平成 12 年度

学士学位論文

顔画像を用いた個人認証システムの性能検討に関する研究

Research on performance examination of individual attestation system using face image

1010429　　箱田和宏

指導教員　竹田史章　教授

2001 年 2 月 5 日

情報システム工学科

＜要旨＞

今日、個人認証を行うものとして多種多様の生体情報をコンピュータでの認証に使用する時代が到来している。その中で 1997 年前半から顔・顔貌が実用領域に入ってきた。顔画像の認証は指紋認証と同等の認証精度を得られるに至っている。本論文では顔画像認証ソフトの FaceIt を使用し、その基本性能の確認および撮像パラメータの一つである撮像角度について認証精度の検証を行う。

The age using various biometrics for the attestation with the computer to attest the individual has come. The face has become practicable since the first half of 1997. The attestation of the face image obtains the attestation accuracy equal the fingerprint attestation. In this paper we discuss the attestation accuracy of the FaceIt system, which is a the parameters of taking picture angle, which is a confirmation of the basic performance. We show the experimental results of this system according to variety of angle on the taking picture.

キーワード：顔画像認識、FaceIt、TrueFace、個人認証

目次

1 章　はじめに

これまでに個人認証の手段として、多種多様の生体情報をコンピュータでの認証に使う時代が到来している。たとえば指紋、掌紋、音声、筆跡、網膜などが列挙できる。その中で 1997 年前半から顔･顔貌が実用領域に入ってきた。本研究ではこの顔画像を用いた個人認証システムの性能検討に関しての研究である。

顔画像認証とは生体認識技術のひとつである。生体認識とは物理的な特性、属性に基づいて、人間を自動的に認識するコンピュータ化された手法のことである。生体認識技術は高い認証精度を持っている。顔認識の理由としては、ひとつには長年、顔の写真を利用してきたことにより親近性があるということである。そして精度、速度、費用面において有利である。そのほかにも、既存のデータベースが使え、容易に使用できデータ採取時に意識する必要がなく単純で、人間によるバックアップが可能であるということである。これが指紋や虹彩のデータの場合には人間は読み取れない。さらに顔画像は履歴情報により、追跡調査が可能であり遠隔からの監視も可能となる。

現在では海外はもちろん、日本でも NHK、KTT、KDD、電総研、東大等で顔の認識の研究が盛んになってきている。顔認識の短所としては人の顔を撮影しなければならないことである。このことはプライバシーの保護の問題に発展する可能性がある。撮影環境と人間工学的な側面を管理する必要があること、また他のバイオメトリクスと同様に万能ではないことである。

顔認識はカメラにおける顔の発見、これは背景から顔の特徴を切り出し見分ける。顔の計測は顔の特徴部分の位置関係が重要な要素になる。人間はいつも同じ表情をしていたり同じ方向を向いているわけではないので、表情による認識や顔の向き、その変化の大きさからの認識も必要となる。認識方法として単純な背景からの顔の切り出しを行うことは簡単である。しかしながら、いつも単純な背景ばかりではないため、複雑な背景だと顔の切り出しが難しくなる。これらのことはコンピュータ上では容易ではない。

しかしながら、このような顔の認証に対して認識精度の高い FaceIt というソフトウェアが報告されている。FaceIt とは米国政府が試験を行い、大学で開発・設計された顔画像認証用のソフトウェアである。このソフトは顔を視覚的なパスワードとしてコンピュータ上でのセキュリティに使用されている。コンピュータロック、ファイルロックがあげられる。FaceIt は現在世界で多種多様なアプリケーションに使用されている。たとえば、銀行の現金自動預け払い機（ATM：Automatic Teller Machine）、空港でのテロリズム防止のための手荷物検査、コンピュータのセキュリティ管理、犯罪捜査などである。これらは認証精度において成果をあげている。

類似顔画像認識ソフトウェアに TrueFace がある。このソフトも米国で開発されたものである。このソフトは FaceIt と性能的には同じであるが、違いは FaceIt がカメ

ラからの画像でのみ認証を行うのに対し、TrueFace は顔の特徴を格納したカードとカメラからの画像で認証を行うことである。また TrueFace は写真による偽装をプロテクトすることが可能である。

本研究では、現在世界で顔認識に使用されている顔画像認識ソフト FaceIt PC を使用して顔認証の精度向上のために二つの実験を行う。まず、データの登録はユーザ自身の良好な顔画像を 3 枚取り込む必要がある。良好な顔画像とは、頭部全体を含み垂直方向の傾きがほとんどないものである。顔画像を取り込んだあと、FaceIt は試験としてユーザの識別を確認する。識別確認はモニタ上で異なる領域を見たり顔を向けることでポーズを変える。FaceIt は各方向のポーズで識別を試み、必要なら顔面の特別な画像を追加する。この登録データをもとにデジタルカメラで撮影した個人写真を用いた認証精度を調査する。本研究では生体情報でない写真が認証可能か否か確認を行う。認証は各写真で 3 回ずつ行う。つぎに、5 人の顔の角度を変化させて認証を行う。こちらはリアル画像で実施する。カメラの正面を 0 度とする。それから上下左右に 5 度ずつずらして認証が不可能になるまで角度を増していく。認証はそれぞれの角度で 3 回ずつ行い、認証時間は 30 秒とする。この実験では FaceIt PC がどの程度撮像角度の変化に対応しているか検証する。

以上のように顔画像認識ソフト FaceIt PC の基本性能の確認および撮像パラメータの一つである撮像角度についてその性能の確認を行う。

2 章　顔の認識とは

人間の顔を計算処理の対象とする試みは、顔のパターン認識の問題として 1970 年代から行われてきた[1]。コンピュータの性能向上とともに画像処理技術が発達し、実時間での画像の認識と合成がある程度可能になった 1980 年代後半に、新しい画像通信の方式として知的符号化という概念が現れた。その中でもテレビ会議を年頭においた分析合成の研究では、顔画像の認識と生成技術を統合した顔情報処理システムに関する多くの試みがなされてきている。コンピュータに対する情報の出入り口として顔を利用する最近のヒューマンコミュニケーション技術も、ある意味では知的符号化の流れの上にあると考えられている。

顔の認識には、顔の発見、個人識別、表情認識などの課題がある。

2.1　顔認識の複雑さ

われわれ人間はすばやく、そして見たところ何の苦労もなく顔を認識しているが、コンピュータ上における問題が簡単であることにはならない。実際、顔以外の視覚認識機能にはまったく異常がないのに、顔だけは認識できないという人を対象にした研究によると、顔の認識だけを専門に司る特別な領域が存在するということが示唆されている。

顔面認識は古典的なパターン・マッチング手法が向いているとは容易にはいえない。実際には 2 つの処理すべき要素があるが、それぞれに課題を抱えている。最初の障害が検出である。システムは、画面の中に顔が存在するか否か判断しなければならない。その上で顔があれば、カメラからの位置および距離を測定する。つぎに、識別の問題がある。顔の位置を割り出したあと、システムはデータベースに格納された顔と整合する必要がある。

顔の検出や認識が困難である理由は、これらが固定の画像パターン―単純なテンプレート・マッチングで検出・分析が可能―で表されないことである。頭部は、どこでも、どんな大きさでも、またいろいろな速度で、様々な照明条件の背景のもとで現れる。さらに図 2.1 に示すように顔の表情、向き、髪型、顔の毛、(眉毛やひげ)、眼鏡のリードなど時間の経過につれて変化し、ある顔に固有なおびただしい量の多様性が生じる。

図 2.1　様々な状況下の顔

2.2　顔の認識

人間は画像がかなりぼやけていても、また、照明条件や背景が大きく変化しても、シーンの中から顔を即座に見つけ出す能力がある。また、髪型や化粧、見る角度、表情が異なっても、個人を識別することができる。さらに、笑顔、怒り顔など基本的な表情は相手が変わっても共通に理解できる。顔の認識をコンピュータで行う際に問題となる顔の発見、個人識別、表情認識などについて以下に述べる。

2.3　顔の発見

室内など背景のあるシーン中の顔認識では、まず画面中の顔がある場所と他の物体と区別して見つける（切り出す）必要がある。顔は目、鼻、口等の部品から構成され、これらの形状や位置関係は個人による多少の違いはあっても、ほぼ共通した特徴を持つ。これらの人の顔が共通して持つ、これらの一般的な特徴を用いて、顔を他の物体と識別して背景から発見する。そのための手がかりとして、肌の色、動き、形、大きさなどが考えられる。この中で、色はカメラからの位置によらずに比較的簡単に使えるのでよく利用されている[2]。つまり、肌の色の部分を画像から抜き出してつぎの処理の対象にするわけである。コンピュータで取り込むカラー画像は、赤、青、緑の三

つの成分に分解されているが、色を問題にする場合はこの 3 成分での表現はあまり便利ではない。たとえば、同じ色でも明るさが変化すると RGB の値が異なってくる。そこで色相、輝度、彩度の 3 成分による色表現に変換し、人の肌の色相を抽出手法がよく使われている。しかしながら肌の色は人種によって大きく異なるし、化粧や日焼けなどによっても変わってくるのでこれも絶対的な方法ということはできない。色情報のないモノクロ画像では、適当な顔テンプレートを画面内で捜査してマッチングにより顔領域を識別することが行われるが、2 次元的な位置と大きさの三つのパラメータを決定する必要があるため計算量が多くなるので工夫が必要である。

顔の発見は画像処理の対象領域を決定するための前処理であるが、実際はこれを容易にするために単色の背景を用意したりカメラとの位置関係を制限することが多い。また画像と同時に音声を参照することにより信頼度を上げる試みもある[(3)]。

2.4　顔の計測

個人の顔を識別したり表情を認識するには、顔の特徴的な部分の位置関係が重要な手がかりとなる。コンピュータで見つけやすい特徴としては、顔の輪郭や眉、目、口、鼻など顔固有の部品の位置と形状がある。輪郭を求めるには、まず、濃淡あるいは色相の変化の大きな部分を取り出すエッジ抽出をした後で、細線化と平滑化を行う。顔の場合通常の画像処理の対象物に比べて顔領域の境界は不明確なことが多いため、途切れたり雑音により変形した輪郭線を連続性やサイズなどの拘束条件によって逐次的に推定する手法が有効である[(4)]。

眉、目などの顔の部品は、標準的な形状のモデルを顔領域内で捜査して重ね合わせるパターン・マッチングで見つけることができる。顔が正面を向いて成立していることを仮定できる場合は、両眼、両眉の縦位置はほぼ同じで顔の中心線に対して対象であること、口は目の下側にあることなど顔全体の構造に関する知識を利用して、部品のありそうなところだけを詳しく探索する工夫によって計算時間を節約することができる。また、部品も含めて顔領域内のエッジ抽出をして横方向と縦方向のプロジェクションを行うことにより、眼や口の位置を推定することができる。部品の位置がわかると、再びその部品の輪郭を求めてサイズや輪郭上の特徴点の座標を求めることにより、顔の数値化が行われる。

動画像の場合は、顔の動きに部品の動きは乗っていること、両目は同時に瞬きすることなど顔の動き特徴を利用することができるためさらに高精度の処理ができるが、それだけ計算量は膨大になる。また、実空間のパラメータで数値化する方法もある。これは顔の全体的な特徴をとらえるには有効である。

2.5　個人の認識

人間は個人ごとに異なった顔を持っているため、顔を見れば個人が識別できる。顔の個人認証はセキュリティシステムにおいて特に重要である。上述の顔の計測データを各個人のデータと比較すれば個人識別が可能となるはずであるが、人の顔は年々変化するし、顔の向きや表情によって画像的な特徴が大きく変化することが個人認識を難しくしている。

個人の顔の認識のもっとも初歩的な方法は、顔の特徴点の位置関係に関するデータベースを作成し、計測した未知の顔のデータとの距離を調べてある程度以上近ければその人と決定する方法であるが、これは、顔を撮影する条件などを厳密にデータベース作成時と同じにておかない限りうまくいかない。また、加齢や健康状態の変化による顔の変形などにも弱い。

細かい部品の形状や位置ではなく、全体的な顔の特徴を比較するほうが、表情や環境の変化に対して強い認識ができると考えられる。離散フーリエ変換や離散コサイン変換による空間周波数スペクトルの低周波成分は画像の大域的な特徴を表すものであるが、対象を顔に限定した場合は、顔画像に特化したほうが記述力が高い[5]。つまり、撮影条件を変えた様々な人の様々な表情の画像を撮り主成分分析を行って、共通の特徴を分析することによって全体的な比較を行うのである。

ほかにも技術的には非常に多くの試みがあるが、最近この分野でも実用化を目指したソフトウェアが作られつつあり一部は公開もされている。それらの多くは、計算時間の節約のために特徴点の比較ではなく生の入力顔画像の大きさを規格化して候補画像と直接比較する手法を取っている。いずれにしても現在の技術のレベルは、カメラの前に特定の位置で正面を向いて撮った顔の個人認識がある程度可能になった程度であるが、コンピュータのパスワードや警備システムの鍵の代わりに本人の顔を使うことができるようになっている。これらは、眼鏡の着用、髪型あるいは加齢などによる見かけの変化にもある程度対応できるとされている。

2.6　表情認識

顔の認識に必要なものとして表情がある。コンピュータで表情が認識できれば、命令を入力しなくてもこちらの気持ちを察した処理をしてくれるようなコンピュータを造ることができる。コンピュータによる顔表情認識もパターン認識技術の一つであり、個人認識と基本的には同じ問題といえる。しかしながら、個人認識では、どんな表情をしていても特定の人を当てなければならないのに対して、表情認識では、人が違っても同じ表情は同じと見なければならないというわけで、認識技術の方向が異な

っている。つまり、個人認識では表情が雑音になり、表情認識ではここの顔の相違が雑音となる。

表情認識では顔部品の形状と位置の変化が重要な手がかりとなる。絶対的な位置関係はあまり問題ではなく、無表情時との差が重要である。そこで、まず特徴点抽出を行い、表情ごとにそれらの変化の傾向を調べて表情を認識するのである。顔の表情の種類は極めて多いと考えられるが、主として基本的であり同時に不変的であるといわれている、「驚き」、「恐怖」、「嫌悪」、「怒り」、「幸福」、「悲しみ」の基本 6 表情が対象となっている。

各表情によって特徴点の変化が一定であれば問題ないが、実際にはかなり複雑な変化をするし、撮影条件にも変化が大きく依存するため、単純なルールを作ることができない。そこで、ニューラルネットワークによって特徴点の変化と表出された表情の関係を学習させる。

個人認識と同様に、顔の全体的な変化から表情を認識する試みも行われている。全体特徴の把握には、顔画像の同じ輝度の点をつないで作った図 2.2 に示す濃度等高線から全体の変化をみる試みも比較的古くから行われている。濃度等高線は照明に依存するが、その変化を顔面全域でのベクトル場としてとらえることにより、表情認識に利用することができる。また、動画像の場合は顔面のオプティカルフローを用いたり、音声認識と同様に隠れマルコフモデルによって表情認識を行う試みもある。

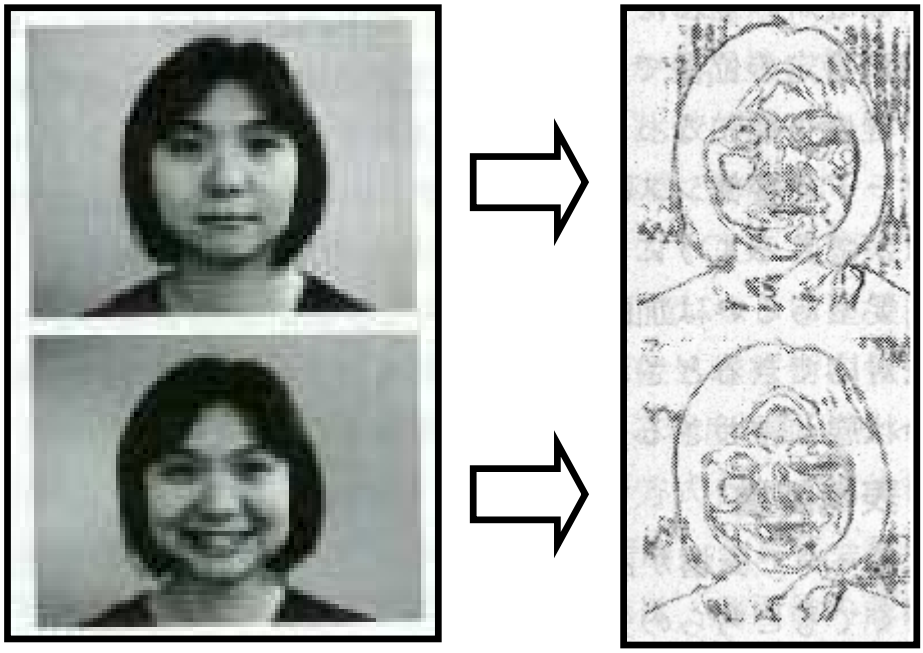

図 2.2　濃度等高線

2.7　顔の向き

個人認識や表情認識のほかに、図 2.3 に示す視線や顔の向きの認識もコミュニケーションにおいては重要である。顔の向きの認識は、あらかじめ色々な向きでの顔画像を方向別に整理した方向別標準画像と比較することで実現される。また、特に肌色領域と部分配置のかたよりを手がかりとする方法も考えられる。また、顔面の特定の特徴点を結ぶ多角形の対称性の崩れによって、顔の向きを検出する試みもある。

ユーザの顔の向きが検出できればインターフェースの入力としてはかなり有効であるが、さらに視線方向を推定することが必要な場合もある[6]。これは、人工現実感システムや臨場感通信などで、ユーザの視線にあわせて画像を提示するのに利用できる。視線方向を画像のみで抽出する試みは少なく顔の向きを視線方向とする近似的な扱いが多いが、眼の部分を十分な精細度で拡大することができれば、いわゆる黒目と白目の領域の関係から眼球の向きの推定は可能であると思われる。これを両眼について行い輻輳角を推定すれば注視位置を 3 次元的に特定することもできるだろう。

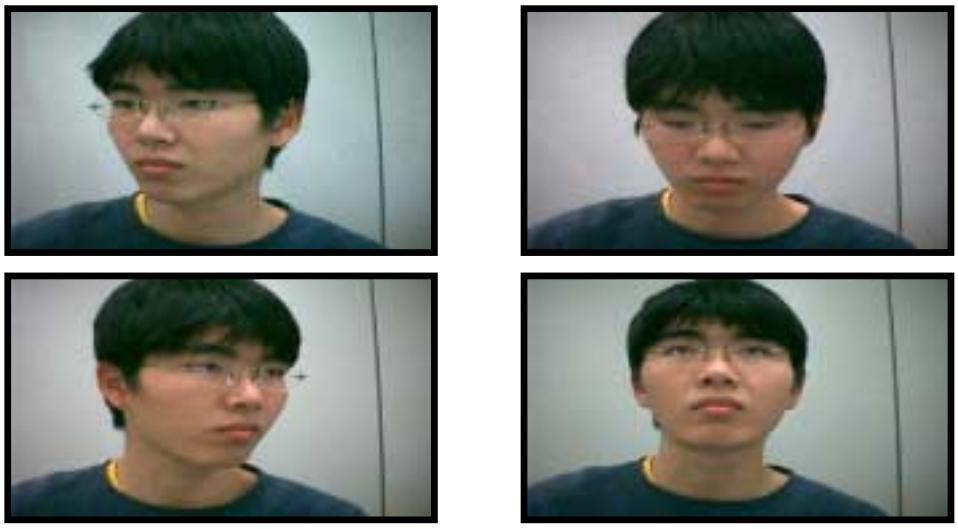

図 2.3　顔の向き

2.8　単純背景／複雑背景

個人認識、表情認識など認識を主体とした研究では認識方法に焦点をおき、顔や人物像の切り出しを簡単にするために、単純な背景を用いることが多かった。記憶した背景画像との差分、オプチカルフローの利用、肌色情報の利用、顔なら顔部品の形状と位置関係の利用などの方法が使われている[7]。しかしながら、実用を考えると、単純な背景をいつも期待できない。複雑な背景から、顔や人物像を検出しようとすると、

ある一つの方法ではその前提とする条件が満たされない部分が必ずあるので、これらの方法を組み合わせて用いる必要がある。しかしながら、照明、背景、ユーザの服装など様々なバリエーションが考えられるので、ターンキーシステムのようにどこでも誰でも直ちに使えて、顔や人物像が切り出せるというシステムは当然ながらまだない。これはかなり難しいと思われるので、現場での簡単なイニシャライゼーションにより使用環境にチェーンアップするよい方法を見つけたいものである[8]。

2.9　見え方モデル／3 次元モデル

3 次元物体は同じ物体でも見る方向により見え方が異なる。また物体との距離により大きさが異なって見える。このため、コンピュータビジョンの研究では、物体の 3 次元モデルを用いてそれを 2 次元の入力画像に当てはめることにより認識するという手法を用いることが多かった。この方法だと 1 種類の物体に対しては一つの 3 次元モデルを準備すればよいのだが、1）モデルの当てはめが複雑な処理を必要とする、2）3 次元のモデルを 2 次元の画像に当てはめるのは本来あいまいさが残るという欠点もある[9]。

見え方モデルの場合、モデルが 2 次元の見え方なので、入力画像との照合が簡単明瞭であるという利点がある一方、視点の大きさや方向の変化に弱いという欠点がある。しかしながら、インタラクティブシステムという点を考えると、コンピュータが認識しやすいように、コンピュータに対して人がある一定の位置と方向にいるということはそれほど難しいことではない。わざわざ認識しにくい状況ではなく、コンピュータに対して、たとえば正面で一定距離の位置にいてコンピュータとインタラクションすることは人にとってそれほどの制約ではない。これが意思を持たない物体の自動認識とは違う点である。また、見え方モデルの利用は処理が簡単なため実時間処理に向いている。このため、顔認識には見え方モデルが使われることが多い[10]。

2.10　向きの変化、大きさの変化

見え方モデルの欠点は向きの変化、大きさの変化に弱い点である。このため、コンピュータに対し一定の位置で一定の向きで向かい合うという制約をつけたが、一定範囲内で自由度を許したほうが当然使いやすい。これは、いくつかの向きからの見え方もデル、またそれぞれに対しいくつかの大きさの見え方モデルを準備することで対処できる[11]。人と人との会話を考えても分かるように、人はコミュニケーションのとき、相対的な位置や向きをそれほど大きく変えるわけではないので、それほど多くの見え方モデルを準備しなくてもよい。

このような方法は、以前なら、多くのメモリも必要だし、照合にも時間がかかるという批判を受けただろうが、コンピュータのメモリも大きくなり、処理時間も早くなったために現実化した方法である。

2.11　マルチカメラ

人の動きが大きいと 1 台のカメラでは不十分なこともある。たとえば、表情認識では正面に近い画像のほうが認証精度が上がるが、顔の動きが大きい場合、1 台のカメラでしか撮像していないと横顔に近い画像が入力されることもある。また、ジェスチャ認識などでは、認識に必要な特徴がセルフオクルージョンにより隠されてしまうことがあり、これでは認識精度が落ちてしまうことになる。

これを解決するには、カメラ（視点）を増やして、入力情報を増やし相互に観測を補完する必要がある。こうすると、あるカメラでは横顔が入力されても、ほかのカメラには正面に近い画像が得られるので、その情報を用いて表情認識すればよいことになる。

マルチカメラは設置が面倒だが、むきの変化が大きいような状況下での精度のよい認識には重要となる[(12)]。

2.12　アクティブカメラ

通常の使用では人とコンピュータの距離はそれほど大きくは変わらない。したがって、一定範囲内での大きさの変化に対処しておけば十分である。しかしながら、監視などへの応用も考えると、人は当然コンピュータを意識することなく部屋の中を自由に移動していることを想定する必要がある。この場合、人がカメラから遠方にいれば、画像上での人物像は小さくなり、人であることは判別できたとしても、その表情認識や個人認識は無理である。これを解決するには、カメラにズーム機能とパン・ティルト機能をつけてアクティブ化し、興味ある部分をクローズアップして撮ることが必要となる。能動的なマルチカメラを用いることによりかなり広い範囲における顔やジェスチャの認識が可能となる。

2.13　分散強調処理による顔の自動検出

画像処理や音声データなどをもとに人と対話し処理を行う知的インターフェースでは、イメージ・シーケンス中からユーザの顔を自動的に抽出・認識し、その表情変

化や個人属性などをリアルタイムに検出することが不可欠となる。人間が顔を認識する場合、これまで述べた方法を複数用いていろいろな手がかりを同時に探しそれらを総合的に判断していると考えられる。ここでは、イメージ・シーケンスの中から人の顔を検出する独立した複数のモジュール（エージェント）を並列に動作させて顔を抽出する顔追跡システムの具体例を紹介する[13]。

このシステムで扱う顔の手がかりは表 2.1 に示すように、色、形状、動きの３種である。これらの特徴を抽出する画像処理モジュールは、その処理の性質によって即応型と塾考型とに分類される。

表 2.1　顔認識の手がかりとなる情報とその特徴

情報の書類	特徴	
	長所	短所
色	肌色の抽出によって大まかな顔の領域、位置決めが可能 高速な処理	証明変化に対する変動
形状	顔の輪郭や部位などを用いた詳細な認識、顔らしさの判断が可能	視点変化によるオクルージョン 複雑な計算
動き	動作している人物の特定が可能	正確な顔の位置の特定は困難

即応型モジュール群には、顔認識処理のために必要な時系列画像の取得および色相、輝度情報の抽出を行う前処理モジュール、および塾考型の顔検出モジュールから受け取った最新の顔画像をテンプレートとしてテンプレート・マッチングを行い現フレームにおける顔の位置を決定するマッチングモジュールがある。図 2.4 はその結果である。

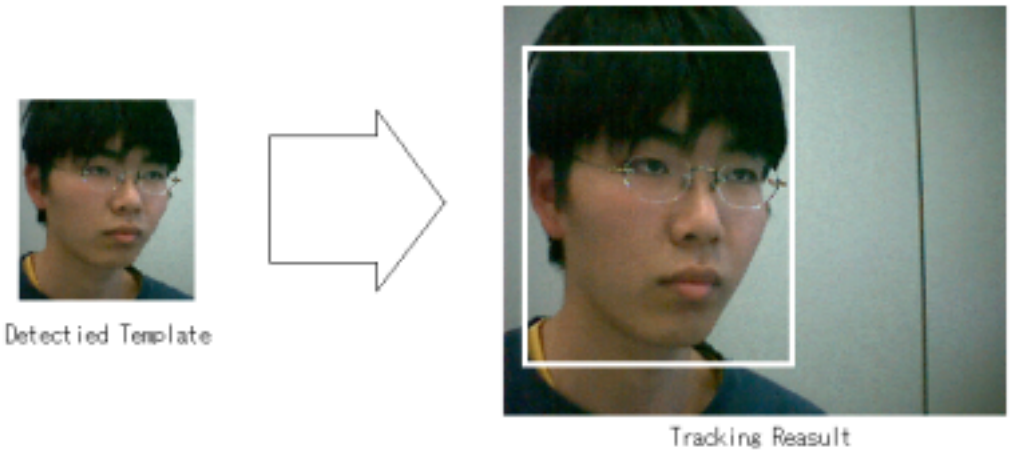

図 2.4　テンプレート・マッチングによる顔追跡処理

さらにマッチング結果を受けて顔を常にシーンの中央にとらえるようにカメラを移動させるマニュピレータ制御モジュール、および顔候補が見つからないときに人間を発見するためにシーン中の動いている部分を検出するモジュールも即応型モジュール群に含まれている。

塾考型モジュール群には、照明条件や人種の違いに対しても安定して肌色領域を検出するために色相ヒストグラムから適応的に閾値を変化させる肌色抽出モジュール、および抽出された各肌色領域に対して縦横比など顔形状が有しているいくつかの特性を満たすかどうかを判定し、顔候補の絞込みを行う顔形状チェックモジュールがある。つぎの図 2.4 は低照度照明下における適応的な肌色領域抽出の効果を示す例である。

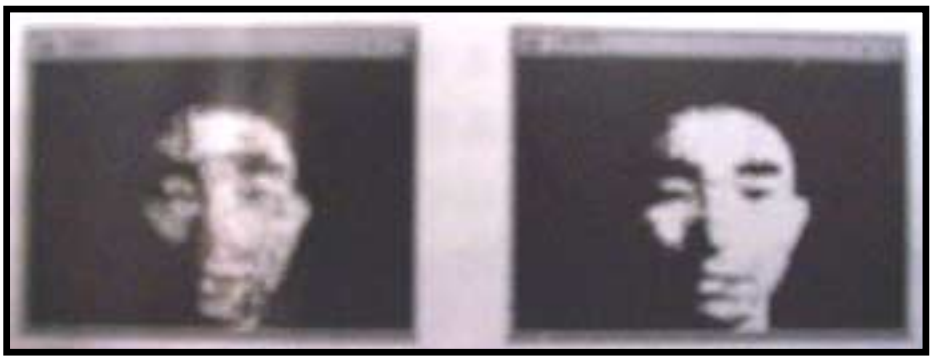

図 2.4　肌色の抽出結果

顔形状チェックモジュールでもっとも顔らしいと判断された領域が追跡対象の顔テンプレートとしてマッチングモジュールに送られる。

3 章　顔画像認証ソフト

この章では 2 章で示した顔認識手法をより精度を高めてソフトウェア化した FaceIt、TrueFace について述べる。

3.1　FaceIt

FaceIt は米国政府が試験を行い、大学で開発・設計されたパソコン用のソフトウェアである。FaceIt は 6 つの基本的な能力を備えたリアルタイム顔認識ソフトウェアエンジンである。その能力は Face Detection（顔検出)、Segmentation(分類)、Tracking(トラッキング)、Faceprint Coding(コード化)、Verification(認証)、Identification(識別)の 6 つである。

顔検出では相手に制約も与えないで、複雑なシーンから、自動的に顔を捕らえる。群衆の中の一人の顔を追跡する最新技術により、同時に複数の顔を処理することができる。分類は捕らえた顔を自動的に背景から顔画像を抽出することである。トラッキングはカメラの枠に入れば顔を自動で追跡することである。コード化は FID または Faceprint と呼ばれる、ある特定の個人に特有な、不変的なディジタル・コードまたはテンプレートを生成することある。認識はデータ・ベースと抽出した画像が本人であるか否かを判定する。識別は識別したい画像をデータ・ベースから探索して名前、ID、確からしさの度合いを表示する。

3.1.1　顔の表現手法

ここでは顔認識技術の表現方法について述べる。顔認識技術の最も基本的要素は、Faceprints を構築する際の表現手法である。Faceprints を構築する際の表現方法には 2 つの代表的なアプローチがある。１つは大局的な方法で Enginfaces(Sirovvich、Pentland など)というもの、もう１つは局所的な方法で、Local Feature Analysis (局所特徴分析、以降 LFA と表現する)である。

Enginfaces は顔の向き、照明、顔の表情、髪等の局所的な変化によって、値が大きく変化したり、また人種、民族の違いに敏感である等の理由で、実用は困難である。

3.1.2　LFA(Local Feature Analysis)

一方 LFA の特徴として、図に示すように、顔は、指紋と同じように、自動的に検出可能な、結節点(Nodal Points)を持ち、その結節点は個人ごとに、幾何学的に特有

な位置関係を持っていて、Enginfaces 等の技術が持つ特有な問題を回避できて、正確に計量が可能である（図 3.1、3.2 参照）。

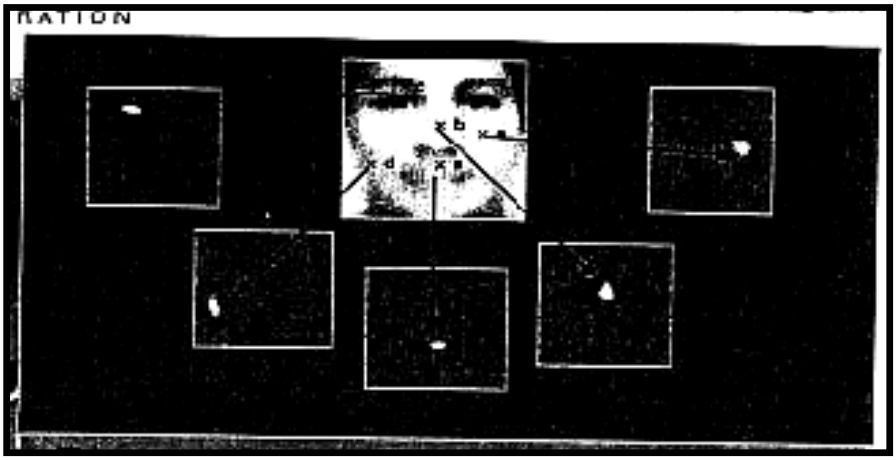

図 3.1　顔の結節点 1

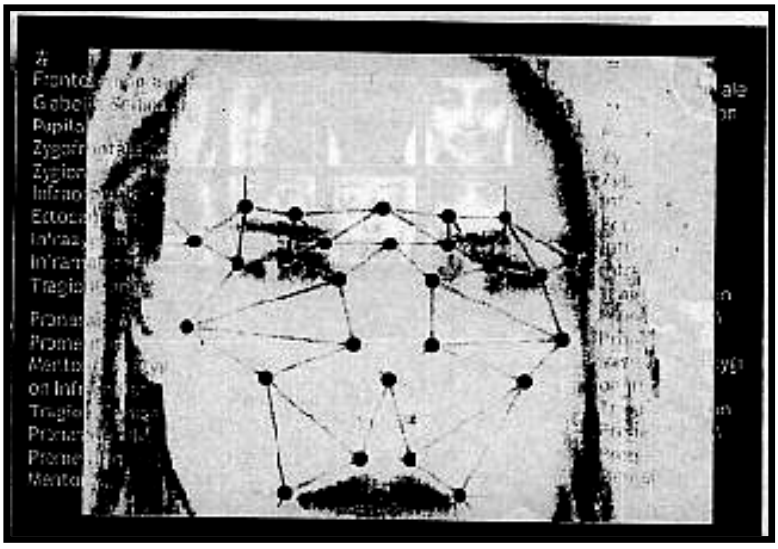

図 3.2　顔の結節点 2

また、色情報や人種に無関係である。これはいろ情報を使用しないため肌の色の変化に強く、性能は人種に関係なく、顔の構造は普遍的なためである。そして各種入力機器に対応しており、赤外線あるいはナイトビジョンも使用可能で、faceprint は経年変化による影響が少ない。

3.1.3　データ照合速度

データの照合速度は、Pentium500Mhz の場合、照合データをハードディスクから読み込む場合、1500 万件／１分（1 件／4 マイクロ秒）で、照合データがメモリに読み込まれている場合は、6000 万件／1 分（1 件／1 マイクロ秒）である。そして Faceprint のコードサイズは 84 バイトです。これらの特徴により、大規模な個人識別システムが構築可能である。

3.1.4　精度

顔認識の精度として、照合は他のバイオメトリクス技術の場合と同様、False Accept Rate（他人受入誤認率)、False Reject Rate（本人拒否誤認率)、および Equal Error Rate（FAR = FRR の誤認率）は、分析のために使用される固有のデータ・ベースに依存する。

しかしながら、実際の大規模データ・ベース上で実行されたベンチマークテストによれば、FaceIt の性能の評価は１０個の指紋の使用を要求する AFIS システムとも十分競合しえることが示される。

図 3.3 のグラフは、認証のスレッシュホールド機能としての、他人受入誤認率および本人排除誤認率を示している。これは、FERET（FacE Recognition Technology）データ・ベース（U.S. Army Research Laboratory）で公開されているものである。

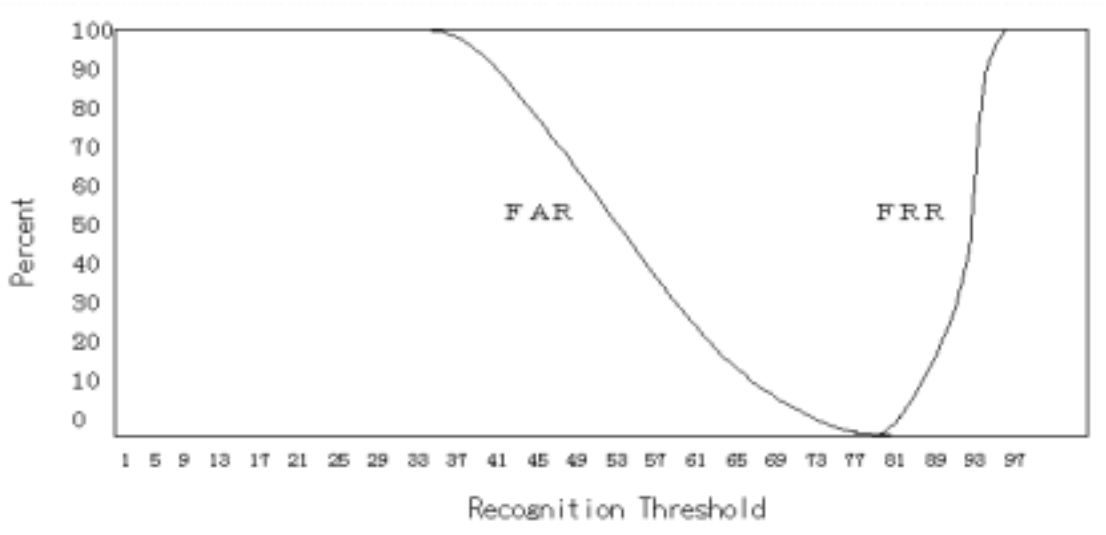

図 3.3　Performance on FERET Database

認識精度は画像データに依存するので特定のデータ・ベースでの比較が必要になる。例えば、FERET の評価では図 3.4 のようになる。

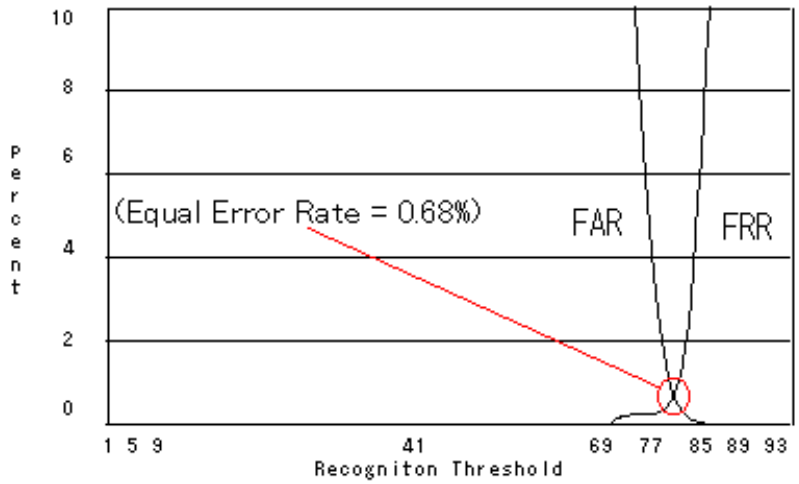

図 3.4　顔認識の精度

さらに、独自のベンチマークテストを実地したい場合、FaceIt DB Evaluation Software を使用し、自分で選択したデータ・ベースをもとに、FAR（他人受入誤認率）および FRR（本人排除誤認率の曲線）を容易に得ることができる。

3.2　FaceIt 機能

ここでは FaceIt がどのように機能するか述べる。FaceIt head detection 顔の検出は絶えずデータストリームの中の顔を探す。頭状のオブジェクトが検出されると、ソフトウェアは様々なパターンマッチングのアルゴリズムを用いて、顔がその場所に確かにあるかどうかを判断する。これらのアルゴリズムは、複数の顔の存在を正確に同時に発見し、それらの正確な位置を決定できる。ある顔を発見したならば、バックグラウンドからそれを切り出し、サイズ、照明、表現および姿勢を補正するため、多くの独自の予備的処理段階に進む。その“正規化された”顔は、LFA（特徴点分析法）という数学的なテクニックによりフェースコード（Faceprint）という固有の情報に変換される。このディジタル・コードはその顔に特有な情報を含んでいる。そのライブのフェースコードをデータ・ベース内の既知の個々人の顔紋と比較して、その顔のアイデンティティを決定する。

FaceIt は照明、肌の色、顔にかかる髪の毛、ヘアースタイル、眼鏡、表情および姿勢の変化に対してフェースコードは強いという事実がある。なぜならば、フェースコードはその顔に特有な形や諸特徴から作られているからである。さらに、フェースコードは数百万人の中からある個人を正確に識別することができる十分な情報を含むということが知られている。市販の一般的なプロセッサ上で、全てのプロセスは完全に自動化され、連続的かつリアルタイムで起動する。どの顔認識システムにとっても、

顔を符号化する方法が重要である。

FaceIt は特徴点分析法 LFA を使い、統計的に導き出されたローカルブロックのより顔の画像を表す。LFA は全ての顔の画像（さらにいえばすべての複雑なパターン）はある非還元性の構成要素の集合（an irreducible set of building elements）により合成できるという認識に基づいた数学的なテクニックである。これらの要素は精巧な統計的手法により、ある複数の顔の集合体（a representative ensemble of faces）より導き出される。それらは複数のピクセル（局所的な）にまたがり、普遍的な顔の形を表すが、正確には一般によく知られている顔の特徴ではない。実際、顔の各パーツよりもさらに多くの顔の構築する要素がある。しかしながら、ある特定の顔の画素を、相当程度の高い精度にまで合成するには、すべての有効な要素のうち、ある小さい部分集合（12 から 40 の特徴的な要素）だけが必要なことが分かる。アイデンティティ（顔の識別）はどの要素が特徴的なのかということだけでなく、どのような幾何学的な結合の関係か（つまりそれらの相対位置）によっても決定されます。この方法により、FaceIt は他のものと一致させたり比較させたりすることができる複雑な数式で個人のアイデンティティを表す。

3.3 FaceIt 技術的使用

つぎに FaceIt の技術的使用について述べる。まずサポート可能なプラットホームとして Windows95/98/NT があり、Unix と Linux にほとんどのエンジンの機能をポート済みであり、1 対複数の検索用の Informix Datablade も可能である。

入力は写真、動画像または録画画像およびディジタルビデオファイルを含むあらゆる視覚信号のソースが入力可能である。また似顔絵も入力可能である。速度として頭の発見速度は 50‐300 ミリセカンド（シーンの複雑さに依存する）。1 対 1 の照合速度は、1 秒以下で、1 対複数の照合速度は、毎分 1500 万から 6000 万件（顔のテンプレートの記憶媒体やコンピュータの仕様に依存する）である。フェースコード（Faceprint）の大きさは、84 バイトから 3.5 キロバイト（必要とする速度と精度に依存する）アプリケーションによっては、両方のテンプレート w を使用する。認証（authentication）用には 84 バイトのテンプレートサイズで十分である。データベースサイズは制限がなく、ハードウェアに依存している。動きは静止画像の顔および動画像の顔を検出する。この技術は正面の画像（横顔ではない）と一致するように設計されている。顔の検出（フェースファインディング）は、両目のある顔を見つけ、正面から見て任意の方向 45 度以内（上下、左右、傾斜）、認識は 15 度までの姿勢の変化に対して不変である。15 度から 35 度までは、照合能力に小さなロスがある。35 度以上の傾きは、照合についてかなりのロスが起こりえる。このアルゴリズムは顔の内側の部分に注目しており、また顔の自然な変動性を補うために内臓のメカニズムを

持っている。したがって、表情、顔にかかる髪の毛、およびヘアースタイルの変化に関しては強いエンジンとなっている。照明は特別なものあるいはバックグラウンドは不要である。拡散したアンビアントライティング中で最適の性能を達成する。そして人物の背後から光があたってない状態がベストである。ただし、ビデオカメラ上のゲインコントロールで補正可能である。目安として、このシステムは人間が見ることができる顔については検出できる。任意のバックグラウンド（プレーンなあるいは雑然とした）の中の顔を見つける。認識はバックグラウンドにはまったく依存しない。画像の色、グレースケール、および解像度は、カラーおよびグレースケール画像で同じ性能で機能し、最低 8 ビットの image depth および 320×240 フレーム解像度が必要である。頭のサイズは 20×30 ピクセルほどの小さな顔、あるいは画像表示の中の 1%未満を占める顔も検出可能である。低解像度の顔の画像でも著しく認証のパフォーマンスには影響しない。頭のサイズが 80×120 ピクセルの場合、顔の認識には最適である。顔の検出は自動的なものがすべての大規模な顔認識システムにとって重要である。なぜならば正確なテンプレートを作成するためには、顔の正確なポジショニングが必要だからである。FaceIt は顔を見つけて、高速かつ正確に位置合わせをする。その後で検出した顔が位置合わせの品質としてよいものかどうかを示して評点を出す。実際のデータ・ベースで行うと約 1%から 2%程度について自動的に位置合わせが行えない。それらの顔については、FaceIt エンジンに添付されるツールを使用して手動で位置合わせを行うことが可能である。

3.4　FaceItPC

ここでは個人認証用顔認識ソフトウェアである FaceItPC について述べる。このソフトは著者が実験に使用したものである。Windows95 用（98 でも使用可）で、スクリーンセイバーロック、ファイルロックが主な目的で、パッケージ品であり、認識登録できる人数は 5 人までである。このソフトに必要な機器は、Microsoft Win95(98)、90MHz Intel Pentium Compatible or higher、 16MB RAM／10MB free hard disk space、VGA or higher video display adapter、VFW(Video For Windows) 対応カメラ&キャプチャボード又は USB カメラである。

このソフトの特徴として、要求により、あるいはあらかじめ設定された休止期間後に自動的にコンピュータをロックできる。これはカメラをのぞき込むだけでアクセスできる。FaceIt は、ユーザの存在を検出して、顔を見つけて識別し、そしてアクセスを許可する。手操作による入力は、まったく必要ない。図 3.5、図 3.6 はロックコンピュータを行うコマンドとロックコンピュータ時の画面である。

図 3.5　ロックコンピュータ

図 3.6　コンピュータロック時の画像

FaceIt は、ユーザの好みのスクリーンセーバと共存して動作可能である。強力な物鑑定機能が画面内のわずかな動きも捉えるので、画像やマスクの顔と、本物の人間の顔とを見分けることができる。また、アクセスを許可、あるいは拒否されたすべての人物の写真などを取り込んだ検査ログ記録を作成する。

FaceIt サイファーを用いて暗号化することにより、機密および秘密のドキュメントを保護する。FaceIt サイファーとは米国第三暗号化ソフトである。また、顔面識別による照合なしでは、解読できないようにしている。ドラッグアンドドロップにより、暗号化および暗号解読は、すばやく簡単にできる。ファイルはもちろん、フォルダー全体をも暗号化できる。暗号化が完全に成功するともとのファイルを消去し、最終的にはファイルシステムからも削除する。銀行で使用されているものと同じ、業界標準の D.E.S 暗号化技術を使用し、経理記録も保護する。Windows95／NT のエクスプローラと完全に統合化されている。つぎの図 3.7 から図 3.10 はファイル暗号化の流れである。

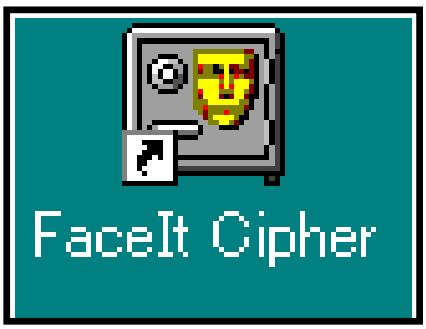

図 3.7　FaceIt サイファー

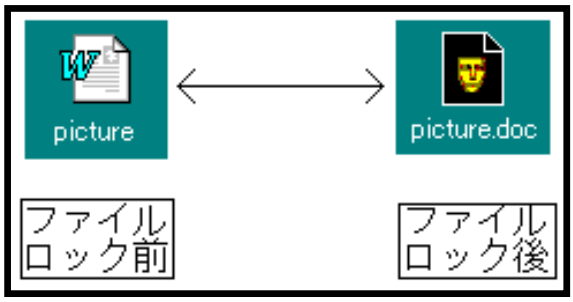

図 3.8　ファイルロックアイコン

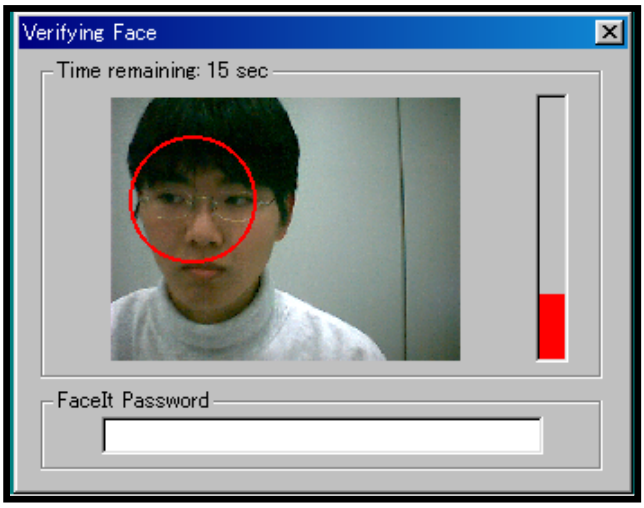

図 3.9　顔の照合

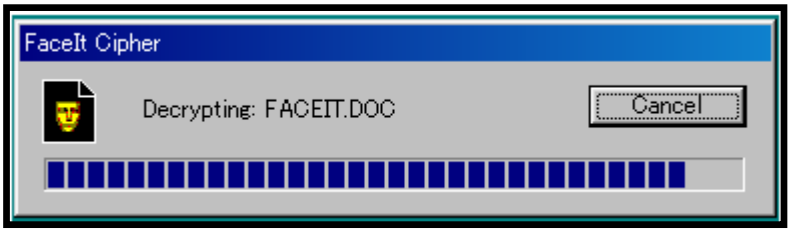

図 3.10　ロック解除中

FaceIt は、ユーザが離れている間の作業領域を監視しており、視野に入った顔面を自動的に補足して保存を行う。顔面は、カラーJPEG 画像として補足し、日付と時間の記録および識別情報を保持する。認識された顔面と認識されない顔面とを別々にログに記録する。画像は定期的に、ハードディスク上の指定されたファイルに保存されるか、あるいは ETP を介してユーザのウェブページにアップロードされる。

FaceIt は、コンピュータを保護する一方で、コンピュータを操作した人物を自動的に検出して、その人物にメッセージを残すように指示することもできる。FaceIt は、ユーザの出力メッセージとして AVI（コンピュータ映画）を再生する。訪問者は、テキストでメッセージ入力を残すことができ、またオプションとして顔のスナップ写真を残すこともできる。メッセージは、コンピュータ上に保持しておくこともできれば、あるいはインターネットを介して世界中のいずれのコンピュータにでも電子メールを用いて自動的に転送することもできる。Microsoft Mail や Qualcom の Eudora3.0 などの Microsoft MAPI 互換の電子メールプログラムとの共存が可能である。

3.5　True Face

ここでは True Face について述べる。

3.5.1　基本性能

まず True Face の特徴として、豊富な納入実績が示す信頼性があげられる。そして各アクセスの履歴に顔画像を残すことが可能であること。顔の特徴データはカードやデータ・ベースに格納可能で、１.５kb（次期バージョンは４００～１５００バイトになる予定）特徴データをチケットやカード上に 2 次元バーコードとして印刷可能であること。機械的なメンテナンスは不要であること。写真による偽装をプロテクトすることが可能なことがある。さらに違反行為を行おうとすると、顔の画像がサーバに残ってしまうので、違反行為そのものを抑制する効果がある。またステレオカメラによる視差情報または 1 台のカメラで顔の傾きの異なる 2 回の撮影を行うことによって、写真での偽装をプロテクトすることができる。米国のインターネットセキュリティアシュアランスサービスを行っている ICSA（International Computer Security Association）から顔認識ソフトウェアとして唯一承認を受けている。

顔認識の動作は図 3.11 に示すようにあらかじめ登録してしていたカードのデータとカメラから捕らえた顔とを比較、照合して本人かどうかを判定する。

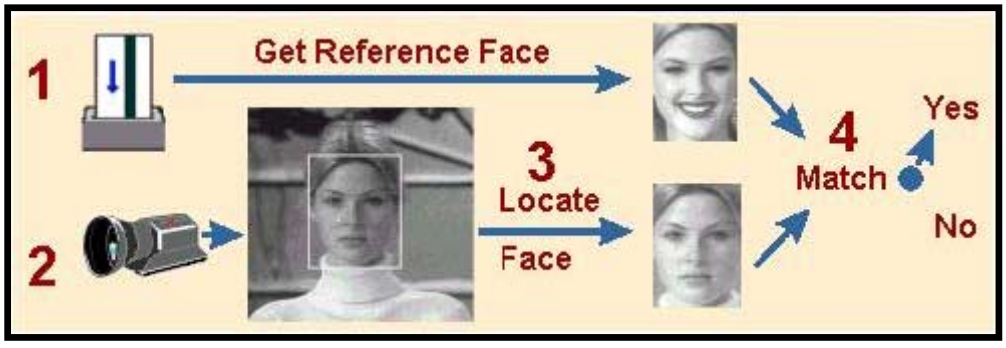

図 3.11 顔認識の動作

3.5.2 アプリケーション

True Face には 1：1 照合アプリケーションと 1：n 照合アプリケーションがある。

1：1 照合アプリケーションは、個人の ID を入力（カード、暗証番号など）し、データ・ベースに登録された個人の特徴データと比較する。入退室管理として、イタリアの銀行／宝石店、インドの石油会社、ブラジルの工場、フィデリティ投信コンピュータセンタ、Ameritech 社、Security Link などで使用。エアラインアプリケーションとして国際線ゲートにおける空港職員チェックに使用。端末／コンピュータアクセ

スで米国 ATM、CCM ネットワークサクセス、Web トランザクションに使用される。といったものがある。

1：n 照合アプリケーションは、ID 入力は不要である。これはデータ・ベースの中から検索し、処理は 1：1 照合と同様に複数の特徴データと比較する。これは監視、犯人捜査、入出国管理、住民管理、米国におけるカジノでモニタリングに使用される。

3.5 TrueFace 製品

ここでは TrueFace 関連の商品について述べる。

3.5.1 TrueFace Engine SDK

この製品はユーザが簡単にオリジナルアプリケーションを構築するための C 言語ライブラリソフトウェア開発キットである。画像の入力、顔の切り出し、顔のベリファイ（照合)、顔のアイデンティティ（特定）がシンプルなコマンドとして提供されている。

このサポート OS は Windows95/98/NT、SUN Solaris（オプション）であり、サポートコンパイラは Microsoft Visual C/C++ 、Visual Basic である。

3.5.2 TrueFace Network

これはコンピュータネットワークにおいて、顔認識により重要ファイルや重要プロセスを保護することができます。サーバ上のアドミニストレーションプログラムから不正アクセスを通知したり、その人の画像を表示したりすることができる。また、サーバ上でオンデマンドのレポーティングシステムが提供される。

この製品はサーバとクライアントがあり、サーバの CPU は Pentium プロセッサ、サポート OS は WindowsNT Server V4.x、アプリケーションは Microsoft SQL Server6.5 である。クライアントには２種類あり、ログインサポートの CPU は Pentium プロセッサ、サポート OS は WindowsNT Workstation V4.x、カメラは Video for Windows 対応カメラ、またはビデオ入力である。もう一つの API サポートの CPU は Pentium プロセッサ、サポート OS は WindowsNT Workstation V4.x、または Windows95/98、カメラは Video for Windows 対応カメラ、またはビデオ入力である。

3.5.3 TrueFace Web

この製品はインターネット、イントラネットの Web トップアプリケーションにお

いて、Web サイトまたは特定のページに対して、顔認識によってセキュリティガードを強化することができる。TrueFace Web で保護されたページをアクセスすると、ユーザのブラウザから画像入力、暗号化、TrueFace クライアント（Active-X コントロールまたはネットスケープのプラグイン）が起動される。顔認識により TrueFace Web サーバが本人であることを確認し、保護された Web ページが通常通りユーザのブラウザに転送される。

この製品もサーバとクライアントがあり、サーバの CPU は Pentium プロセッサ、サポート OS は WindowsNT Server V4.x またはそれ以上、アプリケーションは Microsoft Internet Information Server3.0 またはそれ以上、クライアントの CPU は Pentium プロセッサ、サポート OS は Windows95/98/NT4.x、ブラウザは Microsoft Internet Explorer3.1 またはそれ以上、Netscape Navigator4.04 またはそれ以上、カメラは Video for Windows 対応カメラ、またはビデオ入力である。

4 章　顔画像認証ソフトの利用方

4.1　FaceIt 導入例

この章では現在世界中で使用されている FaceIt 製品の適応アプリケーションについて述べる。

まずは ATM、ベンディングマシンへの応用、これはカメラに顔を見せるだけで OK なので、キャッシュカード、クレジットカード、ID カードなど使用者の個人認証により盗難の防止が行える。現在 ATM に FaceIt を組み込んだ銀行口座を持たない人向けの新しい形式のマシンが既に 500 台稼動していて、3500 台のマシンを契約している。このマシンのユーザ登録数は 640000 人で、150 万件を超える顔による本人認証の実績を残している。

つぎに流通市場への応用として、顧客調査がある。その方法は、ビデオカメラによって顔の検出を行い、来店日時、および顔のデータを記録する。そして顔の顧客データベースとの照合をして、個人別来店頻度、購入品の集計を行う。これは Point of Sale 端末との連携で行う。これのシステム構成は図 4.1 の通りである。

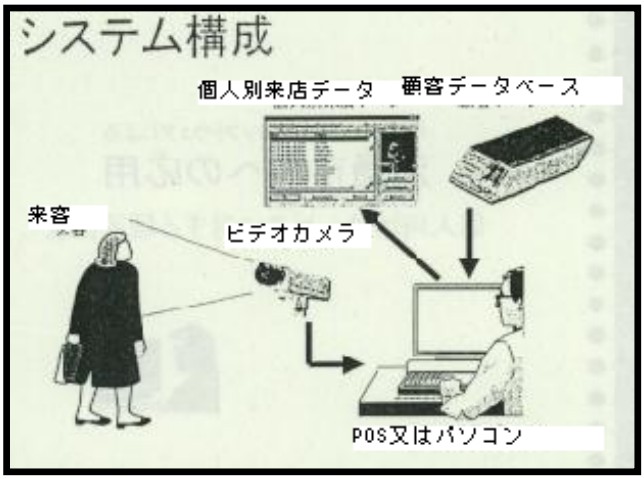

図 4.1　システム構成

ここでの FaceIt の監視の機能はカメラで捕らえた顔を検出して時間データを付加して保存を行う。顔を検出したときに、常連客、得意先などの判断をリアルタイムで行うものである。そして検索の機能は、顔画像データの検索を行う。そしてライブ画像との照合を行い、照合度合いの最も高い顔を同一人ものとして検索を行うものである。システムの拡張として無線方式による通信ネットワーク、サイバーショッピングがある。

つぎに入国管理における応用例について述べる。これは不法入国者、犯罪者、テロリストなどの人物検索を行うものである。人物検索の方法は、ビデオカメラによる顔の検出を行い、撮影日時、および顔のデータを記録する。そして顔のデータベースとの照合。図 4.2、図 4.3 に示すように使用例をあげる。

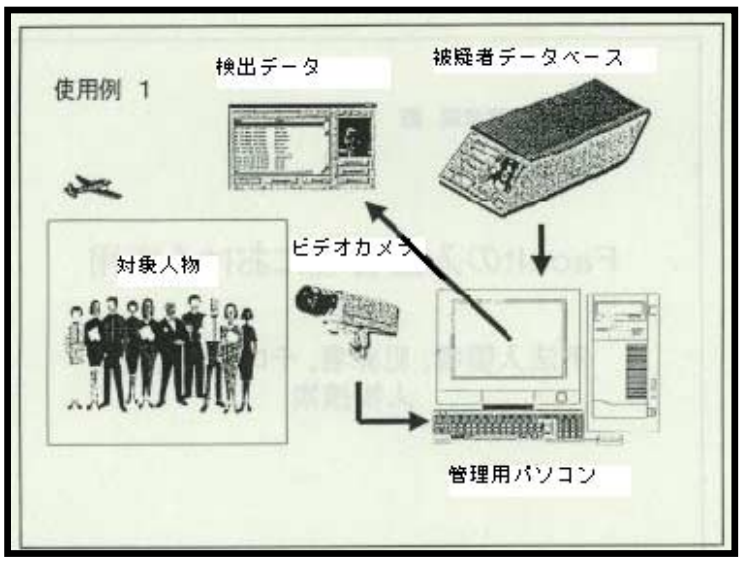

図 4.2 人物検索使用例 1

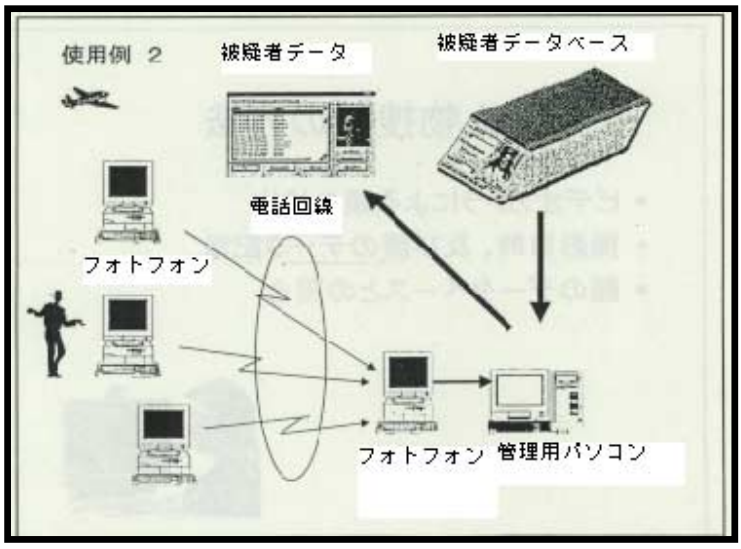

図 4.3　人物検索使用例 2

ここでの FaceIt Surveillance の機能は、カメラで捕らえたフレームから顔を検出して、時間データを付加して保存する。そして顔を検出したときに、特定人物かどうかの判断をリアルタイムで行う。そして FaceIt Database の機能として、顔写真データの検索を行い、静止画またはライブの画像との照合を行い、照合度合いの最も高い顔を検索する。また大量のデータベースから高速検索を行う。顔のデータベースへの

登録は、ビデオカメラからの撮影、ディジタルカメラ、スキャナなど他機の入力、他の画像データベースからの入力がある。これらは犯罪者、迷子、万引、テロリストなどの人物検索も同様に行える。

他にもテロリズム防止のための手荷物検査、国境入国審査の迅速化、入室、入館の安全管理、個人サービスとしての来客認証、コンピュータのセキュリティ管理などがある。

手荷物検査はマレーシア空港の例として、発券時スマートチップ搭乗券に顔を記録し、搭乗口で本人の照合を行い照合が確認されたら手荷物を飛行機に積み込むことで不審な荷物をチェックするものである。国境入国審査は US／メキシコ（米国法務省 SENTRI 計画）の例として、無線装置による登録車両の識別と FaceIt による人物照合を行い入国審査を迅速に行うものである。入室、入館の安全管理は、FaceIt を自動ドアに組み込むことでセキュリティ管理が行える。人物がカメラの前に立つと顔を照合して認証できるとドアが開くものである。これは、一般立入禁止の部屋、電算室、マンションなどに使われる。個人サービスとしての来客認証として、FaceIt により得意先人物を識別し、個別対応を行う。重要人物であれば特別のサービスが行える。店舗の入口、レジスタなどに置き個人サービスが行えるものである。コンピュータのセキュリティ管理では、ログイン時にパスワードの代わりに本人の顔で認証を行う。パスワードの盗難防止が行える。

これまでの容疑者のデータベース検索は、原文のエントリー（すなわち、名前、社会保障番号、出生日付など）に制限されていた。しかしながら、FaceIt は顔のイメージに対して検索を行うことによって即座に容疑者のアイデンティティについて確かめて、何百万もの記録についてすぐに、自動的に、確かな結果をもたらす。他のどんな技術もここまでの結果を残せない。

アイデンティティ詐欺は、アイデンティティ窃盗、架空や別の人物になりすましたりする。個人が想定されたアイデンティティの元で、多重ＩＤドキュメント（国家のＩＤものである運転免許証、パスポート、ビザなど）を受け取るとき、どんなフォームでもアイデンティティ詐欺は始まる。これは出生証明証などのドキュメントはほとんどの国で非常に見せかけやすいため、可能である。データベースには複製を防ぐために必要な情報である顔の写真がある。しかしながら、実際には人間が証明書などの写しを見つけるために何百万枚もの写真を探すのは不可能である。FaceIt はアイデンティティ詐欺をすぐに排除する。

また NewHam に導入されたあと犯罪総数は、34%減少しました。そのないようとして、住居への強盗が 72%減、店舗への侵入は 33%減、犯罪被害は 56%減、追いはぎは 26%減した。そして US Department of Defense（米国国防総省）、US Drug Enforcement Agency、US Customs（米国関税局）などが、導入をけんとうしている。

4.2　TrueFace 導入例

つぎに TrueFace の導入例について述べる。

まずは TrueFace ATM について、これはカード不要で、簡単な捜査、センター集中管理による高速処理、顔画像とともに取り扱い情報を記録する。300 台の ATM よって２百万枚のチェックを現金化した。４億ドル分のチェックを現金化しても不正はなかった。システム構成はセンター集中型で 24 時間、年中無休コールセンターである。クライアントはキャッシュディスペンサー＋Pentium PC により顔の特徴抽出データと JPEG 画像をセンターへ転送する。それは専用回線によるネットワーク接続されている。図 4.4 に顔認証データの流れを記す。

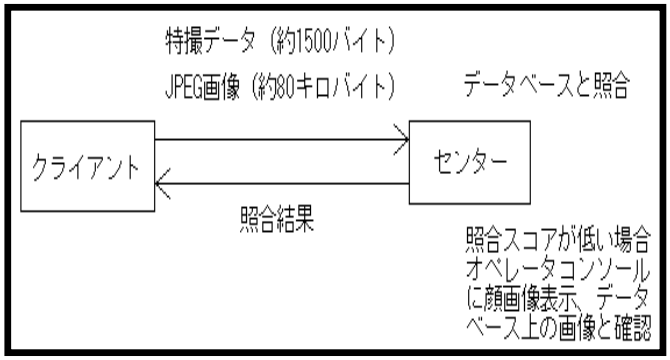

図 4.4 データの流れ

空港に導入されたものは、搭乗者の登録、搭乗者の照合、預け入れ荷物システムとのリンク、Frequent flyer（お得意様）プログラム、入退室管理、入出国管理、パスポート管理、犯罪者捜査、公共安全の目的で使用されている。そのセキュリティ概要は図 4.5 に示すようにまずチェックインのとき、タッチスクリーンを用いてチェックインスタッフが個々の搭乗者を画像と顔特徴データとともに入力する。そして搭乗者の顔写真データと TrueFace の特徴データを搭乗券に 2 次元バーコードで印刷する。その搭乗券をカードリーダに通して、ライブ画像と特徴データと比較し、顔写真を視覚で確認して大丈夫なら出発ゲートに通す。しかしながら、入力したデータがテロリストや出国禁止者ならば警戒発令を出す。

このほかにも FaceIt と同じく入退室管理、これはインドの石油精錬所で複数レーン、複数ゲートを作り、１日 1500 人の 3 交代性の従業員の正確な出退勤管理（不正撲滅）と警備員の削減のために使用している。イタリアの SIND 社、Tonali 社のワンマンパスゲート、銀行や宝石店では、重要施設への入退室ゲートに使用されている。

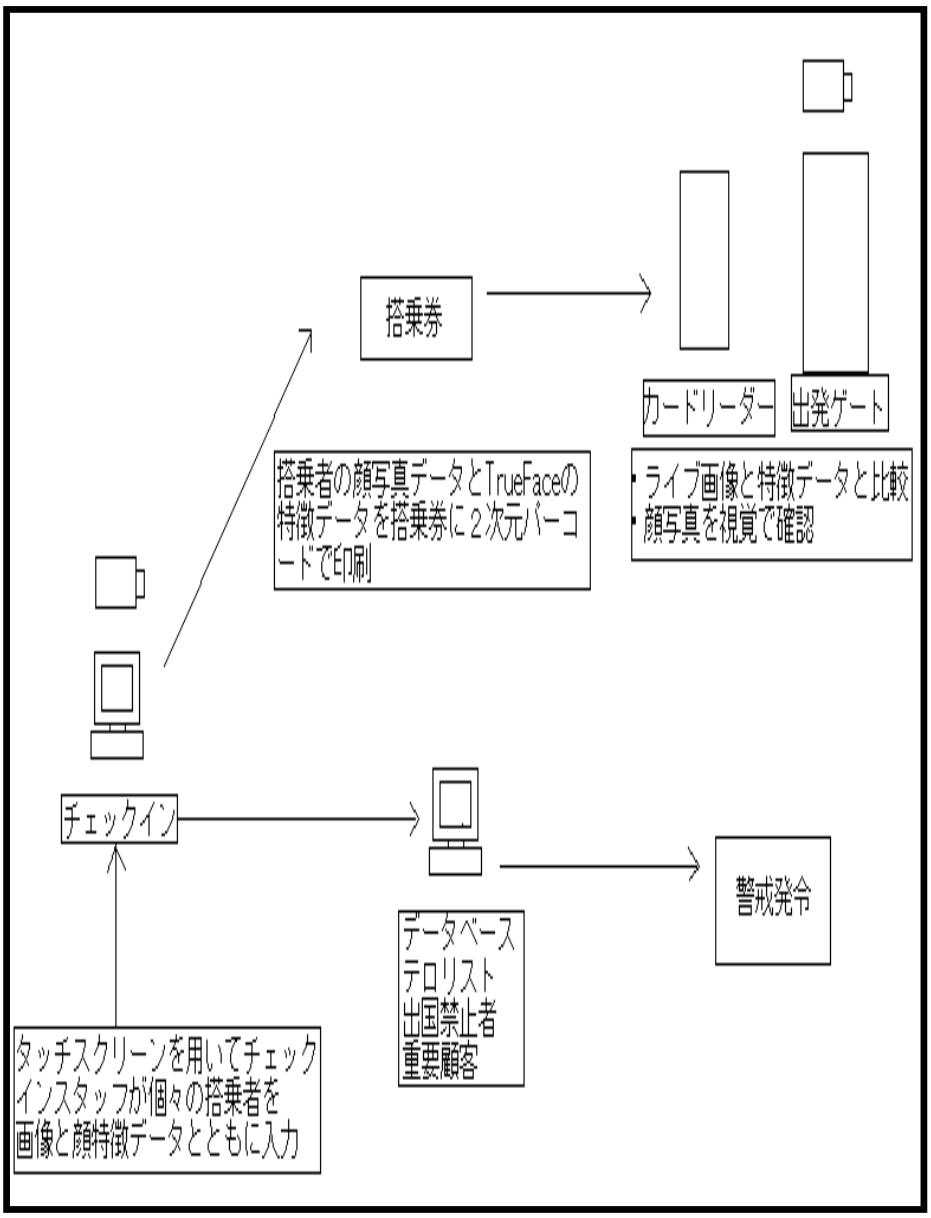

図 4.5　空港のセキュリティ概要

5 章　実験

本研究では FaceIt の精度の向上のために FaceIt PC を使い 2 つの実験を行う。1 つは写真を用いての個人認証である。2 つ目はカメラからの撮像角度を上下左右変えての個人認証である。

以下に FaceIt PC の登録から認証までの説明を述べる。

5.1　FaceIt PC の登録・認証

ここで FaceIt PC の登録から認証までの流れを説明する。

はじめにユーザの名前とオプション情報を入力したあと、図 5.1 に示すライブビデオが起動する。

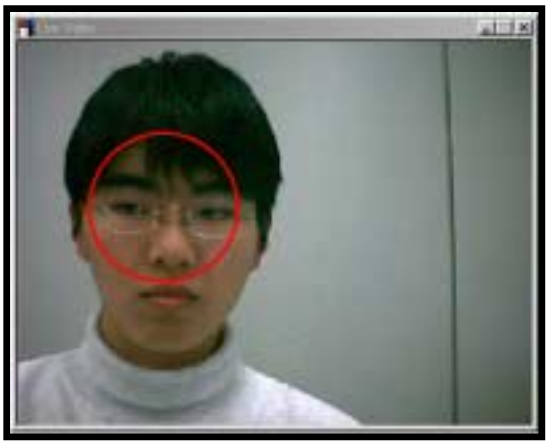

図 5.1　ライブビデオ

FaceIt が頭部を発見できることを確認するために、頭部を（まだ視野にない場合）視野に入れる。また上部や下部が切り取られていないようにする。FaceIt は、頭部を発見すると、赤い円で輪郭を描く。これで FaceIt が頭部を発見したことを確認できる。赤い円は、頭部の位置とスケールを示す。

登録には、ユーザ自身の良好な画像を 3 枚追加することが必要である。良好な写真とは、図 5.2 に示すように頭部全体を含み、垂直方向の傾きがほとんどないことをいう。FaceIt が、いろいろなポーズのユーザを認識できるようにするため、3 枚の画像を変化させる必要がある。最初の画像は、ユーザ・リストのメインの ID 画像としてシステムが使用する。自動的に取り込まれた画像が良好でない場合、[skip]を押すと図 5.3 に示すとおり FaceIt は別の画像を取り込む。3 枚の画像を追加すると登録作業のつぎの段階に進む。

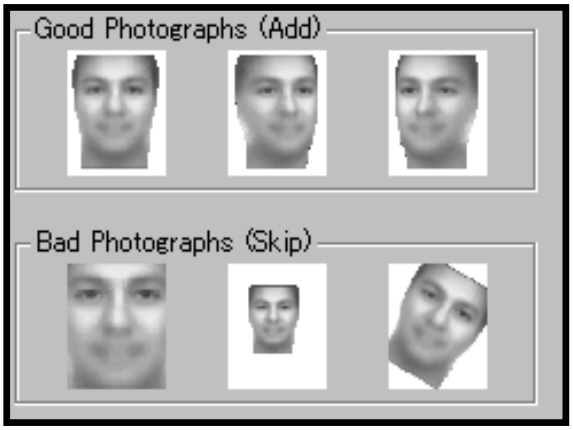

図 5.2　良好な写真、および不良の写真

図 5.3　画像の取り込み

なお FaceIt は図 5.4 に示すように目、鼻、口、額の相対位置関係を特徴量とする。

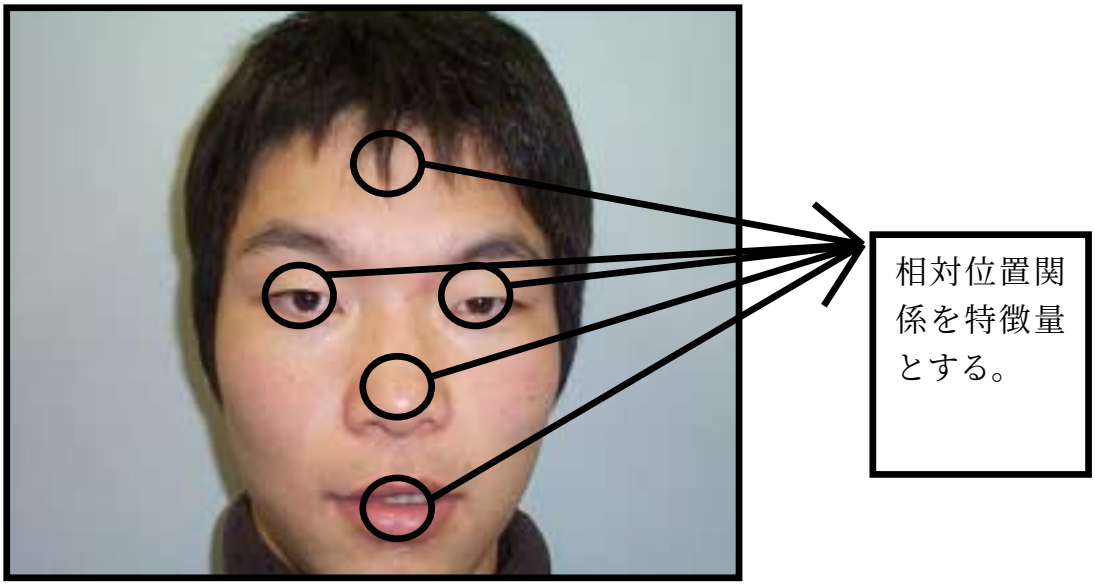

図 5.4　FaceIt の特徴抽出

つぎに、FaceIt は試験として図 5.5 に示すようにユーザの識別を確認する。これには最大４０秒かかかる。用意ができて、顔面が視野にあれば、[start]を押す。モニター上で違う領域を見たり顔を向けたりして、ポーズを変える。進行バーが試験の進み具合を表示する。FaceIt は、各方向のポーズで認識を試み、必要なら、顔面の特別な画像を追加したりして優れた認識レベルが得られるようにする。

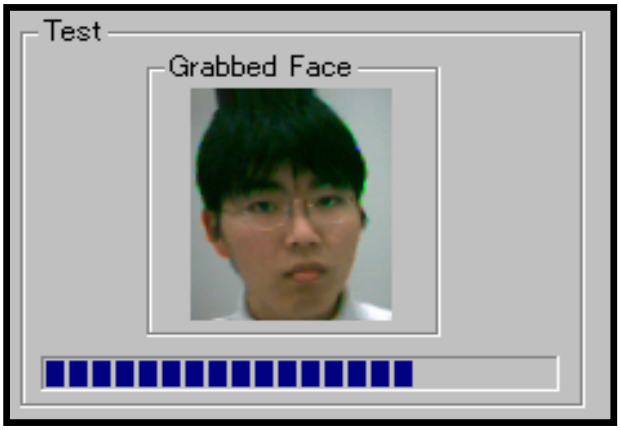

図 5.5　ユーザの識別確認

ユーザの識別確認時に各方向のポーズを多く取れば図 5.6 に示すように追加される画像は増える。

図 5.6　取り込まれた顔画像

著者が登録したときは上図のように 8 枚だったが多い人は 12 枚登録されている。また少ない人は 5 枚である。この登録画像は後に追加することもできる。

試験が終わると、[Finish]ボタンを押して画像を保存しなければならない。登録ウィザードが終了し、これで図 5.7 に示すようにユーザはシステムに完全に登録される

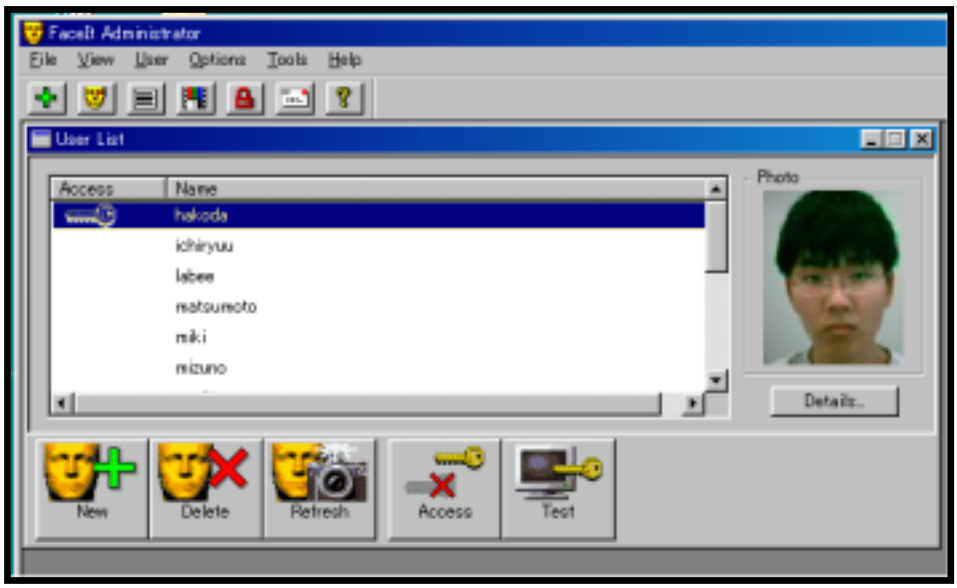

図 5.7　登録ユーザリスト

　ユーザリストの名前の横にあるキーがコンピュータにアクセスすることができることを示している。

　認証は図 5.7 のテストボタンをクリックすれば図 5.8 の画面になり、カメラの中に顔を入れれば、アクセスキーのついた者で下図のようにメーターの半分を超えグリーンになれば本人と認証される。

図 5.8　個人認証

5.2　写真による個人認証

ここでは、写真を用いての個人認証の実験を行う。FaceIt PC に登録されたデータベースと写真を比較して認証できるかを調べる。写真はデジタルカメラで撮影したものをプリントアウトした図 5.9 に示す写真を使用した。

図 5.9　実験用顔写真

これらの写真を通常の認証時のようにカメラの前に持っていき、少しでも 3 次元に見えるように動かして結果を見た。これは 30 秒を一区切りに 3 回ずつ認証する。使用した枚数は 5 枚である。図 5.10 は使用写真との比較対象として登録画像を示したものである。

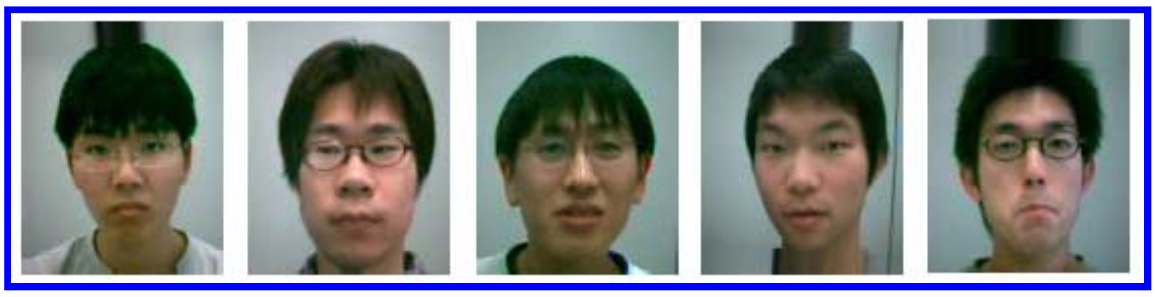

図 5.10　登録画像

結果は図 5.11 の 4 枚の写真は少しの反応はあったが、認証はされなかった。図 5.12 の 1 枚だけは認証できたが時間がかかりすぎた。このことから写真での認証はできにくいことが証明された。

図 5.11　認証不成功写真

図 5.12　認証成功写真

5.3　角度を変えての個人認証

続いて、撮像角度認証の調査としてカメラを固定して、カメラ正面を 0 度とし、図 5.13 に示すように顔の角度を変えて認証を実施した。人数は 5 人で、上下左右に 5 度ずつずらして、5 度から認証が不可能になるまで実施した。この実験の認証時間は最大 30 秒までとし、各角度で 3 回ずつ認証を行った。認証したときはそれを秒数で表し、反応は見せたが認証されなかった場合を△で、まったく反応しなかった場合を、バツで表記した。（表 5.1 参照）

図 5.13　撮像角度認証

結果として左右の 10 度くらいまでは普通に認証できるが、15 度くらいから少しずつ認証精度が落ちてくる。同じ角度内で認証したり、しなかったりするのは目線の移動、顔を動かしてしまい角度が小さくなる、カメラとの距離の問題がある。個人によって差が激しいのは、上下左右とも登録されている画像の差である。一人だけ上の角度の認証がいいのも登録されている画像に上を向いたものがあるからであるし、特に悪い認証結果のものは登録されている顔の数が 5 つと少ないためである。上下の角度は登録画像が少ないため、認証も 10 度くらいまでの認証結果が良い。特別な意識なく顔を登録した場合の認証は上下左右とも 10 度くらいまでが使えるものとなる。

表 5.1　実験結果

	左5度			左10度			左15度			左20度			左25度			左30度			左35度			左40度		
箱田	2s	1s	2s	1s	1s	2s	1s	2s	1s	3s	2s	3s	△	△	△	×	×	×	×	×	×	×	×	×
内田	1s	1s	1s	4s	3s	1s	2s	1s	13s	△	1s	5s	×	×	×	×	×	×	×	×	×	×	×	×
中原	1s	1s	1s	1s	1s	1s	3s	12s	3s	4s	5s	1s	6s	2s	7s	6s	14s	5s	△	△	△	×	×	×
長尾	1s	1s	1s	1s	1s	1s	1s	1s	1s	2s	1s	1s	3s	2s	4s	13s	6s	9s	△	△	△	×	×	×
佐伯	1s	1s	1s	1s	1s	1s	1s	1s	1s	△	18s	2s	7s	2s	△	×	×	×	×	×	×	×	×	×

	右5度			右10度			右15度			右20度			右25度			右30度			右35度			右40度		
箱田	1s	1s	1s	1s	2s	1s	2s	2s	3s	2s	3s	3s	△	△	△	×	×	×	×	×	×	×	×	×
内田	1s	1s	1s	4s	1s	15s	16s	△	△	△	△	△	×	×	×	×	×	×	×	×	×	×	×	×
中原	1s	1s	1s	1s	1s	1s	1s	1s	1s	4s	2s	1s	1s	1s	1s	1s	5s	1s	△	21s	4s	△	△	△
長尾	1s	1s	1s	1s	1s	1s	1s	1s	4s	1s	△	10s	△	△	△	×	×	×	×	×	×	×	×	×
佐伯	1s	1s	1s	1s	1s	1s	2s	7s	1s	△	28s	25s	×	△	△	×	×	×	×	×	×	×	×	×

	下5度			下10度			下15度			下20度			下25度			下30度			下35度			下40度		
箱田	1s	1s	1s	1s	2s	2s	2s	2s	4s	△	△	△	×	×	×	×	×	×	×	×	×	×	×	×
内田	1s	2s	29s	15s	25s	2s	△	△	1s	1s	2s	1s	×	×	×	×	×	×	×	×	×	×	×	×
中原	2s	1s	3s	1s	1s	1s	1s	1s	4s	1s	11s	△	△	△	△	×	×	×	×	×	×	×	×	×
長尾	1s	1s	1s	△	△	△	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
佐伯	△	6s	1s	△	16s	△	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×

	上5度			上10度			上15度			上20度			上25度			上30度			上35度			上40度		
箱田	1s	1s	1s	1s	2s	2s	7s	△	10s	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
内田	1s	1s	1s	10s	7s	2s	△	△	△	×	△	×	×	×	×	×	×	×	×	×	×	×	×	×
中原	1s	1s	1s	1s	1s	1s	1s	1s	6s	1s	△	18s	1s	1s	5s	△	×	×	×	×	×	×	×	×
長尾	1s	1s	1s	1s	1s	1s	1s	1s	1s	1s	4s	4s	4s	1s	8s	2s	1s	4s	△	10s	△	×	×	×
佐伯	1s	1s	1s	×	×	△	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×

5.4　考察

実験の結果を見ると、一つ目の実験で、写真は普通にカメラに見せただけでは認証ができなかった。写真での認証は決して不可能ではないが生体情報でないためかなり難しい。カラー写真で 3 次元に見えるようにもっていけば認証できないこともない。また白黒写真でも登録された画像に近ければ認証できないことはないが。表情の変化や向きが異なれば認証はできないため実用性はあまりない。二つ目の撮像角度の検証では、角度は 10 度くらいまでだと問題なく認証可能である。15 度を超えると、だんだんと認証に時間がかかったり、反応のみとなり認証まではいかない。高角度まで認証できた者は、登録画像に高角度のものがあるためである。すなわち登録時に多くの画像を取り込めば 35 度くらいまでは認証が可能である。ただこれ以上の角度は両目を中心に顔を捕らえるため、目が見えにくくなるので登録もできない。

この実験中に判明したことで正確ではないが表情を変化させても認証にはあまり

支障はないことが判明した。しかしながら、口を開けっ放しの状態では認識はできない。また、登録画像では髪の毛が眉や目にかかっていないのに、髪が伸びて眉や目にかかるようだと認識精度は落ちる。ただこれは目の回りから髪の毛を除けばよいためあまり問題にならない。結論としては登録画像さえしっかりしていれば、認証精度はかなり高いものであることが判明した。

6 章　まとめ

本論文では、バイオメトリクスの 1 つである顔を用いた個人認証にスポットをあて顔画像の認証についての研究を行ってきた。顔認識の精度向上のために顔認識ソフトウェアの 1 つである FaceIt PC を用いてその基本性能および撮像パラメータの一つである撮像角度の性能について確認した。デジタルカメラで撮影した写真での認証精度は、写真は生体情報でないため認証はほとんどされず、認証できた写真でも偶発的なものであったと考えられる。撮像角度の性能検証は、正面を向いた顔画像は 100％成功し、誤認証もない。上下左右とも 15 度くらいからは認証精度は低下するが、正面に近い顔画像ほど認証率は高いことが証明された。しかしながら、個人の認証率にばらつきがあり登録画像に問題があることも判明した。このことは顔画像の登録時になるべく多くの画像を取り込むことで解決する。

また類似したソフトウェアで、TrueFace と呼ばれるものについても比較対象としてあげた。このソフトも世界で ATM、入退室管理、出退勤管理などに使用され、豊富な納入実績があり高い信頼性を誇っている。性能も高い。

FaceIt や TrueFace はその高い認証精度から今後も多種多様なものに利用されることが考えられる。

7 章　謝辞

最後に一年間にわたり本研究にご指導御協力頂いた竹田史章先生に厚く御礼申し上げる。

8 章　参考文献

(1) 南： 顔の識別技術；計測と制御、Vol.25、No.8、pp.707-713 (1986)

(2) J-C. Terrillon, M.David and S. Akamatsu： Automatic detection of human face in natural scene images by use of a skin color model and of invariant moments; Proc. of FG'98, pp. 112-117 (1998)

(3) T. Kurata, D.D. Chang, and S. Hashimoto： Multimedia sensing system for robot; Proc. of ROMAN'95, pp. 164-169 (1995)

(4) T. Yokoyama, Y. Yagi and M. Yachida： Facial contour extraction model; Proc. of FG'98, pp.254-259 (1998)

(5) 赤松, 佐々木, 深町, 末松： 濃淡画像マッチングによるロバストな正面の識別法－フーリエスペクトルの KL 展開の応用－; 信学論(D-Ⅱ), Vol. J76-D-Ⅱ, No.7, pp. 1363-1373 (1993)

(6) J. Heinzmann and A. Zelinsky： 3D facial pos and gaze point estimation using a robust real-time tracking paradigm; Proc. of FG'98, pp.142-147 (1998)

(7) R. Cipolla and A. Pentland, eds.： Computer Vision for Human-Machine Interaction, Cambridge Univ. Press (1998)

(8) 渡辺, 榊原, 谷内田： インタラクティブモデル構築による複雑環境下での実時間ジェスチャ認識：電気学会論文誌, Vol.119-D, No.1, pp.21-29 (1999)

(9) 谷内田： ロボットビジョン, 昭晃堂 (1990)

(10) 谷内田, 岩井： インタラクションのための人物動作解析と認識; 信学技報, PRMU99-55 (1999-11)

(11) H.Wu, Q. Chien and M. Uachida： Face detection from color images using fuzzy pattern matching method; IEEE Trans. Pattern Analysis and Machine Intelligence, Vol. 10, No. 6 (1999)

(12) 渡辺, 谷内田：複数入力画像の固有空間法による実時間ジェスチャ認識; 電子情報通信学会論文誌, Vol. J81-D-Ⅱ, No. 5, pp. 810-921 (1998)

(13) 青木, 久富, 橋本：分散強調処理を用いたロバストな能動的人物追跡システム; 画像電子学会誌, Vol. 28, No. 5, pp. 596-604 (1999)