SCIS 2008 The 2008 Symposium on Cryptography and Information Security
Miyazaki, Japan, Jan. 22-25, 2008
The Institute of Electronics, Information and Communication Engineers

虹彩認証におけるウルフ攻撃確率の理論的考察

A Theoretical Study on Wolf Attack Probability in Iris-pattern Recognition Systems

小島 由大* 繁富 利恵*† 美添 一樹* 井沼 学†
Yoshihiro Kojima Rie Shigetomi Kazuki Yoshizoe Manabu Inuma
大塚 玲*† 今井 秀樹*†
Akira Otsuka Hideki Imai

あらまし 本論文では，虹彩認証アルゴリズムに対するウルフ攻撃確率を検討する．虹彩認証アルゴリズムについても従来法には強力なウルフ攻撃が存在するが，近年，Daugman が提案した正規化法は，取得したアイリスコードがまぶた等に隠れた部分のマスク処理によって短くなっている場合でも，適切に閾値を調整することで FAR を一定に抑える機能を有しており，これが虹彩認証アルゴリズムのウルフ攻撃耐性を高める目的にも有効に働いている．しかし，虹彩の領域を半径方向や円周方向に制限したり，周波数成分ごとにアイリスコードを分割する等のエントロピー分布を考慮したウルフ攻撃を調査した結果，虹彩領域を半径方向に制限し，かつ低周波成分以外をマスクした場合に強力なウルフが存在し，Daugman の正規化法により設定した FAR 値 (10^{-6}) を大幅に上回るウルフ攻撃確率 (10^{-3}) が得られることが示された．

キーワード 生体認証，ウルフ，ウルフ攻撃確率，虹彩認証，アイリスコード

1 はじめに

近年，生体認証システムが金融機関・入国審査・入退室管理等の個人認証において広く使われている．現在，生体認証システムのセキュリティを評価する場合、他人受け入れ率（FAR）や本人拒否率（FRR）で評価されている．

しかし，生体認証システムのセキュリティ評価にはウルフ攻撃確率も検討しなくてはならない．ウルフとは，生体認証システムにおいて複数のテンプレートに対して一致と誤判定される入力情報のことであり，そのウルフのテンプレートに対するなりすましが成功する最大確率がウルフ攻撃確率 WAP である．

WAP は，ある 1 つのウルフが高い確率で攻撃に成功する場合，高い値となる．それに対して，生体認証システムのセキュリティの評価によく使われている FAR は，多くの入力情報を使って誤認証の確率を求めているため，ある 1 つの入力情報がウルフであっても入力情報の数で平均をとってしまい小さな値となる．つまり FAR のみでは，ウルフ攻撃の耐性を評価することができない．そのため，WAP でセキュリティの評価をして WAP を十分に小さく抑えることが大切である．指静脈認証パターン認証アルゴリズムや指紋認証アルゴリズムの主流であるマニューシャ・マッチングアルゴリズムに対して，それぞれ [2] や [3] でウルフが発見されている．

しかし，虹彩認証におけるウルフの存在はまだ検討されておらず，WAP の評価がされていない．本稿では，虹彩認証におけるウルフ攻撃確率を理論的に考察する．

虹彩認証については，近年，Daugman[5] によりまぶた等で虹彩の大半が隠れているような状況においても FAR を一定に保つための正規化法が取り入れられている．

Daugman の正規化法は，まぶた等で隠れている領域を取り除いた後のアイリスコードの長さに応じて，しきい値を適切に調整することで FAR を常に一定に保つ．これは，まず大量のサンプルを用いてアイリスコード間の

* 〒 112-8551 東京都文京区春日 1-13-27 中央大学理工学部電気電子情報通信工学科今井研究室 Imai Lab., Dept. of Electrical, Electronic, and Communication Engineering, Faculty of Science and Engineering, Chuo University 1-13-27 Kasuga, Bunkyo-ku Tokyo 112-8551, Japan E-mail: {yoshihiro-kojima,k-yoshizoe}@imailab.jp
† 〒 101-0021 東京都千代田区外神田 1-18-13 秋葉原ダイビル 1102 号室 産業技術総合研究所 情報セキュリティ研究センター Research Center for Information Security, National Institute of Advanced Industrial Science and Technology 1-18-13 Sotokanda Chiyoda-ku Tokyo 101-0021,Japan E-mail: {rie-shigetomi,manabu-inuma,a-otsuka,h-imai}@aist.go.jp

正規化ハミング距離（ハミング距離をコード長で除した値）の分布を求め，しきい値以下のアイリスコードが出現する確率が指定した FAR 値になるようにしきい値を設定する．次に，取得したアイリスコードの符号長が平均値より短い（長い）際に，先の分布を二項分布と仮定した時の自由度も符号長に比例して変化すると仮定することで，新たな符号長に対応した分布を求め，FAR に対応したしきい値を決定している．

このような正規化を行わない，従来の虹彩認証アルゴリズムでは，まぶた等に隠れている領域を限界まで増やすことで容易に強力なウルフを構成することができたが，この正規化を施したことによってウルフ攻撃に対しても良い耐性が実現されている．

しかし，Daugman[5] は，前述のように取得したアイリスコードの符号長に比例して二項分布の自由度が変化する仮定を置いているため，マスク箇所を意図的に選択して攻撃成功確率を最大化するタイプのウルフ攻撃を考慮していない．

従って，本論文では Daugman によって導入された正規化法 [5] がウルフ攻撃耐性の意味で最良の方法になっていないことを示すために，アイリスコードのエントロピー分布に基づいた攻撃を検討する．

すでに，Daugman[4] により人間同士の照合では平均 911bit のアイリスコードを用いているのに自由度が 249bit しかないということが示されており，このことから，人間の虹彩は人によらず何らかの相関を持ち，その相関によって自由度がアイリスコードの符号長よりも大幅に少なくなっている．

ここで人間の虹彩の働きを考えると瞳孔を広げたり縮めたりして網膜に取り込む光の量を調節する筋肉であるので，その筋繊維は半径方向に向かって伸びている．

これらのことから，半径方向に直線となるポイントでアイリスコードを選んで抽出したとき，大きく情報量が落ちているデータが取れる可能性は十分に考えられる．かし、これでは WAP の評価がされていない．本稿では，虹彩認証におけるウルフ攻撃確率を理論的に考察する．

本稿の構成は以下の通りである．**2章**においてウルフ攻撃確率を説明する．**3章**において Daugman の虹彩認証アルゴリズムを紹介する．**4章**において今回の実験の説明をする．**5章**において今回の実験の結果を述べる．**6章**において**5章**の結果からウルフの存在可能性について考察する．**7章**において今回の結果について考察をおこなう．**8章**においてまとめる．**9章**において今後の課題を検討する．

2　ウルフ攻撃確率（WAP）

生体認証の分野において，複数のテンプレートに対して一致と誤判定されるような入力情報のことを「ウルフ（wolf)」と呼ぶ．そのウルフを生体認証システムに入力することによって，登録されている複数のテンプレートのなりすましに成功する．このような攻撃を「ウルフ攻撃」（wolf attack）と呼び，そのウルフ攻撃の中で最大の攻撃成功確率を「ウルフ攻撃確率」（WAP:wolf attack probability）[1, 6]

詳しくは，WAP は次の式で定義される．

$$\mathrm{WAP} = \max_{s \in S_A} \left(\operatorname*{Ave}_{t \in T_h} \Pr\big[\, \mathrm{match}(s,t) = \text{"}accept\text{"} \,\big] \right)$$

ここで, S_A は人工物 (artifact) も含めた考えうるサンプルデータ全体の集合, T_h は認証システムに保管されたテンプレート全体の集合, $match$ は認証システムで用いられる認証アルゴリズムである．

生体認証システムのセキュリティ評価のうち，「第三者による成りすましに対する耐性の評価」の尺度として「誤受入率（false accept rate)」(FAR) だけではなく, WAP も用いられるべきである．FAR は他人を誤って本人として受け入れてしまう確率として, 次のように定義される．

$$\mathrm{FAR} = \operatorname*{Ave}_{s \in S_h} \left(\operatorname*{Ave}_{t \in T_h} \Pr\big[\, \mathrm{match}(s,t) = \text{"}accept\text{"} \,\big] \right)$$

ここで, S_h は生体情報からなるサンプルデータ全体の集合である．強力なウルフが存在しても人工物のため S_h に含まれないときや, たとえ S_h に含まれていても, その数がわずかであるために FAR の値には反映しないときがある．この場合, ウルフ攻撃による危険性は正しく評価されていない．また, 明らかに FAR $\leq$ WAP であることから，「第三者による成りすましに対する耐性の評価」として, WAP を十分小さく抑えることが大切である．

3　虹彩認証アルゴリズム

この節では，現在ほとんどすべての虹彩認証システムで採用されている J.Daugman の虹彩認証アルゴリズム [4, 5] を解説する．このアルゴリズムは他の生態認証システムと比較して，FAR が極めて低いことが実験で確かめられている．このアルゴリズムは，以下の 4 つのステップ：**虹彩領域の決定，アイリスコードの生成，マスクコードの生成，ハミング距離を用いた照合**から成る．

STEP 1. 虹彩領域の決定

獲得した画像から，瞳孔と虹彩の境目・虹彩と白目の境目を検出し，虹彩領域をドーナツ型に切り取る（図 1 参照）．切り取ったドーナツ型の画像を極座標表示とすることで，長方形の画像となる．（図 2 参照）

このとき，同時に虹彩領域内にある，まぶた・まつげ・光の反射等の部分を検出する．

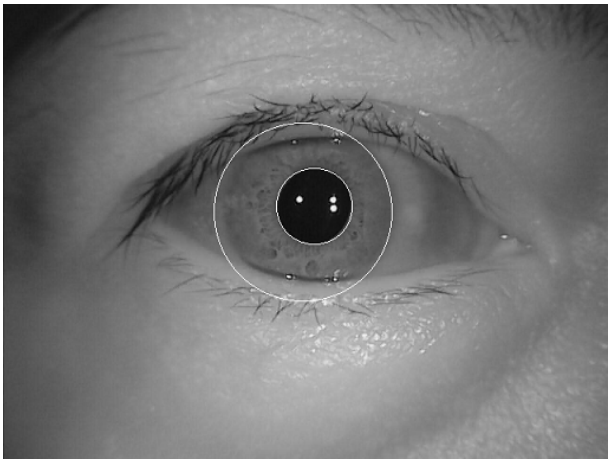

図 1: 虹彩領域の決定

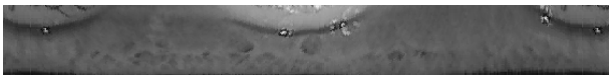

図 2: 極座標で表示された虹彩領域

STEP 2. アイリスコードの生成　**STEP1** で得られた極座標表示された長方形の画像領域を r 方向に８等分し，それぞれの領域をいくつかのポイントを選ぶ．各ポイントで複数の空間周波数に対する *Gabor* フィルターを用いたウェーブレット変換を行い，余弦成分の正負，正弦成分の正負により，それぞれ 0,1 のコードを決定する．これにより，１つのポイントに対して各周波数成分ごとに 2bit，全部で 2048bit のアイリスコードが生成される．虹彩画像 A から **STEP1,STEP2** を用いて作られたコードを A の「アイリスコード」と呼び，$codeA$ と書く．また，1 つのポイントに対して複数の周波数成分ごとにアイリスコードを求めている理由は，虹彩の模様が人によって様々であり，小さなノイズなどがあっても多くの情報を得られるようにしているためである．

STEP 3. マスクコードの生成　虹彩画像 A にアイリスコード $codeA$ と同じ bit 数（2048bit）の「マスクコード」を生成する．**STEP2** で行った各ウェーブレット変換に関して，**STEP1** で検出したまぶた，まつげ，反射が影響していると判定された場合，マスクコードの中の対応する 2bit を両方とも 0 とする．影響していないと判断されたときは，対応する 2bit を両方とも 1 とする．虹彩画像 A から生成されたマスクコードを $maskA$ と書く．

STEP 4. ハミング距離を用いた照合

２つの虹彩画像 A, B に対するハミング距離 HD_{raw}

図 3: r 方向の領域にを制限したイメージ

図 4: θ 方向の領域にを制限したイメージ

を次で定義する．

$$HD_{raw} = \frac{\| (codeA \oplus codeB) \cap maskA \cap maskB \|}{\| maskA \cap maskB \|} \quad (1)$$

n=$maskA \cap maskB$ に応じて補正したハミング距離 HD_{norm} を次のように定義する．

$$HD_{norm} = 0.5 - (0.5 - HD_{raw}) \sqrt{\frac{n}{911}} \quad (2)$$

A, B の照合には，あらかじめ決められたしきい値 T を用いて $HD_{norm} < T$ のとき認証し，$HD_{norm} \geq T$ では認証しない．

Daugman は，ハミング距離を補正することにより，照合に使われる bit 数 n が小さい場合でも FAR を一定に保っている．

4　実験の手法について

4.1　アイリスコードの領域を制限

今回，実験において以下のようにアイリスコードの領域を制限することで，虹彩認証におけるウルフの存在可能性を求めた．

また，その領域の制限の仕方が有効であるかどうかを確かめるために領域を制限せずにランダムに bit を選ぶ方法でも実験した．

4.1.1　r 方向に領域を制限

生成されたアイリスコードを r 方向の領域に制限して，その領域に対して FAR を求める．長方形の画像の縦方向の領域を残すように制限をする．(図３参照)

4.1.2　θ 方向に領域を制限

生成されたアイリスコードを θ 方向の領域に制限して，その領域に対して FAR を求める．長方形の画像の横方向の領域を残すように制限をする．(図４参照)

4.2 周波数成分ごとに領域を制限

4.1 と同様にして，アイリスコードを周波数成分ごとに領域を制限することで，虹彩認証におけるウルフの存在可能性を求めた．

今回使用した虹彩認証アルゴリズムは，3 種類の周波数成分についてアイリスコードを生成しているので，それぞれの周波数成分は低周波数成分・中周波数成分・高周波成分に分けることができる．

また、その周波数成分ごとの制限の仕方が有効であるかどうかを確かめるために周波数成分ごとに制限をしないで 3 種類の周波数成分から求められたアイリスコードを使う方法も実験する．

4.3 今回の実験において使用したもの

4.3.1 データベース

今回の実験に用いたデータベースは CASIA[1] Iris Image Database Ver. 3.0 [2] のデータベースの中の 60 人分の目の画像データを使用して実験を行った．

4.3.2 虹彩認証アルゴリズム

今回使用したプログラムは GET/INT[3] が公開している OSIRIS ver. 1.0[4] である． 上で公開されている．このアルゴリズムにおいても**３章**と同様に **STEP** を示す．大半が同じ部分ことをやっているため，異なる部分だけ以下に示す．

STEP 1. 虹彩領域の決定 ここでは本来，検出された虹彩領域内にある，まぶた・まつげ・光の反射等の部分を検出するのだが，この実験手法にはこの機能がない．

STEP 2. アイリスコードの生成 ここでは，アイリスコードのサイズと周波数成分の違いがある．

生成される極座標表示の画像のサイズが 562×64 ピクセルである．また，*Gabor* フィルターの 3 種類の波長の長さはそれぞれ，15，27，51 となっている．

STEP 3. マスクコードの生成

今回使用したアルゴリズムにはマスクコードは存在するが，生成の **STEP** は存在しない．

STEP 4. ハミング距離を用いた照合 この **STEP** に違いは生じない．

[1] The Chinese Academy of Science - Institute of Automation,
[2] http://www.cbsr.ia.ac.cn/IrisDatabase.htm
[3] Institut National des T élé communications, Groupe des Ecoles des Télécommunications, http://www.int-evry.fr/
[4] http://www.int-evry.fr/biometrics/BMEC2007/

4.4 提案する $mask$ 検出手法

今回の実験手法には，$mask$ の機能がなかった．しかし，前にも述べた通り $mask$ の機能がないまま実験を行ってしまうと期待しない結果が出てしまう恐れがあるため，代わりの手法を提案し，それを $mask$ の機能として代用した．この提案手法では，1 つのポイントに対する HD を計算して，その自由度が極端に下がっているところを $mask$ と判断して，ある程度の bit 数を削っている．これは，実際に虹彩の領域を決定して長方形にした画像を見ると，$mask$ の多くがまぶたの部分であるということがわかり，まぶたの部分では波が検出されないため，人によってアイリスコードの変化があまりないと考え，自由度が下がると予想しているからである．

4.5 領域制限手法

獲得したアイリスコードに提案した $mask$ 検出手法をかけて，残った領域に対してそれぞれの制限をかける手法を提案する．

まず，r 方向の領域に対して制限する手法を周波数成分ごとに次のようにした．r 方向の領域に対して制限をかけるので，引数を θ と照合に使う bit 数 n とした．

4.6 今回の実験のプログラム

- $mask_{(r,L)}(\theta, n)$

  r 方向の領域に制限をし，低周波成分のみ使用

- $mask_{(r,M)}(\theta, n)$

  r 方向の領域に制限をし，中周波成分のみ使用

- $mask_{(r,H)}(\theta, n)$

  r 方向の領域に制限をし，高周波成分のみ使用

- $mask_{(r,All)}(\theta, n)$

  r 方向の領域に制限をし，すべての周波数成分を使用

同様にして，θ 方向の領域に対して制限する手法を作成し，引数を r と n とした．また，ランダムにアイリスコードを選び低周波数成分のみを使用する手法を $mask_L(n)$ とした．他の周波数成分に関しても r 方向の領域に対して制限する手法と同様に作成した．

4.7 評価の方法

今回の実験では，特定のウルフを探しているわけではないので FAR で評価する．

まず，それぞれのアイリスコードの組み合わせから HD の分布を求めて，それらの平均 m と分散 σ^2 を求める．今回の実験した HD の総数は 60×59/2=1770 個である．

自由度（DOF）は以下の式で求められる．

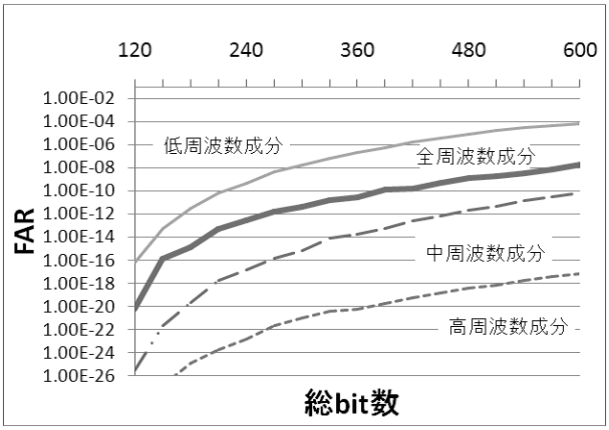

図 5: ランダムに選んだときの総 bit 数と FAR

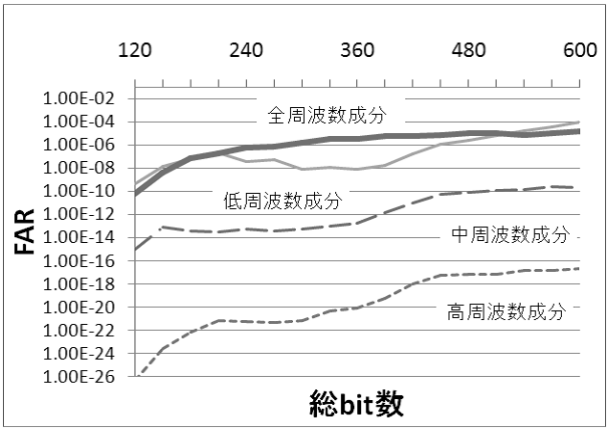

図 6: θ 方向に領域を分割したときの総 bit 数と FAR

$$DOF = \frac{m\,(1-m)}{\sigma^2} \tag{3}$$

このとき，FAR は次で与えられる．

$$FAR = \sum_{i=0}^{DOF \times T_n} {}_{DOF}C_i \cdot m^i \cdot (1-m)^{1-i} \tag{4}$$

ここで，T_n はもともとのしきい値 T_r を次のように正規化したものである．

$$T_n = 0.5 - (0.5 - T_r)\sqrt{\frac{911}{n}} \tag{5}$$

5 実験結果

5.1 ランダムと領域を制限した場合の比較

ランダムにアイリスコードを選んだ場合と r 方向や θ 方向に領域を制限した場合を比較すると，図５，図６，図７より，ランダムにアイリスコードを選んだ場合より領域を制限した場合の FAR の方が大きくなっていることがわかる．

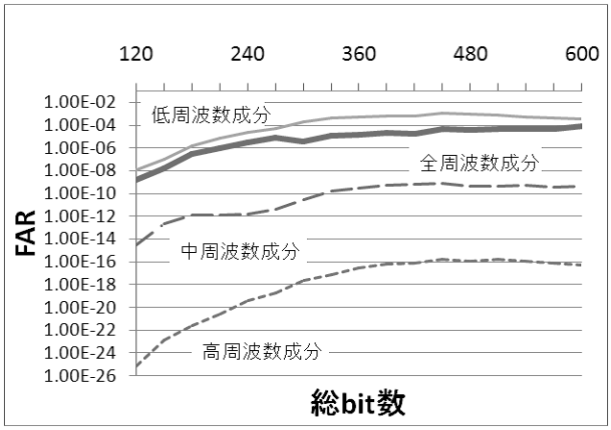

図 7: r 方向に領域を分割したとき総 bit 数と FAR

5.2 領域を θ 方向に制限した場合と r 方向に制限した場合の比較

アイリスコードの領域を θ 方向に制限した場合と r 方向に制限した場合を比較すると，図５，図６より，アイリスコードの領域を θ 方向に制限した場合より r 方向に制限した場合の FAR の方が大きくなっていることがわかる．

5.3 周波数成分ごとの比較

周波数成分ごとに分けた場合は，図５，図６，図７より，高周波数成分に比べ，中周波数成分の方が FAR が大きくなり，中周波数成分に比べ，低周波数成分の方が FAR が大きくなっていることがわかる．

また，図５，図７より，周波数成分を分けない場合よりも，低周波数成分の方が FAR が大きくなっていることがわかる．

6 ウルフ攻撃確率

５章の結果より，最も FAR が大きくなるのは，r 方向の領域に制限した低周波数成分のみのものであることがわかった．その中でも FAR が最大となったのは，bit 数が n=450bit のところでそのときの値は 0.001077 となった．

Daugman の実験において，しきい値 T_r を 0.32 に設定したときの FAR は n によらず 10^{-6} となるという結果が出ている．今回得られた FAR が最大になる領域は Daugman が求めた FAR に対して，1000 倍もの誤一致を引き起こすことになる．つまり，$mask_{(r,L)}$ を用いて作られた r 方向に領域を制限され，低周波数成分ばかりを集めた人工的なアイリスコードは，今回のデータと実験から，ウルフになり得ると考えられる．

7　考察

4章でも述べた通り，今回使用した実験手法はDaugmanの手法に対して，生成されるアイリスコードのサイズが違い，$mask$の機能もない．しかし，同じように周波数成分ごとにアイリスコードを生成していて，サイズの違いだけなので，高周波数成分のみのFARが低周波数成分のみのFARよりも大きくなってしまうような大きな結果の変動は生まれない．

また，$mask$の機能がないことについても今回の実験では，提案手法で自由度が極端に下がるポイントを削除しているので，$mask$の機能が存在しないことによって予期しないFARの増大は生まれない．

よって，Daugmanの手法に対しても有効な攻撃である．

8　まとめ

虹彩認証システムに対して，意図的に領域を制限してHDの分布を求めた場合, FARがどのようなときに大きくなるかを実験によって示した．

r方向の領域に制限した場合とθ方向の領域に制限した場合と領域を制限せずにランダムに選んだ場合のそれぞれについて，3種類（低周波数，中周波数，高周波数）の周波数成分に分けた場合と全周波数成分で見た場合のFARを求めた．

その結果，r方向の領域に制限して低周波数成分を用いた場合，最もFARが大きくなることがわかった．

9　今後の課題

今回の実験では，60人分のデータしか使えなかったが，他のデータを使いサンプル数を多くして同様な結果が得られるかどうかを実験してみる．

今回の実験では，結果を求めただけで理論的にこの結果が出るということを検討していないので，アイリスコードのr方向に関する相関をエントロピーを求めることによって調べる必要がある．

また、今回の結果をもとにして実際に攻撃をしてみるということも考えられる．例えば，低周波数帯を残すためにまつげのような細かいノイズを入れて目の前に用意して，高周波数帯だけを$mask$することにより今回の攻撃が有効になる可能性がある．

さらに，今回の結果はプログラム例からもわかるようにrやθなどのパラメータを入力して得られたものなので，この部分を探索アルゴリズムにすればより強いウルフが見つかる可能性が十分にある．

参考文献

[1] 宇根正志，大塚玲，今井秀樹,“生体認証システムにおける新しいセキュリティ評価尺度：ウルフ攻撃確率,” Proc of SCIS2007，2007.

[2] 渡邉直彦，繁富利恵，宇根正志，大塚 玲，今井秀樹,“指静脈パターン照合アルゴリズムにおけるユニバーサル・ウルフ，” Proc of CSS2006, pp.621-626,2006.

[3] 河上梨恵，繁富利恵，美添一樹，宇根正志，大塚玲，今井秀樹，“マニューシャ・マッチングのウルフに関する理論的考察，” Proc of SCIS2007，2007.

[4] J.Daugman,“How Iris Recognition Works,IEEE Transactions on Circuits and Systems for Video Technology,” vol. 14, No. 1, pp. 21-30, January 2004

[5] J.Daugman,“Probing the Uniqueness and Randomness of IrisCodes : Results From 200 the IEEE, ”vol. 94, No. 11, pp. 1927-1935, November 2006

[6] M. Une, A. Otsuka, H. Imai,“Wolf Attack Probability: A New Security Measure in Biometric Authentication Systems,” International Conference on Biometrics ICB2007, LNCS 4642, pp. 396-406.