（様式５）

学 位 論 文 要 旨

西暦　2022 年　　7 月　27 日

学位申請者
釜石　智史　　印

学位論文題目

覗き見耐性を有し多人数の利用に対応可能な空中筆記による本人確認手法に関する研究

学位論文の要旨

本人確認は，様々なサービスを安全に利用するのにおいて必要不可欠であり，状況に応じていくつかの種類が用いられている．最も一般的な文字列パスワードは，任意に変更可能であるという利点を持つが，覗き見などで推測された場合には攻撃者も入力できてしまう．
推測されにくいようにパスワードを複雑にしてしまうと，覚えておくことが困難になり，簡単にしてしまうと攻撃耐性が低くなる．一部のスマートフォンで用いられているように，パスワードの代わりに指紋や顔の情報を使用することも可能であるが，これらは簡単には変更できない情報であり，漏洩した場合の問題は大きい．特に指紋は偽の指を作ることで攻撃者が突破できてしまう．

本人確認を強化する手段としてライフログや，セキュリティデバイスを使う方法がある．これらは単体で本人確認をするよりもパスワードなどと併用し，2段階の本人確認として使われることが多い．ライフログは個人を識別するものではなく，一定割合の攻撃者を対象から除外するために使われる．しかし，ライフログが漏洩してしまうと攻撃者に行動を真似されて，セキュリティを突破されてしまうことと，GPSなどのログなのでプライバシー侵害を受ける危険性がある．セキュリティデバイスはデバイス本体の管理がずさんだと盗まれたり，なくしたりする危険性がある．デバイスがなくなった場合は再発行までサービスが使用できなくなることも問題である．

以上より，情報漏洩のリスクや変更・再発行のコスト，人間の確認能力に依存しない性質などを考慮すると，
パスワードが最も無難な選択肢であることは間違いない．しかし，パスワードも上述した通り万能ではない．

そこで本研究では，Leap Motionを用いて空中に指で文字を筆記させることによる本人確認を行うことを提案した．本研究は3つの研究で構成されており，3つの研究で共通して空中に書くことで，筆跡を残さず，覗き見によるコピーに対して耐性を持つことができることと，本人確認デバイスの再発行を行わないことを目的とした．本研究の最終的な目的は，補助的にパスワードなどによる本人確認を強化することにある．ICカードやセキュリティトークンのような，本人のみが所有するデバイスは，再発行が迅速に行えないこと，盗難された場合に攻撃者に使用されてしまうことが問題であるため，本研究ではこの点を改善する．

1つ目の研究では，空中に手書きで署名を書かせることで，筆跡を残さないようにすることで，ショルダーサーフィンや，筆跡をなぞられることを防ぎ，更に，筆記した署名が流出しても，登録する文字を変えることで，特徴を変更し，簡単に真似できないようにすることを目的とした．これにより本人確認デバイスの再発行を行う必要がなく，覗き見によるコピー

に対してある程度の耐性を持ち，一度の覗き見によるコピーを行わせないことを目的とした．

この研究ではLeap Motionを使い空中に指で署名を書き，書いた署名と登録されている署名がどれぐらい似ているかで個人の検証を行う．Leap Motionでは人差し指のX，Y，Z軸の座標と加速度の6つの特徴を記録する．登録時の署名は好きなものを書いてもらい，検証時も同じものを書かせる．これらの比較にはDTWを用いる．DTWで6つの特徴1つずつの類似度を求め最も類似している署名が登録のものであれば，検証成功とした．5人の被験者で検証した結果，本人拒否率は46%で，他人受入率は11.5%となった．この研究で登録した署名は人によって違う文字だったため，ある程度は分類することはできていたが，仮に同じ文字を登録した場合は，DTWによる比較では登録してある同じ文字の署名2つと比較したときに，どちらも類似度が同じぐらいになると考えられるため，分類の精度が悪くなると考えられる．更に人差し指の動きの特徴だけではなく，ほかの指など取得する特徴をさらに増やし，個人の差をさらに大きくすることで，分類の精度を改善することができると考えた．そこで，DTWでは検証6つの特徴だけでも時間がかかるため，特徴量を増やしたら遅くなることを考え別の方法を考える必要があった．

そこで2つ目の研究として，取得する特徴量を増やしたうえで，署名を筆記させるのではなく，単純な入力にすることで，同じものを書いても正しく分類できるようにし，機械学習の一つである，自己組織化マップを用いて本人領域を分け，領域の大きさから閾値の設定を行うことにより，検証速度と，精度の向上を目指した．前の方法では人差し指の軌跡しか認識させず，ほかの指は誤検出防止のため認識しないようにしていたため，個人の特徴の差を大きくすることができなかった．特に，筆記するときに指の動きが小さいとLeap Motionが認識できなかったり，誤検出を起こすことがあったりした．そこで，この研究では，Leap Motionへの入力を，筆記するような細かい動作から，手を単一方向に動かすという簡単な動作にした．その代わりに，すべての指を認識させるようにするなどして，手から取得するデータの数を増やした．これにより，個人の差を大きくできると考えた．これにより，前の方法と比べてLeap Motionでの入力は単純にできるうえ，更に，5本の指すべての動きを真似しなくてはならないため，前の研究よりも模倣するのは難しくできると考えた．

このシステムを検証するために専用の装置を作り，全員の指の動きの大きさを同じになるようにした．特徴量も前の研究では6個だったのに対して109個に増やした．これにより取得したデータを，SOMを用いて検証を行った．結果として，SOMの本人領域の半径が9の時本人拒否率は14%となり他人受入率は10.29%となった．前の研究より改善しているが，特徴量が多すぎるせいで特徴がつかめなくなってFRRが上がった可能性があるため，特徴の数については減らす必要があると考えた．この研究の問題点として，一方向しか入力しないので，覗き見をしなくても，何回も試していれば突破できてしまうのではないかと考え，単一方向の1つのデータだけでなく，1回の入力で複数の方向を組み合わせて入力させるのが良いのではないかと考えた．

そこで考えたのが，入力した単語を色々な方向ごとに分解し，分解したデータ1つ1つを機械学習で検証し，最も分類された数が多かった人を本人とする方法である．これにより，空中で文字を書くことで覗き見に対しての耐性を確保できるうえ，登録時と検証時で同じ文字を書かなくても本人として検証できるのではないかと考え，3つ目の研究に行きついた．

そこで3つ目の研究では，1つ目の空中で署名を筆記する研究と，2つ目の機械学習を使用して一方向のみで検証する研究を組み合わせ，空中での筆記動作を分解することを提案した．これにより，検証時に登録時と違う単語を書いても本人の検証をできるため，覗き見や録画攻撃の耐性が高くできるうえ，検証するときには好きな単語でいいため，単語を覚えておく必要がないという利点がある．このシステムは登録フェーズと個人識別フェーズに分かれている．

登録フェーズでは，利用者は，システムから入力を求められる個数の単語を，Leap Motionを使用して筆記して入力する．Leap Motionで取得する特徴は54個である．利用者が入力した筆記情報は，筆記を分解するための訓練済みモデルに入力され，筆記時の特徴として分解される．

筆記の分解のためのモデルの作り方は，4つの向きを作った専用の実験装置で入力させ，これらを訓練することでモデルを作る．Leap Motionで取得したデータは時間により長さが異な

るため，線形補間により長さを統一する．そして機械学習により，4つに分類する．機械学習は複数使用し，評価することで最良のものを決める．このようにして筆記分解用のモデルを作る．

筆記の分解は，単語を筆記したデータを線形補間により伸縮させたものを複数用意し，それらを一定の長さで切り分けていき，サンプルを複数作り出す．作られたサンプル全てを分解用のモデルで分類を行い，出力されるソフトマックス値の高さから高い順に決められた個数のサンプルを抽出する．これによって1単語のサンプルを用意する．抽出されたサンプルを被験者ごとで分け，これらを機械学習により訓練を行うことで個人を分類するためのモデルを作る．これにより作られたモデルが検証で使用される．

個人識別フェーズでは登録フェーズと同様に単語の分解を行う．分解された単語を，個人を分類するためのモデルに入れ，本人であるかの閾値を超えているかで検証を行う．評価を複数の機械学習で行い，結果が最良の機械学習で，登録者の本人拒否率を5.7%とする閾値0.5で未登録者による他人受入率を7.2%に，登録者の本人拒否率を10.7%とする閾値0.7で未登録者による他人受入率を2.6%にできることを示した．

本論文で提案した空中筆記による本人確認手法は，指紋などの身体的特徴を利用した生体認証と異なり，登録内容を変更可能な行動的特徴と本人の癖である身体的特徴の組み合わせを利用したものである．

筆記時の手の動きそのものを機械学習で分類するのではなく，手の動きを分解して利用することで，再登録することなく入力する単語を変更できる点が特徴である．

本手法を実装したシステムは，既存のパスワードによる個人識別を強化するために補助的に使用されるものであり，利用者は本システムの使用を選択可能である．本手法は，今後の電子決済やオンライン投票における不正防止技術のひとつとして有効であると考えられる．

（様式６）

Ｓｕｍｍａｒｙ

Applicant for degree:
Satoshi Kamaishi

Title of thesis ：

Research on an identification method using aerial writing that is resistant to peep and can be used by a large number of people

A common string password can be guessed by an attacker. If passwords are made too complex to be easily guessed, they will be difficult to remember, and if they are made too simple, they will be less resistant to attack. Fingerprints and facial information used in some smartphones can be used, but since these cannot be changed, there are significant problems if they are compromised. There are methods to strengthen identity verification, such as lifelogging and using security devices. In this study, we proposed a method of identity verification using Leap Motion, in which the user writes letters in the air with his or her finger. The goal was to write in mid-air without leaving any handwriting and to make it resistant to copying by prying eyes. In the first study, we verified identity by comparing the words written in the air with the registered words. The rejection rate was 46%, and the acceptance rate was 11.5%. One problem with this study is that the same words cannot be registered by different registrants. Furthermore, once a word was recorded, it could be easily imitated. Therefore, in the next study, we registered a single line that was written in the same way by all registrants, and used machine learning to classify the line to improve speed and accuracy. The results showed that the rejection rate was 14% and the acceptance rate of others was 10.29% when the radius of the SOM's identity region was 9. This research is a system that strengthens the password-based identity verification by combining password input and writing of words. Of course, there are many studies that verify the identity of users by writing, but they do not take into account the large number of users and the increase in the number of users. In addition, since the system registers the entered signature itself, the signature cannot be changed without re-registering. On the other hand, the method used in this system does not require retraining by machine learning even when the number of users increases. The computational cost of machine learning can be kept constant even when the number of users is very large. The evaluation was conducted using multiple machine learning methods, and the results show that the best machine learning method can reduce the stranger acceptance rate by unregistered persons to 7.2% with a threshold of 0.5, which sets the rejection rate of registered persons at 5.7%, and reduce the stranger acceptance rate by unregistered persons to 2.6% with a threshold of 0.7, which sets the rejection rate of registered persons at 10.7%.

備　考

１．要旨は300語程度にまとめること。

２．本様式により、ワープロで作成することを原則とする。

３．用紙はＡ４版 上質紙を使用すること。