

スマートフォンにおけるピクチャパスワードを用いた パターン認証の強化

Enhanced Pattern Authentication Using Picture Passwords in Smartphones

市川 勘吉

Kankichi Ichikawa

法政大学情報科学部デジタルメディア学科

E-mail: kankichi.ichikawa.2w@stu.hosei.ac.jp

Abstract

In recent years, with the increase of mobile devices, threats to personal information handled by individuals are also increasing. Therefore, a high level of security is required for the authentication of mobile devices. However, commonly used authentication methods such as text-based passwords and 3-by-3 pattern authentication have their own problems. Since these depend on the difficulty of the password set by the user, the password might be easy to guess or might be peeped. Although biometric authentication is also increasing to solve these problems, the authentication might be impossible due to sensor failure. This paper proposes to place arbitrary images instead of the 9 points of pattern authentication, and to allow gesture input to be made to the first touched image. Authentication succeeds if both the drawn gesture and the pattern match a registered one. The operability of gesture input is improved by enlarging the image of the first touched point. In the experiment, ten participants were asked to draw three patterns and gestures. In addition, peeping attacks were carried out from two angles of view, and resistance to peeping attacks was evaluated to compare the proposed method with conventional 3-by-3 pattern recognition and image-based pattern recognition.

1. はじめに

近年、モバイルデバイスの増加に伴い、扱う個人情報に対する脅威も増している。よってモバイルデバイスの認証には、高度なセキュリティが求められるようになった。しかし、既存の認証方法には問題がある。一般的によく使われているテキストベースのパスワードでは、セキュリティがユーザーの記憶する文字列や数字列の複雑さに依存する。そのため、パスワードが使いまわされたり、推測されやすくなったりといった問題がある。また、画面上の3×3の点を結ぶ形をパスワードとするパターン認証がある。スワイプする箇所と順序の組み合わせは多く、タッチ操作のため直感的な操作が可能である。しかし、テキストと同様、ユーザーの設定するパスワードの難易度に依存するため、推測されやすいパスワードにな

ったり、パスワードがのぞき見されたりする可能性がある。これらの問題を解決するためにユーザーの身体的な特徴をパスワードとする生体認証も増えている。ユーザーの指紋や顔などをパスワードとすることで高いセキュリティを保つが、誤認証やセンサーの故障で認証できない場合がある。予備の認証として他の認証方法と組み合わせる必要があるため、既存の認証方法の問題解決も必要である。

本研究では、簡単なパスワードは推測されやすく、複雑にすると覚えにくいというセキュリティと利便性のジレンマの解決を目的として、パターン認証の九つの点の代わりに任意の画像を配置し、さらにその最初の画像に対してジェスチャ入力を可能にすることを提案する。点の代わりに画像を配置することで、複雑なパターンの覚えやすさを向上させる。ジェスチャ入力は、単純なパターンにもジェスチャによる選択肢を増加させ、従来よりも推測されにくくなる。これらの組み合わせにより、覚えやすくも推測されにくいパスワードを目指す。実験では10人の被験者が従来のパターン認証と、点の代わりに画像を配置したパターン認証、提案手法のジェスチャとパターン組み合わせた認証をそれぞれ指定された三種の種類で行い、認証率を記録する。また、2方向からののぞき見攻撃を実施し、従来の3×3のパターン認証とののぞき見攻撃に対する耐性を比較する。

2. 関連研究

関連研究として、ユーザーの所有する写真を用いた認証やピクチャパスワードがある。Kosugiらの写真を用いた認証[1]では、単なる点のパターン認証やテキストベースのパスワードに比べて、ユーザーが記憶する率が向上した。しかし、画像を選択するパスワードでは組み合わせが少なく、セキュリティに懸念があった。

星野ら[2]はピクチャパスワードの実用性を評価した。ピクチャパスワードとは、Windowsに採用されている任意の画像の上で、タッチパネル上での指やカーソルの動作による三つのジェスチャの入力をパスワードとするものである。画像を手掛かりとするため複雑な操作を覚えやすく、認証パターンの組み合わせもテキストベースのパスワードと比べて飛躍的に増加する。しかし、単純なパーツで構成される画像ほどジェスチャに違いが現れず、認証精度が下がることが確認された。

Andriotis らの Bu-Dash パスワード [3]は、五つの記号を 4 文字以上で組み合わせたパスワードを 3×3 のグリッド上で入力するものである。また、一つ入力するたびにグリッド上の記号はランダムに変化する。Bu-Dash はショルダーサーフィン攻撃などに對して安全であったが、特定の形状に偏って使用してしまう問題があった。

3. 提案手法

本研究では、パターン認証の九つの点の代わりに画像を配置し、さらにその画像に対してジェスチャ入力を可能にすることを提案する。画像を九つの点に固定で配置することで、従来の点を用いたパターン認証よりも複雑なパターンの記憶を可能にする。また、パターンとジェスチャを組み合わせることで、パターンだけでは単純で推測されやすかった場合でもジェスチャによる選択肢が加わるため、推測されにくくなる。

スマートフォン上でパターン認証を行うため、一つの画像は小さくなる。入力の際に触れた画像を拡大することで、操作性を向上させる。複雑なジェスチャは入力しにくく複雑になりすぎるので、ジェスチャの入力はパターンの最初の画像のみに可能とする。また、一つ一つの画像に入力できるジェスチャは、線を描く、図形を描くという 2 種類に限定し、どちらも一筆書きのみである。これにより、従来のピクチャパスワードの問題点であった、一つの画像では画像の複雑さによって認証精度が低下することを解決する。ジェスチャの入力を一筆書きとしたのは、ジェスチャを入力できる一つ一つの画像が小さいため、複雑なジェスチャの入力で操作性が下がることを防ぐためである。なお、今回の実装では四角形と円など図形による判別は行っていない。ジェスチャを入力できる一つの画像が小さいため、図形による細かい判別で操作性が下がることを防ぐためである。

パターン認証画面では画面上に九つの画像を表示し、ユーザーはこの画像を点としたパターンと一つ一つの画像に対するジェスチャをタッチパネルに描画する。登録ではまず、ユーザーが最初に選択して拡大した画像に対するジェスチャとその画像を点としたパターンを登録用に入力する。拡大した画像の範囲内から出ると、パターン入力に移り、画像に対するジェスチャ入力と最初の画像の点への通過ができなくなる。認証では、描画されたパターンとそれぞれのジェスチャの両方が、ユーザーが登録したものと一致すれば成功となる。

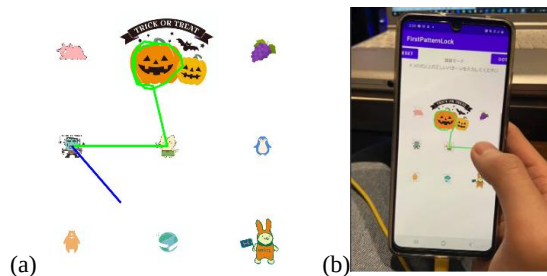


図 1 (a)ジェスチャの入力を可能にしたパターン認証、(b)操作している様子

図 1(a)に提案するパターン認証の画面と操作中の様子を示す。図ではかぼちゃの画像の点を最初の点としたパターンを描画する際の操作をしている。操作中の線を青色で、すでに繋がれた点同士やジェスチャは緑色で表示することで、現在の操作状態をわかりやすくしている。画像へのジェスチャの入力は、図 1(b)のように最初の点を拡大して実装した。最初にタップするとその点の画像が拡大する。拡大されるとその画像に対してジェスチャの入力が可能となる。

4. 実装

実装での使用言語は Java、開発環境は Android Studio、使用端末は Galaxy A41 とする。画像へのジェスチャの入力を容易にするため、3×3 の点の配置は従来のパターン認証よりも大きくしている。入力されたジェスチャの認証では描画された座標を収集し、比較を行う。座標の比較は以下のように入力された x , y 座標それぞれで平均を取り行う。

$$\text{登録座標}(x, y) = \left(\frac{\sum_{i=1}^m x_i}{m}, \frac{\sum_{i=1}^m y_i}{m} \right)$$

ただし、 m は収集した座標の数であり、 x_i と y_i は入力された座標である。完全な座標の一致では本人であっても認証が困難なため、閾値を用いて登録用の座標に範囲を持たせて、 x , y 座標ともにその範囲内にあるならば認証成功とする。 x 座標は以下のような範囲とする。

$$x - (x \times \text{閾値}) < \text{入力}x < x + (x \times \text{閾値})$$

y 座標は x 座標の計算式の x を y に置き換えたものとする。

また、ジェスチャの判定として形だけでなく、描く順番（図形ならば右回りか左回りか）を判定する。入力された座標を多角形の頂点として多角形の面積を求めて、その面積の符号が登録したものと同じかどうかで判断する。

5. 実験

本研究で提案したジェスチャの入力を可能にしたパターン認証について、その認証率とのぞき見攻撃に対する耐性を調べる実験を行った。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。実験は椅子に座り操作し、利き手のみで行った。肘を机の上に置くななどの肘を固定しない条件で行った。

5.1. 手順

使用するパターンを通過する点の数を 4, 6, 8 と変化させながら、後述の認証率を比較する。被験者は指定したジェスチャとパターンを 5 回ずつ練習する。その後、登録用にジェスチャとパターン入力を 2 回と、認証用に 5 回の入力を行う。使用するパターンやジェスチャは図 2 のものを用いる。ジェスチャが加わることで操作が難しくなるため、ジェスチャは画像の一部分を囲う単純な動作に限定した。誤った入力を行ったときは、ジェスチャとパターンのどちらで誤ったのかを記録する。

被験者には実験後にアンケートに答えてもらう。内容は、提案手法と従来のパターン認証それぞれの覚えやすさと操作性のよさを 5 段階で評価してもらうものである。また、ジェスチャの入力の際の画像の大きさが適切かと

大きさ以外でやりにくい点があるかの 2 点について自由記述をする。

認証用の入力では、異なる被験者によりのぞき見攻撃を行う。電車内やカフェなどのスペースで見られる距離で、2 方向（真横と後方）から入力を見る。攻撃者は認証を行い、画像へのジェスチャやパターンのどこまで把握できたのかを記録する。

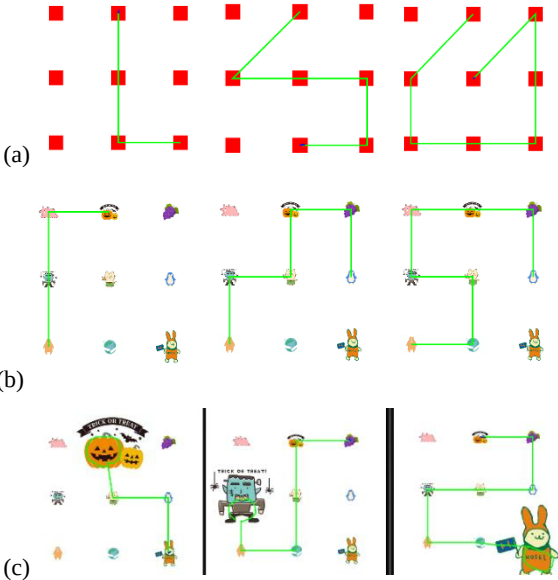


図 2 実験で使用する(a)従来手法のパターン、(b)点の代わりに画像を配置したパターン、(c)提案手法のジェスチャとパターン

5.2. 評価指標

本研究では、生体認証の評価と内部的な閾値の調整のために、本人を認証する確率である認証率と、本人であるのに認証を拒否する確率である本人拒否率、本人ではないのに認証してしまう確率である他人受入率を用いる[4]。これらの定義を以下に示す。

$$\begin{aligned} \text{認証率} &= \frac{\text{本人受入回数}}{\text{本人の試行回数}} \\ \text{本人拒否率} &= 1 - \text{認証率} \\ \text{他人受入率} &= \frac{\text{他人受入回数}}{\text{他人の試行回数}} \end{aligned}$$

5.3. 閾値の調整

ジェスチャ入力の判定に用いる閾値の調整のために、本人拒否率と他人受入率を使用する。ジェスチャの認証では、被験者の入力データと登録データの類似度を判定するための閾値を内部的に設定して用いる。本人拒否率と他人受入率はトレードオフの関係にあるので、誤って他人を受け入れるリスクと、本人を受け入れやすくして使いやすくすることを両立するために最適な閾値を決める必要がある。本人拒否率と他人受入率の一致した値を閾値として設定することで、本人が拒否されにくく他人も受け入れにくくなる適切な値とする。

5.4. 結果

認証率の実験結果を表 1 に示す。結果より、従来のパターン認証と比較して、提案手法は6~10%程度低い認証率となった。従来のパターン認証と点の代わりに画像を配置したパターン認証の認証率に大きな差は見られなかった。提案手法は最初の画像に対するジェスチャとその点を始めとしたパターンによって認証を行った。比較する従来のパターン認証と画像ありのパターン認証はパターンのみにより認証を行った。

表 1 提案手法を用いた認証率

通過する点の数	4	6	8
提案手法の認証率(%)	84	66	68
画像ありパターン認証の認証率(%)	86	84	74
パターン認証の認証率(%)	90	80	78

次ののぞき見攻撃の実験結果を表 2 に示す。結果より、提案手法は真横、真後ろどちらの方向からの攻撃でも従来のパターン認証に比べ、耐性が高いことが分かった。また、方向により他人受入率の差が大きかった。実験データの詳細を確認したところ、真横ではジェスチャの大きさと場所のどちらもものぞき見できていないことが多かった。真後ろではジェスチャの場所はのぞき見できているが、ジェスチャの大きさの細かいミスでのぞき見できていないことがあった。

表 2 のぞき見攻撃への耐性 実験結果

通過する点の数	4	6	8
提案手法の他人受入率(%)：真横	20	20	10
提案手法の他人受入率(%)：真後ろ	60	70	40
パターン認証の他人受入率(%)：真横	70	60	30
パターン認証の他人受入率(%)：真後ろ	100	80	80

アンケート結果を図 3 に示す。5 段階評価で、5 が最も肯定的である。まず、覚えやすさについては、提案手法と従来のパターン認証と比較すると、従来のパターン認証の方が覚えやすいとの回答が多かった。しかし、提案手法も 2 以下の評価はなかった。また、従来のパターン認証と点の代わりに画像を配置したパターン認証に大きな差は見られなかった。操作性のよさについては、提案手法よりも従来のパターン認証の方がすぐれているとの回答が多かった。本研究の被験者は普段からスマートフォンを扱っていたが、従来のパターン認証の操作性の評価は高くなかった。また、従来のパターン認証と点の代わりに画像を配置したパターン認証の操作性に大きな差は見られなかった。自由記述欄の一つ目の項目である、ジェスチャの入力の際の画像の大きさは適切かについては、多くが適切と答えたが、3 人が画像によってはもう少し大きくてもよいと答えた。二つ目の項目である、画像の大きさ以外でやりにくい点があるかに関しては、画像によって細かく入力しにくい、ジェスチャ入力だけでなくパターン入力も素早く入力すると範囲外に出てしまうといった意見が 2 人ずついた。

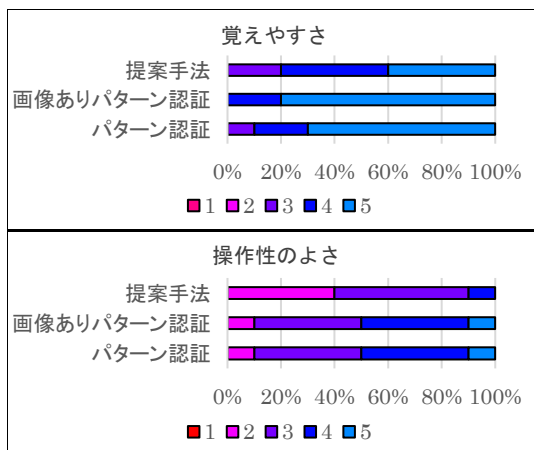


図3 アンケート結果

6. 議論

実験結果より、提案手法の認証率はどの点の数でも従来のパターン認証よりも低い結果となった。これはジェスチャの入力が加わると、単なるパターンをみの認証よりも複雑になるためである。実験後に行ったアンケート結果より、ジェスチャ入力が増えたことで複雑になったのは覚えやすさよりも操作性であると考えられる。実験データの詳細を確認しても、5回の認証で前半は成功したが、ジェスチャの操作ミスにより後半に失敗しているケースが多くみられた。これより、ジェスチャを入力しやすく実装する必要があると分かった。画像によっては入力が範囲外に出てしまったり、被験者によって入りに適切な画像サイズが異なったりしたので、ユーザーや画像によってある程度設定できるように実装すれば、認証率は向上すると考えられる。画像ありのパターン認証の認証率については従来の認証と大きな差はなかった。これは、画像があってもパターンとして記憶する人が多く、画像の順番で記憶することが難しいからだと考えられる。

提案手法のジェスチャ入力だけでなくパターン認証に関しても、通過する点の数が増えると認証率が低下した。点の数が増えて複雑化したためだけでなく、アンケート結果より実装に問題があることが分かった。具体的には、パターンを入力する際に素早く入力すると点が認識されない場合があった。本研究では提案手法、従来のパターン認証ともに実装したため、一般的なパターン認証よりも操作性が悪い部分が生じた。点の数やユーザーによって入力速度が異なることに対応する必要があることが分かった。

のぞき見攻撃の実験結果より、提案手法は真横、真後ろどちらの方向からの攻撃でも、従来のパターン認証に比べて耐性が高いことが分かった。特に真横からの攻撃に対しては、通る点が4点でも20%の成功率であった。従来のパターン認証では70%成功しているため、耐性は高いといえる。実験データを確認すると、真横からは、提案手法のジェスチャを描く最初の画像が合っているにもかかわらずジェスチャの大きさを把握することが難しいことが分かった。例えばウサギの画像にジェスチャを入力する際に、

丸で囲っていると分かっても、顔、胴体、全部どれを囲っているのかを当てることのできる被験者は少なかった。しかし、真後ろからの攻撃では、50～60%程度成功していた。真後ろからは位置や大きさが見えやすいため、攻撃の成功率が上がったと考えられる。パターン認証のみではほぼ90%ののぞき見が可能になっていたことと比較すると、耐性の強化はできているといえる。2, 3回の入力ののぞき見するだけではジェスチャの入力を完全に把握することは難しいことが分かった。

本研究では、認証率に関する実験のために、パターンの描画やジェスチャの描画の線の表示を行った。このため、真後ろからの攻撃の成功率が上がったと考えられる。しかし、実用上は必要最低限の表示だけ行えばよい。また、使用する画像に関しても実験のために統一した。ユーザーが画像の選択をできるようにすることで、のぞき見攻撃に対する耐性の向上が期待できる。

7. おわりに

本研究では、パターン認証の九つの点の代わりに画像を配置し、さらに最初に触れた画像に対してジェスチャ入力を可能にすることを提案した。実験により、認証率は従来のパターン認証より6～10%程度低い値となった。しかし、のぞき見攻撃に対しては提案手法が高い耐性を記録した。覚えやすさはあまり変わらずにのぞき見攻撃に対する耐性を向上できたが、ジェスチャの入力がうまくいかない場合があった。

今後の課題は、操作性の悪さによって入力ミスが生じる問題を解決することである。特に入力する速度によって正しい入力ができない場合があるので、素早いジェスチャの入力に対応する必要がある。また、画像によって入力が範囲外に出てしまうことや、被験者によって適切な画像サイズが異なることがあったため、画像ごとに異なるイラスト部分と画像の端との距離を統一し、画像のサイズを被験者が変更できるようにすることで、入力の精度が向上すると考えられる。

文 献

- [1] M. Kosugi, T. Suzuki, O. Uchida and H. Kikuchi, "SWIPASS: Image-based User Authentication for Touch Screen Devices," *Journal of Information Processing*, vol. 24, no. 2, pp. 227-236, 2016.
- [2] 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.
- [3] P. Andriotis, M. Kirby and A. Takasu, "Bu-Dash: A Universal and Dynamic Graphical Password Scheme," *Proc. HCI international, LNCS*, vol. 13333, pp. 209-227, 2022.
- [4] 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.