

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

塩見 祐哉¹ 杉本 元輝¹ 杉本 彩歌¹ 上原 航汰¹
藤田 真浩¹ 眞野 勇人¹ 大木 哲史¹ 西垣 正勝¹

概要： マイクロ生体認証は、人間の微細生体情報を利用した生体認証メカニズムである。著者らは爪の微細部位を用いることで、「忘れられる権利を満たす生体認証」の提案を文献[3][4]にて行った。しかし、文献[3][4]にて提案した方式には3つの課題点が存在していることから、認証精度や利便性に問題があった。そこで、本稿では、関連研究による着想から、その課題点を解決し、更にリアルタイムマッチングを可能とする改良システムの構築を行った。本稿の内容は次の3つの内容から構成される。はじめに、忘れられる権利を満たす生体認証として、マイクロ爪認証について、その内容を説明する。次に既存研究における課題点を解決する改良システムの詳細について述べる。最後に改良システムの実験を行い、改良システムの可用性、速度について評価する。

Micro Biometric Authentication Using Fingernail Surface : A Study for Practical Use

YUYA SHIOMI¹ GENKI SUGIMOTO¹ AYAKA SUGIMOTO¹
KOTA UEHARA¹ MASAHIRO FUJITA¹ YUTO MANO¹
TETSUSHI OHKI¹ MASAKATSU NISHIGAKI¹

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でき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。これは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できる権利を認めたものである。ここで「個人データ」とは、識別された人または識別可能な人（「データ主体」）に関する情報を意味する。

また、情報端末がPCからスマートフォンに変遷したことから、本人認証の手段として生体認証の重要性が増している。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篤な個人データであり、その取扱いは多大な配慮が必要となる。その中でも、消去権の担保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[3][4]。

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。文献[4]では、マイクロスコープによって撮像される微細爪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実装し、3日間にわたるユーザ実験を実施した。その結果、マイクロ爪認証の短期期間（3日間）における可用性を示した。

ただし、文献[4]で構築したプロトタイプシステムはPoC（Proof of Concept）としての実装であり、実運用に対する課題が存在していた（3.1節にて詳述する）。そこで本稿では、文献[4]で構築したシステムを改良し、PoI（Proof of Implementation）レベルのプロトタイプシステムを構築する。

以降、2章では爪を利用したマイクロ生体認証について概説する。3章でプロトタイプシステムの改良方法を説明し、4章で改良システムを実装する。5章では基礎実験を行い、改良システムの可用性と速度について評価する。最後に6章でまとめと今後の課題を述べる。

2. マイクロ爪認証

筆者らは文献[3][4]にて、マイクロスコープによって撮像

¹ 静岡大学
Shizuoka University

される微細爪画像を利用した「忘れられる権利を満たすマイクロ生体認証」を提案した。本章では文献[3][4]の内容を概説する。

2.1 コンセプト

著者らは、忘れられる権利を満たす生体認証に対する要件として、以下の4つの要件を定義した。

- 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** : 認証システムに提示する生体部位から異なる生体情報を生成可能であること。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。
- 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。

著者らは、要件①～④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①～③を満たす。また、要件④については、PoC レベルの認証システムを構築し、実証実験によりこれを確かめた。

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、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ることが可能であると期待される。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1mm四方の微細部位であれば、1つの爪の表面（表面積を1cm²と想定）中に異なる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。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、短期的な観点での要件③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③が満たされる。

2.2 マイクロ爪認証の認証手順

マイクロ爪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が、1対N認証の場合にも適用可能である。

登録フェーズ :

1. ユーザは自分のIDを認証システムへ登録する
2. 認証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. 認証システムはマークを目印にして、マイクロスコープでユーザが提示した爪表面の微細部位の画像Xを読み取る
5. 認証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. 認証システムはマークを目印にして、マイクロスコープでユーザが提示した爪表面の微細部位の画像X'を読み取る
3. 認証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に近い場合、そのユーザは正規ユーザと判断される

3. プロトタイプシステムの改良

3.1 PoC システムにおける課題点

2章で述べたとおり、筆者らは、文献[3][4]にてマイクロ爪認証のPoC（Proof of Concept）レベルの認証システムを実装し、評価実験を通じて提案方式の有用性を確認した。しかし、PoCシステムは以下の3点の課題を抱えていた。

課題1: 撮影の際の手ブレ、被写体ブレ

PoCシステムでは、マイクロスコープおよび被写体の固定については特別な配慮がなされていなかった。その結果、

撮影の際に手ブレ、被写体ブレが生じ、利便性（撮影の易さ）や認証精度の低下を引き起こす原因となっていた。

課題 2: マークを利用した位置合わせ

PoC システムでは、認証に利用する微細部位を特定するために、ユーザの爪表面にマークを記す必要があった。マークの記載は、審美的感覚からユーザが許容しにくい、マークが消えてしまうと撮影すべき場所が分からなくなり認証が困難になるといった課題が存在し、利便性の低下を引き起こす原因となっていた。

課題 3: 爪の鏡面反射によるノイズ

PoC システムでは、顕微鏡を手で把持して爪表面の撮影を行っていたため、撮影の都度異なった位置、角度から自然光が爪に当たる状態になっていた。爪の表面には微細レベルの凹凸があり、光源からの入射光がその凹凸形状に従って半鏡面反射するため、爪を撮影する際の照明条件の変化は撮影画像において大きなノイズとなり、認証精度の低下を引き起こす原因となっていた。

3.2 課題点に対する改良

課題 1 は、カメラおよび被写体を固定していなかったことに起因する問題である。課題 2 は、カメラと被写体の相対位置を固定できていなかったことに起因する問題である。課題 3 は、照明条件を固定できていなかったことに起因する問題である。そのため、カメラ、被写体、光源を固定する治具を用意することによって、3 つの課題が一挙に改善されることが期待される。

まず、顕微鏡の接眼レンズの周囲に LED（発光ダイオード）を接着することによって、カメラと光源の相対位置を固定する（図 1）。そして、認証時にユーザの指を収容するための「指型（図 2）」を作成し、この指型を顕微鏡スタンドと連結固定させる（図 3）ことによって、カメラと被写体の相対位置を固定する。これらにより、撮影時の顕微鏡、爪、LED の 3 者の相対位置が一意に定まるようになる。ここで、光源の固定による鏡面反射ノイズの抑制は、文献[5]において提案されている FIBAR（Fingerprint Imaging by Binary Angular Reflection）と呼ばれる撮影方法（図 4）から着想を得ている。

3.3 指型の製作

3D プリンタを使って作成した指型を図 2 に示す。顕微鏡と指型の相対位置は常に一意となるように、

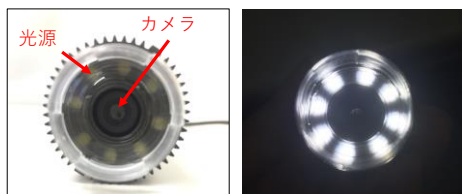


図 1 カメラと光源の取り付け(右図は光源点灯時)

2 今回の実装においては、接眼レンズの周囲に 8 つの LED が設置されている顕微鏡を使用した。

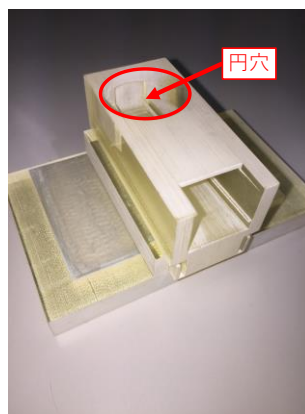


図 2 指型



図 3 顕微鏡スタンドと指型の連結固定

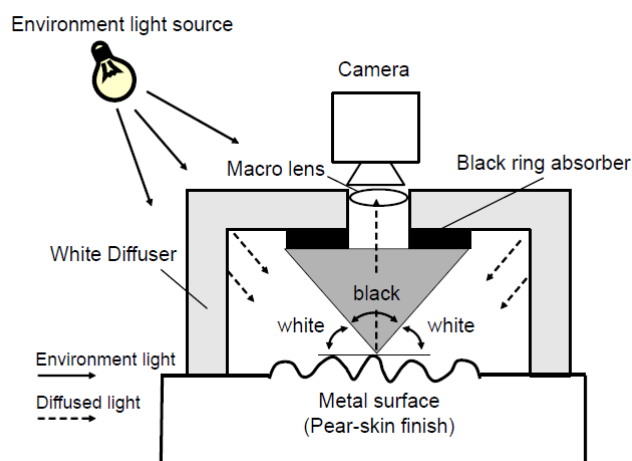


図 4 FIBAR 撮影法（参考文献[5]，図 2 より出典）

指型は顕微鏡スタンドと連結固定される仕組みになっている（図 3）。円穴部に顕微鏡の接眼レンズが収納される構造となっている。

ユーザが指型に指を挿入すると、円穴の中心部に爪が固定される構造となっている（図 5）。ここで、指型内の指の相対位置を常に一意にするためには、指の 3 次元位置（ X 、 Y 、 Z ）と姿勢角（ロール α 、ピッチ β 、ヨー γ ）を固定することができる指型が必要となる（図 6）。

図 7 に記されているように、指型はテーパ構造を有している。これによって、ユーザが指型に指を挿入した際に、ユーザの指の太さに応じた位置で指が止まり、指の位置 X 、 Y がほぼ固定される。また、指型は一般的なユーザの指幅に合わせた縦長の形状となっており、ヨー γ はゼロにほぼ固定される。図 8 に記されているように、指型は底面が平行となっており、指の位置 Z はユーザの指の高さに応じた位置でほぼ固定される。同時に、ピッチ β はゼロにほぼ固定される。図 9 に記されているように、指型内面の右側面に挿入口から奥にかけて一直線の凸状ガイドを設置した。

このガイドに爪の右縁に沿わせるように指を挿入してもらうことで、ロール α の角度もほぼ固定される(図 10)。

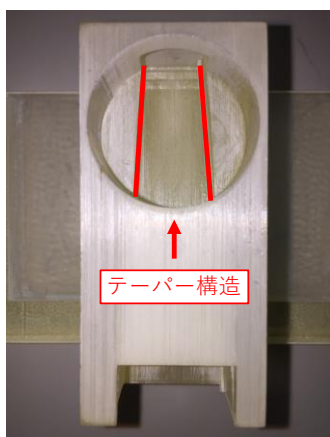


図 5 テーパー構造

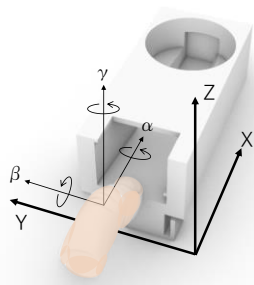


図 6 指型に挿入された指の3次元位置と姿勢角

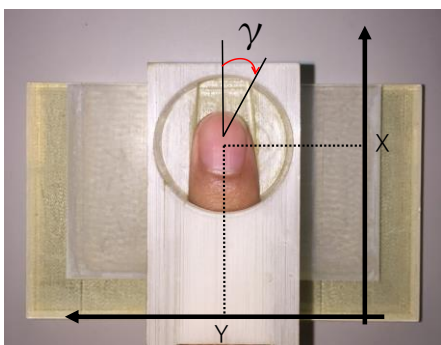


図 7 テーパー構造による X, Y, γ の固定

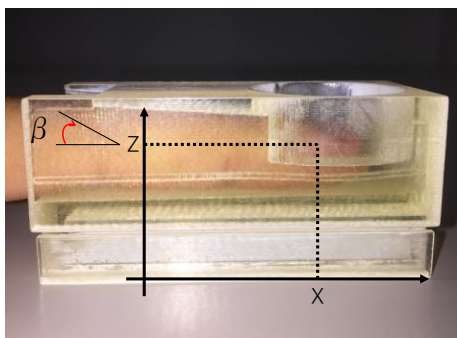


図 8 指型底面による Z, β の固定

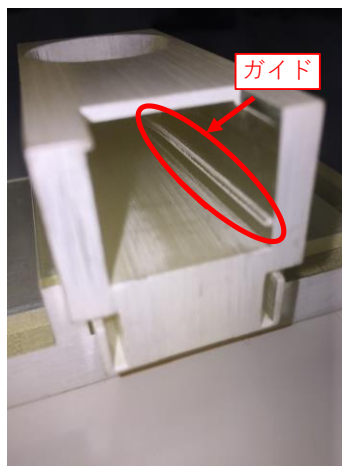


図 9 指型の凸状ガイド

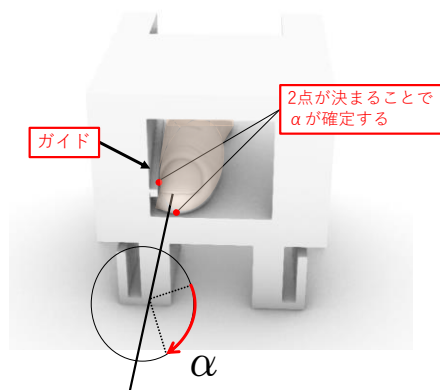


図 10 ガイドによる α の固定

3.4 改良システムの実装

文献[3][4]のプロトタイプシステムに、3章で作成したマイクロスタンドと一体化(連結固定)した指型を適用することによって、改良システムを構築した。改良システムの全体像を図 11 に示す。以下にその詳細を示す。下記において記載されている各パラメータは、予備実験の過程での試行錯誤を通じて経験的に決定したものである。

3.5 爪画像の撮影

マイクロスタンドを用いて爪表面の拡大画像を撮像する。改良システムが採用したマイクロスタンドは AM7915MZT Dino-Lite Edge S (Dino Lite 社製) である。

爪画像の撮影は、ユーザが指型に指を挿入した状態で行われる。撮影倍率は約 200 倍であり、爪表面の約 2.0×1.5 mm の領域を 640×480 pixel の解像度で撮影する。登録時には、 640×480 pixel の画像の中央 256×256 pixel (約 1.0×1.0 mm) をテンプレートとして保存する。認証時には、 640×480 pixel の画像の中央付近の領域の中から、テンプレート画像とのマッチする 256×256 pixel を探すという作業となる。

3.6 リアルタイムマッチング

改良システムでは、ノート PC にマイクロスタンドの映像を表示させつつ、任意のタイミングで爪画像の登録、認

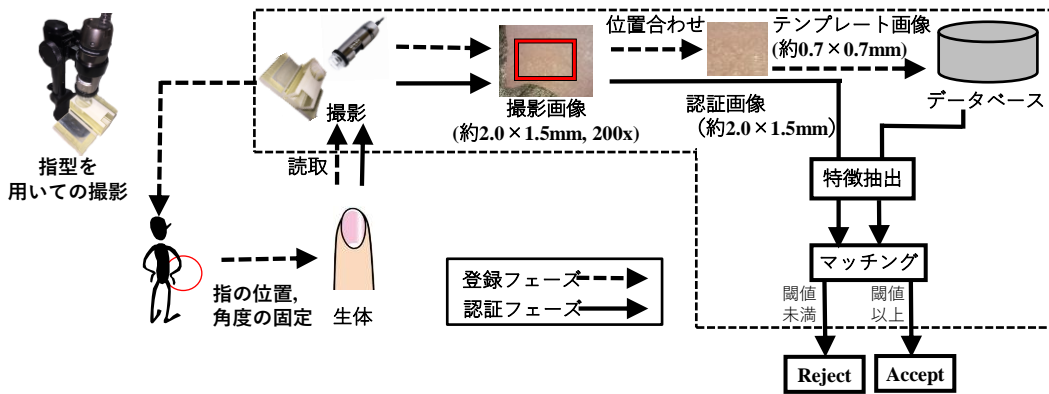


図 11 改良システムの全体像

証が実行できる。登録ボタンの押下により、登録用爪画像の撮影とテンプレート画像の保存が行われる。認証ボタンの押下により、認証用爪画像の撮影と認証可否の判定が行われる。認証可否は、テンプレート画像と認証画像の間のマッチングスコアに基づいて判定される。マッチングアルゴリズムとして、文献[3]で用いたブルトフォースマッチング、AKAZE（特徴点抽出）[6]を利用したマッチング、ZNCC（零平均正規化相互相関）[7]を利用したマッチングを採用した。文献[3]の方式は、処理速度を向上させるために、一部パラメータの再調整を行っている。文献[3]の方式においてはグレースケール化およびLBP変換の前処理が、ZNCCを利用した方式においてはグレースケール化の前処理が、それぞれ適用されている。

4. 基礎実験

4.1 緒言

今回構築した改良システムを用いた基礎的な認証実験を3日間に渡って実施した。被験者は情報学部の大学生12名（男性10名、女性2名）である。実験に際しては、

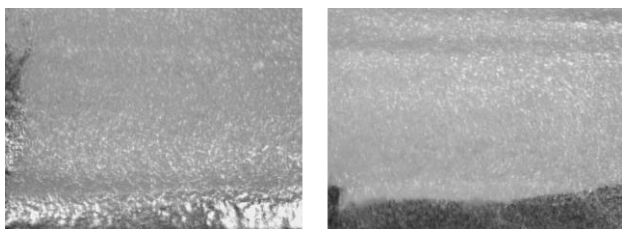


図 12 異なる日時に撮影された同部位の爪画像（既存システム）

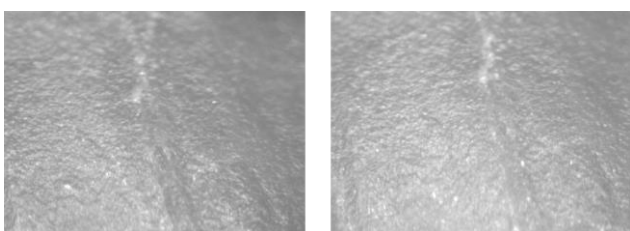


図 13 異なる日時に撮影された同部位の爪画像（改良システム）

大きさの異なる2つの指型を用意した。実験開始時に、全ユーザに右手の人指し指、中指、薬指をそれぞれ2つの指型に挿入してもらい、サイズの最もフィットする指と指型をユーザごとに選択してもらった。テンプレートの撮影は実験1日目に行った。認証画像の撮影は、1日目のテンプレート撮影直後、1日目のテンプレート撮影から一定時間経過後（1時間以上）、3日目の計3回行った。被験者 i ($1 \leq i \leq 12$)のテンプレート画像を t_i と表記し、被験者 j ($1 \leq j \leq 12$)の k 回目 ($1 \leq k \leq 3$)の認証画像を $a_{j,k}$ と表記する。

4.2 可用性評価

爪表面の微細部位を用いて本人認証が可能か否を評価する。本人間のマッチングスコアは同一被験者のテンプレート画像 t_i と認証画像 $a_{i,k}$ ($i=j$)を比較することで算出し、他人間のマッチングスコアは本人のテンプレート画像 t_i と他人の認証画像 $a_{j,k}$ ($i \neq j$)を比較することで算出する。各マッチングアルゴリズムにおけるEERの値を表1に示す。3日目における最良のマッチングアルゴリズムはZNCCであり、閾値 ≈ 0.32 のときでEER ≈ 0.16 であった。

改良システムにおいて導入した指型によって、マイクロスコープと被写体の相対位置を固定することが可能となり、手ブレおよび被写体ブレを軽減するとともに、位置合わせのためマークを不要とすることを達成した。マイクロスコープ、LED、指型を一体化させた結果、照明条件も均質化され、半鏡面反射する爪表面の画像取得も安定した。既存システムと改良システムにおける爪画像の比較を図12図13に示す。

表 1 認証精度結果(EER)

マッチングアルゴリズム	文献[3]方式	AKAZE	ZNCC
撮影日時			
1日目(テンプレート撮影直後)	約25%	約11%	約5%
1日目(一定時間経過後)	約39%	約24%	約11%
3日目	約45%	約27%	約16%

表 2 実行時間結果

	マッチングアルゴリズム		
	文献[3]方式	AKAZE	ZNCC
実行時間	11.05秒	0.14秒	0.025秒
標準偏差	0.437秒	0.051秒	0.011秒

4.3 速度評価

認証1試行あたりの提案システムのマッチングにおける所要時間を評価する。マッチング処理が開始されてから認証結果が出力されるまでの時間を計測する。それぞれのマッチングアルゴリズムに対する所要時間を表2に示す。最も高速なマッチングアルゴリズムはZNCCを用いた方式であり、1試行あたり約0.025秒であった。

5. おわりに

本稿では筆者らが提案している、マイクロスコープによって撮像される微細爪画像を用いた生体認証（マイクロ爪認証）について紹介した。次に、マイクロ爪認証の改良システムの構築を行い、その詳細について説明を行った。最後に構築した改良システムについて実験、および評価を行った。今後は、さらなる認証精度、利便性向上のために、マッチングアルゴリズムの改良や、指型の構造について検討していく。

謝辞

実験協力を快諾してくださった学生諸氏に、心から感謝の意を申し上げます。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ーの検討”, 旭川大学経済学部紀要, no.76, pp. 71-100, (2017).
- [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/科学技術推進機構 編, Vol.58, no.4, pp.271-285, (2015).
- [3] 杉本元輝, 藤田真浩, 眞野勇人, 大木哲史, 西垣正勝, “忘れられる権利を満たす生体認証: 爪を用いたマイクロ生体認証”, 情報処理学会研究報告, Vol.32, No.13, pp.1-6, (2019).
- [4] 杉本 元輝, 藤田 真浩, 眞野 勇人, 大木 哲史, 西垣 正勝, “使い捨て可能な生体認証の提案～ 爪の模様を用いたマイクロ生体認証 ～”, 信学技報, Vol.117, No.520, pp.127-132, (2018).
- [5] Toru Takahashi, Rui Ishiyama, “FIBAR: Fingerprint Imaging by Binary Angular Reflection for Individual Identification of Metal Parts”, Proc EST 2014, IEEE, pp.46-51, (2014).
- [6] Pablo Alcantarilla: “pablo’s home”, available from <http://www.robosafe.com/personal/pablo.alcantarilla/index.html>, (accessed 2019-05-10).
- [7] Luigi Di Stefano, Stefano Mattoccia, Federico Tombari, “ZNCC-based template matching using bounded partial correlation, Pattern recognition Letters”, Vol.26, No14-15, pp.2129-2134, (2005)