録画画像を用いた攻撃に耐性を持つ パズル型認証方式の提案

日隈　光基[a)]・山場　久昭[b)]・久保田　真一郎[c)]・岡崎　直宣[d)]

Proposal of Puzzle Authentication Method with Video Recording Attack Resistance

Koki HINOKUMA, Hisaaki YAMABA, Shin-Ichiro KUBOTA, Naonobu OKAZAKI

Abstract

Currently, user authentication methods such as PINs, passwords and so on, are used to protect important and private data in mobile devices. However, those existing methods are not sufficiently safe against shoulder surfing attacks. Attackers can easily steal PIN codes or passwords. To prevent such attacks, the puzzle authentication method was proposed. In the method, users unlock their devices thorough solving a "puzzle." A user drags an orb to adjacent positions, and the dragged orb swaps places with the orb already there. The authentication will succeed when all of the orbs corresponding to characters of the password are put into the designated positions. The special feature of this method is that users have fun while they unlock their devices. However, it was also known that the method has several drawbacks. First, the method is not strong enough against brute-force attacks. Next, the correct answer is easily revealed by shooting the authenticated screen using a video camera. In this study, several improvements were made to the method to overcome brute-force attacks and video recording attacks. The improved authentication method was implemented and experiments for evaluation were carried out.

Keywords: mobile security, shoulder-surfing, puzzle

1. はじめに

近年，スマートフォンやタブレットなどのモバイル端末が広く普及している．また，クラウドコンピューティングにより，スマートフォンからでもインターネット上に保存してあるデータを閲覧，編集できるようになってきており，モバイル端末から取得できる情報量は増加してきている．そのため，今まで以上にモバイル端末のセキュリティの向上が期待される．しかし，現在スマートフォンやタブレットなどのモバイル端末で使用されている，パスワード認証，PIN 認証，パターンロック認証などの画面ロック機能は第三者の覗き見攻撃への対策が十分ではない．この問題を解決するために，様々な手法が提案されている[1,2,3,4,5]．覗き見攻撃に耐性を持つ認証方式として，従来のパスワード方式による認証にパズルの要素を組み込み，パスワードを指定した位置に揃える，パズル型認証方式がある．この認証方式は楽しく認証することができ，ユーザビリティに配慮した認証方式である．しかし，この認証方式にはランダムな入力により偶然に認証を突破する確率が十分に低く保てないことや，ビデオカメラ等を利用した，認証画面の録画画像を用いた攻撃（録画攻撃）に対して脆弱であることなどの改善すべき点がある．

本研究では，この認証方式に改良を加え，これらの問題点を改善することを目的とする．そこで，認証時の入力を複数回に分割することにより入力情報の候補を増加させ，偶然認証突破確率を低くし，またビデオカメラに記録されにくい，端末のバイブレーション機能などを用いた情報提示手法とすることにより，録画攻撃に対して耐性を持つ新たな認証方式を提案する．

さらに，提案方式を Android 端末上に実装し，録画攻撃に対する耐性などの提案方式の評価を行う．また，ユーザビリティの評価を行うためにアンケートを実施する．

a)工学専攻大学院生
b)情報システム工学科助教
c)情報システム工学科准教授
d)情報システム工学科教授

2. パズル型認証方式

2.1. パズル型認証方式の概要

パズル型認証方式とは，従来のパスワード方式による認証に位置とパズルの要素を組み込み，パスワードを指定した位置に揃えることにより認証を行う[6,7]．この認証方式は覗き見攻撃への耐性を持つ．

この方式の認証画面には，0 から 9 の数字，および，赤，青，緑，黄，紫，白の 16 個のアイコンが 4×4 の 16 個のマスにランダムに配置されている（図 1(a)）．ユーザは，事前に登録しておいた 4 つのアイコン（パスアイコン）を，事前に登録しておいた 4 つの位置（パスロケーション）に移動させれば，認証は成功となる（図 1(c)）．図 1 では，説明のために，パスアイコンを赤色の文字で，パスロケーションに登録されているマスを橙色で示している．ただし，各パスアイコンを移動させるパスロケーションは決まっておらず，どのパスロケーションにどのパスアイコンを移動させても認証は成功となる（図 1(d)）．

ユーザは，移動させたいアイコンにタッチし，そのままドラッグすることにより，上下左右斜めのいずれの方向へも，そのアイコンを移動させることができる．その際，移動先の位置に元からあったアイコンと，場所が入れ替わる．さらに，指を離さずにアイコンを移動させ続けることにより，複数のアイコンの位置がまとめて変化することになる．このため，ユーザがパスアイコンをパスロケーションに移動させる際に，直接ドラッグするアイコンは，必ずしもパスアイコンでなくても良い．

このことから，認証画面を覗き見ても，パスアイコンとパスロケーションがどれであるのかを特定することは困難である．なおこの手法では，最初にアイコンを触ったら，認証が完了するまでは指を離さないという「一筆書き」で認証を行うものとする（図 1(b)）．

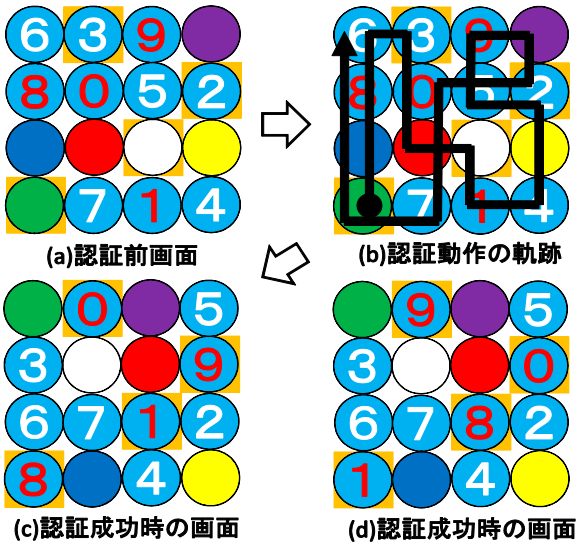


図 1. 既存手法の認証の例.

2.2. パズル型認証方式の問題点

既存のパズル型認証方式では，以下の配置再現法や出現回数推定法による録画攻撃に対して耐性が低いという問題がある．

・配置再現法：認証成功時のアイコンの配置を記録し，攻撃者がその通りにアイコンの配置を再現することで認証が成功してしまう攻撃である．既存手法では，パスロケーションとパスアイコンを固定しているため，認証情報であるパスアイコンとパスロケーションが分からなくても，認証成功時のアイコンの配置さえ記録してあれば，それと同じ配置を再現するだけで，認証を成功させることができてしまう．

・出現回数推定法：マス毎のアイコンの出現回数を数えることにより，パスアイコンとパスロケーションを推定する攻撃である．既存手法では，パスロケーションとパスアイコンを固定しているため，パスアイコンはパスロケーションの位置以外には出現しない．そのため，数多くの認証成功時の画面があれば，4 つのパスアイコンだけが現れる 4 つのパスロケーションと，残る 12 のアイコンだけが現れる 12 のロケーションを見分けることができてしまう．この攻撃は録画した認証画面の数が多ければ多いほど，成功の可能性が上がると考えられる．

また，既存手法がランダムな入力により偶然に認証が突破される確率は，

$4! \times 1/16 \times 1/15 \times 1/14 \times 1/13 = 1/1820$

である．これは，PIN 方式などの，広く用いられている認証方式に比べて高いという問題もある．

3. 提案手法

3.1 目標と設計方針

本研究では，前述した“覗き見攻撃への耐性を持つパズル型認証方式”を改良し，録画攻撃に耐性を持つ認証方式を提案する．提案方式の設計目標を以下に示す．

・録画攻撃への耐性

録画攻撃とは，ビデオカメラ等を利用して認証画面を録画した画像を用いた攻撃のことである．複数回，認証画面の録画をされても認証情報が盗み取られないことを目標とする．

・偶然認証突破確率の低減

偶然認証突破確率は，ランダムな入力により偶然に認証を突破する確率のことである．1/10,000 を強度の目標とする．1/10,000 の強度は広く用いられている PIN 方式の 10 進数 4 桁に相当する．

・ユーザビリティ

ユーザに入力の記憶負荷がかからない認証方式を目指す．

3.2 録画画像を用いた攻撃に耐性を持つパズル型認証方式の提案

提案手法では，既存手法の問題点を緩和するために，2 つの新たな改良を行う．1 つ目は，認証画面の数を増やし，認証時の入力を複数回に分割することである．2 つ目は，パスロケーションの位置が認証の度にランダムに決まり，それを，ビデオカメラに記録されにくい情報提示手法を用いてユーザに伝えることで，録画攻撃に対して耐性を持つようにすることである．以下に，2 つの新たな改良の

詳細を示す.

1 つ目は，認証画面の数を増やし，認証時の入力を複数回に分割することである．これは，入力する入力情報の候補を増加させることで，ランダムな入力により偶然に認証を突破する確率を小さくし，偶然認証突破確率を低減させることと，1 画面で入力するパスワードを減らすことで認証を簡単にすることを目的とする．既存手法では，事前に登録した 4 箇所のパスロケーションに 4 個のパスアイコンを移動させる操作を 1 画面で行っていたが，提案手法では，認証画面を 2 画面に増やす代わりに，1 画面あたりのパスアイコンとパスロケーションの数を減らすことで，覚えるパスアイコンとパスロケーションの数を増やさずに認証画面を増やすことができるようにした（図 2）．始めの認証画面で認証を終えた後，続いて 2 画面目の認証画面に遷移し，2 度の認証を終えた後に認証は完了となる．既存手法と提案手法の，偶然認証突破確率を示す．既存手法は，2.2 で示したように，1/1820 である．これに対し提案手法では，事前に k 個のパスアイコンと k 個のパスロケーションを 2 セット登録し，アイコンが m×n に並んだ 2 画面で認証を行う．今回は既存手法との比較をするため k=2，m=n=4 とする．この時の，偶然認証突破確率は，

$(2! \times 1/16 \times 1/15)^2 = 1/14400$

となり，認証画面を増やすことで偶然認証突破確率は低減する．さらに，1 画面あたりのパスロケーションに動かすパスアイコンの数を減らすことで，パスワード入力の過程でアイコンを動かせる範囲が広くなり，動作の選択肢が広がるとともに，アイコンを目的の位置に動かしやすくなるため，認証が容易になる．一方，認証画面を増やすことにより，認証時間が長くなる可能性があり，これがユーザビリティに与える影響を調査する必要がある．

2 つ目は，パスロケーションの位置が認証の度にランダム決まり，それを，ビデオカメラに記録されにくい情報提示手法を用いてユーザに伝えることで，録画攻撃に対して耐性を持つようにすることある．ここでは，ビデオカメラに記録されにくい情報提示手法として，端末のバイブレーション機能を想定するが，イヤホン等を利用している場合には音による情報提示なども考えられる．この改良により，録画攻撃への耐性が向上するとともに，ユーザが長期にわたり覚えておく必要のある情報を減らして，ユーザの記憶負荷を軽減することが期待できる．既存手法ではパスロケーションはパスアイコンと同様に事前に登録しておき，ユーザはそのパスロケーションを覚えている必要があったのに対し，提案手法ではパスロケーションは認証のたびにランダムに決定されるため，これを長期にわたり記憶しておく必要がない．

次に，情報提示手法を用いてパスロケーションをユーザに伝える方法を説明する．認証画面に表示された m×n のマスに配置されたアイコンを順になぞり，あるマスを通ったとき端末が振動する．その振動したマスがその回の認証におけるパスロケーションとなる．パスロケーションが認証のたびにランダムに決まることで，2.2 で述べた配置再現法や出現回数推定法による録画攻撃を防ぐことができる．以上のように，提案手法では長期にわたり覚えておく必要のある情報がパスアイコンのみになることで，ユーザの記憶負荷を軽減することができる．一方で，振動するパスロケーションの数が多い場合，認証の度に記憶すべき情報が多くなり，短期的な記憶負荷が大きくなるという問題がある．これは，画面を 1 回なぞるだけでは覚えきれないといった，ユーザビリティの低下につながる可能性がある．

そこで，この問題の解決策として，既存手法である事前にパスロケーションを設定する方法と，上記の振動を使ってパスロケーションを設定する方法の両方を使ったハイブリットの方式を合わせて提案する．

ハイブリットの方式は，2 種類のパスロケーションを使用することで，図 3 のように，振動するパスロケーションの数を減らし，長期記憶負荷と短期記憶負荷のバランスを図ることができる．一方で，ハイブリットの方式では，事前に登録するパスロケーションの位置は固定であるため，全てのパスロケーションを振動により決定する方式に比べて録画攻撃への耐性が低下してしまうことが考えられる．

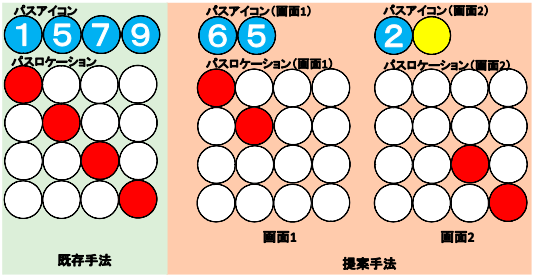


図 2.　認証時の入力の分割.

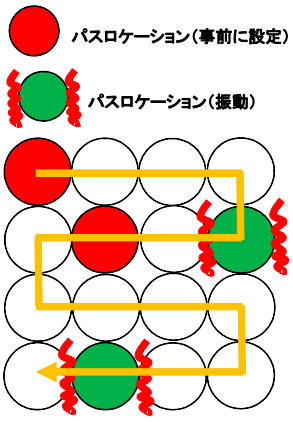


図 3.　ハイブリットの方式のパスロケーションの確認.

4.　実装と評価

4.1 実装

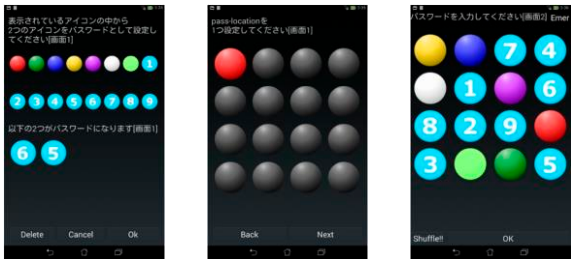
提案方式を実現させるために，実装にはJava言語を用い，開発ソフトはEclipseを使用した．動作検証を行った端末のOSはAndroidOS4.4.2である．図4にパスロケーションとパスアイコンの設定画面，認証画面を示す．

4.1.1　パスアイコンとパスロケーションの設定

図4(a)にパスアイコンの設定画面を示す．パスアイコンを登録する場合は，ユーザは登録したいアイコンをタッチする．「OK」ボタンを押すことで，同図(b)へ移行する．同図(b)にパスロケーションの設定画面を示す．パスロケーションを登録する場合は，ユーザは登録したい位置のマスをタッチする．以上の操作を2セット行うことで，2画面分のパスアイコンとパスロケーションを設定する．

4.1.2　認証

図4(c)に認証画面を示す．認証の度に端末がランダムにパスロケーションの位置を決め，そのマスを指が通過したときに端末が振動する機能を実装している．また，録音をされた場合に振動音を判別しにくくするために，ダミー音として振動音と類似の音を，振動しない時にも出力する機能を実装している．この場合，全てのマスは指でなぞった際にダミー音が鳴るようにした．「OK」ボタンを押すことで認証の成否を判定し，成功の場合，認証は完了となる．



(a)パスアイコンの設定画面　(b)パスロケーションの設定画面　(c)認証画面

図 4.　設定画面と認証画面．

4.2 認証時間と認証成功率の調査

既存手法と提案手法のそれぞれの認証時間，認証成功率を調査した．被験者として宮崎大学工学部生8人に実験を行ってもらった．

実験方法について説明する．まず被験者に実験の流れを説明し，実際に実装したシステムで数回練習してもらい，その後実験を行った．本実験では，既存手法と提案手法の認証方式でそれぞれ5回ずつ認証を行ってもらい，認証の成否と認証時間を記録した．実験で使用した提案手法の認証方式は，事前に2個のパスアイコンと1個のパスロケーションを2セット登録し，アイコンが4×4のマスに並んだ2画面で認証を行う．また，認証画面では1マス振動するマスがあり，そのマスがもう一つのパスロケーションとなる．

実験結果を表1に示す．認証成功率は，5回の認証のうち何回認証が成功したかを示している．表1より，提案手法の認証成功率は既存手法と比べて17.5ポイント低下した．認証成功率低下の原因は，端末が振動してパスロケーションの位置をユーザに伝える際，ユーザが画面を早くなぞりすぎると，どのマスで端末が振動したかがわかりにくいことが挙げられる．認証時間は，認証全体に要する時間で，認証画面が表示されてから認証が成功するまでの時間を計測したものである．表1より，提案手法の認証時間は既存手法と比べて11.24秒増加した．認証時間増加の原因は，提案手法は画面をなぞって振動するマスを確かめる作業を2画面行う必要があるため，その時間が余計にかかってしまうことが挙げられる．また，認証を失敗した場合，提案手法は再度2画面分の認証を行う必要があることも認証時間の増加の原因となっている．

表 1.　認証成功率と認証時間．

	認証成功率(%)	認証時間(秒)
既存手法	95	14.92
提案手法	77.5	26.16

4.3 ユーザビリティに対する評価

提案方式が既存手法と比べて使いやすさが損なわれていないかを確認するために，宮崎大学工学部生8人に実験の後アンケートを実施した．提案手法で追加された機能のユーザビリティを確認するための，以下の3項目の評価について述べる．

(1) 振動機能によるパスロケーションの発見は容易か
(2) 認証画面の数が増えると使いやすいか
(3) 認証画面の数が増えると認証情報を覚えるのは容易か

(1) の項目では，過半数が「容易」「やや容易」と回答しており，「少し難しい」という回答もあるが，「難しい」という回答はなかった．過半数がポジティブな回答をしていることから，振動機能でパスロケーションが決まる方法によりユーザビリティを大幅に低下させる可能性は少ないと言える．

(2) の項目では，半数が「どちらでもない」と回答しており，「少し使いにくい」という回答よりも「使いやすい」「やや使いやすい」という回答が多かった．半数が「どちらでもない」と回答していることから，認証画面の数を増やすことによるユーザビリティへの影響は少ないと言える．

(3) の項目では，半数が「どちらでもない」と回答しており，「容易」「少し難しい」という回答が同程度あった．半数が「どちらでもない」と回答していることから，認証画面の数を増やすことによるユーザの記憶負荷への影響

は少ないと言える.

4.4 録画攻撃への耐性に対する評価

先ず, パスロケーションを事前に設定せず, 振動によりパスロケーションの位置が認証の度にランダム決まる方法のみを使用した認証の場合, 2.2で述べた配置再現法による録画攻撃に対しては, パスロケーションの位置が認証のたびにランダムに変化することで防ぐことができる. また, 2.2で述べた出現回数推定法による録画攻撃に対しても同様に, パスロケーションの位置がランダムに変化することにより防ぐことができる. よって, この方法を使用した場合, 録画された回数に関係なく上記の録画攻撃に対して安全であると言える.

次に, ハイブリットの方式を使用した認証の場合, 配置再現法による録画攻撃に対しては, ランダムに変化するパスロケーションがあるため, 防ぐことができる. しかし, 出現回数推定法による録画攻撃に対しては, 位置が固定のパスロケーションがあるため, そのパスロケーションにはパスアイコンのみが認証成功時に存在することになる. 従って, 事前にk個のパスアイコンとj個のパスロケーションを2セット登録し, アイコンがm×nに並んだ2画面で認証をしたと仮定した場合, 低確率でk+1回の録画攻撃を行っただけで事前に登録したパスロケーションは特定される可能性がある. そのパターンとしては, k+1回の認証で事前に登録したパスロケーション以外のマス全てで, 異なるk+1種類のアイコンが出現する場合である. 対策としては, 同じ種類のアイコンを入れることや1画面で入力するパスアイコンの数を増やすことが考えられる. よって, ハイブリットの方式の場合, k回以下の録画攻撃に対しては安全であると言える.

5. 考察

提案手法によって, 偶然認証突破確率を低減させ, 目標の 1/10,000 の強度を達成することができた. また, 録画攻撃への耐性も, 端末のバイブレーション機能を使用し, パスロケーションの位置が認証の度にランダムに決まる方法のみを使用した認証の場合, 目標の複数回認証画面の録画をされても認証情報が盗み取られないことも達成できた. しかし, 実験により認証成功率, 認証時間は共に既存手法より劣っている結果となった. 今回の実験では, 被験者は数回程度しか認証の練習を行っていない状態で認証成功率や認証時間を記録した. しかし, パズル型認証方式は, 慣れによって認証成功率や認証時間が大きく変動する認証方式のため, 被験者が認証方式に十分に慣れてから実験を行えば認証成功率は向上し, 認証時間は短くなると考えられる. そのため, 今後は慣れを考慮した実験を行う必要がある.

また, アンケートにより, 提案手法で追加された機能によるユーザビリティへの影響は少ないことが分かった. 提案手法によるユーザビリティの向上を期待していたが, 結果は使いやすさが大きく損なわれていることはないが, 劇的に使いやすくなっているわけではないというものであった. しかし, 提案手法によって, 既存のパズル型認証方式の使いやすさを大きく損なうことなく, 偶然認証突破確率を低減させ, 録画攻撃への耐性を持たせることができた.

6. おわりに

本研究では, 覗き見攻撃による情報漏洩を防ぐために, 従来のパスワード方式による認証に位置とパズルの要素を組み込んだパズル型認証方式を改良し, 認証時の入力を複数回に分割することで入力する入力情報の候補を増加させ, 偶然認証突破確率を低減させた. また, ビデオカメラに記録されにくい, 端末のバイブレーション機能などを用いた情報提示手法とすることにより, 録画攻撃に対して耐性を持つ新たな認証方式を提案した. 提案手法を実装し8人での評価を行った. 得られた結果からは, 既存のパズル型認証方式の使いやすさを大きく損なうことはないことが分かった. 認証時間の短縮を含むユーザビリティのさらなる向上が今後の課題である.

参考文献

1) 東山侑真, 岡村真吾, 矢内直人, 藤原融, “タッチパネル端末の特性を利用した覗き見攻撃耐性をもつ個人認証手法”, 情報処理学会 Computer Security Symposium 2014, pp.1023-1028, 2014.
2) 東川創, 満保雅浩, “パターンロックの覗き見耐性向上手法について”, SCIS 2015, 2C1-4, pp.1-7, 2015.
3) 石塚正也, 高田哲司, “振動機能を応用した携帯端末での個人認証における覗き見攻撃対策手法の提案”, 情報処理学会 Computer Security Symposium 2013, pp.708-715, 2013.
4) 杉本洋介, 稲葉宏幸, “背景色と偽入力を用いた覗き見耐性を持つパスワード認証方式の提案”, 情報処理学会 Computer Security Symposium 2014, pp.1029-1033, 2014.
5) 喜多義弘, 菅井文郎, 朴美娘, 岡崎直宣, “モバイル端末における覗き見耐性を持つ認証方式の提案と実装”, 情報処理学会 Computer Security Symposium 2012, pp. 413-420, 2012.
6) Mirang Park, Yoshihiro Kita, Kentaro Aburada, Naonobu Okazaki, "Proposal of a Puzzle Authentication Method with Shoulder-surfing Attack Resistance," International Conference on Network-Based Information Systems, pp.495-500, 2014.
7) Yoshihiro Kita, Kentaro Aburada, Mirang Park, and Naonobu Okazaki, "Proposal of a Puzzle Authentication Method with Shoulder-surfing Attack Resistance and High-usability," IEICE Communications Express, vol.4, No.3, pp.95-98, 2015.