情報処理学会論文誌 Vol.60 No.12 2127–2138 (Dec. 2019)

ワンタイム図形生成に基づく個人認証の生成ルールとその評価

石井 健太郎[1,a)] 香川 将樹[2] 島谷 和樹[1]

受付日 2019年3月12日, 採録日 2019年9月11日

概要：パスワード/パスコード認証やパターンロック認証では，認証場面ののぞき見により他者が不正認証を受けるための情報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，ワンタイム図形生成に基づく認証手法を提案する．提案手法では，正規のユーザが知る認証図形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．画面にはつど生成された図形が提示されるため，のぞき見が行われた場合であっても正解の手がかりをつかみにくいことが期待できる．詳細な検討の結果，提案手法の認証図形群生成ルールとして，4 カテゴリ 12 ルールを定義した．定義したルールについて，1 名の実験参加者が認証を受けている場面をもう 1 名の実験参加者がのぞき見を行う評価実験を行ったところ，のぞき見を認めているにもかかわらず高い本人パス率と他者拒否率を示し，同様の既存手法と比較してのぞき見への対策性能が高いことが示された．

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

Generation Rules and Evaluation of Authentication based on One-time Shape-Pattern Generation

Kentaro Ishii[1,a)] Masaki Kagawa[2] Kazuki Shimatani[1]

Received: March 12, 2019, Accepted: September 11, 2019

Abstract: In password/passcode-based authentication or draw-a-secret authentication, a non-genuine user can infer password/passcode or secret pattern by shoulder surfing. We propose an authentication method based on one-time shape-pattern generation aiming at reducing the shoulder surfing problem. In the proposed method, a one-time correct figure and dummy figures are generated based on a predefined shape-pattern generation rule. The user of the proposed method is authenticated by choosing the correct figure from the presented group of figures. Since different figures are displayed at different locations each time, it can be difficult for another person to acquire the shape-pattern generation rule even if conducting shoulder surfing. With in-depth examination, we defined 12 shape-pattern generation rules categorized into four groups for the proposed method. We performed evaluation experiments, where one participant knowing the shape-pattern generation rule did authentication, while the other participant not knowing the rule did shoulder surfing. The result of the first experiment showed that the proposed method achieved high genuine user pass rate and high non-genuine user rejection rate, and the result of the second experiment showed that the proposed method outperformed existing graphical authentication methods in terms of shoulder surfing defense.

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

1. はじめに

通常のパスワード/パスコード認証やスマートフォンで見られるパターンロック認証では，何らかの方法で他者がパスワード/パスコードやパターンを取得すると，不正認

[1] 専修大学
Senshu University, Kawasaki, Kanagawa 214–8580, Japan
[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, Shinagawa, Tokyo 140–0001, Japan
[a)] kenta@pc.fm.senshu-u.ac.jp

証を受けることができてしまう．また，これらの認証手法では，入力の位置からパスワード/パスコードやパターンを推測することが可能であり，認証場面ののぞき見により他者が不正認証を受けるための情報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，ワンタイム図形生成に基づく認証手法を提案する．認証時にはつど生成された図形が提示されることが提案手法の特徴であり，のぞき見が行われても，他者が次に認証を受けるときには異なる図形が提示されるため，正解の手がかりをつかみにくいことが期待できる．提案手法では，あらかじめ決められた認証図形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．認証図形群生成ルールを知る被認証者は，つど生成された図形であっても正解図形を選ぶことができる．

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調査の手順と結果をまとめる．なお，本論文は，国内会議 [1] にて口頭発表を行ったプロトタイプ実装を基礎として，3.2 節で述べる認証図形群生成ルールの包括的な検討と 4 章で述べる詳細な評価を行ったものである．

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，通常のパスワード認証手法よりも記憶負荷が低いと考えられている．画像認証は，画像そのものを選択する Cognometric 方式・画像の中の特定の場所を選択する Locimetric 方式・図形の描画操作を行い登録された図形と比較する Drawmetric 方式の 3 つに大きく分類されるが，本研究でも用いる Cognometric 方式の画像認証としては，Déjà Vu [2] や PassFaces [3] が提案されている．Déjà Vu では，コンピュータで生成したランダムアート画像から 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．PassFace では，顔画像のデータベースから 5 枚の正解画像がランダムで与えられ，認証は 9 枚の提示画像の中から 1 枚の正解画像を選択することを 5 回繰り返すことによって行う．ランダムアート画像と顔画像では，人間にとって再認しやすさが異なる可能性があるが，いずれにおいても，ユーザとは無関係な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，ユーザ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 [4], [5] 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 [6]．

しかし，以上までの手法は，提示されている画像が正解画像そのものであるため，のぞき見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のぞき見による不正認証を防ぐ手法を扱う．

画像認証におけるのぞき見の影響を低減する手法としては，Cognometric 方式と Locimetric 方式を組み合わせた方法が提案されている [7], [8], [9]．いずれの手法も画面に提示されている多数の画像の中から認証に用いる複数の画像を探し出す Cognometric 方式の作業と，探し出した画像を結んで形成される凸包の中の座標をクリックする Locimetric 方式の作業を行うことが認証の原理であり，クリックした座標からは画像が推測しにくいことが，のぞき見対策となる．Wiedenbeck らの論文では 1 回の認証試行にかかる時間が平均 71.66 秒と報告されており [7]，残り 2 つの論文では認証にかかる時間は記載されていないが同様であると考えられる．本研究は Cognometric 方式のみを用いることで，認証にかかる時間への影響を抑えている点でこれらの研究とは異なり，実験調査の結果に基づき解答時間の差異を議論する．

また，Locimetric 方式の画像認証を視線計測により行うことでのぞき見の影響を低減する手法 [10] や，Drawmetric 方式の画像認証をダミーストロークの追加や描いたストロークの消去を行うことでのぞき見の影響を低減する手法 [11] も提案されている．両者とも画像認証の原理は本研究とは異なる．また，前者は追加のハードウェアを必要とすること，後者は完全なのぞき見対策に主眼を置いたものではないと述べられている点において本研究とは異なる．

Cognometric 方式の画像認証においては，正解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，のぞき見の影響を低減する手法が提案されている [12]．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，この方式は元画像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 [13]．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 [13], [14]．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，本研究の提案手法では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．

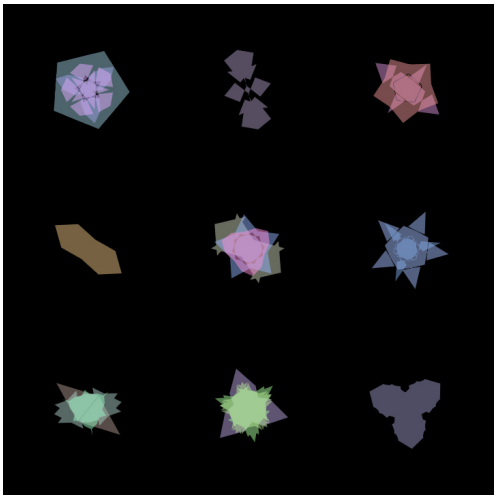


図 1 図形生成基本アルゴリズムによって生成された図形
Fig. 1 Shape patterns generated by the basic algorithm.

3. ワンタイム図形生成に基づく個人認証

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 つの図形の例を示している．図形生成基本アルゴリズムは，Miyashita らの図形生成手法 [15] 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[*1]．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一定の透明度でランダムな枚数だけ重ね合わせる．

(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は後述する (6) の何枚目の重ね合わせであるかのみに依存して毎回同様に決定することとし，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，それらの頂点を A，B として，A から B を結ぶ線分と B から A を結ぶ線分の 2 つの線分

[*1] 検討を経て，プロトタイプ実装 [1] から変更した箇所もある．

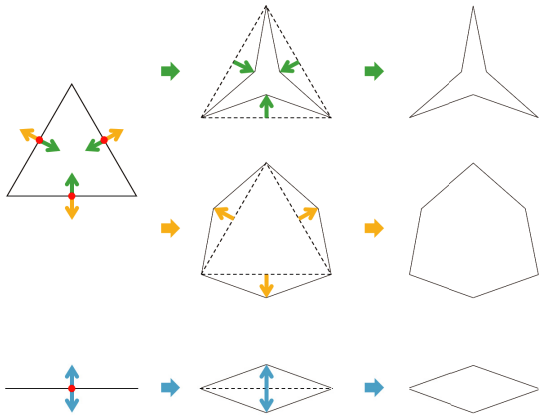


図 2 中点の移動による変形
Fig. 2 Edge middle point deformation.

が，同じ位置に異なる向きであるものとしてその後の操作を進めることと定義した．また，正多角形の中心から各頂点までの距離は，1 枚目が 150 ピクセル・2 枚目が 125 ピクセル・3 枚目が 100 ピクセルと定めた．

(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）．初期頂点が 2 つの場合は，初期に存在する 2 つの線分の向きが異なることにより，2 つの同じ位置の中点は反対方向へ移動するため，1 度目の操作により多角形が生成されることになる（図 2 下）．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．ただし，図形の中心から移動後の頂点までの距離が，中心から初期の正多角形の頂点までの距離を超えないよう制約を設けた．(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．本論文の実装では，RGB 色空間の各成分はそれぞれ，256 階調の 128〜255 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は，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，見た目の方向をつど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，透明度を 256 階調の 127 と定め，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合せを生成する認証図形群生成ルールを定義する．ここでい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，認証図形群生成ルールは，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．たとえば，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によって認証図形群生成ルールを定義する．この方法によれば，原理的には図形生成のランダムパラメータが重複しない範囲で認証図形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ランダムパラメータは，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・回転角度・図形の重ね合わせ枚数の 6 つである．プロトタイプ実装 [1] では恣意的に 6 つの認証図形群生成ルールを定義したが，本論文では 6 つのランダムパラメータそれぞれについて，ルールを知る者にとって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とっては図形群からは類推しにくい小さな差異であることの観点において意味のある制約を設けることができるかを，以下に示すとおり検討した．

3.2.1 ランダムパラメータの検討

初期多角形の頂点の数は，生成図形の形状に大きく影響する．直感的にいえば，多くの生成図形は初期多角形を連想できる形状となる．たとえば，初期多角形の頂点の数が 3 であれば，多くの生成図形は三角形を連想できる形状となる．図形生成基本アルゴリズムの原理上，生成図形は中心に対して点対称となり，初期頂点が重なる回転移動の角度は初期多角形の頂点の数によって一意に定まる．このため，ユーザは初期多角形を自然と連想できるものと考えられ，初期多角形の頂点の数は正解図形をダミー図形から見分けることができるパラメータであると結論づけた．

頂点追加時の移動距離は，生成図形の形状に大きく影響する．たとえば，初回の移動距離が正の大きな値である場合は生成図形は大きく膨らんだ形状となり，初回の移動距離が負の小さな値である場合である場合は生成図形は小さくしぼんだ形状となる．このとき，正解図形の場合は正の一定の範囲の移動距離をとることとし，ダミー図形の場合はそれ以外の移動距離をとることとしてルールを定義したところ，正解図形だけが大きく膨らんだ形状でダミー図形はしぼんだ形状となり，ルールを知らない者にとっても大きな差異となってしまった．負の一定の範囲・0 に近い一定の範囲に制約を設けた場合も同様であり，頂点追加時の移動距離は適切なパラメータではないと結論づけた．

頂点追加の回数は，生成図形の形状にさほど影響しない．これは，初期の頂点追加ほど形状に影響し，繰り返すほど頂点追加は細部の変更となり，本論文の実装では最低 2 回の繰返しが保証されているためである．また，頂点追加時の移動距離がランダムであるため，それが 0 に近い場合は形状はほとんど変化しないということも理由としてあげられる．このため，頂点追加の回数は正解図形をダミー図形から見分けることは困難なパラメータであると結論づけた．

色は，生成図形の見た目に直接的に影響を与える．さらに，複数の図形を俯瞰して眺めても指定の色を持つ図形は見分けやすいようであり，すばやく見分けることができると考えられる．プロトタイプ実装 [1] の評価でも色の特徴は他者に見破られやすいと示唆されてはいるが，すばやく入力しやすく他者に与える情報を少なくできる可能性を考慮し，色は正解図形をダミー図形から見分けることができ，かつ，適切なパラメータであると結論づけた．

回転角度は，見た目の方向を変化させるが，それ単体では生成図形の見た目に大きく影響しない．ただし，ちょうど整った方向を向いている場合に限り，やや際立って見える．たとえば，複数の図形の頂点がすべて同じ方向を向いている場合や，図形の頂点がまっすぐ上や下を向いている場合である．前者は後述する図形の重ね合わせ枚数にも依存するルールであるためここでは除外し，後者はこのパラメータ単体で実現できる表現であるため採用することとし，回転角度は正解図形をダミー図形から見分けることができるパラメータであると結論づけた．

図形の重ね合わせ枚数は，生成図形の見た目に十分に影響する．特に，本研究の図形生成基本アルゴリズムでは，重ね合わせる図形ごとに中心から初期頂点までの距離・形状・色・回転角度を決定するため，これらのパラメータの異なる図形の重ね合わせは図形の複雑度に大きく影響する．直感的にいえば，重ね合わせるほど複雑な図形が生成される．これより，図形の重ね合わせ枚数は正解図形をダミー図形から見分けることができるパラメータであると結論づけた．

3.2.2 認証図形群生成ルールの定義と直感的な解釈

以上より，図形生成基本アルゴリズムのランダムパラメータのうち，初期多角形の頂点の数・色・回転角度・図形の重ね合わせ枚数の 4 つを認証図形群生成ルールの定義に用いることとした．用いるランダムパラメータによってカ

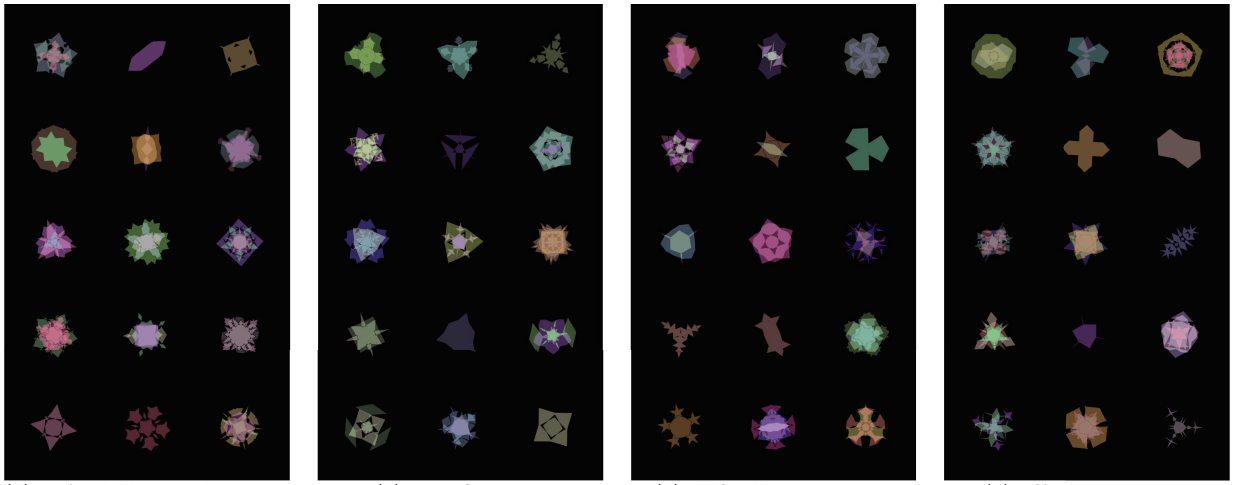


図 3 4 つのカテゴリそれぞれの認証図形群生成ルールによって生成された図形群と直感的なルールの解釈．図形群は 1 つの正解図形と 14 のダミー図形を含む．図形生成基本アルゴリズムを知らなくても，直感的なルールの解釈のみで正解図形を見分けられる．また，ルールによる図形群の大きな差異はない

Fig. 3 Shape patterns generated by the generation rules and interpretations of the generation rules. Each set of shape patterns includes one correct answer and 14 dummy answers. Users do not necessarily need to know the basic generation algorithm. There are no big differences among the sets of shape patterns.

テゴリ分けすると，以下のような 4 つのカテゴリのルールを定義でき，本論文の実装にあわせたそれぞれのパラメータの特徴により，合計 12 の認証図形群生成ルールを定義できる．**図 3** に，4 つのカテゴリから 1 つずつ代表して，認証図形群生成ルールにより生成された図形群を示す．

カテゴリ 1 正解：初期多角形の頂点の数が n，ダミー：初期多角形の頂点の数が n 以外，ルールは 4 種類あり n は $\{2,3,4,5\}$ のいずれかをとる．

カテゴリ 2 正解：RGB 色空間の要素のうち c が最も大きい，ダミー：RGB 色空間の要素のうち c 以外が最も大きい，ルールは 3 種類あり c は $\{R,G,B\}$ のいずれかをとる．

カテゴリ 3 正解：回転角度が θ，ダミー：図形の回転角度が θ 以外，ルールは 2 種類あり θ は $\{\pi/2, 3\pi/2\}$ のいずれかをとる（画面座標系の偏角の定義により $\theta = \pi/2$ は下向き・$\theta = 3\pi/2$ は上向きとなる）．

カテゴリ 4 正解：図形の重ね合わせ枚数が n，ダミー：図形の重ね合わせ枚数が n 以外，ルールは 3 種類あり n は $\{1,2,3\}$ のいずれかをとる．

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ルールを把握することができる．また，カテゴリやルールによる認証図形群の大きな差異はない（図 3）．

カテゴリ 1 {二角形, 三角形, 四角形, 五角形} を連想できるもの

カテゴリ 2 最も {赤い, 緑の, 青い} もの

カテゴリ 3 頂点が {下向き, 上向き} のもの

カテゴリ 4 多角形が {1 枚, 2 枚, 3 枚} 重なったもの

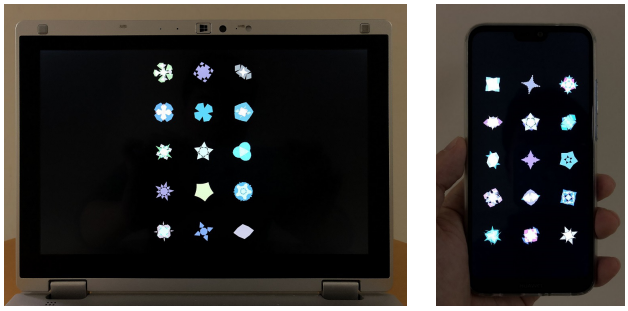


図 4 認証アプリケーション

Fig. 4 Authentication application.

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[*2]．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 15 の図形が提示され，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，画面が切り替わり別の 15 の図形が提示される．このプロセスを 4 回繰り返すと終了

[*2] 検討を経て，プロトタイプ実装 [1] から変更した箇所もある．

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 14 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．

4. 評価

評価は 2 つの実験調査によって行う．第 1 調査では，認証図形群生成ルールと事前知識の条件を様々に設定した場合に，正規の被認証者とのぞき見を行った非正規の被認証者の認証結果がどのようになるのかを調査する．第 2 調査では，既存手法との比較を行う．既存手法は，実用されているパスコード認証・パターン認証の 2 手法と，Cognometric 方式画像認証でランダムアート画像を用いた手法 [2]・顔画像を用いた手法 [3] の 2 手法の計 4 手法を比較対象とする．いずれの実験調査も，Android スマートフォンを機材として用い，提案手法は Android アプリケーションの提案システムを用いる．

いずれの実験調査も，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 名の実験参加者はのぞき見を行う非正規の被認証者役となる．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）」とも呼ぶこととする．

実験参加者は大学の食堂やラウンジで声をかける方法で勧誘し，個人認証手法の評価が目的の実験調査であることと，実験参加者には 500 円分のクオカードが謝礼として渡されることを伝えたうえで，参加の意思を示した者が参加した．

4.1 認証図形群生成ルールと事前知識による影響の調査

4.1.1 実験手順

認証図形群生成ルールを変えて 6 セッションの評価を繰り返すこととし，2 名の実験参加者を A，B とすると，A → A → B → B → A → B の順で正規の被認証者役を行い，もう一方が非正規の被認証者の役を行うというように，実験の最中に正規・非正規の役割は交代して実験を行う．この順序としたのは，最初の 2 セッション・中間の 2 セッション・最後の 2 セッションについて，本認証システムの事前知識に関して異なる条件でのデータを取得するためである．

最初の 2 セッションでは，非正規の役割である B は，認証システムを利用したことがない状態でのぞき見を行う．このとき，認証システムが認証図形群生成ルールに基づいて動作していること，あるいは，ルールが存在することも知らされない．

中間の 2 セッションでは，非正規の役割である A は，最初の 2 セッションで正規の役割を行う際に，認証システムが認証図形群生成ルールに基づいて動作していることを知らされるため，この中間の 2 セッションも何らかのルールに基づいて動作していることを知った状態でのぞき見を行う．ただし，最初の 2 セッションと中間の 2 セッションで用いられるルールのカテゴリは異なるものを適用する．

最後の 2 セッションでは，非正規の役割である A または B は，これまでのセッションで認証システムが認証図形群生成ルールに基づいていることを知るとともに，自分が正規の被認証者として体験したルールと同じカテゴリでありパラメータは異なるルールののぞき見を行う．したがって，似たようなルールを体験済みの状態でのぞき見を行うこととなる．

以上をまとめると，順に認証システム未体験/ルールがあることも知らされていない・認証システム体験済み/当該ルールカテゴリ未体験・認証システム体験済み/当該ルールカテゴリ体験済みの 3 つの条件を比較できるデータを取得することを意図している．以下では，それぞれ「システム未体験」条件・「ルールカテゴリ未体験」条件・「ルールカテゴリ体験済み」条件と呼び，この要因のことを「事前知識条件」と呼ぶこととする．

3.2 節で述べたどのカテゴリ・パラメータをどの順番で実験参加者に割り振るかは，実験参加者ごとにカウンターバランスをとって実施する．

各セッションについては，以下の手続きで実験を実施する．したがって，実験全体としては，以下の手続きを 6 回繰り返すこととなる．

(1) 実験者は実験参加者（正）へ認証図形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，3.2.2 項で述べた直感的な説明のみを行う．
(2) 実験参加者（正）は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）は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）のそばでのぞき見を行う．
(4) 実験参加者（正）の 3 回のテストの終了後，実験参加者（非）は認証アプリケーション利用のテストを 3 回行う．
(5) 実験参加者（非）はのぞき見の際にどのように考えたかを質問紙に記録する．

4.1.2 取得するデータ

実験を通して取得するデータは，解答正誤データ・解答時間データ・認証成否データ・質問紙への回答の 4 つである．

解答正誤データ・解答時間データは，解答試行ごとに，認証アプリケーションによる自動記録により取得する．また，認証成否データは，認証試行ごとに，認証アプリケーションによる自動記録により取得する．実験参加者（正）も実験参加者（非）も，1 セッションあたり 3 回の認証試行を行い，1 回の認証試行につき 4 回の正解図形の解答試行を行う．したがって，1 セッションあたり 12 の解答正誤

表 1 ルールごとの認証成功率（%）・認証成功率（%）・平均解答時間（msec.）
Table 1 Authencication rates (%), correct answer rates (%), and average answer times (msec.) for each generation rule.

	二角形	三角形	四角形	五角形	赤い	緑の	青い	下向き	上向き	1 枚	2 枚	3 枚	全体
認証成功率（正規）	100.0	88.9	100.0	100.0	94.4	94.4	94.4	98.1	94.4	94.4	72.2	83.3	92.8
認証成功率（非正規）	25.9	37.0	22.2	11.1	5.6	16.7	5.6	11.1	7.4	33.3	22.2	22.2	17.1
正答率（正規）	100.0	96.3	100.0	100.0	97.2	98.6	98.6	99.5	98.6	98.6	93.1	94.4	98.0
正答率（非正規）	44.4	50.0	30.6	38.9	21.5	34.7	27.1	21.3	21.8	48.6	41.7	30.6	32.6
平均解答時間（正規）	4,109	5,228	14,995	6,047	2,939	4,172	10,879	6,153	5,079	3,219	8,431	9,677	6,535
平均解答時間（非正規）	9,729	8,577	10,150	3,605	7,349	8,548	9,904	7,029	10,082	5,975	16,647	9,339	8,956

データ・解答時間データを取得し，3 つの認証成否データを取得する．認証成否データは，1 つの認証試行に含まれる 4 つの解答試行すべてに正解したか否かに一致する．

質問紙への回答は，セッションの最後に実験参加者（非）のみが行う．質問文は「のぞいたとき，どのように考えましたか？」であり，実験参加者（非）は自由記述で回答する．したがって，1 セッションあたり 1 つの自由記述文を取得する．

4.1.3 結果とデータ分析

26 組 52 名の実験参加者を招き実験を実施した．ただし，色覚異常を持つために実験を途中で中止したい旨を申し出た実験参加者が 2 名おり，その実験参加者が含まれる 2 組の中途データは除外した 24 組 48 名のデータを評価の対象とした．

評価対象の 48 名すべてにおいて，実験参加者（正）を 3 セッション・実験参加者（非）を 3 セッション行っているため，全体としては実験参加者（正）のデータを 144 セッション分・実験参加者（非）のデータを 144 セッション分取得した．このため，全体としては，144 セッション・432 認証試行・1728 解答試行のデータを，実験参加者（正）と実験参加者（非）の両方について取得したこととなる．ルールカテゴリはカウンターバランスをとって均等に配分したため，4 つのカテゴリそれぞれについて，36 セッション・108 認証試行・432 解答試行のデータを取得した．ルールカテゴリによって，とりうるパラメータの数は異なりルールの数も異なるため，カテゴリ 1 の初期多角形ルールは，それぞれ 9 セッション・27 認証試行・108 解答試行のデータを取得し，カテゴリ 2 の色空間ルールとカテゴリ 4 の重ね合わせ枚数ルールは，それぞれ 12 セッション・36 認証試行・144 解答試行のデータを取得し，カテゴリ 3 の回転角度ルールは，それぞれ 18 セッション・54 認証試行・216 認証試行のデータを取得した．事前知識条件別には，3 条件それぞれについて，48 セッション・144 認証試行・576 解答試行のデータを取得した．

4.1.3.1 認証成功率・正答率

まず，**表 1** 上部に，ルールごとの認証成功率として認証試行に対して成功した割合を示す．どのルールもおおむね似たような傾向を示しており，のぞき見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）の認証成功率は大きく異なっていた．全体として見れば，3 度連続でのぞき見が行われることは，通常利用よりも正規の被認証者に厳しい条件であると考えられ，その条件下で実験参加者（正）と実験参加者（非）の認証成功率が大きく異なっていることは，提案手法が一定の効果を上げていることを示しているといえる．

ルールを個別に見ると，実験参加者（正）に関しては，カテゴリ 4 の重ね合わせ枚数ルールの 2 枚と 3 枚において，ほかと比べて低い認証成功率であった．このことは，2 枚重ね合わせと 3 枚重ね合わせの認証図形群生成ルールが，やや本人にも解きにくいルールであることを示唆している．実験参加者（非）に関しては，カテゴリ 1 の初期多角形ルールの三角形とカテゴリ 4 の重ね合わせ枚数ルールの 1 枚において，ほかと比べて高い認証成功率であった．このことは，初期多角形が三角形と 1 枚重ね合わせの認証図形群生成ルールが，やや盗まれやすいルールであることを示唆している．

以上についてより詳細に調べるため，ルールごとの正答率として解答試行に対して正解した割合を検討する．表 1 中部に示すとおり，100.0%である場合を除き，正答率は認証成功率よりも高い値となっているが，これは認証成功が 4 回の正答の AND 条件となっているためであり，すべての認証試行ですべて正答かすべて誤答でない限りは原理的にそのようになる．このようにしてみると，初期多角形が三角形と 1 枚重ね合わせの認証図形群生成ルールは，依然としてほかと比較して高い値であるが，その差は認証成功率ほど大きくない．無作為に選んだ場合に偶然正解してしまう確率は 1/15 であるので，正答率のチャンスレベルは 6.7%である．実験参加者（非）の正答率がチャンスレベル 6.7%と同等であるかの二項検定を行ったところ，いずれのルールもチャンスレベルとは有意差が認められた（$p < 0.01$，$g = 0.146 \sim 0.433$）．この結果は，統計的には実験参加者（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．したがって，ルールによって程度の差はあるが，実験参加者（正）の解答試行から，ルールを認識できなかった認証試行においても実験参加者（非）がルールの可能性を絞り込めていることが分かる．

表 2 事前知識条件ごとの認証成功率（%）・正答率（%）・平均解答時間（msec.）
Table 2 Authencication rates (%), correct answer rates (%), and average answer times (msec.) for each experience condition.

	システム未体験	ルールカテゴリ未体験	ルールカテゴリ体験済み	全体
認証成功率（正規）	92.4	93.8	92.4	92.8
認証成功率（非正規）	11.8	13.9	25.7	17.1
正答率（正規）	97.6	98.4	98.1	98.0
正答率（非正規）	28.8	25.2	43.9	32.6
平均解答時間（正規）	6,196	5,629	7,779	6,535
平均解答時間（非正規）	8,206	8,800	9,862	8,956

次に，**表 2** 上部に，事前知識条件ごとの認証成功率を示す．実験参加者（正）に関しては，事前知識条件によらず同様にルールの直感的解釈を教示されるため，事前知識条件間に差はない．実験参加者（非）に関しては，システム未体験条件・ルールカテゴリ未体験条件よりも，ルールカテゴリ体験済み条件のほうが認証成功率が高くなった．カイ二乗検定を行ったところ，条件間の認証成功率に有意差が認められた（$p < 0.01$，$V = 0.162$）．このことは，提案手法においては，同様のルールを体験したことのある非正規ユーザは，認証図形群生成ルールを認識しやすいことを示している．表 2 中部に示す事前知識条件ごとの正答率においても，同様の結果が得られている．カイ二乗検定を行ったところ，条件間の正答率に有意差が認められた（$p < 0.01$，$V = 0.173$）．

4.1.3.2 解答時間

まず，表 1 下部に，ルールごとの平均解答時間として認証図形群が提示されてからタップを行うまでにかかった時間の平均を示す．全体としては，実験参加者（正）のほうが実験参加者（非）よりも短い時間で回答している傾向が見られる．実験参加者（正）は認証を解くためのルールを知っているため，解答時間が短くなることは理にかなっているが，それほど大きい差ではないことが分かる．

ルールを個別に見ると，二角形・赤い・緑の・1 枚といったルールで，実験参加者（正）が比較的すばやく回答しているが，全体的にばらつきが多いことが見受けられる．特に，カテゴリ 2 の色空間ルールにおいて，ルールを定義した際には，ほかのカテゴリに比べてすばやく回答できるであろうことを検討したが，青いのルールにおいてはそうではないことが示されている．一方で，カテゴリ内で比較すると，二角形や 1 枚のルールは，同じカテゴリのほかのルールと比べると単純な図形になることから，すばやく見分けやすいことが予想でき，その結果が現れているものと考える．

次に，表 2 下部に，事前知識条件ごとの平均解答時間を示す．実験参加者（正）に・実験参加者（非）ともに，事前知識条件によって解答時間はあまり変化しておらず，事前知識よりもどの認証図形群生成ルールが用いられているかが解答時間に影響しやすいことを示唆している．

4.1.3.3 質問紙への回答

得られた回答を調べたところ，まず注目すべきは，「システム未体験」条件の実験参加者（非）が何らかのルールがあることを多くの場合で予測しているということである．4.1.1 項にて示したとおり，最初に非正規の役割を行う実験参加者は，ルールがあることを知らされないまま第 1 セッションと第 2 セッションを行う．しかし，「角の数が 1 番多い図形を探した」や「パターンを探したが難しかった」といったように，具体的であるものもないものもあるが，ルールあるいはパターンを探したといった記述が見られる．また，「規則性があるかどうかを探した」といったルールの存在を断定はしていないものの可能性を探っている記述も見られる．この両者をあわせると，第 1 セッションの 24 の回答のうち，17 の回答でルールが存在する可能性を知らされずとも考えていたようである．このことは予期していなかったが，見た目には似たような図形が画面に並ぶため，何らかのルールがないと見分けられないのではないかと自然に考えたのではないかと推測される．今後の実験で深掘りして調査すべき課題である．

一方で，ルールがあることを知らされたあとの第 3 セッション以降の回答では，ルールが具体的に何かを考えたという記述が引き続き多く見られたが，「解くスピードが速かったため，比較的簡単な図形ではないかと考えた」や「すばやく解いていたので，自分がすばやく解けたルールではないかと思った」といった，画面の視覚的情報だけでなく，解きかたの情報からルールを推定する記述も見られた．

認証成否データと照らし合わせてみると，実験参加者（非）が複数回認証に成功している場合には，ルールをほぼいい当てている記述が見られる．一方で，1 回のみ認証に成功した場合や，1 度も認証に成功しなかったものの解答正誤データの正答率は 50%以上であるような場合は，いい当てている場合もあるが，ルールは認識していないように見受けられる記述もあり，4.1.3.1 で述べたルールを認識できなかったが可能性を絞り込めている認証試行があることが，質問紙への自由記述からも見受けられる．

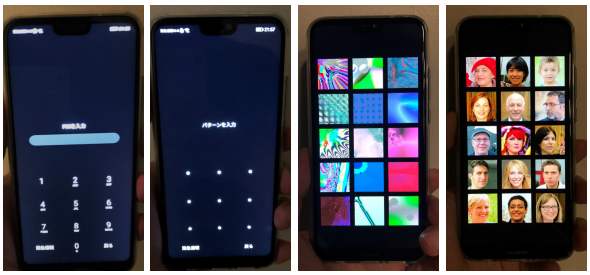


図 5 既存手法：左から，パスコード認証・パターン認証・ランダムアート画像認証・顔画像認証

Fig. 5 Existing authentication methods: from the left, passcode-based, draw-a-secret, random art figure, and face image.

4.2 既存手法との比較

4.2.1 実験手順

まず，2 名の実験参加者ともに，提案手法と比較対象の 4 つの既存手法すべてについてどのように認証されるかを説明し，要望に応じて認証方法の実演を行う．提案手法については，12 の認証図形群生成ルールがあることと，それぞれのルールについても説明を行う．パスコード認証とパターン認証はスマートフォンに用意されているもの・ランダムアート画像認証と顔画像認証は提案手法と条件をあわせてスマートフォンに実装したものを用いる（**図 5**）．ランダムアート画像は既存研究 [2] と同様の方法で，顔画像は実在しない顔を生成する手法 [16] で，それぞれ本実験調査に際して生成し，実験参加者があらかじめ知っている画像が含まれる可能性を排除した．

次に，1 名の実験参加者が正規の被認証者役を行い，もう 1 名は非正規の被認証者役としてのぞき見を行う．この組合せで 5 セッションを連続で行い，5 つの手法すべてについて実験を実施する．その後，正規の被認証者役と非正規の被認証者役を入れ替え，同様に 5 セッションを実施する．どの手法をどの順番で実施するかは，実用認証手法 2 種と画像認証手法 3 種に分けた分類内で均等な順序になるように実施する．

本実験調査では，認証のためのパスコード・パターン・画像・認証図形群生成ルールは，実験参加者本人が設定することとして条件を統一し，1 度設定したあとで練習を行った際に不都合があれば，何度でも設定を変えてよいこととする．

各セッションについては，以下の手続きで実験を実施する．したがって，実験全体としては，以下の手続きを 10 回繰り返すこととなる．

(1) 実験者は実験参加者（正）に対して認証手法を指定し，認証のためのパスコード・パターン・画像・認証図形群生成ルールを決定するように指示する．また，必要があれば，決定した設定を変えてもよいことを伝える．
(2) 実験参加者（正）は認証のためのパスコード・パターン・画像・認証図形群生成ルールを設定したのち，認証アプリケーション利用の練習を好きなだけ行う．
(3) 実験参加者（正）は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）のそばでのぞき見を行う．
(4) 実験参加者（正）の 3 回のテストの終了後，実験参加者（非）は認証アプリケーション利用のテストを 3 回行う．

4.2.2 取得するデータ

すべての手法について認証成否データ・認証時間データを取得し，画像認証手法 3 種については解答正誤データも取得した．パスコード認証・パターン認証においては，複数の数字のコード・複数の線分に分解することができるが，それら 1 つ 1 つの正誤が意味を成すのではなく，組合せで意味を成すものと考え，計測の対象としなかった．

画像認証手法 3 種については，解答正誤データは，解答試行ごとに，認証アプリケーションによる自動記録により取得する．また，認証成否データ・認証時間データは，認証試行ごとに，認証アプリケーションによる自動記録により取得する．実用認証手法 2 種については，自動記録をすることができないため，認証場面をビデオで撮影し，事後にビデオで計測する方法にて認証成否データ・認証時間データを取得する．実験参加者（正）も実験参加者（非）も，1 セッションあたり 3 回の認証試行を行い，画像認証手法については 1 回の認証試行につき 4 回の画像の解答試行を行う．したがって，1 セッションあたり 3 つの認証成否データ・認証時間データと，画像認証手法については 12 の解答正誤データを取得する．画像認証手法における認証成否データは，1 つの認証試行に含まれる 4 つの解答試行すべてに正解したか否かに一致する．

4.2.3 結果とデータ分析

6 組 12 名の実験参加者を招き実験を実施した．12 名の実験参加者すべてが，5 つの手法すべてについて，実験参加者（正）と実験参加者（非）を 1 セッションずつ行っているため，それぞれの手法について実験参加者（正）のデータを 12 セッション分・実験参加者（非）のデータを 12 セッション分取得した．

表 3 に，認証手法ごとの認証成功率・正答率・平均認証時間を示す．認証成功率・正答率については，実験参加者（正）はどの手法もおおむね成功・正答しているが，実験参加者（非）は差異が見られる．実験参加者（非）の認証成功率は，パスコード認証・パターン認証が高く，次いでランダムアート画像認証・顔画像認証が中程度であり，提案手法は最も低い結果となった．画像認証手法における正答率についても同様の傾向である．提案手法の認証成功率・正答率は，第 1 実験調査のルールカテゴリ体験済み条件の結果とおおよそ一致しており，ルールを知っている非正規ユーザには，複数回ののぞき見を許すことでルールが盗ま

表 3 認証手法ごとの認証成功率（%）・正答率（%）・平均認証時間（msec.）
Table 3 Authencication rates (%), correct answer rates (%), and average authentication times (msec.) for each authentication method.

	提案手法	ランダムアート画像	顔画像	パスコード認証	パターン認証
認証成功率（正規）	100.0	100.0	88.9	100.0	100.0
認証成功率（非正規）	27.8	61.1	50.0	100.0	72.2
正答率（正規）	100.0	100.0	97.2	-	-
正答率（非正規）	49.3	81.9	73.6	-	-
平均認証時間（正規）	12,783	5,465	6,336	2,002	1,626
平均認証時間（非正規）	15,927	8,337	10,672	1,533	2,087

れる場合があることが本実験調査でも示された．

認証時間は，パスコード認証・パターン認証が短く，次いでランダムアート画像認証・顔画像認証が中程度であり，提案手法は最も長い結果となった．提案手法ではのぞき見への対策を導入した結果，認証にかかる時間は長くなっているということができる．画像認証手法については，実験参加者（正）のほうが実験参加者（非）よりも短い時間で回答している傾向が見られ，第 1 実験調査と同様の傾向が本実験でも示された．一方，提案手法の平均認証時間は，第 1 実験調査よりも短い結果となった．これは，あらかじめルールをすべて説明していたこと・適用ルールを実験参加者本人が選択できるようにしたことの効果が現れたものと考えられる．

5. 議論

提案手法の利点は，のぞき見がどうしても防げない場合でも，認証に必要な情報が漏えいすることをある程度防げることである．さらに，正規の被認証者の 1 回の認証にかかる時間が，第 1 実験調査で平均 26.1 秒・第 2 実験調査で平均 12.8 秒であることから，Cognometric 方式と Locimetric 方式を組み合わせた手法 [7] が平均 71.66 秒かかっていることと比較すると，ユーザビリティが高まっていると考えられる．一方で，第 1 実験調査で平均 26.1 秒・第 2 実験調査で平均 12.8 秒かかっていることから，難易度が高く，すばやくあるいは繰り返し認証を行う場面には向いていないといえる．このことを考えると，公共の場で周りに人が多い状況で個人認証が必要な場合に，通常の認証手法から切り替えて使用するというのが応用場面ではないかと考える．たとえば，乗車率の高い電車やバスの中で，銀行口座の操作が必要なときに，本手法に切り替えて認証を行うというようなことである．現在の実装では，正規の被認証者でも正解できるが時間がかかる設定となっているということができ，図形を並べる数や 1 認証試行あたりの解答試行数をいくつにするかといったパラメータで難易度を調整する余地がある．どのようなパラメータの値でどのような場面に適してくるかということは，今後取り組むべき課題である．

同じルールカテゴリのルールを体験したことがある実験参加者は，未体験の実験参加者に比べて非正規に認証を受けられることが第 1 実験調査では示され，どのようなルールがあるかを知っている非正規ユーザにどう対応するかということも今後の課題である．理想的には，ルールを知る者がのぞき見を行ってもルールを認識できないことが求められる．現在その可能性の 1 つとして，1 つの解答試行において複数のルールを混ぜることや，1 つの認証試行において複数のルールを切り替えることを検討している．ルールを推測するときには，のぞき見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，そのルールが複合的なものであったり，つど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．

プロトタイプ実装 [1] の実験結果と，本論文の実験調査の結果を比較すると，いくつかの性能向上が見られる．具体的には，プロトタイプ実装 [1] では，カテゴリ 2 に相当する色ルールにて実験参加者（非）の正答率が高く，カテゴリ 1 の初期多角形ルールである三角形・四角形とカテゴリ 4 の重ね合わせ枚数ルールである 2 枚にて実験参加者（正）の正答率が低かった．色ルールにおいては，赤・黄・緑やオレンジ・灰色・青・白の組合せといった特定の色を必ず使用することとしていたため，その他の図形から見分けがついてしまっていたのが原因と考えられる．本論文の実装では，特定の色は定めない範囲の色空間の制約としたため性能が向上したと考えられる．初期多角形ルールにおいては，図形の中心から移動後の頂点までの距離が，中心から初期の正多角形の頂点までの距離を超えないよう制約を設けたことにより，多角形を認識しやすくなったため性能が向上したと考えられる．重ね合わせ枚数ルールにおいては，初期多角形の中心からの距離を何枚目の重ね合わせかによって変更することを導入したことと，透明度をランダムではなく固定とし，毎回ある程度透明にしたことで，重ね合わせを認識しやすくなったため性能が向上したと考えられる．いずれも，本論文にて新たに行った検討によって改善されたということができる．

6. まとめ

本論文では，のぞき見による他者の不正認証を低減することを目指して，ワンタイム図形生成に基づく認証手法を

提案した．提案手法では，認証図形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，のぞき見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．目的に沿うような認証図形群生成ルールを検討した結果，4カテゴリ12ルールを定義した．

評価実験を行ったところ，のぞき見を認めているにもかかわらず高い本人パス率と他者拒否率を示し，同様の既存手法と比較してのぞき見への対策性能が高いことが示された．一方で，解答にかかる時間は通常の認証方法よりも必要であり，のぞき見がどうしても防げない場合に，通常の認証方法から切り替えて使用するのが適切であると考えられる．また，同じルールカテゴリのルールを体験したことがある実験参加者は，非正規に認証を受けやすいことが示されており，このことへの対応として，複数ルールを混ぜることや複数ルールを切り替えることを検討している．これらの課題に対しては今後も検討を重ね，改善を重ねていく予定である．

謝辞 本研究は，令和元年度専修大学研究助成個別研究「ワンタイム画像生成による特定の認証キーのない認証手法」の助成を受けて行われました．

参考文献

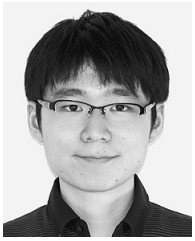
[1] 石井健太郎，香川将樹：ワンタイム図形生成に基づく特定の認証キーのない認証手法，コンピュータセキュリティシンポジウム2018論文集，pp.187–192 (2018).
[2] Dhamija, R. and Perrig, A.: Déjà Vu: A User Study Using Images for Authentication, *USENIX Security Symposium* (2000).
[3] Tari, F., Ozok, A.A. and Holden, S.H.: A Comparison of Perceived and Real Shoulder-surfing Risks between Alphanumeric and Graphical Passwords, *Symposium on Usable Privacy and Security*, pp.56–66 (2006).
[4] Takada, T. and 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).
[5] 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).
[6] 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).
[7] Wiedenbeck, S., Waters, J., Sobrado, L. and Birget, J.C.: Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme, *International Working Conference on Advanced Visual Interfaces*, pp.177–184 (2006).
[8] Man, S., Hong, D. and Matthews, M.: A Shoulder-Surfing Resistant Graphical Password Scheme – WIW, *Security and Management*, pp.105–111 (2003).
[9] Zhao, H. and Li, X.: S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme, *International Conference on Advanced Information Networking and Applications Workshops*, pp.467–472 (2007).
[10] Forget, A., Chiasson, S. and Biddle, R.: Shoulder-Surfing Resistance with Eye-Gaze Entry in Cued-Recall Graphical Passwords, *ACM SIGCHI Conference on Human Factors in Computing Systems*, pp.1107–1110 (2010).
[11] Zakaria, N.H., Griffiths, D., Brostoff, S. and Yan, J.: Shoulder Surfing Defence for Recall-based Graphical Passwords, *Symposium on Usable Privacy and Security*, Article No.6 (2011).
[12] 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).
[13] 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).
[14] Yamamoto, T., Harada, A., Isarida, T. and 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).
[15] Miyashita, Y., Higuchi, S., Sakai, K. and Masui, N.: Generation of fractal patterns for probing the visual memory, *Neuroscience Research*, Vol.12, No.1, pp.307–311 (1991).
[16] Karras, T., Laine, S. and Aila, T.: A Style-Based Generator Architecture for Generative Adversarial Networks, *IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp.4401–4410 (2019).

石井 健太郎 （正会員）

2003年慶應義塾大学理工学部情報工学科卒業．2005年同大学大学院理工学研究科修士課程修了．2009年同博士課程所定単位取得退学．博士（工学）．科学技術振興機構ERATO五十嵐プロジェクト技術員，東京大学大学院情報学環助教，同大学大学院総合文化研究科特任研究員，大阪工業大学情報科学部特任講師を経て，現在，専修大学ネットワーク情報学部准教授．ヒューマンロボットインタラクション・ユーザインタフェースの研究に従事．

香川 将樹

2017年大阪工業大学情報科学部情報ネットワーク学科卒業．同年三菱電機インフォメーションシステムズ株式会社（通称：MDIS）入社．ネットワークの提案から運用保守業務に従事．



島谷 和樹

2016 年専修大学ネットワーク情報学部入学．現在，同学部在学中．コンピュータセキュリティの研究に興味を持つ．