ワンタイム図形生成に基づく特定の認証キーのない認証手法

石井 健太郎[1,a)]　香川 将樹[2]

概要：パスワードをはじめとした認証キーを用いた認証手法では，何らかの方法で認証キーを他者が取得した場合，他者の不正認証を防ぐことができない．本研究では，この問題の低減を目指して，特定の認証キーのない認証手法を提案する．提案手法では，被認証者が知る認証画像群生成ルールに基づいて，ワンタイムの正解図形とダミー図形を生成して画面に提示する．被認証者は，提示された図形群の中から正解図形を選ぶことによって認証を受ける．毎回異なる図形が表示されるため，特定の認証キーはなく，ショルダーハッキングが行われた場合であっても他者の不正認証を防ぐことが期待できる．認証画像群生成ルールを知る実験参加者が認証場面を，別の実験参加者がショルダーハッキングを行う評価実験を行ったところ，認証画像群生成ルールによっては，ショルダーハッキングを認めているにも関わらず高い本人パス率と他者拒否率を示した．一方で，本人パス率や他者拒否率が低い認証画像群生成ルールも存在し，認証画像群生成ルールにナイーブな手法であることも明らかになった．この結果をもとに，本論文では，この手法の現在の制限と改良の可能性を議論する．

キーワード：画像認証，ワンタイムパスワード，ワンタイム図形生成

Authentication Method without Specific Authentication Key based on One-Time Shape-Pattern Generation

Kentaro Ishii[1,a)]　Masaki Kagawa[2]

Abstract: In key-based authentication like usual password authentication, it is hard to except a non-genuine user if the user acquires the authentication key. We propose an authentication method without a specific authentication key aiming at reducing this problem. In the proposed method, a one-time correct figure and dummy figures are generated based on predefined shape-pattern generation rules. The authenticated person is authenticated by choosing the correct figure from the presented group of figures. Since different figures are displayed each time, there is no specific authentication key, and it can be difficult for another person to acquires the authentication key or the shape-pattern rule even if conducting shoulder hacking. We performed an evaluation experiment that one participant who knew the shape-pattern generation rule did authentication, while another participant who did not knows the rule did shoulder hacking. The result showed that high genuine user pass rates and high non-genuine user rejection rates were achieved with some shape-pattern generation rules. Meanwhile, the proposed method showed a naive characteristic by the shape-pattern rules in that, with other shape-pattern generation rules, some showed low genuine user pass rates, and some showed low non-genuine user rejection rates. Based on this result, this paper discusses the limitation and the possible improvements of the proposed method.

Keywords: image-based authentication, one-time password, one-time shape-pattern generation

1. はじめに

パスワードをはじめとした認証キーを用いた認証手法では，何らかの方法で認証キーを他者が取得した場合，他者

[1] 専修大学
Senshu University
[2] 三菱電機インフォメーションシステムズ株式会社
Mitsubishi Electric Information Systems Corporation
[a)] kenta@pc.fm.senshu-u.ac.jp

の不正認証を防ぐことができない．多くの手法では，入力の位置から認証キーを推測することが可能であり，認証場面のショルダーハッキングにより，認証キーを取得することが容易である．

本研究では，この問題の低減を目指して，特定の認証キーのない認証手法を提案する．特定の認証キーがなければ，ショルダーハッキングが行われても，他者が次に認証を受けるときには異なる表示がなされるため，正解を知ることができずに不正認証を防ぐことが期待できる．提案手法では，あらかじめ決められた認証画像群生成ルールに基づいて，ワンタイムの正解図形とダミー図形を生成して画面に提示する．被認証者は提示された図形群の中から，正解図形を選ぶことによって認証を受ける．

本論文では，関連研究をまとめたあと，提案手法であるワンタイム図形生成に基づく認証手法について述べる．また，提案手法を評価するために行った実験の手順と結果をまとめ，提案手法の現在の制限と今後の改良の可能性を議論する．

2. 関連研究

通常のパスワード認証のような文字の記憶と比較して，人間の画像再認能力は高いとされており，このことを利用した画像認証手法は記憶負荷が通常のパスワード認証手法よりも低いと考えられている．本研究でも用いている画像そのものを選択する Cognometric 方式の画像認証としては，Déjà Vu が提案されている [1]．Déjà Vu では，コンピュータで生成した画像から認証キーとなる 5 枚の正解画像をあらかじめ決めておき，認証は 25 枚の提示画像の中から 5 枚の正解画像を選択することによって行う．しかし，被認証者とは無関係で意味のない画像を用いているため，記憶負荷低減の効果が限定的である可能性がある．

そこで，被認証者が自身で正解画像とダミー画像を登録・追加できる仕組みも提案されている．あわせ絵 [2], [3] は，そのような仕組みを持つ認証システムであり，個人のエピソードに基づく再認しやすい画像を認証に用いることができる．また，ダミー画像の登録を検索エンジンの画像検索を用いることによって自動化することで，正解画像の登録のみを必要とする画像なぞなぞ認証も提案されている [4]．

しかし，以上までの手法は，提示されている画像が認証キーである正解画像そのものであるため，ショルダーハッキングが行われてしまうと，他者が不正に認証を受けることが容易である．本研究は，Cognometric 方式の画像認証においてもショルダーハッキングによる不正認証を防ぐ手法を扱う．

画像認証手法を離れると，認証コードを入力する際のマウスカーソルの動きを画面からでは知られないようにするため，ダミーのカーソルを画面に描画する手法 [5], [6], [7] や，入力されたパスワードに加えて打鍵の強さも認証キーとする手法 [8] のように，ショルダーハッキングの影響を低減する手法が提案されている．

Cognometric 方式の画像認証においては，認証キーの画像そのものではなく不鮮明化した画像をチャレンジ画像として提示することで，ショルダーハッキングの影響を低減する手法が提案されている [9]．認証キーとなる元画像を知らない他者には，チャレンジ画像を見ても元画像を特定することが難しい．しかし，この方式は認証キーを特定されなくても，困難ではあるが不鮮明化画像からレスポンスが推定できてしまう可能性が指摘されている．これに対して，この手法を Locimetric 方式の画像認証に応用して，同じチャレンジ画像に対して，指定の部位を変化させることで異なるレスポンスを生成させる手法も提案されている [10], [11]．本研究は，毎回異なるチャレンジ画像が提示される点において前者の提案と異なる．また，画像そのものを選択する Cognometric 方式を用いており，そのために Locimetric 方式よりも認証時のレスポンス生成が容易であることが期待できる点で後者の提案と異なる．

さらに，コンピュータで生成した画像から個人の嗜好を学習し，認証を行う手法も提案されている [12]．この手法は本研究と同様に特定の認証キーを持たない方法であるが，本研究の提案手法は，学習が進むのを待つ必要がない点と，提示画像のうちどれが正解画像であるかの一意性が保たれている点で異なる．

3. ワンタイム図形生成に基づく認証

3.1 図形生成基本アルゴリズム

提案手法で生成されるワンタイム図形は，正解図形もダミー図形も本節で述べる図形生成基本アルゴリズムによって生成される．**図 1** は，この図形生成基本アルゴリズムによって生成された 9 つの図形を例を示しており，1 つの正解図形と 8 つのダミー図形を含む．図形生成基本アルゴリズムは，Miyashita らの図形生成手法 [13] を参考にしてアレンジしたものである．

図形生成基本アルゴリズムの手続きを以下に示す．いずれの操作もランダムに選ばれるパラメータがあり，それにより毎回異なる図形が生成される．

(1) ランダムな数の頂点を持つ正多角形を用意する．
(2) 隣接した頂点を結んだ線分の中点に新しい頂点を作成し，図形の中心から新しい頂点までの距離が増加または減少するように，新しい頂点をランダムな距離だけ移動させる．（**図 2**; 各頂点の移動距離は同一である．）
(3) (2) をランダムな回数繰り返す．
(4) (3) までの操作で生成された多角形をランダムな色・ランダムな透明度で塗りつぶす．
(5) 図形の中心を軸にランダムな角度だけ回転させる．
(6) (5) までの操作で生成された図形をランダムな枚数だけ重ね合わせる．

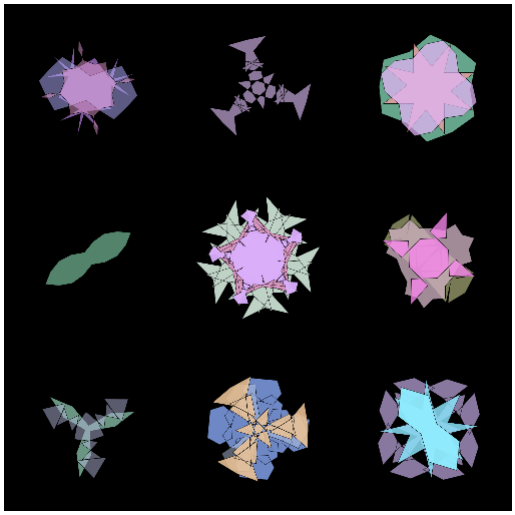

図 1　図形生成基本アルゴリズムによって生成された図形
Fig. 1　Shape Patterns Generated by the Basic Algorithm

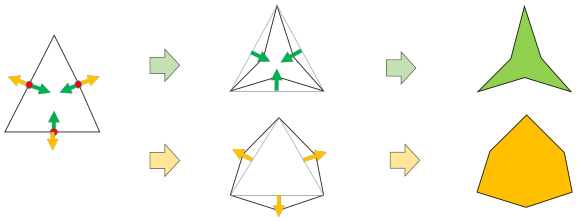

図 2　中点の移動による変形
Fig. 2　Deflection by Translation of Midpoints

(1) は初期図形として正多角形を生成する手続きであり，正多角形の中心から各頂点までの距離を固定とし，何角形となるかのみをランダムとした．本論文の実装では，頂点の数を 2〜5 の整数をとるように定めた．ただし，二角形という図形は一般には存在しないため，頂点が 2 つの場合は，2 つの頂点を結ぶ線分が同じ位置に 2 つあるものとしてその後の操作を進めることと定義した．

(2) は図形生成における最も重要な操作である．ランダムなパラメータが正であるか負であるかによって，中心から離れる方向に移動するか近づく方向に移動するかが決まる．直感的には，パラメータが正であれば図形が膨らみ，負であれば図形がしぼむ操作となる（図 2）．本論文の実装では，図形の中心から初期の正多角形の頂点までの距離の 1/2 が移動距離の絶対値の上限となるようなランダムな実数とした．(3) に示したとおり，この操作は複数回繰り返される．操作を行うごとに頂点の数は倍となり，図形は複雑になっていく．本論文の実装では，2〜4 回繰り返されるように定めた．

(4) は (3) までの操作で定まった頂点を結んでできる多角形に，色をつける操作である．色をランダムで定めるだけではなく，後述する (6) の重ね合わせのため透明な図形とし，その透明度もランダムに定めることとした．本論文の実装では，RGB 色空間の各成分と透明度はそれぞれ，256 階調の 0〜127 の整数をとるように定めた．

(5) は図形の方向を変える操作である．(1) の正多角形は偏角 0 の位置に頂点を持つように生成されるため，それを基礎とする (4) までで生成された図形も，いずれも同じ方向を向いているように見える．そこで，この段階で回転させることにより，見た目の方向を都度異なるようにすることが狙いである．本論文の実装では，角度を 0〜2π の実数をとるように，すなわち，制限を設けずに見た目の方向を変えることとした．

以上の操作により生成した色付きの多角形を，(6) の操作により 1 つ以上重ね合わせて最終的な図形を生成する．このことにより，より多様なパターンの図形が生成される．本論文の実装では，1〜3 枚の多角形を重ね合わせるように定めた．

3.2　認証図形群生成ルールと正解図形・ダミー図形の生成

図形生成基本アルゴリズムをもとにして，正解図形とダミー図形の組み合わせを生成する認証画像群生成ルールを定義する．ここで言う正解図形とは被認証者が認証時に選ぶべき図形であり，ダミー図形とは認証時に選ばざるべき図形である．したがって，認証図形群生成ルールが持つべき特徴として，ルールを知る者には正解図形をダミー図形から見分けることができることと，ルールを知らない者には正解図形からルールを推測できないことの 2 つがある．後者の特徴は，正解図形を画像群から選択する場面をのぞき見られても，他者が認証を受けることを防ぐために必要となる．

本研究では，認証画像群生成ルールは，3.1 節の図形生成基本アルゴリズムのパラメータを制限することで定義することとした．例えば，三角形を連想できるものをルールとする場合，正解図形の初期多角形には必ず三角形が選ばれるようにし，ダミー図形の初期多角形には決して三角形が選ばれないようにする．これは，言い換えると，図形生成基本アルゴリズムではランダムであった初期多角形の頂点の数のパラメータを，正解図形の場合は 3 に固定し，ダミー図形の場合は 3 以外のランダムとすることである．この方法によれば，原理的には図形生成パラメータが重複しない範囲で認証画像群生成ルールを定義することができる．

図形生成基本アルゴリズムのパラメータは，初期多角形の頂点の数・頂点追加時の移動距離・頂点追加の回数・色・透明度・画像の重ね合わせ枚数である．ルールを知る者には正解図形をダミー図形から見分けることができること・ルールを知らない者には正解図形からルールを推測できないことを考慮して検討のうえ，以下の 6 つの認証画像群生成ルールを定義した．6 つの認証画像群生成ルールにより生成された画像群を**図 3** に示す．

ルール 1　正解：初期多角形の頂点の数が 3，ダミー：初

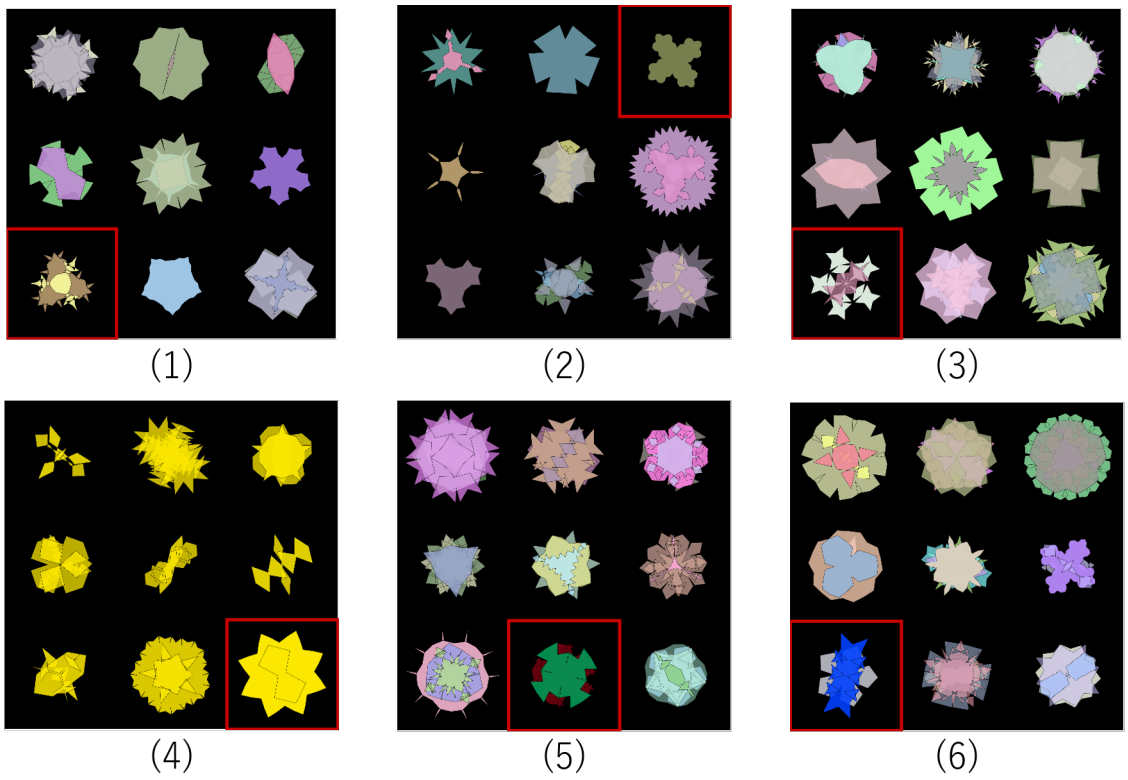

図 3 認証画像群生成ルールによって生成された図形群．1 つの正解図形と 8 つのダミー図形を含む．

Fig. 3 A Set of Shape Patterns Generated by the Authentication Generation Rules. Each includes one correct and eight dummy figures.

期多角形の頂点の数が 3 以外

ルール 2 正解：初期多角形の頂点の数が 4，ダミー：初期多角形の頂点の数が 4 以外

ルール 3 正解：画像の重ね合わせ枚数が 2，ダミー：画像の重ね合わせ枚数が 2 以外

ルール 4 正解：透明度が 0・色が黄色，ダミー：透明度が 55〜127・色は黄色

ルール 5 正解：色が赤・黄・緑のいずれか，ダミー：色が赤・黄・緑以外

ルール 6 正解：色がオレンジ・灰色・青・白のいずれか，ダミー：色がオレンジ・灰色・青・白以外

ルール 4 については，正解図形もダミー図形も色を黄色に固定している．これは，異なる色の図形同士では，その透明度が見分けづらいからである．

直感的には，以上のルールによって生成される正解画像は，以下のように解釈できる．したがって，これは重要なことであると考えるが，プログラムの内部構造やパラメータの種類を知らないユーザでもすぐにルールを把握することができる．

ルール 1 三角形を連想できるもの

ルール 2 四角形を連想できるもの

ルール 3 多角形が 2 枚重なったもの

ルール 4 明度が最も高いもの

ルール 5 信号機に用いられている色の組み合わせ

ルール 6 天気予報に用いられている色の組み合わせ

3.3 認証アプリケーション

認証アプリケーションは 3.2 節の認証図形群生成ルールを組み込み，認証のユーザインタフェースを追加したものである．Processing 言語で実装し，デスクトップアプリケーションと Android アプリケーションの 2 つを用意した（**図 4**）．

このアプリケーションでは，画面上に 9 つの図形が表示され，被認証者がそれらのうちの 1 つを選択するのを待ち受ける．図形の選択を行うと，ユーザフィードバックのための選択枠が表示されたのち，画面が切り替わり別の 9 つの図形が表示される．このプロセスを 3 回繰り返すと終了するようなアプリケーションである．各画面では，認証図形群生成ルールに基づいて 1 つの正解図形と 8 つのダミー図形が含まれており，すべての画面で正解図形を選択できれば認証される．

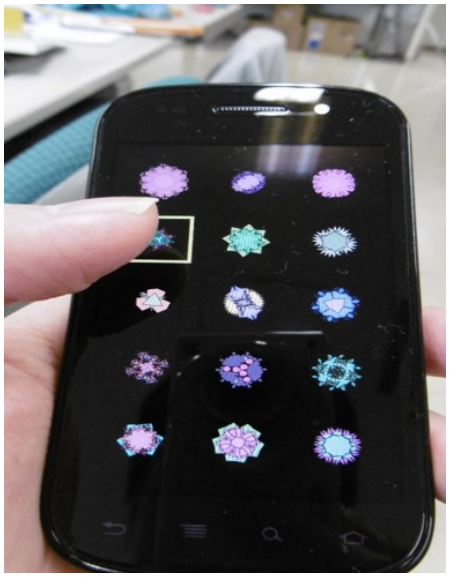

図 4　認証アプリケーション（Android アプリケーション）
Fig. 4　Authentication Application (Android Application)

図 5　実験手順
Fig. 5　Experiment Procedure

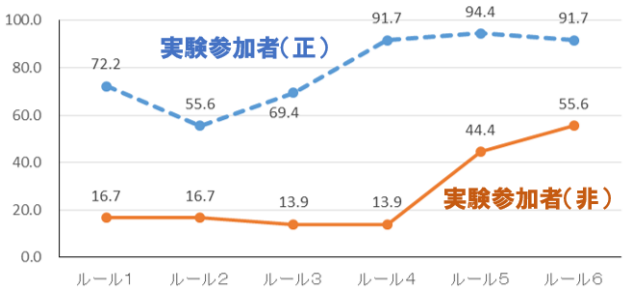

図 6　認証図形群生成ルールごとの平均正答率
Fig. 6　Acceptance Rate by Authentication Generation Rules

4.　評価

4.1　実験手順

実験は 2 名 1 組の実験参加者を招いて行う．1 名の実験参加者が正規の被認証者役となり，もう 1 名の実験参加者はショルダーハッキングを行う非正規の被認証者役となる．3.2 節で述べた 6 つの認証画像群生成ルールを 3 つずつに分け，実験の最中に正規・非正規の役割は交代して実験を行う．どのルールの組み合わせをどの順番で 1 名の実験参加者に割り振るかは，ルール間の学習・推定の効果を避けるためにカウンターバランスをとって実施する．以下では，正規の被認証者役の実験参加者を「実験参加者（正）」・非正規の被認証者役の実験参加者を「実験参加者（非）」と記述する．

各認証画像群生成ルールについて，以下の手続きで実験を実施する (**図 5**).

(1)　実験者が実験参加者（正）へ認証画像群生成ルールを提示する．この際に，パラメータの説明は行わず，3.2 節で述べた直感的な説明のみを行う．

(2)　実験参加者（正）が認証アプリケーション利用の練習を 6 回行う．

(3)　実験参加者（正）が認証アプリケーション利用のテストを 3 回行う．その間，実験参加者（非）は実験参加者（正）のそばでショルダーハッキングを行う．

(4)　実験参加者（正）の 3 回のテストの終了後，実験参加者（非）が認証アプリケーション利用のテストを 3 回行う．

4.2　結果

12 組 24 名の実験参加者を招き実験を実施した．**図 6** に，平均正答率を示す．一般的な傾向として，実験参加者（正）の正答率は実験参加者（非）の正答率より高く，ショルダーハッキングを自由に許しているにもかかわらず，実験参加者（正）と実験参加者（非）の認証成功の度合いは異なっていた．特に，ルール 4 では高い本人パス率と他者拒否率を同時に示した．しかし，ルール 1〜ルール 3 では，実験参加者（正）の正答率も落ち込んでおり，認証図形群生成ルールを知っていても見分けのつきづらいルールとなっていたことがわかる．逆に，ルール 5〜ルール 6 では，実験参加者（非）の正答率が上昇しており，ショルダーハッキングにより，推測できてしまうルールであったことが伺える．実験参加者（非）の平均正答率がチャンスレベル 11.1 と同等であるかの t 検定を行ったところ，有意水準 5%で，ルール 1〜4 では有意な差はなく，ルール 5〜6 では有意差があった．この結果は，統計的にはルール 5〜6 の実験参加者（非）があてずっぽうで回答していたのとは異なることを意味している．

5.　まとめ

本論文では，ショルダーハッキングによる他者の不正認証を低減することを目指して，特定の認証キーのない認証手法を提案した．提案手法では，認証画像群生成ルールに基づいて，ワンタイムの正解図形とダミー図形を生成して画面に提示する．毎回異なる図形が表示されるため，ショルダーハッキングが行われた場合であっても，他者が認証を受ける際の正解を知ることができずに不正認証を防ぐことが期待できる．

評価実験を行ったところ，認証画像群生成ルールによっては，ショルダーハッキングを認めているにも関わらず高

い本人パス率と他者拒否率を示した．一方で，本人パス率や他者拒否率が低い認証画像群生成ルールも存在し，認証画像群生成ルールにナイーブな手法であることも明らかになった．本人にわかりやすいルールであれば，他者にも推測しやすいものとなりやすく，他者に推測しにくいルールであれば，本人もわかりにくいものになりやすい．このジレンマを解決しなければ実用できる手法とはなりえない．現在その可能性の 1 つとして，複数のルールを混ぜることを検討している．ルールを推測するときには，ショルダーハッキングをする者はルールが何であるかを絞り込む作業をしているため，そのルールが都度切り替わるものであれば，他者の推測が十分に進まないことが期待できる．

また，今後はよりよい認証画像群生成ルールを追求するとともに，どのような要因が本人パス率と他者拒否率に寄与しているかの分析を進めていくことを計画している．十分な分析が進めば，画像以外の素材，例えば，文献 [14] にあるような，無意味文字列にも適用の可能性があると考える．

参考文献

[1] Dhamija, R., Perrig, A.: Déjà Vu: A User Study Using Images for Authentication, USENIX Security Symposium (2000).

[2] Takada, T., Koike, H.: Awase-E: Image-Based Authentication for Mobile Phones Using User' s Favorite Images, Human-Computer Interaction with Mobile Devices and Services, pp.347–351 (2003).

[3] 高田哲司，小池英樹：あわせ絵: 画像登録と利用通知を用いた正候補選択方式による画像認証方式の強化法，情報処理学会論文誌，Vol.44, No.8, pp.2002–2012 (2003).

[4] 増井俊之：インターフェイスの街角 (49)—画像を使ったなぞなぞ認証，Unix Magazine, Vol.17, No.1 (2002).

[5] Watanabe, K., Higuchi, F., Inami, M., Igarashi, T.: CursorCamouflage: Multiple Dummy Cursors as A Defense against Shoulder Surfing, ACM SIGGRAPH Conference and Exhibition on Computer Graphics and Interactive Techniques in Asia, Emerging Technologies, Article No.6 (2012).

[6] 渡邊恵太，樋口文人，稲見昌彦，五十嵐健夫：複数ダミーカーソル中における自分自身のカーソル特定，インタラクション 2013 論文集，pp.25–31 (2013).

[7] 渡邊恵太，門城拓，樋口文人，稲見昌彦，五十嵐健夫：SymmetricCursors: 対称的に動くダミーカーソルによる入力操作の隠蔽，インタラクション 2013 論文集，pp.255–256 (2013).

[8] Jun Kato, Daisuke Sakamoto, Takeo Igarashi: Surfboard: Keyboard with Microphone as a Low-cost Interactive Surface, ACM Symposium on User Interface Software and Technology, pp.387-388 (2010).

[9] 山本匠，原田篤史，漁田武雄，西垣正勝：画像記憶のスキーマを利用した認証方式の拡張—手掛かりつき再認方式，情報処理学会研究報告，Vol.2006-CSEC-34，pp.411–418 (2006).

[10] Yamamoto, T., Harada, A., Isarida, T., Nishigaki, M.: Advantages of User Authentication Using Unclear Images —Automatic Generation of Decoy Images—, IEEE International Conference on Advanced Information Networking and Applications, pp.668–674 (2009).

[11] 山本匠，漁田武雄，西垣正勝：不鮮明化画像を利用した暗示・応答型画像認証方式の提案，情報処理学会論文誌，Vol.50，No.9，pp.2062–2076 (2009).

[12] 持田達範，稲村勝樹：個人の嗜好で識別を行う画像認証方式，コンピュータセキュリティシンポジウム 2017 論文集，pp.933–940 (2017).

[13] Miyashita, Y., Higuchi, S., Sakai, K., Masui, N.: Generation of fractal patterns for probing the visual memory, Neuroscience Research, Vol.12, No.1, pp.307–311 (1991).

[14] Takahashi, M.: Memorial consequences of choosing nonwords: Implication for interpretations of the self-choice effect, Japanese Psychological Research, Vol.34, No.1, pp.35–38 (1992).