情報処理学会論文誌 Vol.64 No.6 1–18 (June 2023)

画像内にある特徴点の列を秘密鍵とした視線入力による認証手法

大和 優輝[1,†1,a)] 高橋 伸[1,b)]

受付日 2022年9月5日, 採録日 2023年3月9日

概要：
本研究では，画像内にある特徴点の列を秘密鍵として，それを視線入力により入力する新たな認証手法を提案する．特徴点とは画像内における物体や部位，顔といった意味のある箇所のことである．ユーザは画面上に表示される画像中の特徴点集合から複数の特徴点を順序付きで指定し，それを秘密鍵として登録する．そして，スマートフォンやラップトップコンピュータのロック解除をする際などには，ランダムに表示される類似画像に対して，登録した秘密鍵に対応する特徴点を順番に注視する．システムは登録された秘密鍵の通りにユーザが特徴点を正しく視線入力したかどうかにより，ユーザを認証する．本手法は，ショルダサーフィン攻撃，スマッジ攻撃，サーマル攻撃に強い視線入力認証と，辞書攻撃やブルートフォース攻撃に強く記憶性に優れた画像パスワード認証との双方の長所を持つ．

キーワード：個人認証，視線入力

A Gaze-Based Authentication Method that Adopts a Sequence of Image Feature Points as a Secret Key

Yuki Yamato[1,†1,a)] Shin Takahashi[1,b)]

Received: September 5, 2022, Accepted: March 9, 2023

Abstract:
We propose a new gaze-based authentication method that uses a sequence of feature points in an image as a key (secret). In this method, the user registers a secret by selecting a sequence of several feature points in an image displayed on the screen. Then, the user is authenticated by gazing at the feature points on similar images that are displayed at random. This method has the advantages of both eye gaze input, which is resistant to side-channel attacks such as shoulder surfing, smudging, and thermal attacks, and image password authentication, which is resistant to dictionary/brute force attacks and has excellent memorability.

Keywords: Personal Authentication, Gaze Input

1. はじめに

スマートフォンやタブレット，デスクトップコンピュータ，ラップトップコンピュータといった情報端末が広く普及している．それらは日々の生活から業務に至るまで多様な環境において利用されており，個人情報や社外秘の情報など多くの機密情報を保持している．そのため，機密情報保護の観点からデバイスの利用ユーザを確認する本人認証システムが必要不可欠となっている．認証システムには，従来から利用されてきたパスワードや Personal Identification Number（PIN），スマートフォンにおいて普及したパターン認証，また近年急速に普及してきた指紋認証，顔認証，静脈認証といった生体認証などがある．さらに，それらを組み合わせたり，繰り返し用いることで堅牢性を高める多要素認証，多段階認証がある．

[1] 筑波大学
[†1] 現在，アクセンチュア株式会社
[a)] yamato@iplab.cs.tsukuba.ac.jp
[b)] shin@cs.tsukuba.ac.jp

モバイルデバイスでの認証には，PIN やパスワード，パターン[*1]といった知識ベースの認証が依然として主流である [1]．生体ベース認証は知識ベース認証に比べて認証に用いる秘密鍵が漏洩しにくく，十分な堅牢性と即時認証といった利便性を得られる反面，一度でも秘密鍵が流出するとリセットや再発行が困難であるためユーザにとって生涯続くセキュリティリスクとなる．一方，知識ベース認証は，攻撃者に秘密鍵が知られた場合にも，容易に変更可能である．しかしながら，PIN やパスワードのように単純な数字や文字を使った認証は，辞書にある単語やインターネット上に存在する漏洩したパスワードリスト等を使って攻撃する辞書攻撃や，ありうる秘密鍵のパターンを総当たりで攻撃するブルートフォース攻撃にさらされる危険性を持つ．

そこで，これらの攻撃に強い画像パスワード（Graphical Passwords）を利用した認証が提案されてきた [2], [3], [4], [5]．画像パスワードは視覚的記憶を利用しており，文字や数字の羅列である PIN あるいはパスワードに比べて，多くの利点がある [2], [5]．また，画像パスワードでは，数字や文字を使う場合と比較して，画像の種類数を増やすことでパスワード空間をより拡大できる可能性があり，従って推測攻撃にも強くできる可能性がある [6]．しかしながら，攻撃者に観察され得る入力（タッチ入力，キーボード入力，マウス入力）を必要とするため，入力時の様子を (密かに背後等から) 覗き見ることにより秘密鍵情報を不正に取得することを試みるショルダサーフィン攻撃を受ける可能性がある．特に，公共空間の ATM 等や共有の PC においては，ビデオカメラ等により入力操作を盗撮され，パスワードあるいは PIN が盗用される可能性が存在する．

一方，視線追跡技術の向上により，スマートフォンやタブレット等のモバイルデバイスやラップトップの画面のどこをユーザが見ているかを検出することが容易になってきた [7]．ユーザの視線を利用して，キーボード入力や，タッチ入力の必要がないユーザ認証を行うことが可能となってきている [8], [9], [10], [11]．これらの視線を利用した認証は，物理的接触を伴う入力を必要とせず，タッチフリーであるため，背後から覗き見るショルダサーフィン攻撃や，指紋の汚れをたどるスマッジ攻撃[*2]，操作後の熱を検知するサーマル攻撃[*3]に耐性を持つ．さらに人間の目は高速に動くため，視線に基づく入力の解読はタッチベースの入力に比べて困難である．しかし，極めて単純な視線の軌跡は，攻撃者が目の動きを捉えることができれば，解読可能であることが報告されている [10]．また，視線の軌跡や動きをパスワードとして使う手法では，慣れないパスワードシンボルを覚えなければならないため，パスワードの記憶性が低下する可能性がある [11]．

本研究の目的は他者からの攻撃に強く堅牢な認証を可能とすることである．また，想定する主な認証場面はスマートフォンのロック解除や Windows Hello などの PIN 入力等の代替である．この目的を達成するためのアプローチとして，ユーザが画像内のいくつかの特徴点を順番に注視することにより認証を受けるという手法を提案する．特徴点とは画像内の物体や部位など何らかの特徴を持つ箇所のことであり，例えば，図 1 における耳や鼻，目，足などである．ユーザはこれらの特徴点の中から複数を選択し，順序のついた列としてあらかじめ登録しておく．本論文ではこの列を「特徴点列」と呼ぶ．この特徴点列を認証時の秘密鍵として利用し，画面にランダムに表示される類似画像において，ユーザが各特徴点を登録した順番に注視するかどうかにより認証を行う．類似画像（例えば，犬や猫といった動物の画像）は同じ特徴点を共有しており，一度登録した秘密鍵は複数の画像において適用可能である．

図 1 提案手法を実行するイメージ図．青色の点は鍵として登録した特徴点列内の各点を表しており，オレンジ色の矢印がユーザが認証のために視線を移動させている様子を示している．これらはスマートフォンの画面には表示されず，実際には画面上に画像が表示されているだけである．なお，図はスマートフォン環境での利用を示しているが，スマートフォン環境だけでなく，ラップトップなど他の環境での利用も考えられる．

本手法は，ショルダサーフィン，スマッジ攻撃，サーマル攻撃に強い視線入力と，辞書攻撃，ブルートフォース攻撃に強く，記憶性に優れた画像パスワード認証の両方の長所を持つ．攻撃者がデバイスの画面を盗み見たとしても，視線入力であるため，ユーザが画面を見ていることしか分からない．画面には入力のフィードバックは何も表示されないため，秘密鍵の情報，つまり注視箇所と注視回数や，注視タイミングなどを特定することは難しい．そして，ダイヤルパッドやキーボードのような明確な入力箇所を持たないため，見るべき場所も把握しにくくなっている．これらから，秘密鍵を推測することは困難であると考えられる．また，ユーザの目の動きを観察された場合にも，それだけでユーザが意図して注視した箇所の細かな座標的位置を推

[*1] 画面内に表示された点を順番に指でなぞる認証方法
[*2] タッチパネルに指でタッチするとタッチした位置に残るスマッジ (汚れ) を見て秘密鍵情報を不正取得しようと試みる攻撃
[*3] スマッジ攻撃と同様にタッチの痕跡を元に攻撃する手法であるが，サーマル攻撃では触った場所が周囲より温度が高くなることを利用してタッチした位置の不正取得を試みる．

測することは難しいと報告されている [8]．仮におおよその視線の動きが知られてしまったとしても，認証ごとに表示される画像は異なり，ユーザが注視すべき場所も変わるため，正確に秘密鍵を再現することは非常に困難である．

本論文では，2 節で関連研究を述べた後に，3 節において提案手法の詳細について紹介する．4 節と 5 節は提案手法の評価のためにスマートフォン環境とラップトップコンピュータ環境のそれぞれにおいて実装したプロトタイプシステムについて述べる．4 節では視線追跡の実装について，また 5 節ではプロトタイプのインタフェースを中心に述べる．6 節ではプロトタイプを利用して行った評価実験について述べ，7 節では実装および評価を通して得られた知見や課題について議論する．最後に 8 節で結論を述べる[*4]．

2. 関連研究

スマートフォンやラップトップコンピュータ等の情報デバイスの認証システムをより堅牢に，そして，実行を容易にするために，これまでに多くの認証手法が提案されてきた．本節では，まず情報デバイス利用時の認証手法について述べ，次に画像パスワードに基づく認証手法と，視線入力による認証手法について述べる．最後に本研究の位置付けについて述べる．

2.1 情報デバイス利用時の認証手法

情報デバイス利用時の認証は大きく分けて知識ベース，生体ベースのカテゴリが存在する．知識ベースの手法は，Personal Identification Number（PIN）[13] やパスワードに代表され，ユーザの既知情報を秘密鍵として認証を行う．これらの手法はブルートフォース攻撃やソーシャルエンジニアリング，キーロギングによりハッキングされる懸念が報告されていて，対処するために多くの手法が提案されてきた [14], [15], [16], [17]．例えば，秘密鍵に含める要素として単純な文字列や数字ではなく，位置情報や画像，ユーザの使用履歴を利用した手法がある．Hang らと Thorpe らは，地図内の場所を鍵として用いる手法を提案した [15], [16]．Shone らは，画像を鍵として用いて，ロック画面で鍵となる画像を選択する認証を提案した [17]．Gupta らは，SMS や通話履歴，アプリの使用状況といったスマートフォンの使用履歴を利用する手法を提案した [18]．ユーザはいつ電話をしたかや，使用頻度の高いアプリは何かといった質問に回答することによりスマートフォンの画面ロックを解除できる．

生体ベースの手法は，指紋や顔といったユーザ固有の生体情報を鍵として認証を行う．生体情報はシリコンや樹脂を用いて複製されることによる攻撃を受ける懸念が報告されている [19]．Apple 社の開発した FaceID は顔の深度マップを作成して顔の正確なデータを鍵として利用することにより，顔画像によるロック解除を防止し，より堅牢性を高めた [20]．また，Samsung 社は複製の難しい両目の虹彩を鍵とすることによりデバイスの安全性を高めた [21]．Sandström らと Sepasian らは，生の指と人工の指を区別するプロセスを導入することにより，人工指紋による攻撃に対する堅牢性を高めた [19], [22], [23], [24]．他にも，耳の形を利用したもの [25] や，生体信号を利用するもの [26], [27] がある．近年ではユーザの動きを利用するものも提案されてきた．ユーザがスマートフォンの画面をタップする仕方にはユーザ毎のパターンがあることを利用して，PIN を入力するときのタップの仕方を認証に利用する手法がある [28]．また，Chen らはダブルタップの仕方を鍵として使用した [29]．他にも，画面に表示された曲線のなぞり方を鍵とするもの [30] や，ユーザの歩行の仕方を利用するもの [31]，腕の動きを利用するもの [32], [33], [34], [35] がある．

なお，多段階認証と多要素認証は，これらの認証手法などを複数組み合わせることで，堅牢性を高める手法である．多段階認証は，例えばパスワード入力後にさらにあらかじめ登録したクイズに答えさせるなど，繰り返し認証を行わせる手法である．多要素認証は異なる種類の認証を組み合わせる手法で，パスワード入力に加えて，登録済みの携帯電話にショートメッセージサービスによって送られるコードを入力するなどの例がある．これらの手法の堅牢性は組み合わせられた個々の認証単体より一般に高くなると考えられ，我々の提案手法も組み合わせることが可能である．一方，実際の利用時には不便になってしまう場面も想定できる．Reese らの実験では，2 要素目の認証に必要なデバイスが手元に無くて認証できない場面があったと，3 分の 1 の実験参加者が報告している [36]．求められる堅牢性とユーザビリティのバランスを考慮した認証手法の適用を考える必要がある．

2.2 画像パスワードに基づく認証手法

画像をパスワードに用いる画像パスワード手法は知識ベース認証手法の一つである．文字列や数字を用いる従来の認証システムが持つ，辞書攻撃やブルートフォース攻撃，キーロガーに対する脆弱性を解決するために，多くの画像パスワードを活用する手法が提案されてきた．画像パスワードは，人の視覚記憶を利用しているため，記憶性や使用感の面で多くの利点を持つと報告されている [4], [37]．画像パスワードは，画像の種類数を増やすことでパスワード空間を大きくしやすいため，推測攻撃に対しても強くしやすいと期待できる一方，実質的なパスワード空間は狭くなるという報告もある [38], [39]．

画像パスワードの認証方式は，複数の画像を選択する方式 [2], [40], [41], [42], [43] と画像内の複数の点を選択す

[*4] 本論文は [12] において発表した内容を発展させ評価を一部追加したものである

る方式 [44] の 2 通りが存在する．しかしながら，物理的な入力を必要とする画像パスワードはショルダサーフィン攻撃に対して脆弱であることが報告されている [44]．そのため視線入力による画像パスワード手法が提案されている [6], [45]．視線入力を用いた手法については次節で述べる．

2.3 視線入力による認証手法

視線入力による認証手法には，パスワードや PIN といった従来型パスワードを視線入力する手法 [46] と，視線の軌跡など視線の動きを「視線パスワード」として利用する手法の 2 種類が存在する．いずれにしても視線入力による認証は，物理的接触を伴うインタラクションを必要としないため，ショルダサーフィン攻撃，スマッジ攻撃，サーマル攻撃に対して堅牢であるという大きな利点がある．

従来型パスワードを視線入力する例として，EyePassword [47] や EyePIN [8] がある．これらは，キーボードやタッチパッドによる入力の代わりに，視線に基づくタイピングを利用する認証を実現した．特に公共の場において，ユーザはキーボード入力よりも視線入力を好むことが報告されている [47]．また，GazeTouchPIN [48] は，タッチ入力に続いて視線を左右に向けることにより PIN を入力して認証を行うマルチモーダルな 2 段階認証を取り入れ，ショルダサーフィン攻撃に対してより安全な認証方式を実現した．

視線パスワードには，画像内の単一または複数点を注視するもの [6], [45]，画面内に表示された特定の点を追跡する順序 [49] を利用するもの，事前に定義された視線の軌跡（視線ジェスチャ）を利用するもの [8], [9], [50], [51], [52], [53]，ユーザが自由に決める視線の軌跡 [10] を利用するものなどがある．例えば，Free-Form Gaze Passwords [10] は，あらかじめ決められた視線ジェスチャや注視ポイントに依存しない，自由形状の視線の軌跡を視線パスワードとして利用した．また，視線パスワードを入力している映像を攻撃者が観察し，成り済ましを行う実験により，視線による入力がショルダサーフィンへの対策となることを示した．しかし，完全に自由な形式での視線パスワード作成および入力はユーザに不快感を与えることも報告されている．Heikkila ら [54] は視覚的フィードバックを導入することにより，入力を高速化し，認証時間を短縮したが，これはショルダサーフィン攻撃への優位性を損なう恐れがある．

2.4 本研究の位置付け

本研究では，特徴点列内の各点を順番に注視することにより認証を受けるという手法を提案する．本研究が提案する認証手法は，知識ベースの認証手法の一つに分類され，画像パスワードに基づく認証手法と視線入力による認証手法を組み合わせたものである．従来の画像パスワードに基づく手法には，複数の画像の中からどの画像をどういう順番で選択するかによって認証するもの，特定画像内の特徴点集合からどの点をどういう順番で選ぶかによって認証するものがある．一方，本研究の提案手法は，ランダムに表示される類似画像内の特徴点について，どの点をどういう順番で選択するかにより認証するものである．一つの鍵を複数の類似画像に適用することができ，また，その際に画像が異なれば実際に入力する点の絶対位置が変わる点で，従来手法との違いがある．また，2.3 節にて説明した視線入力による手法とは，視線入力を用いている点は共通であるが，入力する鍵が異なっている．特に，視線パスワードとして画像内の一つ以上の点の位置を利用する手法 [6], [45] は，画像パスワードを視線入力するとも言うことができ，本研究と共通性がある．しかし，本研究の手法ではパスワードが特定画像内の絶対位置として定義されているのではないという点が異なる．本研究のパスワードは特徴点を並べた特徴点列であり，各点は特徴自体によって定義されている．実際に注視すべき点の位置は画像が与えられると決まるものであり，対応する特徴点を含む類似画像を収集あるいは生成することにより，同一パスワードを多数の画像に対して利用することができる．そのため同一パスワードでありながら，認証毎に異なる画像を用いることができ，かつ注視する絶対位置を変更することができる．そのため，観察による攻撃に強いと期待できる．

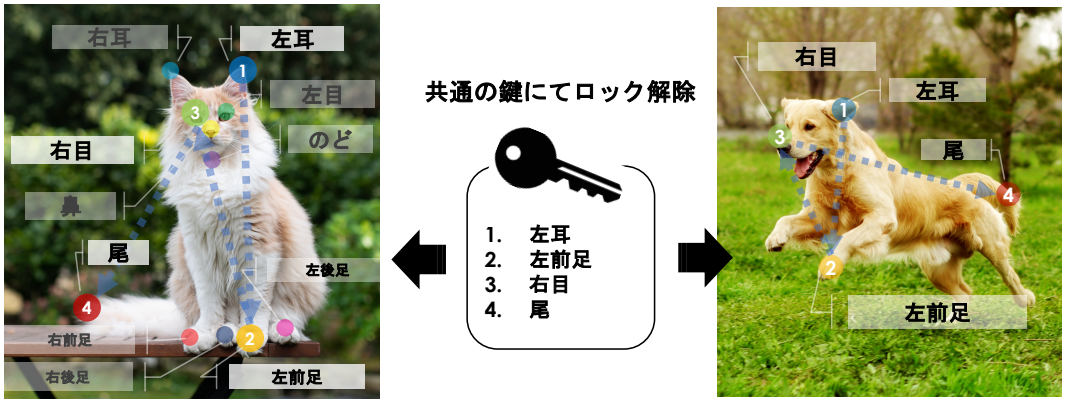
3. 提案する認証手法

3.1 概要

本論文で提案する認証手法は，画像内の特徴点列を秘密鍵とし，その秘密鍵をユーザが視線によって入力するという手法である．秘密鍵とは認証に必要な秘密情報である．本認証手法の秘密鍵は画像内の特徴点を並べた列 (特徴点列) であり，画像に基づくパスワードの一種であると言える．例えば，図 2 の場合，左耳，左前足，右目，尻尾の 4 点から成る特徴点列を秘密鍵として登録している．ユーザは認証時に特徴点列内の各点を順番に注視する．対象となる画像は一定時間ごとにランダムに交換されるが，ユーザは登録した特徴点列内の各点に相当する特徴点を表示された画像において注視することにより認証を受けてロック解除などをすることができる．

3.2 特徴点の利用

本論文における特徴点とは，図 2 の注釈された点のように画像内における特徴的な箇所のことである．ここで特徴点は特徴自体によって定義されている．そのため，似たような画像，あるいは同じ種類の画像には「同じ」特徴点が存在する．例えば，図 2 の猫と犬の画像には，目，足，鼻といった，画像内の位置としては異なるが同じ特徴点が存在していると言える．なお，本論文では特徴点はそれぞれの画像内における領域ではなく座標点として取り扱って



(a) 特徴点とその順番の選択　　(b) 共通の秘密鍵の利用

図 2　ユーザは特徴点の名称とその順番を秘密鍵として記録する．共通の特徴点を持つ画像は共通の秘密鍵を利用してロック解除が可能である．

いる．

ユーザは特徴点列，つまり特徴点の名称とその順番を秘密鍵として登録する．複数の類似画像は特徴点を共有するため，一度登録した秘密鍵 (特徴点列) をそのまま別の類似画像に適用することができる．各画像内における特徴点の位置はそれぞれの画像によって異なるため，認証時に画像を切り替えれば，ユーザに秘密鍵の変更を強いることなく，実際に注視すべき位置を変更することができる．万が一，攻撃者がユーザの目の動きから大まかな注視位置を解読したとしても，別の画像を用いることでシステムの安全性を保つことができる．

3.3　認証インタフェース

ユーザは以下の手順に従い，秘密鍵を登録し認証を受ける．

秘密鍵登録　図 3 左が秘密鍵の登録画面である．画像上に青い点で表示されているのが特徴点であり，これらの中から秘密鍵として登録する点を順番に 1 つ以上タッチ入力で選択する．選択した特徴点は番号付きの赤い点に変化する．また，選択した特徴点の名前が画面上部に番号付きで表示される．最後に Set ボタンを押すと，選択された特徴点列が秘密鍵として登録される．なお，選択する特徴点の数に上限は無いが，現在の実装では同じ特徴点を 2 度選択できないので，画像内の特徴点の選択肢数が上限となっている．また，図 3 左は後述する実験用の実装のスクリーンショットのため，登録する秘密鍵の長さが指定されている．

認証　ユーザはランダムに表示される画像に対して，登録した秘密鍵 (特徴点列) 内の各点を順番に注視することにより認証を受け，デバイスのロックを解除する．秘密鍵の正しい特徴点を注視した場合には 1 回，正しくない特徴点を注視した場合には 2 回の振動あるいは音がフィードバックされる．正しくない特徴点を注視した場合には，最初から入力をやり直す必要がある．より詳細な認証時の動作は，図 9 の通りである．

図 3 右が認証をしている際に表示される画面の例である．写真画像が表示されているだけであり，認証のための視線入力中は表示の変化は無い．ただし，認証されずに一定時間経過した後には画像が更新される．また，一定回数認証に失敗した場合には，一定時間認証できない画像が表示される．

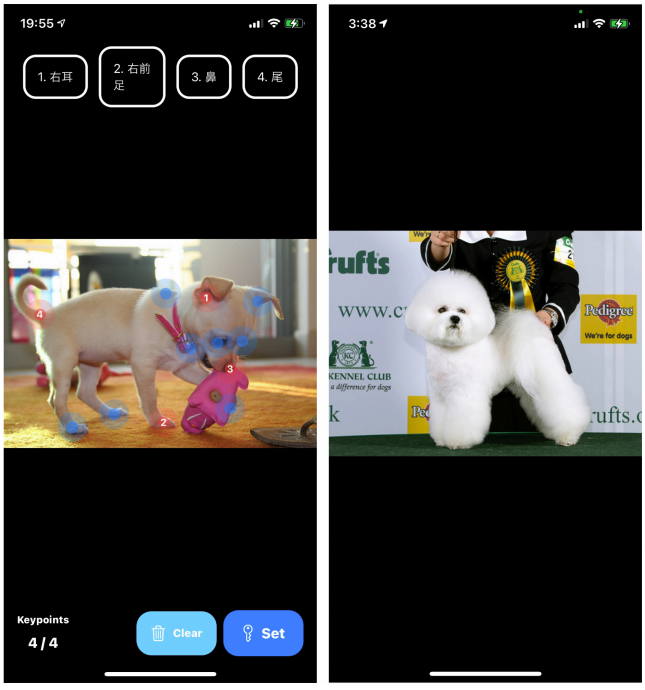


図 3　スマートフォンにおける秘密鍵の登録画面 (左) および認証画面 (右) のスナップショット．

ユーザは単純な文字列や数字列ではなく，画像を見ながら秘密鍵を覚えることができるため，視覚記憶を利用することができ，より高い記憶性を得られる可能性がある．また，スマートフォン画面の特定箇所を見るという自然な動

作を認証に利用しているため，先行研究の視線ジェスチャとは異なり，不自然で不慣れな動作をユーザに強いないと期待できる．

認証時の注視操作を補助するために，特徴点が注視された際にはユーザにフィードバックが与えられる．注視検出のタイミングを秘匿するために，スマートフォンやスマートウォッチといったモバイルデバイスにおいては，触覚フィードバックである振動を用いる．また，ラップトップデバイス等の把持や身につけることをしないデバイスにおいては，イヤホンを通して音によりユーザへ注視検出を伝える．これらにより，ユーザは注視が完了したら，すぐに次の特徴点を注視することが可能となり，実行の高速化及び同じ特徴点の多重入力を防止することができる．

3.4 堅牢性

本手法は，画像パスワード的特徴を持つ秘密鍵と視線入力とを組み合わせた認証であるため，攻撃に対する高い堅牢性を持つと期待される．つまり，画像パスワードの特徴であるブルートフォース攻撃，辞書攻撃への耐性と，視線認証の特徴である物理的接触インタラクションが存在しないことによるショルダサーフィン，スマッジ攻撃，サーマル攻撃等への耐性が期待される．

本手法に対しては，図 4 に示すような，2 種類の攻撃者が想定される．

攻撃者 A スマートフォン等のデバイスの画面に対してショルダサーフィンしようとする人．

攻撃者 B 視線の動きを読み取ろうとする人．

攻撃者 A はデバイスの画面を見ることができるが，PIN やパスワードの場合とは異なり，取得できる情報はランダムに表示されている画像のみである．そのため，攻撃者が秘密鍵を推測することは難しい．攻撃者 B の場合，ユーザの視線を観察することはできるが，ユーザの注視点を推測し，正確に再現することは容易でないことが報告されている [10]．また，仮に攻撃者におおよその視線の動きがわかったとしても，同じ秘密鍵を利用しながら認証の画像をランダムに変更することにより，認証毎に注視場所を変更することができる．そのため，ユーザに秘密鍵の変更や記憶といった負担を強いずに，セキュリティを維持することができる．

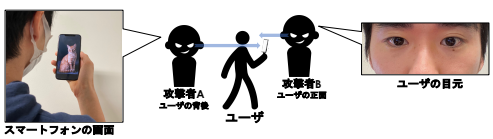


図 4 攻撃者が得ることのできる情報．ユーザの背後にいる攻撃者 A はスマートフォンの画面をショルダサーフィンする．ユーザの正面にいる攻撃者 B はユーザの目元を観察できる．

本手法の理論的パスワード空間（TPS）[*5]は，画像内において利用可能な特徴点の数（N_k）と秘密鍵の長さ (特徴点列の長さ)（n）に依存しており，$\log_2 {N_k}^n$ となる．例えば，図 2 に示す画像の場合，TPS は $\log_2 11^4 \approx 13.8$ となる．本提案手法はダイヤルパッドやキーボードのような固定入力箇所を持たないため，特徴点列内の各点が指し示す明確な位置あるいはその候補位置は攻撃者にとって入手不可能な情報である．つまり，実質的には N_k の値はより大きいと期待できる．一方，画像内において利用可能な入力箇所の数は視線追跡精度の解像度（r）に依存する．解像度が低ければ，おおざっぱな位置を特徴点として利用することが求められるため，N_k は少なくなり，TPS は低下する．

3.5 想定する適用例

本提案手法の想定する主な認証場面はスマートフォンのロック解除や Windows Hello などの PIN 入力の代替である．本提案手法は，画像を表示する画面と視線を追跡するための機構が存在すれば実現可能であるため，利用デバイスはラップトップ型端末とスマートフォンの両方に適用することが可能である．また，カメラが搭載されたスマートウォッチや AR/VR グラスに対しても適用可能であると考えられる．さらに，視線による入力であるため，物理的接触によるインタラクションを必要とせずユーザの入力を隠すことができることから，公共の場において認証操作をしなければならない場面においても非常に有用であると考えられる．

4. 視線追跡の実装

本研究では，認証時の秘密鍵入力に注視を利用するため，ユーザの視線を追跡する必要がある．本節では，提案する認証手法を評価するために実装したスマートフォン向けとラップトップコンピュータ向けの 2 つの視線追跡実装について紹介する．

4.1 スマートフォンにおける視線追跡の実装

4.1.1 利用したデバイスおよびフレームワーク

今回の視線追跡の実装には，Apple 社の iPhone を利用した．また，iPhone においてフロントカメラからの画像や顔の深度情報といった情報を取得するフレームワークとして ARKit[*6]を用いた．ARKit の動作には，TrueDepth カメラが搭載されたデバイスが必要である．ARKit により，フロントカメラに映り込んだユーザの顔の位置と向き，顔の中における目，鼻，口の位置と向き，目の開き加減といったデータをおよそ 60 frames/s にて収集可能である．このフレームレートはユーザビリティテストにおいて十分な速

[*5] TPS（Theoretical Password Space）は指数関数的に上昇していくため，一般的に対数 $\log_2$ を取って比較される [6].

[*6] https://developer.apple.com/documentation/arkit

度であると報告されている [55]．最近の HCI 研究においても利用されており，HeadReach [56] では，ARKit により認識した頭部の向きをスマートフォンに対する新たな入力として活用し，GazeConduits [57] では，複数のタブレットデバイスに対するマルチデバイスインタラクションを ARKit により実現している．

4.1.2 ARKit を用いた視点追跡

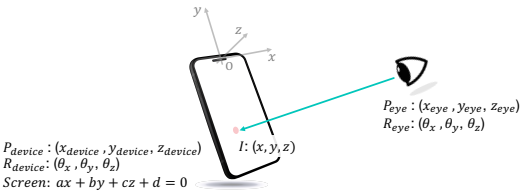


図 5 ARKit の拡張現実空間における視点追跡のイメージ図．それぞれの座標及び回転角は，スマートフォンのカメラの位置を原点とする拡張現実空間の座標系にて表現されており，ARKit の ARAnchor, ARFaceAnchor を通して取得し，座標変換により算出している．

ARKit により取得できるデバイスの位置と角度，および目の位置と角度を利用して，デバイスのスクリーン平面 (デバイスの位置と角度から得られる) と視線ベクトル (目の位置と角度から得られる) の交点を算出し，ユーザの視点を求める．ARKit には，拡張現実空間と呼ばれる概念が存在し，デバイスや顔の位置は，その拡張現実空間の座標系によって表現される．拡張現実空間は，図 5 に示されるようにデバイスのカメラの位置を原点とする座標系である．ARKit はカメラに映り込んだ物体に対して ARAnchor[*7] を設定し，追跡する．特に人については別途 ARFaceAnchor[*8] が設定され，顔に関する情報も追跡される．ARFaceAnchor は，拡張現実空間とは別の座標系である頭の位置を原点とする顔空間座標系を構築し，顔の位置と角度，目の位置と角度，さらには，目の開閉率や眼球の回転角まで取得できる．顔空間座標系において得られた目の位置と角度を，拡張現実空間座標系に変換し，視線ベクトル（P_{eye}，R_{eye}）として利用する．また，デバイスの位置 P_{device} と角度 R_{device} からデバイスのスクリーン平面 $ax + by + cz + d = 0$ を算出する．そして，左右の目それぞれについて，得られた視線ベクトルとデバイスのスクリーン平面の交点を算出する（I_{right}，I_{left}）．I_{right} と I_{left} は僅かに異なるため，その中間にある点を両目の視点位置（I_{center}）として利用する (図 6 左)．ここで得られた視点位置は 3 次元の拡張現実空間座標系上にあるため，図 6 右に示されるスクリーン平面の 2 次元座標系に変換し，出力する（I_{eye}）．この時，I_{eye} は pt 単位で表現される．pt は画面サイズに依存している単位であり，実装に利用した iPhone 11 Pro（画面サイズ 375 pt × 812 pt）においては，1 pt ≃ 0.166 mm である．

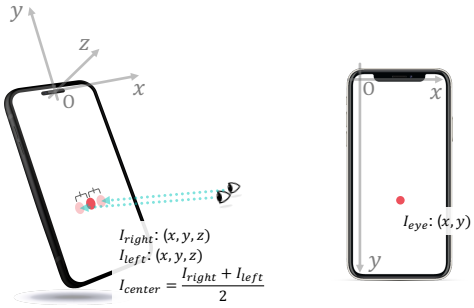


図 6 左）拡張現実空間の 3 次元座標系における視点位置の算出．右）スクリーン平面の 2 次元座標系における視点位置の算出．

4.1.3 キャリブレーションによる補正

ARKit を用いた視線追跡から得られる視線データを評価するために予備実験 [58] を別途実施したところ，視線追跡の真値からのずれは大きいが，各注視毎の追跡結果の分散は小さかった．そのため，ある点を注視していることは検出できると考えられる．ずれに関しては，利用時にキャリブレーションすることで補正を行う．

キャリブレーションは，図 7 において画面内に表示されている青い四隅の丸い点を基準点として行う．ユーザには 4 点をそれぞれ順番に 2 秒間ずつ注視してもらい，それにより得られるデータから計算された視点位置を学習データとして，XY 軸それぞれで回帰を行う．回帰のモデルにはサポートベクタ回帰（SVR）を用いた．実装には，Python のライブラリである scikit-learn[*9] を利用した．回帰によって得られた座標をユーザの視点位置として認証に利用する．

図 7 キャリブレーションに利用する点．画面図内の青い丸 4 点で，左上隅を (0,0)，右下隅を (1,1) としたときに，(0.1,0.1),(0.1,0.9),(0.9,0.1),(0.9,0.9) となる各点である．

4.2 ラップトップコンピュータにおける視線追跡の実装

ラップトップコンピュータにおける視線追跡の実装には，Irisbond 社の開発した商用の視線追跡デバイスである Hiru[*10] を用いた．Hiru は，精度 0.4°，60 Hz にて視線データを収集することができ，キャリブレーション（1 点，5 点，9 点，または 16 点）を必要とする．

[*7] https://developer.apple.com/documentation/arkit/aranchor
[*8] https://developer.apple.com/documentation/arkit/arfaceanchor
[*9] https://scikit-learn.org/
[*10] https://www.irisbond.com/en/products/hiru-the-first-multiplatform-eye-tracker/

Hiru はディスプレイ下部に設置され，PC とは USB により接続する（図 8）．Hiru デバイスと目の距離は推奨距

図 8 Hiru を接続した様子

離である 35 cm–80 cm とした．また，デバイスから視線情報を取得するために IrisbondAPI（C#）を利用した．IrisbondAPI には，視線によるターゲット選択の手法として，一定時間視線を留める事による注視選択，ターゲットを見た状態において瞬きを行うことによる瞬き選択，ターゲットを見た状態においてキーボードにより選択を行う手動選択の 3 種類が用意されており，本実装では注視によるターゲット選択を利用した．注視判定が行われると，注視位置が画面内の 2 次元座標として出力される．出力された注視点を認証システムの入力として利用した．

4.3 視線追跡精度と特徴点数

別途実施した予備実験 [58] の結果では，ARKit を利用した視線追跡システムの二乗平均平方誤差（RMSE） は，画面の縦方向が 62.28 pt（約 10.36mm），横方向が 44.82 pt（約 7.46mm）であった[*11]．この結果から，画面サイズ 812 pt × 375 pt（iPhone 11 Pro）の場合，縦横 13 × 8=104 のグリッド毎に特徴点を配置しても視線入力可能であると考えられる．この場合，TPS は $\log_2 104^4 \approx 26.8$ となる．4 桁の PIN は $\log_2 10^4 \approx 13.3$，4 桁の英数字のパスワードは $\log_2 62^4 \approx 23.8$ であり，同等以上の堅牢性が今回のスマートフォン環境での実装においてもあると考えられる．

Hiru の場合は，精度が 0.4 度であるとされているので，例えば 50cm 離れて画面を見るときの誤差は約 3.5mm であると考えられる．17.3 インチのディスプレイサイズは 382mm × 215mm であるので，109 × 61=6649 のグリッドを配置することができる．TPS は $\log_2 6649^4 \approx 50.8$ となり，さらに堅牢性が高いと考えられる．

また，近年発表された深層学習技術を用いたスマートフォン上で視線追跡を行う手法 [7] では，平均誤差が約 5mm 程度と，PC 向け設置型視線追跡装置に匹敵する程に精度が向上している．この精度であれば，iPhone 11 pro の実画面サイズ 135mm x 62mm の中に，27 × 12=324 のグリッドを配置することができ，TPS は $\log_2 324^4 \approx 33.4$ となる．このような今後の視線追跡精度向上を考慮すれば，本手法はスマートフォンにおいても既存手法の TPS を十分に越えられると考えられる．なお，実利用時の実際のパスワード空間 (Actual Password Space, APS) については，ユーザビリティとの兼ね合いで TPS より狭くなることが考えられる．この点については，7 節において議論する．

[*11] それぞれキャリブレーション前は 252.3pt, 124.5pt.

5. プロトタイプシステムの実装

提案する認証手法を評価するために認証システムのプロトタイプを実装した．実装したプロトタイプは，秘密鍵の登録と，秘密鍵の視線入力によるロック解除を行うことができるアプリケーションである．本節では実装したプロトタイプについて説明した後に，実装で利用した特徴点データ付き画像データセットについて述べる．

5.1 実装環境

プロトタイプは，スマートフォンとラップトップコンピュータとそれぞれにおいて実装した．視線追跡の実装と同様に，スマートフォンは iPhone 11 Pro を利用し，Swift を利用して実装した．ラップトップコンピュータは DELL ALIENWARE（Intel Core i9-10900，GeForce RTX 2080 SUPER，32GB メモリ，17.3 インチディスプレイ），および視線認識のために Hiru を利用している．使用した言語は，C#である．

5.2 認証アルゴリズムの実装

図 9 に，認証アルゴリズムの概要を示す．初めに，ランダムな画像が画面に表示される（P1）．その後，ミダスタッチ問題（操作の意図無く見ているだけなのに操作の注視と検出されてしまうこと）を抑制するために，最初の 1 秒間は注視の検出を行なわず（P2），1 秒後から注視の検出を開始する（C1）．注視が検出されたら，その近くに特徴点があるかをチェックし（C2），もし無ければ再度注視検出を始める（C1）．もし注視点の近くに特徴点があれば（C2），それを記録し（P3），それが秘密鍵内の点と一致するかを判定する（C3）．一致していた場合には，正解のフィードバックとして振動または音を 1 回提示して（P4），秘密鍵の次の特徴点入力のための注視検出待ちとなる（C1）．秘密鍵の全ての特徴点が入力される（C4）と認証成功となる．一方，正しくない特徴点を注視した場合には，不正解のフィードバックとして，振動または音を 2 回提示する（P5）．それまでの特徴点入力は消去され，最初から入力することになる．また，画像を表示してから 10 秒経過すると画像が更新され，最初から入力することになる．ユーザが明示的に画像を更新することもできる．認証失敗回数が 5 回になると，認証に使用できない画像（類似画像でない

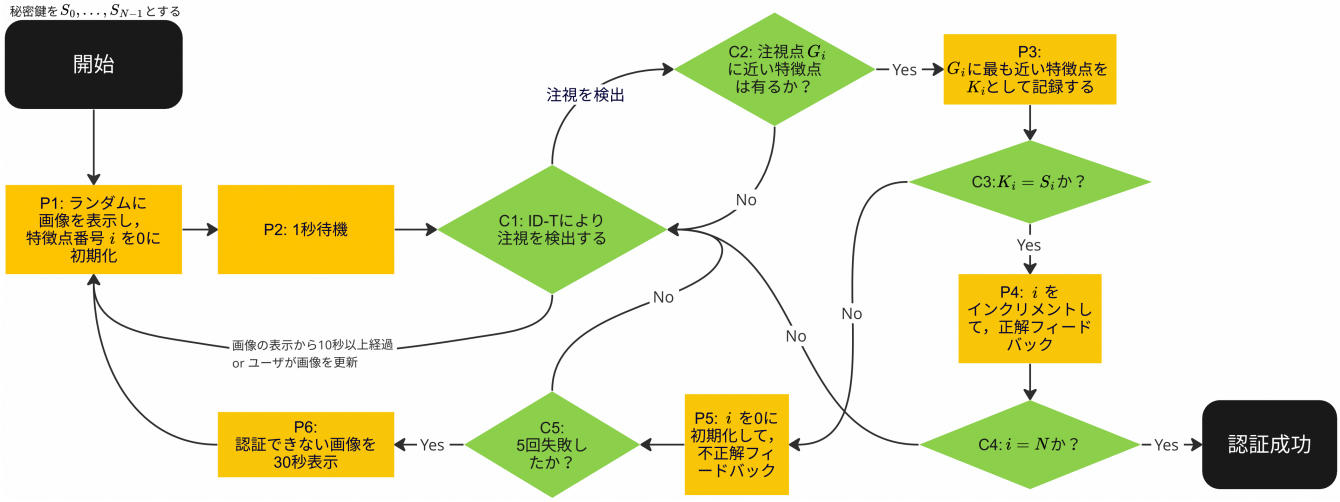


図 9　認証アルゴリズム

画像）が 30 秒間表示される（C5,P6）．

システムが認証を行うためには，ユーザの注視位置に基づいて特徴点を特定する必要がある．ユーザの注視を検出するためには，Dispersion-Threshold Identification (I-DT) アルゴリズム [59] を利用した．ウインドウ幅は $T = 700\,\mathrm{ms}$ とし，標準偏差閾値は th_{gaze}=10 pt と設定した．システムは，I-DT により検出されたユーザの注視点 (G_i) から一定範囲内 ($G_x - d_x \leq K_x \leq G_x + d_x \wedge G_y - d_y \leq K_y \leq G_y + d_y$) に存在する特徴点（$K_i$）を選択する（C2）．ここで，$d_x$ および d_y には，視線追跡の誤差よりも大きい値を指定する．また，複数の特徴点が範囲内に存在する場合には，注視点に最も近い特徴点を選択する（P3）．

なお，スマートフォン環境の視線追跡の誤差としては，各キャリブレーション時に行われる回帰分析計算から得られる二乗平均平方根誤差 (RMSE) を用いた．この値に今回は 5 を足した値を上記の d_x, d_y として用いた．また，ラップトップ環境では，Hiru の SDK によってキャリブレーション後の誤差を得ることができるので，それに 5 を足した値を用いた．

5.3　画像と特徴点データ

本認証システムを実現するためには，共通の特徴点を持つ画像データセットと，各画像内の特徴点の位置情報が必要である．この要件には，画像認識分野において広く利用されている公開画像データセットが該当する．今回は，その中の一つである Animal-Pose Dataset [60] を採用した．このデータセットには，猫，犬，馬，羊，牛の画像が 6000 枚以上収録されており，9 種類（左右の目, 喉, 鼻, 鬐甲 (withers), 左右の耳の付け根 (earbases), 尻尾の付け根 (tailbase), 4 つの肘 (elbows), 4 つの膝 (knees), 4 つの足 (paws)）の位置が記録されている．これらの特徴点の中でも，4 つの肘と 4 つの膝は，他の点との距離が近すぎることが多いので使用せず，7 種類の特徴（計 12 点）を利用した．図 10 は Animal-Pose Dataset に含まれる画像と特徴点例である．画像内の線で結ばれている青色の各頂点が特徴点である．なお，これらの線や点は認証時のスマートフォンの画面には表示されず，画面上には写真画像が表示されているだけである．

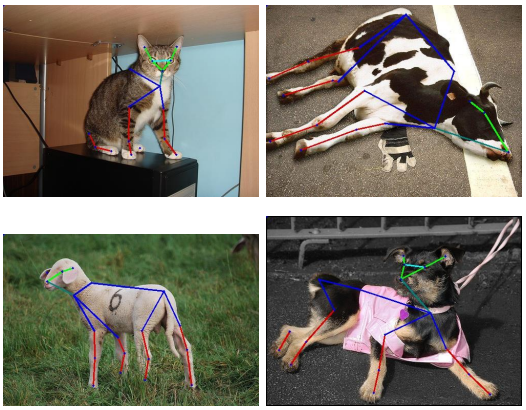


図 10　Animal-Pose Dataset に含まれる画像と特徴点例（画像は元論文 [60] を引用）．

6.　提案手法の予備的評価

本節では，提案手法の予備的評価について述べる．実験参加者数が限られているため，実験参加者の属性に偏りがあり，結果に対して個人差の影響がある可能性があるが，提案手法の実現可能性についての参考にはなると考えられるため紹介する．

6.1　スマートフォンにおける認証システムの評価

スマートフォン上に実装したプロトタイプを用いて提案手法の実現可能性を調査するための実験を行なった．

実験参加者は，5 名（P1–P5，21–22 歳，平均年齢 21.4 歳，男性 3 人女性 2 名）であり，普段からスマートフォン

を使用している著者の所属する研究室内から集めた大学院生・大学生であった．全員が視線入力の経験があった．参加者の内 3 名がコンタクトレンズを着用しており，残り 2 名が裸眼であった．実験は屋内の明るい蛍光灯下にて行われた．使用したデバイスは，iPhone 11 Pro である．参加者は，椅子に座り，図 15 のように顎を台の上に載せて顔の位置を固定した状態で実験に参加した．スマートフォンは，ユーザが普通にスマートフォンを手に持つ位置（顔から 30〜40cm 程度）で，かつ顔がスマートフォンのインカメラ画像に良く写るような向きで三脚に固定した．

参加者のタスクは，秘密鍵登録と秘密鍵の視線入力によるロック解除である．秘密鍵登録では，参加者は画像内に表示された特徴点から 4 点をタッチ入力により選択し，その順番と合わせて秘密鍵として登録した．ロック解除では，参加者はランダムに表示される画像に対して，登録した秘密鍵 (特徴点列) 内の各点を順に注視する．ロック解除では，認証失敗した場合，成功するまでリトライする．秘密鍵登録とロック解除を合わせて 1 タスクとし，1 セット=5 タスクを計 4 セット行う．それぞれのセットの初めに，参加者はキャリブレーションを行った．実験の結果，$5_{\text{回}} \times 4_{\text{セット}} \times 5_{\text{人}} = 100_{\text{タスク}}$ のデータを得た．

最大 6 回のリトライが必要であったが，参加者は全タスクで認証成功することができた．リトライせずに初回の試行で認証が成功した割合は，86.0%であった．各タスクにおいて認証成功となるまでに実行した秘密鍵入力試行回数を図 11 に示す．1 回で認証成功の場合と，1 回失敗+2 回目で成功の場合を合わせた割合は 95%であった．

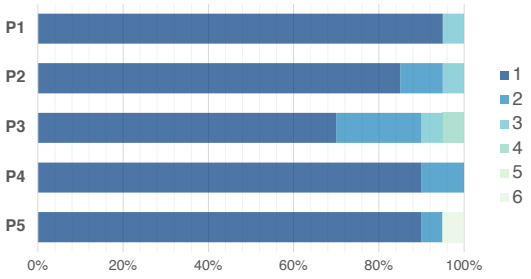


図 11 1 回の認証成功にかかった試行回数の割合（スマートフォン）．各色の番号は何回目の試行で認証成功したかを表している．P1〜P5 は実験参加者．

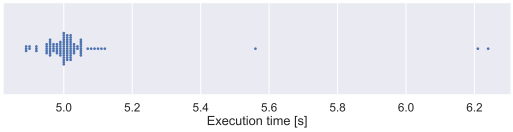


図 12 認証試行 1 回にかかった実行時間の分布（スマートフォン）．外れ値は瞬きや視線のブレにより注視検出に時間がかかってしまった場合である．

認証の平均実行時間は，5.03 s（SD=0.186 s）であった．認証の実行時間は，非常に狭い範囲に分布していた（図 12）．これは実行毎の違いや実行者の違いによる実行時間の差が少ないことを示している．我々が別に行った異なる特徴点数の秘密鍵を登録および入力する予備実験 [58] においては，認証の実行時間はシステムが注視を検出するのに必要な一定時間と特徴点の数の積におおよそ従っていた．本実験の結果もほぼその結果に従っていた．

6.2 ラップトップコンピュータにおける認証システムの評価

スマートフォンより大きな画面かつ精度の高い視線追跡装置を用いた場合の提案手法の実現可能性を調査するための実験を行なった．

実験参加者は，3 名（P1–P3，21–22 歳，平均年齢 21.3 歳，男性 2 人女性 1 名）であった．全員，著者の所属する研究室外から集めた大学生で，視線入力の経験は無かった．参加者の内 2 名がコンタクトレンズを着用していて，残り 1 名は裸眼であった．実験は屋内の明るい蛍光灯下において行った．使用したラップトップコンピュータは，DELL Alienware (17.3 インチディスプレイ)，および視線追跡デバイスの Hiru を利用した．参加者は，椅子に座り，実験に参加した．参加者のタスクは，スマートフォンの場合と同じである．各参加者は，秘密鍵登録とロック解除を，長さ 4 の特徴点列を秘密鍵として，5 回× 4 セット行った．ロック解除では，成功するまでリトライした．各セットの最初にキャリブレーションを行った．実験の結果，$5_{\text{回}} \times 4_{\text{セット}} \times 3_{\text{人}} = 60_{\text{タスク}}$ のデータを得た．

初回の試行で認証が成功した割合は 96.7%であった．認証成功となるまでに実行した秘密鍵入力試行回数を図 13 に示す．全体として 1 回のリトライで，つまり高々 1 回の失敗で 2 回目までに，100%の認証が成功となった．スマートフォンにおける実行と比較して，初回で認証が成功した割合，認証成功するまでの試行回数の観点で良い結果であったが，これは，画面がより広く画像内の特徴点同士の距離が遠かった (視角が大きかった) こと，またより精度の高い視線追跡装置を用いたことによって，特徴点の選択が正確になったためと考えられる．

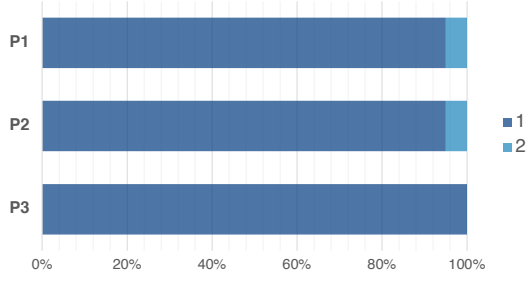


図 13 1 回の認証成功にかかった試行回数の割合（ラップトップコンピュータ）．各色の番号は何回目の試行で認証成功したかを表している．P1〜P3 は実験参加者．

しかし，実行時間はラップトップコンピュータの方がやや長い結果となった（平均実行時間 5.37 s（SD=0.12 s））．原因として特徴点の探索時間及び視線移動の時間が影響していると考えられる．これらは画像のサイズに依存しているため，画面に表示する画像のサイズを調整することにより改善できる可能性がある．ただし，特徴点の選択の正確性にも関わっているため，複数の画像サイズにおいて比較検証していく必要がある．

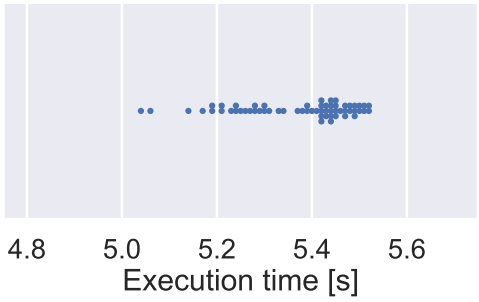


図 14 認証試行 1 回にかかった実行時間の分布（ラップトップコンピュータ）

6.3 攻撃実験

6.3.1 参加者，タスク，手順

提案手法の他者からの攻撃に対する堅牢性を調査するために実験を行なった．実験参加者は，5 名（P1–P5，21–22 歳，平均年齢 21.4 歳，男性 3 人女性 2 名）であった．全員，著者の所属する研究室外から集めた大学生で，視線入力の経験は無かった．これまでに述べた実験参加者との重なりはない．参加者の内 3 名がコンタクトレンズを着用していて，残り 2 名が裸眼であった．実験は屋内の明るい蛍光灯下において行なった．使用したデバイスは，iPhone 11 Pro である．

本実験では，秘密鍵を視線入力しているユーザの目の動きの映像を攻撃に利用する．これらの映像は，事前に行った予備実験 [58] 及び 6.1 節の評価実験において，参加者の正面，顔の高さに設置されたカメラにより撮影した（図 15）．収集したビデオは，181 回の秘密鍵入力試行である．予備実験のビデオには秘密鍵の特徴点数が 1，2，3 の場合があり，6.1 節の実験のビデオは特徴点数が 4 の場合である．実験時には，秘密鍵に含まれる特徴点の数ごとにランダムに抽出して利用した．

参加者のタスクは，ランダム攻撃，秘密鍵再現，および観察攻撃である．ランダム攻撃タスクでは，参加者は推測のみによりロック解除を秘密鍵毎に 5 回試みる．この時，参加者は事前に認証手法について説明され理解しているが，その他の情報は与えられない．攻撃は視線入力で行う．ランダム攻撃時に提示される画像は他の攻撃時に使われる画像とは異なる画像を用いた．図 9 の認証アルゴリズムを用いるので，入力失敗時やタイムアウト時には画像は変更される．

秘密鍵再現タスクは，秘密鍵入力者の目の動きから入力している秘密鍵が再現できるかを調査することが目的である．そのために，秘密鍵入力者の正面映像を見て，秘密鍵をタッチ入力で再現してもらう．この時，参加者は映像を何度でも見ることができる．また，解読のためにノート等の道具を使うことも許可した．動画内の秘密鍵入力者が見ている画像と攻撃者が見ている画像は同じである．また，画像はこの攻撃中は途中で変更されない．

観察攻撃タスクでは，秘密鍵入力中の目の動きから入力している秘密鍵を解読し，認証を突破することが可能であるかを調査することが目的である．そのために，秘密鍵入力者の正面映像を見て，ロック解除を 5 回まで試みてもらう．この時，秘密鍵再現タスクと同様に，映像は何度でも見ることができ，ノート等の使用を許可した．秘密鍵再現タスクと同様に最初は動画内の入力者と同じ画像が表示される．しかし，観察攻撃タスクでは実際の認証アルゴリズムを利用するので，失敗やタイムアウト時には画像が変更される．

上記 3 つのタスクをシークレットに含まれる特徴点の数（1〜4）毎に 1 回ずつ実行することを 1 セットとし，4 セット行う．ランダム攻撃タスクと観察攻撃タスクの初めに，参加者はキャリブレーションを行った．また，攻撃毎にその攻撃はどれほどの確信を持って行なったかを表す確信度（1：自信なし〜5：自信あり）を参加者に質問した．

ランダム攻撃タスクは事前情報なしでの攻撃であるが，3.4 節に記載した攻撃者 A（ショルダサーフィン）に対応するとも考えられる．視線入力の場合，ショルダサーフィンだけでは入力操作に関する情報は得られないため，事前情報無しで攻撃を試みるのと同様と考えられる．

一方，秘密鍵再現タスクと観察攻撃タスクは，どちらも 3.4 節に記載した攻撃者 B に対応するタスクである．秘密鍵再現タスクは秘密鍵の推測可能性をより直接的に調査することを目的とし，観察攻撃タスクはより実運用場面に近い状況を想定して認証を突破できるかどうかを調査することを目的としている．

6.3.2 結果

実験の結果，ランダム攻撃は $16_{\text{秘密鍵}} \times 5_{\text{回}} \times 5_{\text{人}} = 400_{\text{回}}$ の攻撃，秘密鍵再現は $16_{\text{秘密鍵}} \times 5_{\text{人}} = 80_{\text{回}}$ の再現，観察攻撃は $16_{\text{秘密鍵}} \times 5_{\text{回}} \times 5_{\text{人}} = 400_{\text{回}}$ の攻撃が行われた．全ての攻撃の結果を表 1 に示す．

実験後に参加者から以下のコメントを得た．

- 難しすぎる
- 目の動きだけだと，どこから認証が始まっているのかわからない
- なんとなく上から下（右から左）に視線を動かしていることはわかりそうだったが，結局どの点を見ているかわからなかった

図 15　攻撃時に見ることのできる認証実行時の様子のビデオ例.

表 1　攻撃実験全体の結果

	突破率/成功率	突破回数/成功回数	確信度の平均
ランダム攻撃	1.00%	4	-
秘密鍵再現	2.50%	2	1.18 (SD = 0.41)
観察攻撃	2.25%	9	1.11 (SD = 0.32)

- 非常に疲れた

また，試行回数，特徴点の数，攻撃者ごとの突破率・突破回数・確信度を付録の表 A·1–A·11 に示す．ランダム攻撃，秘密鍵再現，観察攻撃全てにおいて，秘密鍵に含まれる特徴点の数が 1 点の時にのみ突破されており，2 点以上の秘密鍵においては一度も突破されることはなかった．また，秘密鍵再現，観察攻撃の確信度については非常に小さな値となっており，攻撃者は提案手法に対して確信を持った攻撃ができなかったことがわかる．

特徴点ごとに突破された回数を図 16 に示す．この中では，右前足や背，尾の特長点が多く突破されていることが確認できる．実際に突破された秘密鍵について内容を確認したところ，特定の秘密鍵入力者が行った 1 回の試行に関して 4 回攻撃が突破されていたことがわかった．

7.　議論と今後の課題

本節では，プロトタイプシステムの実装，予備的評価を通して明らかになった事項について議論し，今後の課題について述べる．

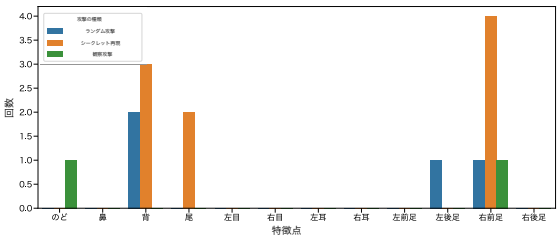


図 16　攻撃され突破された特徴点

7.1　誤認識と誤入力

予備的評価の結果，初回試行で認証が成功した割合は，スマートフォンで 86.0%，ラップトップで 96.7%であった．Microsoft の認証システムの一つである Windows Hello の本人受入率の要件は 95%（理論値，実測においては 90%）以上である [*12] ことが求められているため，特にスマートフォン環境の実装については成功率を向上させる必要がある．認証が成功しなかった場合の原因としては，システム側の誤認識とユーザの誤入力があることが確認された．ユーザが正しく特徴点を見ているにもかかわらず，システムが異なる特徴点を検出してしまう誤認識は，主に視線追跡精度によるものだと考えられる．特に，視線追跡の誤差よりも短い距離に特徴点が存在する場合には，システムが間違った特徴点を検出してしまう可能性が高い．これを防ぐためには，以下の対策が考えられる．

- 深層学習ベースの視線追跡実装などを用いて視線追跡精度を向上させる
- 秘密鍵登録時に近すぎる特徴点を選択できないように候補から削除する
- 秘密鍵の視線入力時に，秘密鍵に含まれる特徴点と距離が近い特徴点を含む画像を表示させないようにする

また，ユーザの視線の振る舞いにより，凝視が検出されなかったり，二重に検出されたりしていた．より頑健な注視検出アルゴリズムを探求する必要がある．

ユーザが秘密鍵に登録した特徴点ではない特徴点を入力してしまう誤入力は，ユーザが秘密鍵を間違えて記憶してしまうことが原因として挙げられる．特に，右足と左足など左右を間違えた特徴点の入力が散見された．このような左右の要因を持つ特徴点は類似画像が鏡像反転した向きの時に間違えやすい．また，秘密鍵を登録する際に左右を混同してしまうといった参加者のコメントもあった．これらの誤入力を軽減するためには，左右の要因を持つ特徴点の場合，左右どちらを入力しても可とすることが考えられるが，画像内の実質的な特徴点数が減り過ぎないようにする必要がある．そのためには，左右の要因を持たない画像群，例えば多数の物体が画像中に存在するような画像群を利用

[*12] https://docs.microsoft.com/ja-jp/windows/security/identity-protection/hello-for-business/hello-biometrics-in-enterprise

し，物体自体を特徴点とすることなどが考えられる．近年の深層学習技術を用いた画像生成手法を用いることで，これらの性質を持つ画像群の生成は比較的容易に可能であると考えられる．

なお，今回のスマートフォン環境の評価実験では顔とスマートフォンを固定した状態で実験を行ったが，これは現在の ARKit による実装では顔の正面画像がうまく撮れないと視線追跡精度が低下するためである．固定せずに，例えばユーザが水平に近い持ち方をする場合，下方からの撮影となり，うまく顔が入らない場合がある．また，スマートフォンを実利用する場面では，歩行時のブレや屋外の逆光など，顔画像がうまく撮影できない状況が想定され，その場合はやはり視線追跡は困難になる．より自由な持ち方と多様な場面での利用を可能にするためには，深層学習等の技術を活用して，よりロバストな視線検出手法を開発して実装に利用する必要がある．

また，今回の実験ではセット毎にキャリブレーションを行った．スマートフォン環境の場合，4.1.3 節の予備実験 [58] においては，キャリブレーションによって誤差は 1/3〜1/4 程度になっていた．実利用の場面においてもキャリブレーションするのであれば，秘密鍵の特徴点列を注視する前に固定の 4 点を追加で注視する必要がある．スマートフォン環境におけるキャリブレーションは全体的なずれを補正するものであるため，特徴点列内の各点の絶対位置ではなく注視位置を結ぶ軌跡のパターンマッチによる認証を行うことで，キャリブレーションの必要性は下がると期待されるが，堅牢性は下がる可能性がある．

7.2 認証の実行時間と堅牢性

認証は情報端末を利用するたびに行うプロセスであり，実行時間は短いことが望ましい．予備実験及び評価実験の結果から，認証時間は秘密鍵に含まれる特徴点の数に影響を受けることが示唆された．そのため，秘密鍵に含まれる特徴点の数を少なくすることにより，認証の実行時間を短くすることが可能となる．一方，少なすぎる特徴点数は他者からの攻撃に対する堅牢性を損なう恐れがある．6.3 節に示したように，特徴点を 1 点だけ含む秘密鍵の場合，無作為に攻撃したときに突破されてしまう可能性が存在する．しかし，2 点以上の場合，計 300 回の攻撃に対しても一度の突破されることがなかったため，秘密鍵に含める特徴点の数は 2 点以上で安全になる可能性がある．ただし，今回の攻撃実験は参加者が 5 人であったため，より大人数の実験により堅牢性を確かめる必要がある．

7.3 他者からの攻撃に対する堅牢性

前節でも述べたように秘密鍵に含まれる特徴点の数が 2 点以上であれば，無作為に攻撃された場合にも，認証しているときの目線を観察された場合にも非常に安全性が高いことが示唆された．また，突破された秘密鍵を確認してみたところ，特定の実行者が特定の特徴点を注視していたときに認証が突破されていたことがわかった．同じ実行者の別の秘密鍵に関しては突破されていなかったため，実行者の注視の仕方により秘密鍵が解読されやすくなる可能性がある．突破された回数が非常に少なく，サンプル数が十分ではないため注視の仕方による解読されやすさを調査する実験を別途実施する必要がある．

今回の認証手法では秘密鍵の特徴点数が固定ではなく，また，秘密鍵の入力終了は明示しない．そのため，例えば，攻撃者が秘密鍵の長さを 3 点だと考えて入力しようとした時に，秘密鍵の長さがそれより短かった場合，最初の 1 点，もしくは 2 点が一致すると，その時点で認証が突破されてしまう．この問題に対処するためにはタイムアウトや特定箇所注視により入力終了を明示することが考えられる．こうすると，秘密鍵に含まれる特徴点の数も入力に含めることができるため認証システムの堅牢性は高まる．一方で，秘密鍵入力に追加の待ち時間等が発生してしまうため，認証時間を伸ばしてしまう要因となる．十分な長さの特徴点数に固定するなども合わせて，必要な堅牢度に応じた検討をする必要がある．

7.4 画像と特徴点

今回作成したプロトタイプ認証システムでは，動物の画像を集めた公開データセットである Animal-Pose Dataset を利用した．しかし，本提案手法はデータセット外の類似画像であっても，その画像内の特徴点位置が取得できれば適用可能である．そのため，ユーザ自前の画像も入力用の画像として利用することが可能である．例えば，ユーザが撮影した自分のペットの画像や，家族写真といった画像に対して，画像の特徴抽出手法 [60], [61], [62], [63], [64], [65] を利用することにより，特徴点の位置を算出し，利用することができると考えられる．ユーザ自前の写真を利用できるようにすることは，本認証手法に関するユーザ体験 (UX) の質を大幅に高められると期待できる．しかし，十分な枚数の写真が用意できなかったり，適度に離れた十分な数の特徴点を含んでいなければ，注視位置が固定的になる恐れがあり，堅牢度の低下につながる恐れがある．十分な画像セットを用意できない場合は，近年の画像生成技術の適用による画像セットの拡張などを検討する必要がある．

堅牢性は 4.3 節で議論した視線追跡精度と画面サイズから決まる配置可能特徴点数を，いかに有効に活用できるかにかかっている．今回の実験で利用した Animal-Pose Dataset では画像中の動物がほぼ 1 匹であった．そのため，指定可能な特徴点数は視線精度に関わらず動物 1 体の特徴点数 (今回は 7 種類 12 点) に限られてしまう．すると，TPS は秘密鍵の長さが 4 の場合，$\log_2 12^4 \approx 14.3$ となり，同じ長さの PIN よりは良いが，さらに堅牢性を高めるに

は，より指定可能特徴点数が多い方が望ましい．この問題に対処するためには，例えば，複数の動物を表示する，異なる種類の物体 (花や葉など植物，自動車や家など人工物) も含まれる画像を用いるなど，より細かい絵柄の画像を用いることで，指定可能特徴点数を増やすことができる．また，「ある特徴点から右に一定距離ずらしたところ」，「特徴点 A と特徴点 B の中央」といった場所を追加することにより，画像内の任意の場所を意味のある特徴点として追加できる可能性がある．これらの「特徴」の追加は秘密鍵を複雑にし，さらに堅牢性を高める可能性があるが，一方でユーザの秘密鍵の記憶性や，入力容易性を損なう恐れがある．7.1 節で議論したように，画像パスワード特有の間違えやすさも考慮しなければならない．堅牢性とユーザビリティを両立させるためには，どのような画像データセットを用意あるいは生成すれば良いかを参加者実験を通して調査することは，今後の課題である．

8. 結論

本論文では，画像内の特徴点列を秘密鍵として，それを視線入力する新たな認証手法を提案した．ユーザは，画像内における特徴点を注視する順番を秘密鍵として登録し，ランダムに表示される類似画像に対して，登録した秘密鍵に従って対応する特徴点を注視することにより認証を受ける．また，本研究では、スマートフォン及びラップトップコンピュータ上にこの認証手法のプロトタイプシステムを実装し，提案した認証手法の予備的評価を行なった．その結果，スマートフォン・ラップトップコンピュータそれぞれにおいて，試行 1 回での認証成功率が 86.0%，96.7%（1 回までの再試行を許容した時に，95.0%，100.0%）であることが示された．また，認証の平均実行時間は，秘密鍵に含む特徴点数が 4 点の時に，スマートフォンにおいて 5.03 s（SD = 0.186 s），ラップトップコンピュータにおいて 5.37 s（SD = 0.120 s）であった．また，攻撃実験では，無作為な攻撃，および認証実行時のユーザの目の動きを観察しての攻撃のどちらにおいても，秘密鍵に含まれる特徴点の数が 1 点の時にはごく少数回突破されたが，2 点以上の時には一度も突破されなかった．このことから，秘密鍵が含む特徴点の数を 2 点以上の小さな値にすることで短時間かつ堅牢な認証を実現できると考えられる．

今後の課題として，スマートフォンにおける実装では視線追跡精度を要因とする誤認識に対応する必要がある．また，誤入力への対処として，画像の特徴の左右混同を軽減する対処が必要である．これらは画像や特徴点の種類，特徴点の数，各種パラメータを変更することにより改善されうるが，認証システムの堅牢性とトレードオフとなる項目も存在するため，より大人数での参加者実験を行い実行容易性とともに安全性を今後調査する必要がある．また，ユーザ保有の画像の利用や動画の利用，深層学習技術の応用による特徴点を含む画像の自動生成，大画面ディスプレイへの適用といった応用的な認証システムの実装及びそれらの堅牢性調査については今後行っていく必要がある．

参考文献

[1] Hintze, D., Hintze, P., Findling, R. D. and Mayrhofer, R.: A Large-Scale, Long-Term Analysis of Mobile Device Usage Characteristics, *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, Vol. 1, No. 2, pp. 1–21 (online), DOI: 10.1145/3090078 (2017).

[2] De Angeli, A., Coventry, L., Johnson, G. and Renaud, K.: Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems, *International Journal of Human-Computer Studies*, Vol. 63, No. 1-2, pp. 128–152 (online), DOI: 10.1016/j.ijhcs.2005.04.020 (2005).

[3] Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A. and Memon, N.: PassPoints: design and longitudinal evaluation of a graphical password system, *International Journal of Human-Computer Studies*, Vol. 63, No. 1-2, pp. 102–127 (online), DOI: 10.1016/j.ijhcs.2005.04.010 (2005).

[4] Moncur, W. and Leplâtre, G.: Pictures at the ATM: exploring the usability of multiple graphical passwords, *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, New York, NY, USA, Association for Computing Machinery, pp. 887–894 (online), DOI: 10.1145/1240624.1240758 (2007).

[5] Everitt, K. M., Bragin, T., Fogarty, J. and Kohno, T.: A comprehensive study of frequency, interference, and training of multiple graphical passwords, *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, New York, NY, USA, Association for Computing Machinery, pp. 889–898 (online), DOI: 10.1145/1518701.1518837 (2009).

[6] Bulling, A., Alt, F. and Schmidt, A.: Increasing the security of gaze-based cued-recall graphical passwords using saliency masks, *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, New York, NY, USA, Association for Computing Machinery, pp. 3011–3020 (online), DOI: 10.1145/2207676.2208712 (2012).

[7] Valliappan, N., Dai, N., Steinberg, E., He, J., Rogers, K., Ramachandran, V., Xu, P., Shojaeizadeh, M., Guo, L., Kohlhoff, K. and Navalpakkam, V.: Accelerating eye movement research via accurate and affordable smartphone eye tracking, *Nature Communications*, Vol. 11, No. 1, p. 4553 (online), DOI: 10.1038/s41467-020-18360-5 (2020).

[8] De Luca, A., Weiss, R. and Drewes, H.: Evaluation of eye-gaze interaction methods for security enhanced PIN-entry, *Proceedings of the 19th Australasian conference on Computer-Human Interaction: Entertaining User Interfaces*, New York, NY, USA, Association for Computing Machinery, pp. 199–202 (online), DOI: 10.1145/1324892.1324932 (2007).

[9] Findling, R. D., Nguyen, L. N. and Sigg, S.: Closed-Eye Gaze Gestures: Detection and Recognition of Closed-Eye Movements with Cameras in Smart Glasses, *Advances in Computational Intelligence*, Cham, Switzerland, Springer International Publishing, pp. 322–334 (online), DOI: 10.1007/978-3-030-20521-8_27 (2019).

[10] Friström, E., Lius, E., Ulmanen, N., Hietala, P.,

Kärkkäinen, P., Mäkinen, T., Sigg, S. and Findling, R. D.: Free-Form Gaze Passwords from Cameras Embedded in Smart Glasses, *Proceedings of the 17th International Conference on Advances in Mobile Computing & Multimedia*, New York, NY, USA, Association for Computing Machinery, pp. 136–144 (online), DOI: 10.1145/3365921.3365928 (2019).

[11] Katsini, C., Abdrabou, Y., Raptis, G. E., Khamis, M. and Alt, F.: The Role of Eye Gaze in Security and Privacy Applications: Survey and Future HCI Research Directions, *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA, Association for Computing Machinery, pp. 1–21 (online), DOI: 10.1145/3313831.3376840 (2020).

[12] Yamato, Y. and Takahashi, S.: Gaze-Based Authentication Method Using Graphical Passwords Featuring Keypoints, *OzCHI 2021: 33rd Australian Conference on Human-Computer-Interaction*, pp. 273–279 (2021). Late-Breaking Work.

[13] Kuckertz, A.: Strategies of Competition in the Bank Card Business, *Technovation*, Vol. 26, No. 7, p. 820 (online), DOI: 10.1016/j.technovation.2005.12.002 (2006).

[14] Agrawal, H.: How Hackers Hack Your Accounts Password & Ways To Avoid Being Hacked, https://shoutmetech.com/how-hackers-hack/ (2020). Accessed: 2022-1-6.

[15] Hang, A., De Luca, A., Smith, M., Richter, M. and Hussmann, H.: Where have you been? using location-based security questions for fallback authentication, *Proceedings of the 11th Symposium On Usable Privacy and Security (SOUPS 2015)*, Ottawa, USENIX Association, pp. 169–183 (2015).

[16] Thorpe, J., MacRae, B. and Salehi-Abari, A.: Usability and security evaluation of GeoPass: a geographic location-password scheme, *Proceedings of the Ninth Symposium on Usable Privacy and Security*, No. Article 14, New York, NY, USA, Association for Computing Machinery, pp. 1–14 (online), DOI: 10.1145/2501604.2501618 (2013).

[17] Shone, N., Dobbins, C., Hurst, W. and Shi, Q.: Digital Memories Based Mobile User Authentication for IoT, *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, Institute of Electrical and Electronics Engineers, pp. 1796–1802 (online), DOI: 10.1109/CIT/IUCC/DASC/PICOM.2015.270 (2015).

[18] Gupta, P., Wee, T. K., Ramasubbu, N., Lo, D., Gao, D. and Balan, R. K.: HuMan: Creating memorable fingerprints of mobile users, *2012 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, Institute of Electrical and Electronics Engineers, pp. 479–482 (2012).

[19] Sandström, M.: Liveness Detection in Fingerprint Recognition Systems, PhD Thesis, Linköping University, Linköping Sweden (2004).

[20] Apple, Inc.: Face ID - Apple, https://support.apple.com/en-us/HT208108 (2021). Accessed: 2022-1-11.

[21] Samsung Electronics Co. Ltd.: How does the iris scanner work on Galaxy S9, Galaxy S9+, and Galaxy Note9?, https://www.samsung.com/global/galaxy/what-is/iris-scanning/ (2021). Accessed: 2022-1-11.

[22] Sepasian, M., Mares, C. and Balachandran, W.: Liveness and spoofing in fingerprint identification: issues and challenges, *Proceedings of the 4th WSEAS international conference on Computer engineering and applications*, Stevens Point, Wisconsin, USA, World Scientific and Engineering Academy and Society (WSEAS), pp. 150–158 (2010).

[23] Yuan, C., Sun, X. and Wu, Q. M.: Difference co-occurrence matrix using BP neural network for fingerprint liveness detection, *Soft Computing*, Vol. 23, No. 13, pp. 5157–5169 (online), DOI: 10.1007/s00500-018-3182-1 (2019).

[24] Xia, Z., Yuan, C., Lv, R., Sun, X., Xiong, N. N. and Shi, Y.-Q.: A Novel Weber Local Binary Descriptor for Fingerprint Liveness Detection, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, Vol. 50, No. 4, pp. 1526–1536 (online), DOI: 10.1109/TSMC.2018.2874281 (2020).

[25] Ali Fahmi, P. N., Kodirov, E., Choi, D.-J., Lee, G.-S., Mohd Fikri Azli, A. and Sayeed, S.: Implicit authentication based on ear shape biometrics using smartphone camera during a call, *2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Institute of Electrical and Electronics Engineers, pp. 2272–2276 (online), DOI: 10.1109/ICSMC.2012.6378079 (2012).

[26] Martinovic, I., Rasmussen, K., Roeschlin, M. and Tsudik, G.: Authentication using pulse-response biometrics, *Communications of the ACM*, Vol. 60, No. 2, pp. 108–115 (online), DOI: 10.1145/3023359 (2017).

[27] Zhang, X., Yao, L., Kanhere, S. S., Liu, Y., Gu, T. and Chen, K.: MindID: Person Identification from Brain Waves through Attention-based Recurrent Neural Network, *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, Vol. 2, No. 3, pp. 1–23 (online), DOI: 10.1145/3264959 (2018).

[28] Zheng, N., Bai, K., Huang, H. and Wang, H.: You Are How You Touch: User Verification on Smartphones via Tapping Behaviors, *2014 IEEE 22nd International Conference on Network Protocols*, Institute of Electrical and Electronics Engineers, pp. 221–232 (online), DOI: 10.1109/ICNP.2014.43 (2014).

[29] Chen, Y., Sun, J., Zhang, R. and Zhang, Y.: Your song your way: Rhythm-based two-factor authentication for multi-touch mobile devices, *2015 IEEE Conference on Computer Communications (INFOCOM)*, Institute of Electrical and Electronics Engineers, pp. 2686–2694 (online), DOI: 10.1109/INFOCOM.2015.7218660 (2015).

[30] Sun, J., Zhang, R., Zhang, J. and Zhang, Y.: TouchIn: Sightless two-factor authentication on multi-touch mobile devices, *2014 IEEE Conference on Communications and Network Security*, Institute of Electrical and Electronics Engineers, pp. 436–444 (online), DOI: 10.1109/CNS.2014.6997513 (2014).

[31] Dandapat, S. K., Pradhan, S., Mitra, B., Roy Choudhury, R. and Ganguly, N.: ActivPass: Your Daily Activity is Your Password, *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, New York, NY, USA, Association for Computing Machinery, pp. 2325–2334 (online), DOI: 10.1145/2702123.2702457 (2015).

[32] Bo, C., Zhang, L., Li, X.-Y., Huang, Q. and Wang, Y.: SilentSense: silent user identification via touch and movement behavioral biometrics, *Proceedings of the 19th annual international conference on Mobile computing & networking*, New York, NY, USA, Association for Computing Machinery, pp. 187–190 (online), DOI: 10.1145/2500423.2504572 (2013).

[33] Neverova, N., Wolf, C., Lacey, G., Fridman, L., Chandra, D., Barbello, B. and Taylor, G.: Learning Human Identity From Motion Patterns, *IEEE Access*, Vol. 4, pp. 1810–1820 (online), DOI: 10.1109/ACCESS.2016.2557846 (2016).

[34] Kumar, R., Phoha, V. V. and Raina, R.: Authenticating users through their arm movement patterns, Vol. abs/1603.02211, Cornell University, pp. 1–25 (2016).

[35] Yang, J., Li, Y. and Xie, M.: MotionAuth: Motion-based authentication for wrist worn smart devices, *2015 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, Institute of Electrical and Electronics Engineers, pp. 550–555 (online), DOI: 10.1109/PERCOMW.2015.7134097 (2015).

[36] Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J. and Seamons, K.: A Usability Study of Five Two-Factor Authentication Methods, *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security*, SOUPS'19, USA, USENIX Association, p. 357–370 (2019).

[37] Biddle, R., Chiasson, S. and Van Oorschot, P. C.: Graphical Passwords: Learning from the First Twelve Years, *ACM Computing Surveys*, Vol. 44, No. 4 (online), DOI: 10.1145/2333112.2333114 (2012).

[38] 兼子拓弥，本部栄成，高橋健太，西垣正勝：計算機援用ユーザ認証，情報処理学会論文誌， Vol. 55, No. 9, pp. 2072–2080 (2014).

[39] Uellenbeck, S., Dürmuth, M., Wolf, C. and Holz, T.: Quantifying the Security of Graphical Passwords: The Case of Android Unlock Patterns, *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, CCS '13, New York, NY, USA, Association for Computing Machinery, p. 161–172 (online), DOI: 10.1145/2508859.2516700 (2013).

[40] Brostoff, S. and Sasse, M. A.: Are Passfaces More Usable Than Passwords? A Field Trial Investigation, *People and Computers XIV — Usability or Else!*, Springer London, pp. 405–424 (online), DOI: 10.1007/978-1-4471-0515-2_27 (2000).

[41] Jansen, W., Gavrila, S., Korolev, V., Ayers, R. and Swanstrom, R.: Picture Password: A Visual Login Technique for Mobile Devices, Technical Report 7030, National Institute of Standards and Technology Interagency Report, Gaithersburg, MD (2003).

[42] Eljetlawi, A. M. and Ithnin, N.: Graphical Password: Prototype Usability Survey, *2008 International Conference on Advanced Computer Theory and Engineering*, Institute of Electrical and Electronics Engineers, pp. 351–355 (online), DOI: 10.1109/ICACTE.2008.34 (2008).

[43] Davis, D., Monrose, F. and Reiter, M.: On User Choice in Graphical Password Schemes, *Proceedings of the 13th Conference on USENIX Security Symposium*, Vol. 13, No. 11, USA, USENIX Association, (online), DOI: 10.5555/1251375.1251386 (2004).

[44] Chee Yeung, A. L., Lee Weng Wai, B., Fung, C. H., Mughal, F. and Iranmanesh, V.: Graphical password: Shoulder-surfing resistant using falsification, *2015 IEEE 9th Malaysian Software Engineering Conference (MySEC)*, Institute of Electrical and Electronics Engineers, pp. 145–148 (online), DOI: 10.1109/MySEC.2015.7475211 (2015).

[45] Forget, A., Chiasson, S. and Biddle, R.: Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords, *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)* (2010).

[46] De Luca, A., Denzel, M. and Hussmann, H.: Look into my eyes! can you guess my password?, *Proceedings of the 5th Symposium on Usable Privacy and Security*, No. 7, New York, NY, USA, Association for Computing Machinery, pp. 1–12 (online), DOI: 10.1145/1572532.1572542 (2009).

[47] Kumar, M., Garfinkel, T., Boneh, D. and Winograd, T.: Reducing shoulder-surfing by using gaze-based password entry, *Proceedings of the 3rd symposium on Usable privacy and security*, New York, NY, USA, Association for Computing Machinery, pp. 13–19 (online), DOI: 10.1145/1280680.1280683 (2007).

[48] Khamis, M., Hassib, M., Zezschwitz, E. V., Bulling, A. and Alt, F.: GazeTouchPIN: protecting sensitive data on mobile devices using secure multimodal authentication, *Proceedings of the 19th ACM International Conference on Multimodal Interaction*, New York, NY, USA, Association for Computing Machinery, pp. 446–450 (online), DOI: 10.1145/3136755.3136809 (2017).

[49] Rajanna, V., Polsley, S., Taele, P. and Hammond, T.: A Gaze Gesture-Based User Authentication System to Counter Shoulder-Surfing Attacks, *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, New York, NY, USA, Association for Computing Machinery, pp. 1978–1986 (online), DOI: 10.1145/3027063.3053070 (2017).

[50] De Luca, A., Weiss, R., Hußmann, H. and An, X.: Eyepass - eye-stroke authentication for public terminals, *Proceedings of the 2008 CHI Extended Abstracts on Human Factors in Computing Systems*, New York, NY, USA, Association for Computing Machinery, pp. 3003–3008 (online), DOI: 10.1145/1358628.1358798 (2008).

[51] Cymek, D. H., Venjakob, A. C., Ruff, S., Lutz, O. H.-M. and Roetting, M.: Entering PIN Codes by Smooth Pursuit Eye Movements, *Journal of Eye Movement Research*, Vol. 7, No. 4, pp. 1–11 (online), DOI: 10.16910/jemr.7.4.1 (2014).

[52] Drewes, H., Khamis, M. and Alt, F.: DialPlates: enabling pursuits-based user interfaces with large target numbers, *Proceedings of the 18th International Conference on Mobile and Ubiquitous Multimedia*, New York, NY, USA, Association for Computing Machinery, (online), DOI: 10.1145/3365610.3365626 (2019).

[53] Almoctar, H., Irani, P., Peysakhovich, V. and Hurter, C.: Path Word: A Multimodal Password Entry Method for Ad-hoc Authentication Based on Digits' Shape and Smooth Pursuit Eye Movements, *Proceedings of the 20th ACM International Conference on Multimodal Interaction*, New York, NY, USA, Association for Computing Machinery, pp. 268–277 (online), DOI: 10.1145/3242969.3243008 (2018).

[54] Heikkilä, Henna and Räihä, Kari-Jouko: Speed and Accuracy of Gaze Gestures, *Journal of Eye Movement Research*, Vol. 3, No. 2, pp. 1–14 (online), DOI: 10.16910/JEMR.3.2.1 (2009).

[55] Greinacher, R. and Voigt-Antons, J.-N.: Accuracy Assessment of ARKit 2 Based Gaze Estimation, *Human-Computer Interaction. Design and User Experience*, Springer International Publishing, pp. 439–449 (online), DOI: 10.1007/978-3-030-49059-1_32 (2020).

[56] Voelker, S., Hueber, S., Corsten, C. and Remy, C.: HeadReach: Using Head Tracking to Increase Reachability on Mobile Touch Devices, *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA, Association

for Computing Machinery, pp. 1–12 (online), DOI: 10.1145/3313831.3376868 (2020).
[57] Voelker, S., Hueber, S., Holz, C., Remy, C. and Marquardt, N.: GazeConduits: Calibration-Free Cross-Device Collaboration through Gaze and Touch, *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA, Association for Computing Machinery, pp. 1–10 (online), DOI: 10.1145/3313831.3376578 (2020).
[58] 大和優輝：画像の特徴点列を鍵とした視線入力による個人認証，筑波大学大学院博士課程理工情報生命学術院システム情報工学研究群修士論文 (2022).
[59] Salvucci, D. D. and Goldberg, J. H.: Identifying fixations and saccades in eye-tracking protocols, *Proceedings of the 2000 symposium on Eye tracking research & applications*, New York, NY, USA, Association for Computing Machinery, pp. 71–78 (online), DOI: 10.1145/355017.355028 (2000).
[60] Cao, J., Tang, H., Fang, H., Shen, X., Tai, Y. and Lu, C.: Cross-Domain Adaptation for Animal Pose Estimation, *2019 IEEE/CVF International Conference on Computer Vision (ICCV)*, Institute of Electrical and Electronics Engineers, pp. 9497–9506 (online), DOI: 10.1109/ICCV.2019.00959 (2019).
[61] Mathis, A., Mamidanna, P., Cury, K. M., Abe, T., Murthy, V. N., Mathis, M. W. and Bethge, M.: DeepLabCut: markerless pose estimation of user-defined body parts with deep learning, *Nature Neuroscience*, Vol. 21, No. 9, pp. 1281–1289 (online), DOI: 10.1038/s41593-018-0209-y (2018).
[62] Tan, M., Pang, R. and Le, Q. V.: EfficientDet: Scalable and Efficient Object Detection, *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, Seattle, WA, USA, Institute of Electrical and Electronics Engineers, pp. 10778–10787 (online), DOI: 10.1109/cvpr42600.2020.01079 (2020).
[63] Chrysos, G. G., Moschoglou, S., Bouritsas, G., Panagakis, Y., Deng, J. and Zafeiriou, S.: P–nets: Deep Polynomial Neural Networks, *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 7323–7333 (online), DOI: 10.1109/CVPR42600.2020.00735 (2020).
[64] Fan, S., Wang, R., Ng, T.-T., Tan, C. Y.-C., Herberg, J. S. and Koenig, B. L.: Human Perception of Visual Realism for Photo and Computer-Generated Face Images, *ACM Transactions on Applied Perception*, Vol. 11, No. 2, pp. 1–21 (online), DOI: 10.1145/2620030 (2014).
[65] Moskvyak, O., Maire, F., Dayoub, F. and Baktashmotlagh, M.: Semi-supervised Keypoint Localization, *Proceedings oh the 9th International Conference on Learning Representations (ICLR)*, OpenReview (2021).

付　　録

A.1 攻撃実験の結果詳細

表 A·1 試行回数ごとの結果（ランダム攻撃）

試行回数	突破率	突破回数
1	0.00 %	0
2	0.00 %	0
3	0.00 %	0
4	2.50 %	2
5	2.50 %	2

表 A·2 特徴点数ごとの結果（ランダム攻撃）

特徴点数	突破率	突破回数
1	4.00 %	4
2	0.00 %	0
3	0.00 %	0
4	0.00 %	0

表 A·3 攻撃者ごとの結果（ランダム攻撃）

攻撃者	突破率	突破回数
1	0.00 %	0
2	2.50 %	2
3	0.00 %	0
4	2.50 %	2
5	0.00 %	0

表 A·4 実行者ごとの結果（ランダム攻撃）

実行者	突破回数
1	0
2	0
3	-
4	0
5	0
6	0
7	2
8	2
9	-

表 A·5 特徴点数ごとの結果（秘密鍵再現）

特徴点数	突破率	突破回数	確信度の平均
1	10.00 %	2	1.35 (SD = 0.49)
2	0.00 %	0	1.30 (SD = 0.57)
3	0.00 %	0	1.00 (SD = 0.00)
4	0.00 %	0	1.05 (SD = 0.22)

表 A·6 攻撃者ごとの結果（秘密鍵再現）

攻撃者	突破率	突破回数	確信度の平均
1	0.00 %	0	1.19 (SD = 0.54)
2	0.00 %	0	1.31 (SD = 0.48)
3	0.00 %	0	1.06 (SD = 0.25)
4	12.50 %	2	1.19 (SD = 0.40)
5	0.00 %	0	1.13 (SD = 0.34)

表 A·7 実行者ごとの結果（秘密鍵再現）

実行者	突破回数	確信度の平均
1	0	1.00 (SD = 0.31)
2	1	1.25 (SD = 0.44)
3	-	-
4	1	1.40 (SD = 0.55)
5	0	1.10 (SD = 0.32)
6	0	1.00 (SD = 0.00)
7	0	1.60 (SD = 0.89)
8	0	1.60 (SD = 0.55)
9	-	-

表 A·8 試行回数ごとの結果（観察攻撃）

試行回数	突破率	突破回数	確信度の平均
1	2.50 %	2	1.21 (SD = 0.44)
2	1.25 %	1	1.18 (SD = 0.38)
3	0.00 %	0	1.08 (SD = 0.27)
4	6.25 %	5	1.04 (SD = 0.19)
5	1.25 %	1	1.06 (SD = 0.24)

表 A·9 特徴点数ごとの結果（観察攻撃）

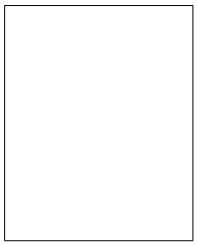
特徴点数	突破率	突破回数	確信度の平均
1	9.00 %	9	1.15 (SD = 0.35)
2	0.00 %	0	1.17 (SD = 0.40)
3	0.00 %	0	1.05 (SD = 0.22)
4	0.00 %	0	1.08 (SD = 0.27)

表 A·10 攻撃者ごとの結果（観察攻撃）

攻撃者	突破率	突破回数	確信度の平均
1	1.25 %	1	1.11 (SD = 0.32)
2	2.50 %	2	1.10 (SD = 0.30)
3	2.50 %	2	1.06 (SD = 0.24)
4	2.50 %	2	1.15 (SD = 0.39)
5	2.50 %	2	1.13 (SD = 0.35)

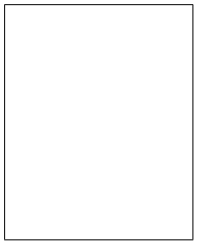
表 A·11 実行者ごとの結果（観察攻撃）

実行者	突破回数	確信度の平均
1	0	1.11 (SD = 0.31)
2	0	1.24 (SD = 0.44)
3	-	-
4	4	1.16 (SD = 0.37)
5	3	1.11 (SD = 0.31)
6	0	1.00 (SD = 0.00)
7	0	1.06 (SD = 0.24)
8	2	1.12 (SD = 0.39)
9	-	-



大和 優輝

2020 年筑波大学情報学群情報科学類卒業．2022 年同大学大学院博士課程理工情報生命学術院システム情報工学研究群卒業．現在，アクセンチュア株式会社所属．ヒューマンインタフェースに関する研究に興味を持つ．



高橋 伸 （正会員）

1991 年東京大学理学部情報科学科卒業．1993 年同大学大学院理学系研究科情報科学専攻修士課程修了．1995 年同博士課程中退．博士（理学）．1995 年東京工業大学大学院情報理工学研究科数理・計算科学専攻助手．2004 年筑波大学大学院システム情報工学研究科コンピュータサイエンス専攻講師．現在，同大学システム情報系准教授．ユーザインタフェース・ユビキタスコンピューティングに興味を持つ．情報処理学会，日本ソフトウェア科学会，ヒューマンインタフェース学会，ACM 各会員．