ワンタイム図形生成に基づく画像認証手法

石井 健太郎[1,a)]

概要：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，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，認証場面のショルダーハッキング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．画面には都度生成された図形が提示されるため，ショルダーハッキングが行われた場合であっても正解の手がかりをつかみにくいことが期待できる．本論文では，まず基礎となるワンタイム図形生成に基づく画像認証の基本手法について述べてから，本人パス率や他者拒否率を高めるためのコンセプトについて議論する．

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，認証場面のショルダーハッキング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．認証時には都度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，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，都度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．

以上のアイディアをもとに，筆者らは，6 つの認証図形群生成ルールを定義し，プロトタイプを実装のうえ，認証図形群生成ルールを知る実験参加者が認証を受ける場面を，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 [1]．その結果，認証図形群生成ルールによっては，ショルダーハッキングを許可し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図形群生成ルールも存在し，認証図形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．

そこで本論文では，提案手法にさらなる改良を加え，本人パス率や他者拒否率を向上させる方策を模索する．具体的には，他者拒否率の向上に寄与する複数ルールの組み合わせ・インラインルール通知・ダミー選択，本人パス率向上に寄与する選択スキップ・ルールのカスタマイズといったコンセプトを導入する．本論文では，関連研究をまとめたあと，まず基礎となるワンタイム図形生成に基づく画像認証の基本手法について述べる．その後，さらなる改良のために新たに導入されたコンセプトについて議論する．

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 [2]．Déjà Vu では，コンピュータで生成した画像から 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．しかし，ユーザ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，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 [3], [4] は，

[1] 専修大学
[a)] kenta@pc.fm.senshu-u.ac.jp

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 [5]．

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，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 [6], [7], [8] 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 [9] 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，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，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 [10]．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 [11]．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 [11], [12]．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．

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 [13]．この手法は本研究と同様に特定の正解画像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 [14] を参考にしてアレンジしたものである．

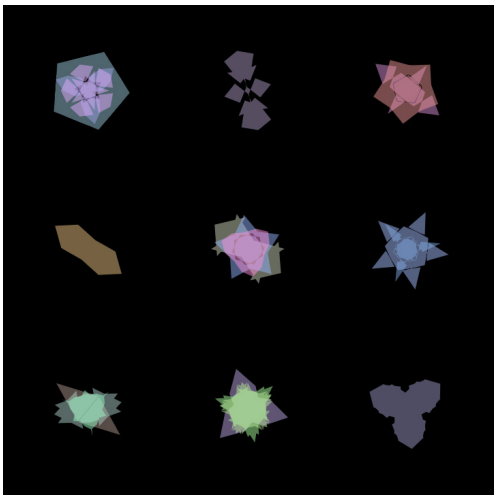


図 1 図形生成基本アルゴリズムによって生成された図形

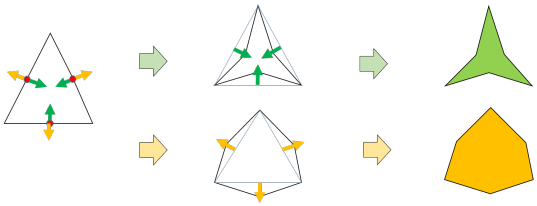


図 2 中点の移動による変形

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，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．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．

[*1] 検討を重ねた結果，先行研究 [1] から変更した箇所もある．

(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，透明度を 256 階調の 127 とし，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図形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こととした．例えば，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．先行研究 [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づら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．

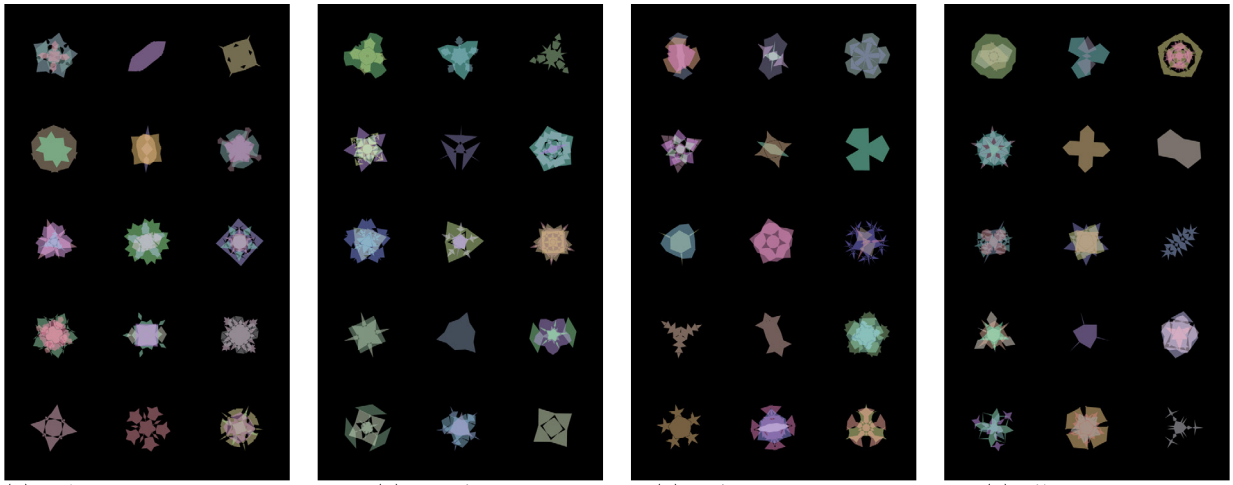
3.2.1 ランダムパラメータの検討

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．直感的に言えば，多くの生成図形は初期多角形を連想できる形状となる．例えば，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．例えば，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，繰り返しの頂点追加は細部の変更となり，本論文の実装では最低 2 回の繰り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挙げられる．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．先行研究 [1] の評価でも色の特徴は他者に



(1) 三角形を連想できるもの　(2) 最も赤いもの　(3) 頂点が上向きのもの　(4) 2枚重なったもの

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．

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．例えば，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．直感的に言えば，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した．**図 3** に，4 つのカテゴリから 1 つずつ選択した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（ただし，二角形は便宜的な呼びかたであり線分を意味する）

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

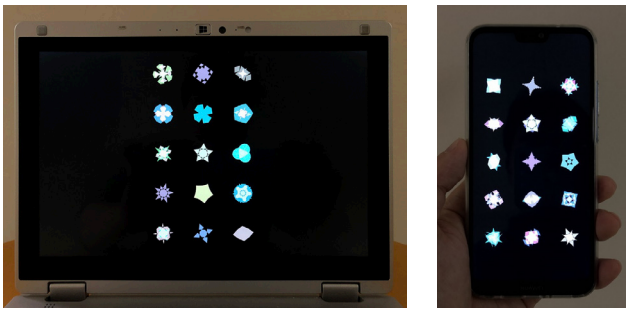


図 4　認証アプリケーション

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.　さらなる性能向上の手法

3 節の基本手法では，短時間のショルダーハッキングでは正解の手がかりを取得しづらいものの，連続したショルダーハッキングに直面するとルールを推定できる場合がある．特に，3.2 節で定義した認証図形群生成ルールにどんなものがあるかを知っている者がショルダーハッキングを行った場合，12 ある認証図形群生成ルールにそっているかを 1 つずつあてはめることによって，徐々にルールが類推されていく．このことに対しては，基本手法だけでは限界があり，対策が必要である．また，正規のユーザにとっての負担を軽減することを考えることは，提案手法をより使いやすいものにするために重要なことである．本節では，これらの観点に対して寄与するコンセプトを導入し，発展的な手法をどのように実現するかを議論する．

4.1　複数ルールの組み合わせ

まず考えられるのは，4 回のチャレンジにより認証されるプロセスにおいて，4 回とも同じ認証図形群生成ルールを用いるのではなく，異なるルールを組み合わせて用いることである．ショルダーハッキングを行う者はどのルールが適用されているかを類推していることが考えられるため，ルールが認証プロセス中に切り替わることによってショルダーハッキングを行っている者の思考をそらすことができると考える．最も単純には，4 度の図形の選択における何度目の選択であるかによって適用するルールを決めておくことである．1 度目と 3 度目はルール A に基づき，2 度目と 4 度目はルール B に基づくというようにしてもよいし，4 度とも異なるルールを適用してもよい．また，ある認証プロセスにおいてルール A →ルール B →ルール C →ルール A と適用した場合は，次の認証プロセスにおいてはルール B →ルール C →ルール A →ルール B というように，順送りに繰り返すということも 1 つの手法として考えられる．この場合，認証に失敗することがあればルール A に戻るというような，ベースラインを担保する方法との併用も考慮する必要がある．

[*2] 検討を重ねた結果，先行研究 [1] から変更した箇所もある．

図 5　インラインルール通知

4.2　インラインルール通知

複数ルールの適用を事前に決められた順序で行うのではなく，ランダムに行うことも考えられる．その場合，何らかの方法で正規のユーザに適用されているルールを通知しなければならないが，これを提示されている図形によりインラインで行うことを考える．図 5 は，インラインルール通知を実装した認証画面の例に説明を加えたものである．この例では，中央に提示された図形によってルールが通知される設定としており，そこに四角形を連想できる図形があることで，この画面の認証図形群生成ルールは四角形を連想できるものであることが通知される．

どの場所にルールが通知されるかは正規のユーザのみが知るとすると，非正規のユーザにはその図形がインラインルール通知であるのか，通常の正解図形・ダミー図形であるのかを見分けることは困難である．なお，図 5 の例では，ルール通知と適用されているルールの図形が同じであるが，適用されているルールとは異なるルールや異なるカテゴリの図形で通知することも可能である．

4.3 ダミー選択・選択スキップ

正解図形の選択をあえて行わないことによって，ショルダーハッキングを行っている他者を惑わすことも考えられる．適用されている認証図形群生成ルールに対して正解図形がない図形群を生成することによって，正規のユーザにはこの手法が実施されたことがわかる．これをダミー選択と呼ぶこととする．正規のユーザは，どの図形を選んでもよいという設定としてもよいし，特定の場所の図形を選択するという設定としてもよい．非正規のユーザには，この手法が実施されたのか通常の正解図形を選択したのかの区別は困難である．

また，正規のユーザが正解を見分けられないときにも，本人パス率の向上のために同様の手法を用いることも考えられる．4 回のチャレンジにおいて，1 回に限り特定の場所の図形を選択することで，そのチャレンジに対して正解を選択できなくても，残りの 3 回で正解を選択できるならば認証成功とする．これを選択スキップと呼ぶこととする．これを許可すれば，他者が認証を突破できる可能性は増えてしまうが，どうしても正解が見分けられないときの本人のストレスを大きく軽減することができる．

4.4 ルールのカスタマイズ

どの認証図形群生成ルールを用いるかや以上の発展的な手法を利用するかどうかは，ユーザがカスタマイズできることが望ましい．難易度やルールや発展的な手法に対する好みや得手不得手には個人差があるため，各ユーザにあわせて変更できれば，提案手法はより扱いやすいものとなる．必ずしも認証アプリケーションに備わっている必要はなく，何らかの手段でルールのカスタマイズは行えれば十分であるが，本論文の実装では，認証アプリケーションにこのカスタマイズ機能を備えることとした．

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，ワンタイム図形生成に基づく画像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，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の手がかりをつかみづらく不正認証を防ぐことが期待できる．

さらに，より他者にはわかりにくく，より本人にはわかりやすくすることを目的として，発展的な性能向上の手法を提案した．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推測して絞り込む作業をしているため，認証の途中でルールを切り替え，どのルールに切り替わるかを固定しないことで，推測・絞り込みが十分に進まないようにすることが主要な狙いである．これらの発展的な手法は，どのようなルールが存在するかを知る他者にとっても効果があると期待している．本格的な評価は未実施で今後の課題であるが，筆者の周辺での小さな評価によれば，特に，複数ルールの組み合わせ・インラインルール通知は，他者拒否率の向上に寄与していると感じられる．また，ルールのカスタマイズは，ユーザの好みをより柔軟に受け止めていると感じられる．会議でのインタラクティブ発表において，読者にも評価いただき議論できれば幸いである．

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., Perrig, A.: Déjà Vu: A User Study Using Images for Authentication, *USENIX Security Symposium* (2000).
[3] 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).
[4] 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).
[5] 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).
[6] 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).
[7] 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).
[8] 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).
[9] 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).
[10] 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).
[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] 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).
[13] 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).
[14] 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).