Improvement of Micro-nail Authentication by Introducing Presentation Attack Detection and QR Code

情報処理学会論文誌 Vol.62 No.12 1996–2010 (Dec. 2021)

プレゼンテーション攻撃検知とQRコードの導入によるマイクロ爪認証の改良

塩見 祐哉[1] 大内 結雲[1] 藤田 真浩[1] 眞野 勇人[1] 大木 哲史[1] 西垣 正勝[1,a)]

受付日 2021年3月8日, 採録日 2021年9月9日

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，名寄せ耐性の観点から課題が存在していた．本論文ではそれらの課題を解決するために，反応性充血を用いたプレゼンテーション攻撃検知（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改良を行った．その結果，プレゼンテーション攻撃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」を確保しつつ低倍率での撮影を可能とし，安定性の改善を実現した．さらに，QRコードを爪表面に印刷し，これを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手ぶら（1:N認証）でのテンプレート保護型生体認証を実現し，利便性と名寄せ耐性の改善を達成した．

キーワード：マイクロ生体認証，爪表面，QRコード，プレゼンテーション攻撃検知，手ぶら（1:多）認証

Improvement of Micro-nail Authentication by Introducing Presentation Attack Detection and QR Code

Yuya Shiomi[1] Yumo Ouchi[1] Masahiro Fujita[1] Yuto Mano[1]
Tetsushi Ohki[1] Masakatsu Nishigaki[1,a)]

Received: March 8, 2021, Accepted: September 9, 2021

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 points to be improved in terms of stability, usability, and un-linkability. In this paper, we tried to develop a micro-nail authentication system that introduces presentation attack detection using reactive hyperemia and QR code as an auxiliary information attachment to solve these issues. We have improved the stability of the system by using a lower-magnification microscope, while maintaining the requirements of "biometric authentication that satisfies the right to be forgotten" by equipping presentation attack detection that enhances the resistance against presentation attacks. In addition, by printing QR codes on the surface of fingernails and using them for authentication, we have achieved template-protected biometric authentication with empty-hands (1:N authentication), which enhances the usability and un-linkability of the system.

Keywords: micro-nail authentication, nail surface, QR code, presentation attack, empty-handed (1:N) authentication

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

[1] 静岡大学
Shizuoka University, Hamamatsu, Shizuoka 432–8011, Japan
[a)] nisigaki@inf.shizuoka.ac.jp

必要となる．そのなかでも，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，いったん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．本論文では，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．

本論文は，文献 [1] のマイクロ爪認証（以下，先行方式）を安定性，利便性，名寄せ耐性の 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，高倍率での撮影は被写体との接眼距離が極端に短くなるうえ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 1 つが「手ぶらでの認証（以下，手ぶら認証）」であるが，実際には生体情報のエントロピ（正確には，個々の認証システムを通じて観測される生体情報のエントロピ）の低さが 1:N 認証（手ぶら認証）の障壁となる．このため，ユーザ ID 等の補助情報を追加して 1:1 認証型の形態をとるか，複数の生体情報を併用してマルチモーダル生体認証の形態をとる必要がある（課題 2）．名寄せ耐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，複数のサービスに対して同一生体部位（爪）の異なる微細部位を登録することにより，生体情報の名寄せに対する耐性を高めている．しかし，爪の生え変わり（あるいは，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されるまでの間は，爪表面の全体画像を媒介とした名寄せのリスクが残る（課題 3）．

これらの課題に鑑み，本論文では，反応性充血を用いたプレゼンテーション攻撃検知（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「爪床部の末梢血流の途絶と反応性充血」を用いたプレゼンテーション攻撃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 2，3 については，ユーザ ID と乱数を埋め込んだ QR コードを爪に添付することによって，1 回の撮像によって QR コード（ユーザ ID および乱数）と爪表面（生体情報）を同時に取得し，爪を提示するだけでテンプレート保護型の 1:1 認証を実行することを可能とする．これにより，手ぶらでのテンプレート保護型 1:N 認証を実質的に達成し，先行方式に対する利便性と名寄せ耐性の改善を試みる．

以降，2 章で先行方式を紹介し，先行方式における課題点について概説する．3 章では本論文で用いた関連研究を紹介する．4 章で提案方式について述べ，5 章で今回実装したシステムを紹介する，6 章，7 章で認証精度および偽造耐性に関する基礎実験を行い，提案方式を評価する．8 章で本論文をまとめる．

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，文献 [2], [3], [4] を参考に以下の 5 つの要件を定義した[*1]．

要件 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．

要件 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．

要件 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．

要件 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．

要件 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．

2.2 爪表面を用いたマイクロ生体認証

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）」の提案が行われている．マイクロ爪認証は，下記のとおり，要件 1〜4 を満たす方式となっている．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が確認されている．

要件 1 に対する充足性：

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，拡大鏡等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，要件 1 が満たされる．文献 [1] では実証実験を通じて，200 倍での撮影によって爪表面の偽造困難性が高まることが確かめられた．

[*1] 文献 [1] では，Diversity の部分要件として Disposability を説明しているが，本論文では両者を別要件として記載する．

要件 2 に対する充足性：

文献 [1] では，200 倍のマイクロスコープによって撮影した約 1 mm 四方の爪表面画像を用いて実証実験を行い，同一被験者の同じ爪であっても撮影部位が異なれば，他人として識別される（マッチングスコアの分布が他人と同程度となる）ことが確かめられている．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等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 に対する充足性：

前述のとおり，約 1 mm 四方の爪表面画像を用いての生体認証の実現可能性が文献 [1] で確かめられており，1 つの爪（表面積を 1 cm^2 と想定）の中に 100 部位の登録可能領域（1 mm 四方の微細領域）が存在する計算となる．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 に対する充足性：

紙やすり等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が可能である．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]．

2.3 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，名寄せ耐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] 爪表面を擦ることによって表面形状が変化することについては自明な物理現象であり，また，爪の生え変わりについては自明な生理現象であるため，文献 [1] においても特にこれらを確認するための実証実験は行われていない．

2.3.1 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うえ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．

2.3.2 課題 2：利便性

生体認証の大きなメリットの 1 つが「手ぶら認証（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，個々の認証システムを通じて観測される生体情報のエントロピ）の低さが 1:N 認証の障壁となる．すなわち，ある程度の数以上のユーザを 1 つの認証システムに収容する場合には，1 種類の生体情報で全ユーザを識別することは困難であり，1:N 認証の実現は困難となる．

このため先行方式 [1] では，ユーザ ID を用いた 1:1 認証の形態でマイクロ爪認証を実装し，評価を行っている．なお，1:1 認証の場合も，人間が無理なく記憶できる情報（典型的には，ユーザの氏名等）をユーザ ID として用いてやれば，持ち物なしでの認証を実現できる．しかし，認証システムにユーザ 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ため，真の意味での手ぶら認証ではない．

1:N 認証を実現するもう 1 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，虹彩を併用して 1:N 認証を実現している [5]．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 [6]．

2.3.3 課題 3：名寄せ耐性

マイクロ爪認証では，複数のサービスに対して同一生体部位（爪）内の異なる微細部位を登録することにより，生体情報の名寄せに対する耐性を高めている．しかし，ある時点における「ユーザの爪表面の全体画像」を攻撃者に盗取されてしまった場合には，全体画像の情報を媒介として，異なるサービスに登録されている同一ユーザの生体情報が名寄せされてしまう．すなわち，爪の生え変わり，あるいは，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されるまでの間は，複数サービス間で生体情報が照合されるリスクが残る．

この問題を軽減するためには，物理的な生体情報の保護を目的とするマイクロ爪認証においても，電子的なテンプレートを保護するためのテンプレート保護技術 [7] を適用することは有効である．しかし，マイクロ爪認証を手ぶら

認証（1:N 認証）の形態で運用する場合には，テンプレート保護技術をそのまま採用することは難しい．テンプレート保護技術では十分なエントロピを有する乱数を使って生体情報を攪拌する．しかし，人間は大きな乱数を記憶することはできないため，ユーザには何らかの記憶媒体の所持が求められることになるためである．

3. 関連研究

生涯不変の生体情報は「物理的な生体情報」の消去権とは相容れない関係にある．このため，忘れられる生体認証を実現するにあたっては，新陳代謝によって日々生え変わる生体部位を利用するというアプローチが基本となり，著者らが調査した限りでは，2 章で説明したマイクロ爪認証が唯一の先行事例であった．そこで本章では，本論文で扱う 3 つの課題（安定性，利便性，名寄せ耐性）の改善に貢献する技術として，血流を利用したプレゼンテーション攻撃検知，テンプレート保護型生体認証，生体貼付型認証情報に関する既存研究をそれぞれ紹介する．

3.1 血流を利用したプレゼンテーション攻撃検知

血流を利用したプレゼンテーション攻撃検知技術が存在する．まず，静脈認証は「近赤外線が生体組織に対して透過性を有する反面，静脈内の還元ヘモグロビンに吸収される」という性質を利用して静脈形状を測定するものであるため，そもそもが「血液の存在」というプレゼンテーション攻撃検知を包含した生体認証となっているととらえることができる [8]．また，血液の酸素飽和度を計測し，その時間変化から脈波の存在を検出する（より正確には，血中酸素飽和度の時間変化を波形としてとらえ，その波形が脈波らしい形状となっているかを検査する）というプレゼンテーション攻撃検知手法が提案されている [9]．

3.2 テンプレート保護型生体認証

マイクロ爪認証が「ユーザが認証システムに提示した生体情報そのもの（物理的な生体情報）」に関する消去権の達成を目的としているのに対し，テンプレート保護技術が実現するのはあくまでも「認証システムによって読み取られコード化された生体情報（電子的なテンプレート）」に関する消去権のみである．

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 [7]．キャンセラブル生体認証では，乱数情報を用いて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，人間は大きな乱数を記憶することはできないため，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 カードの所持をユーザに強制することとなる．このため，手ぶら認証への適用は基本的に不可能である．

3.3 生体貼付型認証情報

文献 [10] では，QR コード化した付加情報をユーザのスマートフォンに表示し，生体情報（顔）と QR コードの両者を使用した二要素認証を構成することにより，生体認証を強化する方法が提案されている．また文献 [11] では，RFID（Radio Frequency IDentification）タグを皮膚に貼付する電子タトゥーが提案されている．これらの事実から，認証用の付加情報（QR コード）を RFID（電子タトゥー）に格納し，これを身体に直接貼付することで生体認証を強化するという拡張が，すでに現在の技術レベルで実現可能であることが分かる[*3]．

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プレゼンテーション攻撃検知と 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 反応性充血によるプレゼンテーション攻撃検知

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，マイクロ爪認証における微細生体部位（爪）の撮影倍率を中倍率（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 が低下してしまう．

生体情報の撮影倍率が低下する分，攻撃者が偽造生体を細部まで精密に偽造する必要が緩和され，なりすましが容易となる．この Unforgeability 低下に対処するために，爪床部の血流途絶と反応性充血を用いたプレゼンテーション攻撃検知を導入する．人間の指先には多数の毛細血管が存在する．血流途絶とはそれらの血流を圧力等で一時的に途絶させることである．反応性充血とは，血流途絶後に圧迫を解いた際に，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 [13]．

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（5.1 節で詳述する）．その際に，ユーザに指を指型に軽く押し付けてもらうことによって，爪床

[*3] RFID に（認証用の付加情報ではなく）認証情報自体を格納してやれば，電子タトゥーをユーザ認証に用いることができる．また文献 [12] では，皮膚貼付型エレクトロニクスが提案されている．今後，身体に認証情報（電子タトゥー）や認証機器（皮膚貼付型エレクトロニクス）自体を貼付することで，ユーザ認証が行われる時代が到来することも想像に難くない．ただし，生体貼付型認証情報（電子タトゥーや皮膚貼付型エレクトロニクス）自体によるユーザ認証は「所持認証」であり，認証情報の盗難やスキャベンジング等によるなりすましのリスクが残る．この観点からふまえると，本論文の目的である「生体貼付型認証情報の併用による生体認証の強化」は，生体貼付型認証情報を生体認証によってアクティベートするという形での所持認証の強化ととらえることもできる．

図 1 爪表面画像（圧迫中）
Fig. 1 Image of nail surface (under pressure).

図 2 爪表面画像（圧迫解放後）
Fig. 2 Nail surface image (after pressure release).

部直下の毛細血管が圧迫され（血流途絶），爪表面が青白く変色したように見える．その後，指の押し付けを解いてもらうことによって，毛細血管が圧迫から解放され（反応性充血），爪表面が再び赤みを帯びる．提案方式では，この一連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．

生体情報の撮影倍率が 1/4 に（約 200 倍から約 50 倍に）低下することにより，1 つの爪表面の中から独立に選べる微細部位の数が $(1/4)^2$ に減少する[*4]．この Diversity 低下の問題を根本的に解決することは難しい．なぜなら，「ユーザの爪表面の全体画像を攻撃者に盗取されてしまった場合には，全体画像の情報を媒介として，異なるサービスに登録されている同一ユーザの生体情報が名寄せされてしまう」というリスクがマイクロ爪認証に残存している以上，独立に選べる微細部位の数がいくつであっても名寄せが実行されてしまう余地が残るからである．すなわち，低倍率での撮影によって生じる Diversity 低下の問題は，先行方式の課題 3（名寄せ耐性）に帰結する．課題 3 の改善については次節で詳説する．

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 と名寄せ耐性の課題 3 は，ユーザ ID と乱数を埋め込んだ QR コードを爪に印刷することによって，その改善を図る．1 回の撮像によって QR コードと爪表面の両方をスキャンし，爪を提示するだけで生体情報，ユーザ ID，乱数を同時に取得する．生体情報とユーザ ID を使用して 1:1 認証を実行することにより，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 を改善する．生体情報と乱数を使用してテンプレート保護型生体認証を実行することにより，爪が生え変わるまでの期間における「電子的なテンプレートに対する名寄せ耐性」の提供を達成し，先行方式の課題 3 を改善する[*5]．

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 [14] 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，生体認証に求められるリアルタイム性，ならびに，マイクロ爪認証に求められる耐久性（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．

遊園地等のサービスにおいては，身体の一部にペイントを施したり，タトゥーを貼付するアミューズメントが一般的になりつつある [15]．加えて，爪は，かねてよりファッションの対象であり，マニキュア，ネイルプリント，付け爪はすでに一般的なコスメティック用品となっている．よって，爪への QR コードの印刷はユーザの心理的負担も少ないことが期待される．ただし，審美的観点から，QR コード自体をそのまま爪に印刷することは許容されにくいであろう．現実的な利用に向けては，QR コードのデザインにアミューズメント要素 [16], [17] を持たせたり，電子透かし技術 [18] を使用してユーザ ID や乱数を任意の画像に埋め込む等，デザイン面の制約を解消する必要がある．

本研究の現段階においては，QR コードの印刷にはネイルプリンタを用いることとした．ネイルプリンタを用いて爪に描画する場合等は，トップコート（透明マニキュア）を塗って印刷面を保護する必要がある．このため，QR コードを印刷した領域（正確には，トップコートを塗った領域）においては，爪表面の凹凸形状は隠されてしまう．このため現時点においては，QR コードを印刷する領域と生体情報を抽出する領域の棲み分けを行い，爪表面の上半領域に QR コードを印刷し，爪表面の下半領域から認証情報（爪表面の凹凸形状）を取得する方法を採用する．QR コード領域の爪表面が隠される分，生体情報部分の情報量（エントロピ）が減少することになるが，QR コードによって乱

[*4] 2.1 節で「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」という例をあげたが，200 倍の拡大鏡に対して 50 倍の拡大鏡の解像度が 1/4 に低下することにより，その分解能は「1 mm 四方の微細部位を識別するレベル」から「4 mm 四方の微細部位を識別する」レベルに低下する．この結果，1 cm^2 の爪表面の中から独立に選べる微細部位は 100 個から約 6（$\fallingdotseq 100 \times (1/4)^2$）個に減少する．

[*5] ただし，先行研究のマイクロ爪認証（テンプレート保護技術が導入されていないマイクロ爪認証）が採用されたままのサービスが残っている場合，そのサービスが名寄せの対象として残存することになる．このため，今回の議論の大前提として，世の中のマイクロ爪認証サービスすべてが統一的にテンプレート保護機能を備えるという状況が必要となる．

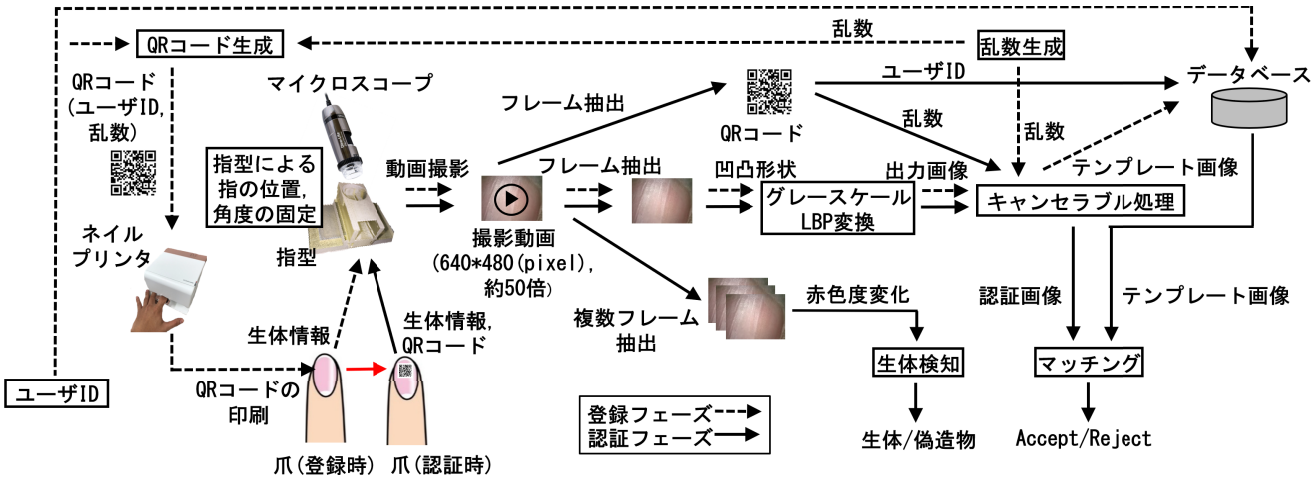


図 3 システム概観図
Fig. 3 System overview.

数が付加される結果，情報量の総量は増加する[*6]．

4.3 認証手順

マイクロ爪認証の手順を以下に示す（図 3）．

登録フェーズ：

(1) ユーザはシステムにユーザ ID と爪を提示する．
(2) システムは生体情報（爪表面の下半領域の凹凸形状）を読み取る．
(3) システムは乱数を生成し，その乱数で生体情報を攪拌する．
(4) 乱数によって攪拌されたテンプレート画像 T をユーザ ID とともにデータベースへ保存する．
(5) システムはユーザ ID と乱数を格納した QR コードを発行し，ユーザの爪表面の上半領域に印刷する．

認証フェーズ：

(1) ユーザはシステムに爪を提示する．
(2) システムは QR コード（爪表面の上半領域に印刷されている），生体情報（爪表面の下半領域の凹凸形状），プレゼンテーション攻撃検知情報（爪表面の下半領域の色変化）を読み取る．
(3) システムは読み取った QR コードからユーザ ID と乱数を抽出する．
(4) システムはプレゼンテーション攻撃検知情報を用いて提示された生体情報が生体であるか判定する．
(5) システムは読み取ったユーザ ID に対応するテンプレート画像 T をデータベースから取得する．
(6) システムは読み取った乱数によって生体情報を攪拌し，認証画像 A を得る．
(7) システムはテンプレート画像 T と認証画像 A が十分に近いか判定する．

4.4 提案方式の貢献

先行方式に対する提案方式のメリットは，撮影倍率が 200 倍から 50 倍に下がることによって，毎回の爪表面の撮影負荷が大幅に改善される点にある．一方で，先行方式に対する提案方式のデメリットとして，認証用付加情報を貼付するために爪表面に QR コードを印刷する負荷と，プレゼンテーション攻撃検知のために爪を指型に軽く押し付ける負荷が新たに発生する．すなわち提案方式は，認証時の撮影負荷を，登録時の QR コード印刷負荷と認証時の爪圧迫負荷に転嫁させた方式であるととらえることができる．200 倍での撮影は品質の良い画像を得ることが極端に難しく，先行方式は認証自体が不能になるリスクを孕んでいた．これに対し，QR コードの印刷と爪の圧迫操作は許容できる範囲の負担であり，提案方式はマイクロ爪認証の可用性向上に貢献している．

提案方式の新規性は，忘れられる権利への配慮，手ぶらでの認証（1:N 認証），テンプレート保護のすべてを具備する高機能な生体認証を，「爪を指型に（軽く押し付けるように）挿入する」というワンアクションで実現する方法を提案したことにある．先行研究 [1] において，マイクロ爪認証の典型的な適用先として，ロッカーの施解錠やアミューズメントパークの入退場管理等のカジュアルなサービス（匿名あるいは仮名で利用することが可能な短期的なサービス）があげられているが，認証の「手ぶら」化はこれらの利用シーンにマイクロ爪認証をさらに合致させるにあたっての重要な観点の 1 つである．カジュアルサービスに適する生体認証方式（マイクロ爪認証）の実現可能性を一歩前進させたことが，本論文の貢献である．

[*6] 今後，耐久性の高いネイル用特殊塗料が開発された暁には，トップコートの塗布も不要になるであろう．インクジェット型のネイルプリンタにおいては，塗料は微粒子状に噴霧されるので，理屈の上では，爪表面に塗料が薄く均一に塗布される形になり，QR コードを印刷した後も爪表面の凹凸形状は維持される．その場合は，QR コード印刷面から爪表面の凹凸形状と QR コードの両者を取得できるため，生体情報（爪表面）の情報量を減じることなく QR コードの情報量を重畳できる可能性がある．

5. 実装

概念実証（Proof of Concept，以下 PoC）を目的としたマイクロ爪認証システムを実装した．本章ではその詳細について説明を行う．

5.1 撮影機器

爪表面は半鏡面になっているため，撮像の際には鏡面反射ノイズ対策が必要であり，鏡面反射ノイズの低減には，撮影時のカメラ，光源，被写体の固定が重要である．そこで，撮影用マイクロスコープとして AM7915MZT Dino-Lite Edge S（Dino Lite 株式会社製）を採用した．本製品の接眼レンズには周囲に 8 つの LED（発光ダイオード）が敷設されており，カメラと光源の相対位置が固定されている（**図 4**）．そして，撮影時にユーザの指を収容するための「指型（**図 5**）」を作成し，この指型を専用のマイクロスコープスタンド DINOMS34B（Dino Lite 株式会社製）と連結固定させる（**図 6**）ことによって，カメラと被写体の相対位置を固定した．

指型は，ユーザの指のサイズに応じたアタッチメントを装着することが可能になっており（**図 7**，**図 8**），指を挿入した際に任意のユーザの爪が適切な位置，角度に固定されるようになっている（**図 9**）．これらにより，撮影時のマイクロスコープ，LED，爪の 3 者の相対位置が一意に定まるようになっている．撮影機器に関する詳細は文献 [19] を参照されたい．なお今回は，実験材料の事前準備の都合上，半透明の 3D プリンタ用樹脂を用いて指型の作製を行ったが，実際の指型は透明樹脂 [28] を用いて作成する予定である．透明の指型とすることで，指型の内部構造が視認できるようになり，利用者が指を挿入するにあたっての抵抗感が低減される．

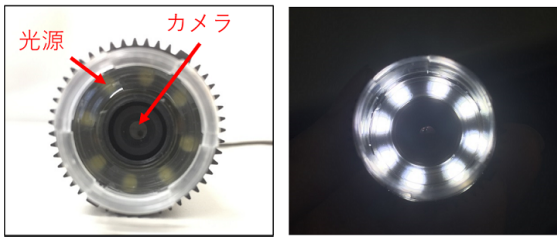


図 4 カメラと光源（右図は光源点灯時）
Fig. 4 Camera and light source (Right figure: lights are on).

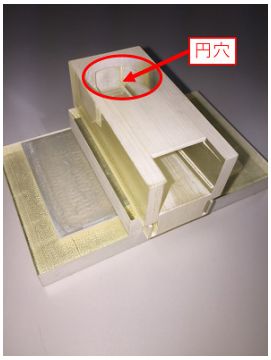


図 5 指型
Fig. 5 Finger mold.

5.2 認証情報の読み取り

指型の円穴（図 5）にマイクロスコープの接眼レンズが収納される構造になっている．ユーザが指を指型に挿入する動作のなかで，接眼レンズの前を爪表面の上半領域が通過する時点で QR コードが撮影され（**図 10**），その後，接眼レンズの前に爪表面の下半領域が到達した時点で認証情報が撮影される（**図 11**）．図 11 の時点で指先が壁に突き当たって指が止まるように指型が作られており（**図 12**），

図 6 マイクロスコープスタンドと指型の連結固定
Fig. 6 Connecting/fixing of microscope stand and finger mold.

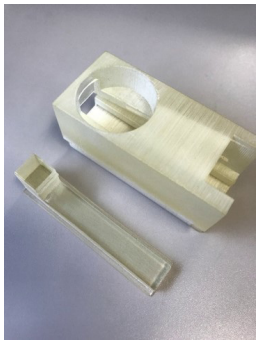


図 7 アタッチメント
Fig. 7 Finger mold and attachment.

図 8 指型へのアタッチメントの装着
Fig. 8 Finger mold with attachment.

図 9 指型とアタッチメントによる固定
Fig. 9 Fixation with finger mold and attachment.

図 10 爪上半領域の撮影
Fig. 10 Image of the upper half of nail surface.

図 11 爪下半領域の撮影
Fig. 11 Image of the lower half of nail surface.

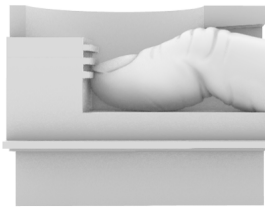


図 12 指型最深部での指の状態
Fig. 12 Finger at the deepest position in finger mold.

この時点でユーザがさらに指を軽く壁に一瞬押し付けると，爪表面に爪床部の血流途絶と反応性充血が表出し，その様子がマイクロスコープによって撮影される．

ユーザに求められるのは，単に「指を指型に挿入して，壁に指を一瞬強く押し付ける」という動作だけである．この動作を指型に設置されたマイクロスコープで動画撮影することにより，マイクロ爪認証のために必要となる QR コード（ユーザ ID および乱数），生体情報（爪表面の凹凸形状），プレゼンテーション攻撃検知情報（爪表面の色変化）を一度に取得することが可能となっている．

マイクロスコープの撮影倍率は 50 倍，フレームレートは 30 fps である．QR コードの読み込みには，公開ライブラリ pyzber0.1.8 [20] を利用した．著者らによる予備実験の結果から，本システムによって「ユーザが指を指型に挿入する」という動作を撮影した動画を当該ライブラリに与えることにより，リアルタイムで QR コードを読み取ることができることが確かめられている．生体情報（爪表面の凹凸形状）の読み込みについては，動画のなかから爪の下半領域が写っている 1 フレームを抽出する．50 倍での撮影により爪表面の約 8.0×6.0 mm の領域が 640×480 pixel の静止画像として取得される．登録時には，取得画像の中央 300×300 pixel をトリミングし，テンプレート画像として利用する．認証時には，取得画像の中央 420×340 pixel の中にテンプレート画像（に十分似ている画像）が含まれているかを検査する．テンプレート画像と認証画像のマッチングについては，5.4〜5.6 節にて詳述する．プレゼンテーション攻撃検知については 5.7 節にて詳述する．

5.3 QR コードの印刷

本システムでは，ユーザ ID は半角英数字 5 文字とした．個々の英数字を 8 bit で表記し，40 bit のデジタル情報としてユーザ ID をコーディングする．乱数は，0 から 24 までの整数を重複なくランダムな順序で列挙した整数列となる（5.5 節にて詳述する）．個々の整数を 5 bit の 2 進数で表記し，25 個の整数を 125 bit のデジタル情報としてコーディングする．ユーザ ID と乱数の両者が QR コードに格納される．QR コードの生成には，公開ライブラリ qrcode 6.1 [21] を利用した．本システムで採用した QR コードは，モデル 2，バージョン 3，誤り訂正レベル H，セルサイズ約 0.051 mm，印刷サイズ約 3.0×3.0 mm である．

QR コードの印刷にはジェルネイルプリンタ NP-N800/P（小泉成器株式会社製）を，ジェルの硬化にはネイルドライヤ LaCurie003（Amplite 株式会社製）を，それぞれ使用した．ジェルネイルの印刷手順は次のとおりである．まず，プライマ（爪表面とベースジェルの密着性を高め，ジェルネイルを長持ちさせる役割を持つ液剤）を爪表面上半領域に塗布し，乾燥させる．次に，市販の透明ベースジェルを塗布し，ネイルドライヤを用いて硬化させる．その上に，専用のプリコート（爪表面の下地を整える役割を持つ透明インク）を塗布する．十分に乾燥した後，ネイルプリンタにて QR コードを印刷する．さらに，市販の透明トップジェル（印刷された QR コードを保護する役割を持つ液剤）を塗布し，ネイルドライヤを用いて硬化させる．爪表面に印刷された QR コードを**図 13**，**図 14** に示す．QR コードの印刷にはこれらの液剤の塗布・乾燥に合計 5〜10 分程度を要し，これが提案方式の登録処理にかかる時間の大部分を占める．現実的な利用に向けては，所要時間の短縮が必要である．

図 13 QR コードが印刷された爪
Fig. 13 Nail with QR Code.

図 14 QR コードが印刷された爪（拡大図）
Fig. 14 Nail with QR Code (enlarged view).

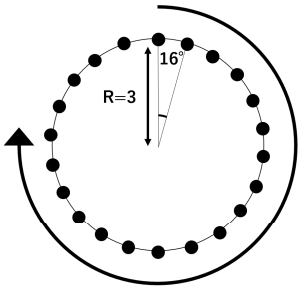


図 15 本実装における LBP 操作
Fig. 15 LBP operation in our implementation.

5.4 特徴抽出

本システムでは，爪表面（の下半領域）の凹凸形状を生体情報の特徴量として利用する．本システムでは，安定した特徴を得るために，テンプレート画像および認証画像に対してグレースケール変換と Local Binary Pattern（以下 LBP）変換を適用する．LBP は画像全体の濃淡値の変化に頑健であるという性質を持つ [22], [23]．各処理は，scikit-image Ver.0.14dev [24] に実装されている公開ライブラリ rgb2gray 関数，local binary pattern 関数を使用してそれぞれ実装した．local binary pattern 関数のパラメータは近傍画素数 P = 22，半径 R = 3，method = Default とした．P = 22，R = 3，method = Default の local binary pattern 関数の動作は次のとおりである．まず，注目画素から半径 R = 3 の位置にある P = 22 カ所の輝度値を双一次補間（バイリニア補間）によって $360°/22 \fallingdotseq 16°$ ごとに求める（**図 15**）．次に，22 カ所の輝度値を上から時計回りに 1 つずつ注目画素の輝度値と比較し，注目画素の輝度値のほうが大きい場合は 1 を，小さい場合は 0 を割り当てる．この結果，得られた 22 bit の 2 進数を 10 進数に変換し，0〜4,194,303 を 0〜255 に正規化することによって，注目画素の LBP 値を得る．以上の操作を各画素に適用することで LBP 画像が出力される．これらの処理を施す前後の画像例を**図 16** に示す．

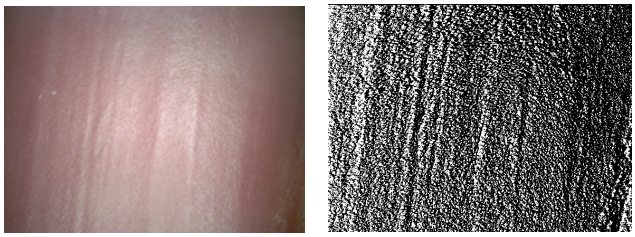


図 16 画像処理前（左図）と処理後（右図）の爪画像
Fig. 16 Nail surface before (left) and after (right) image processing.

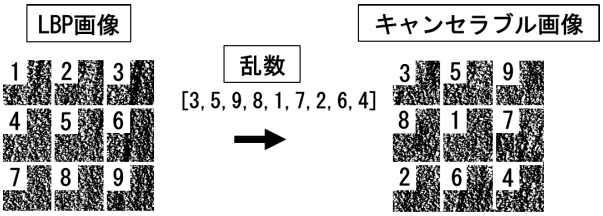


図 17 キャンセラブルアルゴリズム
Fig. 17 Cancelable algorithm.

5.5 テンプレート保護

本システムに導入するテンプレート保護技術としては，ブロックスクランブル方式のキャンセラブル処理 [25] を採用した．具体的なアルゴリズムは以下のとおりである（**図 17**）．

(1) 画像を 5 × 5 ブロックに等分割する．（ただし，図 17 は平明性のために 3 × 3 ブロックで作図している．）
(2) 乱数に従って分割したブロックの順序を変更する．
(3) 順序を変更したブロックを再結合する．

ブロックスクランブル方式自体は安全なテンプレート保護技術とはいえず，攻撃者はスライドパズル[*7]の要領で，ブロック間の境界の模様を手掛かりにしてブロックとブロックの逆置換を行うという攻撃が可能である．概念実証（PoC）が本論文の目的であることに鑑み，本システムではブロックスクランブル方式を採用したが，実際にはより安全なテンプレート保護技術を採用する必要がある．たとえば，Takahashi らによって提案された correlation-invariant random filtering（CIRF）法 [28] によるテンプレート保護の採用が考えられる．CIRF 法は，テンプレート画像と同サイズのランダム画像を用いて，テンプレート画像全体を画素単位でマスクすることによって，キャンセラブル処理

[*7] たとえば，Apple app store: Slide Puzzle Museum, https://apps.apple.com/us/app/slide-puzzle-museum/id1496727488

の完全な不可逆性（キャンセラブル処理を施したテンプレート画像から元のテンプレート画像の情報が漏洩しない）を担保している．

5.6 マッチング

本システムのマッチングには，テンプレートマッチングの1つである Zero-means Normalized Cross-Correlation（以下 ZNCC）を採用した．ZNCC は照明変動に対してロバスト性が高く，爪表面による鏡面反射によるノイズを抑制することが期待できる．今回は OpenCV [26] に実装されている公開ライブラリの cv2.matchTemplate 関数（パラメータは methods = cv2.TM_CCOEFF_NORMED）を参考に，本システムのマッチング関数を実装した．5.2 節で説明したとおり，認証画像の中央 420×340 pixel の中に 300×300 pixel のテンプレート画像が含まれているかの検査が行われる．本システムでは，指型（5.1 節）によって指の挿入方向が物理的に固定されるため，撮像される爪表面の画像においては回転方向の変異が生じることは少ない．このため今回は，テンプレート画像を x 軸方向，y 軸方向に 1 pixel ごと走査させながら，「認証画像中の 300×300 pixel の領域」とテンプレート画像（300×300 pixel）のマッチングスコアの計算を繰り返すという方法によって，認証画像中にテンプレート画像（に十分似ている画像）が含まれているかの検査を行うようにした．

5.7 プレゼンテーション攻撃検知

5.2 節で述べたとおり，本システムでは，「指先が指型の壁に突き当たった時点（図 12）で，ユーザがさらに指を軽く壁に一瞬押し付ける」という動作の際に，爪表面（爪床部）の下半領域に表出する赤色度の変化を確認することにより，プレゼンテーション攻撃検知を行う．今回は爪の赤色度の変化を以下の方法で検査する．

(1) 爪表面の下半領域が撮影された動画から，0.1 秒ごとにフレームを抽出する．
(2) 各フレームの静止画に対して手順 (3)〜(6) を繰り返す．
(3) 鏡面反射によって白飛びしている画素を除くために，画像内において R，G，B の輝度値すべてが 215 以上の画素を間引く．
(4) R，G，B の輝度値が 150 以上の画素数をそれぞれカウントし，その数を nR，nG，nB とする．
(5) nR/(nR + nG + nB) を求め，これを赤色度とする．
(6) 0.1 秒前のフレームと当該フレームの画像を比較し，指の移動距離（ユーザが指を壁に押し付ける際には指が壁方向にわずかに移動し，ユーザが指の押し付けをやめた際には指が壁の逆方向にわずかに移動する）を求める．
(7) 各フレームにおいて取得された爪表面の赤色度と指の移動距離を集約し，赤色度と移動距離の時間推移を得る．「指が壁方向に移動するとともに赤色度が減少し，指が壁の逆方向に移動するとともに赤色度が増加する」という関係がつねに成り立つ場合に（正確には，撮影ごとの揺らぎやノイズに鑑み，Th 以上の確度でこの関係が成り立つ場合に）生体と判定する．

6. 基礎実験 1：認証精度

6.1 概要

提案方式の評価にあたり，本学情報科学系の研究室に在籍する大学生 8 人（男性 5 名，女性 3 名）に協力してもらい基礎実験を行った．各被験者の非利き手の人差し指，中指，あるいは薬指の爪（各被験者が自身で選択）を登録生体部位とした[*8]．実験は 3 日間行った．1 日目に登録フェーズ（4.3 節）を実行し，各被験者の爪表面上半領域に QR コードを印刷した．そしてその直後に 1 回目の認証フェーズ（4.3 節）の実施を行った．2 日目，3 日目は任意の時間帯にそれぞれ 2 回目，3 日目の認証フェーズの実施を行った．なお，概念実証（PoC）が本論文の目的であることに鑑み，今回は爪（と QR コード）の撮影には実験実施者（筆者ら）が立ち合い，良好な形で画像が撮影されるようにガイディングを行っている．

6.2 QR コード読み取り精度

爪表面に印刷した QR コードが正しく保護され，翌日においても読み取りが可能か評価を行った．その結果，1 名を除いた被験者 7 名が 3 日目においても QR コードを正しく読み取ることができた．なお，7 名のなかに，3 日目において QR コードに一部破損（**図 18**）が見られる被験者が生じたが，QR コードは正しく読み取れた．

6.3 認証精度

爪表面（の下半領域）の凹凸形状を利用した撮影倍率 50 倍でのマイクロ爪認証の認証精度を，同じ被験者内のマッチングスコア（本人スコア）と異なる被験者間のマッチングスコア（他人間スコア）を比較することで評価する．ここでは，生体情報自体の認証精度を評価するために，QR

図 18 一部破損が確認できた QR コード
Fig. 18 QR code with partial damage.

[*8] 人間の身体的構造上，親指と小指については指型に挿入する動作が若干困難であることに配慮し，今回の実験の対象から除外した．

コードの読取精度は 100%であるという前提を置き，本人スコアおよび他人スコアはすべて正しい乱数情報を用いて算出した．すなわち，被験者 i（$1 \leq i \leq 8$）のテンプレート画像 T_i，被験者 j（$1 \leq j \leq 8$）の d 日目（$1 \leq d \leq 3$）の認証画像を $A_{j,d}$ とすると，本人間スコアは T_i と $A_{j,d}$（$i = j$）を比較することによって，他人間スコアは T_i と $A_{j,d}$（$i \neq j$）を比較することによって，それぞれ算出される．ただし，本論文では処理時間短縮のため，本人スコアと同数の組合せをランダムに抽出することによって，他人スコアを求めた．ランダム抽出においては，各被験者から同一数のデータが抽出されるように行っている．なお，実験期間中に QR コードが破損した被験者については，今回は，その時点で実験を中止することはせず，実験実施者が当該被験者のユーザ ID および乱数をシステムに別途入力することによってこれを補った．このようにして求めた 1 日目から 3 日目までの本人間スコアと他人間スコアを基に，本人と他人を切り分ける認証閾値を変更した際の本人拒否率（False Rejection Rate，以下 FRR）と他人受入率（False Acceptance Rate，以下 FAR）の変化を**図 19** に示す．このときの等価エラー率（Equal Error Rate，以下 EER）を求めたところ，認証閾値 $\fallingdotseq 0.04$ で EER $\fallingdotseq 3.9\%$ であった．この結果は，先行方式（200 倍での撮影）の認証精度と同程度である．

6.4 プレゼンテーション攻撃検知精度

5.7 節にて説明した方法によってプレゼンテーション攻撃検知を実施した結果，「指が壁方向に移動するとともに赤色度が減少し，指が壁の逆方向に移動するとともに赤色度が増加する」という関係（以下，移動と色の相関）が成立したのは約 72%であった．よって，ユーザが「指型の壁に指を押し付ける」という認証動作を行っている間の任意の 3 時刻において，移動と色の相関が成立することを確認する（検査を 3 回実施する）ようにした場合，非生体がこの検知をすり抜ける確率は約 2%（$= (1-0.72)^3$）である．このように，爪表面の赤色度変化の確認という簡易な検査によって，プレゼンテーション攻撃（なりすまし）に要する攻撃者の偽造コストを大幅に高め得ることが確認された．

今回の実験で撮影された動画を確認したところ，指を押し込む動作が速過ぎて被写体ブレが生じた場合等には，指の移動距離が正しく算出できないことが判明した．「移動と色の相関は成立しているにもかかわらず，被写体ブレ等によりそれが確認できなかった」という状況に対しては，撮影方法や画像処理の改善によってその発生頻度を低減させ得る．仮に，移動と色の相関の成立を 85%の確度で確認することができるようになれば，2 回の検査で同程度のプレゼンテーション攻撃検知精度（約 2%（$= (1-0.85)^2$）の非生体すり抜け率）が得られる．今後の検討課題として調査していきたい．

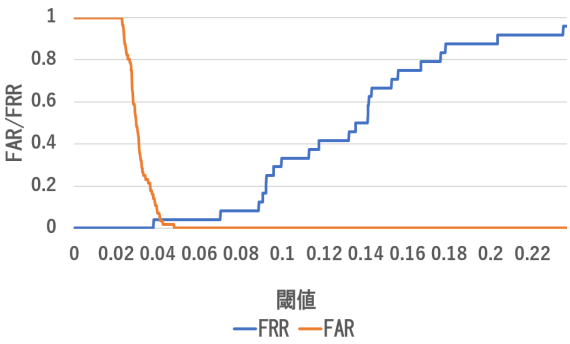


図 19 認証精度
Fig. 19 Authentication accuracy.

7. 基礎実験 2：偽造耐性

7.1 印刷物

提案方式では，爪表面を 50 倍のマイクロスコープで撮影し，その撮影画像を認証に利用する．**図 20** は「爪表面の 8.0 × 6.0 mm の領域を 50 倍のマイクロスコープで撮影した画像」であり，**図 21** は「市販のプリンタ HL3170-CDW（ブラザー工業株式会社製）を使用して，印刷サイズが 8.0 × 6.0 mm の大きさとなるように，図 20 の画像を最高解像度（2,400 dpi）で印刷し，それを 50 倍のマイクロスコープで撮影した画像」である．図 21 より印刷塗料のドットパターンを確認することができる．これより，マイクロ爪認証の撮影倍率を 200 倍から 50 倍に落とした場合も，市販のプリンタ程度の解像度であれば，撮影される画像が本物と比べて大きく異なることが確認できる．

7.2 ディスプレイ

図 22 は「Apple 社 iPhone 12 Pro のディスプレイ（6.1 インチ OLED ディスプレイ，2,532 × 1,170 pixel，460 dpi）

図 20 実物の爪表面画像
Fig. 20 Image of real nail surface.

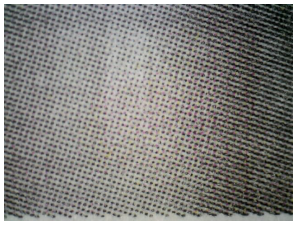


図 21 図 20 を印刷した画像
Fig. 21 Image of printed nail surface of Fig. 20.

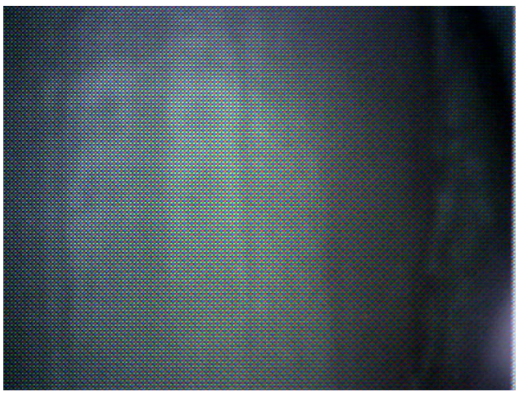


図 22 図 20 をディスプレイ表示した画像
Fig. 22 Image of displayed nail surface of Fig. 20.

図 23 偽造生体（熱可塑性樹脂）
Fig. 23 Counterfeit (thermoplastic resin).

を使用して，表示サイズが 8.0 × 6.0 mm の大きさとなるように，図 20 の画像をディスプレイに表示し，それを 50 倍のマイクロスコープで撮影した画像」である．図 22 よりディスプレイの発光素子を確認することができる．これより，ディスプレイに対しても，マイクロ爪認証の撮影倍率を 200 倍から 50 倍に落とした場合も，撮影される画像が本物と比べて大きく異なることが確認できる．

7.3 偽造物

図 23 は実験実施者（著者）の爪を型取り，キャスト材を使用して作成した偽造生体である．使用した材料は以下のとおりである．

- 型取り材：ブルーミックス II（アグサジャパン株式会社製）
- 離型剤：シリコーン離型剤 KF96SP（信越化学工業株式会社製）
- キャスト材：熱可塑性樹脂「イロプラホワイト」ACG-PC1-W（シード株式会社製）

爪型，人工爪の作製は文献 [27] を参考に以下の手順で行った[*9]．

- 爪型の作製：
  1. 爪型作成用の型取り材（A 材，B 材）をよくかき混ぜ，できる限り気泡を取り除く．
  2. 手順 1 で作成した混合材に指（爪）を押し付け，混合剤が硬化するまで（約 30 分）これを維持する．
  3. 型取り材が完全に硬化したら指を型から取り外す．
- 人工爪の作製：
  1. 上記で作製した型に離型剤を噴霧する．
  2. 偽造爪作成用のキャスト材を熱湯（約 80°C）にて 3 分ほど温め，軟化させる．
  3. キャスト材を取り出し，水気を取り除いた後，空気が入らないように型に押し付け，十分に冷めるまで（約 15 分）放置する．

[*9] 偽造物の作成にあたっては，爪表面の凹凸をできるだけ精巧に模造する必要がある．著者らが行った幾種類の事前実験のうち，爪表面の凹凸を最も精巧に複製できた方法が文献 [27] の方法であった．

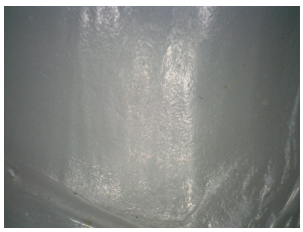


図 24 50 倍で撮影した偽造生体
Fig. 24 Image of counterfeit taken at 50x magnification.

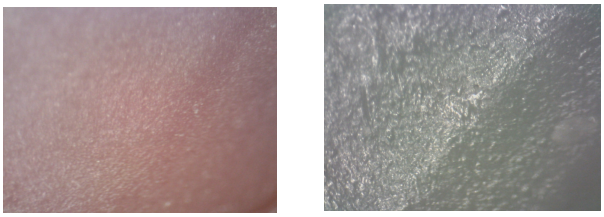


図 25 200 倍の撮影画像（生体が左図，偽造物が右図）
Fig. 25 Images of living body (left) and counterfeit (right) taken at 200x magnification.

図 24 は「図 23 の偽造生体を 50 倍のマイクロスコープで撮影した画像」である．偽造生体も微細な凹凸形状を模れていることが確認できる．5 章で実装したシステム（6.3 節の実験結果に基づき，FAR = FRR となる認証閾値を設定）に図 23 の偽造生体を提示したところ，テンプレート（実験実施者の爪表面同一部位の 50 倍での凹凸形状）とのマッチングスコアは認証閾値を超える結果となった．一方，**図 25** は「図 23 の偽造生体を 200 倍のマイクロスコープで撮影した画像（および，実験実施者の爪表面同一部位を 200 倍で撮影した画像）」である．先行方式のシステム（文献 [1] で実施された実験結果に基づき，FAR = FRR となる認証閾値を設定）に図 23 の偽造生体を提示したところ，テンプレート（実験実施者の爪表面同一部位の 200 倍での凹凸形状）とのマッチングスコアが認証閾値を超えることはなかった．これは，先行方式の安定性を高めるために撮影倍率を 50 倍に落とした結果，先行方式（200 倍での撮影）にて実現されていた偽造耐性が確保できなくなってしまったことを意味している．

当然のことながら，図 23 の偽造生体においては，血流

途絶および反応性充血が現れることはない．このため，提案方式においても（新たに組み込まれたプレゼンテーション攻撃検知機能によって）図 23 の偽造生体を退けることが可能となっている．すなわち，提案方式はプレゼンテーション攻撃検知を導入することで，マイクロ爪認証の安定性を改善（50 倍での撮影）しつつ，先行方式（200 倍での撮影）と同程度の偽造耐性の実現を達成しているといえよう．

8. むすび

本論文では，文献 [1] のマイクロ爪認証（先行方式）における課題を解決するために，反応性充血を用いたプレゼンテーション攻撃検知と QR コードを用いた付加情報添付を併用したマイクロ爪認証の改良を提案した．概念実証（PoC）レベルの基礎実験であったものの，認証精度と偽造耐性の観点からの評価を通じ，先行方式の「忘れられる権利を満たす生体認証に求められる要件」を達成しつつ，先行方式の課題点が改善されることが確認できた．

撮影倍率を 50 倍に落とすことによって，爪表面の撮像が容易となり，認証時の撮影負荷軽減が実現された．テンプレート保護型マイクロ爪認証の「手ぶら」化によって，マイクロ爪認証のカジュアルサービス（匿名あるいは仮名で利用することが可能な短期的なサービス）への親和性向上も達成された．ただし提案方式は，QR コード印刷の負担を新たにユーザに課す方式となっており，5.3 節で述べたように，QR コードの印刷の煩わしさ（液剤を何層も塗り重ねる）と所用時間の課題が残っている．文献 [1] にてマイクロ爪認証の適用先として示されているロッカーの施解錠やアミューズメントパークの入退場管理を想定した場合，登録時の簡便さも重要な要素である．この点については，4.2 節で述べた QR コードの審美面の問題と合わせて，今後の課題として取り扱っていく[*10]．

また，今後，(i) 提案方式の認証精度，安全性，認証速度の向上，(ii) 時間経過による認証精度の変化，(iii) 非接触でのマイクロ爪認証の実現，等についての検討も深めていく予定である．(i) については，爪表面画像の撮像の高速化，マッチング処理，プレゼンテーション攻撃検知処理，キャンセラブル処理の各アルゴリズムの改良が含まれる．(ii) については，4 日以上の日常生活のなかで爪（や QR コード）の状態がどのように変化するのかを確認する必要がある．また，爪には本人の健康状態が現れることが知られているため，その観点からの爪表面の状態変化（健康状態の認証精度への影響）も観察する．(iii) については，コロナ禍でその要求がますます高まっている．

[*10] QR コードの印刷の煩わしさと所用時間の問題に関しては，著者らはすでに QR コードを印刷したラベルシールを爪表面に貼付する方法についても基礎実験を行っている．具体的には，QR コードを市販のラベルシールに印刷し，ラベルシールを爪表面に貼付した上に市販の瞬間接着剤を塗布した．経過観察を行った結果，QR コードは約 1 週間，読み取り可能な状態を保つことが確かめられた（**図 26**）．この方法であれば，「爪にシールを貼って保護液剤（瞬間接着剤）を塗布する」という簡便な手段（所要時間は約 1 分）によって，爪に QR コードを貼付できる．なお，爪表面に付着した瞬間接着剤は市販の除光液等で容易に除去可能である．

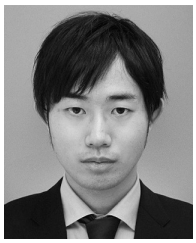
図 26 貼付型 QR コード
Fig. 26 QR ode sticker.

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いただきました．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

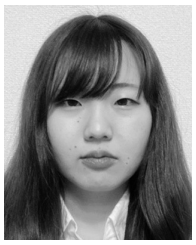
[1] 杉本元輝，藤田真浩，眞野勇人，大木哲史，西垣正勝：忘れられる権利に配慮した生体認証：爪を用いたマイクロ生体認証，情報処理学会論文誌，Vol.60, No.12, pp.2095–2105 (2019).
[2] ISO/IEC DIS 30136: Information technology — Performancetesting of biometric template protection schemes (2017).
[3] Jain, A.K., Nandakuma, K. and Nagar, A.: Biometric Template Security, *EURASIP Journal on Advances in Signal Processing*, Vol.2008, Article ID 579416, p.17 (2017).
[4] 新崎 卓：生体認証と改正個人情報保護法をめぐる動き，電子情報通信学会基礎・境界ソサイエティ Fundamentals Review，Vol.11, No.2, pp.108–112 (2017).
[5] Unique Identification Authority of India, available from ⟨https://uidai.gov.in⟩ (accessed 2021-03-06).
[6] 高橋健太：逐次融合判定に基づくマルチモーダルバイオメトリック暗号，信学技報，Vol.114, No.251, pp.1–6 (2014).
[7] Rathgeb, C. and Uhl, A.: A survey on biometric cryptosystems and cancelable biometrics, *Journal on Information Security*, pp.1–25 (2011).
[8] 森原 隆：安全性と利便性を両立する静脈認証技術，情報処理，Vol.51, No.12 (2010).
[9] 宇根正志，田村裕子：生体検知技術，情報処理，Vol.47, No.6 (2006).
[10] QR コード認証を追加した「SmartOn ID」最新版を提供開始，入手先 ⟨https://www.soliton.co.jp/news/2019/003878.html⟩（参照 2020-03-06）．
[11] Woollaston, V.: 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-reveals-plans-ink-pills-replace-ALL-passwords.html⟩ (accessed 2021-03-06).
[12] 工藤史堯，長谷川慶太，竹内 格，中村 亨，大田幸由：ウェアラブルデバイスを用いた継続認証システムの検討，

信学技報，Vol.116, No.488, pp.79–83 (2017).
[13] 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).
[14] 野村政弘, 澤田善次郎, 星野 裕, 増澤洋一, 藤本義治：QRコード（2次元バーコード）の開発と生産管理，日本生産管理学会論文誌，Vol.8, No.2 (2002).
[15] Pinteres, available from ⟨https://www.pinterest.jp/pin/361273201331291466⟩ (accessed 2021-02-16).
[16] Visualead, available from ⟨https://www.visualead.com/⟩ (accessed 2021-02-16).
[17] DENSO WAVE FrameQR®, available from ⟨https://www.denso-wave.com/en/system/qr/product/frame.html⟩ (accessed 2021-03-06).
[18] 渡辺 創：13章 情報ハイディング，電子情報通信学会知識ベース，1群，3編，13章 (2010).
[19] 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).
[20] pyzbar 0.1.8, available from ⟨https://pypi.org/project/pyzbar/⟩ (accessed 2021-03-06).
[21] qrcode 6.1, available from ⟨https://pypi.org/project/qrcode/⟩ (accessed 2021-03-06).
[22] Ojala, T., Pietikainen, M. and Harwood, D.: Performance valuation of texture measures with classification based on Kullback discrimination of distributions, *Proc. 12th International Conference on Pattern Recognition*, Vol.1, pp.582–585 (1994).
[23] 長谷川修：Local Binary Pattern とその周辺，情報処理学会研究報告グラフィクスと CAD，Vol.202-CG-149, No.3, pp.1–6 (2012).
[24] scikit-image, available from ⟨https://scikit-image.org/⟩ (accessed 2020-11-27).
[25] Ratha, N.K., Connell, J.H. and Bolle, R.M.: Enhancing security and privacy in biometrics-based authentication systems, *IBM SYSTEMS JOURNAL*, Vol.40, No.3 (2001).
[26] OpenCV, available from ⟨https://opencv.org/⟩ (accessed 2020-11-27).
[27] 山田浩二，松本弘之，松本 勉：指紋照合指は人工指を受け入れるか，情報処理学会研究報告コンピュータセキュリティ，Vol.2000, No.68, pp.159–166 (2000).
[28] 3Day プリンター 透明樹脂，入手先 ⟨https://3day-printer.com/material/transparent⟩（参照 2021-06-10）.
[29] Takahashi, K. and Hirata, S.: Cancelable biometrics with provable security and its application to fingerprint verification, *IEICE Trans. Fundamentals*, Vol.E94-A, No.1, pp.233–244 (2011).
[30] Ojala, T., Pietikainen, M. and Maenpaa, T.: Multiresolution Gray-Scale and Rotation Invariant Texture Classification with Local Binary Patterns, *IEEE Trans. Pattern Analysis and Machine Intelligence*, Vol.24, pp.971–987 (2002).



塩見 祐哉

2019 年静岡大学情報学部情報科学科卒業．2021 年同大学院情報科学技術研究科情報学専攻修士課程修了．在学中は情報セキュリティ，特に生体認証に関する研究に従事．



大内 結雲

2020 年静岡大学情報学部情報科学科卒業．2021 年同大学院情報科学技術研究科情報学専攻修士課程在学中．現在は情報セキュリティ，特に情報漏洩対策に関する研究に従事．

藤田 真浩 （正会員）

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．2018 年同創造科学技術大学院博士課程修了．現在，三菱電機株式会社情報技術総合研究所勤務．情報セキュリティ，特に認証システムに関する研究開発に従事．博士（情報学）．2016 年度情報処理学会山下記念研究賞受賞．

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．在学中は情報セキュリティに関する研究に従事．

大木 哲史 （正会員）

2002 年早稲田大学理工学部電子情報通信学科卒業．2004 年同大学院理工学研究科電子・情報通信学専攻修士課程修了．2010 年早稲田大学理工学術院情報・ネットワーク専攻博士（工学）取得．2010 年早稲田大学理工学総合研究所次席研究員．2013 年産業技術総合研究所特別研究員を経て，2017 年より静岡大学大学院総合科学技術研究科講師．情報セキュリティ全般，特に個人認証を中心としたネットワークセキュリティに関する研究に従事．電子情報通信学会会員．

西垣 正勝 （正会員）

1990 年静岡大学工学部光電機械工学科卒業．1995 年同大学大学院博士課程修了．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，2010 年より同創造科学技術大学院教授．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，2019～2020 年情報環境領域委員長，2020 年調査研究運営委員長．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．2016～2020 年日本セキュリティマネジメント学会編集部会長，2021 年より副会長．本会フェロー．