

自己組織化マップを用いたテンキーによる キーストローク認証の基礎的検討

Fundamental examination of keystroke authentication with numeric keypad using self-organizing map

勝山 貴弘^{*1} 石田 秀春^{*2} 納富 一宏^{*1} 斎藤 恵一^{*3}

Takahiro Katsuyama Hideharu Ishida Kazuhiro Notomi Keiichi Saito

1. はじめに

近年、情報セキュリティ強化を目的として、人間の身体的・行動的特徴を用いたバイオメトリクス認証が実用化され始めている。また、現在、企業や研究施設などの重要部署への入退出管理や、マンションなど集合住宅への入室時における本人認証にテンキーを用いたパスワード認証が利用されている。

現在までの研究^[1]では、水平面に置かれたフルキーボードを用いた場合の打鍵リズムによる個人認証の精度について、自己組織化マップを用いた分析により検証を行ってきた。

そこで、本研究では、行動的特徴によるバイオメトリクス認証方式のひとつであるキーストローク認証において、垂直設置されたテンキーを用い、数字4桁からなる暗証番号を打鍵する際の認証精度を実験により評価・検討することを目的とする。

本稿では、基本的検討として、キーストローク認証における実験および自己組織化マップによる分析結果について考察する。

2. キーストローク認証と自己組織化マップ

2.1 本研究におけるキーストローク認証

キーストローク認証(打鍵認証)とは、行動的特徴を利用したバイオメトリクス認証であり、特定のパスフレーズに対する打鍵間隔時間を用いて、事前に登録されたパターンと照合することで、個人を識別するものである。

本研究は、テンキーを垂直に設置した状態で、各被験者に固有のリズムにより数字4桁からなる特定の暗証番号を打鍵してもらう点が特徴となっている。

特に、数字4桁の打鍵中に意図的に長押しを入れた場合の認証精度の検証を行っている。

2.2 自己組織化マップ

自己組織化マップ(SOM: Self-Organizing Maps)とは、多次元のデータを2次元平面に配置するものとして、1982年に Kohonen によって発表されたニューラルネットワークモデルの一つである。近年では、データクラスタリング、データマイニングなどの分野で注目されている。

*1 神奈川工科大学情報工学科 Information and Computer Sciences, Kanagawa Institute of Technology

*2 神奈川工科大学大学院工学研究科 Graduate School of Engineering, Kanagawa Institute of Technology

*3 東京電気大学先端工学研究所 Research Center for Advanced Technologies, Tokyo Denki University

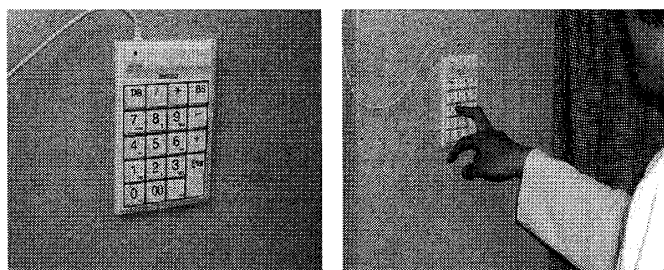
本研究では、打鍵間隔時間から各個人のキーストロークパターンを生成し、これを属性ベクトルとして SOM で学習し、SOM マップを用いて個人を認証する。

3. 実験

3.1 実験方法

被験者として、本学の学生 10 名に協力してもらい実験を行った。被験者には、垂直に設置されたテンキーに対して自身が打ちやすい位置に立ってもらい、入力を行った。また、テンキーの設置位置は、身長差による影響を出さないために被験者の肩の高さに合わせた。入力する際に使用する指の本数に関しては個人に任せ、特に指定はしなかった。

今回の実験では、4桁の入力を単純にリズムのみで行う場合と、4桁の中に1回以上長押しを入れて行う場合の二種類について計測した。また、実験で使用したテンキーと実験風景を図1の(a)、実験風景を図1の(b)に示す。なお、このテンキーは、BTK-U02/WH (BUFFALO 製)のUSB接続の外付けキーボードである。



(a) テンキー

(b) 実験風景

図1 実験で使用したテンキーと実験風景

3.2 実験条件

3.2.1 第一実験

第一実験では1つのキーのみを使用し、計測を行った。被験者には4桁の入力をテンキーの“5”のみを使用し、リズムのみでの入力と、リズムの中に1回以上長押しを入れたものを、各10回ずつ入力してもらい計測を行った。

また、この実験に関しては、高さの比較を行うため、肩の高さから30cm下げた位置にテンキーを設置した場合についても計測も行った。

3.2.2 第二実験

第二実験では2つのキーを使い、手の左右の動きの影響について計測を行った。被験者には4桁の入力をテンキーの“4”と“6”を使用し、第一実験と同様に、リズムのみでの入力と、リズムの中に1回以上長押しを入れたものを、各10回ずつ入力してもらい計測を行った。

3.2.3 第三実験

第三実験では2つのキーを使い、手の上下の動きの影響について計測を行った。被験者には、4桁の入力をテンキーの“8”と“2”を使用し、第一実験および第二実験と同様に、リズムのみでの入力と、リズムの中に1回以上長押しを入れたものを、各10回ずつ入力してもらい計測を行った。

4. 結果

評価には、他人受容率 (FAR : False Accept Rate) と本人拒否率 (FRR : False Reject Rate) を用いた。FAR, FRR の定義式を以下に示す。

$$FAR = \frac{\text{他人受容回数}}{\text{試行回数}}$$

$$FRR = \frac{\text{本人拒否回数}}{\text{試行回数}}$$

また、今回は第二実験と第三実験の長押しを入れて入力してもらった場合の分析結果を表1、図2、および図3にそれぞれ示す。

分解能の関係上、FAR, FRR の交点の値は必ずしも出力できないため FAR, FRR が最も近い閾値を採用した。またこの図に関しては、5人分のデータを平均して求めたものである。

表1 実験の分析結果

	閾値	FAR[%]	FRR[%]
第二実験	21.4	10	12.5
第三実験	14.8	7.5	6.6

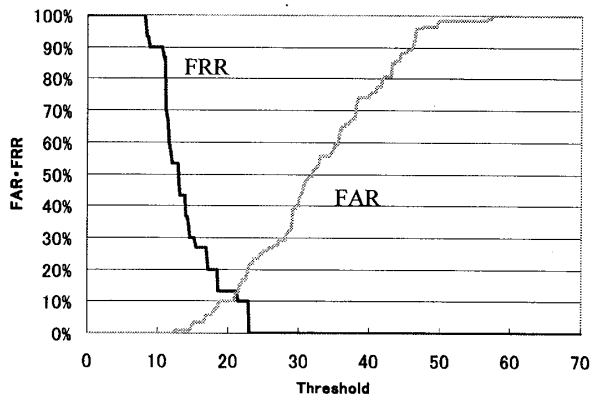


図2 第二実験の分析結果

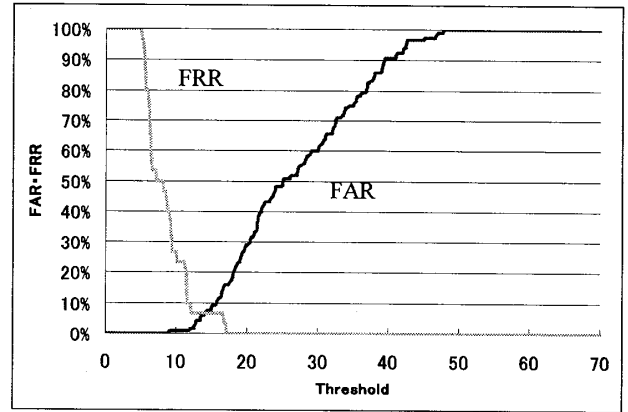


図3 第三実験の分析結果

グラフより、入力する際に長押しを入れた場合に、左右の動き (第二実験) と上下の動き (第三実験) とで FAR および FRR はそれぞれ異なる値となったが、いずれの場合でも認証精度が 80% を超える結果が得られた。

5. 考察

今回の結果から、テンキーを垂直に設置し暗証番号4桁の中に長押しを入れた場合、80%を超える精度となった。先行研究^[1]では、8文字のパスフレーズの入力に対する認証精度は95%程度であった。今回のように打鍵数が少なくても長押しを入れた場合は、認証精度が比較的高く、精度の維持に有効性があると言える。実験結果を見比べると、精度がそれぞれ異なる結果となったが、これは実験の際に使用する指の本数を指定しなかったため、左右の動きと上下の動きでリズムに差が生じたためと考えられる。

今回の実験では、単一キー、左右2キー、上下2キー、のそれぞれについて分析し検証を行った。しかし、最大2つのキーだけを使って暗証番号とすることは考えにくい。よって、今後は他のキーの組み合わせを使った場合についてさらに検討していく必要があると考えられる。

6. おわりに

今回、テンキーを垂直に設置した状態で検証を行った。実験の結果から、長押しを入れた場合、左右の動きと上下の動きの影響については、それぞれの精度が80%を超え、個人の特徴が出ていることが確認できた。

今後は、4桁の中でさらに多くの組み合わせを使った場合について検討していきたい。

参考文献

- [1]石田秀春, 納富一宏, 斎藤恵一: 自己組織化マップを用いた打鍵リズムによる個人認証, 第24回ファジィシステムシンポジウム, TF1-4, (2008).
- [2]小谷賢太郎, 法岡泰樹, 堀井健, “テンキーパネルを用いた打鍵認証システムの構築と評価”, ヒューマンインタフェース学会論文誌, Vol.7, No.1 (2005).
- [3]小越康宏, 日名田明, 広瀬貞樹, 木村春彦 “打鍵間時間を基にした認証システムのリズム打鍵による改善”, 情報処理学会論文誌, Vol.44, No.2 (2003).