

パズル型認証方式の録画攻撃耐性の一検討

日隈光基^{†1} 臼崎翔太郎^{†1} 喜多義弘^{†2} 山場久昭^{†1} 久保田真一郎^{†1}
朴美娘^{†3} 岡崎直宣^{†1}

概要: パスワードや PIN などの覗き見攻撃に脆弱な認証方式に対して、人による覗き見攻撃に耐性を持つパズル型認証方式がある。従来の認証方式にパズルゲームの要素が加わり、楽しく認証できる点が大きな特徴である。しかし、偶然認証突破確率を低く保てないことや、録画攻撃に対して脆弱であるなどの問題点がある。そこで本稿では、次の改良を加えた。まず偶然認証突破確率の低減のために認証の入力を複数回に分けた。次に録画攻撃への耐性を向上させるために、認証に必要な情報を動的に変化させ、録画データとして記録されにくい方法を使用してユーザに提示するようにした。そして、提案方式の実装を行い、安全性やユーザビリティの観点から評価した結果を示す。

キーワード: 2120606 RFID・モバイルセキュリティ, 2120610 認証

An Examination on Video Recording Attack Resistance of Puzzle-like Authentication Method.

KOKI HINOKUMA^{†1} SHOTARO USUZAKI^{†1} YOSHIHIRO KITA^{†2}
HISAAKI YAMABA^{†1} SHINICHIRO KUBOTA^{†1}
MIRANG PAKU^{†3} NAONOBU OKAZAKI^{†1}

Abstract: Currently, many authentication methods for mobile terminals including PINs or passwords are widely used. However, they are known for their vulnerability against shoulder surfing attacks. We have proposed a puzzle-like authentication method which is resistant against human eye's shoulder surfing attacks. In this method, users can unlock their own devices by way like playing a small puzzle game. In this method, however, it remains problems of its insufficient strength against the brute-force attack and video recording attack. In this paper, we improve our puzzle-like authentication method so as to have sufficient strength against the brute-force attack and video recording attack. We implement our improved method and discuss its effectiveness with some experiments.

Keywords: 2120606 RFID・mobile security, 2120610 authentication

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利用されており、ビジネスの場でも活用され始めている。また、クラウドコンピューティングの普及により、スマートフォンからオンラインストレージに保存してあるデータを閲覧、編集できるようになっており、モバイル端末が持つ情報の量と、その重要性は年々増加している。

しかし、モバイル端末で使用されるパスワード認証、PIN認証、パターンロック認証などの画面ロック機能は、第三者から肩越しに画面を見られることで認証情報を盗み取られる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覗き見攻撃に耐性を持つ様々な認証方式が提案されている[1][2][3][4][5]。覗き見攻撃に耐性を持つ認証方式の1つに、従来の認証方式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ことで認証を行う、パズル型認証方式がある。この方式の大きな特徴は、ユーザがパズルを解くように楽しく認証することができる

挙げられる。しかし、この認証方式には、ランダムな入力でも偶然に認証を突破してしまう確率を低く保てていないこと、またビデオカメラを用いて認証画面を録画し、その画像を利用して画面ロックを解こうとする録画攻撃[6]に対して脆弱であることなど改善すべき点が存在する。本稿では、この問題点を解決することを目的としている。そこで、認証時の入力を複数回に分割し入力情報の候補を増加させることで偶然認証突破確率を低下させ、また、認証に必要な情報を認証の度にランダムに変化させるとともに、その情報をビデオカメラ等に記録されにくいバイブレーション機能によってユーザに提示する方法を提案する。

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の評価を行う。また、ユーザビリティの観点から評価を行うため、アンケートを実施する。

^{†1} 宮崎大学
University of Miyazaki.
^{†2} 東京工科大学
Tokyo University of Technology

^{†3} 神奈川工科大学
Kanagawa Institute Technology

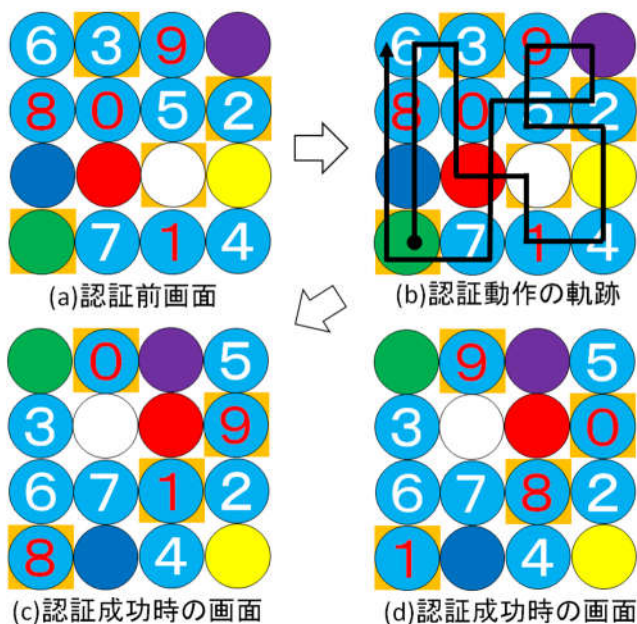


図 1 既存手法の認証の例

Figure 1 Examples of authentication of conventional method.

2. 既存のパズル型認証方式

2.1 既存の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パズルの要素を組み込み、パスワードを指定する位置に揃えることにより認証を行う方式である[7][8]。この認証方式は覗き見攻撃に耐性を持つ。

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、白色の計 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。模式図を図 1 に示す。

ユーザは、事前に登録しておいた 4 種類のアイコン（以降、パスアイコンと呼ぶ）を、また事前に登録しておいた 4 つの位置（以降、パスロケーションと呼ぶ）に移動させれば認証が成功となる（図 1 (c) 参照）。

図 1 では説明のためにパスアイコンを赤色の文字、パスロケーションを橙色の背景で示している。ただし、どのパスアイコンがどのパスロケーションに配置されても認証は成功となる（図 1 (c), (d) 参照）。

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で上下斜めの八方向に移動させることができる。アイコンを移動させると、その移動先にあるアイコンと場所が入れ替わる（図 2 (a) (b) 参照）。また、指を離さずにドラッグし続けることで、他のアイコンも位置が入れ替わる（図 2 (c) (d) 参照）。そのため、ユーザは関係の無いアイコンをドラッグし続けることで間接的に目的のアイコンを動かすことができる。これにより、認証画面を覗き見られた時にパスアイコンとパスロケーションが特定されるのを困難にしている。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指を離さない「一

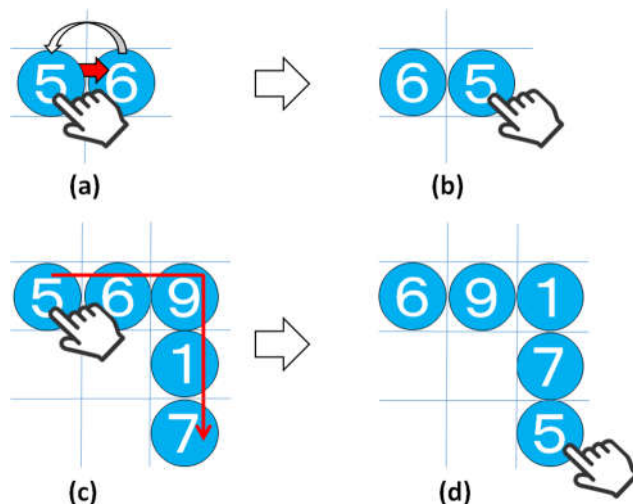


図 2 パズル型認証方式におけるパスアイコンの動かし方

Figure 2 How to move pass an icon in the puzzle authentication method.

筆書き」で認証を行うものとする。

2.2 既存のパズル認証方式の問題点

既存のパズル型認証方式は、以下に示す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画像で記録し、攻撃者がその画像通り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、認証情報が分からなくても、記録してあるアイコンの配置を再現すれば、認証を突破す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で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しまっているため、パスロケーションの位置以外にパスアイコンが出現することはない。そのため、数多くの認証成功画面を録画されてしまうと、4 種類のパスアイコンのみが現れる 4 箇所のパスロケーションが判別されてしまう。この攻撃は録画した認証画面の数が多いほど、認証突破の可能性が上がると思われる。

また、既存手法がランダムな入力によって偶然に認証を成功してしまう確率は、

$$4! \times \frac{1}{16} \times \frac{1}{15} \times \frac{1}{14} \times \frac{1}{13} = \frac{1}{1820}$$

であり、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。

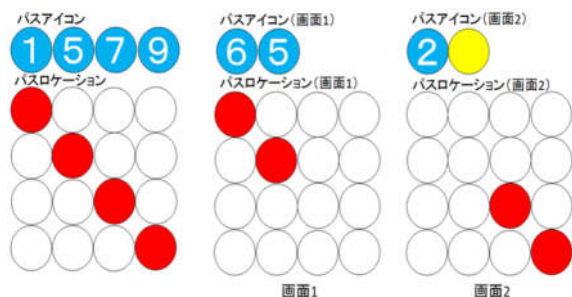


図 3 認証時の入力画面の分割

Figure 3 Partition of input sequence for authentication.

3. 提案手法

3.1 設定の目標と方針

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パズル型認証方式を提案する。提案方式の設計目標を以下に示す。

- ・偶然認証突破率の低減

偶然認証突破率とは、ランダムな入力によって偶然に認証が成功してしまう確率である。本稿では 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。

- ・録画攻撃への耐性向上

録画攻撃とは、ビデオカメラ等で認証画面を録画した画像を用いて認証を突破しようとする攻撃である。本稿では複数回認証画面の録画を行われても、認証情報を特定されないことを目標とする。

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

提案方式では、既存手法の問題点を解決するため、2 つの改良を行う。1 つ目は、認証画面の数を増やすことで、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を認証のたびにランダムに変化させ、それをビデオカメラ等に記録されることなくユーザに提示することで、録画攻撃の耐性を向上することである。以下に、この 2 つの改良の詳細を示す。

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、入力の候補を増加させることで、ランダムな入力で偶然に認証を突破する確率を低くし、また、1 画面で入力する認証情報を減らしてユーザビリティを向上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、事前に登録した 4 個のパスアイコンを配置する操作を 1 画面で行っていたが、提案手法では画面を 2 画面に増やした (図 3 参照)。1 回目の認証のための画面で認証を終えた後、続いて 2 回目の認証のための画面に遷移する。2 度目の認証を終えた後に、認証が成功する。また、画面を 2 画面に分割し

た代わりに 1 画面あたりのパスアイコン、パスロケーションの数を減らし、覚える情報を少なくすることでユーザビリティを向上させている。

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 で示した通り、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登録し、アイコンが $m \times n$ のマスに並んだ 2 画面で認証を行う。今回は既存手法と比較するため、認証画面あたりのアイコン数、マス数を既存手法と同じ状況に合わせ、 $k=2, m=n=4$ に設定する。この時の偶然認証突破確率を求めると、

$$\left(2! \times \frac{1}{16} \times \frac{1}{15}\right)^2 = \frac{1}{14400}$$

となり、偶然認証突破確率は既存手法より低減する。また、これは目標の強度である 1/10000 より確率が低くなっている。さらに 1 画面あたりのパスロケーションに配置するパスアイコンの数を減らしたことで、認証成功までの過程で動かすパスアイコンの範囲が広くなり、アイコンを目的の位置に移動させやすくなる効果がある。

2 つ目は、パスロケーションの位置を認証のたびにランダムに決めて、それをビデオカメラに記録されにくいようユーザに提示することで、録画攻撃に対して耐性を持つようにすることである。本稿では、ビデオカメラに記録されにくい情報提示方法として端末のバイブレーション機能を使用している。今回は実装していないが、イヤホンなどを端末に接続していた場合には音によって情報を提示することも考えられる。この改良により、録画攻撃への耐性が向上するとともにランダムにパスロケーションが決められるため、ユーザが長期にわたって覚えなければならない認証情報を少なくできる。

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が認証のたびに端末によって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、パスロケーションをビデオカメラに記録されることなくユーザに伝える方法を説明する。認証画面に表示された $m \times n$ のマスに配置されたアイコンをドラッグさせていくと、指があるマスを通ったときに端末が振動する。そのマスがその回の認証におけるパスロケーションとなる (図 4 参照)。

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、ユーザの記憶負担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、短期的な記憶負担が大きくなるという問題がある。これは、画面を数回なぞるだけではパスロケーションを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。

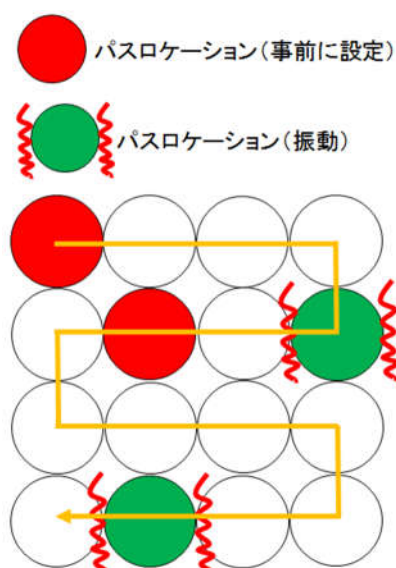


図 4 ハイブリッドの方式のパスロケーション
Figure 4 Pass-location in the hybrid system.

そこで、この問題の解決策として、既存手法の事前にパスロケーションを設定する方法と、上記に示した、ランダムにパスロケーションを設定する方法の両方を採用した、ハイブリッドの方式を合わせて提案する。ハイブリッドの方式は、あらかじめ登録しておくものと、認証の際にランダムで決まるものの2種類のパスロケーションを使用することで、図4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とのバランスを図ることができる。一方で、ハイブリッドの方式は、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ランダムに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。

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、開発ソフトに Eclipse を利用した。動作検証を行った端末の OS は AndroidOS4.4.2 である。図5にパスロケーションとパスアイコンの設定画面、図6に認証画面を示す。

4.1.1 パスアイコンとパスロケーションの設定

図5(a)に1回目の認証画面の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16種類あるアイコンの中から登録したいアイコンを2種類タッチする。パスアイコンを選択した後に「OK」ボタンを押すことで、同図(b)へ移行する。同図(b)に1回目の認証画面の、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1箇所タッチする。パスロケーションを選択したあとに「Next」ボタンを押すことで、同図(c)へ遷移する。同図(c)に2回目の認証画面の、パスアイコンの設定画面を示す。機能は同図(a)の設定画面と同じである。同図(d)に2回目の認証画面の、パスロケーションの設定画面を示す。機能は同図(b)の

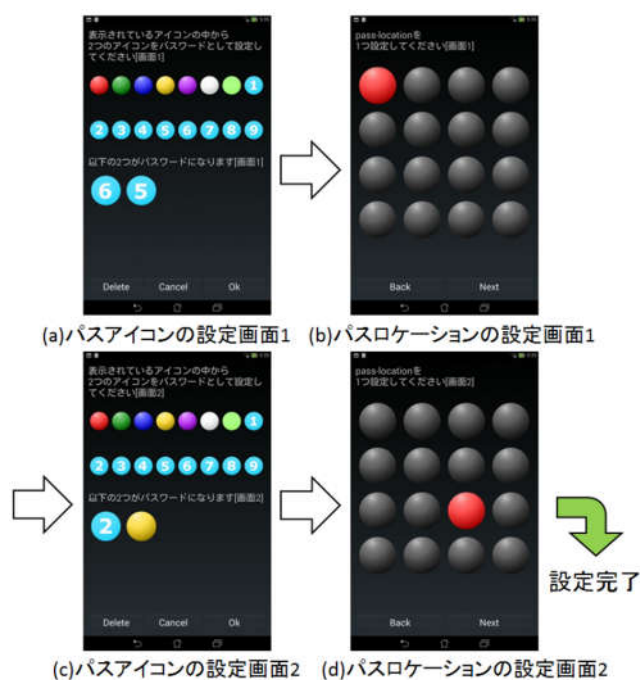


図 5 提案手法の認証情報登録画面
Figure 5 Setting screen of new authentication method.



図 6 提案手法の認証手順
Figure 6 Process of new method.

設定画面と同じである。同図(d)の画面においてパスロケーションを選択した後に「Next」ボタンを押すことで、同図(a)(b)(c)で選択したパスアイコンとパスロケーションが登録される。

4.1.2 認証

図6(a)に1つ目の認証画面を示す。「Shuffle」ボタンを押すと、アイコンをランダムに再配置直することができる。これは、最初に表示されたパスアイコンの配置が自分の設定したパスロケーションと離れた位置にある場合など、アイコンの移動が困難であると判断した場合に使用される。また、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、そのマスを指が通ったときに端末が振動する機能を実装している。また、録音された場合に振動音でラン

表 1 認証成功率と認証時間

Table 1 Authentication success and authentication time.

	認証成功率	認証時間
既存手法	95	14.92
提案手法	77.5	26.16

ダムに決まったパスロケーションを判別されないよう、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、全てのマスにおいて、指でなぞった際にダミー音が鳴るようにした。同図(b)に2つ目の認証画面を示す。機能は同図(a)の認証画面と同じである。「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。

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、実装したシステムで数回練習してもらった後実験を行った。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。なお、実験で使用した提案手法の認証方式は、事前に各画面につき2個のパスアイコンと1個の固定パスロケーションを登録し、アイコンが4×4のマスに並んだ2画面で認証を行うハイブリッドの方式を採用している。また、認証画面では、指でなぞることで端末が振動するマスが1つあり、そのマスがランダムで決まる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。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のか分かり辛くなることが挙げられる。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として、提案手法は画面をなぞって振動するマスを確認する作業を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、提案手法では、認証を失敗した場合、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になっている。

4.3 ユーザビリティに対する評価

提案手法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人に実験を行った後、アンケートを実施した。提案手法で追加された機能によるユーザビリティの影響を確認するため、以下に示す6項目について調査し、それぞれの項目について5

段階で評価を行った。アンケートの結果を図7に示す。

- (1) 提案方式を理解できたか
- (2) 振動機能によるパスロケーションの発見は容易か
- (3) 認証画面の数が増えると使いやすいか
- (4) 認証画面の数が増えると認証情報を覚えるのは容易か
- (5) 認証にかかる時間は短い
- (6) 録画耐性をもつ認証が必要な立場になったとき使ってみてみたいと思うか

(1)の項目では、すべての人が理解できたと回答していた。本実験は学生に対して行ったので、学生には理解されやすい認証だということが分かる。

(2)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」という回答も見受けられたが、「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であったので、認証の際にランダムにパスロケーションを決定し、それを振動機能で伝える方法によってユーザビリティが低下する可能性は少ないといえる。

(3)の項目では、半数が「どちらでもない」と回答している。「とても使いやすい」という回答と「使いやすい」という回答が、「少し使いにくい」という回答よりも多かった。半数が「どちらでもない」と回答していることから、認証画面の数によってユーザビリティに与える影響は少ないものと思われる。

(4)の項目では、半数が「どちらでもない」と回答し、「容易」という回答と「少し難しい」という回答が同程度見受けられたが、「難しい」という回答はなかった。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したことによる、ユーザの記憶負荷への影響は少ないものと思われる。

(5)の項目では、「少し長い」という回答が過半数を超えていたが、「短い」という回答も見受けられた。ユーザビリティに考慮した認証方式としては致命的な問題であるので、改善が必要である。この原因としては、認証画面が増えたことによって入力時間が増大したこと、失敗すると再度2画面分の認証を行わなければならないことが挙げられる。

(6)の項目では、「どちらでもない」という回答も見受けられたが、全体的に使ってみたいという意見が多かった。この結果から、提案した認証方式の安全性はユーザによく伝わっており、録画攻撃に対する耐性が必要な時は使用される可能性が高いと考えられる。

4.4 録画攻撃への耐性に対する評価

まず、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を述べる。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を認証のたびにランダムに決定することで、攻撃を防ぐことができる。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、認証の際にパスロケー

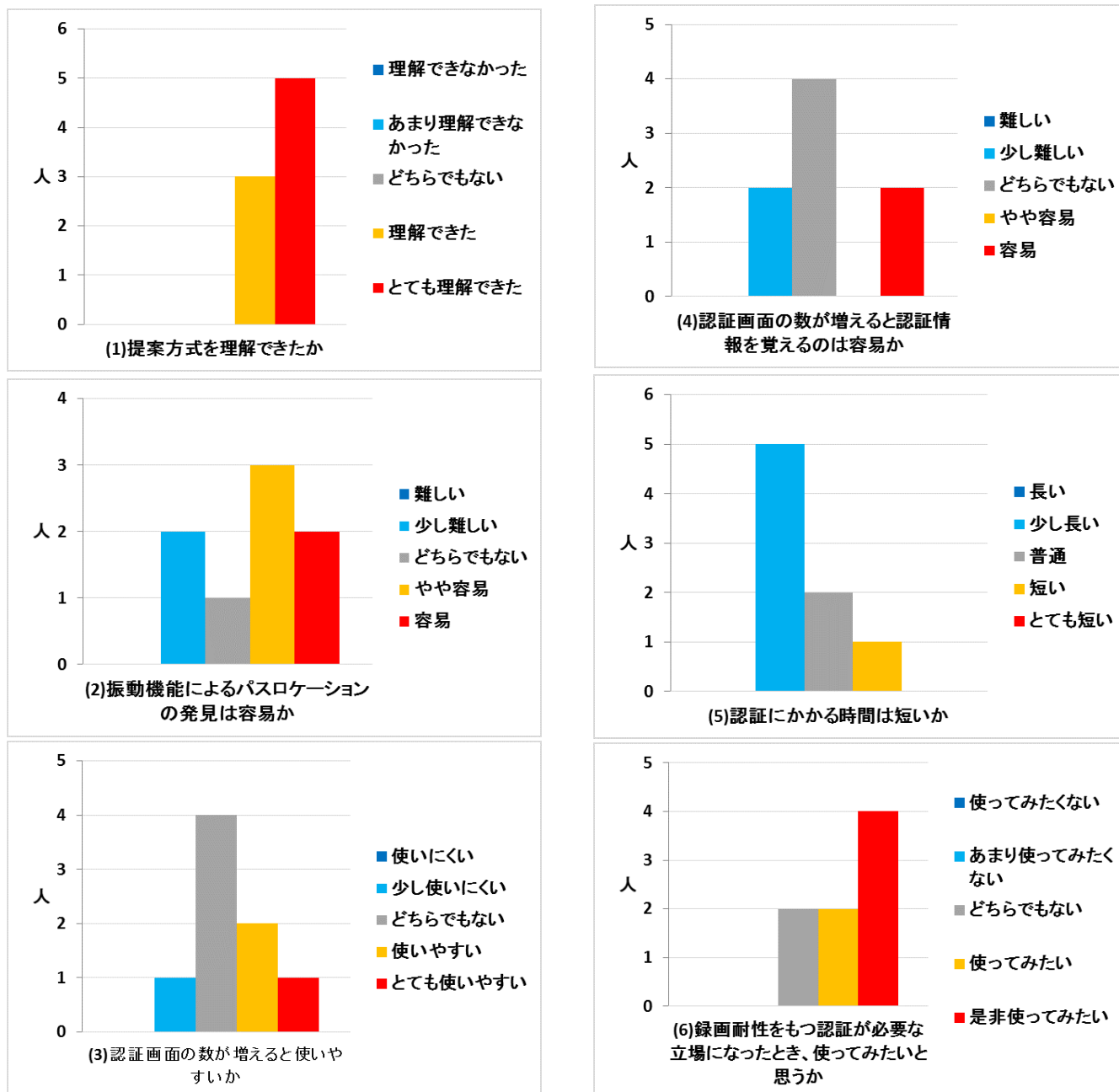


図 7 アンケートの結果
Figure 7 Result of questionnaire.

ションの位置をランダムに決定することによって防ぐことができる。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、ハイブリット的方式を使用した認証の場合を述べる。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存在するため、認証成功時には、その固定のパスロケーションにはパスアイコンのみが配置されることになる。したがって、あらかじめ 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 $m \times n$ に並んだ 2 画面で認証を行ったと仮定すると、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が特定される可能性がある。その状況とは、 $k+1$ 回の認証で事前に登録したパスロケーションでないマス全ての、異なる $k+1$ 種類のアイコンが出現する場合である。パスロケーションでない場所に重複なくパスアイコン以外のアイコンが出現すると、パスアイコンが必ず重複して出現するパスロケーションの位置が判別できてしまう。対策としては、ダミーとして同じ種類のアイコンを追加することや 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。したがってハイブリット方式の場合、 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、目標強度である $1/10000$ を達成することができた。また、録画攻撃への耐性も、認証のたびにランダムに決まるパスロケーションのみを使用し、それを端末のバイブレーション機能によって知らせる方法を使用した場合に、複数回認証画面を録画されても認証情報を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、認証時間はともに既存手法に比べて劣っている結果になった。今回の実験では、被験者は数回程度しか認証操作の練習を行わなかったが、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に大きく変動がある方式であるため、被験者が操作に慣れていた場合はもう少し認証成功率が向上し、認証時間が低減することも考えられる。そのため、今後は操作の慣れを考慮に入れた実験を行う必要がある。

アンケートの結果から、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。入力を複数回に分割する代わりに記憶する認証情報を減らしたことによって、ユーザの記憶負荷という観点からユーザビリティが向上する結果を期待したが、劇的に向上することにはなかった。しかし、提案手法によって、ユーザビリティを大きく損なわずに、偶然認証突破確率を低減させ、録画耐性への耐性を付加することができた。また、認証にかかる時間は少し長いという意見が多く見られたが、録画耐性をもつ認証が必要な立場になったときには使用するという意見も多かったことから、手法の安全性は伝わっており、少々時間がかかっても機密情報の保護のためには使用される可能性が高いことが考えられる。しかし、ユーザビリティに配慮した認証として、時間の短縮は今後解決すべき課題である。

6. おわりに

本稿では覗き見攻撃に耐性を持つ従来の認証にパズルの要素を組み込んだパズル型認証方式の改良を行った。認証時の入力を複数回に分割することによって、入力情報の候補を増やして偶然認証突破確率を低減させ、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を用いた認証情報提示手法によって、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。提案手法を実際に実装し、宮崎大学工学部の学生 8 人による評価実験を行い、ユーザビリティを評価した。得られた結果から、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無いことが分かった。認証時間の短縮、認証精度の向上を含めた、ユーザビリティのさらなる向上が今後の課題として挙げられる。

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] 高田哲司, “Fake Pointer: 映像記録による覗き見攻撃にも安全な認証手法”, 情報処理学会論文誌, Vol.49, No.9, pp.3051-3061, 2008.
- [7] 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.
- [8] 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.