Vol.2019-SPT-32 No.13
2019/3/7

忘れられる権利を満たす生体認証：爪を用いたマイクロ生体認証

杉本　元輝[†]　藤田　真浩[†]　眞野　勇人[†]　大木　哲史[†]　西垣　正勝[†]

概要：近年，プライバシ保護の観点から「忘れられる権利」の必要性が度々議論されている．本権利は EU の一般データ保護規則に「消去権」として記載されたことで世界的に注目を集めており，生体認証の分野においてもこの「忘れられる権利」を有することが求められる．その一実現形態としてテンプレートに乱数を付与するキャンセラブル生体認証が存在する．この技術により，登録された電子的な生体情報を保護することは可能だが，登録する前の物理的な生体情報の漏洩まで保護することは不可能である．本稿では，人間の微細生体部位を用いたマイクロ生体認証システムを爪に応用することで，物理的な生体情報に対して「忘れられる権利」を満たす生体認証を提案する．

キーワード：生体認証，微細生体部位，爪，忘れられる権利，プライバシ保護

Biometrics with the Right to be Forgotten: Micro Biometric Authentication Using Fingernail Surface

GENKI SUGIMOTO[†] MASAHIRO FUJITA[†] YUTO MANO[†]
TETSUSHI OHKI[†] MASAKATSU NISHIGAKI[†]

Abstract: In recent years, the necessity of "right to be forgotten" is frequently discussed from the viewpoint of privacy protection. Furthermore, since this right was described as "right to erasure" in the general data protection rule of the EU, it attracted worldwide attention and it is required to have this "right to be forgotten" even in the field of biometric authentication. As one of such implementations, there is a cancelable biometric authentication which gives a random number to a template. Although it is possible to protect registered biometric information by this technique, it is impossible to protect up to the leak of physical biometric information before registration. In this paper, we applied a micro biometric authentication system, which uses a human micro body part, to the nail to construct a biometric authentication system that satisfies the "right to be forgotten" against physical biometric information.

Keywords: Biometric authentication, Minute biometric part, Nail, A right to be forgotten, Privacy preservation

1. はじめに

近年，インターネットの普及に伴い，様々な情報を手軽に利用できるようになった一方で，個人にとって好ましくない情報がインターネット上に残り続け，多くの人が検索エンジン等によって容易にアクセスや拡散が可能であるといった問題が存在する．そのため個人にとって好ましくない情報は，本人の意志で他人の目に触れないように削除され，忘れてもらうことの出来る権利を設けるべきであるということが主張されている．日本ではこれを「忘れられる権利」と呼び，その必要性について度々議論されている[1][2]．EU においてもこのような権利を認める議論が活発に行われ，2016 年 4 月に欧州議会が可決した EU 一般データ保護規則（General Data Protection Regulation：GDPR）の 17 条には「消去権（忘れられる権利）」（Right to erasure (‘right to be forgotten’))として明記されている[3]．これは個人データ主体が一定の条件を満たす場合に個人データの抹消を請求することの出来る権利を認めたものである．この「個人データ」とは，識別された人又は識別可能な人（「データ主体」）に関する情報を意味する．

また現在，忘却・紛失の恐れがないといった利点から生体認証がさまざまな場面で用いられている．近年では普及が進み，ATM や入出国審査のようなセンシティブなサービスだけではなく，スマートフォンのロック解除やアミューズメントパークの入退場管理[4]などのカジュアルなサービスにも利用されており，今後のさらなる普及が予想される．しかし一方で，生体情報が基本的に生涯不変で変更することのできないことから，一度生体情報が漏洩してしまうと，永遠に攻撃の危険に晒され続けるという課題も存在する．そのため生体認証システムにも，個人データである生体情報を抹消できる権利，つまり「忘れられる権利」を満たすことが求められる．その一実現形態としてキャンセラブル生体認証（テンプレート保護技術）が存在する[5]．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，その情報をテンプレートとしてサーバに登録する．この乱数情報を変更することにより，テンプレートの更新が可能となる．このテンプレート更新により以前のテンプレートが消去される，つまりこれは，忘れられる権

[†] 静岡大学
Shizuoka University

利を有しているテンプレートであると言える．

しかしキャンセラブル生体認証が忘れられる権利を満たしているのはあくまでもデータベースに保存された電子的な生体情報（テンプレート）に関してのみであり，虹彩や指紋そのものといった物理的な生体情報まで保護することは出来ない．近年，カメラの高性能化により，遠距離から虹彩や指紋などの高繊細な画像を盗撮することも困難ではなくなっており，実際にピース写真から指紋を復元し偽造に成功したという事例も報告されている[6]．そのため，物理的な生体情報に対しても忘れられる権利を満たす生体認証が必要である．

物理的に忘れられる権利を満たす生体認証の要件は，電子的に忘れられる権利を満たすテンプレート保護の要件として一般的に用いられている以下の 4 つの要件をベースに議論する[7][8][9].

① Irreversibility : 生体情報から生成された登録照合用の識別データ（生体特徴データ）から，もとの生体情報の類推ができないこと．
② Un-linkability : ユーザのプライバシ保護のため，システムで用いられている識別データを利用して，意図しない他の生体認証システムとの照合ができないこと．
③ Diversity：同じ生体情報から異なる識別データを生成可能であること．漏洩した識別データを利用不可にして，新しい識別データを生成して安心安全に生体認証システムで利用できる．
④ 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．

しかし要件①は，電子的な生体情報に対する要件であるため，物理的な生体情報を対象とする本稿では不適切である．そのため以下のように要件①を再定義する．

① Unforgeability : 生体情報が漏洩しない，もしくは漏洩したとしてもその情報を用いて本人になりすまして認証を突破することが困難である．

本稿では，上記の要件を全て満たす生体認証として爪表面の微細部位を用いた認証方式を提案する．以降，2 章で既存・関連研究を紹介し，3 章で微細部位を用いた生体認証と提案方式について説明する．次に 4 章で今回実装したシステムを紹介し，その後 7 章で考察を述べ，8 章で本稿をまとめる．

2. 関連技術・関連研究

著者らが調査した限りでは，爪表面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，関連研究として爪を利用した生体認証を紹介する．

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，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[11][12]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．

2.3 Garg らの提案

Garg らは爪表面全体に確認される縦の筋溝（longitudinal striations）を特徴として利用した認証を提案し，その有用性を示している[13]. しかし，縦の筋溝は指紋同様不変の特徴量であると示されており，模造物によるなりすましに対する耐性が低いと考えられるため要件①を満たさない．

3. 忘れられる権利を満たす生体認証

3.1 マイクロ生体認証

1 章で述べたとおり，要件①～④を満たし，忘れられる権利を有する生体認証が求められる．著者らは要件①～④を部分的に満たす生体認証として「マイクロ生体認証」と呼ばれる方式を提案している[14]．マイクロ生体認証は微細生体部位の静的な特徴量を認証情報として利用することで，以下のように各要件を満たす．

要件①：

一般的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，利便性を保ったまま不正者の偽造コストが高まり要求①が満たされる．

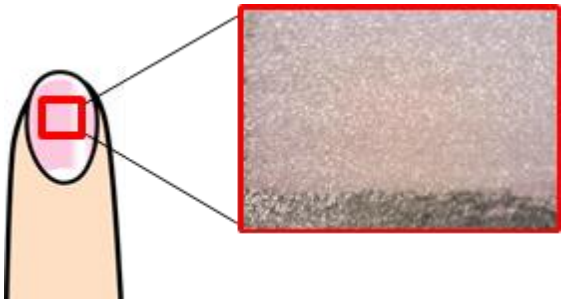


図 1：爪の表面の模様（黒い領域はマーク）
Figure 1: Texture pattern on the fingernail plate
(the black area is a part of mark)

要件②：

微細生体部位を用いることで，通常の生体認証と比較すると登録可能回数（未使用部位が枯渇するまでの回数）が激増する．例えば通常の指紋の 100 分の 1 サイズの微細部位を認証に利用するとする．通常の指紋は 1 つの指につき 1 つしかないが，100 分の 1 サイズの微細部位ならば同じ領域に 100*100=10000 の部位が存在することになる．そのため異なるシステムでは別の部位を登録することが容易であり，ゼロエフォートの攻撃者に対しては要件②を満たす．しかし，ユーザの変更可能な全ての生体情報を得るなどの攻撃を仕掛けてくる攻撃者（グレイトエフォート攻撃者）に対しては，異なるシステムで別の生体情報を利用していたとしてもそれらがリンクされてしまうため要件②を完全には満たしているとは言えない．

要件③：

前述のとおり，微細生体部位を用いることで通常の生体認証と比較すると登録可能回数が激増する．登録可能回数と更新可能回数はほぼ同義のため，マイクロ生体認証の更新可能回数は膨大となる．よって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，ユーザ自身の意志で登録部位を変更することが可能となり．要件③を満たす．

3.2 爪表面の微細部位を利用したマイクロ生体認証

要件②を完全に満たすマイクロ生体認証を実現するために，時間の経過で生え変わる生体部位を利用する．本稿では，その一実現形態として，爪の微細部位を利用したマイクロ生体認証を検討する．

爪は，爪先，爪床，爪郭，爪母基，遊離縁などから構成される皮膚の一部である[15]．図 1 に示すとおり，爪の表面を大きく拡大すると，爪の表面上に不規則な模様の存在を確認できる．この模様を認証情報として利用することで，爪画像を利用したマイクロ生体認証が実現可能であると期待される．一般的な若い成人男性の爪の伸びるスピードは，約 0.1 [mm/day]であると言われている[16]．爪が成長すると登録部位が遊離縁まで達し，その爪を切ることでそれまでの生体情報が抹消される．それと同時に，新しい特徴を持つ爪が生え変わるため，同じ爪の同じ位置であっても一定期間が経過することで生体情報が一新される．また，紙やすりなどで爪表面を軽く擦ることによって，爪の成長を待たずとも能動的に特徴を変更することも可能である．マイクロ生体認証のメカニズムにこのメカニズムが加わることにより，爪表面の模様を用いたマイクロ生体認証は下記のように要件①～③を満たす．

要件①：

マイクロ生体認証のメカニズムにより不正者の偽造コストが高まり，要件①が満たされる．

要件②：

マイクロ生体認証のメカニズムによりゼロエフォートの攻撃に対して要件②を満たす．提案方式ではそれに加えグレイトエフォート攻撃に対しても要件②を満たす．仮にある時点での変更可能な全ての爪表面情報を攻撃者が入手したとしても，爪の生え変わりや爪表面へ摩擦で生体情報が変更されることで，ユーザの生体情報は攻撃者が入手した生体情報とは異なる生体情報となり，異なるシステム間でのリンクは不可能となる．

要件③：

マイクロ生体認証のメカニズムにより登録可能回数が増大し，要件③を満たす．それに加え，爪の生え変わりなどによって生体情報が変化する度に登録可能回数がリセットされる．そのため，爪表面の模様を用いたマイクロ生体認証の登録可能回数は実質的に無限に近いと言える．

3.3 認証手順

提案方式の手順を以下に示す（図 2 も参照）．ここでは 1:1 認証の手順を示すが，1:N の認証への適用も可能である．

登録フェーズ：

1. ユーザは自分の ID をシステムへ登録する
2. システムはユーザに，爪表面へマークを印字するよう要求する
3. ユーザは爪表面へマークを印字する
4. システムはマークに従い，マイクロスコープでユーザの微細生体情報 X を読み取る
5. システムはそのユーザのテンプレートとして X をデータベースへ保存する

認証フェーズ：

1. ユーザは自分の ID をシステムへ提示する
2. システムはマークに従い，マイクロスコープでユーザの微細生体情報 X’を読み取る
3. システムはデータベースよりそのユーザのテンプレート X を参照する
4. X’が十分 X と近い場合，そのユーザは正規ユーザと判断される

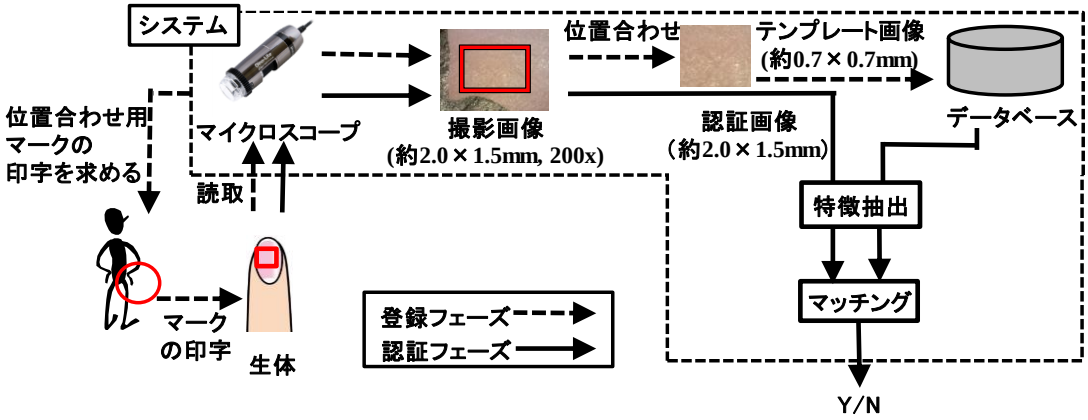


図 2：システム概要図

Figure 2: System overview

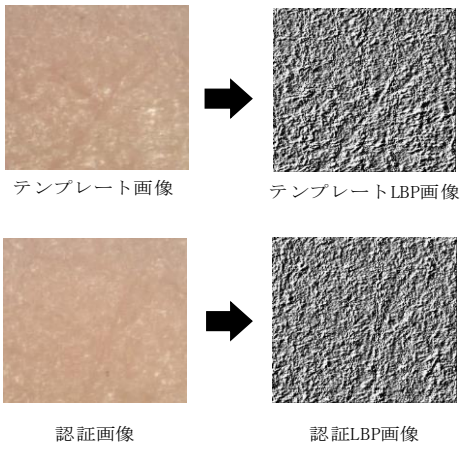


図 3：特徴抽出

Figure 3: Feature extraction

4. システム

今回構築したシステムについて詳細に説明する．本システムは，文献[14]で実装したマイクロ生体認証システムをベースに実装を行った．その構成を図 2 に示す．

4.1 登録部位の発見

マイクロ生体認証においては，システムが爪全体の中から登録微細部位を発見するために，爪の表面にマークを印字する必要がある．本稿では，水性インクを用いて爪の表面にマークを直接印字し，その上からトップコート（透明のマニキュア）を塗ってマークを保護する方法を採用する．油性インクを用いた場合，トップコートが油性のため互いに反発し，インクが滲んでしまうという問題が確認された．そのため本稿では油性インクではなく水性インクを用いる．

4.2 生体部位の撮影

本稿では爪の撮影にマイクロスコープを使用する．使用するマイクロスコープは AM7915-Dino Lite Edge S（サンコー株式会社製）である．このマイクロスコープを用いて爪表面の約 2.0×1.5mm の領域を 200 倍で撮影することによって，2592×1944 pixel の爪画像が得られる．登録時には，爪画像の中央 800×800 pixel をトリミングし，テンプレート画像として利用する．

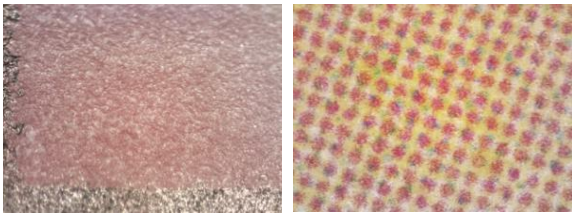
4.3 特徴抽出

本システムでは，爪の表面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，テンプレート画像および認証画像はグレースケール変換した後に Local Binary Pattern（以下 LBP）変換を行なう．LBP とは 1994 年に Ojala らによって提案された手法であり，画像の濃淡値の変化に頑健であるという性質を持つ[17][18]．なお，各処理は scikit-image Ver.0.14dev[19]に実装されている関数，rgb2gray，local_binary_pattern を使用して実装した．local_binary_pattern のパラメータは P を 24，R を 3，method を default とした．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画像を図 3 に示す．

4.4 マッチング

マッチングは LBP 変換後の画像のヒストグラムを比較することで行なう．ヒストグラムの比較には OpenCV3[20]に実装されている cv2.compareHist 関数を使用し，パラメータは method を cv2.HISTCMP_CHISQR とした．

認証画像の撮影時，マイクロスコープの傾きや位置をテンプレート画像の撮影時と全く同じにすることは非常に困難である．しかし，これらの傾きや位置のズレはノイズとなり認証率の低下を引き起こす．そこでまず，テンプレート画像に射影変換を施し，ひずみノイズを補正する．その後，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マッチングを行なうことで平行移動ノイズを補正する．これらの補正を施した上でテンプレート画像と認証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通りである．



(a) 元画像　　(b) プリンタ画像

図 4：市販のプリンタによるなりすまし攻撃

Figure 4: Impersonation by a commercially available printer

手順：

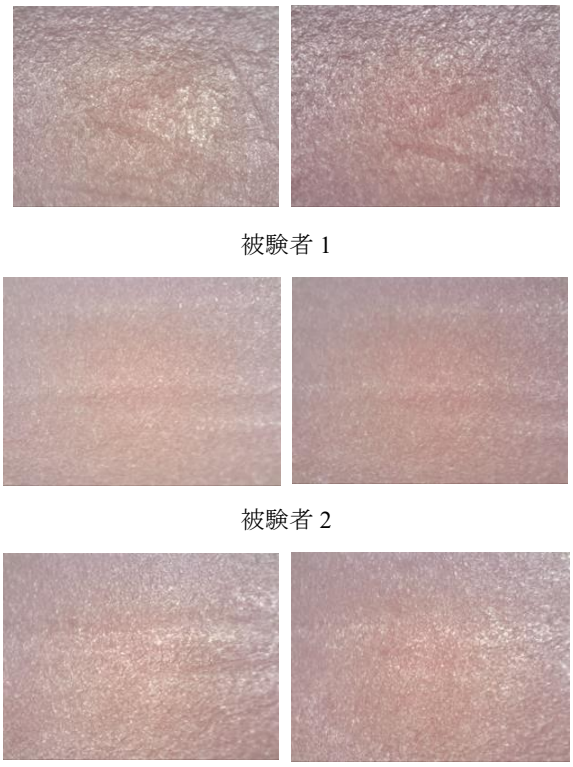
1. テンプレート画像の各頂点を左上から反時計回りに $P_{t0}, P_{t1}, P_{t2}, P_{t3}$ とする．
2. 認証画像撮影時のひずみや位置ずれの発生によって，認証画像の各頂点はテンプレート画像の $P_{ti}(0 \leqq i \leqq 3)$ と完全には一致しない可能性が高い．そこで，テンプレート画像の各頂点を中心とした 5×5 画素の集合を候補点群 $C_0 \sim C_3$ とする．
3. 4 つの候補点 C_0, C_1, C_2, C_3 によって囲まれる領域が 800×800 pixel の矩形画像となるように射影変換を施した画像群を用意し，テンプレート画像群とする．
4. 認証画像（2492×1944 pixel）に対してテンプレート画像（800×800 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マッチングを行い，認証画像の中でテンプレート画像と最も類似度の高い領域におけるマッチングスコアを算出する．
5. 3.で得たテンプレート画像群の全てに対し 4.を行い，最も類似度の高いマッチングスコアがテンプレート画像と認証画像のマッチングスコアとなる．

5. 考察

5.1 Unforgeability に関する考察

本節では爪表面の微細部位を利用したマイクロ生体認証がなりすまし耐性を有しているか考察する．本システムは画像ベースの類似度によって認証を行っているため，最も一般的ななりすまし手段である「印刷」に焦点を当てる．

本システムは爪表面を約 200 倍に拡大した部位を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 4 (a)は爪表面の約 2.0mm×1.5mm の領域をマイクロスコープで撮影した画像，図 4(b)はその画像を市販のプリンタ（Brother HL3170-CDW）を使用して，印刷サイズがそれぞれ約 2.0mm×1.5mm の大きさとなるように最高解像度（2400dpi）で印刷し，それをマイクロスコープで撮影した画像である．市販のプリンタ程度の解像度であれば，本物と比べて大きく異なることが確認できる．このように，本システムは，仮に生体情報が漏洩したとしても，攻撃者が本人になりすますことが困難となる機構を備えているため要件 1 が達成できていると言える．



被験者 1

被験者 2

被験者 3

図 5：圧迫前後の撮影画像
(左)圧迫前，(右)圧迫後

Figure 5: Images before/after shot fingers are pressed
left images are before pressed, right images are after pressed

しかし，不正者が高解像度のプリンタを使用した場合は，上記の対策だけでは不十分となる可能性もある．そういった場合には偽造物と生体を区別するための生体検知を組み込む必要があるだろう．爪表面を利用したマイクロ生体認証に適用可能な生体認証の一例として，反応性充血を利用する方法が考えられる．爪における反応性充血とは，指に圧力を加えることによって，爪の下の皮膚に流れる血流が増加する（皮膚が赤くなる）現象のことである[21]．これを利用し，撮影時に少し強く撮影部位を軽く圧迫して色素の変化を確認することで生体検知が可能であると考えられる．実際に 3 人の被験者に対し，指を軽く圧迫する前後の爪表面の微細部位を撮影した画像が図 5 である．目視でも圧迫後の画像は少し赤みが増していることが確認できるが，以下の方法で数値的に比較した．

1. 白飛びを抑制するために，画像から R,G,B 値全てが 200 以上の画素を間引く．
2. R,G,B それぞれで，値が 150 以上の画素数をカウントし，その数をそれぞれ R’,G’,B’とする．
3. 画像がどの程度赤色傾向にあるのかを R’/(R’+G’+B’)

を計算して求める．

こうして求めた値を図 5 の画像で比較すると，圧迫前：圧迫後の値はそれぞれ，0.44:0.59（被験者 1），0.34:0.48（被験者 2），0.38:0.43（被験者 3）となった．普通，印刷物や偽造物は圧迫前後で色素が変化しないため，簡易的ではあるが,反応性充血を利用した生体検知の可能性が示された．

5.2 想定される攻撃に関する考察

提案方式は一般的な生体認証と異なり，ユーザ自身が大量の生体情報を身体の中に有している．そのため，不正者は正規ユーザの生体を盗むまでもなく不正者自身が大量に有している生体情報を利用することで，ある程度大きな回数の攻撃を行うことが可能である．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．想定される対策としては，マークそのものの人工物メトリクスも併用し，生体情報とマーク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．生体とマーク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

6. むすび

本論文では，物理的な生体情報に対して忘れられる権利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を提案し，ハンディタイプのマイクロスコープを利用した生体認証システムを実装した．

今後は，実験を通じて本システムの可用性を評価していくと共に 6.1 節，6.2 節でも少し触れた，生体検知や想定される攻撃方法についても更に検討を深めていく予定である．

謝辞

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] 安藤均．「忘れられる権利」は新しい人権か：「忘れられる権利」をめぐるプライバシの検討．旭川大学経済学部紀要. 2017, no. 76, p. 71-100.
[2] 石井夏生利．「忘れられる権利」をめぐる論議の意義．情報管理/科学技術振興機構 編. 2015, vol. 58, no. 4, p. 271-285.
[3] “THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016”. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, (参照 2019-01-24).
[4] “Privacy Information Center”. https://www.universalorlando.com/web/en/us/privacy-info-center/index.html#subnav-e, (参照 2019-01-24).
[5] C. Rathgeb, and A. Uhl.. A survey on biometric cryptosystems and cancelable biometrics. Journal on Information Security. 2011, p. 1-25.
[6] “「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”. http://www.sankei.com/affairs/news/170109/afr1701090002-n1.html, (参照 2019-01-24).
[7] ISO/IEC DIS 30136. Information technology -- Performance testing of biometric template protection schemes. 2017.
[8] A. K. Jain, K. Nandakuma, A. Nagar. Biometric Template Security. EURASIP Journal on Advances in Signal Processing. 2017, vol. 2008, Article ID 579416, p. 17.
[9] 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. 2017, vol. 11, no. 2, p. 108-112.
[10] “Security Features of the New Bank of Japan Notes”. https://www.boj.or.jp/en/note_tfjgs/note/security/bnnew3.htm/ (参照 2019-01-24).
[11] 松本勉，岩下直行．金融業務と人工物メトリクス．金融研究. 2004, vol. 23, no. 2，p. 169-186.
[12] 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. 2014，論文 No. 2E2-3.
[13] Shruti Garg, Amjoy Kumar, and M. Hanmandlu. Finger Nail Plate: A New Biometric Identifier. International Journal of Computer Information Systems and Industrial Management Applications. 2014, vol. 6, p. 126-138.
[14] 藤田真浩，眞野勇人，村松弘明，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．電子小情報通信学会論文誌(A). 2017. vol. J100-A, no. 12, p. 465-474.
[15] R.クルスティッチ，牛木辰男，金沢寛明．立体組織学アトラス(原題：Human Microscopic Anatomy An Atlas for Students of Medicine and Biology)．西村書店, 2017, p. 23-237.
[16] S Yaemsiri, N Hou, MM Slining, and K He. Growth rate of human fingernails and toenails in healthy American young adults. Journal of the European Academy of Dermatology and Venereology. 2010, vol. 24, no. 4, p. 420‑423.
[17] T.Ojala, M. Pietikainen, and D. Harwood. Performance evaluation of texture measures with classification based on Kullback discrimination of distributions. Proceedings of 12th International Conference on Pattern Recognition. 1994, vol. 1.
[18] 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. 2012, Vol. 202-CG-149, no. 3, p. 1-6.
[19] “scikit-image”. https://scikit-image.org/, (参照 2019-01-24).
[20] “OpenCV”. https://opencv.org/, (参照 2019-01-24).
[21] 蔵本築，矢崎義雄．冠血管の反応性充血．呼吸と循環. 1969, vol. 17, no. 9, p. 793-799.