THE IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS, COMMUNICATIONS AND COMPUTER SCIENCES (JAPANESE EDITION)

電子情報通信学会 論文誌 A 基礎・境界

VOL. J100-A NO. 12
DECEMBER 2017

基礎・境界ソサイエティ

一般社団法人 電子情報通信学会
THE ENGINEERING SCIENCES SOCIETY
THE INSTITUTE OF ELECTRONICS, INFORMATION AND COMMUNICATION ENGINEERS

マイクロ生体認証の提案とその一事例報告*

藤田　真浩[†]　眞野　勇人[†]　村松　弘明[†]　高橋　健太[††]
西垣　正勝[†a)]

Micro Biometric Authentication: A Proposal and the First Attempt*

Masahiro FUJITA[†], Yuto MANO[†], Hiroaki MURAMATSU[†], Kenta TAKAHASHI[††], and Masakatsu NISHIGAKI[†a)]

あらまし　本論文では,「マイクロ生体認証」と呼ばれる新たな生体認証メカニズムを提案する．本メカニズムは，生体の微細部位を生体認証へ応用するものである．微細部位を利用することによって，なりすましに対する高い耐性を有し，かつ，プライバシー（追跡可能性）に対する配慮がなされた生体認証が実現される．生体部位の静的な生体情報を利用することで，実用レベルの認証精度も達成可能である．本論文では，マイクロ生体認証の一事例として，マイクロスコープによって撮像される人間の微細肌理画像を用いた生体認証システムを構築した．ユーザ実験を通じて，肌理を利用したマイクロ生体認証の有用性を検証した．その結果，肌理を利用したマイクロ生体認証が，なりすましに対する高い耐性を有すること，追跡可能性に対する十分な配慮がなされていること，実用レベルの認証精度を有することを確認した．

キーワード　生体認証，微細生体部位，肌理，なりすまし，追跡可能性，認証精度

1. まえがき

生体認証とは，人間の身体的特徴や行動的特徴から個人を認証する技術である．通常，事前に採取した生体情報をテンプレートとして登録し，認証時に取得した情報とテンプレートを比較することで認証を行う．近年では実用化が進み，PC，ATM，パスポートの認証手段としても利用されてきている．最近では，オンライン認証の新業界標準の確立を狙う Fast Identity Online Alliance（FIDO）[1] が，ユーザ端末をアクティベートさせる認証手段として生体認証を有力視していることから，生体認証に益々注目が集まっている．また，公開鍵基盤（PKI）における秘密鍵を生体情報で置き換える「テンプレート公開型生体認証基盤（PBI）」が提案されている [2]．FIDO や PBI によって，今後更なる生体認証の普及が予想される．

生体認証は，パスワードやトークンを用いた認証方式と異なり，忘却・紛失・盗難の恐れがないという利点がある．しかし一方で，生体認証には生体情報を用いるが故の課題がある.「生涯不変の情報であり，取り替えが効かない」ことに起因する「なりすまし」及び「追跡可能性」の問題である．

「なりすまし」は，攻撃者が生体情報を入手して偽造生体を作成する攻撃である．実際に，攻撃者が盗んだ生体情報から顔写真や人工指を複製し，なりすましに成功した例が報告されている [3], [4], [18]．近年では，カメラの高性能化により，遠距離から虹彩や指紋の高精細な画像を盗撮することも困難ではなくなっている．また攻撃者は，生体情報読取装置を正規ユーザの生活環境内に密かに仕込んで生体情報を収集したり，生体認証によってログインする正規の Web サービス提供サイトを装ったダミーサイトを設置したりして生体情報をフィッシングすることも可能である．生体認証を実現するにあたっては，この「なりすまし」に対する耐性を有する必要がある（要求 1：なりすましに対する高い耐性）．

「追跡可能性」に関して，生体情報は，パスワードやトークンのように変更や交換によって本人との間の紐づきをリセットできないため，匿名ユーザ群または仮

[†] 静岡大学，浜松市
Shizuoka University, 3–5–1 Johoku, Naka-ku, Hamamatsu-shi, 432–8011 Japan
[††] (株) 日立製作所研究開発グループ，横浜市
Hitachi, Ltd., Research & Development Group, 292 Yoshida-cho, Totsuka-ku, Yokohama-shi, 244–0817 Japan
a) E-mail: nisigaki@inf.shizuoka.ac.jp
＊ 本論文はバイオメトリクス研究専門委員会推薦論文である．

名ユーザ群の中から生体情報を用いて同一ユーザを名寄せすることが可能である．例えば，ある生体情報を秘密情報として用いて「アカウント A」のユーザ名でシステムに登録していた正規ユーザが，アカウント A の登録を削除し，同じ生体情報を用いて「アカウント B」として再登録したとする．このとき，システム管理者はアカウント A とアカウント B の秘密情報が同一の情報であることを確認することによって，アカウント A と B が同一ユーザのものであることが判明してしまう．追跡可能性の観点から，生体情報の漏えいを防ぐ必要がある（要求 2：追跡可能性に対する考慮）．

要求 1，2 を部分的に達成する方法として，テンプレート保護型生体認証方式が提案されている．その代表例が，生体情報と乱数情報を組み合わせることにより，テンプレートを保護するキャンセラブル生体認証 [5] である．乱数情報によって生体情報が秘匿されるため，テンプレートからの生体情報の漏えいが防がれ，要求 1 を満たす．また，乱数情報を変更することによってテンプレートの更新が可能となるため，要求 2 も満たしている．しかし，生体情報そのもの（テンプレート以外の経路での生体情報）の漏えいに対する対策にはなり得ていない．

生体情報そのものが漏えいしてしまった場合に対する対策としては，提示された生体情報が偽造物でないことを検査する生体検知技術 [6] や生体情報読取装置の真正性を検査するデバイス認証 [7] が存在する．しかし，これらはいずれも要求 1 に対処するものであり，要求 2 に対する対策とはなり得ていない．

生体情報そのものが漏えいしてしまったとしても，要求 1，2 を達成する方式が，生体情報のワンタイム化である．テキスト独立（text independent）型あるいはテキスト指定（text prompted）型の手書き署名認証や音声認証がその実例である．しかし，生体情報のワンタイム化が可能なのは基本的に動的な生体情報に限られる．一般に動的な生体情報を利用した場合の認証精度は低いことが知られており [8]，静的な生体を利用することで高い認証精度を確保することが望ましい（要求 3：静的な生体情報の利用による認証精度の確保）．

以上の議論から，「静的な生体情報のワンタイム化」が実現できれば，要求 1〜3 を全て満たす生体認証となり得ると考えられるが，「静的」な生体情報は本質的にワンタイム化とは相容れない．

そこで，生体の微細部位を生体認証へ応用することで要求 1〜3 を満たす生体認証を実現する．本論文では，この生体認証メカニズムを「マイクロ生体認証」と呼ぶ．マイクロ生体認証の一例として，マイクロスコープによって撮像される人間の肌理画像を用いた認証システムを構築し，実験からマイクロ生体認証の可能性を示す．なお本論文は，文献 [19], [20] を基に，プロトタイプシステムの改良，ユーザ実験の拡充，及び，提案方式に関する更なる考察を行ったものである．

以降，**2.** で関連技術・関連研究を概説し，**3.** で提案方式を示す．**4.** では提案方式のプロトタイプシステムを構築する．**5.** で評価実験を行ったのち，**6.** でその結果を利用して，提案方式に関する考察を行う．最後に，**7.** でまとめと今後の課題を記す．

2. 関連技術・関連研究

著者らが調査した限りでは，生体の微細部位を認証に利用した先行事例は見当たらなかった．そこで本章では，微細情報を取り扱う関連技術としてマイクロ文字，人工物メトリクスを，生体情報のワンタイム化の関連研究としてキャンセラブル生体認証，貼付型生体認証トークンを紹介する．

2.1 マイクロ文字

一般に，小さいものであればあるほど，偽造することは難しい．この性質を利用した偽造防止技術として，「マイクロ文字」と呼ばれる極小文字を印刷する技術があげられる [9]．証券や紙幣などに利用されており，書込みの解像度が低い印刷装置ではこれらを複製できないという効果を有している．技術進歩により市販の印刷装置の解像度が向上すると，有効性が低下する危険性を孕んでいる．

2.2 人工物メトリクス

人工物メトリクスとは，人工物の個体ごとに固有な物理的特徴を用いて個体識別や真贋判別を行う技術 [10], [11] である．同じ製造技術を用いれば同じ製造物を量産することは可能である．しかし，微細部まで見ると，個体ごとの固有パターン（例えば紙であれば繊維の絡まり具合など）をもつことが確認できる．人工物のこの固有パターンを，生体認証における指紋のように利用することによって，個々の人工物を識別することが可能となる．人工物の固有パターンは，製造工程内での制御が不可能な要因によって生成されるため，一般に耐クローン性を有する．これによって人為的な偽造物や複製物を判別することができる．

通常，固有パターンが微細であるほど複製を作製す

るにあたっての困難度が激増する．微細レベルの最たるものの一例として，ナノメートルレベルのシリコン基板上の凹凸情報を利用した人工物メトリクスが研究されている [11]．

2.3 キャンセラブル生体認証

キャンセラブル生体認証 [5] では，乱数情報を用いて生体情報をマスクし，その情報をテンプレートとしてサーバに登録する．

登録フェーズは以下の手順で行われる．

1. 登録者の生体情報 X を読み取る．
2. 登録者に対して乱数 R を生成し発行する．
3. 乱数 R を用いて生体情報 X を $T = F_R(X)$ に変換する．ここで，$F_R(\cdot)$ は乱数 R による変換処理を表す．
4. T をサーバに登録する．

乱数 R は，ユーザの IC カードなどのトークンまたは第三者機関のサーバに保管され，認証の際に補助情報として使用される．

認証フェーズは以下の手順で行われる．

1. 認証要求者の生体情報 X' を読み取る．
2. 認証要求者の乱数 R を取得する．
3. 乱数 R を用いて生体情報 X' を $T' = F_R(X')$ に変換する．
4. T と T' が十分類似していれば認証成功とする．

乱数 R や変換関数 $F_R(\cdot)$ を変更することで，テンプレート情報の更新が可能である．

2.4 生体貼付型使い捨て認証トークン

生体情報以外の認証情報を用いつつ生体認証と同様に紛失や盗難の恐れのない認証を実現する試みとして，RFID（Radio Frequency IDentification）を利用した「使い捨て認証トークン」を身体に直接装着する方法が研究されている．RFID タグを内包するカプセルを飲み込んで認証を行う経口カプセル型や，RFID タグを皮膚に張り付けて認証を行う電子タトゥー型が提案されている [12]．

本論文執筆時現在において，これらの技術は商用化に至っていないが，疑似的にワンタイム生体認証を実現する方式として注目されている．しかし，認証の主体はトークン本体であるため，トークンの偽造に関する脆弱性が残る．特に電子タトゥー方式では，受け渡しが可能であることや使い捨てられた RFID が悪用される恐れがある．また，カプセル方式では，異物を飲み込むことや，異物を体内に保管することに不快感を覚える利用者がいることも想定される．

3. マイクロ生体認証

3.1 コンセプト

前述のように，要求 1〜3 を満たす生体認証が求められる．静的な生体情報を利用すれば，要件 3 を満たすことが可能である．しかし，（通常の）静的な生体情報は，なりすましが容易であり，ワンタイム化が困難であるため，要求 1 と 2 を満たさない．そこで，本論文では静的な生体情報の微細部位を生体認証へと応用することで，要求 1〜3 を満たすことを実現する．このメカニズムを「マイクロ生体認証」と呼ぶ．マイクロ生体認証は，下記のとおり，要求 1〜3 を満たす．

要求 1：

一般に，模倣品をより細部まで作り込むにつれて，その製造にかかる手間が非常に高くなるが，ズームレンズを使って対象物の細部を撮影することは，模造に比べはるかに容易である．この「撮影と偽造のコストの非対称性」を利用し，ある微細部位の生体情報をテンプレートとして登録することによって，たとえその部位の情報が盗まれたとしても偽造に大きなコストを要する生体認証が実現される．

要求 2：

生体部位を微細にすることで，生体部位の更新可能回数（微小部位を一つずつ使っていった際に未使用部位が枯渇するまでの回数）が激増する．ユーザは，パスワードの変更やトークンの交換と同様の感覚で，その必要が生じた際に，ユーザ自身の意思で，今まで利用していた生体部位を別の生体部位に変更する．ユーザが生体部位を更新するたびに，認証に用いる生体情報が変更され，追跡可能性が分断されることになる．

要求 3：

生体部位の静的な情報を利用するため，認証精度も（動的な生体情報を利用する認証と比較して）高い．

3.2 肌理を利用したマイクロ生体認証

本論文では，マイクロ生体認証の一事例として，マイクロスコープで拡大した肌理画像を生体認証へと応用する．

人の皮膚表面を細かく観測すると凹凸があることが認められる．これらは「皮溝」と呼ばれる種々の深さや長さの溝，「皮丘」と呼ばれる浅く細い皮溝で囲まれる細かい隆起，「皮野」と呼ばれるやや深い皮溝で囲まれる多角形の隆起により構成される [13]．その他にも毛穴や汗腺などの要素もあり，毛穴は皮溝の交点に多く見られ，ほとんどの場合で開口部の面積と深さは比

例していることや，汗腺は皮丘の頂上に開いていることが報告されている [14]．肌理はこれらの要素により形作られる皮膚紋様であり，そのパターンは大きくとも数百 μm 程度 [13] で微細であり，一様ではないため，精密に模造することは困難であることが期待できる．

本論文では，肌理の表層状態（凹凸パターン）に注目する．肌理の凹凸パターンが安定して取得可能であり，かつ，十分な多様性が認められるならば，指紋や掌紋のように個人認証に利用することが可能となる．なお，肌分析のための手法は化粧品開発の分野などで活発に研究されている．これらの分析はあくまで医療目的などに限定されており，著者らが調べた範囲ではいずれの方法でも肌理を用いた認証に関する既存研究は報告されていない．

3.3 肌理を利用したマイクロ生体認証の認証手順

以下では，拡大した肌理画像を利用する例を用いて，マイクロ生体認証の手順を説明する．ここでは 1 対 1 認証を例として説明をする．提案方式は 1 対 N 認証の場合にも適用可能である．なお，デバイス認証等を用いることによって，生体情報を撮影する撮影機器の真正性は担保されているものとする．

【登録フェーズ】

1. ユーザは，ユーザ ID を決定しシステムへ登録する．
2. システムは，登録部位を示す位置合わせ用のマークの印字をユーザに要求する．
3. ユーザは，自分の身体の任意の位置にマークをつける．
4. システムは，マークの近くの部位の生体情報を読み取り，その特徴量を X とする．X はデータベースに登録される．

【認証フェーズ】

1. ユーザは，ユーザ ID をシステムに入力する．
2. システムは，マークで示された部位の生体情報を読み取り，その特徴量を X′ とする．
3. システムは，データベースからユーザ ID と紐付いている登録情報 X を取り出す．
4. システムは，X と X′ が十分類似していれば認証成功とする．

なお，提案方式における認証フェーズにおいては，ユーザが身体にマークを保持し続けていることが前提となることに注意されたい．

4. プロトタイプシステムの実装

3.3 で示したマイクロ生体認証についてプロトタイプシステムの実装を行った．その構成を図 1 に示す．以下に実装において留意した点を述べる．

4.1 登録部位の発見

マイクロ生体認証においては，システムが登録部位（肌理）を発見するために，ユーザが肌の表面にマークを印字する必要がある．このマークの位置を変更するたびに，ユーザは認証で利用する生体情報を変更することが可能となる．本論文では，プロトタイプであるため，最も単純な方法である「油性インクによってマークを印字する方法」を採用した．

4.2 生体部位の撮影

皮膚表面の形態情報を取得するには主に 3 種類の手法があげられる．レプリカを用いて表面形態を転写し共焦点顕微鏡などで取得する方法，三次元スキャナを用いて非接触で表面形態情報を取得する方法，マイクロスコープを用いて表面形態の拡大画像を撮像する方法，の三つである [14]．本論文は，プロトタイプで

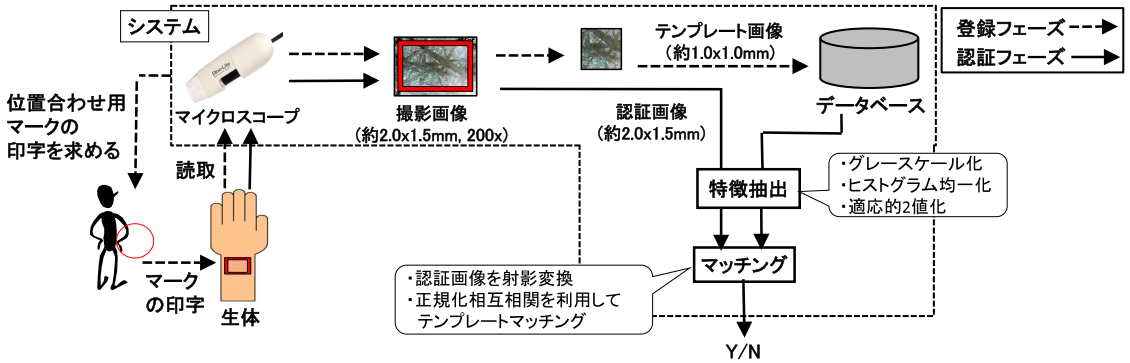


図 1 プロトタイプシステムの構成
Fig. 1 Overview of prototype system.

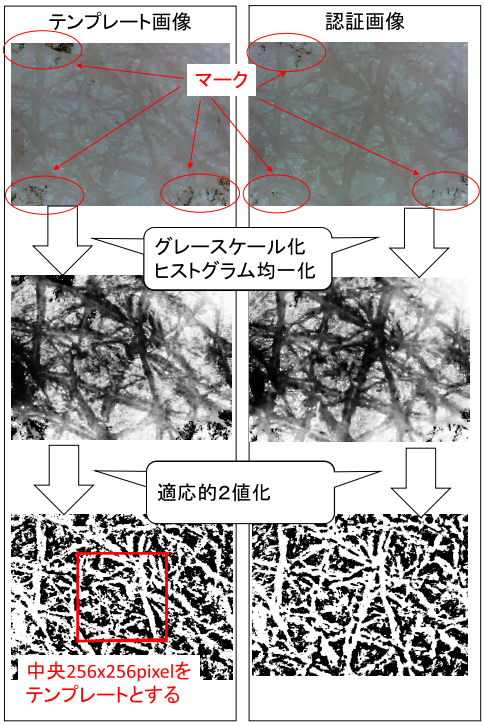


図 2　特徴抽出の手順
Fig. 2　Flow of future extraction.

あるため，最も安価で容易に利用可能な，マイクロスコープを利用する方法を採用した．使用したマイクロスコープは AM2001-Dino Lite Basic（サンコー株式会社製）である．

本システムにおいては，200 倍に拡大したマイクロスコープで撮影した肌理画像（640 × 480 pixel，約 2.0 × 1.5 mm）の中央 256 × 256 pixel（約 1.0 × 1.0 mm）を切り出し，それをテンプレート画像として利用する．

4.3　特 徴 抽 出

本論文では，肌理の凹凸パターンを特徴量として利用する．安定した特徴を得るために，テンプレート画像，及び，認証画像は，マッチング前にグレースケール化，ヒストグラム均一化，適応的 2 値化をこの順に施して 2 値化画像に変換している．それぞれの処理は，Open CV Ver. 2.4.9 [15] に実装されている関数 cv::cvtcolor, cv::equalizeHist()，cv::adaptiveThreshold() によって行った．cvAdaptiveThreshold() のパラメータは，maxValue を 255，adaptiveThreshold を CV_ADAPTIVE_THRESH_MEAN_C，thresholdType を CV_THRESH_BINARY_INV，inBlockSize を 39 とした．図 2 は，あるテンプレート画像・認証画像に対して，これら特徴抽出の処理を施した様子である．

4.4　マッチング

マイクロスコープの位置や傾きのずれによって，認証画像には（テンプレート画像と比較して）平行移動やひずみが混入する．これらは，ノイズとなり，マッチングスコアの低下（認証率の低下）を引き起こす．そこで，まず，認証画像に対してテンプレート画像を水平・垂直方向に走査させながらテンプレートマッチングを行うことによって，平行移動ノイズを補正する．そして，射影変換を適用し，ひずみノイズを補正する．これらの補正操作を施した上で認証画像とテンプレート画像のマッチングスコアを求める．具体的な手順は下記のとおりである(注1)．

【手順 1】

① テンプレート画像の各頂点を左上から半時計回りに Pt_0，Pt_1，Pt_2，Pt_3 とする(注2)．

② 認証画像（640 × 480 pixel）に対してテンプレート画像（256 × 256 pixel）を水平方向並びに垂直方向に 1 pixel ずつ平行移動させながらテンプレートマッチングを行い，認証画像の中でテンプレート画像と一番マッチングスコアの高い画像領域（256 × 256 pixel）を発見する．これによって特定された 256 × 256 pixel の矩形領域の各頂点を左上から半時計回りに Pa_0，Pa_1，Pa_2，Pa_3 とする．

③ ひずみや位置ずれの発生によって，テンプレート画像の Pt_i（$0 \leq i \leq 3$）に対応する点は，認証画像においては（Pa_i とは完全に一致せずに）Pa_i の周辺にある可能性も高い．そこで，各 Pa_i の周囲の候補点の集合を C_i とする．

④ C_0，C_1，C_2，C_3 からそれぞれ任意の候補点 (P_0, P_1, P_2, P_3)（$P_i \in C_i$，$i = 0, 1, 2, 3$）を選択する場合の全ての組み合わせについて，4 点 (P_0, P_1, P_2, P_3) によって囲まれる領域が 256 × 256 pixel の矩形画像となるように射影変換を施した画像（射影変換後の認証画像）群を用意する．

(注1)：本来であれば，マイクロスコープの位置や傾きのずれによって，回転移動ノイズも混入するため，その補正のためにアフィン変換も適用されることが一般的である．しかし，本研究の現段階では，「目視によって，テンプレート画像と可能な限り一致するように認証画像の撮影を行う」という制約を課すことによって，回転移動ノイズの混入を抑えるようにした．このため，今回のマッチング処理においては，回転移動ノイズの補正は行っていない．

(注2)：登録時には，640 × 480 pixel の中央 256 × 256 pixel をテンプレート画像として利用しているため，Pt_0，Pt_1，Pt_2，Pt_3 の座標は (192, 112)，(192, 368)，(448, 368)，(448, 112) である．

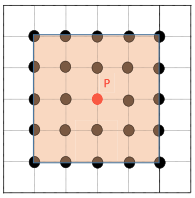


図 3　点 P を中心とした 5 × 5 画素の候補点
Fig. 3　Candidate points of 5×5 pixels around central point P.

⑤　④で得た射影変換後の認証画像群とテンプレート画像とのマッチングスコアを得る．その最大値を認証画像とテンプレート画像のマッチングスコアとする．

ただし，上記の処理においては，③の処理回数が $|C_0| \times |C_1| \times |C_2| \times |C_3|$ 回必要となる．例えば，C_i の候補点を Pa_i を中心とした 50 × 50 画素の 2500 点とした場合，この回数は 2500^4 となる．すなわち，マッチング処理にかかる時間が非常に莫大なものとなる．

そこで，認証時間短縮のため，今回のプロトタイプシステムでは，処理③④を簡略化した実装を行った．具体的には，次の手順である．

【手順 2】

①　テンプレート画像の各頂点を左上から半時計回りに Pt_0，Pt_1，Pt_2，Pt_3 とする．

②　認証画像（640 × 480 pixel）に対してテンプレート画像（256 × 256 pixel）を水平方向並びに垂直方向に 1 pixel ずつ平行移動させながらテンプレートマッチングを行い，認証画像の中でテンプレート画像と一番マッチングスコアの高い画像領域（256 × 256 pixel）を発見する．これによって特定された 256 × 256 pixel の矩形領域の各頂点を左上から半時計回りに Pa_0，Pa_1，Pa_2，Pa_3 とする．そのマッチングスコアを max_score とする．

③　Pa_0 を中心とした 5 × 5 画素の 25 点の集合を候補点群 C_0 とする（図 3）．

④　C_0 内の任意の候補点について，4 点 (P_0, Pa_1, Pa_2, Pa_3)（$P_0 \in C_0$）によって囲まれる領域が 256 × 256 pixel の矩形画像となるように射影変換を施した画像（射影変換後の認証画像）群を用意する．

⑤　④で得た射影変換後の画像群とテンプレート画像とのマッチングスコアを得る．その最大値を max_score とし，そのときの P_0 を Pa_0 とする．

⑥　⑤で max_score が更新されていた場合（すなわち，Pa_0 が更新されていた場合），③に戻る．

⑦　Pa_1 に対して③～⑤と同様の処理を行う．

⑧　⑦で max_score が更新されていた場合（すなわち，Pa_1 が更新されていた場合），⑦に戻る．

⑨　Pa_2 に対して③～⑤と同様の処理を行う．

⑩　⑨で max_score が更新されていた場合（すなわち，Pa_2 が更新されていた場合），⑨に戻る．

⑪　Pa_3 に対して③～⑤と同様の処理を行う．

⑫　⑪で max_score が更新されていた場合（すなわち，Pa_3 が更新されていた場合），⑪に戻る．

⑬　③～⑫で max_score が更新されていた場合，③に戻る．そうでない場合，⑭に進む．

⑭　その最大値をマッチングスコアとする．以上の処理を終えたとき，max_score が認証画像とテンプレート画像のマッチングスコアとなる．

テンプレートマッチングは，Open CV Ver2.4.9 で実装されている cv::matchTemplate() で行い，引数 method（テンプレートマッチングの方法）の値は CV_TM_CCOEFF_NORMED を利用した．

5. 実　　験

肌理を利用したマイクロ生体認証の認証精度をユーザ実験によって求める．

5.1 肌理画像の収集

静岡大学の学生 10 名（男性 8 名，女性 2 名）に協力してもらい，1 名当たり任意に 5 箇所の肌理を採取した．体毛が少ないことや，撮影が比較的容易な部位であることから，撮影範囲は前腕部内側に限定した．利用する腕は，各被験者に選択してもらった．実験実施期間は 5 日間である．

1 日目にテンプレート画像の撮影を行った．各被験者の前腕部 5 箇所に油性インクでマークを印字し，それぞれのマークを基準にして，(マーク近くの）肌理をマイクロスコープで撮影した．**4.2** で示したとおり，この画像の中央 256 × 256 pixels をテンプレート画像として利用する．その結果，10 名 × 5 箇所 = 50 枚のテンプレート画像を収集した．

2, 3, 4, 5 日目に，認証画像の撮影を行った．認証画像の撮影は，実験実施者（著者）が目視で調整することで行った．具体的には，肌に印字された各マークを参考にして，登録部位を発見したのち，撮影する肌理画像の見た目がテンプレート画像とできる限り一致するように撮影を行った．日常生活の中でマークが消

えそうになった場合，マークの上からできる限り同じ位置になるように，マークを打ち直した．これらの結果，10 名 × 5 箇所 × 4 日間 = 200 枚の認証画像を収集した．

5.2 評価方法

5.1 で得た被験者 i（$1 \leq i \leq 10$）の p（$1 \leq p \leq 5$）箇所目のテンプレート画像 $t_{i,p}$ と定義する．同様に，被験者 j（$1 \leq j \leq 10$）の d 日目（$2 \leq d \leq 5$）の q 箇所目（$1 \leq q \leq 5$）の認証画像を $a_{j,d,q}$ と定義する．これらを利用して，**4.3**（特徴抽出），**4.4**（マッチング手順 2）の手順に沿って，以下の三つのマッチングスコアを計算する．

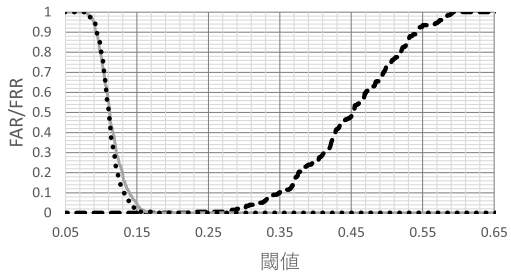
① 同じ被験者内の同箇所間のマッチングスコア．すなわち，$t_{i,p}$ と $a_{j,d,q}$（$i = j$，$p = q$）間のマッチングスコア．このとき，$t_{i,p}$ と $a_{j,d,q}$ の組み合わせは 200 通りであるため，得られるスコアの総数は 200 である．

② 同じ被験者内の違箇所間のマッチングスコア．すなわち，$t_{i,p}$ と $a_{j,d,q}$（$i = j$，$p \neq q$）間のマッチングスコア．このとき，$t_{i,p}$ と $a_{j,d,q}$ の組み合わせは 800 通りである．ただし，本論文では，処理時間短縮のため，このうち 200 通りの組み合わせをランダムに抽出し，それらのスコアを求めた．すなわち，得られるスコアの総数は 200 である．

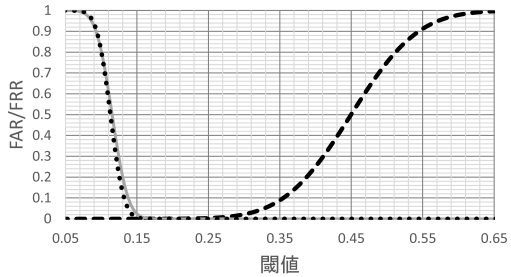
③ 異なる被験者間のマッチングスコア．すなわち，$t_{i,p}$ と $a_{j,d,q}$（$i \neq j$）間のマッチングスコア．このとき，$t_{i,p}$ と $a_{j,d,q}$ の組み合わせは 9,000 通りである．ただし，本論文では，処理時間短縮のため，このうち 200 通りの組み合わせをランダムに抽出し，それらのスコアを求めた．すなわち，得られるスコアの総数は 200 である．

5.3 結　　果

5.2 に示した三つのスコアの計算を行った．スコア①（同被験者同箇所間），スコア②（同被験者異箇所間），スコア③（異被験者間）に対して，それぞれ本人と他人を切り分けるしきい値を変更した場合の本人拒否率（FRR）と他人受け入れ率（FAR）の変化を記したグラフが図 4 (a) である．スコア①～③を，それぞれ，正規分布であると仮定して，スコア①，②，③に対して FAR と FRR の変化を記したグラフが図 4 (b) である．図 4 (b) において，等誤率（EER）を計算したところ，スコア①とスコア②間では，認証しきい値 ≒ 0.18 の際に EER ≒ 0.01%であった．スコア①とスコア③間においては，認証しきい値 ≒ 0.17 で EER ≒ 0.01%であることが確認できた(注3)．



(a) 実験結果



(b) 各スコアが正規分布だと仮定した場合

図 4　実験システムにおける FRR, FAR
Fig. 4　FRR and FAR of prototype system.

6. 考　　察

6.1 要求 1 に関する考察

今回のプロトタイプシステムは画像ベースの類似度によって認証可否を判定しているため，本節では，画像に対する最も一般的な偽造手段である「印刷」に焦点を当てて提案方式の偽造耐性を考察する．

今回のプロトタイプシステムでは，皮膚をマイクロスコープで撮影した約 200 倍の肌理画像を認証に用いている．図 5 (a) は手の甲の約 2.0 × 1.5 mm の領域を 200 倍のマイクロスコープで撮影した画像である．この画像をプリンタ A（Brother MFC-8520DN），プリンタ B（FUJI Xerox DocuPrint C525 A），プリンタ

(注3)：**4.4** で示した本プロトタイプシステムのマッチング処理における射影変換の効果を確認するために，**4.4** 手順 2 の処理③～⑭を割愛した形態で同様の評価を実施したところ，スコア①とスコア②間では，認証しきい値 ≒ 0.13 の際に EER ≒ 0.54%であった．スコア①とスコア③間においては，認証しきい値 ≒ 0.12 で EER ≒ 0.45%であった．

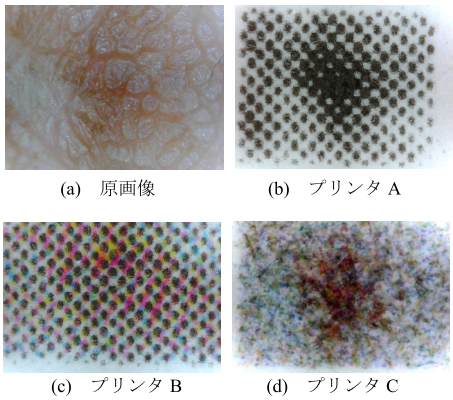


図 5 市販プリンタによる偽造
Fig. 5 Forged images made by consumer-level printers.

C（Canon PIXUS MP610）を使って，印刷サイズがそれぞれ約 2.0 × 1.5 mm の大きさとなるように最高解像度で印刷した画像が図 5 (b)(c)(d) である．解像度の低い市販向けのプリンタでの偽造物は，本物と比べ大きく異なることが確認できる．このように，200 倍程度の倍率であっても，現在の市販品レベルのプリンタでは偽造が不可能であるため，偽造に要する不正者のコストを増加させることが達成できている（要件 1 が達成できている）．

不正者が高解像度のプリンタを使用した場合は，画像ベースの類似度を用いるだけでは不十分となる可能性もある．ただし，微細領域を高倍率で観察するマイクロ生体認証なら，汗腺から汗の分泌を確認することも可能であり，生体検知を組み込みやすいという利点があると期待される．また，撮影用の照明を斜め方向から照射することで，肌理の凹凸パターンに応じた影が発生するため，立体物かどうかの判定も可能であろう．

なお，本来であれば，プロトシステムに限定した議論ではなく，マイクロ生体認証という方式全体に関し，「どれだけの微小さが必要か」について評価すべきである．しかし，複製技術は時代とともに進歩するため，定量的な分析は困難である．ただし，少なくとも光の波長程度までのサイズの物体であれば，レンズを使うだけで高倍率の画像を撮像し得るため，「撮影する技術のほうが複製する技術よりも容易である」という論述は原理的には成り立つと考えられる．

6.2 要求 2 に関する議論

5.3 に示した結果より，同じ被験者の同じ箇所間の FRR と同じ被験者の異箇所間の FAR を求めた結果，それらの EER は約 0.01%であった．本結果は，同じ被験者であっても利用する肌理の部位が違えば，異なる生体情報としてみなせることを意味している．すなわち，登録部位を変更することによって，登録情報（生体情報）を手掛かりとした同一ユーザの名寄せを断ち切ることができる（要件 2 が達成できている）．

人間の肌の総表面積は約 1.6 m^2 であるといわれているため [16]，仮に 1.0 × 1.0 mm を登録面積とすると，理論上約 1.6×10^6 通りの生体情報を利用可能となる．服を脱がないと採取できない部位を考慮したとしても，数千から数万パターンの生体情報が利用可能である．これらのパターンを利用することで，ユーザは自身の登録生体情報を更新し続けることが可能となる．

6.3 要求 3 に関する考察

5.3 に示した結果より，今回の評価実験において，プロトタイプシステムが有する EER は同被験者異箇所間で約 0.01%，異被験者間で約 0.01%であった．筆者らが知る限り，提案方式と同等の認証精度を誇る動的生体認証は存在しない．したがって，プロトタイプシステムは，要求 3（静的な生体情報の利用による認証精度の確保）を満たしているといえる．

6.4 シールの利用

今回のプロトタイプシステムでは，位置合わせ用のマークに油性インクを利用した．位置合わせ用のマークにはシールを利用することも可能である．シールの利用は油性インクに比べて，価格はわずかに高くなるが，シールに更に補助情報を所持させる（シールの表面に印字する，あるいは，シールに RFID を埋め込む）ことで様々な応用が可能である．例えば，シールにユーザ ID に関する情報を付加すれば，生体情報の提示とともにユーザ ID の読み取りが可能となり，ユーザ ID の提示を必要とする 1 対 1 型の認証であっても，ユーザ ID の入力が不要となる．シールに乱数情報を付加すれば，持ち物なしでキャンセラブル生体認証の運用が可能となる．シールにヘルパー情報（誤り訂正情報）を付加すれば，持ち物なしでバイオメトリック暗号 [17] の運用が可能である．

6.5 総当たり攻撃に関する考察

提案方式は従来の生体認証方式と異なり，ユーザ個々人が自身の身体の中に数多くの登録可能部位を有する方式となっている．そのため，不正者は正規ユーザの生体を盗む手間をかけることなく，不正者自身の生体情報を用いてある程度のボリューム（**6.2** の議論

に基づけば，1.6×10^6 通りの情報を利用可能である）の総当たり攻撃をしかけることが可能である．

この攻撃に対する詳細な分析は今後行っていく必要がある．ただし，この対策として，シールそのものの人工物メトリクスも併用し，生体情報とシールの双方の固有パターンを利用して認証を行うという方法が考えられる．生体とシールに含まれる情報が揃わなければ認証できないため，総当たり攻撃に対する耐性が飛躍的に増大するだけでなく，偽造コストを増加させるという点でも大きな効果が期待できる．

7. むすび

本論文では，生体部位の微細パターンを利用するマイクロ生体認証方式を提案した．取り扱う生体情報は微細であるため偽造困難性が高く，部位を変更することで更新も可能である．本論文では，マイクロスコープで撮像された微細肌理画像を利用したマイクロ生体認証のプロトタイプシステムを提案・実装・評価した．被験者 10 名による小規模な実験ではあるものの，評価実験の結果，EER $\fallingdotseq 0.01\%$の認証精度が得られ，提案方式の有用性が確かめられた．

今後は，認証画像の位置合わせの自動化など，システムを更に改良するとともに，より微細な領域を利用した認証の実現可能性の評価，肌理以外の微細パターンの利用についても模索する．マイクロ生体認証に関する攻撃方法に関しても更に検討を深めていく予定である．

謝辞　静岡大学大木哲史講師にはマッチング手法及び精度評価に関しての有益な助言を頂いた．静岡大学中谷広正教授，佐治斉教授には画像処理手法に関しての有益な助言を頂いた．ここに深く謝意を表する．

文　献

[1] FIDO Alliance, Inc., “FIDO 1.0 Specifications are Published and Final Preparing for Broad Industry Adoption of Strong Authentication in 2015 (online),” available from https://fidoalliance.org/news/item/fido-1.0-specifications-published-and-final1 (accessed 2015/02/26).

[2] 高橋健太，村上隆夫，加賀陽介，松原佑生子，米山裕太，本部栄成，西垣正勝，“テンプレート公開型生体認証基盤，” 2012 年暗号とセキュリティシンポジウム予稿集，no.1F1-3, 2012.

[3] 星野　哲，松本弘之，松本　勉，“指紋画像からの人工指作製，” 2011 信学技報，ISEC2001-60, 2001.

[4] Z. Kleinman, “Politician’s fingerprint ‘cloned from photos’ by hacker (online),” available from http://www.bbc.com/news/technology-30623611 (accessed 2015/02/07).

[5] C. Rathgeb and A. Uhl, “A survey on biometric cryptosystems and cancelable biometrics,” J. Information Security, pp.1–25, 2011.

[6] 宇根正志，田村裕子，“生体認証における生体検知機能について，” 金融研究，vol.24, 別冊 2, pp.1–56, Dec. 2005.

[7] 瀬戸洋一，“バイオメトリックセキュリティ認証技術の動向と展望，” 情報処理学会，vol.47, no.6, pp.571–576, June 2006.

[8] バイオメトリクスセキュリティコンソーシアム，バイオメトリックセキュリティ・ハンドブック，バイオメトリクスセキュリティコンソーシアム，オーム社，東京，2006.

[9] Bank of Japan, “Security features of the new bank of Japan notes (online),” available from https://www.boj.or.jp/en/note_tfjgs/note/security/bnnew3.htm/ (accessed 2017/03/13).

[10] 松本　勉，岩下直行，“金融業務と人工物メトリクス，” 金融研究，vol.23, no.2, pp.169–186, June 2004.

[11] 松本　勉，花木健太，鈴木僚介，関口大樹，法元盛久，大八木康之，成瀬　誠，竪　直也，大津元一，“レジスト倒壊パターンを用いたナノ人工物メトリクスとその評価，” 2014 年暗号とセキュリティシンポジウム予稿集，no.2E2-3, 2014.

[12] V. Woollaston, “The hi-tech tattoo that could replace ALL your passwords: Motorola reveals plans for ink and even pills to identify us (online),” available from http://www.dailymail.co.uk/sciencetech/article-2333203/Moto-X-Motorola-reveals-plans-ink-pills-replace-ALL-passwords.html (accessed 2013/08/20).

[13] 白土寛和，野々村美宗，前野隆司，“肌質感を呈する人工皮膚の開発（皮膚の表面凹凸パターンと弾性構造の模倣に基づく肌質感の実現と評価），” 機械学論，vol.73, no.726, pp.541–546, 2007.

[14] 荒川尚美，大西浩之，舛田勇二，“ビデオマイクロスコープを用いた皮膚の表面形態解析法の開発とキメ・毛穴の実態評価，” 日本化粧技術者会誌，vol.41, no.3, pp.173–180, 2007.

[15] “OpenCV,” available from http://opencv.org/ (accessed 2015/03/13).

[16] A.E. Bender and D.A. Bender, “Body surface area,” in A Dictionary Food and Nutrition, Oxford University Press, Oxford, England, 1995.

[17] A. Juels and M. Wattenberg, “A fuzzy commitment scheme,” Proc. 1999 ACM Conference on Computer and Communications Security, pp.28–36, 1999.

[18] 産経新聞，“「ピースサインは危険!!」3 メートル離れて撮影でも読み取り可能，” available from http://www.sankei.com/affairs/news/170109/afr1701090002-n1.html (accessed 2017/03/17).

[19] 眞野勇人，兼子拓弥，高橋健太，西垣正勝，“マイクロ生体認証の提案とその一事例報告，” 信学技報，BioX2014-64, 2015.

[20] M. Fujita, Y. Mano, T. Kaneko, K. Takahashi, and M. Nishigaki, “A micro biometric authentica-

tion mechanism considering minute patterns of the human body," Proc. 19th International Conference on Network-Based Information Systems, pp.159–164, 2016.

（平成 29 年 3 月 21 日受付，8 月 2 日再受付）

藤田　真浩

2013 年静岡大学情報学部情報科学科卒業．2015 年同大学院修士課程修了．現在，同創造科学技術大学院博士後期課程．情報セキュリティ，ヒューマンインタフェースに関する研究に従事．2016 年度情報処理学会山下記念研究賞受賞．2016 年度電子情報通信学会バイオメトリクス研究専門委員会 BioX 研究会奨励賞受賞．

眞野　勇人

2012 年会津大学コンピュータ理工学部卒業．2015 年静岡大学大学院修士課程修了．在学中，情報セキュリティに関する研究に従事．

村松　弘明

2015 年静岡大学情報学部卒業．2017 年同大学大学院修士課程修了．在学中，情報セキュリティに関する研究に従事．

高橋　健太　（正員）

1998 年東京大学理学部情報科学科卒業．2000 年同大学大学院理学系研究科情報科学専攻修士課程修了．同年 (株) 日立製作所入社．2012 年東京大学大学院情報理工学系研究科博士後期課程修了．博士 (情報理工学)．2015 年より東京大学大学院客員准教授．現在，(株) 日立製作所研究開発グループユニットリーダ主任研究員．生体認証，暗号技術及び情報セキュリティの研究開発に従事．2008 年情報処理学会論文賞，2011 年 SISAP Best paper，2012 年 IEEE BTAS Best reviewed paper，2015 年情報処理学会長尾真記念特別賞，2016 年ドコモ・モバイル・サイエンス賞先端技術部門優秀賞，関東地方発明表彰発明奨励賞など受賞．情報処理学会，電子情報通信学会各会員．

西垣　正勝　（正員）

1990 年静岡大学工学部光電機械工学科卒業．1992 年同大学院修士課程修了．1995 年同博士課程修了．日本学術振興会特別研究員（PD）を経て，1996 年静岡大学情報学部助手．同講師，助教授の後，2006 年より同創造科学技術大学院助教授．2007 年同准教授，2010 年同教授．博士（工学）．情報セキュリティ全般，特にヒューマニクスセキュリティ，メディアセキュリティ，ネットワークセキュリティ等に関する研究に従事．2013–2014 年情報処理学会コンピュータセキュリティ研究会主査．2015–2016 年電子情報通信学会バイオメトリクス研究専門委員会委員長．2016 年より日本セキュリティマネジメント学会常任理事．