6Y-08

iOS端末のフィンガープリントを用いた識別における手法ごとの精度の比較

柴田　怜 †i　　野田　隆文 ‡　　齋藤　孝道 †
明治大学 †　　明治大学大学院 ‡

1　はじめに

Webトラッキング技術の一つにフィンガープリンティングがある．フィンガープリンティングとは，ブラウザから取得可能な情報を収集し，端末情報を複数組み合わせたもの（以後フィンガープリントと呼ぶ）の差異を基にサーバ側で端末を識別する技術である．

しかし，iOS端末は取得可能な情報の種類が少ない上に，詳細な情報を得ることが難しい [1]．例えばUser-Agentの文字列の中に機種名が含まれていないことがその代表例である．こうした理由から取得した情報の差異も生じにくく，iOS端末は他のOSの端末に比べて識別が難しくなる．本論文ではルールベースと深層学習の2つの手法を用いて，iOS端末の識別精度を求めた．加えて，2つの手法の実行時間の計測も行った．

2　実験

2.1　実験データ

本論文では2013年12月6日から2019年12月4日の間に収集したiOS端末のアクセスデータの2336サンプルを実験に利用した．

2.1.1　使用する情報の種類

本実験で用いるアクセスデータの情報に，IPアドレスとUAから，位置情報やOSのバージョンを含む新たな情報を生成し追加した．総数93の端末情報 (以降，特徴点と呼ぶ) を端末の識別に利用する．

2.1.2　アクセスデータからベクトルデータへの変換

実験のためにアクセスデータをベクトルデータへ変換する手順を説明する．本実験では以下の手順で122388組のベクトルデータが得られた．

なお，以降で示す一致ラベルとは特徴点の値が一致しているかを示すラベルである．正解ラベルとは2件のアクセスデータが同一端末のブラウザから送信されたかどうかを表すラベルである．ともに一致している場合は1，不一致の場合は0で表す．

1. 任意の2件のアクセスデータを組み合わせ1次元のベクトルデータを作成する．
2. 各特徴点の値を比較し一致ラベルと正解ラベルを作成する．
3. 手順1で作成したベクトルデータの中で使用するものをデータ収集日の差が7日以内のものに限定する．

2.1.3　学習用データ・検証用データの作成

深層学習の検証において2.1.2の手順で作成したベクトルデータから学習用データと検証用データの作成する．今回は7 : 3の割合で分割し，それぞれを学習用データと検証用データとする．

2.2　深層学習による実験

2.2.1　ニューラルネットワークの構造

2.1.3で作成した学習用データと検証用データを用い，ニューラルネットワークの構造で教師あり深層学習を行い推定用モデルを作成する．教師データは正解ラベルを用いる．本実験に使用したニューラルネットワークは4層で構成され，各層が全結合層 [2] である．損失関数は交差エントロピー関数 [3]，最適化関数にはAdam[4]を使用した．

2.3　ルールベースによる実験

2.3.1　推定用アルゴリズム

以下に本実験で用いる推定アルゴリズムの手順について示す．図1が推定アルゴリズムの概要図である．

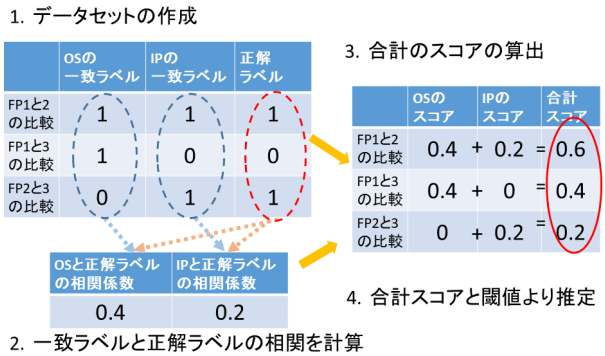

図1: 推定アルゴリズム概要図

1. 2.1.2節を基にアクセスデータをベクトルベータに変換し，一致ラベルと正解ラベルを作成する．
2. 各特徴点において一致ラベルと正解ラベルから相関係数を算出する．
3. 相関係数を重みとして各一致ラベルに掛け合わせ，特徴点ごとにスコアを算出する．また，これらの総和を求め合計スコアとする．

Consideration on required skill set based on Security Incidents
†Satoshi SHIBATA ‡Takahumi NODA†Takamichi SAITO
†Meiji University
‡Graduate School of Meiji University

4. 合計スコアが閾値を上回る場合，同一と判定する．

3 実験結果

3.1 識別精度の比較

表 1 にルールベースと深層学習の識別精度を示す．精度の指標は F_1 値 を使用し，予測結果と正解ラベルを基に算出している．また，recall と precision は参考までに示す．

表 1: 識別精度の比較

	recall	precision	F_1
ルールベース	0.9960	0.5090	0.6739
深層学習	0.9058	0.7726	0.8339

表 1 からルールベースよりも深層学習の方が F_1 値が 0.16 高い精度であると分かる．

3.2 実行時間の比較

計測した実行時間を図 2 に示す．ルールベースは 2.3.1 節の手順 2 から手順 4 までの処理，深層学習はモデルによる推定処理をそれぞれ計測した．

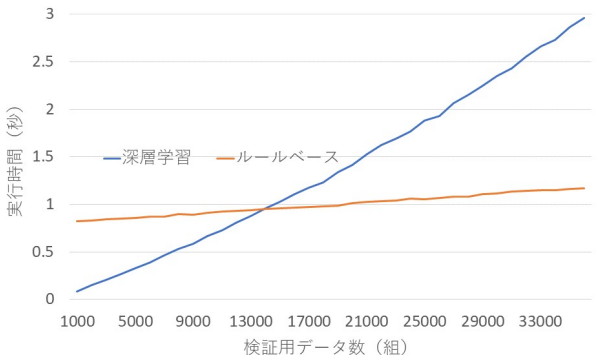

図 2: 検証用データ数と各手法の実行時間

図 2 からデータ数が多いほどルールベース，少ないほど深層学習による実行時間の方が短いことが読み取れる．また深層学習，ルールベースともにデータ数に比例し実行時間が増加するが，深層学習の方がよりデータ数に影響を受けていることが読み取れる．

4 考察

本節ではルールベースの改善点，実行時間について考察する．

4.1 ルールベースの改善点

2.3 節で重み付けに利用された相関係数に着目し，正解ラベルと一致ラベルの値の上位 5 個を表 2 に示す．

表 2: 正解ラベルと一致ラベルの相関係数の絶対値 (上位 5 個)

特徴点名	相関係数
送信元 IP アドレス	0.542
送信元 IP アドレスから推測される位置情報	0.542
送信元 IP アドレスのホスト部	0.542
送信元 IP アドレスの第 4 オクテット	0.451
送信元 IP アドレスの第 3 オクテット	0.416

表 2 では送信元 IP アドレスから派生した特徴点 15 個の内の 5 つの値が 0.4 以上であった．理由としては IP アドレスの変化が少ないためだと考えられる．原因の一つに，ユーザの利用するアクセスポイントが時間帯によって固定化していることが挙げられる．この場合アクセスデータの時間帯と IP アドレスを関連づけることで，精度の向上を見込める可能性が高い．

また，一致ラベルは 2 組のアクセスデータの特徴点の値が完全に一致しているかで作成される．そのため同一端末でもベンチマークのような計算値などは比較が難しい．採取できる情報の少ない iOS 端末の識別においては，値の差や類似度をみて，これらの特徴点を活用すると精度の向上する可能性がある．

4.2 実行時間

図 2 よりデータ数が多くなるとルールベースによる実行時間が深層学習より短いことが分かる．ルールベースの場合，一致ラベルの重み付けの処理は一回である．しかし深層学習の手法の場合，各層で重み付けを行っているためルールベースよりも実行時間がかかったと考えられる．そこで深層学習における実行時間を短くするには説明変数を減らす，あるいはモデルを小さくすることが挙げられる．しかし同時に識別精度に影響を与える可能性もある．

5 まとめ

本論文では iOS 端末においてルールベースの手法より深層学習の手法がフィンガープリントを高い精度で識別できることを示した．また，実行時間はデータ数が多い場合ルールベースの方が短いことが分かった．

参考文献

[1] 北条 大和, 齋藤 裕太, 齋藤孝道, ”深層学習を用いたパッシブフィンガープリンティング手法の提案と実装”, コンピュータセキュリティシンポジウム（CSS）2019
[2] https://keras.io/ja/layers/core/
[3] https://keras.io/ja/losses/
[4] https://keras.io/ja/optimizers/