ワンタイム顔画像生成に基づく画像認証手法

石井 健太郎[1]

概要：スマートフォンのようなタッチ操作をともなう端末では，入力の位置からパスワード/パスコードやパターンロックの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．この課題に対して，本研究では人間の顔画像を都度生成して利用する手法を提案する．提案手法では，Generative Adversarial Networks (GAN) の 1 種の画像生成技術である StyleGAN の style mixing と呼ばれる 2 つの画像の特徴を混ぜ合わせる技術を利用して，正規のユーザがあらかじめ決めておいた特徴を持つ顔画像と持たない顔画像を新規に生成して画面に提示する．認証を受けようとするユーザは，提示された複数の顔画像の中から，画像の特徴を手がかりにして，正解画像を選ぶことによって認証を受ける．都度異なる顔画像が提示されるため，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．プロトタイプ実装を Android スマートフォンに行い，実験者が認証を受けている場面を実験参加者がのぞき見を行う評価実験を行ったところ，パスワード/パスコード認証・パターンロック認証・固定の画像認証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．

Authentication based on One-Time Face-Picture Generation

KENTARO ISHII[1]

1. はじめに

スマートフォンのようなタッチ操作をともなう端末では，入力の位置からパスワード/パスコードやパターンロックの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 [1], [2]．この課題に対して，都度表示される画像を切り替えることでのぞき見のリスクを低減するワンタイム図形生成に基づく画像認証手法 [3] や，その発展的手法として図形生成のルールをランダムに切り替える手法 [4] が提案されている．これらの先行研究ではパラメトリックな図形を生成して利用しているが，本研究では人間の顔画像を生成して利用する手法を扱う（**図 1**）．

個人認証に画像を利用することの背景には，認証情報の入力を求める再生記憶よりも，提示された情報が目的のものであるかを求める再認記憶のほうが記憶負荷が低いとされることが挙げられる [5]．画像認証は，Cognometric 方式・Locimetric 方式・Drawmetric 方式の 3 つに大きく分類されるが，画像そのものを選択する Cognometric 方式が最もシンプルに再認記憶を用いる方式であり，さまざまな提案がなされている [5], [6], [7], [8], [9]．しかし，これらの手法は，提示されている画像が正解画像そのものであるため，のぞき見によって画像を記憶されてしまうと，認証を受けるために必要な情報が完全に盗まれてしまうこととなる．これは，通常の Cognometric 方式画像認証の原理的な短所と言える．

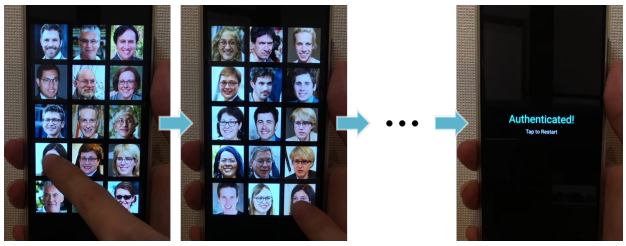


図 1 ワンタイム顔画像生成に基づく画像認証手法．ユーザは正解画像をあらかじめ決められた回数正しく選択できれば認証される．

Cognometric 方式画像認証におけるのぞき見のリスクの低減手法として，Locimetric 方式と組み合わせる手

[1] 専修大学
Senshu University

法 [10], [11], [12] や，正解画像そのものを提示するのではなく加工した画像を提示する手法 [13], [14] が提案されている．これらは，高いのぞき見耐性性能を示している一方で，ユーザへの負荷は高く，シンプルな再認が原理である Cognometric 方式の長所を妥協するものと考えられる．

そこで，本研究では，目的の顔画像を選択する Cognometric 方式のシンプルさを維持しながら，のぞき見耐性を持つ手法を追求する．提案手法ののぞき見対策の原理は，都度表示される画像を切り替えることで，非正規ユーザには画像を記憶されづらいとともに，画像を記憶されてもそのものが認証を受けるために必要な情報ではない点にある．一方で，正解画像が持つ特徴を知っている正規ユーザには，提示された画像の中から正解画像を見分けることが可能である．以上を実現するために，Generative Adversarial Networks (GAN) [15] の 1 種の画像生成技術である StyleGAN [16], [17] を利用する．人間の顔画像を学習した StyleGAN を用いると，現実には存在しない人物の顔画像を生成することができ，さらに style mixing と呼ばれる利用法を用いて 2 つの画像の特徴を混ぜ合わせて新しく 1 枚の画像を生成することができる．style mixing のパラメータを調整することにより，メイン画像の粗い特徴を保存しながらサブ画像の細かい特徴を混ぜ合わせた画像を生成することができる．この結果，メイン画像の顔の大きさ・形・眼鏡・性別といった特徴とサブ画像の顔のパーツ・髪の色・背景といった特徴が混ざり合い，メイン画像の人物の顔の特徴を残しているが別の人物に見える顔画像を新しく生成することができる．このことを利用して，認証システムに利用する画像の生成を行う．

本論文では，まず提案手法の基礎となる図形生成による先行研究 [3] について，認証の原理と評価実験の結果を抜粋して簡潔にまとめる．その後，提案手法である顔画像生成による画像認証について述べる．さらに，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．

2. ワンタイム図形生成による画像認証

2.1 認証の原理

ワンタイム図形生成による画像認証では，認証画面に都度生成された図形が提示され，正規ユーザはあらかじめ設定した図形の特徴を手がかりに正解図形を選ぶ．図形生成の基本アルゴリズムは以下のとおりであり，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仕組みである．

(1) ランダムな数（2〜5）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（中心から移動後の頂点までの距離が「0〜初期頂点までの距離」の範囲内となる値）だけ移動させる．（**図 2**; 各頂点の移動距離は同一である．）

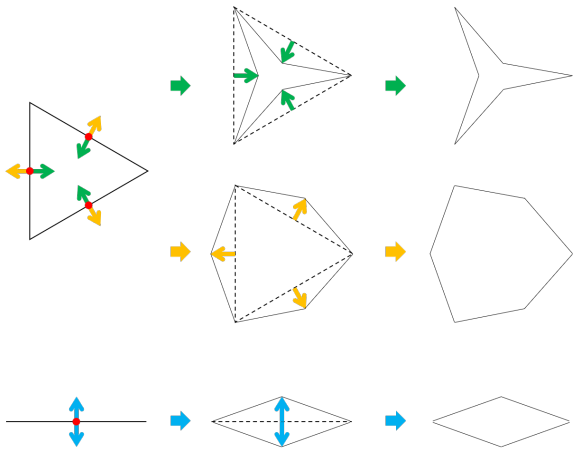


図 2 中点の移動による変形

(3) (2) をランダムな回数（2〜4）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（RGB それぞれ 128〜255）で塗りつぶす．

(5) 図形の中心を軸にランダムな角度（0〜2π）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（1〜3）だけ重ね合わせる．

(1) において頂点が 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，この場合 (2) において，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）．

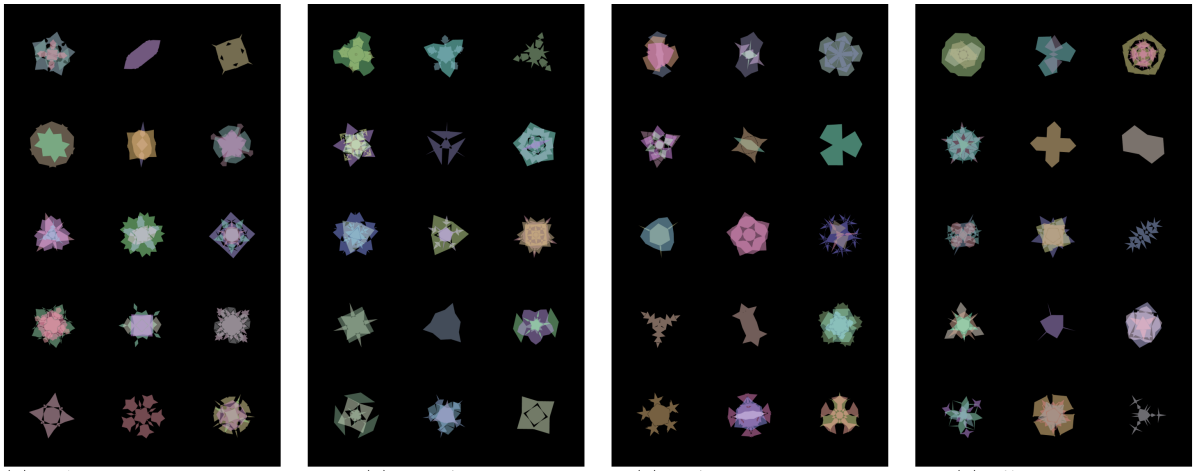
認証に用いる図形群は，以上の図形生成アルゴリズムのランダムパラメータを制限することによって生成する．このランダムパラメータの制限方法を，認証図形群生成ルールとして定義する．詳細な検討の結果 [3]，以下の 4 カテゴリ 12 ルールを定義した．ここで重要なことは，図形生成アルゴリズムとしては認証図形群生成ルールのメカニズムはランダムパラメータの制限であるが，それぞれのルールに直感的な解釈を与えることができることである．このことによって，プログラムの内部構造やパラメータの種類を知らないユーザでもルールを把握することができる．**図 3** に，4 つのカテゴリから 1 つずつ代表して，認証図形群生成ルールにより生成された図形群を示す．

カテゴリ 1 { 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



(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．

2.2　評価実験の結果

実験調査は，認証図形群生成ルールを知る正規ユーザが認証を受けている場面を 3 回連続で見たあとに，非正規ユーザ役の実験参加者が認証を受けられるかをテストする方法で行われた．ルールに関する事前知識別に評価することを目的として，ルールに基づいて動作していることやルールが存在することも知らされないシステム未体験条件と，ルールに基づいて動作していることは知っているものの同じカテゴリのルールは未体験であるルールカテゴリ未体験条件と，同じカテゴリのルールも体験済みであるルールカテゴリ体験済み条件の 3 つの事前知識条件にて，実験調査を設計した．

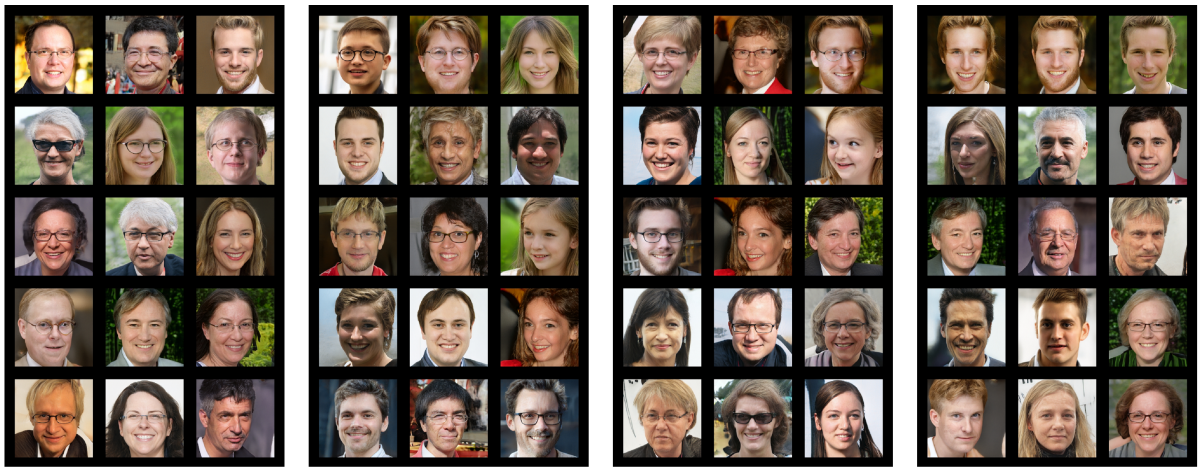
その結果，システム未体験条件の認証成功率は 11.8%，ルールカテゴリ未体験条件の認証成功率は 13.9%，ルールカテゴリ体験済み条件の認証成功率は 25.7%であった．質問紙調査によると，ルールが存在することを知らされていないシステム未体験条件の段階で，多くの実験参加者が何らかのルールに基づいて動作していることを推測しており，そのことを裏付けるように，システム未体験条件とルールカテゴリ未体験条件の認証成功率には有意な差は認められなかった．一方，ルールカテゴリ体験済み条件の認証成功率は有意に高い結果となった．

3.　ワンタイム顔画像生成による画像認証

図形生成による画像認証は，同じカテゴリのルールを未体験である 2 条件をまとめた認証成功率は 12.8%であり，同じカテゴリのルールも体験済みの条件でも 25.7%と，一定ののぞき見対策の効果を示している．ただし，生成される画像はパラメータを操作することによって定まるいわゆるパラメトリックな画像である．パラメータのとりうる値の多様性は十分確保されていると考えているが，定義できるルールは原理的に有限である．本研究では，ノンパラメトリックな画像生成手法を用いて，生成画像のさらなる多様性の確保やより制限の少ないルール定義の可能性を探る．本論文で用いる画像生成技術は，顔画像に限らず任意の画像に適用できるものであるが，第 1 の検討として本論文では人間の顔画像を題材とする．人間の顔画像を採用した理由は，公開されていてすぐに利用可能であった学習済み画像生成モデル[*1]のうち，正規ユーザにとって最も正解画像の特徴が識別しやすい画像であろうと考えたことによる．

図 4　style mixing によって生成された顔画像．1 行目をメイン画像・1 列目をサブ画像として，同じ列のメイン画像と同じ行のサブ画像を混ぜ合わせて生成された画像を並べている．概ね，メイン画像の顔の大きさ・形・眼鏡・性別といった特徴は残したまま別の人物に見える顔画像が生成されている．

[*1] 実装を開始した時点で，人間の顔のほかに猫の全身・車・ベッドのあわせて 4 つの画像生成モデルが利用可能であった．



(1) 眼鏡なし女性　(2) 眼鏡あり女性　(3) 眼鏡なし男性　(4) 眼鏡あり男性

図 5　4 つの認証ルールによって生成された認証問題の例．各認証問題は 1 つの正解画像と 14 のダミー画像を含む．

3.1　StyleGAN による顔画像生成

本研究で利用する StyleGAN には，style mixing と呼ばれる 2 つの画像の特徴を混ぜ合わせて新しく 1 枚の画像を生成する利用法があり [16]，style mixing のパラメータを調整することにより，メイン画像の粗い特徴を保存しながらサブ画像の細かい特徴を混ぜ合わせた画像を生成することができる．**図 4** は，style mixing におけるメイン画像・サブ画像・それらを混ぜ合わせて新しく生成された画像の 3 種類によって構成されている．1 行目はメイン画像を横に並べたものであり，1 列目はサブ画像を縦に並べたものである．その他の画像は，同じ列の 1 行目の画像をメイン画像・同じ行の 1 列目の画像をサブ画像として生成した画像である．この結果，メイン画像の顔の大きさ・形・眼鏡・性別といった特徴とサブ画像の顔のパーツ・髪の色・背景といった特徴が混ざり合い，メイン画像の人物の顔の特徴を残しているが別の人物に見える顔画像を新しく生成することができる．このことを利用して，認証システムに利用する画像の生成を行う．

3.2　認証ルールの定義

本研究の認証の原理は，毎回異なる画像群から，特定の特徴を持つ正解画像を言い当てることである．正解画像の手がかりとなる画像の特徴とは，例えば，「眼鏡をかけていない女性」といったものであり，これを認証ルールと呼ぶこととする．正解画像でない画像をダミー画像と呼ぶことにすると，認証ルールが「眼鏡をかけていない女性」である場合は，眼鏡をかけている人物の顔画像はダミー画像であり，男性の顔画像はダミー画像であり，このようにして正解画像とダミー画像を見分ける．

提案手法は毎回異なる画像を提示することがのぞき見対策の原理であることから，正解画像とダミー画像をともに大量に生成する必要があり，3.1 節で述べた style mixing を利用する．メイン画像は，認証ルールに合致する特徴を持つ顔画像を手作業で選定しなければならない．しかし，サブ画像は任意の顔画像でよい．図 4 に示すとおり，メイン画像に認証ルールに明確に沿う画像を選定する限り，認証ルールに合致しないサブ画像を混ぜ合わせても，生成される画像は概ね認証ルールに沿っている．したがって，認証ルールの定義は，style mixing のメイン画像として与えられる明確に分類できる顔画像を用意することによってなされると言うことができる．

本論文の実装では，認証ルールとして「眼鏡をかけていない女性」（以降「眼鏡なし女性」と呼ぶ）・「眼鏡をかけている女性」（以降「眼鏡あり女性」と呼ぶ）・「眼鏡をかけていない男性」（以降「眼鏡なし男性」と呼ぶ）・「眼鏡をかけている男性」（以降「眼鏡あり男性」と呼ぶ）の 4 つを用意することとした．そして，「眼鏡なし女性」・「眼鏡あり女性」・「眼鏡なし男性」・「眼鏡あり男性」である顔画像を，メイン画像として 4 つのルールについてそれぞれ 10 枚用意し，そのそれぞれに任意のサブ画像を混ぜ合わせて認証問題作成の材料とする．なお，style mixing の材料となるメイン画像・サブ画像はともに StyleGAN の同じ学習済みモデルから生成し，ランダムで繰り返し生成した顔画像の中から手作業で認証ルールに沿うものメイン画像として選定し，選定しなかったものすべてをサブ画像として利用した．原理的には，サブ画像の生成を追加する限り，認証問題に沿った異なる顔画像が生成されることとなる．

図 5 は，4 つの認証ルールにおける認証問題の例である．毎回異なる顔画像が並ぶことになるが，どの画面にも認証ルールに合致する正解画像が 1 枚だけ表示される．本論文の実装では，4 つの認証ルールは互いに排他的であるため，適用されていない認証ルールの画像をダミー画像としてそのまま用いることとした．

図 6　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 節の認証ルールを用いて生成した画像を組み込み，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，Android スマートフォンのスマートフォンアプリとして用意した（図 6）．

このアプリケーションでは，画面上に 15 の画像が提示され，ユーザがそれらのうちの 1 つを選択するのを待ち受ける．画像の選択を行うと，画面が切り替わり別の 15 の画像が提示される（図 6 左）．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，認証ルールに基づいて 1 つの正解画像と 14 のダミー画像が含まれており，すべての画面で正解画像を選択できれば認証される．また，認証ルール選択のための設定画面も用意し，「眼鏡なし女性」・「眼鏡あり女性」・「眼鏡なし男性」・「眼鏡あり男性」の代表画像を選択することにより，認証ルールを切り替えることができる実装である（図 6 右）．

4.　評価実験

4.1　目的と方法

のぞき見耐性が重要な要件である一方で，複雑になりすぎて，熟練したユーザでないと利用できないというものであると，利用価値を損なってしまうと考えられるため，評価はのぞき見に対する効果を示しているか・初めてのユーザが即座に利用できるかの 2 つの観点で行う．それぞれの目的のため，実験調査は 2 段階に分けて実施する．

はじめに，実験者が正規ユーザ役となり，実験参加者はのぞき見を行う非正規ユーザ役となる実験調査を行う．非正規ユーザの役割である実験参加者は，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，実験参加者には，各認証画面に 1 つの正解画像があることのみが知らされ，認証システムが認証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．これは，先行研究 [3] のシステム未体験条件と同様の手法を踏襲したものである．その後，実験参加者が認証問題を解けるかを，認証アプリケーションの利用によってテストする．

次に，実験参加者に「眼鏡をかけていない女性」というように，認証ルールの直感的な解釈のみを与え，認証問題を解けるかを，もう 1 度認証アプリケーションの利用によってテストする．のぞき見の段階において，認証問題の解きかたがわかった場合には，どのようにすれば認証問題が解けるのかを尋ねる．認証ルールを明言しない場合など，答えがはっきりしない場合は，はっきりしない箇所について追加の質問を行う．解きかたが正しい場合は実験調査はそれで終了となり，誤っている場合は正しい認証ルールの直感的な解釈を与えて，認証問題が解けなかった実験参加者と同様に，もう 1 度認証アプリケーションの利用によってテストする．

3.2 節で述べたどの認証ルールを利用するかは，それぞれの認証ルールの実験参加者が同数になるように割り当てる．以上をまとめると，実験調査は以下の手続きで実施する．

(1)　実験者は実験参加者に，認証アプリケーションは正解画像を選ぶことによって動作していること・1 回の認証試行につき 4 回の画像の選択 (解答試行) が必要であること・いまから 3 回認証を受ける場面を連続でのぞき見したのち認証を受けられるかをテストすることを説明する．

(2)　実験参加者は，のぞき見をしやすい位置どりを自由に選ぶ．このとき，実験者との体格差などでのぞき見をしやすい位置どりができない場合は，実験者はいすに座る・かがむ・スマートフォンを実験参加者のほうへ傾けるといったことをする．

(3)　実験者は認証アプリケーション利用を 3 回認証を受けるまで連続で行う．その間，実験参加者は実験者のそばでのぞき見を行う．

(4)　実験者の 3 回の認証試行の終了後，実験参加者は認証を受けることを目指して，認証アプリケーション利用のテストを認証を受けられるかあきらめるまで行う．

(5)　実験参加者が認証を受けることができた場合は，実験者は実験参加者に，どのようにすれば認証問題が解けるのかあるいは認証ルールは何であったのかを尋ねる．実験参加者が認証を受けることができずあきらめた場合は，実験者は認証ルールを伝え，もう 1 度認証アプリケーション利用のテストを行う．

4.2　結果

16 名の実験参加者を招き実験調査を実施した．4 つの認証ルールには，4 名ずつ割り当てることとなった．結果，いずれも「眼鏡なし男性」の実験参加者 2 名がのぞき見後に認証問題を解くことができ，残りの 14 名は認証問題を

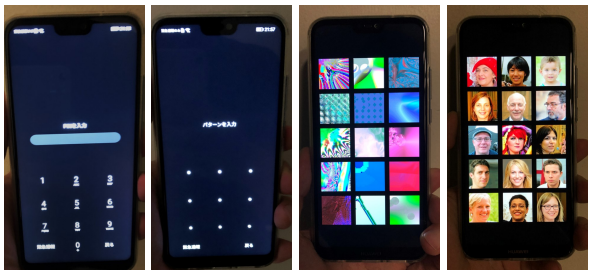


図 7　既存手法: 左から，パスコード認証・パターンロック認証・ランダムアート画像認証・顔画像認証

解くことができなかった．非正規ユーザののぞき見による認証成功率は 12.5%である．また，認証問題を解くことができた実験参加者 2 名はいずれも，「眼鏡なし男性」の画像を選べば認証を受けられることを言い当てた．さらに，当初認証問題を解くことができなかった 14 名全員が，認証ルールを与えられたあと認証問題を解くことができた．

4.3　既存手法との比較

2.2 節で述べた図形生成を用いた先行研究 [3] の結果と比較すると，システム未体験条件と同様の結果が出ている．ルールカテゴリ未体験条件とルールカテゴリ体験済み条件に相当する実験の設定では未検証であるため，今後そのような設定の実験調査の実施を予定している．

また，実用されているパスコード認証・パターンロック認証の 2 手法と，本研究と同じ画像認証で固定のランダムアート画像を用いた手法 [5]・固定の顔画像を用いた手法 [6] の 2 手法の計 4 手法に対しても，同様ののぞき見実験調査を行った（**図 7**）．いずれの手法も，提案手法と同じ Android スマートフォンを機材として用いた．

12 名の実験参加者を招き実験調査を実施した．実験参加者は 4 つの手法すべてについて手順を繰り返すこととし，本実験と同様に，のぞき見を行ったあとの認証のテストを実施した．結果，パスコード認証の認証成功率は 100%，パターンロック認証の認証成功率は 72.2%，ランダムアート画像の認証成功率は 61.1%，顔画像の認証成功率は 50.0%であった．

以上の結果から，のぞき見耐性は向上していると言うことができる．一方で，初めてシステムを利用した実験参加者でも認証ルールを知らせたあとは問題なく認証を受けることができていたことから，既存の手法と同等の利用しやすさを有していると考えられる．

5.　議論

4 章の評価実験によって，提案手法には一定の効果があることが示されたが，提案手法の有効性は以下の 2 点を検証することで，より深く議論できると考える．それぞれについて，現在追加の実験調査を準備しており，さらなる検討を行う予定である．

第 1 に，認証ルールとして利用する style mixing のメイン画像にどのようなものが利用できるのかを検証する．本論文では，眼鏡のありなしと女性か男性かを画像の特徴として利用したが，原理的にはこれらの特徴に制限されるものではなく，混ぜ合わせたあとの画像が元の画像の特徴を残すものであればよい．混ぜ合わせた場合に残りづらい特徴というものがあることも考えられるため，その限界を見極めることが重要である．認証ルールとして有効な画像の特徴が十分広く確保されるのであれば，4 カテゴリ 12 ルールと設定できるルールに限りがあった先行研究 [3] の欠点を克服することができる．また，顔画像以外の画像生成モデルを利用することで，さらなる認証ルールの多様性を確保できる可能性がある．

第 2 に，のぞき見する者の事前知識が不正認証に与える影響を検証する．本論文の実験の設定とは異なり，提案手法が認証ルールに基づいて動作していることを実験参加者に知らせた状況での追加実験を予定している．認証ルールの定義は style mixing のメイン画像を用意するだけでよいため，先行研究 [3] とは異なり，のぞき見する者が知らないメイン画像を用意することで，ルールカテゴリ体験済みという状況自体を原理的に避けられる可能性がある．そのため，先述の認証ルールの多様性とセットで検証する予定である．

さらに，ワンタイム図形生成による画像認証でも有効であった 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 [4] も，提案手法には適応しうるものである．認証ルールを把握している者であっても設定を明かさなければ，認証に必要な情報を取得することを防ぐことが示されており，提案手法自体の有効性の検証とは別に，応用上の効果が求められる場面においては，認証ルール切り替えを導入することも検討すべきことである．

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，ワンタイム顔画像生成に基づく画像認証手法を提案した．提案手法では，認証ルールに沿うような特徴を残した正解画像とそうでないダミー画像を多数生成することで，毎回異なる画像を表示する．そのため，のぞき見が行われた場合であっても，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．

プロトタイプを実装して，評価実験を行ったところ，のぞき見を認めているにも関わらず高い他者拒否率を示し，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．今後，認証ルールとして利用できる画像の範囲の検証と，のぞき見する者の事前知識が不正認証に与える影響を検証する追加実験を計画している．

参考文献

[1] Aviv, A.J., Davin, J.T., Wolf, F., Kuber, R.: Towards Baselines for Shoulder Surfing on Mobile Authentication, *Annual Computer Security Applications Conference*, pp.486–498 (2017).

[2] 石塚正也，高田哲司：CCC：携帯端末での暗証番号認証における振動機能を応用した覗き見攻撃対策手法，情報処理学会論文誌，Vol.56, No.9, pp.1877–1888 (2015).

[3] 石井健太郎，香川将樹，島谷和樹：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，情報処理学会論文誌，Vol.60, No.12, pp.2127–2138 (2019).

[4] 石井健太郎：インラインルール通知を用いたワンタイム図形認証，マルチメディア，分散，協調とモバイルシンポジウム 2019 論文集，pp.1161–1167 (2019).

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

[6] Tari, F., Ozok, A.A., 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).

[7] 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).

[8] 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).

[9] 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).

[10] Wiedenbeck, S., Waters, J., Sobrado, L., 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).

[11] Man, S., Hong, D., Matthews, M.: A Shoulder-Surfing Resistant Graphical Password Scheme - WIW, *Security and Management*, pp.105–111 (2003).

[12] Zhao, H., 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).

[13] 原田篤史，漁田武雄，水野忠則，西垣正勝：画像記憶のスキーマを利用したユーザ認証システム，情報処理学会論文誌，Vol.46，No.8，pp.1997–2013 (2005).

[14] 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).

[15] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., Bengio, Y.: Generative Adversarial Nets, *International Conference on Neural Information Processing Systems*, pp.2672–2680 (2014).

[16] Karras, T., Laine, S., Aila, T.: A Style-Based Generator Architecture for Generative Adversarial Networks, *IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp.4401–4410 (2019).

[17] Karras, T., Laine, S., Aittala, M., Hellsten, J., Lehtinen, J., Aila, T.: Analyzing and Improving the Image Quality of StyleGAN, *IEEE/CVF Conference on Computer Vision and Pattern Recognition*, (to appear) (2020).