

GPSとWi-Fiデータでの多要素認証におけるニューラルネットを用いたスコアフュージョン手法

松岡 勝也¹ IRVAN MHD¹ 小林 良輔¹ 山口 利恵¹

概要: 近年, 認証での脆弱性の問題などにより個人認証への関心や重要性が高まっている. 高い機密性が求められる場面では, 複数の認証要素を組み合わせる多要素認証が一般的に用いられる. この多要素認証には, 各要素からの認証スコアなどを組み合わせるフュージョン方式がある. 本研究ではこのフュージョン方式のスコアレベルに着目している. 従来のスコアレベルでのフュージョン手法ではそれぞれの要素での重み付けが固定されている. このため, 行動認証のような各ユーザの性質に依存し認証精度がユーザ間で大きく異なるような場合には適していない. そこで, 本研究ではこのようなユーザ間で傾向が異なる場合での認証精度の向上を目的とし, ニューラルネットを用いたユーザ毎に最適な重み付けのスコアフュージョン手法を提案する. 本提案手法では, ユーザ毎に独立な二値分類のモデルを構築する. そして, GPSとWi-Fiの実データを用いた評価から, 従来手法と比較して本提案手法ではTAR(True Acceptance Rate)が向上することを確認した. このため, TARを優先する場面では本提案手法は有用であると言える.

Score Fusion Method by Neural Network in Multi-Factor Authentication with GPS and Wi-Fi Data

KATSUYA MATSUOKA¹ MHD IRVAN¹ RYOSUKE KOBAYASHI¹ RIE SHIGETOMI YAMAGUCHI¹

1. 序論

昨今, サイバーセキュリティへの関心は高まっており, その中でもパスワードなど個人を認証する技術について注目が集まっている. これは, 人々がインターネットを通して様々なサービスを利用し, オンラインサービスの際には個人認証が必要とされているためである. 個人認証の際に利用する要素には知識認証, 所有認証, 生体認証や行動認証などがある. これらの要素のうち単一の要素のみを利用した認証方式ではセキュリティ的に不十分である場合もある. このため, オンライン決済など高い機密性が要求される様々な場面では, これらの要素を複数個組み合わせた多要素認証が用いられる. 多要素認証は複数の要素を用いることで単一の場合と比べて強力に安全な認証を実現することができる [1]. また, 多要素認証には多段階方式とフュージョン方式が存在する [1]. 多段階方式では, それぞれの

要素において本人であるかの判定が行われる. そして, 本人であると判定されると, 次の要素へと進み, 全ての要素で本人と判定された場合に認証成功となる. 一方, フュージョン方式の場合, それぞれの要素で得られるセンサデータ, 特徴量や認証スコアなどを組み合わせることによって最終的な認証結果を求める. フュージョン方式ではそれぞれの要素で本人であるかの二値で判定されるのではなく, 各要素からの値をフュージョンした後に判定を行うため柔軟な認証方式であると言える. 多要素認証では一般的にどの認証要素で高い認証精度が出るかという傾向があるためフュージョン方式での各要素の重み付けはその傾向に基づき固定されている [2], [3], [4], [5], [6]. しかし, 行動認証などはユーザ毎の特性に大きく左右され, どの認証要素での精度が高いかという傾向がユーザ間で大きく異なる場合がある. このように, ユーザ間で傾向が異なる場合に適したフュージョン方式, すなわち動的な重み付けによるフュージョン手法は少ない. また, 行動認証では例外的な行動など普段の生活習慣とは関係のないノイズが入る場合がある.

¹ 東京大学大学院情報理工学系研究科
Graduate School of Information Science and Technology,
The University of Tokyo

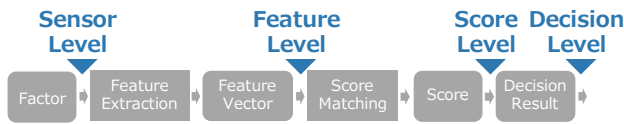


図 1 Processing flow and fusion levels.

このため、生データではそれらのノイズの影響を受けて精度が悪くなる可能性がある。そこで、ノイズの影響を抑えるために各要素について生データから変換したスコア [7] を用いてフュージョンを行う手法を提案する。

本研究ではユーザ全体としての要素別の傾向はなく、ユーザ毎に異なった要素別の傾向がある場合での多要素認証の精度向上を目的とする。そこで、要素毎の重み付けを固定したフュージョン手法ではなく、ニューラルネットを用いてユーザ毎に動的な重み付けを行うフュージョン手法を提案する。本提案手法では、各ユーザについてそのユーザ本人と他人のデータでの学習により、ユーザ毎に独立なモデルを構築する。そして、このモデルを用いた二値分類により本人であるか他人であるかを判定する。また、57,000 人規模の実証実験 [8] により集められた GPS と Wi-Fi の実データから無作為に抽出した 30 人分のデータを用いて本提案手法を評価する。

2. 関連研究

本章では、本研究で着目している多要素認証でのフュージョンについて説明し、その従来手法と課題点を紹介する。

2.1 フュージョン手法

フュージョン手法では、多要素認証での各要素から得られたセンサデータ、特徴量、認証スコアなどを組み合わせた値によって最終的な判定を行う [9]。フュージョン手法はどの段階でフュージョンを行うかのレベルによって分類することができる。図 1 に示す通り、センサレベル、特徴レベル、スコアレベル、決定レベルの 4 つのレベルがある [3]。

センサレベルフュージョン (Sensor level fusion)

センサレベルフュージョンはセンサからの生データを融合する方式である [10]。センサレベルフュージョンは、複数の互換性のあるセンサから取得されたデータか、単一のセンサから取得された複数のデータに対してのみ行える [11]。また、センサレベルフュージョンは異なるセンサからの情報を結合するためセンサの調整やデータの登録などの前処理が必要である。

特徴レベルフュージョン (Feature level fusion)

特徴レベルフュージョンは異なるセンサから取得した特徴量を融合する方式である。特徴を組み合わせると次元の呪いが発生するため、特徴変換または特徴選択のいずれかを適用して融合された特徴量の次元を減ら

す必要もある [11]。

スコアレベルフュージョン (Score level fusion)

スコアレベルフュージョンでは異なるマッチスコアが融合される。このマッチスコアとは、入力とテンプレートの特徴ベクトルの類似性の尺度を表す値である [11]。ただし、マッチスコアの範囲が異なる場合にはマッチスコアを正規化する必要がある [10]。

決定レベルフュージョン (Decision level fusion)

決定レベルフュージョンはそれぞれの要素での比較結果を融合する方式である。このレベルで使用されるアプローチの多くには AND, OR ルール、多数決、加重多数決、ベイジアン決定などが利用される [10]。

上述した通り、フュージョン手法にはいくつかのレベルがある。本研究では、その中でスコアレベルフュージョンに着目している。以下、スコアレベルフュージョンをスコアフュージョンと呼ぶ。多要素認証では一般的にどの要素での認証精度が高いのかという傾向があるため、スコアフュージョンにおいてその傾向に基づいた固定の重み付けを定義するケースが多い [2], [3], [4], [5], [6]。

2.2 平均値によるスコアフュージョン

J. Aravinth らの研究では、3 つの分類器 (ABC-NN, ファジールール分類, 単純ベイズ分類) を使用したスコアフュージョンの手法が提案されている [12]。この手法では分類器のハイブリッド化によって性能が改善されている。各分類器の出力と目標値との相関を求め、それらの平均値を最終的なスコアとする。すなわち、各分類器からの出力の重み付けは等しく、平均値をとるスコアフュージョンであると言える。本提案手法との差異は、それぞれの要素での重みが等しいという点である。

2.3 固定の重み付けによるスコアフュージョン

Devu Manikantan Shila らの研究では、ユーザの歩行パターンや頻繁に訪れる場所や物理的距離などの行動要素を用いた認証方式が提案されている [2]。この手法ではそれぞれの要素のスコアをフュージョンする際に、固定の重み付けによるスコアフュージョンが用いられている。近接センサによるスコアの重み w_1 、歩行パターンによるスコアの重み x_2 、位置によるスコアの重み w_3 とすると、

$$w_1 + w_2 + w_3 = 1 \quad (1)$$

$$w_2 > w_1 > w_3 \quad (2)$$

となるように固定の重みを定義している。これはスコアの精度が高い要素ほど重み付けを大きくし、重みを固定したスコアフュージョンである。本提案手法との差異は、ユーザ間でそれぞれの要素の重みが等しいという点である。

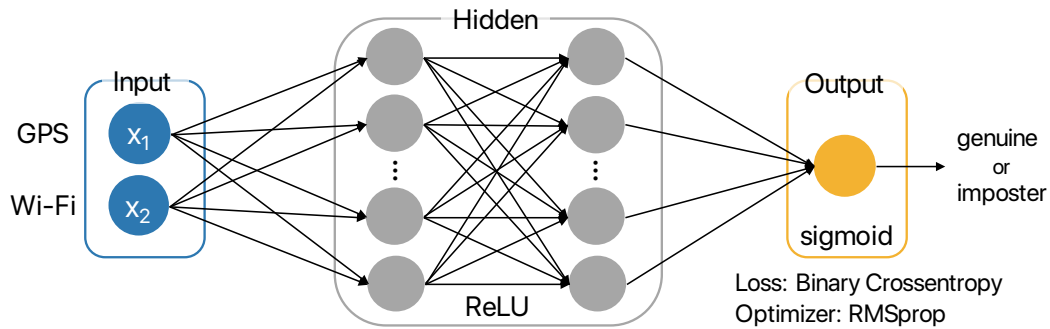


図 2 Binary classification network used in our proposed method.

2.4 従来手法の課題点

上述したスコアフュージョン手法はいずれも重み付けを固定した方式である。要素毎に精度の高さの傾向がある場合にはこのような固定の重み付けによるスコアフュージョンは適している。一般的に多要素の生体認証においてどの要素での認証精度が高いのかという傾向が事前に分かっているため、これら従来手法である重み付けを固定したスコアフュージョンが適している。一方で、ユーザ毎にその傾向が異なる場合については固定の重み付けでは高い精度を得られない。このため、ユーザ毎に異なった要素別の傾向があるデータについてスコアフュージョンする際には動的にユーザ毎に適切な重み付けを行う手法が必要となる。この具体例として GPS と Wi-Fi 情報を用いた認証がある。例えば、あるユーザが会社勤めだった場合、自宅か職場にいることが多いため位置情報による認証精度が高くなる。このため、このユーザについては GPS に基づく結果に優先度を置くべきである。一方で、別のユーザがフリーランスとして働いていた場合、様々な場所で仕事をしているため位置情報による認証精度はそれほど高くない。しかし、常にポケット Wi-Fi を持ち歩いているため Wi-Fi 情報による認証精度は高いといった場合が考えられる。このユーザについては位置情報よりも Wi-Fi 情報を優先すべきである。このように、行動認証などではユーザの生活スタイルに応じて傾向が大きく異なる。そこで、本研究ではこのようなユーザ毎にどの要素での認証精度が高いのかという傾向が異なる場合での多要素認証の精度向上を目的としている。

3. 提案手法

本研究では、ニューラルネットワークを用いてユーザ毎に動的な重み付けを行い認証精度を高めるスコアフュージョン手法を提案する。ニューラルネットワークは動的な重み付けに適しており信頼性の高い精度が得られるが、スコアフュージョンにはまだ適用されていない。そこで、本研究ではニューラルネットワークを用いてユーザ毎に独立な二値分類のモデルを構築する。このモデルはユーザ毎に構築されるため、重みはユーザ毎に個別に調整される。各ユーザのモ

デルは、そのユーザ本人のデータと他人のデータから学習して構築される。ユーザ数が増えればモデル数は増えるが、各モデルを構築するための学習データ数は変わらない。また、認証の際には対応するユーザのモデルにスコアデータを入力する。

本提案手法では、図 2 に示すようなネットワークを構築した。各要素の認証スコアが入力され、本人であるかどうかの二値を出力する。また、過学習を抑制するため隠れ層についてはドロップアウト [13] を行なっている。隠れ層の活性化関数は Rectified Linear Unit (ReLU)、出力層の活性化関数は sigmoid 関数とし、最適化アルゴリズムは Root Mean Square Propagation (RMSprop)、損失関数は二値交差エントロピー (Binary Crossentropy) を用いた。これは二値分類のモデルであり、このようなタスクには ReLU, sigmoid, Binary Crossentropy が適している [14] と知られているためこれらの関数を採用した。また、RMSprop とは AdaGrad を改良したアルゴリズムのことであり、AdaGrad では勾配の二乗の平均を計算するのに対し、RMSprop では勾配の二乗の指数移動平均を取る [15]。このため、初期の影響が指数的に減衰し、より新しいパラメータ更新の度合いによって学習率が調整される。

4. 実験

GPS と Wi-Fi の実データを用いて本提案手法の評価を行った。この比較実験では、小林らの類似度スコアアルゴリズム [16] によって生データから算出されたスコアデータを用いた。このため、本実験では小林らと同じデータセットを用いて従来手法（平均値によるスコアフュージョン、固定の重み付けによるスコアフュージョン）と本提案手法を比較する。

4.1 データセット

今回用いたデータセットは東京大学大学院情報理工学系研究科ソーシャル ICT 研究センター次世代個人認証講座が 2017 年 1 月 11 日から 4 月 26 日にかけて実施した大規模実証実験 MITHRA プロジェクト [17] により収集された

データである。MITHRA プロジェクトでは実験参加者のスマートフォンから GPS や Wi-Fi のログデータなどが収集された。実験参加者はインターネットなどを通して募集され、約 57,000 人が参加した。また MITHRA プロジェクトは東京大学大学院情報理工学系研究科の倫理審査委員会による約半年間の倫理審査によって適切であると判断されている [18]。

収集されたデータのうち GPS ログデータはその時刻でのユーザの位置情報であり、Wi-Fi ログデータはその時刻にユーザが受信した周囲の無線 LAN アクセスポイントの情報である。複数の無線 LAN アクセスポイントの情報を取得した場合、全てのアクセスポイントについて Wi-Fi ログデータとして収集される。このアクセスポイントの情報には SSID、BSSID や信号強度などが含まれているが、本実験では BSSID のみを用いる。約 57,000 人の全ユーザのうち GPS と Wi-Fi 情報の両者を提供したユーザは約 16,000 人である。これらのユーザから小林らの抽出手法と同じ以下の条件で 30 人のユーザを無作為に抽出した [16]。

- Android 端末で実験参加していること
- 60 日間以上実験参加していること

そして、抽出した 30 人のユーザについて生データから類似度スコアを算出した。

4.2 類似度スコアアルゴリズム

同じ人が同様の行動パターンを取った場合でもわずかな時間のズレなどのゆらぎが生じてしまうため、行動認証の際にはそのゆらぎを軽減する必要がある。そこで、生データから類似度スコアに変換することによって、このゆらぎを吸収している。本実験では、以下の小林らの類似度スコアアルゴリズムを使用する [16]。今回用いる生データは 60 日間の GPS と Wi-Fi のログデータである。まず、ユーザ毎のテンプレートが前半 30 日分のデータから作成される。そして、後半 30 日分のデータとテンプレートとの比較により類似度スコアが算出される。ここで、3 種類のゆらぎを吸収する処理を行っている。まず 1 つ目は時間情報のゆらぎについてであり、生データは 5 分毎の GPS と Wi-Fi 情報であるが、それを 1 時間毎のデータに丸める。次に位置情報のゆらぎに関しては位置情報を緯度経度のピンポイントではなくメッシュコードを用いて表現する。メッシュとは、緯度経度に基づき地域をほぼ同じ大きさの網目に分割したものであり [19]、このメッシュを識別するコードをメッシュコードと呼ぶ。ここでは、1km 四方のメッシュを採用している。最後に Wi-Fi 情報のゆらぎについてであり、ある 1 時間のうちに検出された頻度が多い上位 5 つのアクセスポイントをその時間での Wi-Fi 情報とし、それ以外を切り捨てる。これらの処理を行うことでそれぞれのゆらぎを抑えたスコアデータを算出できる。また、テンプレートは GPS と Wi-Fi 情報それぞれについてそのデー

タの頻度に応じて重みが大きくなるように作成されているため、このテンプレートとの比較により算出されるスコアはそれぞれのゆらぎを吸収したものとなっている。これによって、ゆらぎが軽減された 1 時間毎のスコアデータが得られる。

4.3 比較実験

本提案手法を従来手法と比較し、FRR(False Rejection Rate)、FAR(False Acceptance Rate) を用いて評価した。各ユーザのテンプレートについてユーザ 30 人分の類似度スコアを算出するため、合計で 30×30 通りのスコアデータがある。これらのスコアデータをそれぞれのユーザについて本人のスコアデータと他人のスコアデータに分類し、他人のスコアデータから本人のスコアデータと同量になるように無作為に抽出した。そして、その本人のスコアデータと抽出した他人のスコアデータを合わせて、そのユーザのスコアデータとした。1 時間毎のスコアデータであるので本人のスコアデータは $30 \text{ 日} \times 24 \text{ 時間} = 720$ 、他人のスコアデータも同量になるように抽出するのでユーザ毎に 1440 のスコアがある。このうち 60% を学習に用いた。

1 時間毎のスコアデータに加えて、6 時間と 24 時間の移動平均をとったスコアデータを用意した。本実験ではこの 3 種類のスコアデータを用い、それぞれの組み合わせについて実験を行った。GPS 単体や Wi-Fi 単体の場合についても同様な実験を行い、従来手法として平均値によるスコアフュージョンと比較した。GPS と Wi-Fi の両方を用いた実験については平均値によるスコアフュージョンに加えて、固定の重み付けによるスコアフュージョンとも比較を行った。本実験での従来手法の判定の際の閾値は 0.01 に設定した。また、固定の重み付けによるスコアフュージョンでの GPS の重みは Wi-Fi の 5 倍になるように設定した。これは、実験的に Wi-Fi の認証精度よりも GPS の精度の方が高いことがわかってきたため、このような値にした。

5. 実験結果

本章では、3 種類のスコアデータ (1 時間毎、6 時間毎、24 時間毎) を用いた従来手法と提案手法との比較結果を説明する。また、スコアデータの要素については GPS のみ、Wi-Fi のみ、GPS と Wi-Fi の両方の場合の 3 通りについて実験した。

5.1 GPS のスコアデータでの結果

表 1 に GPS のスコアデータのみを用いた場合での提案手法と平均値によるスコアフュージョンの比較結果を示す。この表からわかる通り、提案手法での FRR はどのスコアデータを用いた場合でも大きく減少している。すなわち、提案手法により TAR(True Acceptance Rate) を大きく改善できたと言える。一方で FAR は増加しているた

表 1 Comparison result with GPS only.

score data	average score fusion		proposed method	
	FRR	FAR	FRR	FAR
1, 6h	0.04114	0.00029	0.00012	0.04007
1, 24h	0.01647	0.00163	0.00012	0.01634
6, 24h	0.01657	0.00059	0.00000	0.01740
1, 6, 24h	0.01672	0.00045	0.00000	0.01953

表 2 Comparison result with Wi-Fi only.

score data	average score fusion		proposed method	
	FRR	FAR	FRR	FAR
1, 6h	0.15235	0.00029	0.00000	0.14136
1, 24h	0.06956	0.00040	0.00013	0.06684
6, 24h	0.06882	0.00119	0.00000	0.06449
1, 6, 24h	0.06961	0.00094	0.00000	0.06401

表 3 Comparison result with both GPS and Wi-Fi.

score data	average score fusion		fixed weighting		proposed method	
	FRR	FAR	FRR	FAR	FRR	FAR
1h	0.07227	0.00053	0.07294	0.00053	0.00071	0.07423
6h	0.03053	0.00289	0.03472	0.00029	0.00000	0.03187
24h	0.01222	0.00000	0.01276	0.00000	0.00000	0.01275
1, 6h	0.03212	0.00121	0.03506	0.00087	0.00037	0.03521
1, 24h	0.01222	0.00054	0.01267	0.00054	0.00000	0.01359
6, 24h	0.01222	0.00069	0.01271	0.00000	0.00000	0.01332
1, 6, 24h	0.01222	0.00124	0.01331	0.00064	0.00000	0.01274

め, TRR(True Rejection Rate) は減少している. ここで, TAR と TRR は次の式で定義されている.

$$TAR = 1 - FRR \quad (3)$$

$$TRR = 1 - FAR \quad (4)$$

また, 24 時間の移動平均をとったスコアデータを含む場合では FAR の増加分が小さいことがわかる. このため, 期間の長いスコアデータほど他人を他人であると正しく判定できていると言える.

5.2 Wi-Fi のスコアデータでの結果

表 2 に Wi-Fi のスコアデータのみを用いた場合での提案手法と平均値によるスコアフュージョンの比較結果を示す. GPS のみの場合と同じく, TAR は改善し TRR は減少している. また, GPS のみの場合と比較すると TAR はより顕著に増加しているが, FAR が全体的に高くなっている.

5.3 GPS と Wi-Fi のスコアデータでの結果

表 3 に GPS と Wi-Fi のスコアデータを用いた場合での提案手法と従来手法 (平均値によるスコアフュージョン, 固定の重み付けによるスコアフュージョン) の比較結果を示す. この表から, GPS や Wi-Fi 単体の場合と比較して FAR を低く抑えられていることがわかる. すなわち, 要素を増やしたことによって FAR を改善することができたと言える. 図 3 と図 4 に TAR と TRR それぞれの比較結果を示す. これらの図から, 提案手法について 1, 6, 24 時間のスコアデータを比較すると 24 時間のスコアデータが最も高い TRR であることがわかる. このため, 期間の長いスコアデータほど FAR の増加を抑えられると考えられる. これは, 期間が長いほど行動認証においてノイズとなるゆらぎの影響を抑えることができるためであると考えられる.

本実験ではゆらぎを抑えるために生データから類似度スコアへ変換する前処理の際に, 4.2 節で説明した既存の類似度スコアアルゴリズムを用いている. この類似度スコア算出の際にデータを削減しすぎていることが FAR が大きくなった要因の一つとして考えられる. しかし, FRR は提案手法により改善しているため, FRR を重要視する場面では提案手法は有用であると言える.

6. 結論

従来スコアフュージョン手法はユーザ毎にスコアの傾向が異なる場合には適していないという課題があった. そこで, 本研究ではニューラルネットを用いた二値分類に基づくスコアフュージョン手法を提案する. そして, GPS と Wi-Fi の実データを用いて本提案手法を評価し, 従来手法 (平均値によるスコアフュージョン, 固定の重み付けによるスコアフュージョン) と比較した. この比較結果から, このような傾向が異なる場合においても本提案手法により TAR が向上したことを確認した. GPS や Wi-Fi のようなユーザのライフスタイルに大きく依存し, ユーザ間で傾向が異なる多要素認証において, 本提案手法では FRR を大きく改善することができる. 一方で, FAR は従来手法よりも大きくなっている. このため, 本提案手法は FRR をより優先する場面では有用であると言える. また, 今回の比較実験では既存の類似度スコアアルゴリズムにより算出されたスコアデータを用いた. この類似度スコアへの変換の際にデータが削減されすぎていることが FAR が大きくなった要因の一つとして考えられる.

今後の研究としてモデルの改善が考えられる. また, 類似度スコア算出の前処理においてデータを削減しすぎない類似度スコアアルゴリズムを適用することも必要である. そして, FRR と FAR の両者を改善することを目指す. 本

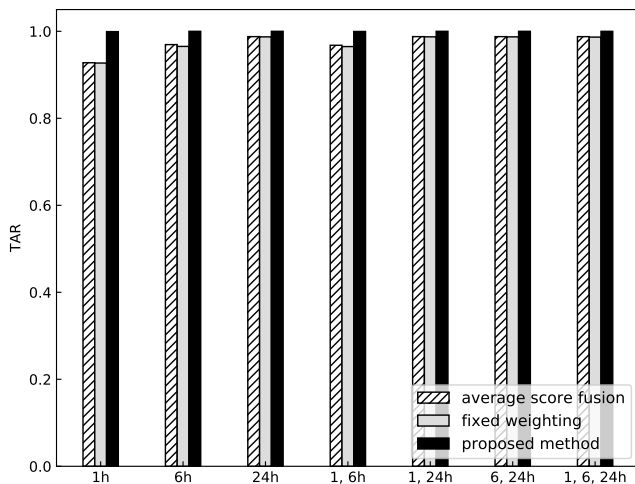


図 3 TAR result with both GPS and Wi-Fi.

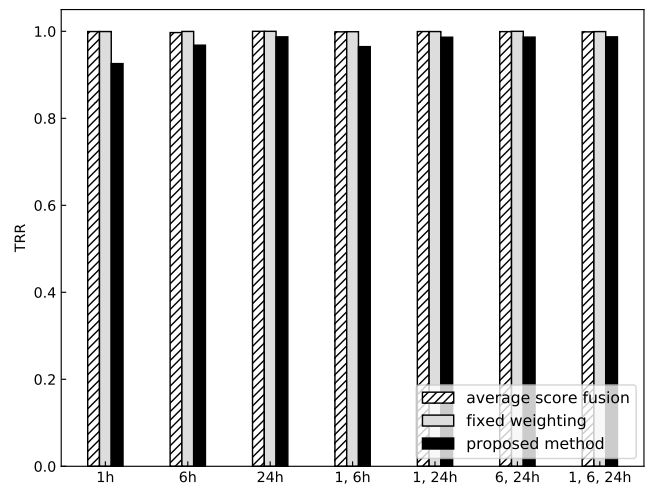


図 4 TRR result with both GPS and Wi-Fi.

研究では GPS と Wi-Fi のデータを用いた実験を行ったが、さらに IP アドレスやアプリ履歴などの要素を増やして評価を行うことも検討している。

参考文献

- [1] S. Ibrokhimov, K. L. Hui, A. Abdulhakim Al-Absi, h. j. lee, and M. Sain. Multi-factor authentication in cyber physical system: A state of art survey. In *2019 21st International Conference on Advanced Communication Technology (ICACT)*, pp. 279–284, Feb 2019.
- [2] D. M. Shila, K. Srivastava, P. O’Neill, K. Reddy, and V. Sritapan. A multi-faceted approach to user authentication for mobile devices —using human movement, usage, and location patterns. In *2016 IEEE Symposium on Technologies for Homeland Security (HST)*, pp. 1–6, May 2016.
- [3] W. Kabir, M. O. Ahmad, and M. N. S. Swamy. A multi-biometric system based on feature and score level fusions. *IEEE Access*, Vol. 7, pp. 59437–59450, 2019.
- [4] X. Yan, F. Deng, and W. Kang. Palm vein recognition based on multi-algorithm and score-level fusion. In *2014 Seventh International Symposium on Computational Intelligence and Design*, Vol. 1, pp. 441–444, Dec 2014.
- [5] M. S. Madane and S. D. Thepade. Score level fusion based multimodal biometric identification using thepade’s sorted ternary block truncation coding with varied proportion of iris, palmprint, left fingerprint right fingerprint with assorted similarity measures different colors. In *2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT)*, pp. 824–828, Sep. 2016.
- [6] N. Damer, A. Opel, and A. Nouak. Cmc curve properties and biometric source weighting in multi-biometric score-level fusion. In *17th International Conference on Information Fusion (FUSION)*, pp. 1–6, July 2014.
- [7] 小林良輔, 山口利恵. 移動・wi-fi 履歴情報から見る個人ごとの生活習慣類似性評価. マルチメディア, 分散協調とモバイルシンポジウム 2018 論文集, 第 2018 巻, pp. 1559–1565, jun 2018.
- [8] Ryosuke Kobayashi, Nobuyuki Saji, Nobuo Shigeta, and Rie Shigetomi Yamaguchi. Large scale poc experiment with 57,000 people to accumulate patterns for lifestyle

authentication. In *Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy, CODASPY ’19*, p. 161–163, New York, NY, USA, 2019. Association for Computing Machinery.

- [9] Ryan Connaughton, Kevin W. Bowyer, and Patrick J. Flynn. *Fusion of Face and Iris Biometrics*, pp. 219–237. Springer London, London, 2013.
- [10] J Matse Jones Siphon. Multi-factor biometrics: An overview, 11 2014.
- [11] Arun A. RossAnil K. JainKarthik Nandakumar. *Handbook of Multibiometrics*. 2006.
- [12] J. Aravinth and S. Valarmathy. Multi classifier-based score level fusion of multi-modal biometric recognition and its application to remote biometrics authentication. *The Imaging Science Journal*, Vol. 64, No. 1, pp. 1–14, 2016.
- [13] Nitish Srivastava, Geoffrey Hinton, Alex Krizhevsky, Ilya Sutskever, and Ruslan Salakhutdinov. Dropout: A simple way to prevent neural networks from overfitting. *J. Mach. Learn. Res.*, Vol. 15, No. 1, pp. 1929–1958, January 2014.
- [14] Francois Chollet. *Deep Learning with Python 1st Edition*. 2017.
- [15] Geoffrey Hinton. Lecture 6e rmsprop: Divide the gradient by a running average of its recent magnitude, coursera: Neural networks for machine learning.
- [16] Ryosuke Kobayashi and Rie Shigetomi Yamaguchi. Evaluation of personal lifestyle habits similarity using location and wi-fi history information. In *Multimedia, Distributed, Cooperative, and Mobile Symposium 2018*, Vol. 2018, pp. 1559–1565, jun 2018. (written in Japanese).
- [17] 鈴木宏哉, 小林良輔, 佐治信之, 山口利恵. ライフスタイル認証実証実験レポート -mithra データセット-. マルチメディア, 分散協調とモバイルシンポジウム 2017 論文集, 第 2017 巻, pp. 223–230, jun 2017.
- [18] R. Kobayashi, H. Susuki, N. Saji, and R. S. Yamaguchi. Lifestyle authentication and mithra project. In *2018 10th International Conference on Communication Systems Networks (COMSNETS)*, pp. 464–467, 2018.
- [19] 総務省. 地域メッシュ統計の特質・沿革. <http://www.stat.go.jp/data/mesh/pdf/gaiyo1.pdf>. (Accessed on 05/13/2020).