

マウス操作を用いた個人認証方式の提案と その覗き見耐性およびユーザビリティの評価

2017SC059 奥田泰友希 2017SC062 酒井聡太

指導教員：石原靖哲

1 はじめに

現在、仕事場やネットカフェなど公共の場で PC を用いて個人認証を行う機会が増えている。そこでは、主にキーボードによるパスワード認証が使われている。しかし、このキーボードによる認証はモニターやキーボードから覗き見や録画による認証情報の漏洩の危険性がある [1]。また、パスワード長増加に伴い記憶負荷が大きくなる問題点がある。

そこでキーボードに代わる認証として、PC において覗き見耐性を持つマウス操作を用いた個人認証方式が提案されている [2]。利用者がマウスを机の下などで操作することが可能かつ視覚によるフィードバックがないので、従来のキーボード認証より覗き見や録画耐性をもつと考えられる。また利用者はシステムより与えられたマトリクス上のセルの場所やセルの情報 (数字と色) を認証情報として記憶するので、記憶負荷を少なくできると考えられる。本研究ではこのマウス操作を用いた個人認証方式に着目する。

長友らの認証方式はマウス音による覗き見耐性の低下やユーザビリティの改善が課題となっている。本研究では、登録情報の組み合わせの増加により覗き見耐性を向上させ、かつ、セルの場所を直接指定することによりユーザビリティを改善した認証方式を新たに提案する。そして、提案方式と既存方式の覗き見耐性とユーザビリティの実験を行う。この実験では、被験者 9 人の認証時間、マウス音と覗き見による特定率、ユーザビリティに関するアンケートの回答を取得した。その結果、パスワード長とマトリクスサイズの増加に伴う認証時間の増加量が既存方式と比べ小さくなり、かつ、認証時間が短くなった。また、アンケートの回答では「使いやすさ」「また使いたいか」などの項目でセルの場所を直接指定する方式がマトリクス上を移動する方式と比べ高い評価を得た。覗き見耐性の実験では提案方式はマトリクスの増加に伴いパスワードの特定率が低くなり、かつ、既存方式と比べて一番パスワードの特定率が低くなった。以上のことから、提案方式は、ある一定以上のパスワード長とマトリクスサイズをもつ状況において、既存方式よりも覗き見耐性とユーザビリティを両立させやすいと結論できる。

2 関連研究

2.1 SECUREMATRIX

SECUREMATRIX[3] はマトリクスと数字を使った認証方式である。4 × 4 のマトリクス上で利用者は自分で決めたセルの場所を指定し、認証情報として登録する。各セ

ルには 0 から 9 のランダムな数字が表示されており、利用者は登録したセルの場所の数字をキーボードから入力することで認証する。この認証方式は、利用者の記憶負荷が少なくなることが利点であるが、モニターやキーボードの覗き見、または録画されると認証情報が漏洩する可能性があることが問題である。

2.2 覗き見耐性をもつ認証

覗き見耐性を持つマウス操作を用いた認証 [2] には、マトリクス上で行うパターンを用いた方式、数字と色を用いた方式、マウスの組み合わせを用いた方式がある。

パターンを用いた方式は、 $N \times N$ のマトリクス上で、利用者はマウス操作を用いてセルの場所を複数選択し、その順番とともに認証情報として登録する。認証を行う際は、登録と同じようにマウス操作を用いて、マトリクス上のセルの場所を登録した順番に指定することで認証する。

数字と色を用いた方式は、 $N \times N$ のマトリクス上で、利用者はマウス操作を用いてセルを複数選択する。各セルはランダムな色が塗られており、その上にランダムな数字が表示されている。利用者はセルの色と数字の組み合わせと、その選択の順番を認証情報として登録する。認証を行う際は、マウス操作を用いて、マトリクス上のセルの色と数字の組み合わせが一致する場所を登録した順番に指定することで認証する。

マウス操作の組み合わせを用いた方式は、 $N \times N$ のマトリクス上で、利用者はマウス操作を用いてセルの場所を選択し、認証情報として登録する。ただし、マウスクリック、ホイールクリック、ホイール回転とマウス移動の組み合わせ操作を行うことで直接マトリクス上の位置を指定する。認証を行う際は、登録と同じマウスの組み合わせ操作を行う。

以上の三つの方式は、マウスを机の下に隠しながら操作を行うことである程度の覗き見耐性がある。しかし、マウス音による覗き見耐性の低下やユーザビリティの改善が今後の課題となっている [2, 4]。

3 提案手法

マウス操作の組み合わせを利用し、指定した行と列に対応した数字と色のセルを登録情報とした認証方式を提案する。入力インタフェースを図 1 に示す。ここで、マウスは以下の動作ができるものとする。

- 右クリック・左クリック
- ホイールクリック・上下のホイール回転

この方式では、セルに書かれた数字と色が認証情報とし

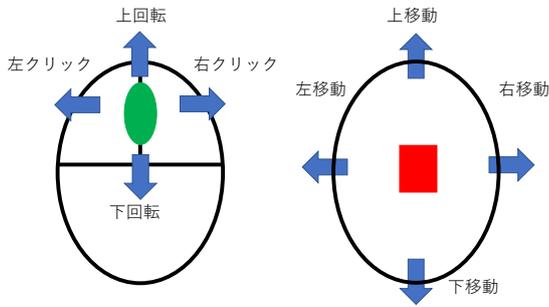


図1 入力インターフェース



図2 マウス操作の組み合わせ

て保存される。この時、数字と色のセルに対応したマウスの組み合わせ操作を行うことにより指定する。ただし、行、列の順にマウスの組み合わせ操作を行う。マウスの組み合わせ操作の画像を図2に示す。認証を行う際は、登録した数字と色のセルに対応した画像のマウスの組み合わせ操作を行、列の順に行う。この方式で考えられるメリットを以下に示す。

- パターン用いた方式と数字と色を用いた方式と比べ、ユーザビリティが向上
パターンと数字と色の方式は、マウス操作によるマトリクスの移動を視覚上確認することができない。そのため、操作ミスが生じる可能性があると考えられる。我々の提案方式では、画像に書かれたマウスの組み合わせ操作を行うことで直接マトリクス上のセルを指定することが出来る。
- 組み合わせの方式と比べマトリクスサイズを増加でき、視き見耐性が向上
組み合わせを用いた方式では、マウス操作の一つの動作で場所を指定するため、マウス操作の組み合わせに限りがありマトリクスを4×4より大きくすることが出来ない。我々の提案方式では、二つの動作で場所を指定するためマトリクスサイズを大きくでき、視き見耐性を容易に向上させられる。

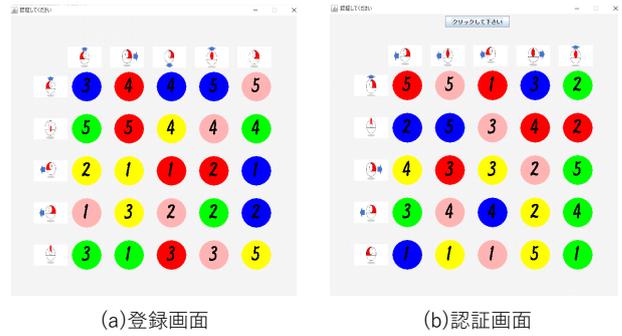


図3 実装画面

4 実装

上記の提案手法を基に統合開発環境 Eclipse 上で Java 言語を用いて実装を行った。以下でマトリクスサイズが5×5の時の登録段階と認証段階の例を説明する。

4.1 登録段階

マウスの組み合わせ操作を示した画像と5×5のマトリクスが画面に表示される(図3(a))。マウスの組み合わせ操作を示した画像は図2に示した17個からランダムに選出され、縦に5個、横に5個表示される。またマトリクスの各セルには、ランダムな色と数字が配置されている。利用者が緑の1を登録するとき次の動作を行う。緑の1は5行目と2列目に位置している。そのため5行目に表示されている画像の「ホイール上回転」、2列目に表示されている画像の「右クリックしながら右移動」の順にマウス操作を行い、緑の1を登録する。

4.2 認証段階

マウスの組み合わせ操作を示した画像と5×5のマトリクスが画面に表示される(図3(b))。マウスの組み合わせ操作を示した画像は17個からランダムに選出され、縦に5個、横に5個表示される。またマトリクスの各セルには、ランダムな色と数字が配置されている。利用者が緑の1を登録したとき次の動作を行う。緑の1は5行目と5列目に位置している。そのため5行目に表示されている画像の「左クリック」、2列目に表示されている画像の「ホイールクリックしながら上移動」の順にマウス操作を行い、緑の1を指定する。最後に認証ボタンを押し認証を完了する。

5 マトリクスとパスワードの増加に伴うユーザビリティの実験

SECUREMATRIX, キーボードによる認証の組み合わせの数に近づけるために、パスワード長とマトリクスサイズを増加させ、それに伴う認証時間を計測する。マトリクスサイズは3×3, 5×5, 7×7, パスワード長は4, 5, 6とする。これらの条件で長友らのマウス操作を用いた方式(パターンを用いた方式, 数字と色を用いた方式)と本論文

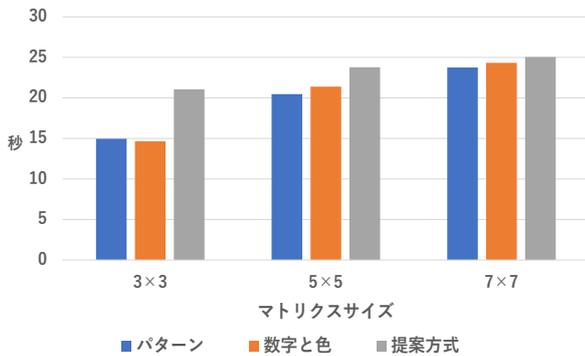


図4 パスワード長が4の時の平均認証時間

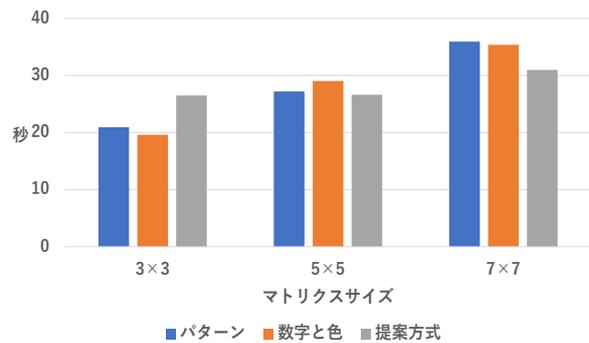


図6 パスワード長が6の時の平均認証時間

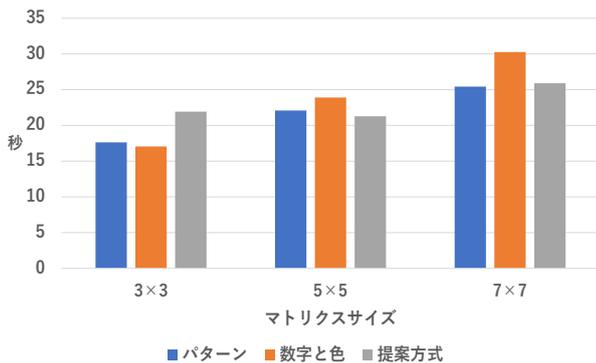


図5 パスワード長が5の時の平均認証時間

で提案した方式の認証の際にかかった時間(認証時間)を比べ、パスワード長とマトリクスサイズの増加に伴うユーザビリティの評価を行う。認証時間とは被験者が最初に入力した時点から最後のパスワードの入力が終わる時間を表す。組み合わせを用いた方式はマウス操作の組み合わせに限りがあり、マトリクスサイズを4×4より大きくすることが難しいため、実験は行わない。

5.1 実験環境

被験者9人(20代男性7人, 20代女性1人, 50代女性1人)に実験を行った。実験のはじめとして、各認証方式の操作説明を行う。その後、被験者に認証情報を登録してもらい操作に慣れてもらう。最後に画面上のマトリクスサイズが3×3の条件下で、それぞれパスワード長が4, 5, 6における認証を行い認証時間を計測する。同様にマトリクスサイズが5×5, 7×7の条件下で認証時間を計測する。

5.2 実験結果と考察

マトリクスサイズが3×3, 5×5, 7×7の条件下でパスワード長が4, 5, 6の時の各認証方式の認証時間の平均をそれぞれ、図4, 図5, 図6に示す。実験の結果、パスワード長が4の時はパターンを用いた方式と数字と色を用いた方式はいずれのマトリクスサイズの条件下でも差はあまりみられず、我々の提案方式よりも短い結果となった。しかし、我々の提案方式では、パスワード長を5, 6と長くした

とき認証時間の増加量が既存方式と比べ小さい。特に、パスワード長が5, 6のとき提案方式は既存方式と比べ認証時間が一番短くなった。よってパスワードを長くするにつれ、我々の提案方式の認証時間が既存方式と比べ短くなると予想される。また、同様にマトリクスサイズが5×5, 7×7と大きくなると認証時間の増加量が既存方式と比べ小さくなった。

6 アンケートを用いたマトリクスの指定方法によるユーザビリティの比較

アンケートを用いて認証方式においてマトリクス上を移動する方式(パターンを用いた方式, 数字と色を用いた方式)とマトリクスの位置を直接指定する方式(組み合わせを用いた方式, 提案方式)を比較する。アンケートに関する項目は以下の通りであり、各項目を1~5の5段階評価してもらう。ただし、5が最高評価で1が最低評価とする。

- 使いやすさ
認証成功率が高いだけでは、ユーザビリティが高いとは言えず、認証方式の使いやすさを測る必要があるため。
- 慣れによる使いやすさ
慣れによる認証成功率や認証時間の向上があるかを判断する必要があるため。
- 今後使用したいか
印象による認証の受け入れを測るため。この項目が高ければ、今後の認証方式として実用された場合の普及率が高いと言える。

図7に3項目の平均を示す。

使いやすさについて評価する。組み合わせを用いた方式の平均は3.89, 我々の方式の平均は3.22である。これは、マトリクス上を移動する方式と比べて評価が高い。この結果からマトリクス上のセルを直接指定するほうが使いやすいと言える。一方、パターン方式においては平均が2.11と低く、操作性に問題があると考えられる。

慣れによる使いやすさを評価する。組み合わせを用いた方式の平均は4.11, 我々の方式の平均は3.89である。これは、マトリクス上を移動する方式と比べて評価が高い。

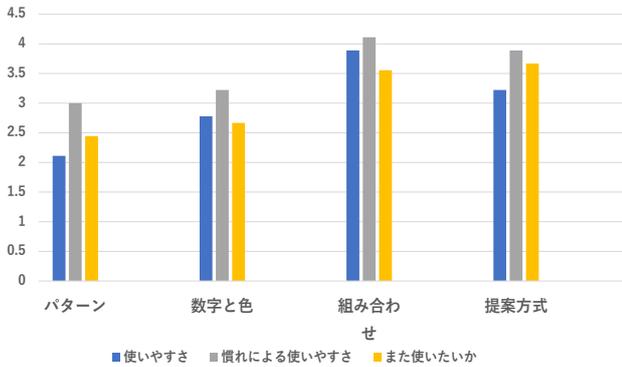


図7 アンケートの評価平均

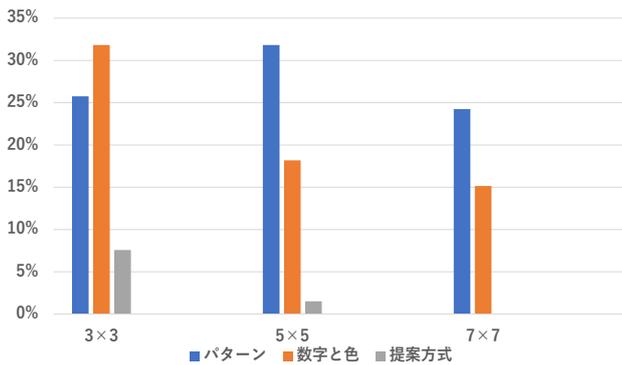


図8 特定率の平均

この結果からマトリクス上のセルを直接指定するほうが慣れによる認証成功率や認証時間の向上が見込めると言える。

今後使用したいかについて評価する。組み合わせを用いた方式の平均は 3.56、提案方式の平均は 3.67 である。これは、マトリクス上を移動する方式と比べ評価が高い。この結果からマトリクス上のセルを直接指定するほうがまた使いたいという結果になった。しかし、組み合わせを用いた方式の平均は 3.56、提案方式の平均は 3.67 であり、ニーズに対して改善の余地があると言える。

7 マウス音と覗き見による特定率の実験

7.1 実験環境

この実験では、認証する人はマウスを机の下に隠し、モニターを見ながら認証する。覗き見をする人は、認証する人の 1m 以内で覗き見をし、認証する人が行うマウス操作のクリック音、ホイール回転、マウス移動や入力時間を推測材料とし、認証情報を推測する。

7.2 実験結果と考察

覗き見の特定率について考察する。認証者が 2 回覗き見をされた時の、認証情報の特定率の平均を図 8 に示す。パターンを用いた方式では、特定率がマトリクスサイズの増加に対する変化が見られなかった。これは認証者が認証情報の登録箇所を分かりやすい形で覚えようとするため、覗

き見をする人が場所を推測しやすくなったからである。一方、数字と色を用いた方式と我々の提案方式では、マトリクスサイズの増加に伴い特定率が小さくなる結果を得た。我々の提案方式ではマトリクスサイズが 3×3 の条件下で 7.58 %、 5×5 の条件下で 1.52 %、 7×7 の条件下で 0 % であり他の方式に比べて特定率が小さい。提案した方式が最も覗き見に対する耐性があると言える。

8 まとめ

本論文ではマウス操作を用いた個人認証方式について提案をし、提案方式と長友ら認証方式で覗き見耐性とユーザビリティの実験を行った。

ユーザビリティの実験の結果、我々の提案方式では、パスワード長を 5、6 と長くしたとき認証時間の増加量が既存方式と比べ小さいという結果になった。特に、パスワード長が 5、6 のとき提案方式は既存方式と比べ認証時間が一番短くなった。また、同様にマトリクスサイズが 5×5 、 7×7 と大きくなると認証時間の増加量が既存方式と比べ小さくなった。よってパスワード長とマトリクスサイズを大きくするにつれ、我々の提案方式の認証時間が既存方式と比べ短くなると予想される。また、被験者のアンケート結果では、マトリクスサイズの増加ができる認証方式の中で 3 つの項目の平均点が一番高くなった。

次にマウス音による覗き見耐性の実験の結果、色と数字を用いた方式と提案方式ではマトリクスの増加に伴いパスワードの特定率が下がる結果となった。さらに、提案方式では既存方式と比べマトリクスサイズが 3×3 、 5×5 、 7×7 のどの場合でも特定率が一番低い結果となった。

以上のことから、提案方式は、ある一定以上のパスワード長とマトリクスサイズをもつ状況において、既存方式よりも覗き見耐性とユーザビリティを両立させやすいと結論できる。

参考文献

- [1] Davide Balzarotti, Marco Cova, and Giovanni Vigna. Clearshot: Eavesdropping on keyboard input from video. *2008 IEEE Symposium on Security and Privacy*, pp. 170–183, 2008.
- [2] 長友誠, 朴美蘭, 岡崎直宣, 高田司郎. 覗き見耐性をもつマウス操作を用いた個人認証方式の提案. 情報処理学会研究報告, Vol. 2017-CSEC-78, No. 29, pp. 1–8, 2017.
- [3] CSE:SECUREMATRIX. <https://www.cseltd.co.jp/securematrix/>, (2021-01-10 参照).
- [4] 長友誠, 喜多義弘, 油田健太郎, 岡崎直宣, 朴美娘. マウス操作を用いた個人認証方式のユーザビリティと覗き見耐性の実験と評価. コンピュータセキュリティシンポジウム 2017 論文集, Vol. 2017, No. 2, pp. 23–25, 2017.