

多要素認証におけるスコアフュージョンへの ニューラルネットの適用

松岡 勝也^{1,a)} Irvan Mhd¹ 小林 良輔¹ 山口 利恵¹

概要: 昨今セキュリティへの関心は高まっており、パスワードなどの知識認証や指紋などの生体認証といった個人認証に関する技術がより重要となってきた。そこで本研究では個人認証の一種である多要素認証に着目し、多要素認証での各要素のスコアフュージョンの手法を比較検討する。これまでも多要素でのスコアフュージョンに関する研究は行われてきているが、スコアフュージョンの際のそれぞれの要素の重み付けは固定されており、どの段階でスコアフュージョンするかという部分にフォーカスされていた。各要素において認証スコアの傾向がある場合は固定された重み付けが良いが、ユーザ毎に各要素の認証スコアのばらつきがある場合にはユーザ毎に適切な重み付けをした上でスコアフュージョンをするべきである。このため、本研究ではユーザ毎に異なる各要素の重み付けが必要な場合でのスコアフュージョンの手法としてニューラルネットを用いた手法を提案し、他の手法と比較検討する。

キーワード: 多要素認証, スコアフュージョン, 重み付け, ニューラルネット

Application of neural network to score fusion in multi-factor authentication

KATSUYA MATSUOKA^{1,a)} MHD IRVAN¹ RYOSUKE KOBAYASHI¹ RIE SHIGETOMI YAMAGUCHI¹

Abstract: Recently, information security has attracted more interest. Personal authentication, such as knowledge authentication and biometric authentication have become more important than ever. In this study, we focus on score fusion in multi-factor authentication, a type of personal authentication. There are previous studies on score fusion in multi-factor authentication. However, Most of these studies are focused on level of score fusion (e.g. decision level, score level, feature extraction level) and the weighting factor on score fusion is fixed. These methods work well when there is a tendency of authentication score in each factor. However, if there is no tendency, the score fusion should be performed using weighting value depending on each user. In this study, we propose a user dependent weighting score fusion using neural network.

Keywords: multi-factor authentication, score fusion, weighting, neural network

1. 序論

本章では本研究の背景と目的について説明する。

1.1 背景

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。個人認証には大きく分けて3つの方式があり、パスワードや合言葉などの知識認証、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]。また、これらの要素を複数個組み合わせる多要素認証という方式も存在する。多要素認証は複数の要素を用いることで強力な安全な認証を実現しているため、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利用されている [2]。そして、多要素認証

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

^{a)} matsuoka@yamagula.ic.i.u-tokyo.ac.jp

においてこれらの各要素を組み合わせる際のスコアフュージョンにはいくつかの方式が存在する。これらの方式はスコアフュージョンを行うレベルが異なり、スコアレベルフュージョン、特徴抽出レベルフュージョン、決定レベルフュージョンなどがある [3]。一般的に、多要素認証における各要素には良いスコアの出やすさなどの傾向があるためスコアフュージョンの際の各要素の重み付けは固定されている [3], [4], [5], [6], [7]。このため、要素別の傾向がない場合に適したスコアフュージョン、すなわち動的な重み付けによるスコアフュージョンの方式はない。

1.2 目的

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の多要素認証の精度向上を目的とする。このため、スコアフュージョンの際の要素毎の重み付けを固定ではなく動的に行うことでユーザ毎に最適な重み付けのスコアフュージョンを実現する。これまでは多要素認証においてユーザ全体として要素別の傾向がある場合について考えられていたため、固定の重み付けによるスコアフュージョンがほとんどであった [3], [4], [5], [6], [7]。これを解決する手法として、ユーザ毎にスコアの重み付けを最適に行う手法を提案する。今回のユーザ毎の最適なスコアの重み付けにはニューラルネットワークが適していると考えたため、ニューラルネットワークを適用したスコアフュージョンの手法を提案する。具体的には、ニューラルネットワークを用いて、ユーザの要素別の傾向を学習させ、本人であるかどうかの二値分類をすることによりスコアフュージョンを実現する。

1.3 本論文の構成

本論文の構成は次の通りである。まず第2章で多要素認証におけるスコアフュージョンの関連研究と課題を説明する。第3章でその課題を解決する提案手法を説明する。次に第4章で提案手法と比較する従来の手法とその際に用いるダミーデータについて説明する。第5章で提案手法と従来の手法を比較した結果についてまとめる。最後に第6章で本研究のまとめと今後の展望を説明する。

2. 関連研究

多要素認証におけるスコアフュージョンに関する研究を調査した。特にスコアフュージョンする際の手法や各要素の重み付けに着目した。

2.1 スコアフュージョンのレベル

スコアフュージョンとは、多要素認証において単一の出力を生成するためのデータの組み合わせのことである [8]。スコアフュージョンには大きく分けて次の4つのレベルの方式がある [9]。

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 (Match score level fusion)

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]。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。ただし、マッチスコアの範囲が異なる場合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]。

2.2 複数の分類器を用いたスコアレベルフュージョン

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) を使用したスコアレベル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。

2.3 生体認証へのスコアフュージョンの適用

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要素を用いた認証方式が提案されている [4]。この手法ではそれぞれの要素のスコアを融合する際に、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。

2.4 固定の重み付けによるスコアフュージョンの課題

上述したスコアフュージョンの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で問題はないが、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。

3. 提案手法

従来のスコアフュージョンでは要素毎に傾向があると仮定して、重み付けを固定としている。このため、ユーザ毎に傾向が異なるデータに対しては適していない。そこで、この課題を解決する手法として、スコアフュージョンにニューラルネットワークを適用し、ユーザ毎に動的な重み付けを行い認証精度を高める手法を提案する。

3.1 ニューラルネットワークを用いたスコアフュージョン

ニューラルネットワークは、入力層・出力層・隠れ層から構成され、層と層の間にはニューロン同士のつながりの強さを示す重みがあり、これを調整していくことで学習する。このため、今回のユーザ毎の最適なスコアの重み付けにはニューラルネットワークが適していると考えた。そこで、ニューラルネットワークを用いた二値分類により個人を判別するスコアフュージョンの手法を提案する。本提案手法はユーザ毎に二値分類のシンプルなネットワークを構築する。ユーザ毎にモデルを構築するので、重みはユーザ毎に独立である。ユーザ毎に本人のデータとそれと同量の他人のデータを学習させ、二値分類を行う。図1に示すように入力層のユニット数は5つ、隠れ層は2層、出力層のユニット数が1つであるネットワークを構築した。今回は5要素の多要素認証について比較を行なったため、入力層のユニット数を5つとした。入力 x_1, x_2, x_3, x_4, x_5 が各要素のスコアに対応し、出力 y は本人であるかどうかの二値を表す。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。今回は二値分類のニューラルモデルのため、Binary Crossentropy や sigmoid 関数を用いた。今回のタイプでは ReLU, sigmoid, Binary Crossentropy が向いている [13] と知られているためこれらを用いた。また、RMSprop とは AdaGrad を改良したアルゴリズムのことであり、AdaGrad

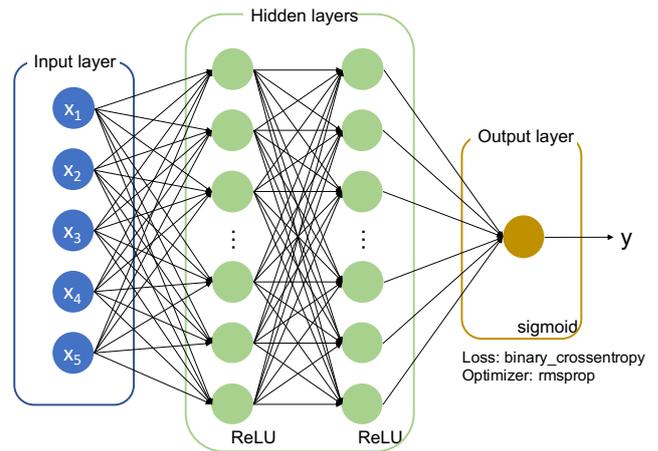


図1 二値分類のニューラルネットワーク。

Fig. 1 Binary classification neural network.

```
1 model = Sequential()
2 model.add(Dense(64, input_dim=5,
3     activation='relu'))
4 model.add(Dropout(0.5))
5 model.add(Dense(64, activation='relu'))
6 model.add(Dropout(0.5))
7 model.add(Dense(1, activation='sigmoid'))
8
9 model.compile(loss='binary_crossentropy',
10     optimizer='rmsprop',
11     metrics=['accuracy'])
```

図2 二値分類のモデルのソースコード。

Fig. 2 Binary classification model source code.

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 [14]。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。このモデルを構築した際のソースコードを図2に示す。

4. スコアフュージョン手法の比較

ユーザ毎に要素別の傾向が異なるデータについて本提案手法と従来の固定の重み付けによるスコアフュージョンを比較する。本章では、比較の際に用いるダミーデータとスコアフュージョンのそれぞれの手法について説明する。

4.1 ダミーデータの生成

本研究ではダミーデータを用いてスコアフュージョンの手法を比較した。ダミーデータはユーザ数100、要素数5とした。本提案手法ではユーザ毎にモデルを構築してニューラルネットワークの重みを独立に求めるため、精度はユーザ数に依存しない。そこで今回はダミーデータのユーザ数を100と仮定した。また、ユーザ毎のデータ数は1000、2000、3000の3種類を比較した。また、ユーザ毎に要素別の傾向があると仮定し、各要素の基準値と分散をユーザ毎

にランダムに生成する。この時、基準値の範囲は 50 から 90、分散は 10 から 20 とする。そして、各データはこの基準値と分散から正規分布に従いランダムに生成する。このダミーデータ生成のアルゴリズムを以下に示す。また本研究では、ユーザ毎に異なった傾向がある場合の多要素認証におけるスコアフュージョンについて検討しているため、このようにユーザ毎に要素別の傾向があるダミーデータを用意した。

Algorithm 1 Create Dummy Data

Require: $N_{user} \leftarrow 100, N_{factor} \leftarrow 5, N_{data} \leftarrow 2000$

Ensure: $dummyData[N_{user} * N_{data}][N_{factor}]$

```

for user = 0 to  $N_{user}$  do
  for factor = 0 to  $N_{factor}$  do
    referenceValue  $\leftarrow$  random[50, 90]
    variance  $\leftarrow$  random[10, 20]
    for data = 0 to  $N_{data}$  do
      dummyData[user *  $N_{data}$  + data][factor]
         $\leftarrow$  NormalDistribution(referenceValue, variance)
    end for
  end for
end for
end for

```

4.2 ニューラルネットを用いたスコアフュージョン

本研究での提案手法であるニューラルネットを用いた二値分類により個人を判別するスコアフュージョンについて説明する。ユーザ毎に本人のデータとそれと同量の他人のデータを学習させ、二値分類を行う。この時データセット全体（1人あたりのデータ数 2000 のダミーデータ）から本人の全データ（2000 個）を抽出し、データセットの残りからそれと同量になるように他人のデータをランダムに抽出する。そして、それぞれにラベルを付けて学習させ、ユーザ毎にモデルを構築した。本人のデータ（2000 個）と他人のデータ（2000 個）のうちそれぞれ 6 割を訓練データとした。そして、残りの 4 割をテストデータとし、本人のデータを本人と判断した割合（再現率: Recall）と他人のデータを他人と判断した割合（特異度: Specifity）を用いて評価を行った。真陽性（True Positive）を TP、偽陰性（False Negative）を FN、偽陽性（False Positive）を FP、真陰性（True Negative）を TN とすると、

$$\text{Recall} = \frac{TP}{TP + FN} \quad (3)$$

$$\text{Specifity} = \frac{TN}{TN + FN} \quad (4)$$

となる。抽出する他人のデータや訓練データが毎回ランダムなため、これらをユーザ毎に複数回導出した。

4.3 固定の重み付けによるスコアフュージョン

生体認証の多要素認証でよく用いられる重み付けを固定したスコアフュージョンについてである。これは要素毎に

良いスコアの出やすさや精度などの傾向があるという仮定の下でそれに基づいて重み付けをあらかじめ固定で定義するという手法である。具体例として 5 要素の多要素認証の場合を考え、各要素を $factor_1, factor_2, \dots, factor_5$ とする。 $factor_1, factor_2, factor_3$ が同じ精度で、 $factor_4$ がその 3 倍の精度、 $factor_5$ がその 4 倍の精度である場合、各要素の重み付けを $[0.1, 0.1, 0.1, 0.3, 0.4]$ とする。そして、それぞれの要素のスコアとこの重みを掛けて足し合わせたものが最終的なスコアとなる。より一般的に、要素数を N_{factor} 、 i 番目の要素のスコアを $score_i$ 、その重みを $weight_i$ とすると、最終的なスコア $fusionScore$ は、

$$fusionScore = \sum_{i=1}^{N_{factor}} score_i * weight_i \quad (5)$$

となる。今回用いるダミーデータではこのような傾向はないと仮定しているため、固定の重み付けを適切に定めることができない。このため、今回は各要素の重みを $[0.1, 0.1, 0.1, 0.3, 0.4]$ と仮定した。また、本研究ではダミーデータを生成した際のそれぞれの基準値 $referenceValue$ とその値との差の絶対値をスコアとし、重み付けを考慮して足し合わせた値を最終的なスコアとした。これが閾値より小さいかで本人であるかの判別をした。閾値は 0 から 30 まで 0.25 刻みとし、本人拒否率 (FRR: False Rejection Rate) と他人受入率 (FAR: False Acceptance Rate) を求めた。

4.4 平均値によるスコアフュージョン

平均値によるスコアフュージョンでは各要素の重みは考えず、単純に全要素の平均値を最終的なスコアとする手法である。固定の重み付けによる手法と同様に、基準値 $referenceValue$ とその値との差の絶対値をその要素のスコアとし、その平均値が閾値を下回るかで判定した。同じく閾値は 0 から 30 まで 0.25 刻みとして FRR と FAR を求めた。今回用いるダミーデータでは全体としての要素毎の傾向がないため、固定の重み付けによる手法よりも良い精度が出ると考えられる。

4.5 多数決によるスコアフュージョン

多数決によるスコアフュージョンでは、要素毎に本人であるかどうかを判別し、多数決により最終的な判定を決めるというものである。各要素のスコアは他の手法と同じく基準値 $referenceValue$ との差の絶対値とする。これらそれぞれが閾値を下回るかを判定し、閾値を下回った数が過半数を超えた場合には本人と判定する。今回は 5 要素のデータを用いているため、閾値を下回る要素の数が 3 要素以上の場合に本人とする。これについても同様に閾値を変動して FRR, FAR を求めた。

表 1 ニューラルネットを用いたスコアフュージョンの評価指標の
平均値.

Table 1 Average value of each evaluation index of score fusion
using neural network

| データ数 | 再現率 | 偽陰性率 | 特異度 | 偽陽性率 |
|------|----------|----------|----------|----------|
| 1000 | 0.797665 | 0.202335 | 0.673690 | 0.326310 |
| 2000 | 0.854948 | 0.145052 | 0.686031 | 0.313969 |
| 3000 | 0.846102 | 0.153898 | 0.696162 | 0.303838 |

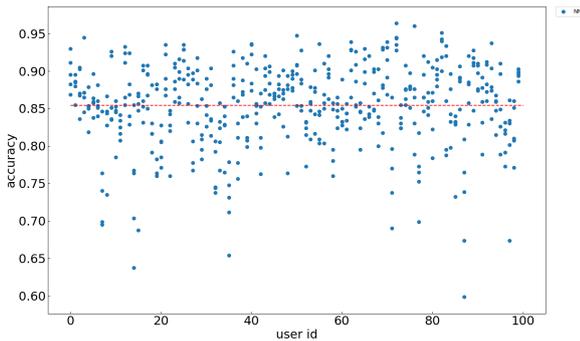


図 3 ニューラルネットを用いたスコアフュージョンによるユーザ
毎の再現率.

Fig. 3 Recall for each user of score fusion using neural network.

5. 結果

本章では、第 4 章で述べたそれぞれのスコアフュージョン
手法の比較結果をまとめる.

5.1 ニューラルネットを用いたスコアフュージョンの結果

3 種類のダミーデータ (1 人あたりのデータ数 1000, 2000,
3000) について、各ユーザに対してモデル構築の際の他人
データや学習データをランダムに変えて評価指標を 5 回
求めた。これらのニューラルネットを用いたスコアフュ
ージョンのそれぞれの評価指標 (再現率, 偽陰性率, 特異度,
偽陽性率) の平均値を表 1 にまとめる。データ数 2000 と
3000 を比較すると、評価指標の値が大きく変わらないた
めデータ数は 1 人あたり 2000 で十分であると考えられる。
このため、他の手法との比較はデータ数 2000 のダミーデ
ータを用いる。また、再現率と特異度は高いため、本人は正
しく本人と、他人は正しく他人と判定できていると言える。
次に、1 人あたりのデータ数 2000 のダミーデータに対して
ニューラルネットを用いたスコアフュージョンのユーザ毎
の再現率の結果を図 3 に示す。この再現率の値が高いほど
本人を正しく本人と認証できる。これらのユーザ全体での
平均値は 0.854948 であり、図 3 に赤破線で示した。ほとん
どの値が 0.8 以上となっているため再現率は高いと言える。

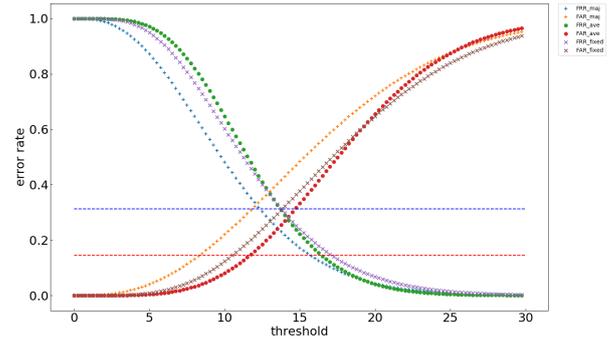


図 4 それぞれのスコアフュージョン手法別の本人拒否率 (FRR) と
他人受入率 (FAR).

Fig. 4 False Rejection Rate and False Acceptance Rate by each
score fusion method.

5.2 スコアフュージョンの比較結果

第 4 章で述べたそれぞれのスコアフュージョン手法の比
較結果を図 4 に示す。これは閾値を 0 から 30 まで変動さ
せた際の本人拒否率 (FRR) と他人受入率 (FAR) をプロ
ットしたものである。この比較には 1 人あたりのデータ数
2000 のダミーデータを用いた。平均値をとる手法、多数
決による手法、固定の重み付けによる手法の 3 つについて
比較した。また、ニューラルネットを用いたスコアフュ
ージョンでの FRR (偽陰性率) を赤破線、FAR (偽陽性率)
を青破線で示す。また、多数決による手法については水色
のプロットが FRR, 橙色が FAR, 平均値をとる手法につ
いては緑色が FRR, 赤色が FAR, 固定の重み付けによる手
法については紫色が FRR, 茶色が FAR を表している。こ
の図において、それぞれの FRR 曲線と FAR 曲線の交わる
部分がバランスの取れた閾値であると言える。この交わる
点でのそれぞれの精度を表 2 に示す。この表からわかる通
り、特異度の値はどの手法でもほとんど変わらない。しか
し、再現率に関してはニューラルネット (NN) を用いた手
法では大きく向上していると言える。

6. 結論

本章では本研究のまとめと今後の展望について述べる。

6.1 まとめ

従来のスコアフュージョンの課題として、スコアの傾向
がユーザ毎に異なる場合に固定の重み付けによるスコア

表 2 各スコアフュージョンの評価指標.

Table 2 Evaluation index of each score fusion method.

| | 再現率 | 偽陰性率 | 特異度 | 偽陽性率 |
|-----|----------|----------|----------|----------|
| 多数決 | 0.664970 | 0.335030 | 0.678885 | 0.321115 |
| 固定 | 0.686010 | 0.313990 | 0.691505 | 0.308495 |
| 平均 | 0.728840 | 0.271160 | 0.714710 | 0.285290 |
| NN | 0.854948 | 0.145052 | 0.686031 | 0.313969 |

フュージョンが適していないという問題があった。この課題に対し、本研究ではニューラルネットを用いた二値分類によるスコアフュージョンの手法を提案した。従来の手法としては、固定の重み付けによるスコアフュージョン、平均値をとるスコアフュージョン、多数決によるスコアフュージョンなどがある。これらの手法と提案手法に対してダミーデータを用いて精度の比較を行った。この比較結果から、本提案手法により要素別の傾向が異なる場合のデータについての精度が向上したことを確認した。

6.2 今後の課題

今後の課題としては、実データへの適用などが挙げられる。今回は、比較をわかりやすくするためにダミーデータを作成し、それを用いて比較を行った。しかし、実用に向けて、実データを用いた実験・比較が必要であると考えられる。また、モデルをより改善し、精度を向上させることも今後の課題として考えられる。

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] 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] 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.
- [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] Flynn P.J. Connaughton R., Bowyer K.W. “fusion of face and iris biometrics”. *Advances in Computer Vision and Pattern Recognition*, 2013. (Accessed on 08/11/2019).
- [9] G Hemantha Kumar and Imran Mohammad. “research avenues in multimodal biometrics”. *International Journal of Computer Applications*, 01 2010.
- [10] Jones Siphon-J Matse. “multi-factor biometrics: An overview”. <https://pdfs.semanticscholar.org/cf02/30fd9b16cdf0d03835d8a758ebe62eff0698.pdf>, 11 2014. (Accessed on 08/11/2019).
- [11] Arun A. Ross Anil K. Jain Karthik 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] Francois Chollet. “*Deep Learning with Python 1st Edition*”. 2017.
- [14] Geoffrey Hinton. “lecture 6e rmsprop: Divide the gradient by a running average of its recent magnitude”, coursera: Neural networks for machine learning. https://www.cs.toronto.edu/~tijmen/csc321/slides/lecture_slides_1ec6.pdf. (Accessed on 08/21/2019).