広島県立総合技術研究所東部工業技術センター研究報告　No.22 p.14-18 (2009)
技術報文(4)

# インターネットを利用した産業機械の遠隔診断に必要な通信技術の開発

## 高画素イメージセンサを使った虹彩認証システム

廣川勝久，門藤至宏

# Industrial Machine Diagnosis over Firewall Networks

## Authentication System Using Iris Code Obtained from High-Resolution Image Sensor

HIROKAWA Katsuhisa and MONDO Munehiro

The principal parameters of Daugman's algorithm [U.S. Patent No. 5, 291, 560, 1 March (1994)] generating iris codes for the biometric authentication are clarified. We experimentally demonstrated that the authentication system using the clarified parameters completely discriminates iris patterns captured from several persons. To obtain the iris patterns, a high-resolution image sensor captures a whole face image and detects an eye. The process of iris code generation from the iris pattern of an eye is described in detail.

高精細イメージセンサが撮影した顔全体の画像から，瞳を検出し，虹彩画像を切り出して個人認証を行う生体認証システムを開発した。認証には，人の虹彩画像から生成したデジタル符号コードを認証データとして用いる。このデジタル符号コードを得るために，J. G. Daugman のアルゴリズムを使用した。しかし，符号化アルゴリズムを適用する場合，パラメータの一部が未公開であるため，プログラム化にあたり，実際の画像を使用して認証を行いパラメータを明らかにした。実験では，その解明したパラーメータを使って符号化した数人の虹彩コードから，他人の虹彩コードと本人の虹彩コードとの識別が可能であることが確認できた。

キーワード：個人認証，バイオメトリクス，虹彩，符号化，生体認証

## 1. 緒　　言

製造業では，グローバル化に伴い，厳しい納期短縮・コスト削減要求に対応するために製造機械の稼働率向上が求められている。そのため，稼動率に直結する保守・メンテナンスサービスを，安価・広域・高速化するインターネットの利点を活かしたネットワーク接続によって迅速に行う方法が考えられている。このような遠隔操作による診断・保守では，製造機械の稼働率や生産能力などの生産情報が外部に流出しないようなセキュリティ対策が必要とされる。

我々は，これまでの研究により，ネットワークのセキュリティを確保しながら生産機械の遠隔診断を行うシステムの開発を行った。本報告では，さらに，機械操作や遠隔診断するオペレータのセキュリティを確保するための生体認証システムについて述べる。生体認証には，指紋や音声など様々な本人しか持ち得ない生体情報が鍵として利用されている。生体情報を鍵として用いる利点は，パスワードのように忘れてしまうことがなく，鍵のように紛失することやコピーされることがないなどの点が挙げられる。このような生体認証の中でも，特に虹彩認証は，非常に高い認証精度を備えている。工場などの汚れや騒音の中で，製造機器のメンテナンスを行う場合，指紋認証では手袋や手の汚れなどの問題があり，音声も騒音環境下では利用できない。このような諸問題を勘案すると，虹彩認証は，汚れの影響を受けにくく，また，両手が塞がった状態でも，非接触に認証が可能であることから，工場内での利用に最適であると考えられる。本稿では，このような工場内の製造機械を遠隔に診断するために利用可能な生体認証装置として研究を行った虹彩認証システムについて報告する。

2009.5.15 受理　加工技術研究部

## 2. 虹彩認証アルゴリズム

### 2.1 虹彩認証処理のフロー

図 1 は，虹彩認証を行う場合の，プログラムの流れを示す。まず，虹彩認証の処理の流れについて簡単に述べる。虹彩を用いた生体認証を行う場合，イメージセンサが捕らえた眼球の画像の中から，認証に必要な虹彩の画像部分を切り出すために，瞳孔との境界と白目と黒目の境界を検出する。次に，ドーナツ状に切り出された虹彩の画像を矩形の帯状に展開する。矩形になった画像を，さらに横 128 個，縦 8 個の小さな矩形に分割する。この分割された画像から，デジタル符号化処理を行い，2048

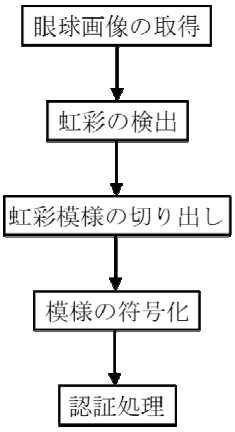



図１　虹彩認証処理のフローチャート

ビットの個人認証コードを生成する。最後に，このデータと認証したい個人のデータとの照合を行う。次節以降から，これら個別の処理について，さらに詳しく述べる。

## 2.2 虹彩の検出

虹彩から認証に必要な符号化データを得るためには，顔全体の画像から眼球付近の画像を切り出した後に，虹彩の範囲を検出する必要がある。しかし，**図 2** に示すように，虹彩がまぶたに覆われている場合などがあり，虹彩の境を検出するためには，不完全な円を検出する必要がある。そこで，虹彩と瞳の輪郭を検出するアルゴリズムとして Hough 変換を用いた。**図 2** は，プログラム開発環境 Xcode に画像処理用ライブラリー OpenCV を組み込み，Hough 変換が検出した円と虹彩の画像を重ねあわせたものを示す。Hough 変換は不完全な円でも検出することができるため，瞼が虹彩に重なった場合にも虹彩の外周が検出可能である。

## 2.3 線形補完による直交座標変換

符号化アルゴリズムを適応する前に，検出された円形の虹彩画像を極座標から直交座標に変換する。この時，計算に必要な極座標は，かならずしも対応する画素の中心でないため，回りの画素から線形補完によってその画素値を計算する。線形補完では，極座標とその回りの４画素をとの距離に反比例するように各画素に重み付けを行なった後に，重み付けされた各画素をたし合わせたものをその座標の画素値とした。**図 3** は，**図 2** から線形補間法により直交座標に変換した虹彩の画像を示す。矩形の画像は，横 800 画素，縦 90 画素から構成されており，それぞれが極座標における角度と原点からの距離に対応している。

## 2.4 符号化アルゴリズムとパラメータ

虹彩認証では，虹彩画像から認証に必要な各個人に特有な生体認証コードを生成する必要がある。現在虹彩認証で用いられるこのコードを生成するアルゴリズムは J. G. Daugman によって提案された [1,2,3]。このアルゴリズムを用いた虹彩認証は，現在，他の指紋や音声などと

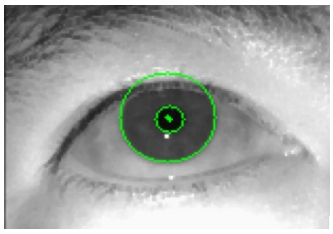


図 2　Hough 変換による虹彩の検出

図 3　線形補完により直交展開した虹彩画像

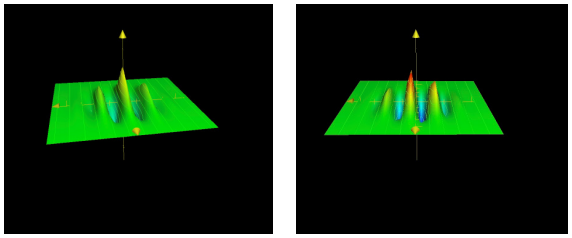
比較して，最も安全性が高い。次式はこの符号化アルゴリズムの演算カーネルを示したものである。

$$W(r,\theta)=e^{-i\omega(\theta_0-\theta)}e^{-\left[(r_0-r)^2/\alpha^2+(\theta_0-\theta)^2/\beta^2\right]} \quad (1)$$

認証コードを生成するアルゴリズムの演算カーネルには Gabor のウェーブレット関数を用いている。この関数は複素関数であり，実数部は Y 軸の面を中心とした偶関数となり，また虚数部が Y 軸の原点を中心とした奇関数である。**(図 4)** いま，入力の虹彩画像を I(r, θ)とすると符号化の演算は（２）式のような

$$h_{\{\mathrm{Re,Im}\}}=\mathrm{sgn}_{\{\mathrm{Re,Im}\}}\iint I(r,\theta)W(r,\theta)drd\theta \quad (2)$$

入力画像とウェーブレット関数の相関演算として記述できる。ウェーブレット関数をフーリエ変換した場合，直流成分を持たないことが知られている。このことは，(２)式の演算では，入力画像の明るさが演算に影響を与えないことを意味する。従って Gabor のウェーブレット関数を用いることにより，虹彩認証では明るさなどの外乱の影響を受けない安定した画像処理アルゴリズムであると言える。符号化時は，実数部と虚数部のそれぞれの正負の値から２ビットの認証コードを決定する。すなわち，**図 5** に示すように実数部の符号が正の場合１とし，負の場合０とする。同様に，虚数部においても値を決定し，２ビットの符号化コード生成する。この計算を($r_0$, θ)の各座標で行うことにより，2048 ビットの個人認証用のコードを作ることができる。



(a)　　(b)

図 4　演算カーネルの(a)実数部と(b)虚数部

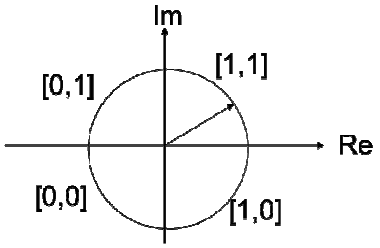



図 5　演算結果とデジタル符号化の関係

### 2.5 ハミング距離を使った認証

個人の認証には，生成された認証コードを用いて，記憶済みの個人コードとのハミング距離を計算することにより個人の照合を行う。ハミング距離は２つのコードが似ている場合短くなり，異なる場合長くなる。次式は，ハミング距離の計算を式で表したものである。個人 A のコード(CodeA)と個人 B のコード(CodeB)の XOR を計算することによって，不一致のビットのみが残る。この残りビットの数がハミング距離となる。

$$HD = \frac{\left\| (codeA \otimes codeB) \cap maskA \cap maskB \right\|}{\left\| maskA \cap maskB \right\|} \qquad (3)$$

Q⊗　$XOR$

この時，マスク用のコード(maskA，maskB)を用いて演算に使うことができる有効部分にビットを立て，不要なビット部分の演算を行わない。また，（3）式の分母は，有効ビット数の違いにより距離に差が生じるため，有効なビット数で規格化するためのものである。

## 3. 実験と結果

### 3.1 眼球を検出するためのハードウェア

これまでに市販されている虹彩認証の装置は，顔全体を撮影し，眼球を検出するイメージセンサと，検出された眼球位置にイメージセンサ方向を合わせ拡大した画像を撮影するためのイメージセンサを備えた大規模なものが多かった。我々の認証システムでは，１個のイメージセンサの画素数を３万画素程度に増やし，顔全体の画像から，眼球の位置をハードウェアにより検出・追跡する方法により，小型化・低価格化を図った。

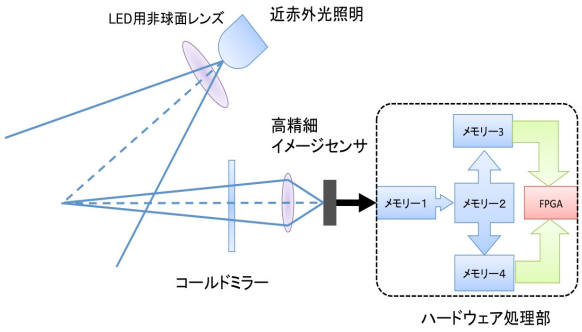


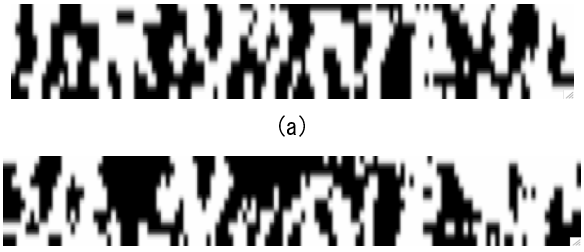

図 6　システムの概念図

虹彩の画像をイメージセンサにより取得する場合，日本人のような黄色人種の虹彩部分には色素が多く含まれおり，カラーイメージセンサにより，虹彩を撮影することは困難である。そのため，実験では，虹彩を撮影するための光源として図 6 に示すような近赤外光 LED 照明を用いた。この時の照明用 LED の発光波長はλ=735nm である。また，一般的な LED 照明の照度分布は，中心部が明るく周辺に部分は暗いという特性がある。本研究では，１個の LED のみで顔全体を均一に照明するために，LED の前に LED 照明用に開発された非球面レンズを採用した。また，イメージセンサが可視光の外乱を受けることなく，近赤外光のみを透過するように，イメージセンサの前にコールドミラーを置いた。コールドミラーの採用することにより，ミラーに目が映るため，目の位置や開いた状態を確認しやすいと言った副次的な効果もある。システムでは，眼球の検出に，高精細のイメージセンサにより顔全体を撮像する構成とした。撮像後，FPGA を用いたハードウェア処理により，全体の画像の中からリアルタイムに眼球を検出することができる。また，瞳位置をハードウェアで追跡し，瞳孔を中心として 160×120 画素の範囲を切り出し，虹彩認証用の入力画像として用いる。

### 3.2 符号化に必要なパラメータの決定

イメージセンサから得られた虹彩の画像から直交変換を使って矩形の画像データを作る必要がある。Daugman の論文では，虹彩部分を８個の同心円に分割すると述べられているが，計算に必要な画素数（サンプリングの点数）や(1)式のα，β，ωなどのウェーブレット関数の周期や大きさを決めるパラメータなどについて不明な点がある[1,2]。実験では，これらのパラメータを，実際の認証結果と比較しながら明らかにした。また，これらのパラメータを決定するに当たり，W.A. Barret[4]が Daugman の特許資料から検討したパラメータの値についても参考に最終的なパラメータを決定した。

まず，128×8 のエリアに分割した場合のエリア１個当



(a)

(b)

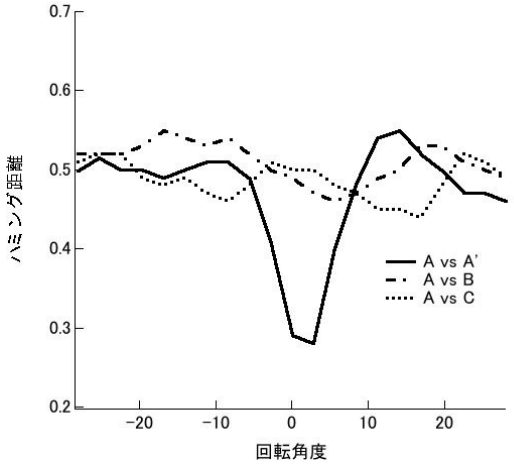
**図７　デジタル化された認証コード(a)実数部(b)虚数部**

たりの大きさは 7×13 画素とした。これにより，矩形の総画素数は 896×104 画素となる。次にωの周期は 7 画素とした。これには，まず Daugman の説明では利用する矩形の範囲は X 軸方向にウェーブレットの周期の３オクターブ分との記述があり，また Barrat では X 軸方向と Y 軸方向の大きさの比は 4:1 とされている点を考慮した結果である。従って，この両方の条件を満たすためには，ωの周期は 7 画素とし，X 軸方向に８個 Y 軸方向に１個分の矩形を使って（２）式の２ビットの計算を行うことになる。ただし，計算にあたり， Gabor のウェーブレット関数は８個分の矩形エリアに限定されるため，計算には簡単な調整が必要となる。一般的にウェーブレット関数は無限遠まで計算することを想定している。これを有限の範囲のみで計算した場合，問題が発生する。Gabor ウェーブレット関数の虚数部は奇関数であるため，有限の範囲であっても正負の範囲が同じであれば，その範囲で関数を積分した値は０となる。しかし，実数部は偶関数であるため，積分の範囲を変化させると積分値が変化してしまう。これは，認証アルゴリズムにおいても，画像の明るさが計算結果に影響を与えることになる。そこで，今回の計算では，実数部については，積分する範囲内で，関数のみの積分値を計算し，あらかじめ，その値だけオフセット値を与えた。これにより，画像の明るさの影響を排除することができた。

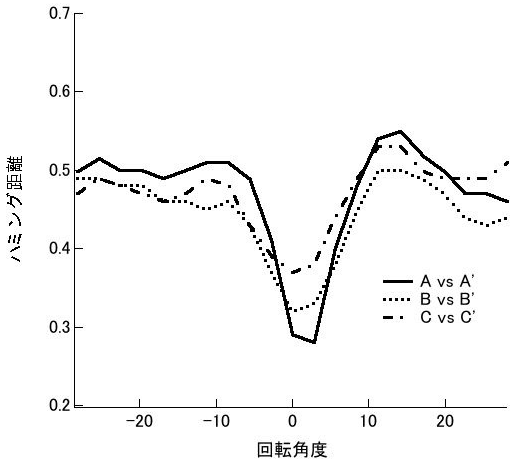
βのパラメータについては，詳細な記述は無く認証実験によりパラメータの値を決定した。βの値が小さい場合，非常に狭い範囲の画素のみが計算に影響する。逆に，βの値を大きくすると，広範囲の画素の影響を受けるため，計算後の個人コードにおいて，隣り合ったビットが同じような値をとる可能性がある。今回βについては，7, 14, 28 画素の値を使って実験したが，実際に認証データとして利用できるのはβ=7 画素の場合のみであった。αについては，α方向に画像に変化は少なく，使用画素数も少ないため計算結果に影響しないことからα=7画素とした。**図 7(a), (b)**は虹彩の画像から最終的に符号化した認証コードの実数部と虚数部を示す。

### 3.3 認証実験

認証アルゴリズムに必要なパラメータが推定できたので，このパラメータを使って，実際の認証の判定を行うためのハミング距離を調べた。まず，３人の被験者から




(a)




(b)

**図８　(a)本人と他人とのハミング距離**
**(b)本人のハミング距離の個人差**

それぞれ２枚の異なる時間に撮影した虹彩画像を使用した。次に，これら６枚の虹彩画像から６種類の認証コードを生成した。

はじめに，本人と他人とを判定するために，被験者 A に対して，被験者 A のもう一つの認証コードと被験者 B，被験者 C の認証コードとのハミング距離を計算した。この時，頭の傾きなどが，虹彩画像の回転に与える影響を調べるため-28° から 28° の角度の異なる認証コードのハミング距離を計算した。**図 8(a)**にその結果を示す。縦軸がハミング距離，横軸が，虹彩の回転角度を示す。認証コードは，０または１の１ビットデータであるため，全くランダムに値を割り付けた認証コードに対してもハミング距離は 50%程度一致する。したがって，被験者 A に対して B, C のハミング距離は 0.5 程度であることから，いかなる回転角度でも被験者 A のコードとは全く一致していないことがわかる。また，被験者 A’ の場合は，0° 付近でハミング距離が小さくなっているため，他の２人の被験者とは数値的に分離可能となり識別できる。また，回転角度については，±3° 程度の範囲内でハミング距離

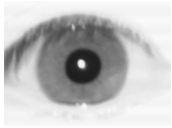


図９　まつげが虹彩に被った入力画像

が最低値をとり，それ以上の角度では全く一致しない。したがって,実際に認証システムとして利用する場合は,虹彩の回転については,考慮する必要は無いと思われる。

次に，本人の異なる虹彩画像から生成した二つの認証コードを使ってハミング距離を計算し，その個人差を見た。**図 8(b)**はその結果を示す。ハミング距離の最低値については，個人差が見られる。虹彩の回転角度については，個人差は無く，どの被験者についても±3° 程度の範囲内でハミング距離が最も低い値を取った。これらの計算のなかで，被験者 B，C には，**図 9** に示すようなまつげが虹彩に被さった画像も入力画像として用いており，まつげ部分も認証コードに含んで計算を行った。このため，まつげ部分については認証コードが一致せずハミング距離が長くなったと考えられる。

最後に被験者 A,B,C の認証コードにそれぞれ被験者 A’,B’,C’ の認証コードを入力した場合のハミング距離を**表 1** にしめす。どの被験者の場合においても，被験者本人の認証コードを入力した時に,最も小さい値を取り,他人の認証コードでは，0.5 付近の値となった。このことから，最低値となる認証コードから，特定の個人を認証・識別することができると考えられる。

表１　３人の被験者からのハミング距離

| | A | B | C |
|---|---|---|---|
| A’ | 0.29 | 0.49 | 0.51 |
| B’ | 0.44 | 0.32 | 0.45 |
| C’ | 0.48 | 0.46 | 0.37 |

## 4. 結　　言

高精細のイメージセンサが撮影した顔全体の画像から，虹彩画像を切り出して個人認証を行う生体認証システムを開発した。システムでは J. G. Daugman のアルゴリズムを使用し虹彩画像から認証に必要なデジタル符号データを生成した。符号化アルゴリズムを適用するにあたり，実際の画像を使用して認証を行いアルゴリズムの不明パラメータを明らかにした。最後に，そのアルゴリズムを適用した数人の虹彩コードから，他人の虹彩コードと本人の虹彩コードとの識別が可能であることを実験により確認した。

本研究では，眼球の検出を高速化する方法として FPGA にハードウェア処理を用いたが，処理時間は撮像素子の入力・転送速度により制限されている。そのため，より実用的な認証システムとするためには，最初に顔全体を撮像し，眼球の位置を検出した後は，撮像素子の中から眼球のエリアの画素のみを入力・転送することが可能な高速画像入力ハードウェアの開発が必要である[5]。

## 謝　　辞

研究を推進するにあたり，(株) システムアートウェアの森合雅朗氏，大亀勝久氏には虹彩認証用のハードウェアについてご協力いただきました。この場を借りて深謝いたします。

## 文　　献

1) J. G. Daugman, ‘High Confidence Visual Recognition of Persons by a Test of Statistical Independence’, IEEE Trans., **15**(11), 1148-1161 (1993).
2) J. G. Daugman, ‘How Iris Recognition Works’, IEEE Trans., **14**(1), 21-30 (2004).
3) John Daugman, ‘Biometric personal identification system based on iris analysis’, U.S. Patent No. 5, 291, 560, 1 March (1994).
4) http://www.engr.sjsu.edu/wbarrett/.
5) Ashit Talukder, John-Michael Morookian, Steve Monacos, Raymond Lam, Clayton LeBaw, and James L. Lambert ‘Eye-tracking architecture for biometrics and remote monitoring’, Appl. Opt., **44** (5), 693-700 (2005).