

第2章

バイオメトリクス認証の動向と周波数解析法

指紋/顔パターン認識アルゴリズム

吉嶺 達樹

本章では、バイオメトリクス認証の大まかな概要を紹介する。特に指紋の認証について、センシング方式と指紋認証アルゴリズムの概要を紹介する。その中でも、特に周波数解析法について概要と応用製品を紹介する。また、Appendixでは、同じく周波数解析法を用いた顔認証について、技術および製品の紹介を行う。

(編集部)

バイオメトリクス認証の動向

指紋パターンの認識アルゴリズムについて紹介する前に、近年のバイオメトリクス認証の動向について説明します。

● 個人情報保護法の施行によりバイオメトリクス認証が注目される

近年のコンピュータ技術の進歩により、企業は顧客情報をデータベース化し、効率的に業務利用する傾向にあります。そのため、私達はさまざまな場面で、企業に個人情報を教えています。このようにして収集される個人情報は、氏名、住所、電話番号、性別にとどまらず、年齢、家族構成、年収、趣味趣向、クレジット・カードの番号など、多種多様におよびます。

企業を信頼して、もしくは必要に迫られて教えている個人情報ですが、最近ではこれら個人情報の流出問題が世間を賑わせています。

デジタル・データとしてデータベース化された個人情報は、紙に記録されたものよりも複写が容易であり、ネットワーク経由や小型記録媒体へのコピーという形で、比較的容易に外部持

ち出しが可能です。加えて、情報を扱うオペレータの「個人情報を持っている」という意識の不足や、情報を持ち出しても犯人がなかなか特定できないという情報管理システムの甘さなどがあります。

この事態を解決する方法の一つとして、身体的な特徴/特性など、個人に固有の情報を利用して、本人の確認を行う認証方式である、バイオメトリクス認証が脚光を浴びてきました(表1)。

データを扱うときの「鍵」としてバイオメトリクスによる認証を用いることにより、権限を持ったオペレータ以外はデータにアクセスできない強固なセキュリティが実現できます。さらに、生体認証の隠れたメリットとして、認証を行っているオペレータに対してセキュリティの重要性を啓蒙できるという点が挙げられます。つまり、バイオメトリクス認証装置を別途用意してオペレータに使わせることで、「このような装置・操作を必要とする重要な情報を扱っている」と意識させることができます。

また、認証時に操作状況および認証結果をログに記録し、「すべての操作は後で必ずチェックされている」と意識させることで、特に最近増加している内部犯罪への抑止効果が期待できます。

2005年4月より「個人情報保護法^{注1}」が施行されるということもあり、個人情報を扱う多くの企業や公官庁では、バイオメトリクス認証による個人情報保護対策が急速に進められています。

● 利便性の向上——パスワード入力よりは簡単

バイオメトリクス認証を導入すると、先に述べた個人情報保護以外にも、大きな利点があります。

それは、機器の操作・運用が簡単になるということです。コンピュータへのログインやデータ保護には、パスワードが用いられていますが、これをバイオメトリクス認証で代用したとしましょう。

パスワードに代えてバイオメトリクス認証を用いることで、

表1 バイオメトリクス認証の種類

種 類	概 要
指紋	指紋を利用した認証方法
虹彩	瞳孔の薄膜組織模様を利用した認証方法
顔	顔を利用した認証方法
掌形	掌の幅、長さ、厚さなどの形状を利用した認証方法
声	音声(声紋)を利用した認証方法
署名	筆跡、筆圧、書き順、リズムなどを利用した認証方法
網膜	網膜上の血管パターンを利用した認証方法
静脈	手のひらや指の静脈パターンを利用した認証方法

注1：個人情報保護法：個人の権利と利益を保護するために、個人情報を取得して取り扱っている事業者に対し、さまざまな義務と対応を定めた法律。この法律によって、従来は「企業の財産」、「営業機密事項」として扱われてきた「顧客情報」に、「個人情報」という認識が加えられ、情報を収集した企業であっても、その情報を「企業の財産」として自由に扱うことが禁じられる。



図1 指紋認証機能が搭載されたパソコン



図2 Windows用指紋認証ユニット
UBF((株)ディー・ディー・エス)

指紋認証ユニット UB-P010



図3 指紋認証が搭載されている携帯電話 (NTT ドコモ)

パスワードを覚えられない→単純なパスワードをつい使ってしまう→第三者に容易に推定される→セキュリティを破られる、という負の連鎖を断ち切ることができます。

また、ユーザにとっても、覚えにくい文字列(パスワード)を定期的に変更するという負担から解消されます。記憶する手間、入力する手間、管理する手間などから解放されるのです。

最近では、上記の機能を網羅した「指紋認証機能搭載ノート・パソコン」が発売されています。これらのノート・パソコンは、おもに企業ユーザ向けに発売されていますが、次第に一般にも普及しつつあります(図1)。(株)ディー・ディー・エスから発売されている Windows 用指紋認証ソリューションである UBF は、Windows2000/XP のログオン、スクリーン・セーバからのロック解除をパスワード認証に代わり指紋認証で行うことができます。ブラウザ中のパスワード入力を、指紋認証で代替する機能もあります(図2)。

また、NTT ドコモから発売されている携帯電話の中には、F901iC のように指紋センサが搭載されているモデルがあります(図3)。電話帳やメール、発着信履歴などの他人に見られたくないデータを、指紋認証によって保護することができます。もちろん、従来どおりのパスワードでも保護できますが、指紋認証を利用することで、パスワードを入力する煩雑な操作から解

放され、かつパスワード入力を覗き見られる不安からも解放されます。番号を入力するより、指をセンサの上で滑らせるという簡単な操作で良いのです。

バイオメトリクスによる認証、特に指紋認証は、このような背景と技術進歩によって、すでに世間に広く浸透し始めているのです。

指紋センサの種類

指紋認証を行うには、指紋センサと呼ばれる“指紋の隆線を読み取るセンサ”が必要です。このセンサから得られる情報は、“指の表面の凹凸”を“二次元のデジタル画像データ”に変換したものです^{注2}。

指紋センサは、センサの原理による区別と、センシング・エリアの大きさ・形状による区別が可能です。

● センサの原理による区別

センサの原理としては、昔前はコピー機の原理にも似た光学式が主流でしたが、現在ではさまざまな方式の指紋センサが登場しています。以下に、主要な5方式について解説します。

▶ 光学式

指の表面に光を照射あるいは走査し、指表面の凹凸に対応して生じる反射光の強弱を CCD などの光電変換素子を利用して

注2：指紋センサの中には、指の表面ではなく内部(真皮)の凹凸を読み取るものもある。

画像化する方式です。良好な画像を撮像するために、プリズムなどの光学系を必要とします。

▶ 静電容量式

シリコン・チップ上に微小電極を二次元に配置し、それぞれを指の皮膚との間のコンデンサとして利用します。これらコンデンサにそれぞれ微小電流を流し、そのときに生じる電位差を測定して画像化する方式です。

▶ 電界式

シリコン・チップ・センサの周囲にマイナス極のガイドを設置し、指を置いたときにガイドに触れるような構造にします。センサ上に置かれた指の皮膚内部に、マイナス極から電子を流入させます。それにより、指先とシリコン・チップ・センサの間に発生する電界の強弱を画像化する方式です。

▶ 感熱式

温度により抵抗値が変化する微小な温度センサを二次元に配置します。センサに指が触れた部分のセンサ素子から熱が逃げる、あるいは体温の熱が伝わることにより発生する温度差を抵抗値の変化として検出し、画像化する方式です。

▶ 感圧式

圧力により抵抗値が変化する微小な半導体センサを二次元に配置します。その上に置かれた指表面の凹凸によって生じるセンサにかかる圧力の違いを電位差として取り出し、それを画像化する方式です。

各方式ともそれぞれに、長所・短所があるため、指紋認証機能を組み込む最終製品に合わせて選択することが必要です。

● センシング・エリアの大きさ・形状による区別

指紋を読み取る領域(センシング・エリア)が正方形に近いも

のをエリア・センサ、細長い長方形をしている物をライン・センサと呼びます。

どちらの指紋センサも指紋の隆線を読み取りますが、入力時の操作方法が異なります。

エリア・センサの場合は、拇印を押すときの要領でセンサ面に指を押し付けます。ライン・センサの場合は、センサ長手方向に直交するように指を滑らせます。

エリア・センサからは1回の押印で指紋全体の画像が得られますが、ライン・センサでは短冊状の細長い画像しか得られません(図4)。

ライン・センサから得られる短冊状の指紋画像は、高さが1mmにも満たない範囲をキャプチャしたものです。よって、縦方向は数ラインしかない、細長い画像となります。しかし、この画像を連続して採取し、各画像間で重なっている部分を検出、重ね合わせていくことで、指紋の全体像を得ることができま^{注3}。

こうして得られた指紋画像は、時にはエリア・センサよりも広範囲の指紋画像となります(図5)。

指紋認証ソフトウェア

● 指紋認証ソフトウェアの機能構成

指紋認証を実現しているソフトウェアは、大きく五つの機能から構成されています(図6)。

▶ 指紋取得部

前節で記した、指紋センサを用いて指紋画像を採取する部分です。システムが採用している指紋センサとアルゴリズムの種類によっては、指紋の全体像を得るための指紋再構成処理が必要となる場合があります。

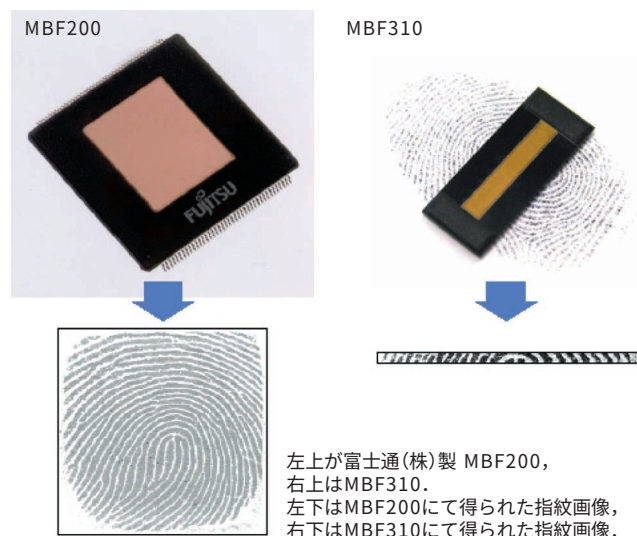


図4 エリア・センサとライン・センサ

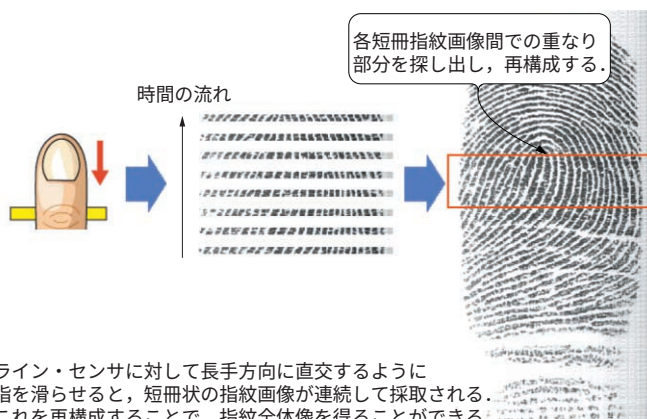


図5 短冊画像から指紋の全体像を得る

注3：ライン・センサから得られた短冊状の指紋画像を用いて指紋の全体像を再構成し、メモリ上に指紋全体のイメージを持つ技術は、ATMEL 社が特許申請している。日本では特許審査中だが、ATMEL 社以外の指紋センサを使用する場合には、注意が必要。DDS 社製の指紋認証ライブラリ UB-safe は、アルゴリズムに指紋の全体像が不要な技術を採用することにより同社の特許侵害を防いでいる。

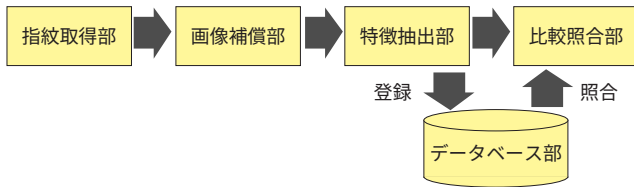


図6 指紋認証システムの構成

▶ 画像補償部

入力された指紋画像を、各種アルゴリズムに適した画像に変換する部分です。さまざまな種類の画像フィルタが開発されています。

▶ 特徴抽出部

画像処理を施された指紋画像から、「個」を表す特徴を抽出する部分です。抽出された特徴データは「指紋テンプレート」と呼ばれています。指紋認証を行うには、照合対象となる各ユーザの指紋テンプレートを、あらかじめ登録しておく必要があります。

▶ データベース部

登録時に抽出された指紋テンプレートを、保存しておく部分です。

▶ 比較照合部

データベース部に登録された指紋テンプレートと、照合のために入力された指紋テンプレートのマッチング処理を行う部分です。これにより登録時と同一指か否かを判定します。

登録した時点とまったく同じ指紋が入力されることはありませんので、マッチングする際にある程度の許容誤差をもたせる必要があります。

ただし、許容誤差を大きくすると認証性能が低下します。逆に認証性能を高めると、許容誤差が少なくなります。すなわちこの二つはトレードオフの関係にあります。

● 指紋認証ソフトウェアの性能評価

認証性能を測るための指紋認証のしくみについて説明します。指紋は万人不同、終生不変の二つの大きな特徴を持つといわれています。しかし、指紋を採取する対象が生体であるために同一人物の同一指であっても、指紋採取ごとに得られる紋様は微妙に異なります。この微妙な違いを吸収して、登録された指紋と他人の指紋を区別することが、指紋認証システムに求められるもっとも基本的な要求です。

各種指紋認証アルゴリズムは、その手法こそ異なりますが、登録される指紋を指紋テンプレートへと数値化し、かつ入力された指紋を照合用の指紋テンプレートへと数値化し、さらにこれら二つの指紋テンプレートの類似度を数値で表現するという点では同じです。

数値化された類似度は、同一指の指紋テンプレート間では小さな値を示し、異なる指の指紋テンプレート間では大きな値となります。これら同一指どうし・異なる指どうしの類似度の分布例を、図7に示します。

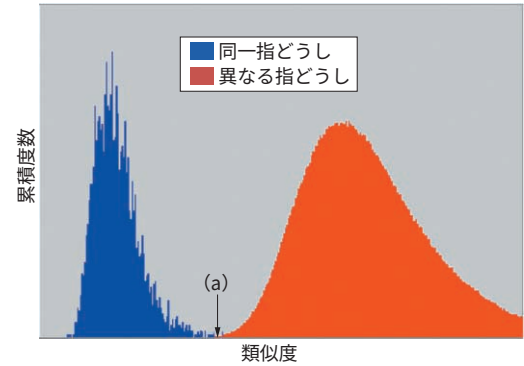
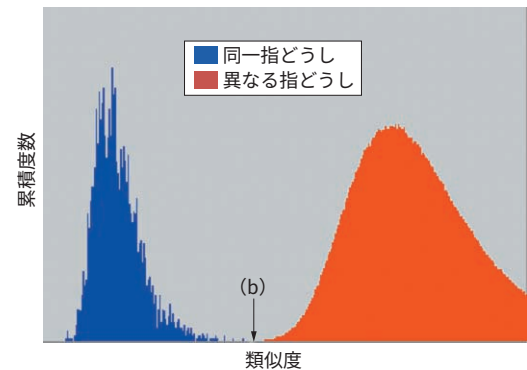


図7 指紋の類似度分布



しきい値を(b)近辺に設定すると、それぞれの分布を完全に分離できる。このようなシステムでは、誤照合は発生しない。

図8 理想的な類似度分布

同一の指か、異なる指かの判断は、しきい値を図7の(a)近辺に設定し、得られた類似度が(a)より小さければ同一指、大きければ異なる指と判断します。しかし、図7では、それぞれの分布に重なりがあります。この重なりにより、誤照合が発生します。

誤照合とは、登録されている指紋を入力しても認証が拒否される、または登録されている指紋と異なる指紋で認証してしまうことです。これらは一般的に、本人拒否率(FRR : False Rejection Rate)、他人受入率(FAR : False Acceptance Rate)という二つの指標によって表されており、これは指紋認証アルゴリズムの性能を表す指標にもなっています。

図7に示された二つの分布が重ならないければ誤照合は発生しないのですが、この二つを完全に分離する手法は存在しません。いかにして分布の重なりを減らすか＝誤照合をなくすかが、指紋認証アルゴリズムの最大の研究テーマであるといえます(図8)。

指紋認証アルゴリズム

代表的な指紋認証のアルゴリズムには、以下の3種類があります。

- パターン・マッチング方式
- 特徴点(マニューシャ)方式

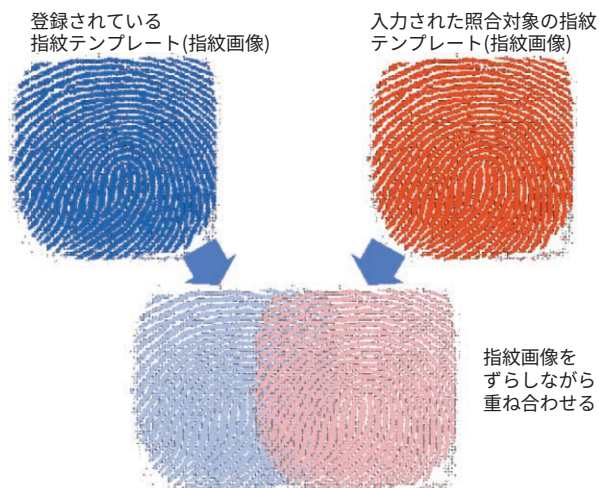


図9 パターン・マッチング方式の照合イメージ

● 周波数解析方式

以下に、各アルゴリズムの処理概要を解説します。

● パターン・マッチング方式

テレビの刑事ドラマなどで見かける、2枚の指紋画像を重ね合わせて照合する方法です。

登録された指紋画像と入力された指紋画像をずらしながら類似度を算出する方式は比較的高速に処理が可能ですが、指の経時変化など指紋画像の局所的な変形に弱いという問題があります。

また、指紋画像そのものを指紋テンプレートとして保存するため、指紋テンプレートのサイズが大きくなりすぎたり、プライバシーの問題がある、という欠点があります。パターン・マッチング方式をシステムとして採用する場合は、これらの問題を解消するためにデータ圧縮・データ暗号化などの要素技術と組み合わせる必要があります(図9)。

● 特徴点(マニューシャ)方式

指紋認証アルゴリズムでは、多くのベンダが採用している方法です。

マニューシャ方式は、指紋の隆線における端点や分岐点(特徴点)などの属性とそれらの相対的な位置関係を特徴データとして登録・照合を行う方法です(図10、図11)。

この方式は、マニューシャを抽出するまでの画像補償部と特徴抽出部の処理に時間がかかりますが、指紋テンプレートのサイズが小さいという利点があります(図12)。

さらに、マニューシャの情報に加えてマニューシャ間を横切る隆線の数を特徴として捕らえ、照合精度を向上させた「マニューシャ・リレーション方式」(図13)や、検出されたマニューシャ周辺の画像を特徴として登録し、パターン・マッチングを行う「チップ・マッチング方式」もあります(図14)。

● 周波数解析方式

周波数解析方式は、指紋テンプレートを抽出するアルゴリズム

図10
マニューシャについて

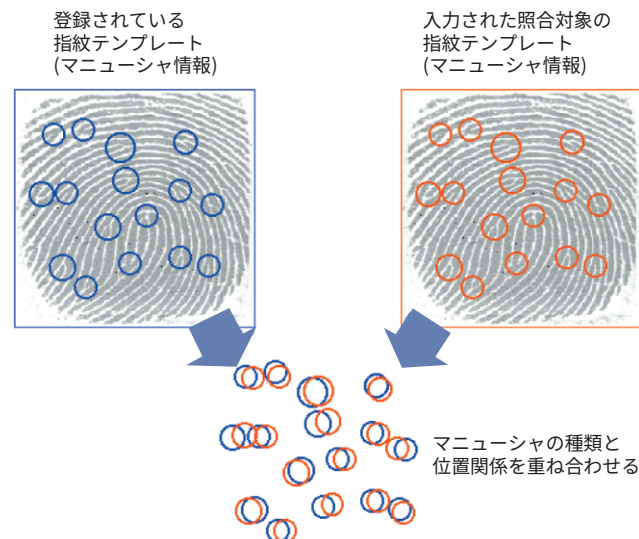


図11 マニューシャ方式の照合イメージ

と、抽出されたテンプレートを登録テンプレートと比較するアルゴリズムの二つによって構成されています。

▶ 指紋テンプレート抽出方法

周波数解析方式は指紋画像を短冊状にスライスし、スライスした画像(波形)ごとに紋様のスペクトル解析を行う方式です。

図15に、指紋画像を横方向に切り出した例を示します。横方向に指紋の位置を、縦方向に指紋の凹凸(画像の濃淡)をとると、切り出された指紋画像は1ラインの波形とみなすことができます。この波形を解析することにより、ラインごとのDFTスペクトルを得ることができます。周波数解析方法は、このDFTスペクトル群をさらに演算し、元情報の1/20～1/30まで圧縮した情報を指紋テンプレートとして登録します(図16)。

実際のプログラムでは、処理の高速化のため、パワー・スペクトルの近似値を求めるなどの改良を行います。

この手法における周波数解析処理では、手荒れや磨耗が原因でマニューシャが少ない指でも登録できるという特徴があります(図17)。

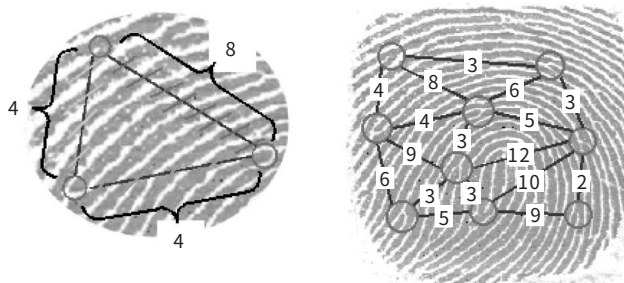
▶ 指紋テンプレートのマッチング方法

前述したテンプレート抽出方法により得られた指紋テンプレートを、登録済みの指紋テンプレートと比較し、その類似度を算出できなければ、指紋認証ができません。

マニューシャ抽出を行うまでに必要な画像処理例。 左から順に処理されていく。



図12 マニューシャ法の画像処理例



マニューシャ間を横切る隆線の数も特徴として利用する

図13 マニューシャ・リレーション方式

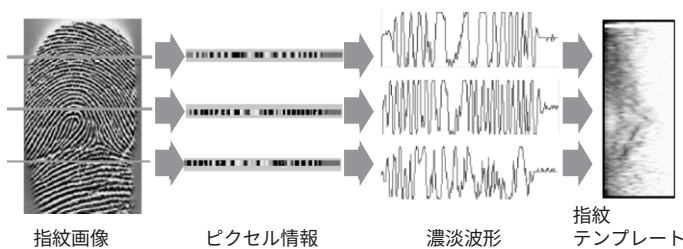


図15 指紋画像の濃淡波形と、周波数解析方法による特徴抽出の関係

パワー・スペクトルとして得られる指紋の特徴は、指紋の入力状態によって微妙に変化するため、単純に比較することができません。

図18、図19は、データ系列“ABCDEF”と“ABCCDEF”の比較を示したものです。この二つのデータ系列は、主観的にはかなり類似しています。しかし、単純に先頭から比較していくと、図18のように類似度は低いと判定されてしまいます。この問題を解決するためには、図19のような比較を行う必要があります。

この比較方法は、音声認識の分野などで広く知られているパターン・マッチング手法の一つ、DP マッチング (DP :



図14 チップ・マッチング方式

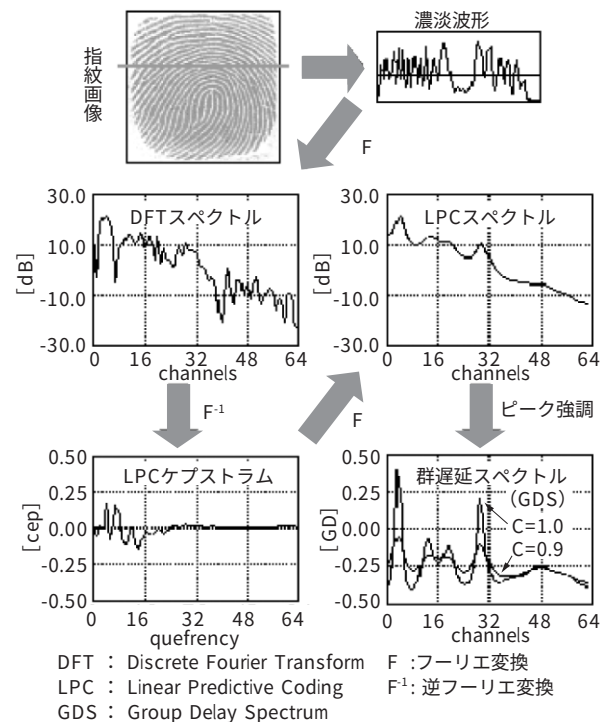


図16 周波数解析法の特徴抽出処理 (文献1)

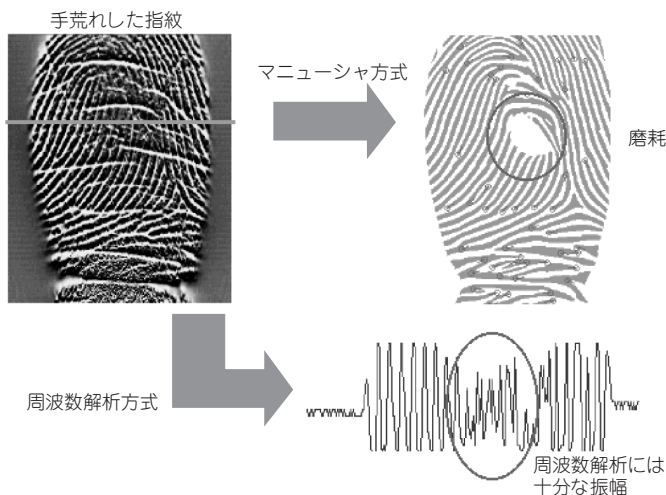


図17 磨耗した指紋におけるマニューシャ方式と周波数解析方式の特徴抽出の違い

Dynamic Programming)を使用することで実現できます。これにより、時系列長(指紋の長さ)が異なる場合、ずれを吸収して類似度を計算することが可能となるのです。

▶ 応用アルゴリズム

周波数解析方法を応用したアルゴリズムとして、カシオ計算機(株)が独自に開発した指紋認証アルゴリズム VeriPat があります。

このアルゴリズムは、指紋に現われる曲線の曲率と線間隔を解析し、照合には二つの指紋データの二次元スペクトル・データの解析を行います。同一指紋の場合にはスペクトルは一致し、線間隔は互いに同じになります。この解析を一つの指紋に対し、数か所で行い、局所的データの相対的配置を合否判定に使用します。

▶ 周波数解析方法を採用した製品

周波数解析法は、そのアルゴリズムから、「処理速度が一定」、「計算の近似により、高速化が可能」、「原則として、登録拒否が発生しない」などの特徴があります。ディー・ディー・エス製の指紋認証エンジンである UB-safe は、これらの特徴を最大限に活かした指紋認証エンジンです。

韓国 Pantech 社の ARM7 を搭載した GSM 携帯にも採用されており、1 対 1 認証時の速度は 0.62 秒とたいへん高速です(図 20)。

おわりに

二次元パターン認識の応用技術として、指紋認証アルゴリズムを紹介しました。コンピュータ技術の進歩とバイオメトリクスのニーズの高まりにより、指紋認証技術の応用用途は、企業向けの製品から個人向けの製品へと広がっています。今後は、携帯電話、携帯情報端末、ノート PC などのモバイル端末から、自動販売機、金庫、自動車、ドアなどの大型製品まで、さまざ

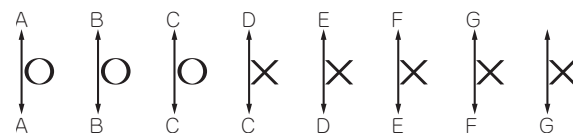


図18 データの単純比較

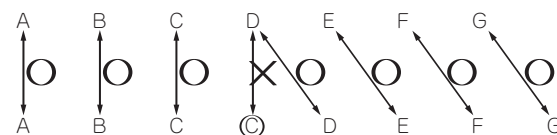


図19 DP マッチング



図20 周波数解析方法の指紋認証搭載携帯 G1100 (Pantech 社)

まな分野の製品に指紋認証機能が組み込まれていくことが予想されます。

本章で紹介した内容が指紋認証を搭載した製品を理解するための一助となれば幸いです。

参考 URL

- (1) 個人情報の保護に関する法律
<http://www.kantei.go.jp/jp/it/privacy/houseika/hourituan/>
- (2) NTT Communications 個人情報保護法対策ガイド
<http://www.ntt.com/vcn/security/gaiyo.html>
- (3) カシオ独自の指紋認証アルゴリズム VeriPat を開発
<http://www.casio.co.jp/productnews/veripat.html>

参考文献

文献1：松本，佐藤，藤吉，梅崎「LPC 分析に基づく指紋照合法の評価」電気学会論文誌 (2002 年 5 月)

■ (株)ディー・ディー・エス

TEL：052-323-3012

URL：<http://www.dds.co.jp/>

E-mail：info@dds.co.jp

よしみね・たつき (株)ディー・ディー・エス