⁷⁾ での本人認証に利用され、国際的な市場拡大に一役買っている。

掌形認証は 1993 年ごろから米国で INSPASS (Immigration and Naturalization Service Passenger Accelerated Service System)¹⁸⁾ の登録者に対する入国許可のために採用されていた。装置の決められた位置に手を置き、指の長さや甲の高さといった物理量をもとに認識するもので、きわめて少ないデータサイズ (9 バイト) で認証できる¹⁾ が、わが国ではあまり利用されていない。

DNA 認証では認証時間や導入経費の問題とともに人間の遺伝的な情報を扱うことから、犯罪捜査などではよいが、一般用途に至るまでには今後セキュリティ上の問題のほか、倫理面での問題も解決する必要がある¹⁸⁾。

1.2 行動的特徴の概要

音声による個人認証は、声道の物理的な形状によって決まる共振周波数に着目した方法で、テレホンバンキングにおける認証¹⁹⁾ や通常の鍵を忘れてしまったときのマンションへ入館の際に、第二の鍵として利用されている²⁰⁾。特徴量

である声道の共振周波数の時間的変化が必ずしも安定でないことから、本人の間でも変動が大きく、用途が限定される。ただし、自然かつ非接触で音声を採用できることから心理的な負担は少ない。

署名による個人認証は、紙に書かれた署名どうしを比較するオフライン署名認証²¹⁾とタブレットと呼ばれる署名時の時系列を採取する装置で得たデータを利用するオンライン署名認証²²⁾とに分類される。音声同様、毎回の署名から抽出される特徴量が本人のものであっても安定しないことから、用途が限定される。社内の電子決済²³⁾などで実用化されている。

1.3 市場規模

世界の生体認証に関する市場規模の2009年のIBG（International Biometric Group）による報告書²⁴⁾によると、AFISのような犯罪捜査目的を含む指紋認証システムが66.7%を占め、次いで顔認証が11.4%、虹彩認証が5.1%、音声認証が3.0%、静脈認証が2.4%、掌形認証が1.8%、ミドルウェア・その他が9.6%となっている。図1.1は2009年から2014年にかけての世界のバイオメトリクス市場の規模（予測を含む）を表したもので、34億2230万ドルから93億6850万ドルに拡大するとしている。

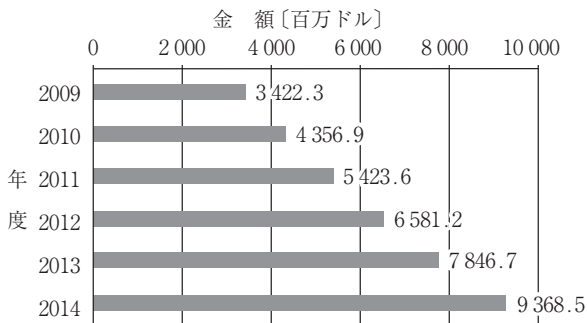


図1.1 世界のバイオメトリクス市場（金額ベース）

図 1.2 は、わが国の生体認証に関わるマーケットの 2009 年から 2014 年の市場拡大の様子（予測を含む）を示したものであるが、世界の市場の増加率と比べると鈍化していることがわかる。

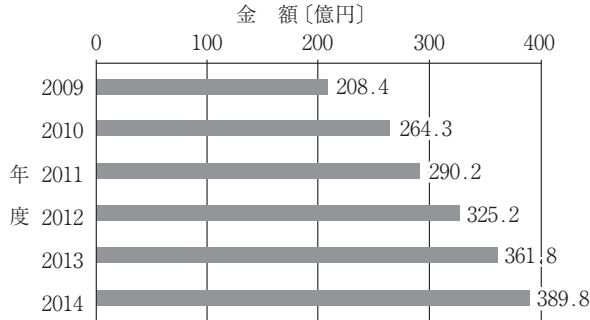


図 1.2 日本のバイオメトリクス市場（金額ベース）

一方、わが国の調査機関によると²⁵⁾、2009 年におけるわが国のバイオメトリクス市場は 208 億円で、2010 年度 264 億円、2011 年度予測 290 億円と成長してきているが、伸び率は鈍化している。その大きな理由は、静脈認証系の市場が 2009 年の 115 億円から 2010 年に 167 億円、2011 年予測で 198 億円と伸びているものの、指紋認証装置は単価が低くなりつつあるために、数量は伸びても市場拡大につながっていない。

2010 年度における、わが国のモダリティ別の市場は、数量ベースでみると、指紋認証が 57.9% を占め、次いで署名認証が 10.6%、静脈認証が 8.1%、顔認証が 5.9%、音声認証が 5.0%、虹彩認証が 0.01%、掌形認証が 0.01% となっている。ただし、金額ベースでみると、静脈認証が 63.2% を占め、次いで指紋認証が 30.0%、顔認証が 3.3%、音声認証が 1.1%、署名認証が 0.8%、虹彩認証が 0.2%、掌形認証 0.2% であり、静脈認証の占める割合が圧倒的に多い。

索 引

<p>【い】</p> <p>位置ずれ 91</p> <p>位置ずれ補正 90, 91</p> <p>1対1照合 61</p> <p>1対N照合 61</p> <p>イメージインテンシ ファイア 80</p> <p>イメージセンサ 12</p> <p>【え】</p> <p>永続性 85</p> <p>【か】</p> <p>回 転 30</p> <p>開放型 89, 90</p> <p>ガウス分布 134</p> <p>顔画像認証 96</p> <p>顔姿勢 104</p> <p>拡 大 30</p> <p>隠れマルコフモデル 36</p> <p>可視光 79</p> <p>画像アーティファクト 94</p> <p>画像相関 90</p> <p>仮想部分空間法 101</p> <p>画像ゆがみ 95</p> <p>カーネル判別分析 148</p> <p>感圧方式 66</p> <p>完全非接触型 86</p> <p>眼底血管像 86</p> <p>眼底撮影 85</p> <p>感熱式 66</p>	<p>【き】</p> <p>幾何学的特徴モデル 96</p> <p>基準データ 152</p> <p>偽 筆 116</p> <p>偽マニューシャ 73</p> <p>キャンセルラブルバイオ メトリクス 153, 162</p> <p>近赤外光 79, 80</p> <p>【く】</p> <p>空間周波数 20</p> <p>空間分解能 82</p> <p>クライアント認証モデル 10</p> <p>【け】</p> <p>結果レベル統合 141</p> <p>血管像のゆがみ 91</p> <p>ケプストラム 123</p> <p>【こ】</p> <p>コ ア 61</p> <p>光学式 64</p> <p>虹彩認証 85</p> <p>高 度 111</p> <p>光透視 79</p> <p>行動的特徴 3</p> <p>硬判定 36</p> <p>後方散乱光 82</p> <p>固有顔 99</p> <p>固有ベクトル 29</p> <p>コンデンサ型マイクロホン 14</p> <p>コントラスト 82</p>	<p>【さ】</p> <p>最近傍法 31</p> <p>撮影方式 81</p> <p>サーバ認証モデル 10</p> <p>3次元形状計測 97</p> <p>酸素化ヘモグロビン 83</p> <p>【し】</p> <p>しきい値 42</p> <p>色相成分 23</p> <p>識 別 122</p> <p>識別器 122, 140</p> <p>識別辞書 100</p> <p>識別的手法 144</p> <p>時系列データ 109</p> <p>指紋画像の品質 66</p> <p>指紋照合 67</p> <p>指紋スキャナ 63</p> <p>指紋特徴点への総当たり 攻撃 164</p> <p>指紋認証システム 62</p> <p>指紋の特徴点 61</p> <p>シャープネス 82</p> <p>重 心 28</p> <p>周波数解析方式 69</p> <p>縮 小 30</p> <p>主 軸 28</p> <p>主成分得点 28</p> <p>出入国管理 78</p> <p>手部静脈像 86</p> <p>照合プロセス 102</p> <p>上方開放型 89</p> <p>静脈認証 79</p>
--	---	--

掌 紋	87	谷 線	60	取り消し可能な	
署 名	109	他人受入誤差	43	バイオメトリクス	162
人工指	77	他人受入率		トロイの木馬	157
伸縮曲線	113		43, 46, 50, 116		
身体的特徴	2	ダービン法	127	【な】	
シンボル発生確率	36	弾性グラフマッチング	99	ナイキスト周波数	19, 21
信頼度	45	端 点	61	なぞり偽筆	116
				成りすまし	153, 160
【す】		【ち】		【に】	
スコアレベル統合	141	チップマッチング方式	69	2次元特徴量	26
スニッフィング	157	チャレンジコード	161	ニューラルネットワーク	
スペクトル包絡	125	チャレンジレスポンス		モデル	38
		方式	161	認 証	47
【せ】		【て】		認証精度	46
正弦波グレーティング	17	テキスト依存型	120, 131	認証モデル	40
整合窓	35	テキスト指定型	132		
脆弱性	77	テキスト独立型	120, 132	【は】	
生体検知技術	153, 158	デルタ	61	バイオメトリック	
静電容量	13	電界強度方式	65	システムセキュリティ	155
静電容量方式	65	電子透かし埋め込み	161	バイオメトリック	
精 度	41	電子パスポート	79	セキュリティ	155
精度評価ガイドライン		電磁誘導	15	バイオメトリック	
	47, 54	テンプレート		認証モデル	40
精度評価フォーム	52		7, 96, 120, 156	バイキュービック法	31
セキュリティ強度	163	【と】		排他的論理和	30
線形伸縮	33	等誤り率	116	バイリニア法	31
線形判別分析	148	同一性の判定	154	パスワードモデル	40
線形予測分析	127	透過型	89	パターンマッチング方式	68
		透過型撮影	88	波長選択	83
【そ】		透過方式	81, 89, 90	バックプロパゲーション法	
総当り攻撃	163	統計的手法	143		39
相互部分空間	100	統計のパターン照合	98	ハミング距離	29
ソフトバイオメトリクス	150	登録プロセス	102	反射型	89
		特徴抽出	122	反射型撮影法	86
【た】		特徴点処理	88	反射方式	81, 89, 90
第一主成分	29	特徴ベクトル	103	判定処理	35
対応率	45, 52	特徴量	2, 25, 104		
ダイナミック型マイクロ		特徴量範囲	104	【ひ】	
ホン	14	特徴レベル統合	141	比較アルゴリズム	104
タイプIエラー	43			微細構造	125
タイプIIエラー	43				

ヒストグラム	24	本人認証	40		
非線形伸縮	34			【ゆ】	
筆 圧	109	【ま】		唯一性	85
筆 跡	109	前処理	122	ユークリッド距離	8, 25
標準化周波数	19	マッチング処理	88	指静脈像	87
		マニユーシャ	8, 61	指内散乱光センサ	65
【ふ】		マニユーシャの品質値	74	指表面反射光センサ	64
フィルタリング	16	マニユーシャマッチング		【よ】	
フォトダイオード	12	方式	67	横照射方式	81, 82
部分テンプレート		マニユーシャリレーション		【ら】	
	92, 93, 94	方式	68	ラグランジェ補間	33
部分テンプレート法		マハラノビス二乗距離	26	【り】	
	92, 93, 94	マルチアルゴリズム	139	離散コサイン変換	22
普遍性	85	マルチインスタンス	139	離散フーリエ変換	19
プライバシー	165	マルチサンプル	139	リプレイアタック	156
プライバシー影響評価	166	マルチセンサ	139	隆 線	60
プライバシー保護	165	マルチモーダル	139, 154	【る】	
分岐点	61	マルチモーダル認証	95	類似度	42, 93
		【み】		【ろ】	
【へ】		未対応	45, 52	論理的手法	141
平均攻撃空間	163	見まね偽筆	116	【わ】	
平行移動	30	【め】		話者識別	120
ペンタブレット	15	メルケプストラム係数	127	話者照合	120
ペンの傾き	109	【も】		話者認識	119
【ほ】		網膜静脈像	85		
方位角	111	網膜認証	85		
本人拒否誤差	42	モダリティ	2, 104, 138		
本人拒否率	42, 46, 50, 115				

【A】		BOZORTH3	74	【D】	
AFIS	3	【C】		DCT 係数	22
【B】		CCD	12	DP マッチング	34
Baum-Welch		CELP	131	d-prime	43
アルゴリズム	134	CMOS	12	DTW	35, 112
Best Practice	54	Compact フォーマット	119	【E】	
biological window	80	Compressed		EER	116
		フォーマット	119		

Eigenface 98	LSP 129	
EM アルゴリズム 135		【S】
【F】	【M】	Scenario 評価 54
FAR 9, 43, 116	MFCC 127	SIFT 4
FERET 106	MINDTCT 70	Sum Rule 143
FRGC2006 107	【N】	【T】
FRR 9, 42, 115	NBIS 70	Technology 評価 54
FRVT2000, 2002 107	NIST 70, 107	【V】
Full フォーマット 118	NNM 38	Viterbi アルゴリズム 134
【G】	【O】	【Y】
GMM 120	Operational 評価 54	yC_bC_r 信号 23
【H】	【P】	【数字】
HMM 36, 120	Product Rule 143	19794-7 118
【I】	【R】	19794-11 119
INSPASS 4	rgb 空間 22	
【L】	rgb 信号 23	
LPC ケプストラム 125	ROC 9, 44, 52	

— 編 著 者 略 歴 —

- 1975年 東京理科大学工学部電気工学科卒業
1981年 東京理科大学大学院博士課程修了(理工学研究科電気工学専攻)
工学博士(東京理科大学)
1981年 東京理科大学助手
1987年 東京理科大学講師
1991年 東京理科大学助教授
1996年 スタンフォード大学客員研究員(1年間)
2001年 東京理科大学教授
現在に至る

バイオメトリクス教科書—原理からプログラミングまで—

A Textbook of Biometrics

©一般社団法人 映像情報メディア学会 2012

2012年7月6日 初版第1刷発行

検印省略

編 者 一般社団法人
映像情報メディア学会
編 著 者 半 谷 精 一 郎
はん がい せい いち ろう
発 行 者 株式会社 コロナ社
代 表 者 牛 来 真 也
印 刷 所 萩原印刷株式会社

112-0011 東京都文京区千石 4-46-10

発行所 株式会社 コロナ社

CORONA PUBLISHING CO., LTD.

Tokyo Japan

振替 00140-8-14844・電話(03)3941-3131(代)

ホームページ <http://www.coronasha.co.jp>

ISBN 978-4-339-00835-7 (高橋) (製本:愛千製本所)

Printed in Japan



本書のコピー、スキャン、デジタル化等の無断複製・転載は著作権法上での例外を除き禁じられております。購入者以外の第三者による本書の電子データ化及び電子書籍化は、いかなる場合も認めておりません。

落丁・乱丁本はお取替えいたします