

# ニューラルネットによるスコアレベルフュージョンを用いた 電子チラシアプリの閲覧履歴による多要素認証

松岡 勝也<sup>1,a)</sup> IRVAN MHD<sup>1</sup> 小林 良輔<sup>1</sup> 山口 利恵<sup>1</sup>

**概要:** インターネットの発展に伴い、人々はインターネットを通して様々なサービスを利用している。それぞれのサービスで個人情報を適切に保護する必要があるため、オンラインサービスを利用するには個人認証が必要となる。個人認証では堅牢な高い安全性が求められるが、その一方でユーザの利便性も重要となっている。安全性に加えて、ユーザの利便性を考慮した認証手法の一つとしてライフスタイル認証という個人認証手法が近年提案されている。ライフスタイル認証は日々の生活リズムを認証要素に用いた行動認証である。本研究ではこのライフスタイル認証の中の電子チラシアプリの利用履歴による認証に着目した。この利用履歴に基づく複数の認証要素に対して、ニューラルネットを用いたスコアレベルフュージョンを適用することにより精度の向上を目指した。そして、従来手法との比較実験により、FAR(False Acceptance Rate), FRR(False Rejection Rate) 共に改善していることを確認した。

**キーワード:** 多要素認証, スコアレベルフュージョン, ニューラルネット, ライフスタイル認証

## Multi-factor authentication with browsing history of flyer application using score level fusion by neural network

KATSUYA MATSUOKA<sup>1,a)</sup> MHD IRVAN<sup>1</sup> RYOSUKE KOBAYASHI<sup>1</sup>  
RIE SHIGETOMI YAMAGUCHI<sup>1</sup>

**Abstract:** With the development of the Internet, people are using various services through the Internet. Since each service needs to protect personal information appropriately, individual authentication is required when using online services. Robust and high security is required for personal authentication, though user convenience is also important. In recent years, a personal authentication method called lifestyle authentication has been proposed as authentication methods that consider user convenience and security. Lifestyle authentication is behavioral authentication that uses daily life rhythm as an authentication factor. In this research, we focused on the authentication based on the browsing history of the electronic flyer application in this lifestyle authentication. We aimed to improve the accuracy by applying score level fusion using a neural network to multiple authentication factors based on this browsing history. The comparison result with the conventional methods shows that both FAR (False Acceptance Rate) and FRR (False Rejection Rate) were improved.

**Keywords:** multi-factor authentication, score level fusion, neural network, lifestyle authentication

### 1. 序論

インターネットの発展に伴い、人々はインターネットを

通して様々なサービスを利用している。それぞれのサービスで個人情報を適切に保護する必要があるため、オンラインサービスを利用するには個人認証が必要となる。このため、多くの人々が認証技術を利用しており、サイバーセキュリティへの関心が高まってきていると言える。個人認証には大きく分けて、パスワードや合言葉などの知識認証、

<sup>1</sup> 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

<sup>a)</sup> matsuoka@yamagula.ic.i.u-tokyo.ac.jp

ワンタイムパスワード用のトークンや電子証明書などの所有認証、指紋や顔などの生体認証がある [1]。さらに、近年ではこれらに加えて行動認証の研究も進んできている。個人認証では堅牢な高い安全性が求められるが、その一方でユーザの利便性も重要となっている。安全性に加えて、ユーザの利便性を考慮した認証手法の一つとしてライフスタイル認証という個人認証手法が近年提案されている。ライフスタイル認証は日々の生活リズムを認証要素に用いた行動認証である。ライフスタイル認証での認証要素は位置情報やアプリケーションの利用履歴など生活スタイルに関連する情報を利用している。このため、1つ1つの要素の認証精度はパスワードや生体認証などと比較するとあまり高くはなく、単一の要素のみを利用した方式ではセキュリティ的に不十分な場合もある。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な安全な認証を実現することができる [2]。

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 [2]。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 [3], [4], [5], [6], [7]。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。このようなユーザ間で傾向が異なる場合に適したフュージョン手法は少ない。

本研究ではライフスタイル認証の電子チラシアプリに着目し、この閲覧履歴による多要素認証の認証精度の向上を目的とする。電子チラシアプリの閲覧履歴は、ユーザの生活圏や購買頻度などの生活スタイルを大きく反映しているデータであり、個人認証に適していると考えられるため本研究では電子チラシアプリの利用履歴での認証を提案する。また、フュージョンの際に要素毎の重み付けを固定した手法ではなく、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適用することで精度向上を目指す。本提案手法のフュージョンでは、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

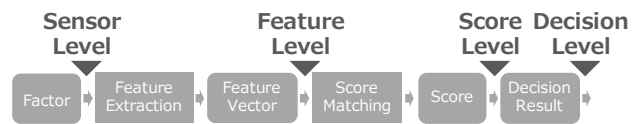


図 1 Processing flow and fusion levels.

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] により集められたデータを用いて評価する。実証実験の参加者 57,000 人のうち、電子チラシアプリの利用履歴と位置情報などを併せて提供したユーザは 1,500 人であった。本手法の評価では、これらユーザのうち使用頻度の高かった 36 人分の実データを用いて従来手法との比較を行った。

## 2. 関連研究

本章では、本研究で着目しているライフスタイル認証と、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 ライフスタイル認証

ライフスタイル認証は行動認証の 1 つであり、人々の生活習慣や生活リズムなどのライフスタイルに基づく個人認証手法である [9]。ここで、ライフスタイルとは日々の生活の中で無意識に繰り返す行動パターンを意味している。また、人々は固有の生活リズム、生活サイクルがあるものの、毎日必ず同じような行動をするとは限らない。このため、ライフスタイルの情報にばらつきが生じ、認証精度が低下する可能性がある。このリスクを軽減するための対策として、複数のライフスタイルによる認証要素を組み合わせた多要素認証が考えられる。そこで、本研究では多要素のライフスタイル認証に着目している。また、これまでにライフスタイル認証では、ユーザの位置情報や Wi-Fi 情報に基づく手法 [10], [11]、ウェアラブルデバイスから得られた運動履歴情報に基づく手法 [12]、マンガ閲覧アプリの利用履歴による手法 [13]、電子チラシアプリの利用履歴に基づく手法 [14] などが認証要素として提案されている。本研究では、この中で電子チラシアプリの閲覧履歴に基づく手法に着目している。

### 2.2 フュージョン手法

フュージョン手法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る [15]。そして、その値により最終的な判定を行う。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 [4]。以下でこれらのレベル毎の詳細を説明する。

(1) センサレベルフュージョン

センサレベルフュージョンは、センサからの生データをフュージョンする方式である [16]。このフュージョンは、複数の互換性のあるセンサから取得されたデータか、もしくは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 [17]。すなわち、互換性のあるセンサーデータに対してのみ適用できる。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。

## (2) 特徴レベルフュージョン

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 [17]。特徴量に対して最小値、最大値や中央値での正規化を行った後に、特徴選択を行う必要がある。

## (3) スコアレベルフュージョン

スコアレベルフュージョンは異なるマッチスコアをフュージョンする方式である。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 [17]。スコアレベルフュージョンを行う際にはマッチスコアの範囲が統一されていなければならないため、そ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 [16]。

## (4) 決定レベルフュージョン

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フュージョンする方式である。決定レベルフュージョンでは 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 [16]。

本研究では、これらのフュージョン手法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手法が多い [3], [4], [5], [6], [7]。

## 2.3 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 [18]。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。本提案手法でのフュージョンとの差異は、それぞれの要素での重みが等しいという点である。

## 2.4 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り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 [3]。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。本提案手法でのフュージョンとの差異は、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。

### 2.4.1 エラー率に基づく重みによるスコアフュージョン

Attaullah Buriro らの研究では、スマートフォンを利用する際の動きに基づく行動認証が提案されている [19]。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、エラー率に基づき固定の重みを定義するスコアフュージョンが用いられている。この重みを定義するアルゴリズムを以下に示す。

$er$  をそれぞれの要素に対するエラー率とする。すなわち、要素 1 に対するエラー率は  $er_1$ , 要素 2 は  $er_2$  となる。これらそれぞれのエラー率  $er_i$  は特徴量毎の FRR(False Rejection Rate) と FAR(False Acceptance Rate) が等しくなるような閾値を取った時の等価エラー率 EER(Equal Error Rate) である。この  $er$  を元に、エラー率が小さいほど値が大きくなるような指標を定める。要素  $c$  に対するこの指標  $index(c)$  を以下の式で定義する。

$$index(c) = 1 - \frac{er(c)}{\sum_{i=1}^n er(i)} \quad (3)$$

そして、指標  $index(c)$  を用いて次式により、要素  $c$  の重み  $weight(c)$  を求める。

$$weight(c) = \frac{index(c)}{\sum_{i=1}^n index(i)} \quad (4)$$

## 2.5 従来のフュージョン手法の課題点

上述したスコアフュージョン手法は重み付けを固定した方式が多く、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課題を解決するフュージョン手法を適用した行動認証手法を提案する。

### 3. 提案手法

本章では、提案手法について用いたデータセット、電子チラシアプリの閲覧履歴による各認証要素のスコア算出手法、それらの要素を組み合わせるフュージョン手法について説明する。

#### 3.1 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 26 日から 3 月 31 日にかけて実施した大規模実証実験 MITHRA プロジェクト [20] 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電子チラシアプリやマンガ閲覧アプリの利用履歴、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 [9]。実験参加者 57,000 人のうち、電子チラシアプリの利用履歴を提供したユーザは約 31,000 人であり、電子チラシアプリの利用履歴と併せて位置情報などを提供したユーザは約 1,500 人である。本研究では、これらの情報を提供したユーザに限定した。また、これらの収集されたデータのうち、実験期間の 65 日間で毎日 1 回以上閲覧したユーザは 36 人であった。利用履歴が多いほど精度が高い認証ができると考えられるため、本研究では毎日閲覧した 36 人のユーザのデータに限定して利用した。

##### 3.1.1 電子チラシアプリの利用履歴データ

今回利用した電子チラシアプリの利用履歴データについて説明する。まず、この電子チラシアプリとは配信されている大手スーパー、ドラッグストア、家電量販店などの電

子チラシを閲覧することができるアプリケーションである。利用履歴データはユーザがチラシを閲覧する度に記録され、取得した項目は以下の 7 つである [14]。

- ユーザ ID
- 性別
- 年齢
- 利用デバイス
- チラシ閲覧時刻
- 閲覧したチラシの店舗 ID
- 閲覧したチラシ ID

#### 3.2 スコア算出方法

本研究では、従来手法 [21] で提案されたスコア算出アルゴリズムを参考に電子チラシアプリの利用履歴から閲覧傾向、閲覧回数、閲覧店舗の 3 つの特徴量に基づく認証スコアを算出した。収集したデータのうち、ユーザ ID、チラシ閲覧時刻、閲覧したチラシの店舗 ID を用いた。実験期間 65 日のうち前半 14 日間で各ユーザのテンプレート作成に用いて、残りのデータを類似度スコアの算出に利用した。

##### 3.2.1 閲覧傾向に基づく類似度スコア

閲覧傾向とは、どの時間帯にチラシを閲覧するかという情報である。日中に閲覧することが多いユーザや夜間の方が多いうるユーザなど、ユーザ毎に特異な傾向がある。このため、異なるユーザでは閲覧する時間帯に差異があり、同一ユーザでは異なる日でも概ね同じ時間帯に閲覧すると考えられる。以下に類似度スコア算出のアルゴリズムを説明する。

###### (1) 特徴抽出。

取得した利用履歴データからベクトル  $v_{i,day_j}$  を生成する。 $v_{i,day_j}$  はユーザ ID が  $i$  であるユーザのデータのうち日付  $day_j$  の 1 時間毎の閲覧回数を表すベクトルである。 $v_{i,day_j}$  の第  $k$  成分は  $(k-1)$  時 0 分から  $(k-1)$  時 59 分の間にチラシを閲覧した回数を表す。

###### (2) データ分割。

$v_{i,day_j}$  とテンプレート作成用  $D_{time}^{tpl}$  と類似度スコア算出用  $D_{time}^{score}$  に分ける。今回は前半 14 日分をテンプレート作成に、残りを類似度スコア算出に利用したため、 $\{v_{i,day_j} | i = 1, 2, \dots, 36, j = 1, 2, \dots, 14\}$  を  $D_{time}^{tpl}$ 、 $\{v_{i,day_j} | i = 1, 2, \dots, 36, j = 15, 16, \dots, 65\}$  を  $D_{time}^{score}$  とする。

###### (3) テンプレート作成。

ユーザ ID が  $i$  であるユーザの閲覧回数についてのテンプレート  $T_{time}^i$  を次の式で定義する。

$$T_{time}^i = \frac{1}{14} \sum_{k=1}^{14} v_{i,day_k} \left( v_{i,day_k} \in D_{time}^{tpl} \right) \quad (5)$$

###### (4) 類似度スコア算出。

閲覧傾向の類似度スコア算出はコサイン類似度を計算

する。ユーザー ID が  $i$  であるユーザーのテンプレート  $T_{time}^i$  と類似度算出用のデータ内にある  $v_{j,day_k}$  間の類似度スコア  $S_{tend}(T_{time}^i, v_{j,day_k})$  を次の式で定義する。

$$S_{tend}(T_{time}^i, v_{j,day_k}) = \frac{\sum_{n=1}^{24} T_n v_n}{\sqrt{\sum_{n=1}^{24} T_n} \sqrt{\sum_{n=1}^{24} v_n}} \quad (6)$$

類似度算出用データの 1 日目は式 (6) により求めるが、2 日目以降は直近 24 時間のデータを  $v_n$  として、1 時間毎の類似度スコアを算出する。

### 3.2.2 閲覧回数に基づく類似度スコア

閲覧回数とは、1 時間毎の閲覧回数の情報である。閲覧傾向と同様に、各時間帯について同一ユーザでは概ね同じ閲覧回数となり、他のユーザとは閲覧回数が大きく異なる。以下に類似度スコア算出のアルゴリズムを説明する。(3) テンプレートの作成までは 3.2.1 章と同様であるため省略する。

- (1) 特徴抽出。
- (2) データ分割。
- (3) テンプレート作成。
- (4) 類似度スコア算出。

閲覧回数の類似度スコア算出は、ユークリッド距離を計算することで実現する。ユーザー ID が  $i$  であるユーザーのテンプレート  $T_{time}^i$  と類似度算出用のデータ内にある  $v_{j,day_k}$  間の類似度  $S_{num}(T_{time}^i, v_{j,day_k})$  を以下の式で定義する。

$$S_{num}(T_{time}^i, v_{j,day_k}) = \frac{1}{1 + \sqrt{\sum_{n=1}^{24} (T_n - v_n)^2}} \quad (7)$$

また、正規化するために、ユークリッド距離に 1 を加えた逆数をとっている。そして、類似度算出用データの 1 日目は式 (7) により求めるが、2 日目以降は直近 24 時間のデータを  $v_n$  として、1 時間毎の類似度スコアを算出する。

### 3.2.3 閲覧店舗に基づく類似度スコア

閲覧店舗とは、1 日のうちにどの店舗を閲覧したかという情報である。各ユーザは自身の生活圏の店舗のチラシを見るため、ユーザ毎に閲覧店舗が異なると考えられる。以下に類似度スコア算出のアルゴリズムを説明する。

- (1) 特徴抽出。

取得したアプリ利用履歴データから、集合  $S_{i,day_j}$  を生成する。 $S_{i,day_j}$  はユーザー ID が  $i$  であるユーザーが日付  $day_j$  のときに閲覧したチラシの店舗 ID を要素とする集合である。

- (2) データ分割。

閲覧傾向や閲覧回数と同じく、テンプレートは前半 14 日間であり、残りを類似度スコア算出用データとしているため、 $\{S_{i,day_j} | i = 1, 2, \dots, 36, j = 1, 2, \dots, 14\}$  を  $D_{shop}^{tpl}$ 、 $\{S_{i,day_j} | i = 1, 2, \dots, 36, j = 15, 16, \dots, 65\}$

を  $D_{shop}^{score}$  とする。

- (3) テンプレート作成。

テンプレート期間に 1 回以上チラシを閲覧した店舗 ID を要素とする集合をテンプレートとする。ユーザー ID が  $i$  であるユーザーのテンプレート  $T_{shop}^i$  を次の式で定義する。

$$T_{shop}^i = \bigcup_{k=1}^{14} S_{i,day_k} \quad (S_{i,day_k} \in D_{time}^{tpl}) \quad (8)$$

- (4) 類似度スコア算出。

閲覧店舗の類似度スコア算出は、dice 係数を計算することで行う。ユーザー ID が  $i$  であるユーザーのテンプレート  $T_{shop}^i$  と類似度スコア算出用のデータ内にある  $S_{j,day_k}$  間の類似度  $S(T_{shop}^i, S_{j,day_k})$  を以下の式で定義する。

$$S(T_{shop}^i, S_{j,day_k}) = \frac{2|T_{shop}^i \cap S_{j,day_k}|}{|T_{shop}^i| + |S_{j,day_k}|} \quad (9)$$

類似度算出用データの 1 日目は式 (9) により求めるが、2 日目以降は  $S_{j,day_k}$  を直近 24 時間のデータとして、1 時間毎の類似度スコアを算出する。

## 3.3 フュージョン手法

本提案手法のフュージョンには、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い認証精度を高めるスコアフュージョン手法を適用する。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。ユーザー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。本研究では、電子チラシアプリの閲覧履歴から 3 種類の類似度スコアを算出したため、入力は 3 つのスコアとなっている。図 2 の上から 1 つ目の入力 time score は 3.2.1 で説明した閲覧傾向に基づく類似度スコア、2 つ目の count score は 3.2.2 で述べた閲覧回数に基づく類似度スコア、3 つ目の shop score は 3.2.3 で説明した閲覧店舗に基づく類似度スコアを表している。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 [22] を行っている。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

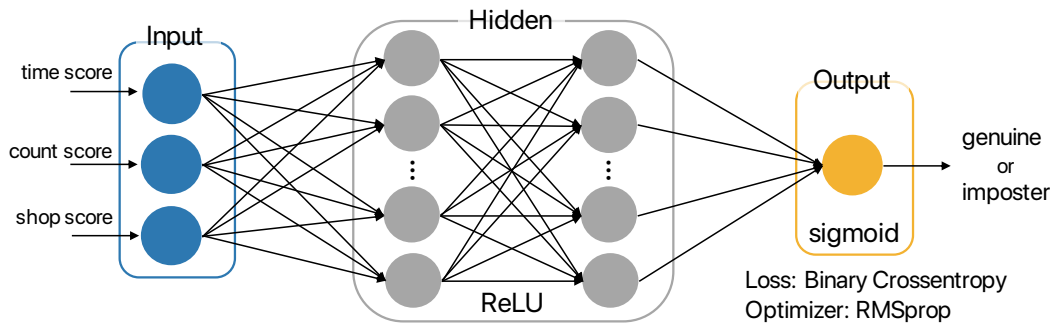


図 2 Binary classification network used in our proposed method.

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 [23] 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 [24]。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割合によって学習率が調整される。

#### 4. 実験

本章では比較実験について, 比較対象の従来手法と実験方法の詳細について説明する。

##### 4.1 比較対象の従来手法

本実験では以下の 3 つの従来手法との比較を行った。

###### (1) 平均値によるスコアフュージョン。

これは 2.3 章で説明した通り, 各認証要素の平均値をとるスコアフュージョンである。

###### (2) Buriro らの固定の重み付けによるスコアフュージョン [19]。

これは 2.4.1 章で説明したエラー率に基づいた指標により算出した重み付けによるスコアフュージョンである。

###### (3) エラー率の逆数を重みとする固定の重み付けによるスコアフュージョン。

これは Buriro らの手法 [19] を参考に, 各要素の等価エラー率 EER の逆数を取り, それらを正規化した値を重みとして固定したスコアフュージョンである。

これら従来手法を用いて FRR(False Rejection Rate), FAR(False Acceptance Rate) を求める際の閾値は, FRR と FAR が等しく, EER となるような最適な値としている。

##### 4.2 比較実験

本提案手法を従来手法と比較し, FRR, FAR を用いて評価した。比較実験の際には 3.2 章で述べたアルゴリズム

表 1 Comparison result of FRR and FAR.

method	FRR	FAR
average score fusion	20.52%	19.02%
fixed weighting (Buriro et al.)	17.62%	16.17%
fixed weighting (EER inverse)	10.17%	8.17%
proposed method	1.25%	3.95%

により算出された 3 種類のスコアを用いた。この 3 種類のスコアをフュージョンする手法を従来手法と比較した。各ユーザのテンプレートについてユーザ 36 人分の類似度スコアを算出するため, 合計で  $36 \times 36$  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  $51 \text{ 日} \times 24 \text{ 時間} = 1224$ , 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 2448 のスコアがある。このうち 60% を学習に用いた。

#### 5. 実験結果

表 1 に FRR と FAR の比較結果の表を示す。ここで, 従来手法の average score fusion は 4.1 章の (1) を, fixed weighting (Buriro et al.) は (2) を, fixed weighting (EER inverse) は (3) を表す。表 1 での FRR の比較からわかる通り, 平均値によるスコアフュージョンや固定の重み付けによるスコアフュージョンなどの従来手法と比較して本提案手法では FRR を大幅に改善していることがわかる。また, 表 1 での FAR の比較からわかる通り, FAR についても同様に大きく改善していることがわかる。提案手法により FRR, FAR 共に大きく改善しているが, FRR の方がより顕著に改善している。

#### 6. 結論

本研究では, ライフスタイル認証の 1 つとして提案されている電子チラシアプリの利用履歴を用いた多要素認証に

着目し、精度の向上を目指した。従来手法のスコアフュージョン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適用した。そして、電子チラシアプリの閲覧履歴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、従来手法と比べ FRR, FAR 共に改善していることを確認した。しかし、FAR は FRR ほど顕著に改善されていないため、本提案手法は FRR を優先する場面ではより有用であると言える。

今後の研究としては、類似度スコア算出のアルゴリズムやフュージョン手法のモデルの改善が考えられる。そして、FAR についても FRR と同程度に改善することを目指す。本研究で電子チラシアプリのデータのみを用いた実験を行ったが、さらに GPS や Wi-Fi などと紐付けて要素を増やしていくことも検討している。

#### 参考文献

- [1] 独立行政法人情報処理推進機構. オンライン本人認証方式の実態調査報告書. <https://www.ipa.go.jp/files/000040778.pdf>, 8 2014. (Accessed on 08/04/2019).
- [2] 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.
- [3] 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.
- [4] 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.
- [5] 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.
- [6] 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 colorspace. In *2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT)*, pp. 824–828, Sep. 2016.
- [7] 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.
- [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] 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.
- [10] 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.
- [11] R. Kobayashi and R. S. Yamaguchi. A behavior authentication method using wi-fi bssids around smartphone carried by a user. In *2015 Third International Symposium on Computing and Networking (CANDAR)*, pp. 463–469, 2015.
- [12] 鈴木宏哉, 山口利恵. ウェアラブルデバイスを活用した個人の行動によるユーザ認証の検討. SCIS2015 暗号と情報セキュリティシンポジウム, pp. 4C2–4, 2015.
- [13] 小林良輔, 山口利恵. マンガアプリの閲覧作品と閲覧時間を利用した個人認証手法. マルチメディア, 分散協調とモバイルシンポジウム 2016 論文集, 第 2016 巻, pp. 189–194, jul 2016.
- [14] 西山双輝, 鈴木宏哉, 小林良輔, 山口利恵. 電子チラシアプリの利用履歴の個人性に関する検証. 電子情報通信学会技術研究報告 = IEICE technical report : 信学技報, Vol. 117, No. 287, pp. 27–32, 2017.
- [15] Ryan Connaughton, Kevin W. Bowyer, and Patrick J. Flynn. *Fusion of Face and Iris Biometrics*, pp. 219–237. Springer London, London, 2013.
- [16] J Matse Jones Siphon. Multi-factor biometrics: An overview, 11 2014.
- [17] Arun A. Ross Anil K. Jain Karthik Nandakumar. *Handbook of Multibiometrics*. 2006.
- [18] 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.
- [19] Attaullah Buriro, Bruno Crispo, Filippo Del Frari, Jeffrey Klardie, and Konrad Wrona. Itsme: Multimodal and unobtrusive behavioural user authentication for smartphones. In Frank Stajano, Stig F. Mjøl̄snes, Graeme Jenkinson, and Per Thorsheim, editors, *Technology and Practice of Passwords*, pp. 45–61, Cham, 2016. Springer International Publishing.
- [20] 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.
- [21] 西山双輝. 電子チラシアプリの利用履歴を用いた認証. Master’s thesis, 東京大学大学院 情報理工学系研究科 電子情報学専攻, 2019.
- [22] 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.
- [23] Francois Chollet. *Deep Learning with Python 1st Edition*. 2017.
- [24] Geoffrey Hinton. Lecture 6e rmsprop: Divide the gradient by a running average of its recent magnitude, course: Neural networks for machine learning.