生体検知とQRコードの導入によるマイクロ爪認証の改良にむけての一検討

生体検知と QR コードの導入による マイクロ爪認証の改良にむけての一検討

塩見 祐哉[1]　大内 結雲[1]　奥寺 瞭介[1]
藤田 真浩[1]　眞野 勇人[1]　大木 哲史[1]　西垣 正勝[1]

概要：マイクロ生体認証とは人間の微細部位の生体情報を利用した生体認証である．著者らは爪表面の微細部位を用いることで物理的な生体情報において「忘れられる権利を満たす生体認証」の提案を行った．しかし，提案したシステムには安定性，利便性，同時刻照合困難性の観点から課題が存在していた．本稿ではそれらの課題を解決するために，末梢血流による反応性充血を用いた生体検知と QR コードを用いた補助情報添付を導入したマイクロ爪認証の提案を行った．その結果，生体検知を用いたなりすまし耐性の強化によって，先行方式における「忘れられる権利を満たす生体認証の要件」を確保しつつ，安定性の改善を行った．さらに，QR コードを爪表面に印刷し，認証時に利用することで先行方式において達成できなかった 1:N 認証や複数サービス間での生体情報照合耐性の実現を行い，利便性，同時刻照合困難性の観点における課題解決を行った．

キーワード：マイクロ生体認証　爪表面　QR コード　生体検知

Study on the Improvement of Micro-Nail Authentication by Introducing Liveness Detection and QR Code

Yuya Shiomi[1]　Yumo Ouchi[1]　Ryosuke Okudera[1]
Masahiro Fujita[1]　Yuto Mano[1]　Tetsushi Ohki[1]　Masakatsu Nishigaki[1]

Abstract: Micro-biometric authentication is a biometric authentication system that uses biometric information of small human body parts. We proposed a "biometric authentication that satisfies the right to be forgotten" in physical biometric information by using a minute part on the nail surface. However, the proposed system has some problems in terms of stability, convenience, and difficulty registering multiple services at a certain time. In this paper, we proposed a micro-nail authentication system that introduces biometric detection using reactive hyperemia in peripheral blood flow and QR code as an auxiliary information attachment to solve these problems. We have improved the stability of the system by enhancing the resistance to identity theft using biometric detection, while maintaining the requirements of biometrics to satisfy the right to be forgotten in the preceding method. In addition, we have achieved 1:N authentication and tolerance of biometric information matching between multiple services by printing a QR code on the surface of the nail and using it for authentication, which could not be achieved in the previous system, as well as solving the problems in terms of convenience and difficulty in matching the same time.

Keywords: Micro-Nail Authentication, Nail Surface, QR Code, Liveness Detection

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．生体認証には，キーボード操作を必要としないという利点に加え，忘却・紛失・盗難の恐れがないという利点があり，様々な場面において広く用いられている．しかし，生体認証において使用される生体情報は重大な個人データであり，その取扱いには多大な配慮が必要となる．その中でも，消去権の保障は特に難度の高い課題である．生体情報は生涯不変であるため，一旦漏洩してしまうと取り換えが利かない．この問題に対し，著者らは「忘れられる権利を満たす生体認証」として爪の微細部位を用いたマイクロ生体認証を提案した[1]．マイクロ生体認証とは人間の微細部位の生体情報を利用した生体認証である．本稿では，爪の微細部位を用いたマイクロ生体認証を「マイクロ爪認証」と呼称する．

本稿は，文献[1]のマイクロ爪認証（以下，先行方式）を安定性，利便性，同時刻照合困難性の 3 つの観点から改良する．安定性の観点から見た先行方式の課題について述べる．先行方式では「忘れられる権利を満たす生体認証」が有すべき要件を，約 200 倍の高倍率撮影により得られる爪表面の微細特徴により担保していた．しかし，高倍率での

1 静岡大学
Shizuoka University

撮影は被写体との接眼距離が極端に短くなる上にわずかな手ブレが大きなノイズとなるため，認証部位の撮影が困難であるだけでなく，品質の良い撮影画像を得ることが難しいという問題を残していた（課題 1）．利便性の観点から見た先行方式の課題について述べる．生体認証の大きなメリットの一つが「手ぶらでの認証（1:N 認証）」であるが，実際には生体情報のエントロピ（正確には，ある生体認証装置に対する生体情報のエントロピ）の低さが阻害要因となる．このため，ある程度の数以上のユーザを 1 つの生体認証システムに収容する場合には 1:N 認証の実現が困難であり，ユーザ ID 等の補助情報を追加して 1:1 認証型の形態を採るか，複数の生体情報を併用してマルチモーダル型の形態を採る必要がある（課題 2）．同時刻照合困難性の観点から見た先行方式の課題について述べる，マイクロ爪認証では，爪の生え変わり（あるいは，爪表面をやすりで擦る）によって生体情報を物理的に失効させる．これにより，時間経過に基づく生体情報の廃棄，更新を実現している．しかし，ある時刻においては個々の生体認証（爪）は 1 つしか存在しない．すなわち，同時に複数のサービスに生体情報を登録する場合には同一の生体情報を登録しなければならない．このため，複数サービス間で生体情報が照合されるリスクが残る（課題 3）．

これらの課題に鑑み，本稿では，反応性充血を用いた生体検知と QR コードを用いた補助情報添付を導入したマイクロ爪認証（以下，提案方式）を提案する．課題 1 については，爪表面にて観測される「末梢血流による反応性充血」を用いた生体検知を導入することによって，マイクロ爪認証のなりすまし耐性（Unforgeability）を強化する．これにより，撮影倍率を中倍率（約 50 倍）に下げても「忘れられる権利を満たす生体認証の要件」を確保することを可能とし，先行方式に対する安定性の改善を試みる．課題 2 については，ユーザ ID を埋め込んだ QR コードを爪に添付することによって，1 回の撮像によってユーザ ID（QR コード）と生体情報（爪表面）を同時に取得し，爪を提示するだけで 1:1 認証を実行することを可能とする．これにより，低エントロピの生体情報（爪）を用いながら手ぶら認証を達成し，先行方式に対する利便性の改善を試みる．課題 3 については，乱数を埋め込んだ QR コードを爪に添付することによって，キャンセラブル生体認証の適応を可能とする．これにより，物理的な生体情報（爪）は 1 つであるが，サービスサイトごとに異なるテンプレートを登録させることを可能とし，先行方式に対する同時刻照合困難性の改善を試みる．

2. マイクロ爪認証（先行方式）

2.1 忘れられる権利を満たす生体認証の要件

著者らは，文献[1]にて，忘れられる権利を満たす生体認証に求められる要件として，以下の 5 つの要件を定義した※a.

1 Unforgeability：認証システムに提示した登録生体情報が漏洩したとしても，その情報を用いた他人がシステムに認証されないこと．
2 Un-linkability：認証システムに提示した登録生体情報を利用して，意図しない他のシステムに登録されている生体情報との照合ができないこと．
3 Diversity：同じ生体部位から異なる生体情報を生成可能であること．
4 Disposability：漏洩した生体情報を利用不可にし，新しい生体情報を登録して安心安全にシステムを利用できること．
5 Performance：上記の条件を満たすにあたり，本人拒否率，他人受入率を劣化させないこと．

文献[1]では，要件 1〜5 を満たす生体認証として「爪表面の微細部位を用いたマイクロ生体認証(マイクロ爪認証)」の提案を行った．マイクロ爪認証は，下記のとおり，要件 1〜4 を満たす．また，要件 5 については，実証実験によりこれが満たされることを確認した．

要件 1：

一般に，認証情報の物理サイズが微細になるほど，偽造生体を精密に作成するためのコストが高まる．一方，拡大鏡などで対象物の微細部分を撮影することは，偽造物を作成するより，はるかに容易である．この撮影コストと偽造コストの非対称性により，認証システムに登録されている生体情報が漏洩したとしても，攻撃者が偽造生体を作成してなりすましに成功するまでの障壁を高められることが期待される．この結果，要件 1 が満たされる．

要件 2：

爪は 1 指につき 1 つしかないが，登録情報が 1 mm 四方の微細部位であれば，1 つの爪の表面中（表面積を 1 cm^2 と想定）に異なる 100 部位が存在することになる．したがって，ユーザは異なる認証システムごとに別の部位を登録することが可能であり，異なる認証システムに登録されているユーザの生体情報間の名寄せを攻撃者が行うことは困難である．これにより，認証システムに登録されている生体情報のみを盗取した攻撃者に対し，要件 2 が満たされる．

攻撃者が認証システムに登録されている生体情報に加え，ある時点におけるユーザの爪表面の全体画像をも盗取した場合には，登録生体情報と全体情報とのパターンマッチングを行うという攻撃が可能である．このような攻撃に

※a　文献[1]では，Diversity の部分要件として Disposability を説明しているが，本稿では両者を別要件として記載する．

対しては，異なる認証システムで別の微細生体部位を登録していたとしても，全体画像の情報を媒介として異部位の生体情報が名寄せされてしまう．しかし，短期的にはユーザが故意に紙やすりなどで爪を擦ることにより，長期的には爪の生え変わりにより，攻撃者が盗取した爪表面の全体画像は不能となる．この結果，ユーザの爪表面の全体画像を盗取する攻撃者に対しても，要件 2 が満たされる．

要件 3：

前述のとおり，1 つの爪の中に 100 部位の登録情報が存在する．よって，ユーザは，使用する爪を変えることなく，パスワードの変更やトークンの交換と同様の感覚で登録部位を変更することが可能となる．これにより，要件 3 が満たされる．

要件 4：

紙やすりなどで爪表面を擦ることによって，それまでの登録情報を完全に廃棄することも可能である．これにより，短期的な観点で要件 4 が満たされる．また，爪の生え変わりによって新たな登録可能部位が順次成長してくるため，長期的な観点においても要件 4 が満たされる．

2.2 先行方式の課題

文献[1]にて提案したマイクロ爪認証には安定性，利便性，同時刻照合困難性の観点の課題が存在していた．本節ではその課題点について概説する．

2.2.1 課題 1：安定性

先行方式では「忘れられる権利を満たす生体認証」が有すべき要件の中の Unforgeability および Diversity の要件を，200 倍の高倍率撮影により得られる爪表面の微細特徴により担保していた．しかし，高倍率での撮影は被写体との接眼距離が極端に短くなる上にわずかな手ブレが大きなノイズとなるため，認証部位の撮影が困難であるだけでなく，品質の良い撮影画像を得ることが難しい．

2.2.2 課題 2：利便性

生体認証の大きなメリットの一つが「手ぶらでの認証（1:N 認証）」である．しかし，実際には生体情報のエントロピ（正確には，ある生体認証装置に対する生体情報のエントロピ）の低さが阻害要因となり，ある程度の数以上のユーザを 1 つの生体認証システムに収容する場合には 1:N 認証の実現は困難となる．

このため先行方式では，「ユーザ ID」という補助情報を追加し，1:1 認証の形態でマイクロ爪認証を実装し，評価を行った．1:1 認証の場合も，ユーザの氏名等をユーザ ID として用いてやれば，「手ぶらでの認証」を実現できる．たたし，認証装置にユーザ ID（氏名）を入力するという手間がユーザに課されることになる．

1:N 認証を実現するもう一つの方法が，複数の生体情報を併用するマルチモーダル生体認証である．近年，インドで導入された国民 ID システム「Aadhaar」では，指紋，顔，虹彩を併用した 1:N 認証が可能となっている[2]．マルチモーダル生体認証においては，コスト（複数の生体情報センサが必要となる），手間（ユーザは複数の生体情報をすべて提示しなければいけない），速度（個々のモーダルの生体認証をすべて実行するため計算量が増加する）の課題がある．

2.2.3 課題 3：同時刻照合困難性

マイクロ爪認証では，1〜2 ヶ月の周期で爪が生え変わることによって，あるいは，ユーザが任意のタイミングで爪表面をやすりで擦ることによって，生体情報が物理的に失効する．これにより，時間経過に基づく生体情報の廃棄，更新を実現している．しかし，ある時刻においては個々の生体認証（爪）は 1 つしか存在しない．すなわち，同時に複数のサービスに生体情報を登録する場合には同一の生体情報を登録しなければならない．このため，複数サービス間で生体情報が照合されるリスクが残る．

3. 関連研究

3.1 キャンセラブル生体認証

テンプレート保護技術の一方式としてキャンセラブル生体認証が存在する[3]．キャンセラブル生体認証では，乱数情報を用いて「符号化された生体情報」をマスクし，これをテンプレートとして認証システムに登録する．乱数情報を変更することにより，テンプレートの廃棄，更新が可能となる．しかし，キャンセラブル生体認証では乱数情報を格納しておくデバイスや IC カードが必要となる．そのため，手ぶらでの認証は基本的に不可能である．

3.2 ウェアラブル生体認証

腕時計や眼鏡といった身体に装着するウェアラブルデバイスが普及している．ウェアラブルデバイスから得られるユーザの動的な生体情報を利用した生体認証の研究開発が始まっている．文献[4]では究極なウェアラブルデバイスの一形態として，皮膚貼付型エレクトロニクスの提案も行われている．今後，身体に情報やデバイスを貼付することで，ICT を活用した人間の能力の拡張は益々一般的になると考えられる．

4. 提案方式

2.2 節で説明した先行方式の課題に鑑み，反応性充血を用いた生体検知と QR コードによる補助情報添付を導入することによって，マイクロ爪認証の改善を試みる．

4.1 反応性充血による生体検知

先行方式における安定性の課題 1 は，高倍率（約 200 倍）での撮影に起因するものであった．そのため，撮影倍率を中倍率（約 50 倍）に下げることで，課題 1 の改善を試みる．しかし，単純に撮影倍率を下げてしまった場合，「忘れられる権利を満たす生体認証」が有すべき要件の中の Unforgeability および Diversity の要件が満たされなくなる．これに対処するために，爪表面の反応性充血を用いた生体検知を導入する．人間の指先には多数の毛細血管が存在す

図 1　爪表面画像(圧迫前)

図 2　爪表面画像(圧迫後)

る．反応性充血とは，それらの血流を圧力等で途絶させた後に圧迫を解いた際には，一時的に血管の拡張が起こり，血流が増加して皮膚が赤くなる現象のことである[6].

マイクロ爪認証においては，爪表面の画像を撮影する際に，指型を使用する（4.3 節で詳述する）．その際に，ユーザに指の腹を指型に押し付けてもらうことによって，爪床部の下層の毛細血管が圧迫される．その後，指の腹の押し付けを解いてもらうことによって，毛細血管を圧迫から解放する．その際の爪床部の色度の変化を確認することで，生体か偽造物かを判定する．図 1，図 2 に圧迫前後による爪床部の色の変化の様子を示す.

4.2 QR コードによる付加情報の添付

先行方式における利便性の課題 2 と同時刻照合困難性の課題 3 は，QR コードを爪に印刷することによって，その改善を図る．課題 2 については，ユーザ ID を埋め込んだ QR コードを爪に添付することによって，1 回の撮像によってユーザ ID（QR コード）と生体情報（爪表面）を同時に取得し，爪を提示するだけで 1:1 認証を実行することを可能とする．これにより，低エントロピの生体情報（爪）を用いながら手ぶら認証を達成し，先行方式の課題 2 が改善される．課題 3 については，乱数を埋め込んだ QR コードを爪に添付することによって，キャンセラブル生体認証の適応を可能とする．これにより，物理的な生体情報（爪）は 1 つであるが，サービスサイトごとに異なるテンプレートを登録させることを可能とし，先行方式の課題 3 が改善される.

QR コードは，大容量の情報を小さな領域に格納できる，高速で安定な読み取りが可能，誤り訂正機能による破損耐性を有する，等の特長から，様々な場面において用いられている．特に，その読み取りの高速性，高精度性，高破損耐性は，マイクロ爪認証に求められる「認証時のリアルタイム性」ならびに「日常生活における爪表面の摩擦や摩耗による QR コードの損傷に対する耐久性」に合致しており，マイクロ爪認証と相性が良いと考える.

QR コードは，テンプレート登録時にネイルプリンタで爪表面に印刷し，トップコートにて保護する．現時点においては，QR コードは爪表面の上半分のエリアのみに印刷し，爪表面の下半分のエリアから認証情報（爪表面の特徴量）を取得することを想定している．マイクロ爪認証においては，爪表面の画像を撮影する際に，指型を使用する（4.3 節で詳述する）．ユーザが指を指型に挿入する動作の中で，マイクロスコープの前を爪表面の上半分が通過する時点で QR コードが撮影され，その後，マイクロスコープの前に爪表面の下半分が到達した時点で認証情報が撮影される．これにより，ユーザは単に指を指型に挿入するだけで，各種補助情報の利用が可能となる.

4.3 撮影機器

撮影用マイクロスコープとして AM7915MZT Dino-Lite Edge S（Dino Lite 社製）を採用している．撮影時の爪の鏡面反射によるノイズを低減するために，専用のマイクロスコープ固定台 DINOMS34B（Dino Lite 社製）と文献[5]にて作成した指型を採用している（図 3）．この指型には指型底面に合致するアタッチメントを連結接続することが可能になっており（図 4，図 5），ユーザの指のサイズに応じて適切な位置，角度にユーザの爪表面を固定することができる（図 6）.

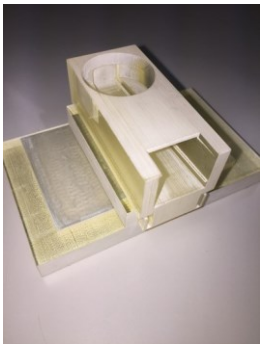

図 3　指型

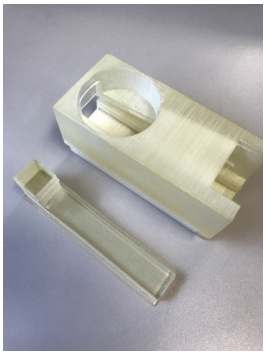

図 4　指型アタッチメント

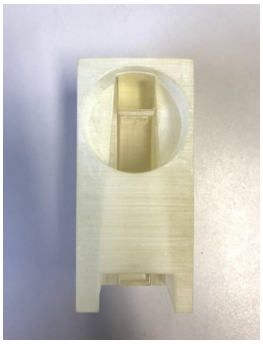

図 5　指型とアタッチメントの連結接続

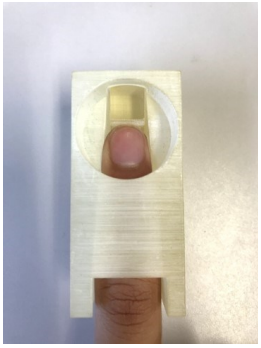

図 6　指型とアタッチメントによる固定

提案方式では，爪表面の画像を撮影する際に，ユーザに指の腹を指型に押し付けてもらうことによって，反応性充血を促す．そこで，指型内部の底面の「指腹部が接するエリア」半球面の突起物を配置し，爪床部の下層の毛細血管が圧迫されやすくなるように工夫した．これによって，ユーザの認証操作に大きな影響を与えず，かつ，爪表面の認証中に生体検知を同時に実行できるようになっている．

5. 考察

5.1 既存要件の達成

撮影倍率を中倍率に変更し，反応性充血による生体検知を導入したことによって，2.1 節に記載した「忘れられる権利を満たす生体認証」の要件がどのように満たされるのかについて説明を行う．なお，要件 5 については今後の実証実験により，満たされるかどうかを確認する必要がある．

要件 1：

既存方式では撮影部位の微細化による偽造物作成困難性によるなりすまし耐性から要件 1 を満たしていた．本方式においても生体検知によるなりすまし耐性から，同程度のなりすまし耐性を有していると考え，要件 1 が満たされる．

要件 2：

撮影倍率の変更により，1 つの爪表面における登録可能部位の数は減少したと考えられる．しかし，一般的な暗号鍵の空間と比べてエントロピが小さいことを考慮すると大差がないと考えられる．さらに，キャンセラブル生体認証の導入により，乱数情報を変更することで異なるテンプレートの登録が可能となるため，要件 2 が満たされると考えることができる．

要件 3：

要件 2 と同様に，キャンセラブル生体認証の導入によって，乱数情報を変更することで登録テンプレートの変更が可能となるため，要件 3 が満たされると考えることができる．

要件 4：

既存方式と同様に爪を用いた認証システムであるので，爪を紙やすり等で擦ることや，生え変わりによって短期，長期の両方の観点で要件 4 が満たされると考えることができる．

5.2 先行方式の課題の改善

先行方式の課題が生体検知や QR コードの導入によってどのように改善されるのかについて考察する．

5.2.1 安定性

反応性充血を用いた生体検知の導入によって既存方式で定義した忘れられる権利を満たす生体認証の要件を満たしつつ撮影倍率を中倍率に変更することが可能となった．これにより，高倍率での撮影に起因する課題を解決し，利便性の向上が期待される．

5.2.2 利便性

認証画像撮影時に QR コードを同時に読み取り，ID 情報を利用することでデータベースに ID と紐づけされているテンプレートと認証画像を比較することが可能になる．これにより 1:1 認証に落とし込むことが可能となり，実質的な 1:N 認証が実現する．本来，生体情報以外に ID カード等の提示物を必要とする生体認証は 1:N 認証とは定義されず，1:1 認証として扱われる．しかし，QR コードの読み取りの高速性や爪表面に直接印刷されていることから，別途提示しなければならないというユーザに対する負担は無いため，ユーザビリティの観点から 1:N 認証と同等のシステムであると考えられる．

5.2.3 同時刻照合困難性

キャンセラブル生体認証を導入し，テンプレート登録時に乱数情報を用いて生体情報をマスクしたものをテンプレートとする．QR コードには複数の乱数情報を格納することができるので，サービス毎に異なる乱数情報を用いることで，同部位の生体情報である場合においても，異なるシステム間で異なるテンプレートを登録することが可能となる．これにより生体情報のリスト攻撃耐性を実現することができる．また，キャンセラブル生体認証を実現するためには乱数情報を IC カード等に格納する必要があり，認証時には生体情報と同時に提示する必要がある．これは手ぶらでの認証や紛失しないことといった生体認証の長所を損なっていると考えられる．しかし，提案方式においては乱数情報を格納した QR コードを認証画像と同時に提示することが可能であり，手ぶらでのキャンセラブル生体認証についても実現する．

6. 今後の予定

本論文で説明を行った内容はコンセプトレベルでの提案であり，現時点において具体的なシステムの実装には至っていない．したがって，今回提案したシステムを実現するために様々な実装や仕様の決定を行う必要がある．今後の予定の一例として，生体検知機能の組み込み実装やキャンセラブル生体認証の導入に向けてのアルゴリズムの検討，QR コードのサイズや誤り訂正レベルの最適化などが挙げられる．その後実験により，本提案システムが有効なものであるかを評価する予定である．

謝辞 提案内容の検討にあたり，日立製作所高橋健太様，加賀陽介様，東京工業大学尾形わかは先生には懇切丁寧なご指導を頂きました．本研究は一部，情報通信研究機構（NICT）の委託研究（契約番号 193）の助成を受けました．

参考文献

[1] 杉本元輝，藤田真浩，眞野勇人，大木哲史，西垣正勝：忘れられる権利に配慮した生体認証：爪を用いたマイクロ生体認証，情報処理学会論文誌，Vol.60，No.12，pp. 2095-2105，(2019).

[2] “インド 13 億人の「生体認証」国民 ID に，知られざる日本企業の貢献”. https://wisdom.nec.com/ja/collaboration/2019051701/index.html(参照 2020-08-14).

[3] Rathgeb, C. and Uhl, A.: A survey on biometric cryptosystems and cancelable biometrics, Journal on Information Security, pp.1–25 (2011).

[4] Marin Okamoto, Mizuho Kurotobi, Shinji Takeoka, Junki Sugano, Eiji Iwase, Hiroyasu Iwata* and Toshinori Fujie,: Sandwich fixation of electronic elements using free-standing elastomeric nanosheets for low-temperature device processes, Journal of Materials Chemistry C, DOI：10.1039/c6tc04469g

[5] 塩見祐哉，杉本元輝，杉本彩歌，上原航汰，藤田真浩，眞野勇人，大木哲史，西垣正勝：爪表面を用いたマイクロ生体認証：実用化に向けての一検討，マルチメディア,分散協調とモバイルシンポジウム 2019 論文集，pp. 1846-1851，(2019).

[6] 蔵本築，矢崎義雄：冠血管の反応性充血，呼吸と循環，Vol.17, No.9, pp.793–799 (1969).