複数ボタンの移動追跡困難性を利用した覗き見耐性を持つ暗証番号・パスワード入力手法の操作性改善

小林 心[†1]　小國 健[†2]　中川 正樹[†1]

概要：スマホなどの暗証番号・パスワード入力では，それを覗き見されるショルダーハッキングの問題がある．我々はその防止策として，ボタンに色や形などの属性を付与してから，キー表示を消し，すべてのボタンを移動させ，移動後に目的のボタンをタッチする方式を提案している．覗き見する人は多数のボタン移動を同時には追えないが，利用者は目的のボタンが分かっているので，単一のボタンだけ追って入力できる．本手法は強度最優先ではないが，既存の入力方式の延長で利用でき，サーバサイドの変更も不要である．評価実験により，覗き見に対して耐性があることが確認された．しかし，操作者が目的のキー移動を見逃してしまう問題があった．そこで，移動をプレイバックできる機能を追加した．本稿ではその評価を提示する．

Usability Improvement of an Anti-Shoulder-Hacking PIN Code/Password Input Method exploiting Tracing Difficulty of Multiple Button Movements

Kokoro KOBAYASHI[†1]　Tsuyoshi OGUNI[†2]　Masaki NAKAGAWA[†1]

Abstract: When a person inputs a PIN code or password to a smartphone, etc., there exists risk of shoulder hacking of the PIN code or password to be stolen. To decrease the risk, we assign colors or shapes to buttons, remove codes from buttons, move them simultaneously and let the user to touch the target button. Peepers can't trace movements of all the buttons at the same time, but the user only need to trace a single button and touch it. This method does not have the highest security, but it is easy to use and free from change to a server side. However, there is a risk to miss the movement of the target button. Therefore, we add a function to rewind and replay the movements. This paper presents the new function and its evaluation.

1. はじめに

近年，スマートフォン・タブレット端末の普及に伴い，電車・バスの車内など，第三者の目に触れうる場所で，暗証番号やパスワードを入力する機会は格段に増えている．また，コンビニエンスストアやショッピングセンターなどに ATM が設置されることも多くなっており，こちらも人目につきやすい場所での暗証番号を入力する機会の増加につながっている．

暗証番号・パスワードを入力する際に，第三者に覗き見されることを，ショルダーハッキング（あるいはショルダーサーフィン）という．ショルダーハッキングが行われると，暗証番号・パスワードが推測されたり盗難されたりする恐れがあり，第三者に知られてしまうと，利用者の情報や資産を守ることができなくなってしまう．

これまでに，このショルダーハッキングに対応するために，様々な技術が研究されてきた[1〜7]． 総じて，新たな情報を追加したり，別の記憶や頭の中での計算を要するなどして利用者の認知的負荷を増したり，システムへの変更を要したりするため，導入がためらわれるものが多い．

このことから，我々は，スマートフォンやタブレットでの利用を主に想定し，キーを入力する瞬間の覗き見に耐性があり，かつ，ビデオ撮影への耐性を犠牲にしても，認知的負荷が少なく，サーバサイドへの変更の必要性がない暗証番号・パスワード入力手法を提案してきた[8]. 本方式は，ボタンに色や形などの属性を付加してから，キーの表示を消し，すべてのボタンを移動させ，移動後に目的のボタンをタッチすることでキーを選択することを基本とする．しかし，操作者が目的とするボタンの移動を見失う問題があった．そこで，ボタン移動を再生する機能を追加した．結果として，盗み見のリスクを若干増加させるが，操作エラーをなくすることができた．

†1 東京農工大学工学府情報工学専攻
Department of Computer and Information Sciences, Tokyo University of Agriculture and Technology
†2 NTT データ
NTT DATA

2. 基本手法

基本手法では，初期状態として一般的なキーボードと似た形式で表示されたボタンに，対応する文字または数字を表示する．

誰もいない場所であれば，キーを直接タッチして文字・数字を入力してもよいが，人目が気になる場所であれば，キー配列をシャッフルする．すると，すべてのキーの表示が消えてボタンが移動する．覗き見する人は，多数のボタン移動を同時には追えないが，利用者は目的の文字・数字が分かっているので，単一のボタンだけ追って，それを入力する（図１）．カメラで録画していない限り，非常に安価

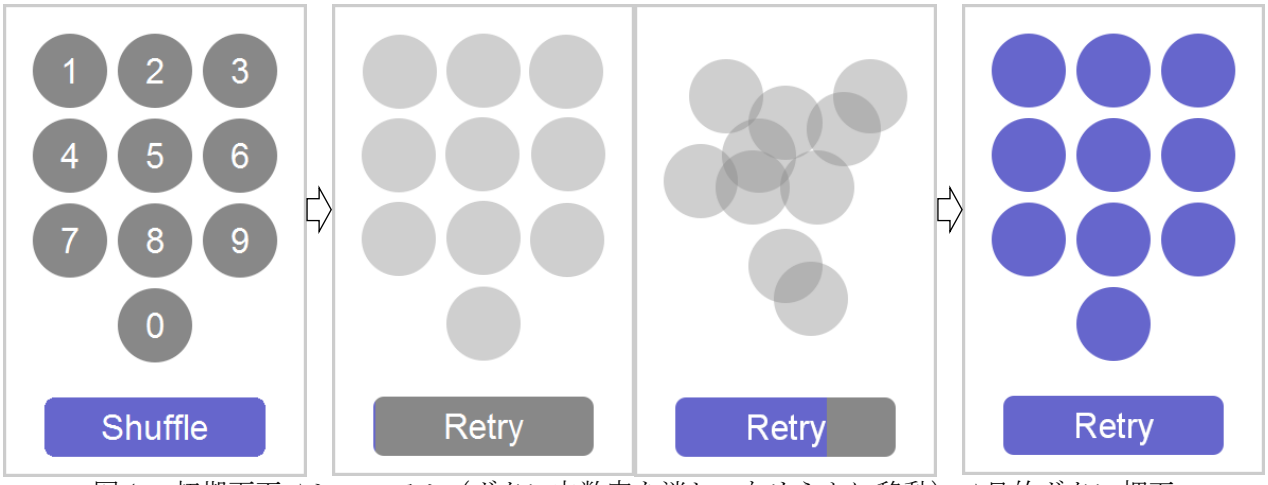

図１．初期画面⇒シャッフル（ボタン内数字を消し，なめらかに移動）⇒目的ボタン押下
ボタンを見失った場合は [retry] ボタンを押す

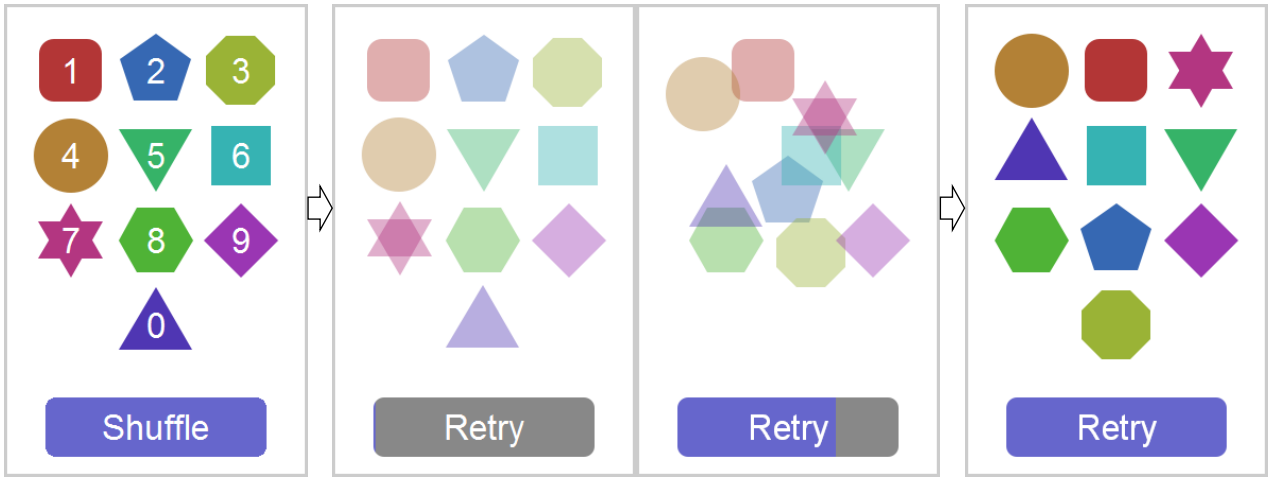

図２．多色・多形方式初期画面⇒シャッフル（ボタン内数字を消し，なめらかに移動）⇒目的ボタン押下

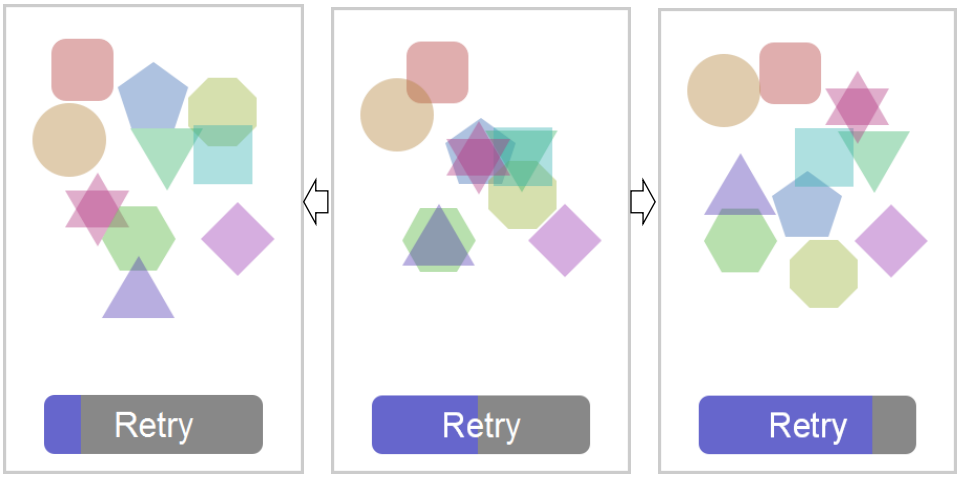

図３．プレイバック機能
図２で移動した後，ボタンを左右にドラックすることで自由にプレイバックすることができる

でセキュアに暗証番号を入力できる. この変形として, 色, 形，大きさをボタンにつけておいて，表示を消し，位置を変えた後に入力させること方法も併せて提案する（図２）. このとき，移動を表示させなければ入力の時間を短くできる．この動作を 1 文字ごとに繰り返すことで 2 文字以上の暗証番号・パスワードを入力できる.
本方式は強度最優先ではない（たとえば録画には耐性がない）が，既存の暗証番号・パスワード入力の延長で利用でき，サーバ側のプログラム変更も不要である.

3. 操作性改善

この手法では，移動を見逃した場合にはリトライをして移動をやり直す必要があり，移動速度の調整や見直しが不可能であった．そこで，移動を指示するボタンがスライダを兼ね，移動中または移動後にスライダを操作することで移動を戻したり進めたりできるようにした．スライダの左端が移動前，右端が移動後と対応しており，スライダを移動させることで対応した任意の位置に移動させることができる．（図３）

4. 評価実験

本章では，提案手法の覗き見強度や利用者の負荷を測定するための評価実験について述べる.

4.1 評価実験の構成

スライダにより移動を行うことでどの程度覗き見が可能となるかを測定することと，スライダを導入したことによる利用者の負荷を測定することである．本実験ではボタンやキーボードの種類が異なる，4 種類のテンキー・キーボードを準備した.

表 1 実験用キーボード一覧

実験No	キーボード	ボタン色	ボタン形状
1	テンキー	同一色	円形
2		多色	10形状
3	QWERTY	同一色	円形
4		多色	10形状

表 1 の多色では，特定の明度・彩度において，色相を等間隔に分割し，各ボタンにランダムに割り振っている．また，ボタン形状の 10 形状には，円形・上向き三角形・下向き三角形・正方形・ひし形・五角形・六角形・八角形・角丸・星型を用いている．これらは基本手法と同一とし，比較が可能となるようにした.

実験では，被験者を二人一組のペアとし，一人を利用者，もう一人を覗き見者とし，キーボード 1 種類ごとに交互に実験を行った．実験で用いる暗証番号・パスワードはキーボード・被験者ごとにランダムに生成した．テンキーで用いる暗証番号は 4 桁の数字列, QWERTY 拡張で用いるパスワードは 4 文字の英数字列とした. 計測には 7 インチ･1024 x 600 のタブレット PC を横長の向きにして使用した．実験は，23 歳から 25 歳までの男性 4 名に対し行った.

4.2 実験手順

提案手法の各キーボードに対し，覗き見の可否，入力の成否，入力時間などを計測した．キーボードの順番による偏りをなくすため，キーボードの順番は被験者ごとにランダムに行った.

各キーボードでは同じ暗証番号・パスワードを 3 回入力してもらい，覗き見者は各回でどこまで覗き見をすることができたかを記録してもらった.

今回，すべての文字で移動を見逃した場合を仮定し，実験を行った．まず，最初の移動を見逃したこと想定して，利用者は移動を見ないようにし，覗き見者だけが移動を見た状態で，ボタンを最後まで移動させる．次に利用者と覗き見者両方がキーボードを見ながら，利用者がスライダを使ってボタンの移動を確認し，移動後のボタンを押して文字を入力することとした．これは，覗き見者にはもっとも有利な条件であり，また，覗き見の距離も 30cm 程度とかなり近い位置から常に覗き込んでいるため，これを覗き見可能性の上限と考えることとした.

4.3 実験結果

実験結果を次に要約する.

4.3.1 入力成功文字数とリトライ回数

今回の実験では, 入力に失敗することはなかった. また, 実験の性質上リトライも発生しなかった.

4.3.2 入力時間

各キーボードにおける，1 文字あたりのスライダ操作開始から入力までの時間を表 2 に示す.

表 2 入力時間（秒）

実験No	入力時間
1	8.4
2	4.9
3	12.8
4	8.5

一度のプレイバックに対し平均 8.5 秒ほどの時間がかかることが示された.

4.3.3 覗き見成功率と 4 文字覗き見成功率

各キーボードにおける，平均の覗き見成功文字数を表 3 に示す.

表 3 覗き見成功文字数（文字）

実験 No	プレイバックあり			なし(基本研究[8])		
	1回目	2回目	3回目	1回目	2回目	3回目
1	0.00	0.50	2.25	1.20	2.00	1.60
2	0.75	1.75	2.50	0.83	1.50	1.83
3	0.00	0.00	0.25	0.00	0.25	0.00
4	0.00	0.25	0.50	0.00	0.20	0.00

テンキーでは 3 回の入力で最大で 3 文字，平均 2.5 文字程度覗き見に成功した．また，キーボードでは最大で 2 文字，平均 0.5 文字程度の覗き見に成功した.

なお，今回の実験では 4 文字すべてを覗き見られ，暗証番号・パスワードが盗まれることはなかった.

4.3.4 被験者の評価

被験者からは，ボタン色が同一色のみの場合に入力・覗き見ともに難しいという意見が多く見受けられた．また，移動の感度が高すぎるという操作性のさらなる改善を求める意見もあった.

5. 考察

本実験により，提案手法を用いると最大で 16.8%発生していた入力の失敗及び最大 1.17 回発生していたリトライが 0 となることが確認された．これにより，提案する操作性の改善手法が有用であることが確認された.

操作性の改善に対し，3 回の覗き見で 1 文字あたり最大 17%程度覗き見成功率が増加する結果となった（表 4）.

表 4 覗き見成功文字数の増減率（%）

実験 No	覗き見成功文字数の増減		
	1回目	2回目	3回目
1	−30.0	−37.5	16.3
2	−2.0	6.3	16.8
3	0.0	−6.3	6.3
4	0.0	1.3	12.5

しかしながら，2 回までの覗き見では覗き見成功文字数の増加は 6%程度ととどまっており，これは基本手法の 2 回までの覗き見に耐えるという実験結果と同様の結果となった.

これらの結果より，操作性の改善を施した場合でも，2 回までの覗き見に対し耐性を有することが確認された．一方，3 度の覗き見に対する強度は大きく低下していることから，プレイバックの多用は大きな耐性の低下を招くことも確認された.

入力時間については，1 回プレイバックを行うことでテンキーでは約 8 秒, キーボードでは最大 13 秒ほど時間がかかることが判明しているが，入力失敗に伴う再入力にはテンキーでは約 17 秒，キーボードでは約 28 秒かかることから，これらのリスクをなくすためには必要なコストであると考えている．また，プレイバックを利用するためのシャッフルボタンが小さすぎて，細かな操作が難しかったことも時間がかかっている要因となっているため，さらなる改善により今後の解決すべき課題とした.

6. おわりに

本稿では，覗き見耐性を持つ暗証番号・パスワード入力手法に対する操作性の改善を提案した．最初に，基本手法について，その利点と問題点をまとめた．次に，移動を見逃してしまう問題に対する対策を提示した．続いて，対策を施したことによる覗き見強度と，ユーザ負荷に対し評価実験を行った．最後に，評価実験についてまとめ，操作性の改善を施した場合でも，2 回までの覗き見に対しては大きな耐性の低下を招かず，かつユーザに過度な負荷をかけないことが確認された.

本稿の改善により，一定の覗き見耐性を保ちつつ，操作性が改善されることが確認された．今後は，覗き見耐性を維持しつつ，さらなるユーザ負荷の軽減が課題となる.

謝辞

評価実験に参加頂いた方々に深謝します.

参考文献

[1] Tandy Willeby：Secure key entry using a graphical user interface, US20020188872 A1(US 09/874,274).
[2] 田中進，高橋信介：暗証番号入力装置及び暗唱番号入力方法, 特願 2002-134808 (特開 2003-330888).
[3] 桜井鐘治，高橋渉：モバイル個人認証方式の提案と実装，情報処理学会研究報告コンピュータセキュリティ，No.122, pp.49-54, 2002-12-20.
[4] 牧田和久：パスワード入力装置及びパスワード入力方法，特願 2005-340699 (特開 2007-148658).
[5] 高田哲司:フェイクポインタによる暗証番号入力装置及び暗唱番号入力方法，特願 2007-175073（特開 2008-33924).
[6] 高田哲司：fakePointer：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, 2008-09-15.
[7] 柿沼泰，丸山一貴：画像における色の近さを用いたスマートフォン画面の認証方式，情報処理学会，第 76 回全国大会講演論文集，No.4, pp121-12, 2014-03-11.
[8] 小林 心，小國 健，中川 正樹：複数ボタンの移動追跡困難性を利用した覗き見耐性を持つ暗証番号・パスワード入力手法，コンピュータセキュリティシンポジウム 2017，pp.728-733，2017.10.23-25