

科学研究費助成事業 研究成果報告書

令和 5 年 6 月 7 日現在

機関番号：34315

研究種目：基盤研究(B)（一般）

研究期間：2020～2022

課題番号：20H04189

研究課題名（和文）同軸型アダプティブ生体センサと機械学習による高度生体電磁偽装物検出技術の創生

研究課題名（英文）A Novel Electromagnetic Liveness Detection System against High-Level Fingerprint Spoof Attacks using Machine Learning for Fingerprint Authentication Systems

研究代表者

前田 忠彦（Maeda, Tadahiko）

立命館大学・情報理工学部・教授

研究者番号：40351324

交付決定額（研究期間全体）：（直接経費） 13,600,000円

研究成果の概要（和文）：指紋認証や静脈認証装置の脆弱性を排除し、生体偽装攻撃に対抗するためには、従来の生体認証装置が認証処理に利用する生体情報源とは原理的に異なる情報源に基づく高精度生体検知技術への研究着手が急務である。照合対象が非生体の偽装物を含むかを判別する方式として、「電磁応答特性に基づく生体検知技術」が提案されている。この生体検知技術を発展させ、「極めて高度な偽装物」が将来出現した場合にも、生体認証を防衛する技術を構築することは重要である。本報告は、人体の電磁応答という攻撃側が遠隔的に取得・模擬することが原理的に困難である生体情報に基づく、新しい生体検知技術の高度化要素技術に関する研究成果を記述している。

研究成果の学術的意義や社会的意義

人体指紋の撮像画像を判定基準として使用する指紋認証方式は、多要素認証を構成する重要要素技術の一つであり、情報社会のセキュリティを支える技術として期待されている。一方、日常生活においては素手で活動することが一般的であり、外部に露出している人体指紋情報を判定情報源とする判定方式は、本人が意識しない状況下で指紋撮像や残留指紋から指紋が複製される本質的な脆弱性が存在している。本研究では外部から遠隔では取得することが出来ない生体電磁応答特性を指紋認証に適用することに注目し、独自の生体検知センサ構造に機械学習アルゴリズムを組み合わせることで、高度偽装物に対抗するための指紋認証高度化要素技術を検討した。

研究成果の概要（英文）：In recent years, spoofing attacks against fingerprint authentication technologies caused by fake fingerprints have been reported and raised severe social security issues. This report describes systematic countermeasures for fingerprint authentication systems. A multi-ring liveness detection sensor was proposed to improve the detection accuracy, and measurements were carried out for human and fake fingers to evaluate the effectiveness of the proposed sensor. Also, a modified C-type sensor and a coplanar-type sensor were designed and fabricated for the measurements. Besides, we have proposed a novel two-step judgment method to improve detection accuracy and assessed the accuracy to demonstrate the effectiveness of the proposed algorithm. We have also developed and evaluated unique person-specific templates generated with the sensor's scattering responses for the frequency range from 9.5 GHz through 14 GHz using a neural network to enhance the overall detection accuracy for the system.

研究分野：ワイヤレスシステム

キーワード：生体認証 リックス 指紋認証 生体検知 CSRR 機械学習 ニューラルネットワーク Autoencoder バイオメトリックス

科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属します。

様式 C - 19、F - 19 - 1、Z - 19 (共通)

1. 研究開始当初の背景

指紋認証の高度化の内外の研究動向としては、撮像した画像の分析に基づく研究があり、画像解析により偽装物を検出する手法である。また、これに関連して、近年のデジタルカメラの画像解像度が進歩し、スナップ写真の指先の画像から指紋を複製する偽装に関するテレビ報道がなされていた。これらの研究は人体指紋の指紋情報から判定する技法であるため、外部に露出している指の指紋を盗み取られる場合に根本的脆弱性を持っている。これに対して本研究提案は外部から遠隔的には取得することが困難である人体電磁応答を生体検知に適用する手法である。

2. 研究の目的

既存の指紋・静脈認証技術の脆弱性が顕在化しており指紋偽装防止技術高度化の研究は重要である。特に、入国管理等の重要施設では個人認証の確実性を高レベルで担保・確保することが必要となるため、極めて高いレベルの「なりすまし」攻撃用偽装物に対抗できる卓越した偽装物判定技術の研究・開発が極めて重要である。本研究は、一般生活における認証偽装攻撃に比べて、高いレベルの生体偽装技術を用いた「高度なりすまし偽装物攻撃」に対抗するための「高度偽装物判定技術」を研究・開発し社会に提供することで、情報化社会の安定性と保安性を確保することを目的とする。

3. 研究の方法

生体偽装物分析と電磁界解析による特性分析から「同軸型センサ構造を最適化」する。具体的には、複数の平面多層構造を電磁界シミュレーションすることで基礎資料を蓄積し、センサ実現に適する基本構造を探索する。特に多重同軸型生体検知センサのリング数の増加とストリップ線路側の結合構造に注目した構造分析を行う。判定アルゴリズムに関しては、従来の類似度と平均差を用いる2次元平面での判定方法に加えて、機械学習を活用した特徴量抽出の高度化を進め、さらにニューラルネットワークや深層学習を活用する生体検知アルゴリズムの開発を進める。

4. 研究成果

生体検知センサ[1]の検知精度向上と電磁応答特性取得のための周波数帯域を検討し、先行研究で提案された生体検知センサ[2]の構造変更を行い、シミュレーションと生体検知実験による提案構造評価を行った。特に、先行研究で提案された多重同軸型センサにおいて、被検知物の載置を行う CSRR (Complementary Split-Ring Resonator) 構造の検討と、伝送線路部構造の周波数特性に注目する検討を進めた。

さらに伝送線路部の高周波化を進めることを目的として、コプレーナ構造を採用したセンサの電磁応答特性把握のために必要となる基礎的検討に着手した。さらに、CSRR 電磁生体検知センサ用偽装指判定アルゴリズムの高度化を目的とし、機械学習及び深層学習を併用した判定手法の検討・提案を行った。

(1) リング数を増加した CSRR 型生体検知センサ[3]

生体検知センサの検知精度向上と電磁応答特性取得のための周波数帯域検討を目的に、先行研究で提案された生体検知センサの構造変更を行い、シミュレーションと生体検知実験による提案構造評価を行った。特に、先行研究で提案された多重同軸型センサにおいて、被検知物の載置を行う CSRR 構造のリング数検討と、伝送線路部構造の周波数特性に注目する検討を進めた。図1はリング数を従来の4個から6個に増加させた生体検知センサの構造図[3]である。当該センサは人体指と CSRR 構造の接触面積が従来センサよりも2倍程度となる構造となっており、人体指の電磁応答範囲が増加したセンサ構造となっている。

従来センサ[2]よりも CSRR 構造のリング数を4個から6個に増加することで厚さ0.1 mm のシリコーンゴムに対しては、人体指の最大値と最小値の差分を1とした場合、類似度[1]において、従来センサは0.6倍、提案センサでは2.7倍となった。平均差[1]においては、従来センサは0.6倍、提案センサは0.9倍となり、判別平面上の相対距離[3]により検知精度の向上が確認された。また、提案センサは周波数範囲を1~8 GHz とすることで類似度においては14.1倍、平均差においては1.0倍となり、検知精度の向上を図れることを確認した。

(2) ストリップライン構造を変更した C 型 CSRR 生体検知センサ[4]

センサの高度化に関わる研究では従来センサのストリップライン構造を C 型の構造に変更したセンサを試作し、提案構造の検出精度評価を進めた。多重同軸型センサの CSRR 構造のリングに沿った C 型スタブをマイクロストリップラインに適用した構造[4]を提案し、電磁界シミュレーションによる構造解析を進めることで、当該構造の設計のための基礎的データを取得した。図2に提案センサの構造を示す。検出精度評価のための、偽装物としては厚さ0.1 mm のシリコーンゴムを用いて、周波数帯域は1 GHz から16 GHz の帯域での評価を進めた。提案センサは従来センサに対して類似度は3.6倍、平均さは12.6倍となり、提案センサの判別平面上における人体指と偽装指の分布距離が増加する評価結果が得られた。

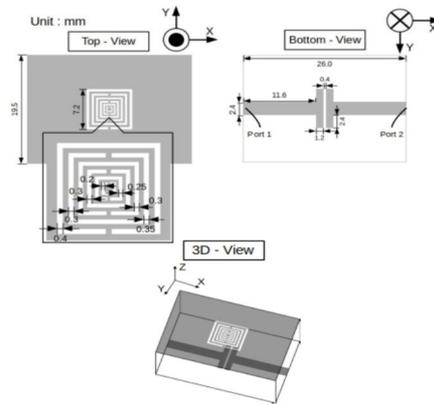


図 1 多重同軸型生体検知センサ構造[3]

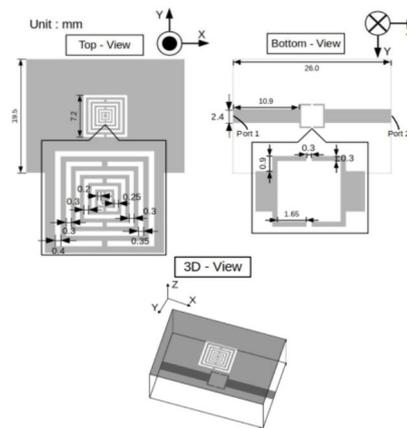


図 2 ストリップライン構造を変更した C 型生体検知センサ[4]

(3) コプレーナ構造を採用した生体検知センサ[5]

伝送線路部の高周波化を進めることを目的として、伝送線路の構造としてコプレーナ構造を持つセンサについても検討し、当該センサの検知特性を実験的に評価した。図 3 にコプレーナ構造を採用した生体検知センサの構造を示す[5]。厚さ 0.1 mm のシリコンゴムに対して相対距離[3]を用いた検知精度評価を行った結果、人体指の最大値と最小値の差分を 1 とした場合、平均差において従来センサでは 0.8、提案センサでは 5.1 となった。また、類似度において従来センサでは 12.2、提案センサは 16.2 となる評価結果が得られた。

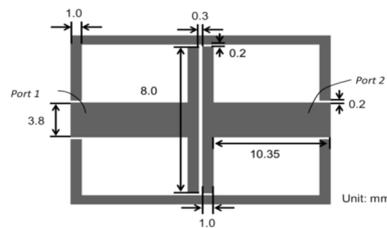


図 3 コプレーナ構造を採用した生体検知センサ[5]

(4) LOF - One Class SVM 二段階判定法[6]

CSRR 電磁生体検知センサ用偽装指判定アルゴリズムの高度化を目的とし、機械学習及び深層学習を併用した判定手法の検討・提案を行った。生体検知手法において、LOF (Local Outlier Factor) を用いた判定手法が提案されていたが、一定の誤検知が発生しており、改善が望まれる。まず、LOF と OCSVM (One Class Support Vector Machine) のパラメータ調整を行い、各判定手法において FRR (False Rejection Rate) 及び FAR (False Acceptance Rate) それぞれの判定信頼性向上について検討を行った。

これらに加えて、FRR 及び FAR それぞれに優れた 2 つのアルゴリズムを組み合わせ、CSRR 電磁生体検知センサに適用するための二段階判定手法を提案し[6]、複数の偽装物による検知精度評価を行った。二段階判定手法の処理の流れを図 4 に示す。皮膚ファントム (0.3 mm 厚) と

シリコン（0.1 mm 厚）を用いた二段階判定手法の検知精度評価を実施することで、二段階判定手法の有効性を評価し、複数の偽装物に対する判定精度を検証した。

学習用データセットから構築した三つの学習モデル（Model 1, Model 2, Model 3）、テスト用に皮膚ファントム（0.3 mm 厚）データセット及びシリコン（0.1mm 厚）データセットを用いて、本手法による偽装指検知精度評価実験を行った。検知精度評価の結果、皮膚ファントム偽装指においては、提案手法により FRR は Model 1 のみ 1.5 % だが、FAR は全モデルで 0 % となり、誤検知が低減し検知精度が改善された。

また、シリコン偽装指においては、従来手法より FRR が Model 1, 3 においてそれぞれ 4.0 % 悪化した。一方で、FAR が全てのモデルにおいて 4.0 % から最大 24.0 % 改善した。シリコン偽装指において、従来の単一の機械学習による判定手法では FRR もしくは FAR どちらかが悪化し、安定的な評価に課題があったが、提案手法では FRR と FAR をバランス良く抑えられる判定特性を示した。

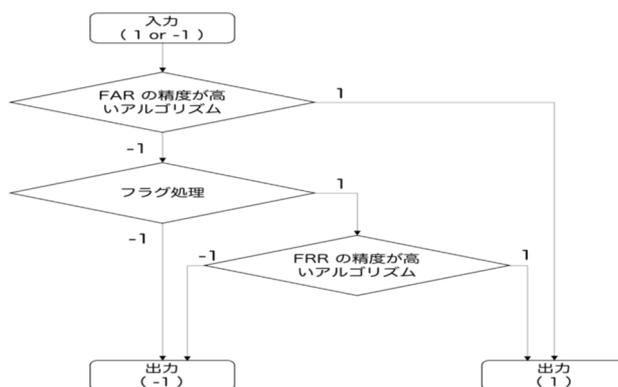


図 4 二段階判定手法の処理の流れ[6]

(5) Autoencoder 及び One Class SVM を用いた判定アルゴリズム[7]

Autoencoder は、入力層と出力層に同じデータを用いて教師なし学習を行う。具体的には、入力データを圧縮し、復元された出力データと入力データの差異（復元誤差）を最小化することを目的に学習する。人体指の|S21|を 1120 データ学習させた Autoencoder モデルに、人体指、偽装指の|S21|を入力する検証を行った。偽装指には皮膚ファントム（0.3 mm 厚）、及びシリコン（0.1 mm 厚）の 2 種類の偽装物を用いた。なお、今回使用した Autoencoder のネットワーク構造は入力層、中間層、出力層がそれぞれ 1 層ずつであり、損失関数には平均 2 乗誤差、最適化手法には Adam (Adaptive moment estimation) を適用した。また、学習時のエポック数は 1000 エポックとした。

図 5 に人体指、皮膚ファントム偽装指、シリコン偽装指の|S21|をテストデータセットとして各 65 データずつ入力した際の Autoencoder の復元誤差を示す。図 5 より、偽装指の|S21|が入力されると復元精度が低下し、人体指の|S21|を入力した場合よりも復元誤差が大きくなる事が確認できる。Autoencoder により復元された人体指データは、復元前の人体指データとの差異が少ないのに対して、復元された偽装指データは、不自然な復元となっているため復元前の人体指データとの差異が拡大する。

これらを踏まえると、あらかじめ復元前の人体指データのみを学習させた OCSVM で各復元データを判別することで、偽装指検知精度の向上が期待できるため、これを応用した新しい判定手法を提案した[7]。この手法は従来の機械学習による判定手法と異なり、特徴量を手動で選定が不要となる利点がある。検知精度評価の結果、皮膚ファントム及びシリコンの各偽装指の誤検知は発生せず、提案手法により 4.6% の誤検知改善が確認された。

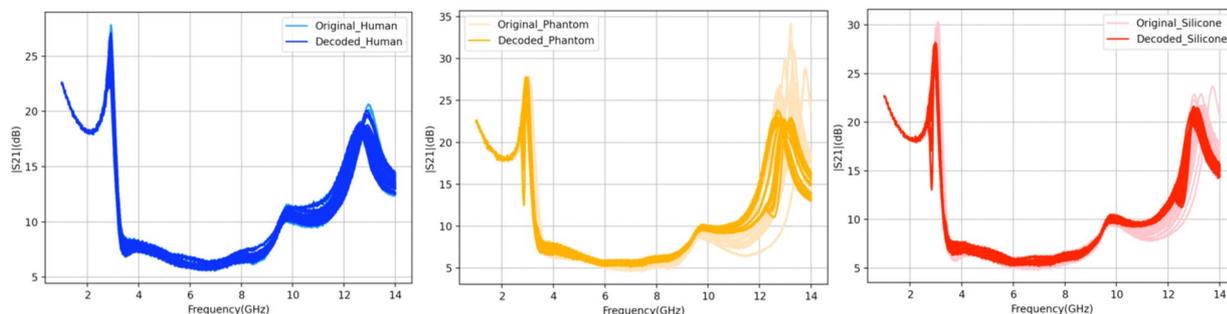


図 5 復元誤差 a)人体指

b)ファントム偽装指

c)シリコン偽装[7]

(6)ニューラルネットワークを利用した生体検知用テンプレート生成法[8]

テンプレートの選択による検知性変動を評価することを目的として、人体指と偽装指の電磁応答特性差が顕著に表れる周波数帯域である 9.5 - 14 GHz に着目し、生体検知特性を評価した。まず、本人指テンプレート手法に対する検知精度を確認し、次に、ニューラルネットワークを用いて被験者特有の電磁応答特性を数理モデル化する方向で研究を進めた。さらに、このニューラルネットワークから出力させた予測値をテンプレートとして用いる偽装指検知手法を提案し[8]、実験的に検知精度評価を行うことで、提案手法の有効性を検証した。

提案手法では、事前に被験者本人の $|S_{21}|$ と三つの電磁応答特性(S_{21} , $|S_{11}|$, S_{11}) を学習させた数理モデルを作成しておく。生体検知を行う際には、測定データの三つの電磁応答特性を前述の学習済み数理モデルに入力することで、 $|S_{21}|$ の予測値を取得する。この予測値をテンプレートとして $|S_{21}|$ の実測値と比較することで生体検知を行う。提案したテンプレート生成法を図 6 に示す。

テンプレート生成に用いる数理モデルにはニューラルネットワークを採用し、被験者 1 名に対する 10 個の測定データから説明変数を S_{21} , $|S_{11}|$, S_{11} とし、目的変数を $|S_{21}|$ としたニューラルネットワークを学習させた。なお、ニューラルネットワークの学習には MathWorks 社の Deep Learning Toolbox を使用し、長短期記憶ニューラルネットワークの学習を行い、数理モデルの生成を行った。ネットワークアーキテクチャは隠れユニット 200 個、その後続くサイズ 450 の全結合層とドロップアウトの確率が 0.5 のドロップアウト層を定義した。学習条件はサイズ 10 のミニバッチで 60 エポックを定義し、学習率を 0.01 に指定した。周波数 9.5 ~ 14 GHz のテンプレートをを用いた場合の検知精度を検証した結果、提案手法は全モデルにおいて FRR, FAR のいずれも検知精度が向上する評価結果が得られた。

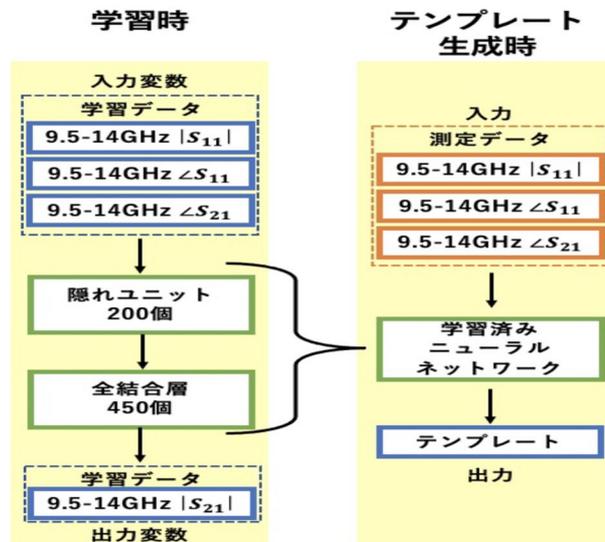


図 6 提案テンプレート生成法[8]

- [1] 青木洗一, 前田忠彦, “CSRR-BPF 生体検知センサの小型化と指紋認証方式への適用,” 電子情報通信学会論文誌 B, Vol. J98-B (9), pp. 979-990, Sep. 2015.
- [2] 飯島主匡, 大矢佑磨, 前田忠彦, “CSRR を使用した指紋認証用生体検知センサの小型化,” 電子情報通信学会論文誌 B, Vol. J103-B (11), pp. 588-590, Sep. 2017.
- [3] 岸俊宏, 前田忠彦, “リング数を増加した CSRR による生体検知センサの改善,” 電子情報通信学会論文誌 B, Vol. J103-B (11), pp. 588-590, Sep. 2020.
- [4] 松浦悠之亮, 前田忠彦, “ストリップライン構造を変更した C 型 CSRR 生体検知センサ,” 電子情報通信学会論文誌 B, Vol. J105-B (7), pp. 512-514, Sep. 2022.
- [5] 鶴友宏, 前田忠彦, “コプレーナ構造を採用した生体検知センサの提案,” 電子情報通信学会論文誌 B, Vol. J105-B (11), pp. 908-910, Sep. 2022.
- [6] 水山桂乃, 前田忠彦, “CSRR 電磁生体検知センサによる高度偽装物の検知精度向上を目的とした LOF-One Class SVM 二段階判定法の提案,” 電子情報通信学会論文誌 B, Vol. J104-B (11), pp. 907-917, Sep. 2021.
- [7] 水山桂乃, 前田忠彦, “Autoencoder 及び One-Class SVM を用いた CSRR 電磁生体検知センサ用偽装指判定手法の提案,” 電子情報通信学会論文誌 B, Vol. J105-B (11), pp. 911-913, Sep. 2022.
- [8] 山本連, 前田忠彦, “ニューラルネットワークを利用した生体検知用テンプレート生成法の提案,” 電子情報通信学会論文誌 B, Vol. J105-B (11), pp. 914-917, Sep. 2022.

5. 主な発表論文等

〔雑誌論文〕 計6件（うち査読付論文 6件/うち国際共著 0件/うちオープンアクセス 0件）

| | |
|--|-------------------------|
| 1. 著者名 山本 蓮、前田 忠彦 | 4. 巻 J105-B |
| 2. 論文標題 ニューラルネットワークを利用した生体検知用テンプレート生成法の提案 | 5. 発行年 2022年 |
| 3. 雑誌名 電子情報通信学会論文誌B 通信 | 6. 最初と最後の頁 914 ~ 917 |
| 掲載論文のDOI (デジタルオブジェクト識別子) 10.14923/transcomj.2022APL0007 | 査読の有無 有 |
| オープンアクセス オープンアクセスではない、又はオープンアクセスが困難 | 国際共著 - |

| | |
|---|-------------------------|
| 1. 著者名 水山 桂乃、前田 忠彦 | 4. 巻 J105-B |
| 2. 論文標題 Autoencoder及びOne-Class SVMを用いたCSRR電磁生体検知センサ用偽装指判定手法の提案 | 5. 発行年 2022年 |
| 3. 雑誌名 電子情報通信学会論文誌B 通信 | 6. 最初と最後の頁 911 ~ 913 |
| 掲載論文のDOI (デジタルオブジェクト識別子) 10.14923/transcomj.2022APL0002 | 査読の有無 有 |
| オープンアクセス オープンアクセスではない、又はオープンアクセスが困難 | 国際共著 - |

| | |
|--|-------------------------|
| 1. 著者名 鶴 友宏、前田 忠彦 | 4. 巻 J105-B |
| 2. 論文標題 コプレーナ構造を採用した生体検知センサの提案 | 5. 発行年 2022年 |
| 3. 雑誌名 電子情報通信学会論文誌B 通信 | 6. 最初と最後の頁 908 ~ 910 |
| 掲載論文のDOI (デジタルオブジェクト識別子) 10.14923/transcomj.2022APL0004 | 査読の有無 有 |
| オープンアクセス オープンアクセスではない、又はオープンアクセスが困難 | 国際共著 - |

| | |
|--|-------------------------|
| 1. 著者名 松浦 悠之亮、前田 忠彦 | 4. 巻 J105-B |
| 2. 論文標題 ストリップライン構造を変更したC型CSRR生体検知センサ | 5. 発行年 2022年 |
| 3. 雑誌名 電子情報通信学会論文誌B 通信 | 6. 最初と最後の頁 512 ~ 514 |
| 掲載論文のDOI (デジタルオブジェクト識別子) 10.14923/transcomj.2021BLL0013 | 査読の有無 有 |
| オープンアクセス オープンアクセスではない、又はオープンアクセスが困難 | 国際共著 - |

| | |
|--|-----------------------|
| 1. 著者名 水山 桂乃 前田 忠彦 | 4. 巻 Vol. J104-B |
| 2. 論文標題 CSRR電磁生体検知センサによる高度偽装物の検知精度向上を目的としたLOF - One Class SVM二段階判定手法の提案 | 5. 発行年 2021年 |
| 3. 雑誌名 電子情報通信学会論文誌 B | 6. 最初と最後の頁 907-917 |
| 掲載論文のDOI (デジタルオブジェクト識別子) 10.14923/transcomj.2021APP0007 | 査読の有無 有 |
| オープンアクセス オープンアクセスではない、又はオープンアクセスが困難 | 国際共著 - |

| | |
|--|----------------------------|
| 1. 著者名 岸 俊宏 前田 忠彦 | 4. 巻 Vol. J103-B No. 11 |
| 2. 論文標題 リング数を増加したCSRRによる生体検知センサの改善 | 5. 発行年 2020年 |
| 3. 雑誌名 電子情報通信学会論文誌 B | 6. 最初と最後の頁 588-590 |
| 掲載論文のDOI (デジタルオブジェクト識別子) 10.14923/transcomj.2020APL0002 | 査読の有無 有 |
| オープンアクセス オープンアクセスではない、又はオープンアクセスが困難 | 国際共著 - |

[学会発表] 計9件(うち招待講演 0件/うち国際学会 0件)

| |
|---------------------------------------|
| 1. 発表者名 松浦 悠之亮 前田 忠彦 |
| 2. 発表標題 ストリップライン構造を変更したCSRR生体検知センサ |
| 3. 学会等名 電子情報通信学会ソサイエティ大会 |
| 4. 発表年 2021年 |

| |
|--|
| 1. 発表者名 水山 桂乃 前田 忠彦 |
| 2. 発表標題 LOFとOne - Class SVMを用いた複合判定手法による偽装指検知精度評価 |
| 3. 学会等名 電子情報通信学会ソサイエティ大会 |
| 4. 発表年 2021年 |

| |
|--------------------------------|
| 1. 発表者名 松浦 悠之亮 前田 忠彦 |
| 2. 発表標題 小型化CSRR生体検知センサの電気特性 |
| 3. 学会等名 電子情報通信学会総合大会 |
| 4. 発表年 2021年 |

| |
|--|
| 1. 発表者名 大友 健 小林 和貴 前田 忠彦 |
| 2. 発表標題 CSRR構造を用いた生体検知センサによる高度偽装物判別のための特徴量の検討 |
| 3. 学会等名 電子情報通信学会総合大会 |
| 4. 発表年 2021年 |

| |
|---|
| 1. 発表者名 小邨 綾果 笠間 直樹 前田 忠彦 |
| 2. 発表標題 Elliptic Envelope 法を用いた生体検知手法の検討 |
| 3. 学会等名 電子情報通信学会総合大会 |
| 4. 発表年 2021年 |

| |
|--|
| 1. 発表者名 寺西 ひろ葉 小林 和貴 前田 忠彦 |
| 2. 発表標題 高度偽装物検知を目的とした機械学習判定のための位相特徴量の検討 |
| 3. 学会等名 電子情報通信学会総合大会 |
| 4. 発表年 2021年 |

| |
|--------------------------------|
| 1. 発表者名 鶴 友宏 前田 忠彦 |
| 2. 発表標題 指紋認証用生体検知センサの小型化の検討 |
| 3. 学会等名 電子情報通信学会総合大会 |
| 4. 発表年 2021年 |

| |
|-----------------------------------|
| 1. 発表者名 松浦 悠之亮 前田 忠彦 |
| 2. 発表標題 テンプレートの選択が生体検知精度に与える影響 |
| 3. 学会等名 電子情報通信学会ソサイエティ大会 |
| 4. 発表年 2020年 |

| |
|--|
| 1. 発表者名 水山 桂乃 前田 忠彦 |
| 2. 発表標題 One Class SVM を用いた偽装指検知精度評価 |
| 3. 学会等名 電子情報通信学会ソサイエティ大会 |
| 4. 発表年 2020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 |
|---------------------------|-----------------------|----|
|---------------------------|-----------------------|----|

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 |
|---------|---------|
|---------|---------|