Computer Security Symposium 2017
23 - 25 October 2017

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

小林 心[†1]　小國 健[†2]　中川 正樹[†1]

概要：本稿では，安全な暗証番号・パスワードの入力手法を提案する．銀行の端末や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．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．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，ユーザ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，それを入力する．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，実用性が高い．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．

キーワード：暗証番号，パスワード，個人認証，覗き見，ショルダーハッキング

A PIN Code/Password Input Method Resilient to Shoulder Hacking using Difficulty of Tracing Multiple Button Movements

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

Abstract: This paper presents a secure PIN code/password input method. When a person inputs a PIN code or password to a smartphone, tablet, banking terminal, 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. In performance evaluation, we confirmed that this method has resistance to shoulder hacking.

Keywords: PIN code, Password, User Authentication, Peeping, Shoulder Hacking

1. はじめに

暗証番号は，ユーザを識別認証するために，システムとユーザの間で設定される秘密の数字であり，ユーザの情報や資産・機器などにアクセスするために用いられる．また，パスワードとは，暗証番号と同じ用途で用いられ，一般的に数字のみではなく，文字や記号などの様々な字種を利用できるものであり，暗証番号はパスワードの一種とみなすことができる．

日常生活において，暗証番号・パスワードなどの機密情報を使う機会は格段に増えており，金融機関の ATM，クレジットカードの電子決済，スマートフォン・タブレット端末における個人認証など多岐にわたる．

特に，近年のスマートフォン・タブレット端末の普及は著しく，それに比例して野外や電車・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．

これらの暗証番号・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，ユーザ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．単純に，キー配列を入力の度ごとにランダムに配置し直すことで，操作者の腕や指の位置による暗証番号の推測を困難にする提案がある [1]．しかし，この方法では操作者がキーを探す必要が生じる．そこで，田中らは，円形に沿って 0 から 9 の数字キーを配列するとともに，基本となる 0 の数字キーを他の数字キーとは色を変えて識別しやすくしておき，暗証番号を 1 桁入力するたびに数字全体を回転させることで，目的の数字キーを探す時間の増大を抑えつつ，操作者の腕・指の位置による暗証番号の推測を困難にする技術を提案している [2]．しかし，この方法では，キーを入力する瞬間の覗き見には耐性がない．桜井らは，パスワードとして利用できる

†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

文字をグループ化し，各グループに割り振ったランダムな値を選択させることで，操作者の腕や指の位置によるパスワードの推測を困難にしている．さらに，それらの値を加算した値を入力させることでパスワードの推測をより困難にする技術を提案している[3]．しかし，ユーザは文字を探したり計算したりしないといけないため，ユーザの認知的負荷が大きくなる．また，グループに割り振った値を利用するため，パスワードの情報量が減少してしまう．牧田は，入力値表の一部の領域だけを表示し，この入力値表を上下左右にスライド（スクロール）させながらパスワードを入力することで，各入力値の相対位置を保持しつつ，操作者の腕や指の位置によるパスワードの推測を困難にする技術を提案している [4]．しかし，この方法も，キーを入力する瞬間の覗き見には耐性がない．高田は，既存の認証に利用している秘密情報に加えて，回答選択情報と呼ぶ使い捨てのパスワード（図形）を導入し，上位層に通常の数字キー，下位層に図形の並びを重ねて表示し，ユーザは上位層の数字キーがパスワードの図形に一致するまでキー配列を１個ずつ移動し，一致したときに確定する方式を提案している．[5, 6]．この方法は，ビデオ撮影を含めて，キーを入力する瞬間の覗き見に耐性がある．しかし，暗証番号という秘密情報を隠すために新たな秘密情報を導入している．柿沼らは，色の列をパスワードとして利用し，画像上に表れる同一色をタッチすることを繰り返してパスワードを入力させる方法を提案している．画像を入力の度に変えることで，指の動きからパスワードを推定することを難しくしている[6]．しかし，色をパスワードとして利用するため，色覚異常者は利用が困難である．また，パスワードに色や背景の情報を利用するため，既存のパスワード認証方式をそのまま利用することはできない．このように，ショルダーハッキング防止の研究がいろいろなされているが，新たな秘密情報を追加していたり，別の記憶や頭の中での計算を要したりするため，ユーザの認知的負荷の増大やシステムへの変更を要し，導入がためらわれるものが多い．

一方，これらとは別に，生体情報を利用した認証方式がある．個々人に固有な情報である，指紋，指・手静脈，虹彩，網膜，顔，声帯などを利用した方式が研究されている[7]．これらの手法は，パスワードや物による認証と比べ，忘却や紛失により認証ができなくなる，あるいは，漏洩や盗難により第三者に認証される危険性が低いと考えられる．そのため，ユーザにとって手軽な認証手段として電子機器の簡易認証から，より認証精度の高い認証方式としてパスポートやキャッシュカードの認証などに幅広く利用されている．しかし一方で，生体情報は更新することが不可能であることから，一度漏洩してしまうと回復不可能であるため，ユーザ・管理者共に取扱に慎重を要する．また，第三者が誤って認証されたり，ユーザ本人が認証に失敗したりする危険性もある．さらに，機器の整備などシステムを変更する必要があることから，導入コストが高いという問題もある．

以上のことから，本稿では，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・パスワード入力方法を提案する．

本稿で提案する手法では，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．

第 2 章では，一定の覗き見強度をもつ暗証番号・パスワード入力手法を提案する．第 3 章では，提案手法に対する評価実験の構成と手順，その結果を提示する．第 4 章では，評価実験から得られた結果をもとに，本手法の覗き見強度について議論する．

2. 暗証番号入力の提案手法

前章では，既存の手法における問題点として，ユーザ負荷やハードウェアの制約，サーバサイドの変更の必要性などを挙げた．本章では，既存の入力装置の拡張として利用可能であり，かつ一定の覗き見強度をもつ暗証番号の入力手法を提案する．

2.1 提案手法の基本方針

提案手法では，図 1 に示すように，システムは各ボタンに色や形を付加することができる．ユーザは，周囲に覗き見の心配がない場合は，表示されているボタンをそのままタッチして暗証番号を入力する．周囲に覗き見の可能性がある場合には，システムにボタンの移動を指示する．ボタンの移動を指示されたシステムは，図 2 に示すように，ボタンの文字表示を消し，図 3 に示すように，複数のボタンを同時に移動させる．ユーザは，図 4 に示すように，移動した先にある目的のボタンをタッチすることで暗証番号を入力する．図 2・図 3・図 4 では説明のため「１」のボタンだけ文字を表示しているが，本来は表示しない．

ユーザは目的のボタンを知っているため，単一のボタンだけを見ていればよいが，覗き見者はすべてのボタンの動きを追わなければならない．一般的に複数のボタン全ての移動を同時に追うのは困難であることから，本手法で入力した方が，何も対策をせずに入力するよりも，覗き見に対してより安全であると期待できる．

本手法は，安全性を最優先とする入力手法ではない．例えば，カメラ等により録画されることに対する耐性はない．しかしながら，本手法はボタンの動きだけを利用しているため，暗証番号として保存する機密情報の変更が必要なく，導入はクライアント側だけで行える．これにより，サーバ

のプログラムの変更やユーザの記憶する機密情報の変更といった負荷がなく，既存の手法と比べ，導入が比較的容易であるという利点がある．

図 1　初期状態
Figure 1　Initial state

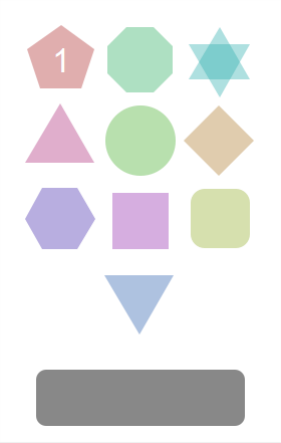

図 2　キー表示の消去状態
Figure 2　Erasing keys

図 3　移動中
Figure 3　Under movement

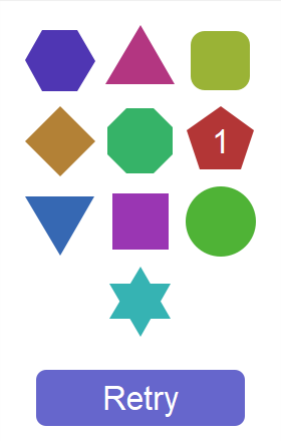

図 4　移動後
Figure 4　After movement

2.2　提案手法の種類と拡張

提案手法では，移動の視認性の向上や利用者の特性や障害を考慮し，表 1 に示すように，ボタンに幾つかの種類を想定している．

表 1 ボタンの種類
Table 1　Variations of buttons

種類	例	補足
ボタン色	同一色	特定の色を用いる
	多色	ボタンごとに異なる色を用い
ボタン形状	単一形状	円形・矩形など
	多形状	多角形・星型など ボタンの一部，または全部に異なる形状を用いる
ボタン背景	特殊効果	グラデーション・パターンなど
	画像	テクスチャ・写真など

これらを組み合わせることで，様々な種類を想定できる．これらのうち，ボタンごとに異なる色や形状を付与するものを利用する場合，視認性は向上する一方で，覗き見の追跡困難度が低下することも考えられる．また，機器による制約により，これらの一部が使えないことも考えられる．

また，ボタンの移動方法についても，表 2 に示すように幾つかの種類を想定している．

表 2　移動の種類
Table 2　Variations of movement

例	概要
通常移動	時間をかけて移動先へ移動する
瞬間移動	時間をかけずに移動先へ移動する

瞬間移動を用いる場合，通常移動の場合と異なり，ボタン同士が完全に識別できる必要がある．それにより，ボタンの種類にある程度の制約が発生する．

また，提案手法の拡張として，図 5 に示すように，様々なパスワードに対応するために，QWERTY 配列を模したものに拡張することなどが考えられる．

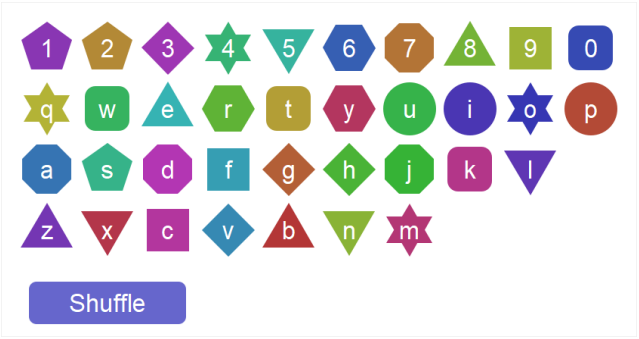

図 5　QWERTY 配列を模したキーボード
Figure 5　QWERTY like keyboard

3.　提案手法の評価

本章では，提案手法の覗き見強度やユーザ負荷を検証するための評価実験について述べる．

3.1　評価実験の構成

本評価実験の目的は，本手法の覗き見強度やユーザ負荷を測定することと，ボタンの種類による覗き見強度やユーザ負荷の違いを測定することである．本実験では，表 3 に示すように，通常のキーボードと比較するための，ベンチマーク用の実験 2 種類（B1 と B2）と，ボタンの種類や移動方法の異なる，13 種類のテンキー・キーボードを準備した．

表 3　実験用キーボードリスト

Table 3　List of keyboards for evaluation

実験No	キーボード	ボタン色	ボタン形状	移動方法
B1	テンキー	同一色	円形	移動なし
B2	QWERTY			
1	テンキー	同一色	円形	通常移動
2		多色		
3		同一色	10形状	
4		多色		
5		多色	円形	瞬間移動
6		同一色	10形状	
7		多色		
8	QWERTY	同一色	円形	通常移動
9		多色		
10		同一色	10形状	
11		多色		
12		多色	円形	瞬間移動
13		多色	10形状	

表 3 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．

瞬間移動を行う場合，色および形状がどちらも単一であると識別ができないため，どちらか一方が異なるものと，色と形の両方異なるものを実験の対象とした．また，ボタン形状が 10 種類しか用意しておらず，またこれより多い場合，形状の記憶・識別が困難となることから，36 キーを要する QWERTY 拡張では，瞬間移動を行う場合には，色が異なるものだけを実験の対象とした．

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，22 歳から 59 歳までの男女 6 名に対し行った．内訳を表 4 に示す．

表 4　被験者リスト

Table 4　List of subjects

No	年齢	性別	利き手
1	22	男	右
2	23	男	右
3	22	男	右
4	23	男	右
5	54	女	右
6	59	男	右

3.2 実験手順

被験者はペアとなり，実験を行った．以下被験者 2 名をそれぞれ A・B と表記する．

1. 事前説明：実験手順と入力方法について事前の説明を行った．この際，テンキー・キーボードそれぞれにつき，1・2 度のデモを実験者が行った．

2. ベンチマーク：本手法のような移動を行わずに入力した場合についての覗き見強度とユーザ負荷を計測した．利用者・覗き見者を交代しながら，テンキー・キーボードの順に，交互に計測を行った．

3. 入力実験：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．ただし，被験者によって一部実施していないキーボードも存在する．

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．ただし，途中ですべての文字の覗き見に成功した場合はその時点で終了し，残りの試行でも覗き見に成功したとしている．また，利用者が 1 文字で 3 回リトライした場合，その文字の入力に失敗したものとして，次の文字に移行することとした．

4. アンケート：すべての実験終了後，簡単なアンケートを実施した．

3.3 実験結果

3.3.1 覗き見成功率

各キーボードにおける，各回の覗き見成功文字数と 4 文字覗き見成功率を表 5 に示す．

移動をしないベンチマークでは 1，2 度の覗き見で暗証番号を盗まれてしまっていたが，提案手法では多くの場合で 3 度の覗き見に耐えることができることが確認できた．また，QWERTY 拡張でも，3 度の入力で盗まれていたパスワードが，すべての場合で最大でも 1，2 文字程度しか盗まれなくなった．

表 5　覗き見成功文字数と 4 文字覗き見成功率

Table 5　Number of stolen characters and rate of stolen PINs/passwords.

実験	キーボード	ボタン色	ボタン形状	移動方法	覗き見成功文字数			4文字覗き見成功率		
					1回目	2回目	3回目	1回目	2回目	3回目
B1	テンキー	同一色	円形	移動なし	3.33	4.00	4.00	0.83	1.00	1.00
B2	QWERTY				3.67	3.83	4.00	0.67	0.83	1.00
1	テンキー	同一色	円形	通常移動	1.20	2.00	1.60	0.00	0.00	0.20
2		多色			0.83	1.17	1.83	0.00	0.00	0.17
3		同一色	10形状		1.00	0.67	1.50	0.00	0.00	0.00
4		多色			0.83	1.50	1.83	0.00	0.00	0.17
5		多色	円形	瞬間移動	0.00	0.00	0.17	0.00	0.00	0.00
6		同一色	10形状		0.40	1.00	0.80	0.00	0.00	0.00
7		多色			0.40	0.60	1.40	0.00	0.00	0.00
8	QWERTY	同一色	円形	通常移動	0.00	0.25	0.00	0.00	0.00	0.00
9		多色			0.17	0.17	0.33	0.00	0.00	0.00
10		同一色	10形状		0.00	0.00	0.40	0.00	0.00	0.00
11		多色			0.00	0.20	0.00	0.00	0.00	0.00
12		多色	円形	瞬間移動	0.00	0.00	0.00	0.00	0.00	0.00
13		多色	10形状		0.00	0.00	0.00	0.00	0.00	0.00

表 6　入力成功文字数とリトライ回数

Table 6　Number of successfully input characters and number of retries.

実験 No	キーボード	ボタン色	ボタン形状	移動方法	全体		20代		50代	
					入力成功文字数	リトライ回数	入力成功文字数	リトライ回数	入力成功文字数	リトライ回数
B1	テンキー	同一色	円形	移動なし	3.94	0.00	4.00	0.00	3.83	0.00
B2	QWERTY				3.78	0.00	3.92	0.00	3.50	0.00
1	テンキー	同一色	円形	通常移動	3.93	0.27	4.00	0.00	3.83	0.67
2		多色			4.00	0.00	4.00	0.00	4.00	0.00
3		同一色	10形状		3.94	0.06	4.00	0.00	3.83	0.17
4		多色			4.00	0.00	4.00	0.00	4.00	0.00
5		多色	円形	瞬間移動	3.83	0.50	3.92	0.42	3.67	0.67
6		同一色	10形状		3.60	0.47	3.78	0.22	3.33	0.83
7		多色			3.87	0.13	3.89	0.00	3.83	0.33
8	QWERTY	同一色	円形	通常移動	3.75	0.58	3.83	0.00	3.67	1.17
9		多色			3.80	0.33	4.00	0.22	3.50	0.50
10		同一色	10形状		3.67	0.27	3.89	0.00	3.33	0.67
11		多色			4.00	0.07	4.00	0.00	4.00	0.17
12		多色	円形	瞬間移動	1.67	0.67	2.00	0.50	1.33	0.83
13		多色	10形状		3.87	0.20	3.89	0.11	3.83	0.33

表 7　入力時間（秒）

Table 7　Input time (Sec)

実験 No	キーボード	ボタン色	ボタン形状	移動方法	全体			20代			50代		
					入力時間	1文字あたり移動込み/抜		入力時間	1文字あたり移動込み/抜		入力時間	1文字あたり移動込み/抜	
B1	テンキー	同一色	円形	移動なし	2.86	0.95		2.89	0.96		2.79	0.93	
B2	QWERTY				5.45	1.82		1.39	0.46		13.59	4.53	
1	テンキー	同一色	円形	通常移動	12.91	1.99	0.99	9.87	1.72	0.72	17.46	2.40	1.40
2		多色			12.09	1.99	0.99	9.82	1.77	0.77	16.64	2.44	1.44
3		同一色	10形状		13.46	1.99	0.99	10.13	1.74	0.74	20.13	2.50	1.50
4		多色			12.17	2.00	1.00	9.94	1.74	0.74	16.63	2.50	1.50
5		多色	円形	瞬間移動	12.99	1.60		10.89	1.39		17.18	2.01	
6		同一色	10形状		14.80	1.96		11.08	1.67		20.39	2.39	
7		多色			11.54	1.40		7.82	1.08		17.13	1.88	
8	QWERTY	同一色	円形	通常移動	22.03	2.52	1.31	16.18	1.97	0.64	26.90	2.97	1.97
9		多色			20.98	2.19	1.19	17.51	1.89	0.89	29.32	2.78	1.78
10		同一色	10形状		16.77	2.27	1.27	12.05	1.88	0.88	23.85	2.86	1.86
11		多色			19.02	2.20	1.20	11.93	1.84	0.84	29.66	2.73	1.73
12		多色	円形	瞬間移動	27.88	3.15		29.66	3.37		25.20	2.81	
13		多色	10形状		22.00	2.58		15.91	2.10		31.12	3.30	

3.3.2 入力難度

各キーボードにおける，入力に成功した文字数と，リトライを行った回数の平均を表 6 に示す．20 代については，予備実験と比べて，入力成功文字数に大きな差はなく，リトライ回数も数回程度にとどまっている．50 代については，同じ条件においては，色や形が異なっているほど，入力成功率が高く，リトライ回数が少なくなることが確認された．

また，全体として，実験 12 番の入力成功文字数が少ないが，これについては考察で述べる．

3.3.3 入力時間

各キーボードにおける，4 文字の入力にかかった時間と，1 文字あたりの，移動指示から入力までの時間，移動完了から入力までの時間を表 7 に示す．

移動をしないベンチマークと比べ，最小で 2.7 倍，最大で 10 倍以上の時間がかかっている．また，20 代による 12 番の実験や 50 代のベンチマーク実験 2 番において大きな値を記録しているが，これについては考察で述べる．

4. 考察

実験 12 番の実験結果について先に述べる．12 番の入力結果は入力成功文字数・入力時間ともに非常に悪い結果となっている．12 番のボタンには色以外の識別可能な情報が存在しないため，36 個のボタンに個々を識別できる色を配色する必要がある．しかし，本実験では 36 個のボタンの色を色相において等間隔に配置した結果，色同士が色相で最小 10 度しか違わないため，ディスプレイの色再現性の悪さと合わさり，識別が困難であったことに起因するものである．入力成功文字数が 2 文字以下となっていることから，実験 12 番については実用性がないものであると判明した．以下では，12 番を除いた残りのキーボードについて述べる．

本実験により，提案手法は覗き見に対し，一定の強度を有していることが確認された．テンキーにおいては，2 回までの覗き見では，暗証番号のすべての文字を取得することはできず，3 回の覗き見でも，覗き見に成功した文字数は半数にとどまっている．QWERTY 拡張では，3 回の覗き見ではパスワードを取得することはできず，最大で 1 文字の覗き見にとどまった．

入力成功文字数については，本手法導入により最大 15% 程の低下が見られた．とくに同一色の場合にその傾向が強く，色が重要な情報となっている事が判明した．また，瞬間移動は入力失敗を招きやすいが，色や形の情報により，失敗を防ぐことができることも確認できた．リトライ回数も同様に，色や形が異なるほど，リトライ回数が少なくなっている．これらの結果から，十分な色や形の情報が付加される場合，移動しない場合とくらべてユーザ負荷が過剰に大きくなることはないと考えられる．

入力時間に関しては，移動しない場合と比べて数倍必要となっており，システムによっては許容できない増加となることも考えられる．しかし，本手法では，移動せず直接入力対象をタッチすることを許容できるため，ユーザ及び管理者が許す場合には，直接番号を入力することができる．これにより，非常時や覗き見の心配のない場合には入力の時間を省くことができる．

なお，50 代の QWERTY 拡張が特に時間がかかっている傾向にあるが，これは，50 代の被験者の一人が普段から QWERTY キーボードを取扱う環境にいないため，入力に時間がかかったことが原因と考えられる．

5. 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を提案した．最初に，従来の手法について，その利点と問題点をまとめた．次に，覗き見耐性を持ち，導入が比較的容易な，新たな暗証番号・パスワードの入力手法を提案した．続いて，本手法の覗き見強度と，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，本手法は複数回の覗き見に対し，一定の耐性を持っており，かつユーザに過度な負荷をかけないことが確認された．

本手法は，安全性を最優先とする入力手法ではない．しかしながら，暗証番号・パスワードを変更する必要なく，サーバの変更を必要としない，比較的導入が容易な手法としては，一定の覗き見耐性を持っていることが確認された．今後，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] 坂野鋭：生体認証技術の最近の動向，日本法科学技術学会誌，Vol.12, No.1, pp.1‐12, 2007-06-27.