仮想スティックを用いた生体認証とパターンロックへの応用
Biometric Authentication Using a Virtual Stick and Its Application to Pattern Locks

原田 侑弥
Yuya Harada
法政大学情報科学部ディジタルメディア学科
E-mail: yuya.harada.8e@stu.hosei.ac.jp

Abstract

In recent years, many people have become able to handle personal information using smartphones. As a result, higher levels of security are required for smartphones. The pattern lock is a method of personal identification on smartphones. There are many kinds of patterns that can be created, and unlike PINs and passwords, this method is easy to handle because it requires only one shape to remember. However, this method has possibilities that the pattern can be guessed from the fingerprints on the screen and that the pattern can be peeked. Therefore, it is necessary to improve the security. This paper proposes introducing biometrics authentication using a virtual stick and applying it to pattern locks. It presents an implementation that draws a pattern by manipulating a cursor with a stick and performs biometrics authentication based on finger sizes and positions, operation times, and sensed accelerations. In the experiments, subjects drew four types of shapes (triangles, rectangles, rhombuses, and stars) ten times for registration and authentication, and the equivalent error rate was examined. The experiments achieved equivalent error rates of 10% for these shapes.

1. はじめに

近年，スマートフォンの普及により，多くの人がスマートフォンを用いて個人情報を扱うことができるようになった．そのためスマートフォンに，より高度なセキュリティが求められるようになっている．スマートフォンでの個人識別には，PIN やパスワードなどの文字入力を行う手法が一般的である．これらの方法では文字列や数字列を覚える必要があるため，認証コードが長くなるほどそれを覚えにくくなる問題がある．

画面上の点をつなぎ特定の形を作ることで認証を行うパターンロックがある．作成できるパターンの種類は多く，PINやパスワードとは異なり，1つの形を覚えればよいため扱いやすい認証手法である．しかしこの方法では画面上の指の跡からパターンを推測されてしまう可能性や，パターンが覗き見されてしまう可能性があるため，よりセキュリティを向上させる必要がある．

本研究では，これらの問題の解決を目的として，生体認証を適用したパターンロックに対して仮想スティックを導入することを提案する．一般的にパターンロックは指でパターンをなぞるが，仮想スティックという画面上に表示したスティックを用いることで画面上のカーソルを動かしパターンを描画する．また，パスワードが流出した場合に備えて本手法に行動的生体認証を導入する．特徴として仮想スティックを用いて 3×3 の点をつなぎパターンを描画する際取得できる 指のサイズ，仮想スティックの X 軸，Y 軸の座標，通過時間，スマートフォンに働く加速度の値，ジャイロセンサーによって取得した X 軸，Y 軸，Z 軸の傾きを記録し，これらの値を用いて生体認証を行う．実験では 10 人の被験者が 4 つの指定したパターン描画を行う．パターンの点を通過した際の特徴を収集し，特徴量を計算する事でそれぞれの認証率を計算する．この結果全てのパターンで 87.65%以上の認証率，最高で 93.80%の認証率を記録した．

2. 関連研究

行動的生体認証とは，入力の速度や指圧などの行動的な特徴を用いて認証を行う手法である [1]．入力者ごとの特徴を用いた認証のため，パスワード入力による認証や指紋などの静的生体認証よりも盗難やハッキングの危険性が低いことが特長である．しかし，静的生体認証よりも認証精度が低いため，本人の入力も拒否してしまう場合がある．よって，行動的生体認証は認証精度を上げることが課題である．Yuhua ら [2] は PIN に対して行動的な生体認証を導入し，適切な特徴の選択と仮想の特徴生成により等価エラー率 0.12%を達成した．星野ら [3]はピクチャーパスワードに対して操作時の軌跡とデバイスの傾きに基づいた特徴量を用いた生体認証を行った．実験の結果，軌跡では 2%，傾きでは 12%の等価エラー率を達成した．実験から，図形の全形が複雑なほど認証精度が上がると考察された．また，軌跡が大きく移動しないなぞり方だと傾きが変化せず，認証精度が下がってしまったと考えられている．山田ら [4]はスマートフォンのフリック操作，タッチジェスチャーを用いた個人識別手法を提案した．実験の結果，フリック操作では 20%の等価エラー率，タッチジェスチャーでは 15%の等価エラー率を達成した．牧野ら [5]はパターンロック入力の軌跡とスマートフォンの傾きを特徴として利用した個人識別の手法を提案した．この手法では軌跡と傾きそれぞれ等価エラ

Supervisor: Prof. Hiroshi Hosobe

一率 25%を達成した．また，軌跡と傾きを組み合わせた認証方法では 10%以下の等価エラー率を達成した．しかしこの手法の課題として，画面端の操作が多いほど画面操作が不安定になってしまい，入力の再現性が低いことが挙げられている．また複雑な図形ほど認証率は上がるが，被験者からは操作がしにくいことが報告された．これらの結果から，タッチジェスチャーやパターンロックに対する生体認証の導入は等価エラー率が高くなってしまう問題がある．

仮想スティックの研究として平沼ら [6]の片手操作を目的とした仮想スティックの研究がある．実験より，仮想スティックにより手の疲労や快適さは向上するが，微調整を伴う操作はエラー率が高くなるとわかった．

3. 準備

認証を行う際，本人の特徴に対して本人の入力が失敗する確率を本人拒否率(FRR)，別人の入力が認証に成功してしまう確率を他人受入率(FAR)と呼ぶ [1]．FRR と FAR の式を以下に示す．

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

$$\mathrm{FAR} = \frac{\text{他人受入回数}}{\text{他人の試行回数}}$$

等価エラー率(EER)は生体認証の評価指標である [1]．認証のために入力された特徴は全て特徴量を持つ．特徴量が設定した閾値を達成すると認証に成功するため，閾値を厳しくすると FRR が上がり，FAR が下がる．適切な閾値を設定し，FRR と FAR が一致した値が等価エラー率である．EER が低いほど精度の良い認証プログラムであると言える．認証精度は以下の式で求められる．

$$\text{認証精度} = 100 - \mathrm{EER}$$

4. 提案手法

本研究では，画面操作が不安定になってしまう問題と画面の痕跡からパターンが推測されてしまう問題の解決を目的として，生体認証を適用したパターンロックに対して仮想スティックを導入することを提案する．仮想スティックとは，画面上に表示されたスティックであり，このスティックをスライドさせると画面上のカーソルを動かして操作を行うことが可能となる．仮想スティックを用いることで画面端の操作がなくなり，端末の傾きが少なくなることで，手を滑らせる，端末を落とすといったことがなくなる．そのため端末を安定して操作できるようになり，再現性を向上できる．また画面を指でふさぐことがないため，桂馬のような動きを伴う複雑なパターンの描画も行いやすくなることが期待される．操作が仮想スティック付近のみで行うことができるため，画面に入力の跡が残りづらいことも特徴である．これによりパターンの形が盗難されづらくなる．

パターンロック画面では画面下部に仮想スティックを表示し，画面上部にパターンを描くための点を 9 個表示する．仮想スティックによってカーソルを動かし，カーソルが通過した点をつなぎパターンを描画する．登録ではユーザーが数回ほど登録用のパターンを入力する．この時，登録者の特徴を収集する．認証では，描画されているパターンが登録されているパターンに一致した時点で入力を終了し，その時点でのユーザーの特徴と，登録されている特徴の比較を行う．特徴が本人であるとされれば認証成功となり，ロックが解除される．特徴の比較は入力された特徴の特徴量という値を算出することで行う．この特徴量が設定した閾値を達成すると認証成功となる．特徴量の計算式を以下に示す．

$$\text{特徴量} = \sum_{i=1}^{m} k_i$$

ただし，mは収集した特徴の数であり，kは以下の式で定められる．

$$k_i = \frac{\left|\text{登録した特徴}i\text{の平均値} - \text{入力した特徴}i\text{の値}\right|}{\text{登録した特徴}i\text{の平均値}}$$

図 1 に提案するパターンロックの画面と操作の様子を示す．図では星形を描画する際の操作をしている．通過していない点は白く，通過した点は赤く表示する．すでに繋がれた点同士や，直前に通過した点からカーソルまでを線で表示することで現在の操作状況がわかりやすくなっている．仮想スティックの操作は図 2 のように親指で行うことを想定し，スティックを大きく実装した．

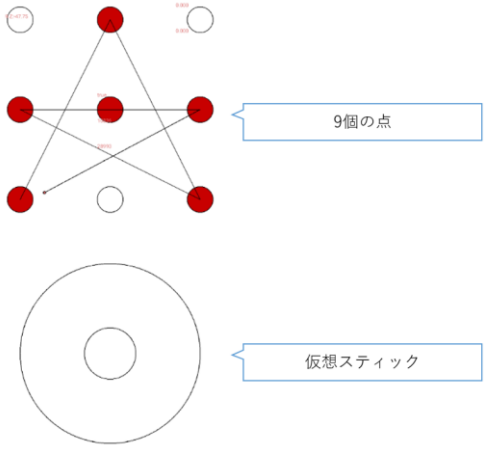

図 1．仮想スティックを用いたパターンロック

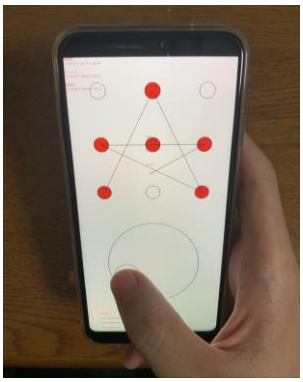

図 2．操作している様子

5. 実装

実装での使用言語は Java，開発環境は Android Studio，使用端末は HUAWEI P20 lite とした．仮想スティックはスティックが中心から離れるほどカーソルの移動速度が上昇するように実装した．また速度の調整を簡単にするため，平沼ら [6]の仮想スティックの操作範囲よりもサイズを大きくしている．パターン描画の際は通過した点を赤く描画し，最後に通過した点からカーソルまで線を伸ばすことで使用者が描画の状況をわかりやすくなるように実装した．通常のパターンロックでは同じ点を 2 度通ることはないが，本研究の実装では最初の点と最後の点は同じとする．この時，これらの点では 2 回分の特徴を収集する．

6. 実験

本研究では仮想スティックを用いたパターンロックに対する生体認証の認証率を実験により調べた．被験者は普段スマートフォンを扱っている 20 代の男女 10 人である．実験は，操作を利き手のみで行う，椅子に座って操作する，肘を机の上に置くなどして固定しないという条件で行った

6.1. 手順

本実験ではパターン入力の形や順番自体がのぞき見によって流出した場合を想定して，同じ形の図形を，指定された点の順番で描画する．使用する図形は牧野ら [5]の行った実験で使用されたものを用いる(図 3)．被験者は練習としてそれぞれの図形を 10 回ずつ描画する．その後，それぞれの図形を被験者の特徴登録用のデータ 5 回と，認証用のデータ 5 回，合わせて 10 回の入力を行う．

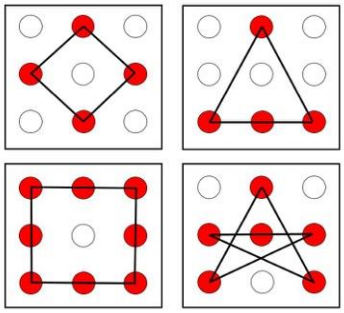

図 3. 実験で使用する図形

これらの図形では点を通過する際の特徴を収集して生体認証を行う．特徴は各点を通過した際の指のサイズ，仮想スティックの X 軸，Y 軸の座標，通過時間，スマートフォンの加速度の値，ジャイロセンサーによって取得した X 軸，Y 軸，Z 軸の傾きを記録する．加速度はスマートフォンの加速度センサーを使用する，図 4(a)に示される方向に加速度を感知するとその軸の値が変動する．地球上には常に真下に重力加速度が働いているため，加速度センサーを用いることでスマートフォンの真下方向への傾きを調べることができる．ジャイロセンサーはスマートフォンに働く回転の動きを検知する．図 4(b)に示される方向に回転を感知するとその軸の値が変動する．

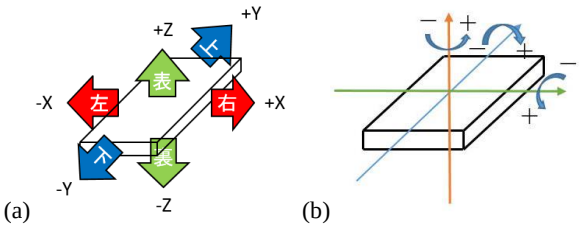

図 4. (a)加速度センサーと(b)ジャイロセンサーの方向

描画は点から点に移動する．その際，移動方向に個人差が検出されると考えたため，移動方向への仮想スティックの座標と加速度センサーの傾き，ジャイロセンサーの傾きをベクトルの回転を行うことで記録する．

6.2. 結果

提案手法で述べた特徴量に基づいて分析を行う．10 回の入力の前半 5 回の入力の平均値を求め，平均値と認証用のデータそれぞれを用いて特徴量を計算する．10 人が 5 回ずつ認証を行うため，それぞれの図形で 50 回分の認証データを集めることができる．それぞれの図形で FAR, FRR を計算して EER を出力する．それぞれの図形で EER を出力したところ，約 80%の EER となった．入力データを確認したところ，特徴の比較の際ジャイロセンサーと加速度センサーの X 軸方向の情報が特徴量の計算のノイズとなってしまうことが分かった。理由として，スマートフォン操作中にあまり機器が動かないため、ジャイロセンサーと加速度センサーの値が有意に変化していないためだと考えられる。そのため機器の揺れなどを個人差として検出してしまい、適切な個人差が見られなかった。一方で加速度センサーの Y 軸と Z 軸の値は重力加速度の影響により、持ち方を区別する値を取得する事ができた．よってジャイロセンサーと加速度センサーの X 軸の値を特徴量の計算に含めずに EER を求めることとする．

この EER を先行研究である牧野ら [5]の論文と比較する．牧野らはパターンロック操作時の端末の傾きと軌跡によって認証を行った．これらそれぞれの認証精度，またその 2 つを組み合わせた認証精度を出力しているため，これらと本実験の認証精度を比較する．また各分析によって出力された FAR，FRR を図 5 に示す．青いグラフが FRR であり，赤いグラフが FAR である．この 2 つの線分が交わっている場所が EER である．また本提案手法と牧野らの認証精度の結果を表 1，表 2 に示す．

表 1. 提案手法を用いた認証精度

認証図形	認証精度(%)
ひし形	93.80
三角形	89.61
四角形	87.65
星形	93.91

表 2. 牧野らの認証精度

認証図形	軌跡の認証精度(%)	傾きの認証精度(%)	2 つを組み合わせた認証精度(%)
ひし形	72.28	74.23	92.86
三角形	75.28	74.09	95.49
四角形	77.12	77.43	93.60
星形	77.84	79.78	94.82

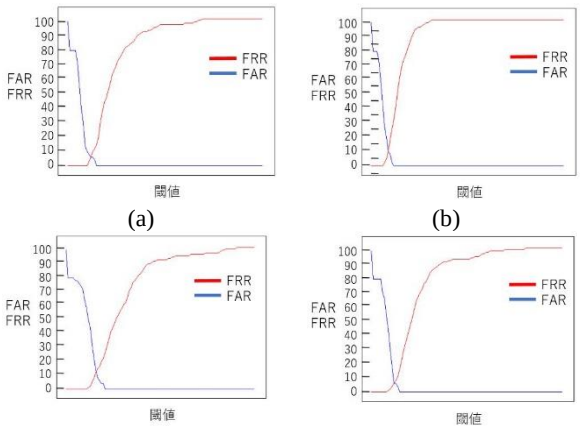

図 5. (a)ひし形，(b)三角形，(c)四角形，(d)星形の認証精度

7. 議論

実験結果より，認証精度は 90%付近であった．牧野らの軌跡と傾きを組み合わせた認証精度と比較すると，ひし形の認証精度は提案手法が高くなったが，他の図形は低い結果になった．認証に用いたデータを確認したところ，入力者によって自分の登録データと同じように入力できる人とそうでない人がいることがわかった．この原因として仮想スティックの扱いが難しいことが考えられる．特徴量からは点を通過する際の指の大きさ，通過時間，スマートフォンの傾きでは大きな差は見られなかったが，仮想スティックの座標に関して同じ入力者のデータにも差が見られた．これより，仮想スティックをより操作しやすく実装する事で認証精度が上がると考えられる．被験者からはカーソルの動きが早く，操作が難しいという意見があったため，カーソルの移動速度を入力者が設定できるように実装するべきである．これにより仮想スティックの座標に関する個人差だけでなく，点の通過時間などの個人差もより表れやすくなると考えられる．

パターン描画の際指の太さが関係ないため斜めの動きや点と点の間を移動する描画が簡単だったという意見があった．点同士の間隔が狭くても入力が可能であることから，3×3 の点配置に限らず，より多くの点を使ったパターンロックも作ることができると考えられる．一方でカーソルが小さいため，点を通過した際にカーソルを見失ってしまうという意見もあった．そのため通過した点の色に対してカーソルの色を補色にすることで，カーソルを見失わないよう実装するべきである．またカーソルの初期位置をパターンの上部に配置したが，カーソルが小さいため入力者は入力開始時にカーソルがどこにあるのか判断が難しいことがあった．よってカーソルの初期位置や大きさも入力者が設定できるように実装し，カーソルを見失わないようにするべきである．

本提案手法は仮想スティックの慣れによって入力の速さなどの特徴が変化しやすい．これを解決するためには登録データを常に最新の特徴で登録する必要がある．そこでこの手法を長期的に使用する場合，入力に成功した特徴を新たに本人の登録データに含めることで登録データを更新するなどの対策を取るべきである．

本研究の実装では，認証率に関する実験のために，繋いだ点の表示や線の描画を行った．しかし，のぞき見対策の観点からは，実用上は必要最低限の描画を行うように実装する必要があると考えられる．

8. おわりに

本研究では仮想スティックと行動的生体認証を用いたパターンロックを提案した．実験より認証精度は従来と同程度の値となった．仮想スティックを用いることで機器が安定し，加速度センサーの X，Z 軸の値を用いた認証が正確に行えるようになったが，仮想スティックの操作が難しく，一定の入力ができない場合があった．入力の精度をあげるために，より仮想スティックを使用しやすく実装する事が必要であると考えられる．

文　献

[1] 清水孝一, "バイオメトリクス：生体特徴計測による個人認証," 生体医工学：日本エム・イー学会誌, vol. 44, no. 1, pp. 3-14, 2006.

[2] Y. Wang, C. Wu, K. Zheng and X. Wang, "Improving Reliability: User Authentication on Smartphones Using Keystroke Biometrics," *IEEE Access*, vol. 7, pp. 26218-26228, 2019.

[3] 星野祐樹, 納富一宏, 斎藤恵一, "ピクチャーパスワードへの 行動的特徴量付与による生体認証手法の実用性評価," バイオメディカル・ファジィ・システム学会誌, vol. 18, no. 1, pp. 11-17, 2016.

[4] 山田健一朗, 納富一宏, 斎藤恵一, "スマートフォン操作時における行動的特徴量を利用した個人識別手法," バイオメディカル・ファジィ・システム学会誌, vol. 16, no. 1, pp. 41-48, 2014.

[5] 牧野隆典, 山田健一朗, 納富一宏, 斎藤恵一, "スマートフォンにおけるパターン認証の強化～軌跡情報および傾き情報に基づく生体認証～," バイオメディカル・ファジィ・システム学会大会講演論文集, vol. 26, pp. 25-28, 2013.

[6] 平沼一輝, "仮想的なスティックを用いた大画面スマートフォンの効率的な片手操作手法," 法政大学情報科学部卒業論文, 2019.