

量子論的生体認証：
生体情報の新たな物理的様相に踏み込む微細生体認
証技術

メタデータ	言語: ja 出版者: 公開日: 2024-03-22 キーワード (Ja): キーワード (En): 作成者: 西垣, 正勝 メールアドレス: 所属:
URL	http://hdl.handle.net/10297/0002000420

令和 5 年 6 月 21 日現在

機関番号：13801

研究種目：基盤研究(B)（一般）

研究期間：2018～2022

課題番号：18H03239

研究課題名（和文）量子論的生体認証：生体情報の新たな物理的様相に踏み込む微細生体認証技術

研究課題名（英文）A quantum approach for biometric authentication: micro biometric authentication technology to break into a new physical aspect of biometric information.

研究代表者

西垣 正勝（NISHIGAKI, Masakatsu）

静岡大学・情報学部・教授

研究者番号：20283335

交付決定額（研究期間全体）：（直接経費） 13,100,000円

研究成果の概要（和文）：生体認証には、「生体情報は生涯不変であり、任意に更新できない」という物理的性質に起因する、なりすましと追跡可能性の問題が存在する。本研究では、なりすまし耐性と追跡不可能性の両要件を満足する生体認証の実現を目指し、「微細」生体部位を利用した生体認証システムを構築する。拡大鏡によって撮影される微細「爪」画像を用いた生体認証システムの設計・実装・評価と、利便性・安全性の強化を行う。物理的な生体情報そのものの保護を達成する本研究と、既存のテンプレート保護技術（ビット列に符号化された生体情報を保護する技術）を融合し、プライバシーを保ちながら生体認証の安全性を確保する。

研究成果の学術的意義や社会的意義

近年は、コインロッカーの利用などの「カジュアルなサービス」でも生体認証が用いられるようになってきている。カジュアルなサービスでは、本人性の確認は不要で、属性（代金を支払った利用者であるか）の確認で事足りる。また、登録から短期間の内に認証が実行される（例：コインロッカーに荷物を預ける 取り出す）ケースが多い。このような利用シーンにおいては、利用者のプライバシー保護が重要なニーズとなる。今やEUの一般データ保護規則に「消去権」が記載され、生体認証の分野においても「生体情報の消去」への配慮が必須となっている。忘れられる権利を満たす生体認証の実現を目的とする本申請の学術的意義および社会的意義は大きい。

研究成果の概要（英文）：Biometric authentication has the problems of impersonation and traceability due to the physical nature of biometric information, which is invariant throughout life and cannot be arbitrarily updated. This research constructs a "micro" biometric authentication system to realize a biometric authentication system that satisfies both impersonation resistance and un-traceability. A biometric authentication system using minute "fingernail" images captured by a microscope is designed, implemented, and evaluated in this research.

研究分野：情報セキュリティ

キーワード：微細生体 爪 肌理 なりすまし プライバシ

1. 研究開始当初の背景

生体認証は、事前に生体情報をテンプレートとして登録し、認証時に取得した生体情報とテンプレートを比較することで認証を行う。携帯端末には生体（指紋・顔）認証が標準搭載され[1]、FIDO Alliance も端末認証の手段として生体認証を有力視している[2]ことから、生体認証に対する期待は非常に高い。公開鍵基盤（PKI）における秘密鍵を生体情報で置き換える「公開生体認証基盤（PBI）」が提案されている[3]。

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。しかし一方で、生体情報の「生涯不変であり、任意に更新できない」という物理的性質に起因する、なりすましと追跡可能性に関する課題が存在する。

「なりすまし」は、攻撃者が正規ユーザの生体情報を入手して偽造生体を作成する攻撃である。攻撃者が顔写真や人工指を複製し、なりすましに成功した例が既に多数報告されている（[4]他）。攻撃者は、生体認証によってログインする正規の 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不正に収集（フィッシング）することも可能である。安全性の観点から、なりすまし（偽造生体の作成）を困難にする必要がある（要求 1）。

「追跡可能性」は、匿名・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できるという問題である。生体情報は、ユーザ本人との紐づきをリセット（変更・交換）できないため、ある人物が 2 つのサービスにおいて異なるユーザ ID を使ってユーザ登録をしたとしても、認証情報である生体情報から同一人物であることが判明してしまう。プライバシー保護の観点から、登録情報を「消滅」させて追跡可能性を断絶する必要がある。近年、EU の一般データ保護規則[5]に「忘れられる権利（消去権）」が記載されたこともあり、生体認証の分野においてもこの「消去権」への配慮が求められる（要求 2）。

要求 1, 2 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が提案されている。その代表が、乱数情報を用いてテンプレート（生体情報）を秘匿（マスク）するキャンセル生体認証[6]である。乱数マスクによってテンプレートからの生体情報の漏洩を防ぎ（要求 1 の解決）、乱数情報を変更することによって過去のテンプレートを失効させることも可能である（要求 2 の解決）。しかし、テンプレート保護技術は、文字通り、「テンプレート（ビット列に符号化された生体情報）」を守るための対策であり、生体情報そのものを保護する対策にはなり得ていない。

2. 研究の目的

本研究では、「生体情報そのもの」に対して要求 1 と 2 を満足する生体認証技術の確立という目的の達成に向けて、微細生体部位の利用というアプローチによって生体情報の「生涯不変であり、任意に更新できない」という物理的制約に対処する（図 1）。

要求 1 の解決：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、（光の波長程度までのサイズの物体であれば）ズームレンズを使って対象物の細部を撮影することは、模造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認証情報とすることによって、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される。

要求 2 の解決：我々の身体は、指紋のパターンや骨格の形状などは比較的長期に渡って変化しないが、皮膚組織や骨組織のレベルでは新陳代謝によって日々入れ替わっている。このように、生体情報も、取り扱うサイズが微細になれば、その物理的様相が変わる。ユーザがある時点で生体情報を登録したとしても、生体部位が入れ替わる度に、その生体情報自体が消滅し、追跡可能性が断絶されることになる。

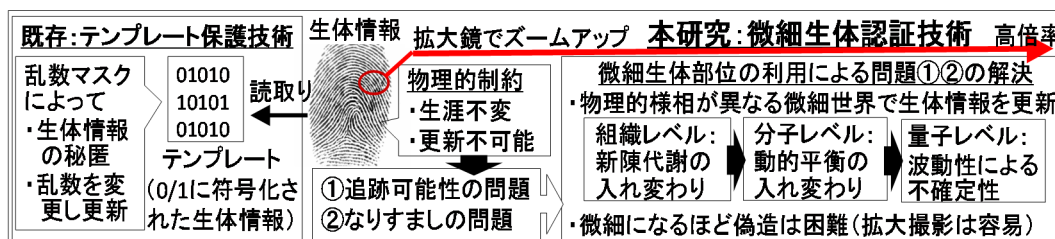


図 1：微細生体認証の概念

3. 研究の方法

μm（マイクロメートル）レベルの微細生体部位の利用によって、要求 1（なりすまし耐性：偽造生体作成の困難化）と要求 2（追跡困難性：登録生体部位の消失）を同時に達成する生体認証技術を実現する。本研究では、1mm 角の爪の表面の微細凹凸模様を 200 倍に拡大した画像を用いた生体認証システム（マイクロ爪認証システム：図 2）を実装・評価し、その有用性を示す。図 2 の認証手順は以下の通りである。

【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、マイクログラフ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、マイクログラフ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 と近い場合、そのユーザは正規ユーザと判断される。

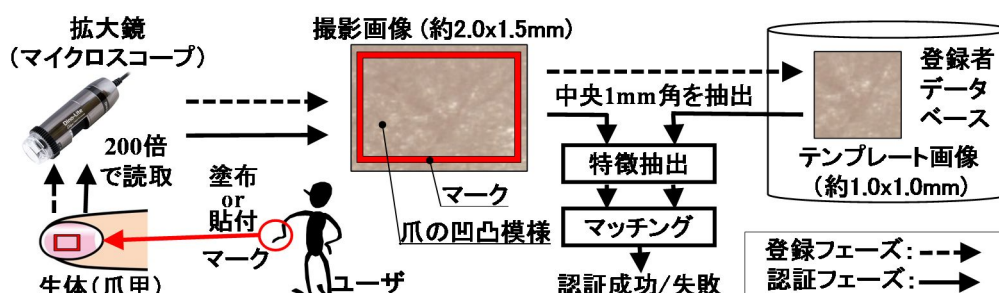


図 2：微細爪画像を利用した生体認証：マイクロ爪認証システム

爪の表面（爪甲）を大きく拡大すると、不規則な凹凸パターンの存在を確認できる。この爪甲パターンを認証情報として利用する。爪甲パターンは数十 μm 程度で微細であり、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（要求 1）。爪母（爪の根本）にある細胞が細胞分裂を起こすことで、新しい爪が作られる。爪が伸びて登録部位が遊離縁（爪先）まで達し、爪が切られた時点で、追跡可能性は完全に分断される（要求 2）。

認証の際には、登録部位に正しく拡大鏡（マイクログラフ）を押し当てる必要がある。すなわち「位置合わせ」が非常に重要となる。図 2 のシステムにて、ユーザが自身の爪に「マーク」を付けるのは、この位置合わせを実現するためである。マークは、ネイル化粧品型（塗布型マーク）、ネイルアート型（貼付型マーク）など、用途に応じ使い分ける。

更に、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、図 2 の 1:1 認証型マイクロ爪認証システムの利便性と安全性を拡張する。QR コードにユーザ ID を埋め込むことにより、爪を提示するだけでユーザ ID も同時に認証システムに読み取らせることが可能となり、図 2 の認証システムの仕様を変更することなく、1:N 型の手ぶら認証が実現される。QR コードに乱数を埋め込むことにより、爪を提示するだけでテンプレート保護用の乱数情報も同時に認証システムに読み取らせることが可能となり、図 2 の認証システムの仕様を変更することなく、テンプレート保護型認証が実現される。

4. 研究成果

図 2 のマイクロ爪認証システムに対し、定性的、定量的の両面から評価を行った。

【定性的評価】

テンプレート保護型生体認証において定義されている 4 項目[7]を拡張する形で、「物理的な生体情報そのものに対する消去権を満たす生体認証に求められる項目」を定義した。

- ・項目 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。
- ・項目 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。
- ・項目 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。
- ・項目 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。
- ・項目 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。
マイクロ爪認証は、下記のとおり、項目 ~ を満たす方式となっている。なお、項目 については、定量的評価（実証実験）によりこれが満たされることを確認した。
- ・項目 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、項目 が満たされる。

・項目 に対する充足性：

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つの爪の表面中(表面積を1cm²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、項目 が満たされる。

・項目 に対する充足性：

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、項目 が満たされる。

・項目 に対する充足性：

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が可能である。これにより、短期的な観点で項目 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項目 が満たされる。

【定量的評価】

マイクロ爪認証の有効性をユーザ実験によって評価した。被験者は静岡大学生の男女10名である。1人あたり右手の人差し指、中指、薬指の3つの爪を使用し、各爪で縦方向(爪が成長する方向)に任意の2箇所を登録生体部位として設定し、それらの画像(計6箇所)を撮影した。実験は、テンプレートを撮影した日を1日目として5日間行った。1日目の午前中にテンプレート画像を撮影し、午後1回目の認証画像を撮影した。その後3日目と5日目に日中の任意の時間帯で認証画像の撮影を行った。今回の実験で収集した認証画像は10名×6部位×3日間=180枚である。

(1) Performance 評価：

マイクロ爪認証が忘れられる生体認証の項目 を満たしているかを、同じ被験者内の同部位間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(他人スコア)を比較することで評価した。実際の実験を通じて求められた本人スコアと他人スコアを基に、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(FRR)と他人受入率(FAR)の変化を図3に示す。この時の等価エラー率(EER)を求めたところ、認証閾値=182でEER 7%であった。

また、認証閾値=150を採用した場合には、FRR 15%、FAR 2%という認証精度となるといった結果が得られた。このような特徴を有する生体情報の場合は、複数部位を利用したOR型認証を構成することによって、その認証精度を更に高めることが可能である。例えば、爪の微細部位2箇所を利用したOR型認証の認証精度は、単純な理論計算では、FRR 2%(2箇所とも本人拒否される事象の確率のため、 0.152×0.023)、FAR 4%(2箇所とも他人受入が起こらない事象の余事象の確率のため、 $1 - \{1 - (0.02)\}^2 = 0.040$)となる。微細生体情報の場合は、1つの爪画像の中から2箇所の領域を互いに重ならないように抽出することができる。これによって、撮影の手間を増加させずに2箇所の微細部位を用いたOR型マイクロ生体爪認証を実行することが可能である。

このように、被験者10名による基礎実験の結果ではあるが、本システムが、爪の微細部位1箇所でもEER約7%の認証精度を達成し、また、2箇所のOR型認証でFAR約4%のときにFRR約2%の認証精度向上を達成することが確認できた。適用先によっては十分な認証精度とは言えないものの、マッチングアルゴリズムの改良等を通じて認証精度を更に改善する余地は残されていると期待される。以上より、マイクロ爪認証システムが項目 を満たす可能性が示唆された。

(2) Un-linkability 評価、Diversity 評価：

マイクロ爪認証が忘れられる生体認証の項目 および を満たしているか、同一被験者の同じ爪であっても部位が異なれば別の生体情報とみなせるか(爪母基で都度生成される爪の表面の凹凸模様に規則性はないか)という観点から評価する。同一被験者の異爪間の凹凸模様の不規則性については、同一被験者内の異部位間を比較したマッチングスコア(同人異部位間スコア)を算出することによって評価することができる。今回の基礎実験では、爪ごとに爪の成長する方向に2箇所の異なる微細部位を登録しているので、同一被験者の同じ爪の異部位間の比較に特化したマッチングスコア(同爪異部位間スコア)についても算出し、同一爪内の微細部位間の凹凸模様の不規則性についても評価する。

実際の実験を通じて求められた本人スコアと同人異部位間スコアを基に、認証閾値を変更した際の本人拒否率(FRR)と他人受入率(FAR)の変化を図4に示す。そして、本人スコアと同爪異部位間スコアを基に、認証閾値を変更した際の本人拒否率(FRR)と他人受入率(FAR)の変化を図5に示す。図4ならびに図5の等価エラー率(EER)をそれぞれ求めたところ、前者は認証閾値182でEER 6%、後者は認証閾値180でEER 7%であった。これはPerformance評価の結果(本人スコアと他人スコアを比較した際の閾値およびEER)とほぼ同等である。すなわち、提案システムにおいては、同一ユーザであっても爪が異なれば、また、同一の爪であっても微細部位の位置が異なれば、爪表面の凹凸模様は他人と同程度に異なるということが確かめら

れた。ただし、今回の結果は、爪の表面の凹凸模様に基づいた攻撃に対し、項目 および が満たされたことが確認されたに過ぎない。今後は、それ以外の攻撃方法に対しても項目 や が満たされ得ることを調査していく必要がある。

(3) Unforgeability 評価：

マイクロ爪認証が忘れられる生体認証の項目 を満たしているかを、印刷物に対するなりすまし耐性、生体検知技術の併用の観点から評価した。

・印刷物に対するなりすまし耐性：

図 2 のマイクロ爪認証システムは、爪表面を約 200 倍に拡大した部位をマイクログラフで撮影し、その撮影画像を認証に利用する。図 6 は「爪表面の約 2.0×1.5 mm の領域をマイクログラフで撮影した画像」、図 7 は「市販のプリンタ (Brother HL3170-CDW) を使用して、印刷サイズが約 2.0×1.5 mm の大きさとなるように、図 6 の画像を最高解像度 (2400 dpi) で印刷し、それをマイクログラフで撮影した画像」である。市販のプリンタ程度の解像度であれば、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。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、攻撃者が印刷画像を使って本人になりすますことが困難となっている。単純な理論計算からは、200 倍の撮影の場合、攻撃者は 33,020 dpi 以上の解像度のプリンタを用いなければなりすましが不可能であると算出できる。

・生体検知技術の併用：

マイクロ爪認証に好適な生体検知の一例として、末梢血管における血流途絶や反応性充血[8]の利用が考えられる。指先を机に強く押し付けるなどの方法によって、指の腹に圧力を加えた場合には、爪の下の皮膚に流れる抹消血流の血流が途絶えて、爪床下の皮膚の色が白くなる。そして、指の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。これらの現象を利用し、撮影時に少し強く撮影部位の爪あるいは指腹を軽く圧迫して、撮影される画像の色度の変化を確認することで生体検知が可能である。実際に 3 人の被験者に対し、指腹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 8 である。目視でも圧迫解放後の画像は少し赤みが増していることが確認できる。

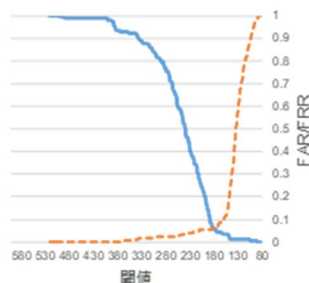


図 3：本人スコアと他人スコアの FAR/FRR

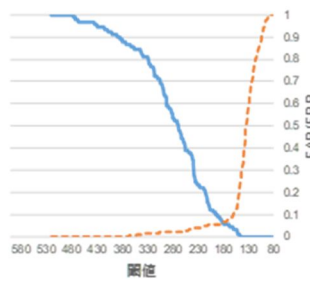


図 4：本人スコアと同人異部位間の FAR/FRR

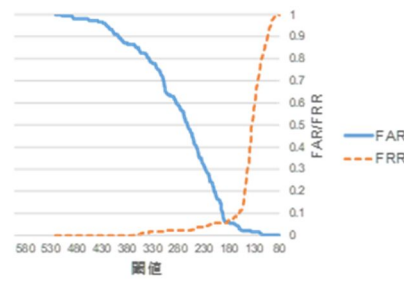


図 5：本人スコアと同爪異部位間の FAR/FRR

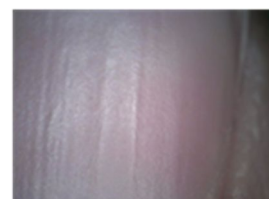
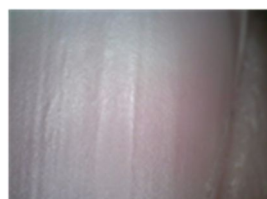
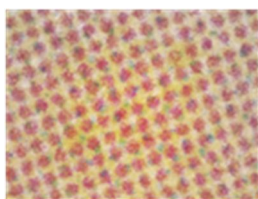


図 6：元画像 図 7：プリンタ印刷画像 図 8：圧迫中 (左) および圧迫解放後 (右) の爪表面

< 参考文献 >

- [1] Apple Face ID. <https://support.apple.com/ja-jp/HT208108>.
- [2] FIDO (Fast Identity Online) Alliance. <https://fidoalliance.org/>.
- [3] Y. Kaga, et.al. Biometric Authentication Platform for a Safe, Secure, and Convenient Society—Public Biometrics Infrastructure. Hitachi Review, vol.64, no.8, pp.472–479, 2015.
- [4] BBC news online. Politician's fingerprint 'cloned from photos' by hacker. <http://www.bbc.com/news/technology-30623611>.
- [5] 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>
- [6] C. Rathgeb, et.al. A survey on biometric cryptosystems and cancelable biometrics. Jour. Info. Sec., pp.1–25, 2011.
- [7] ISO/IEC DIS 30136. Information technology - Performance testing of biometric template protection schemes. 2017.
- [8] 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, pp. 793-799.

5. 主な発表論文等

〔雑誌論文〕 計4件（うち査読付論文 4件/うち国際共著 0件/うちオープンアクセス 4件）

1. 著者名 吉平瑞穂, 野崎真之介, 芹澤歩弥, 中原正隆, 馬場昭, 窪田歩, 大木哲史, 西垣正勝	4. 巻 63(12)
2. 論文標題 順列インデックスを用いた1対多掌紋認証のN位認証率向上に関する検討	5. 発行年 2022年
3. 雑誌名 情報処理学会論文誌	6. 最初と最後の頁 1804 ~ 1820
掲載論文のDOI (デジタルオブジェクト識別子) 10.20729/00222734	査読の有無 有
オープンアクセス オープンアクセスとしている (また、その予定である)	国際共著 -

1. 著者名 塩見祐哉, 大内結雲, 藤田真浩, 眞野勇人, 大木哲史, 西垣正勝	4. 巻 62(12)
2. 論文標題 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	5. 発行年 2021年
3. 雑誌名 情報処理学会論文誌	6. 最初と最後の頁 1996 ~ 2010
掲載論文のDOI (デジタルオブジェクト識別子) 10.20729/00214242	査読の有無 有
オープンアクセス オープンアクセスとしている (また、その予定である)	国際共著 -

1. 著者名 杉本元輝, 藤田真浩, 眞野勇人, 大木哲史, 西垣正勝	4. 巻 60(12)
2. 論文標題 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	5. 発行年 2019年
3. 雑誌名 情報処理学会論文誌	6. 最初と最後の頁 2095-2105
掲載論文のDOI (デジタルオブジェクト識別子) なし	査読の有無 有
オープンアクセス オープンアクセスとしている (また、その予定である)	国際共著 -

1. 著者名 高橋洋介, 遠藤将, 松野宏昭, 村松弘明, 大木哲史, 西垣正勝	4. 巻 60(12)
2. 論文標題 眼球-頭部協調運動における生体反射型反応に基づく生体認証方式に関する検討	5. 発行年 2019年
3. 雑誌名 情報処理学会論文誌	6. 最初と最後の頁 2106-2117
掲載論文のDOI (デジタルオブジェクト識別子) なし	査読の有無 有
オープンアクセス オープンアクセスとしている (また、その予定である)	国際共著 -

〔学会発表〕 計15件（うち招待講演 2件 / うち国際学会 5件）

1. 発表者名 Masakatsu Nishigaki
2. 発表標題 Humanics Information Security: How to go above and beyond?
3. 学会等名 BWCCA 2022 & 3PGCIC 2022 Keynote Talk I (招待講演) (国際学会)
4. 発表年 2022年

1. 発表者名 Ayumi Serizawa, Ryosuke Okudera, Yumo Ouchi, Mizuho Yoshihira, Yuya Shiomi, Naoya Nitta, Masataka Nakahara, Akira Baba, Yutaka Miyake, Tetsushi Ohki, Masakatsu Nishigaki
2. 発表標題 Improving Palmprint-Region Estimation for ID-less Palmprint Recognition
3. 学会等名 Proceedings of 2022 International Conference on Broad-Band Wireless Computing, Communication and Applications (BWCCA 2022) (国際学会)
4. 発表年 2022年

1. 発表者名 芹澤歩弥, 吉平瑞穂, 野崎真之介, 中原正隆, 馬場昭, 窪田歩, 大木哲史, 西垣正勝
2. 発表標題 骨格情報を用いた1対多掌紋認証のN位認証率向上に関する検討
3. 学会等名 情報処理学会 コンピュータセキュリティ研究会
4. 発表年 2022年

1. 発表者名 Mizuho Yoshihira, Ayumi Serizawa, Ryosuke Okudera, Yumo Ouchi, Yuya Shiomi, Naoya Nitta, Masataka Nakahara, Akira Baba, Yutaka Miyake, Tetsushi Ohki, Masakatsu Nishigaki
2. 発表標題 Improving Rank-N Identification Rate of Palmprint Identification Using Permutation-based Indexing
3. 学会等名 Proceedings of 2022 International Conference on Human-Computer Interaction (HCI 2022) (国際学会)
4. 発表年 2022年

1. 発表者名 吉平瑞穂, 芹澤歩弥, 奥寺瞭介, 大内結雲, 塩見祐哉, 新田修也, 中原正隆, 馬場昭, 三宅優, 大木哲史, 西垣正勝
2. 発表標題 1対多掌紋認証における順列インデックスを用いたN位認証率向上に関する一検討
3. 学会等名 情報処理学会 マルチメディア, 分散, 協調とモバイルシンポジウム2021
4. 発表年 2021年

1. 発表者名 Yuya Shiomi, Genki Sugimoto, Ayaka Sugimoto, Kota Uehara, Masahiro Fujita, Yuto Mano, Tetsushi Ohki, Masakatsu Nishigaki
2. 発表標題 Micro Biometric Authentication Using Fingernail Surfaces: A Study of Practical Use
3. 学会等名 Proceedings of 2020 International Conference on Advanced Information Networking and Applications (AINA 2020) (国際学会)
4. 発表年 2020年

1. 発表者名 塩見祐哉, 大内結雲, 奥寺瞭介, 藤田真浩, 眞野勇人, 大木哲史, 西垣正勝
2. 発表標題 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
3. 学会等名 コンピュータセキュリティシンポジウム2020
4. 発表年 2020年

1. 発表者名 塩見祐哉, 大内結雲, 奥寺瞭介, 藤田真浩, 眞野勇人, 大木哲史, 西垣正勝
2. 発表標題 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
3. 学会等名 バイオメトリクスと認識・認証シンポジウム2020 (ポスター発表)
4. 発表年 2020年

1. 発表者名 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
2. 発表標題 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
3. 学会等名 情報処理学会 マルチメディア, 分散, 協調とモバイルシンポジウム2019
4. 発表年 2019年

1. 発表者名 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
2. 発表標題 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
3. 学会等名 バイオメトリクスと認識・認証シンポジウム2019 (ポスター発表)
4. 発表年 2019年

1. 発表者名 奥寺瞭介, 大内結雲, 塩見祐哉, 杉本彩歌, 杉本元輝, 藤田真浩, 眞野勇人, 大木哲史, 西垣正勝
2. 発表標題 発汗を用いた生体検知手法の一検討
3. 学会等名 電子情報通信学会 バイオメトリクス研究会
4. 発表年 2020年

1. 発表者名 杉本元輝, 塩見祐哉, 藤田真浩, 眞野勇人, 大木哲史, 西垣正勝
2. 発表標題 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-
3. 学会等名 バイオメトリクスと認識・認証シンポジウム2018 (ポスター発表)
4. 発表年 2018年

1. 発表者名 杉本元輝, 藤田真浩, 眞野勇人, 大木哲史, 西垣正勝
2. 発表標題 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
3. 学会等名 情報処理学会 セキュリティ心理学とトラスト研究会
4. 発表年 2018年

1. 発表者名 西垣正勝
2. 発表標題 マイクロ生体認証：微小生体特徴を利用したユーザ認証
3. 学会等名 第149回微小光学研究会（招待講演）
4. 発表年 2018年

1. 発表者名 Genki Sugimoto, Yuto Mano, Tetsushi Ohki, Masakatsu Nishigaki
2. 発表標題 Disposable Biometric Authentication Micro Biometric Authentication Using Fingernail Textures
3. 学会等名 Proceedings of 2018 International Conference on Biomedical Imaging, Signal Processing (ICBSP 2018) (国際学会)
4. 発表年 2018年

〔図書〕 計0件

〔産業財産権〕

〔その他〕

-

6. 研究組織

	氏名 (ローマ字氏名) (研究者番号)	所属研究機関・部局・職 (機関番号)	備考
研究 分担者	大木 哲史 (TETSUSI Ohki) (80537407)	静岡大学・情報学部・准教授 (13801)	

6. 研究組織（つづき）

	氏名 (ローマ字氏名) (研究者番号)	所属研究機関・部局・職 (機関番号)	備考
研究 分 担 者	大塚 玲 (OTSUKA Akira) (50415650)	情報セキュリティ大学院大学・その他の研究科・教授 (32721)	

7. 科研費を使用して開催した国際研究集会

〔国際研究集会〕 計0件

8. 本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関