Micro Biometric Authentication : A proposal and a case study

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

信学技報
IEICE Technical Report

マイクロ生体認証の提案とその一事例報告

眞野 勇人† 兼子 拓弥† 高橋 健太‡ 西垣 正勝†

†静岡大学大学院情報学研究科 〒432-8011 浜松市中区城北 3-5-6
‡(株)日立製作所横浜研究所 〒244-0817 横浜市戸塚区吉田町 292
E-mail: †nisigaki@inf.shizuoka.ac.jp

あらまし 生体情報は基本的に生涯不変である性質を持つため，漏洩した場合のリスクは非常に大きいものとなる．このため，使用する生体部位を利用者が任意のタイミングで更新することが可能な生体認証が強く望まれる．また，その際，偽装生体の作成の脅威，および，生体部位から抽出されるユーザ本人に関する情報量が十分低くなければならない．また，実用レベルの認証精度を有することも必要である．これらの要件を満たすために，本研究では，生体部位の微細パターンを利用したマイクロ生体認証方式を提案する．本論文では，そのプロトタイプとして，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，基礎実験から提案方式の可能性を示す．

キーワード 生体認証，生体情報，微細生体部位，肌理

Micro Biometric Authentication：A proposal and a case study

Yuto MANO† Takuya KANEKO† Kenta TAKAHASHI‡ and Masakatsu NISHIGAKI‡

†Shizuoka University 3-5-1 Johoku, Naka-ku, Hamamatsu, 432-8011 Japan
‡Yokohama Research Laboratory, Hitachi, Ltd. 292 Yoshida-cho, Totsuka-ku, Yokohama-shi, Kanagawa, 244-0817 Japan
E-mail: †nisigaki@inf.shizuoka.ac.jp, ‡kenta.takahashi.bw@hitachi.com

Abstract The biometric information are unchangeable basically throughout the life, and hence there is a high risk in the case of the leak. Therefore, a biometric authentication that a user can reregister body parts in any time is desirable. In addition, a threat of the generation of counterfeit and a disclosurability for user's personal information extracted from the body part should be reduced enough. To satisfy the requirements, we propose a micro-biometric authentication using the minute pattern of the body part in this study. In this article, we implemented a prototype system for the micro-biometric authentication using the human skin texture imaged by a microscope.

Keywords biometric authentication, biometric information, micro biometrics, skin texture

1. はじめに

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，今後さら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．その一つが，生体情報の「基本的に生涯不変であり，任意に更新できない」という性質に起因するなりすましの問題，および，プライバシ侵害の問題である．もう一つが，生体情報の「測定の度に読取誤差が混入する」という性質に起因する認証精度の問題である．

「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（課題 1）．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も報告されている[3][4]．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画質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，不正な生体情報読取装置を密かに仕込んで生体情報を収集したり，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て生体情報をフィッシングすることも可能である．

「プライバシ侵害」は，追跡可能性（traceability）と暴露可能性（disclosurability）の問題がある．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．すなわち，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（課題 2）．また，生体情報は，個人の身体的な情報であり，生体情報から本人を特定することや，本人に関する副次的な情報（DNA から得られる劣性遺伝子情報がその典型例）を得ることが可能である．そのため，暴露可能性の観点からも生体情報の保護が求められる（課題 3）．

「認証精度」は，本人拒否と他人受入の問題である．生体情報は基本的にアナログ情報であり，登録および認証の度に読取誤差が混入するため，本人であったとしても生体情報は完全には一致せず，本人拒否が発生する．一方で，生体情報は基本的に他人間であっても類似した形状となる（例えば，指紋が市松模様の形状となっている人はいない）ため，他人受入が発生しやすい傾向にある．また，一般的に，手書き署名や音声などの動的な生体情報のほうが，指紋や静脈などの静的な生体情報よりも本人内変動が大きい[5][6]．このため，認証精度の低さは，動的生体認証において特に顕著な問題として認識されている（課題 4）．

課題 1〜3 を部分的に解決する方法として，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[7]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，課題 1（偽造生体の作成）および課題 3（暴露可能性）の問題に対処できる．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，課題 2（追跡可能性）の問題に対処できる．しかし，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．

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[8]や生体情報読取装置の真正性を検査するデバイス認証[9]が存在する．しかし，これらはいずれも課題 1（偽造生体の生成）に対処するものであり，課題 2（追跡可能性）および課題 3（暴露可能性）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，課題 1〜3 のリスクを低下させることができる対策が，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ため，課題 4（動的生体認証の精度）が未解決な問題として残る．また，動的生体認証には，訓練や機器による模倣（音声の場合はモノマネや録音）の脅威も存在する．

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，課題 1〜4 のすべてを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．そこで本研究では，「課題 2 に配慮した認証方式」と「課題 1，課題 3，課題 4 に配慮した生体情報」の組合せによって，課題 1〜4 を満たす生体認証を実現する．

「課題 2（追跡可能性）に配慮した認証方式」とは，使用する生体情報をユーザが任意のタイミングで更新可能な生体認証である．ユーザが生体情報を更新する度に，追跡可能性が分断されることになる．「課題 1（偽造生体の作成），課題 3（暴露可能性），課題 4（動的生体認証の精度）に配慮した生体情報」とは，微細生体部位の静的な生体情報である．認証のために利用する生体部位が微細になればなるほど，不正者側の偽造コストは大きく増すことになり，かつ，生体部位から得られる「ユーザ本人に関する情報」が小さくなる．また，生体部位が微細になるほど，生体部位の更新可能回数（微小部位を 1 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）も増加する．生体部位の静的な生体情報を利用するため，認証精度も（動的生体認証と比較して）高い．

本論文では，そのプロトタイプとして，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，基礎実験から提案方式の可能性を示す．以降，2 章では関連技術・関連研究を，3 章では提案方式を，4 章でまとめを記す．

2. 関連技術・関連研究

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[10]. 証券や紙幣などに利用されており，（読取りや）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]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）を持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，微細パターン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する方式が研究されている[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[7]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$X \to T = F_R(X)$と変換する．
4. Tをサーバに登録する．
5. 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$X' \to F_R(X')$と変換する．
4. Tと$F_R(X')$が十分類似していれば認証成功とする．

ここで，$F_R(\cdot)$は乱数Rによる変換処理を表す．乱数や変換関数を変更することで，テンプレート情報の更新が可能である．

2.4. 貼付型生体認証トークン

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方式として，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].

これらの技術は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，生体情報そのものの漏えいに対処するためには，課題 1〜4 への対応が必要である．「静的な生体情報のワンタイム化」が実現できれば，課題 1〜4 のすべてを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．そこで本研究では,「課題 2 に配慮した認証方式」と「課題 1，課題 3，課題 4 に配慮した生体情報」の組合せによって，課題 1〜4 を満たす生体認証を実現する．

「課題 2 に配慮した認証方式」とは，使用する生体情報をユーザが任意のタイミングで更新可能な生体認証である．静的な生体情報をワンタイム化することは基本的には不可能であるので，生体情報の更新によって課題 2（追跡可能性）に対応する．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情報を別の生体情報に変更する．ユーザが生体情報を更新する度に，追跡可能性が分断されることになる．

「課題 1，課題 3，課題 4 に配慮した生体情報」に関しては，まず，課題 4（動的生体認証の精度）に配慮し，静的な生体情報を用いることが要件となる．

課題 1（偽造生体の作成）に関しては，偽造生体の作製にかかるコストをできる限り大きくすることが肝要となる．すなわち，特殊な技術，素材，あるいは装置がなければ偽造生体が製造できないようにすることが必要である．その候補の一つとして考えられるものが，超微細加工でなければ偽造できない生体情報である. 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，それ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する．

微細生体部位の利用は，課題 3（暴露可能性）に対しても有効なアプローチとなる．認証のために利用する生体部位が微細になればなるほど，微細生体部位から得られる「ユーザ本人に関する情報」が小さくなる．更に，生体部位が微細になるほど，生体部位の更新可能回数（微小部位を 1 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）も増加するため，課題 2（追跡可能性）に対する効果も強化されることになる．

微細生体部位を利用する場合は，生体情報の撮像精度に加え，登録部位を発見する際の精度も要求されることになる．今回は登録部位の目印としてシールを生体に直接貼付する方法を検討する．RFID 回路を皮膚に直接貼り付ける電子タトゥー型の認証トークン[12]の例から，絆創膏やサージカルテープのように装着していることがほとんど感じられない貼付物であれば，ユーザも負担なく貼付物を常時装着できると考えられる．シールの位置を貼り変えることにで，登録部位の位置情報の更新，すなわち登録情報の更新が可能である．

シールは生体部位の位置を特定する単なるマーカであり，シールそのものの情報でユーザ認証が行われるものではないことに注意されたい．電子タトゥー方式では貼付トークンそのもので認証するため，廃棄後のトークンが悪用される恐れがあり，この点で提案方式とは大きく異なる．また，シールに補助情報を印字または埋め込むことによって，シールの補助情報とユーザの生体情報をセットにして認証を実施することも可能である．

3.2. 肌理とその認証への応用

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]．肌理はこれらの要素により形作られるものである．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]．皮膚紋様は大きくとも数百 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）に注目した．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，指紋や掌紋の様に個人認証に利用することが可能となる．ただし，年齢や季節により，肌理の粗さや皮溝の深さが変化することが示唆されており，生涯不変の情報ではないと推察される．そのため短期的な認証に向く生体情報であると考えられる．

皮膚表面の形態情報の取得には主に 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，三次元スキャナー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である[14]．

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. 提案方式

以下では，マイクロスコープによって撮像される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（図 1）．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．

【登録フェーズ】

1. ユーザは，ユーザ ID を決定しシステムに登録する．
2. システムは，位置合わせ用のシールを印刷する．
3. ユーザは，自分の肌の任意の位置にシールを貼付する．
4. システムは，シールが貼付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．X はデータベースに登録される．

【認証フェーズ】

提案方式における認証フェーズにおいては，ユーザがシールを貼付し続けていることが前提となる．

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，シールが貼付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．

ユーザがシールを剥がしてしまえば，システムは登録部位を発見することが難しくなるため，本人でさえ認証に成功することが困難になる．よって，シールの管理を通じて，ユーザ自身が認証可能期間をコントロールできる．

上記の説明ではシールに位置合わせのためのマーカとしての機能のみを持たせているが，シールにさらに補助情報を所持させる（シールの表面に印字したり，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[15]が可能である．

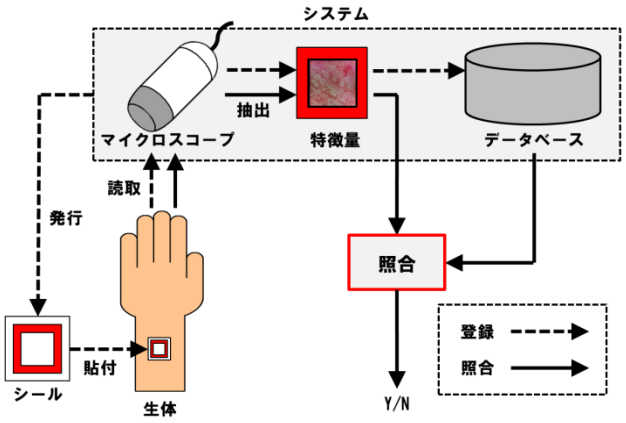

図 1：マイクロ生体認証方式の概念図

4. まとめ

生体情報そのものが漏えいした場合のリスクを低下させるために，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，提案方式のプロトタイプとして，マイクロスコープとシールを用いた認証システムを提案した．本方式は，微細パターンの特性上，既存の生体認証と比べても，他人受け入れが起こりにくい認証方式である．

今後は，シールによる位置合わせの自動化や，より微細な領域での実現性の評価など，提案システムの認証方式をさらに改良するとともに，肌理以外の微細パターンを利用した認証システムの提案も行っていきたい．

謝　辞

本研究の過程におきまして議論を通じて多くの知識や示唆を頂いた産業技術総合研究所の大塚玲様，大木哲史様に感謝申し上げます．

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),” <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，論文 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 電子情報通信学会技術研究報告，ISEC2001-60，Vol.101, No.311, pp.53-60, 2001.

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

[5] 梅本功太，西垣正勝，“人間の動作を用いた認証方式に関する検討，” マルチメディア，分散，協調とモバイルシンポジウム論文集，pp.1338-1346, 2007.

[6] 梅本功太，西垣正勝，“限界能力認証：握力を用いた生体認証方式に関する検討，” バイオメトリックシステムセキュリティ研究会，第 12 回研究発表回予稿集，pp.31-35, 2008.

[7] N. K. Ratha, J. H. Connell and R. M. Bolle, “Enhancing Security and Privacy in Biometrics-based Authentication Systems, ”IBM Systems Journal, Vol.40, No.3, pp.614-634, 2001.

[8] 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.

[9] 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

[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，論文 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），” 日本機械学会論文集，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] Ari Juels, Martin Wattenberg, “A Fuzzy Commitment Scheme,” Proceedings of 1999 ACM Conference on Computer and Communications Security, pp.28-36, 1999.