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

画像の特徴点列を鍵とした
視線入力による個人認証

大和 優輝

修士（工学）

（情報理工学位プログラム）

指導教員　高橋 伸

2022 年 3 月

概要

近年，技術の進歩によりスマートフォン，タブレット，コンピュータ，スマートウォッチなど，パーソナルコンピューティングデバイスが広く普及しており，それらに保存されている個人情報を保護するためのユーザ認証が必要不可欠となってきた．本研究では，画像内の特徴点列を鍵（シークレット）として，視線入力によりシークレットの入力を行う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り，ユーザは画面上に表示される画像に対して，画像内の特徴点を複数指定し，注視する順番をシークレットとして登録する．認証時には，ランダムに表示される類似画像に対して，登録したシークレットに対応する特徴点を順番に注視していくことによりロック解除することができる．本手法は，ショルダサーフィンやスマッジ，サーマル攻撃といったサイドチャネル攻撃に強い視線入力と，辞書/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．画像内の特徴点を利用することにより，ユーザは新たなパスワードを覚える必要なく，認証毎に注視する場所が変更できる．また，本手法の認証画面には，明確な入力箇所は存在せず，一枚の画像が次々に表示されていくだけである．そのため，ロック解除を試みる攻撃者は，デバイスの画面からもユーザの目線からもシークレットを予測することは困難であり，観察攻撃に強い耐性を持つ．この認証システムを実現するために，スマートフォン及びラップトップコンピュータにおいて視線推定システムを実装した．また，その性能を調査及び認証システムにおける各種パラメータを決定するための予備実験を行った．予備実験において，ARKit を利用した視線推定システムでは $\mathrm{RMSE}_{(x,y)} = (44.82\,\mathrm{pt}, 62.28\,\mathrm{pt})$，深層学習を利用した視線追跡システムでは $\mathrm{RMSE}_{(x,y)} = (35.50\,\mathrm{pt}, 91.82\,\mathrm{pt})$ を達成した．その後に，認証システムのプロトタイプ実装を行い，提案手法の実現可能性を調査するための評価実験を行った．結果として，スマートフォン・ラップトップコンピュータそれぞれの認証の受入率が 86.0%・96.7%（一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．認証実行時間は，シークレットに含む特徴点数が 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，何も情報がない状態にて行われるランダム攻撃及び，認証実行時のユーザの目の動きを観察してシークレットを解読する観察攻撃のどちらにおいても，シークレットに含まれる特徴点の数が 1 点の時にはごく少数突破されているが，2 点以上の時に一度も突破されないことがわかった．これらから，本提案手法は，2 点以上の特徴点にて構成されたシークレットを用いれば他者からの攻撃に対しても堅牢である可能性があることが示された．

目 次

図目次

表 目 次

第1章　序論

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．日々の生活から業務に至るまで多様な環境にて利用されており，個人情報や社外秘の情報といった多くの情報を保持している．それらの機密情報保護の観点からデバイスの利用ユーザを照合する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 Personal Identification Number（PIN）やパスワード，スマートフォンにて普及したパターン認証，近年急速に普及してきた指紋認証，顔認証，静脈認証等の生体認証が利用されてきた．本研究では，パーソナルコンピューティングデバイスにおいて日常的に利用される認証システムについて，既存手法の問題及び，その問題を解決するために行われた既存研究の問題を解決するための手法を示す．

本章でははじめに，現在利用されている主な認証方法とその問題点について述べ，それらを解決するために行われた既存研究について述べる．その後，これらの問題点を解決するための手法を提示し，最後に本論文の構成を述べる．

1.1　背景

ラップトップコンピュータやスマートフォンのロック画面のように，個人情報保護のために個人識別を行うさまざまな認証方式が存在する．その中でも，PIN やパスワード，パターンといった「知識ベース認証」と指紋認証，顔認証，静脈認証等の「生体ベース認証」が広く用いられている．モバイルデバイスでの認証には，PIN やパスワード，画面内に表示された点をなぞるパターンといった知識ベースの認証が依然として主流である [HHFM17]．生体ベース認証は知識ベースに比べて個人識別に用いる秘密情報（シークレット）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，一度でもシークレットが流出するとリセットや再発行が不可能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，知識ベースは，攻撃者にシークレット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/パスワードのように単純な数字や文字を使った認証は，辞書攻撃や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 [DACJR05, WWB+05, ML07, EBFK09]．画像パスワードは膨大な容量と高い能力を持つ視覚的な記憶を利用しており，文字や数字の羅列である PIN/パスワードに比べて，多くの利点がある [DACJR05, EBFK09]．また，画像を利用したシークレットは理論的にパスワード空間が大きくなるため推測攻撃にも強い特徴がある [BAS12]．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，ショルダサーフィン攻撃を受ける可能性がある．特に，ATM や共有の PC といった公共空間においては，ビデオカメラや偽物のキーパッドといったデバイスが盗聴やパスワード・PIN の盗用に利用され，安全性を脅かす可能性が存在する．

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検出することが容易となった [VDS+20]．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 [DLWD07, FNS19, FLU+19, KAR+20]．これらの視線を利用した認証は，物理的な入力を必要とせず，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 Smudge Attacks，操作後の熱を検知するサーマル攻撃に耐性を持つ．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．単純な視線の軌跡は，攻撃者が視線の動きを捉えることができれば，解読することができることが報告されている [FLU+19]．また，視線パスワードは，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，シークレットの記憶性 å が低下する可能性がある．

1.2　本研究の目的とアプローチ

図 1.1: 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．

本研究では他者からの攻撃に強く，堅牢な認証を可能とすることを目的とする．この目的を達成するためのアプローチとして，画像内の特徴点を注視するパターンにより認証を行うことを提案する．特徴点とは画像内における物体や部位等の特徴を示す点のことであり，例えば，図 1.1 における耳や鼻，目，足のことである．画像の特徴点列を認証を解除するための秘密情報である鍵（シークレット）として利用し，ロック画面にランダムに表示される類似画像上における各特徴点を登録した順番に注視することにより端末のロックを解除することができる．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，複数の画像において一度登録したシークレットを適用可能である．

本手法は，ショルダサーフィン・スマッジ・サーマル攻撃に強い視線入力と，辞書/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．デバイスの画面を盗み見ることのできる攻撃者に対しては，タッチ入力とは異なり視線を入力としているため，操作している内容はわからず，得ることのできる画像は画面に表示された画像のみとなる．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，シークレット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，目の動きだけからユーザの視線を予測することは難しいことが報告されている．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が異なっており，目の動きを観察したときの画像を知ることは難しく，ユーザが認証ごとに注視する場所も異なるため正確にシークレットを再現することは非常に困難である．さらには，本認証のログイン画面は，画像が表されているだけであるため認証方法及び認証しているタイミング自体も隠蔽されている．そのため，観察時にもユーザの動作を認識すること自体が難しく，本認証を知らない人にとっては認証を試すことすら困難である予測される．

1.3 本研究の貢献

本研究の貢献は，以下の通りである．

- 画像内の特徴点列を鍵とした視線に基づく認証を提案した．
- スマートフォンおよびラップトップコンピュータにおける提案手法の実現可能性を示した．
- 認証実行中のユーザを観察することによる観察攻撃実験を行い，提案手法の安全性を調査した．

1.4 本論文の構成

本章では，本論文の背景及び研究目的とアプローチを述べた．第 2 章では，関連研究について説明し，本研究の位置付けを明らかにする．第 3 章では，提案手法である認証システム

の設計を述べる．第 4 章では，提案手法を実現するために実装したスマートフォン及びラップトップ環境における視線推定システムについて説明する．第 5 章において，認証システムの実装する．第 6 章では，提案する認証手法の実現可能性及び他者からの攻撃に対する堅牢性を調査するための評価実験について述べる．第 7 章では，本研究に関する議論と今後の展望について述べる．最後に第 8 章にて，結論を述べる．

第2章　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端末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．本章では，まずデバイスの認証手法について述べ，次に視線をデバイスの入力に用いる手法について述べる．最後に，本研究と関わりの深い認証の秘密情報である鍵（シークレット）を発展することにより堅牢性を高めた画像パスワードに基づく認証手法と，認証の入力方法を変更することにより堅牢性を高めた視線入力による認証手法について述べる．その後，本研究の位置づけを示す．

2.1　デバイスの認証手法

近年，技術の進歩によりスマートフォン，タブレット，コンピュータ，スマートウォッチなど，パーソナルコンピューティングデバイスが広く普及しており，それらに保存されている個人情報を保護するためのユーザ認証が必須となっている．パスワードや指紋などといった従来の認証方式が不正利用されやすいことが指摘されており，その問題を解決するための手法が多く提案されてきている [SK19]．デバイス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）[Kuc06] やパスワードに代表され，ユーザの既知情報を鍵（シークレット）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おり，対処するために多くの手法が提案されてきた [Agr20, HDLS+15, TMSA13, SDHS15]．シークレット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存在する．Hang らや Thrope らは，地図内の場所を鍵として用いる手法を提案した [HDLS+15, TMSA13]．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 [SDHS15]．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 [GWR+12]．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ロック解除時できる．

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 [San04]．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 [App21d]．

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 [Sam21]．Sandstorom 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 [San04, SMB10, YSW19, XYL+20]．他にも，耳の形を利用したもの [AFKC+12] や，生体信号を利用するもの [MRRT17, ZYK+18] が存在する．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ときに独自の行動パターンをとっていることを利用して，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 [ZBHW14]．また，Chen らはダブルタップの仕方を鍵として使用した [CSZZ15]．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 [SZZZ14] や，ユーザの歩行の仕方を利用するもの [DPM+15]，腕の動きを利用するもの [BZL+13, NWL+16, KPR16, YLX15] が存在する．

2.2 画像パスワードに基づく認証手法

文字列や数字を用いる従来の認証システムがもつ，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知識ベースの手法の一つとして，画像パスワードが提案されてきた．画像パスワードは，人の視覚記憶を利用しており，記憶性や使用感の面で多くの利点があることが報告されている [BCVO12]．記憶性と使いやすさの向上 [ML07] に加えて，画像に基づくパスワードは理論的にパスワード空間が大きくなる可能性が高いため，推測攻撃に対する抵抗力も高くなる．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 [BS00, DACJR05, JGK+03, EI08, DMR04] と画像内の複数の点を選択する方式 [CYLWWF+15] 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等のサイドチャネル攻撃に対して脆弱であることが報告されている [CYLWWF+15].

2.3 視線入力による認証手法

視線入力による認証は，視線を介して，アルファベットや数字を入力するパスワード・PIN といった従来型パスワードを利用するタイプ [DLDH09] と，視線の軌跡などの視線行動に基づく視線パスワードを利用するタイプの二種類が存在する．視線パスワードには，画面内に表示された特定の点を注視する順序 [RPTH17]，事前に定義された視線の軌跡（視線ジェスチャ）[FNS19, DLWD07, DLWHA08, CVR+14, DKA19, AIPH18]，注視点や視線ジェスチャに制限されない自由形式の視線の軌跡 [FLU+19] を利用するものがある．視線入力による認証は，物理的な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存在する．

EyePassword [KGBW07] や EyePIN [DLWD07] 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行うことにより認証を実現した．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 [KGBW07]．GazeTouchPIN [KHZ+17] は，タッチによる PIN 入力と同時に視線を左右に向けることにより

認証を行う 2 段階認証を取り入れ，反復攻撃やサイドチャネル攻撃に対してより安全な認証方式を実現した．Free-Form Gaze Passwords [FLU+19] は，視線ジェスチャや注視点に依存しない，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．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が示された．しかし，完全に自由な形式での視線パスワード生成や実行はユーザに不快感を与えることも報告されている．Heikkila ら [RH09] 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 視線によるデバイスの操作手法

近年, カメラ技術の進歩により, ユーザの視線を認識することが容易になってきた [KAB18]. コンピュータ等のデバイスにおいては，トビー・テクノロジー社等の商用アイトラッキングデバイスが多く利用されている一方で，スマートフォンやタブレットに代表されるモバイルデバイスにおいては視線追跡モジュールを内蔵することやアイトラッキングデバイスを外部接続して利用することは本来の使用感を損なう恐れがある．これらの問題を解決するために，デバイス搭載カメラからの映像を利用して視線を追跡する手法が提案されてきた．深層学習を利用する手法 [PLH17, PSL+16, XEZ+15] が主流である．モバイルデバイスにおいても同様の手法が適用されてきた [KKK+16, PPC21, VDS+20]．最近では Apple 社の開発した拡張現実フレームワークである ARKit[App21c] を利用したものも存在する [AYM18, VHH+20].

また，画面内のオブジェクトを選択する手法として，凝視に基づく手法が提案されてきている [Jac90, Jac91]．一定時間，特定の場所に視点を留めることにより，対象のオブジェクトを選択する．

2.5 本研究の位置付け

本研究では，画像内の特徴点を注視するパターンにより認証を行うことを提案する．本研究にて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は，複数の画像の中から特定の画像を選ぶパターンにより認証するもの，特定の画像内における固定の特徴点を選ぶパターンにより認証するものである一方，本研究の提案手法は，ランダムに表示される画像内の特徴点を選択するパターンにより認証するものである点にて異なる．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にて類似しているが，鍵とする対象が異なる．

第3章　画像の特徴点を注視するパターンに基づく認証

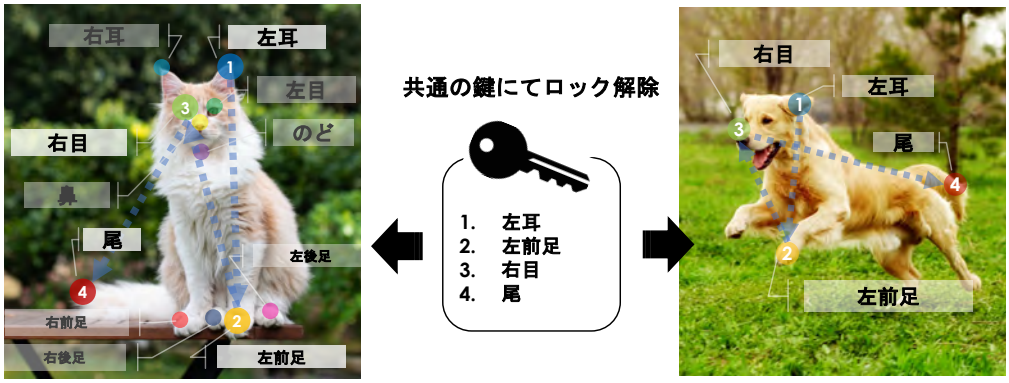
本論文にて提案する認証手法は，画像に基づくシークレットを視線により入力することによりロック解除する手法である．ユーザは，画像内の特徴点を選択する順番を登録し，ランダムに表示される画像に対して注視により特徴点を選択しロックを解除する．本章ではまず，提案する認証手法の概要について述べ，続いて本手法にて利用する画像の特徴点について述べる．その後，提案手法の「シークレット登録とロック解除の認証手順」について述べ，続いて堅牢性について述べる．最後に，本手法の適用例について述べる．

3.1　概要

本研究では画像内の特徴点を選択する順番をシークレットとし，注視により登録したシークレットを入力する認証手法を提案する．シークレットは画像像内の特徴点を利用する画像に基づくパスワードであり，入力は視線により行われる．例えば，図 3.1 の場合，左耳，左足，右目，尻尾の 4 つの特徴点を注視する順番を登録・保存し，認証時には，シークレットに対応する特徴点を入力する．ユーザは，一定時間ごとに変化するランダムな画像において，登録したシークレットの順に，対応する特徴点を注視することによりロックを解除することができる．

3.2　特徴点の利用

特徴点とは，図 3.1 の注釈された点のような画像内における特徴的な点のことである．ここでの特徴点とは，部位ではなく画像内における XY 座標にて表される点を特徴点を定義している．似たような画像，つまり同じ種類の画像（例えば，図 3.1 の猫と犬のような動物の画像）は，同じ特徴点を共有している．ユーザは特徴点の名前とその順番をシークレットとして記録する．特徴点は，複数の類似画像間において，特徴点を共有できるため，一度登録したシークレットはそのまま，別の画像に適用することができる．そして，画像内における特徴点の位置は画像によって異なるため，認証時に別の画像を表示することによりユーザにシークレットの変更を強いることなく，注視する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，解読したときの画像は次の認証時には表示されていないためシステムの安全性は保たれる．



(a) 特徴点とその順番の選択　　(b) 共通のシークレットの利用

図 3.1: ユーザは特徴点の名前とその順番をシークレットとして記録する．共通の特徴点を持つ画像は共通のシークレットを利用してロック解除が可能である．

3.3　認証インタフェース

ユーザは以下の手順に従い，利用するシークレットの登録と認証を行う

シークレット登録　ユーザは表示される画像に対して，画像内の特徴点を複数指定し，注視する順番をシークレットとして登録する（図 3.2 左，図 3.3 上）．

認証　ユーザはランダムに表示される画像に対して，登録したシークレットに対応する特徴点を順番に注視することによりデバイスのロックを解除する（図 3.2 右，図 3.3 下）．

ユーザは単純な文字列や数字列だけではなく，画像を見ながらシークレット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，画像内の特徴点を注視することは，画面上の特定の場所を見るというスマートフォンを使用する上で自然な動作により認証を行うことができる．そのため，視線ジェスチャとは異なり，不慣れな動作をユーザに強いずにロック解除を可能とする．

認証の使用感向上のために，注視判定時にユーザへフィードバックを行う．注視検出のタイミングも秘匿するために，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与える．ラップトップデバイス等の把持や身につけることを行わないデバイスにおいては，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しにいくことが可能となり，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．

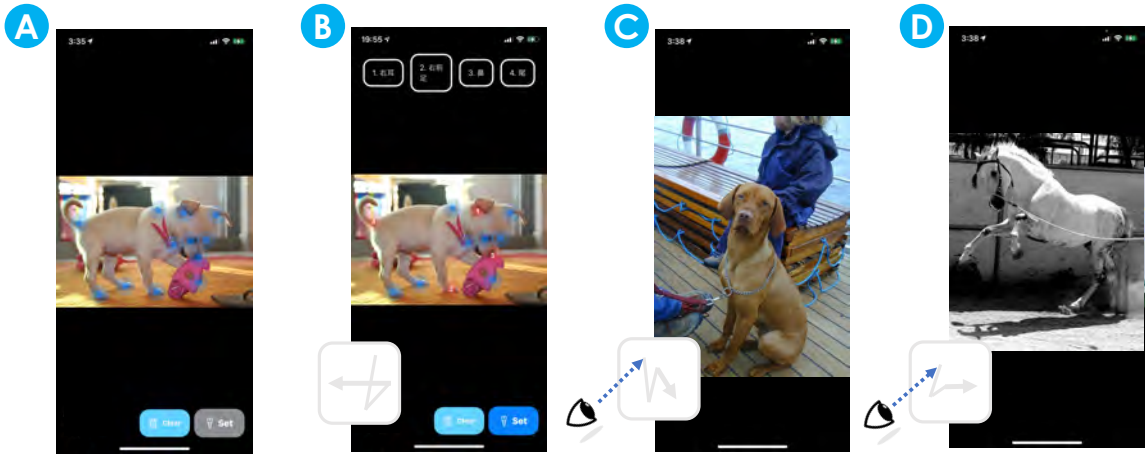


図 3.2: スマートフォンにおけるシークレットの登録画面例. （A）選択前と (B) 選択後. （CD）認証画面例.

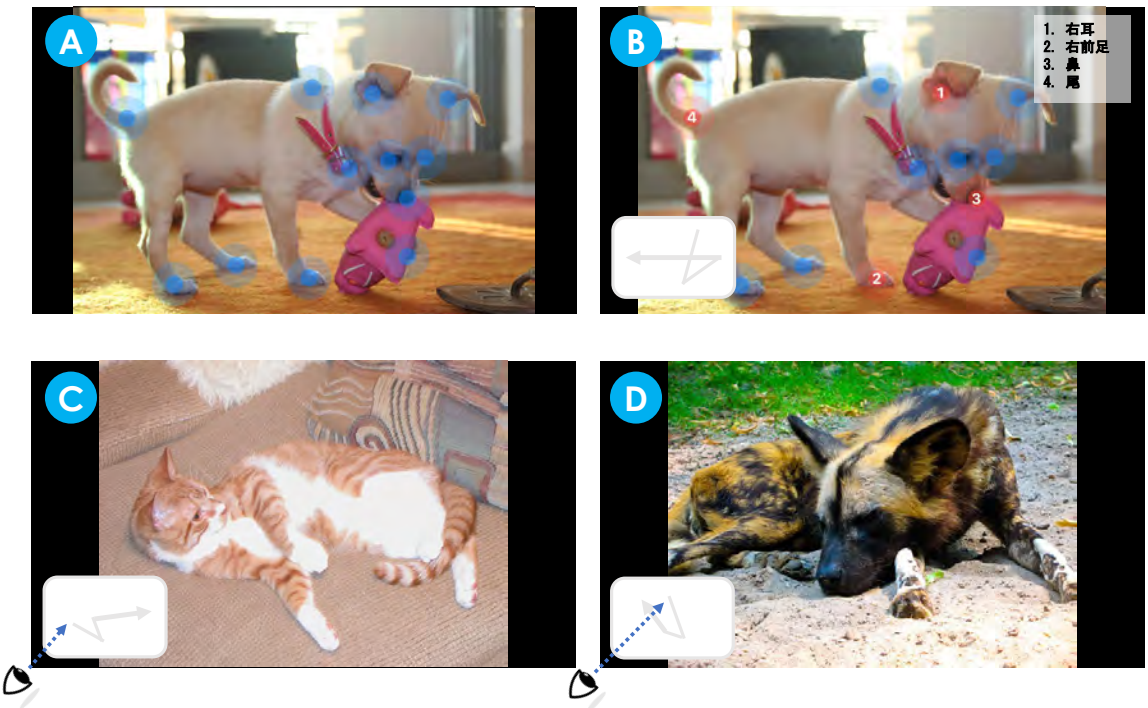


図 3.3: ラップトップコンピュータにおけるシークレットの登録画面例. （A）選択前と (B) 選択後. （CD）認証画面例.

3.4 堅牢性

本手法は，画像パスワードと視線入力による認証を組み合わせているため，攻撃者に対する堅牢性の向上が期待される．特に，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，サーマル攻撃等のサイドチャネル攻撃への耐性が期待される．本手法に対して，図 3.4 に示すような，2 種類の攻撃者を想定している．

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 はデバイスの場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，攻撃者がシークレット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，ユーザの視線を推測し，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 [FLU+19]．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，同じシークレット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，ユーザにシークレットの変更や記憶といった負担を強いずにに，セキュリティを維持することができる．

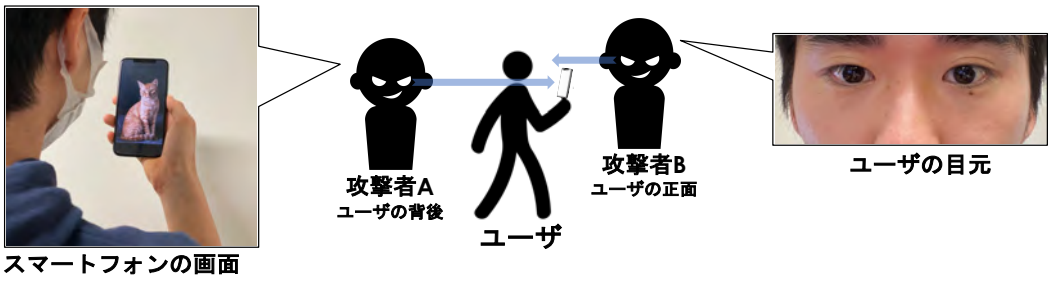


図 3.4: 攻撃者が得ることのできる情報．ユーザの背後にいる攻撃者 A はスマートフォンの画面をショルダサーフィンする．ユーザの正面にいる攻撃者 B はユーザの目元を観察できる．

本手法のパスワード空間（TPS[1]）は，画像内にて利用可能な特徴点の数（N_k）とシークレットに含む特徴点の数（n）に依存しており，$\log_2 {N_k}^n$ となる．例えば，図 3.1 に示す画像の場合，TPS は $\log_2 11^4 \approx 13.8$ となる．また，本提案手法は，ダイヤルパッドやキーボードのような入力箇所を持たないため，シークレットに含まれる明確な場所は攻撃者にとって入手不可能な情報である．そのため，画像内にて利用可能な入力箇所の数は視線追跡制度の解像度（N_r）に依存する．したがって，$\mathrm{TPS} = \log_2 {N_k}^n$ で表すことができる．

[1]TPS（Theoritical Password Space）は指数間的に上昇していくため，一般的に対数関数 $\log_2$ にて比較される [BAS12].

さらには，本認証のログイン画面は，画像が表されているだけであるため認証方法及び認証しているタイミング自体も隠蔽されている．そのため，観察時にもユーザの動作を認識すること自体が難しく，本認証を知らない人にとっては認証を試すことすら困難である予測される．

3.5 適用例

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コンピュータとスマートフォンの両方に適用することが可能である．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．また，視線を入力としているため，物理的な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，公共の場における認証（例えば，ATM や公共の場での大画面デバイス）においても非常に有用であると考えられる．更には，手の不自由な人も視線によりシークレットを入力できるため利用可能である．

第4章　視線推定システムの実装

本研究において，認証の鍵の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．スマートフォンにおいては，デバイスに搭載されたフロントカメラの画像を利用した視線追跡システムを実装し，ラップトップコンピュータにおいては，商用の視線追跡デバイスを用いた．

4.1　スマートフォンにおける視線推定システムの実装

従来，モバイル環境における視線追跡は特殊なハードウェアを必要としてきたが，近年，商用スマートフォンの性能が向上し，それに伴いフロントカメラも高性能化してきている．それにより，追加のカメラやデバイスを接続することなく，ユーザの視線を追跡できるようになった [KAB18]．スマートフォンにおける視線追跡が可能となったことにより，研究室内だけでなく実環境における視線動作の研究が可能となってきている．さらには，商用スマートフォンにアプリケーションをインストールするするだけで，ユーザに視線ジェスチャや注視といった視線入力によるインタラクションを可能としている．これらを踏まえて，スマートフォンにおける視線推定システムを「ARKit を利用した手法」と「深層学習を利用した手法」の二種類の実装にて実現した．

4.2　手法 1: ARKit を利用した視線追跡

本節では，ARKit を利用した視線追跡システムの実装について説明する．はじめに実装に用いるスマートフォンとフロントカメラからの情報を取得するためのフレームワークについて述べる，続いて，得られた情報から視線を推定するための視線推定アルゴリズムについて述べ，本システムの予備調査の結果を示す．最後に，キャリブレーションについて説明する．

4.2.1　利用するデバイス

視線推定システムの実装において，利用するスマートフォンには Apple 社の開発した iPhone を採用した．商用のスマートフォンの一つである iPhone には，RGB カメラの他に深度マップ・赤外線画像を取得可能な TrueDepth カメラが搭載されている．これらは顔認証に利用されており，顔の深度マップから正確な顔の形状を読み取り，登録データとの照合が行われて

いる．正確な顔の情報を取得できるカメラを搭載している iPhone を利用することにより，追加の機器なしにて視線推定システムを構築できると考えた．

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[1] を採用した．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 frame/s にて収集可能である．このフレームレートは HCI 分野におけるユーザビリティテストにおいて十分な速度であると報告されている [GVA20]．最新の HCI 研究においても利用されており，HeadReach[VHCR20] 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，GazeConduit[VHH+20] 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 により実現した．

4.2.2 視線推定アルゴリズム

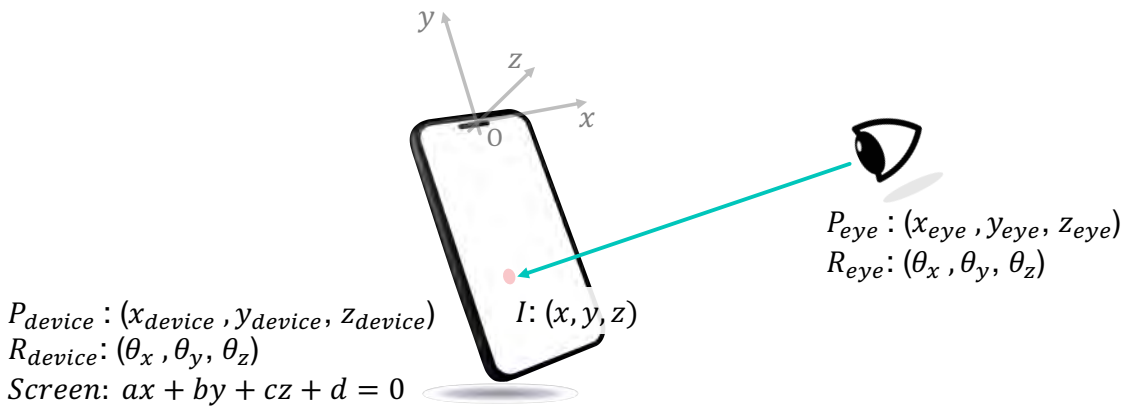


図 4.1: ARKit の拡張現実空間における視線推定のイメージ図．それぞれの座標及び回転角は，スマートフォンのカメラの位置を原点とする拡張現実空間の座標系にて表現されており，ARKit の ARAnchor, ARFaceAnchor を通して取得し，座標変換により算出している．

ARKit から得られるデータを基に視線推定を行う．具体的には，ARKit により取得できるデバイスの位置と角度，目の位置と角度を利用して，デバイスのスクリーン平面と目の位置と角度から得られる視線ベクトルの交点を算出し，ユーザの視点位置とする．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て表現される．拡張現実空間は，図 4.1 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[App21a] を設定し，

[1] https://developer.apple.com/documentation/arkit

追跡する．特に人については別途 ARFaceAnchor[App21b] 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，顔の位置や角度，目の位置や角度，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（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．左右の目それぞれにおいて，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}，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 4.2 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であるため，図 4.2 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 にて表現される．pt は画面際時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，1 pt ≃ 0.17 mm である．

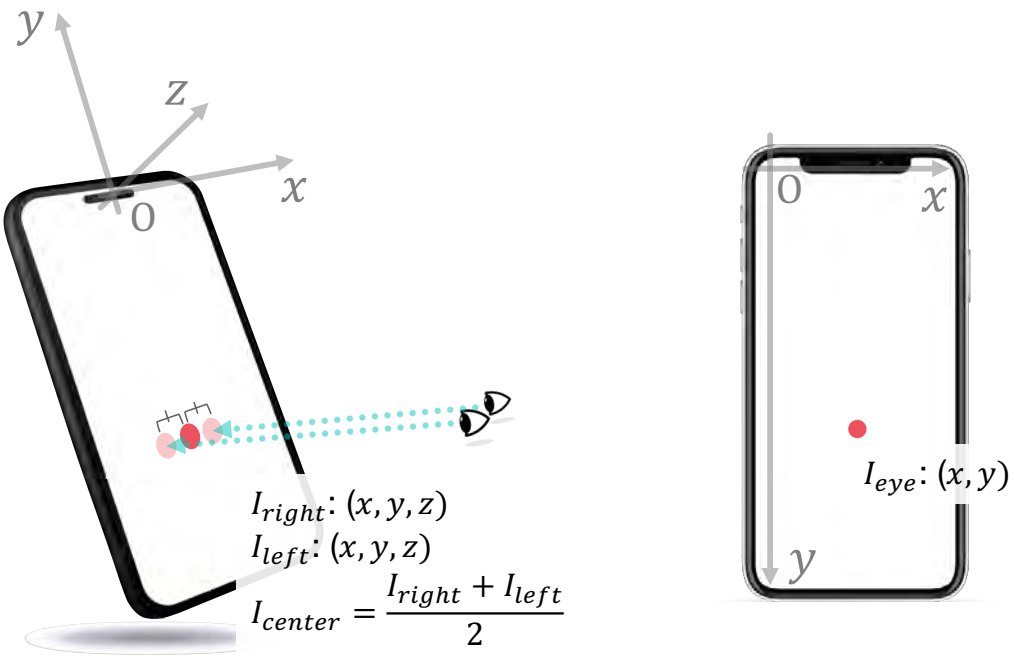


図 4.2: 左）拡張現実空間の 3 次元座標系における視点位置の算出．右）スクリーン平面の 2 次元座標系における視点位置の算出．

4.2.3 予備調査：ARKit による視線推定システムから取得できるデータの観察

前節にて，実装した視線推定アルゴリズムから得られる視線データを検証するために予備調査を行った．実行者は著者 1 名であり，iPhone 11 Pro を利用し，屋内にて実施した．デバ

イスを手に持ち，図 4.3 のように明るく表示された点を 5 秒間注視する．取得したデータは，$6_{targets} \times 5_{seconds} \times 60_{frames}$ である．

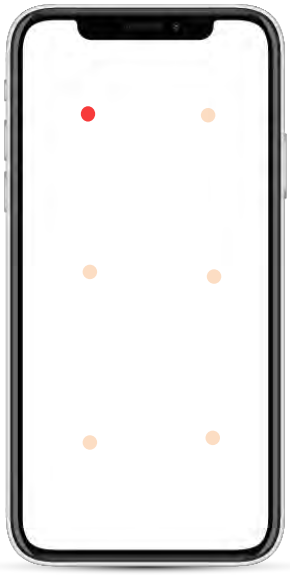


図 4.3: 予備調査：データ収集を行う注視点

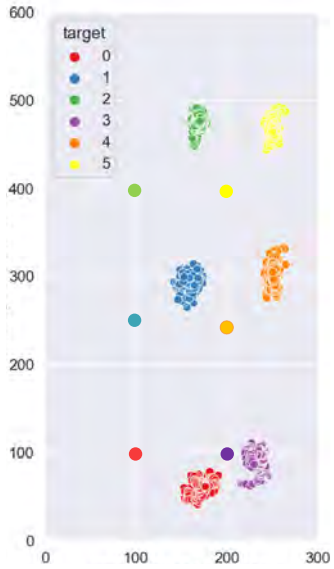


図 4.4: 予備調査：視線推定可視化結果

視線推移結果を可視化した（図 4.4）ところ，誤差は大きいが，各点ごとの分散は小さくなっており，画面内の点を注視していることは検出できると考えられる．また，視線推定結果が全体的に右にずれていることから，キャリブレーションによる補正が必要である．

4.2.4 キャリブレーション

図 4.5 における 4 角の点をキャリブレーションの基準点として利用する．ユーザは，4 点をそれぞれ 2 秒間ずつ注視し，注視した際に取得したデータから推定された視点位置を学習データとして，XY ごとに回帰分析を行う．回帰分析のモデルにはサポートベクタマシン（SVR）を用いた．実装には，Python のライブラリである scikit-learn[2]を利用した．回帰分析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．

4.3 手法 2: 深層学習を利用した視線追跡

本節では，深層学習を利用した視線追跡システムの実装について説明する．本視線追跡システムは，畳み込みニューラルネットワークを利用した深層学習モデルを視線追跡システム用の大規模公開データセットを用いて学習させ，ベースモデルを構築する．続いて，スマートフォンを利用して取得したデータを用いて，追加学習を行い，今回実装する環境に最適化

[2] https://scikit-learn.org/

図 4.5: キャリブレーションに利用する点

させる．最後に，深層学習モデルの出力をもとに，回帰モデル（SVR）を利用して，ユーザ毎にキャリブレーションを行う．

4.3.1 実行環境

本システムの実装には，スマートフォンと深層学習モデル及び回帰モデルを学習するための PC が必要となる．スマートフォンは，iPhone 11 Pro を利用した．PC の仕様は，Intel Core i9-10900K CPU @3.70GHz，GeForce RTX 3090，32GB Memory であった．利用した主なライブラリとして，深層学習モデルの構築及び学習には，TensorFlow[3]，SVR の学習には scikit-learn，学習したモデルの利用には，TensorFlow Lite[4]，顔画像内における目の特徴点抽出には MediaPipe[LTN+19] を使用した．

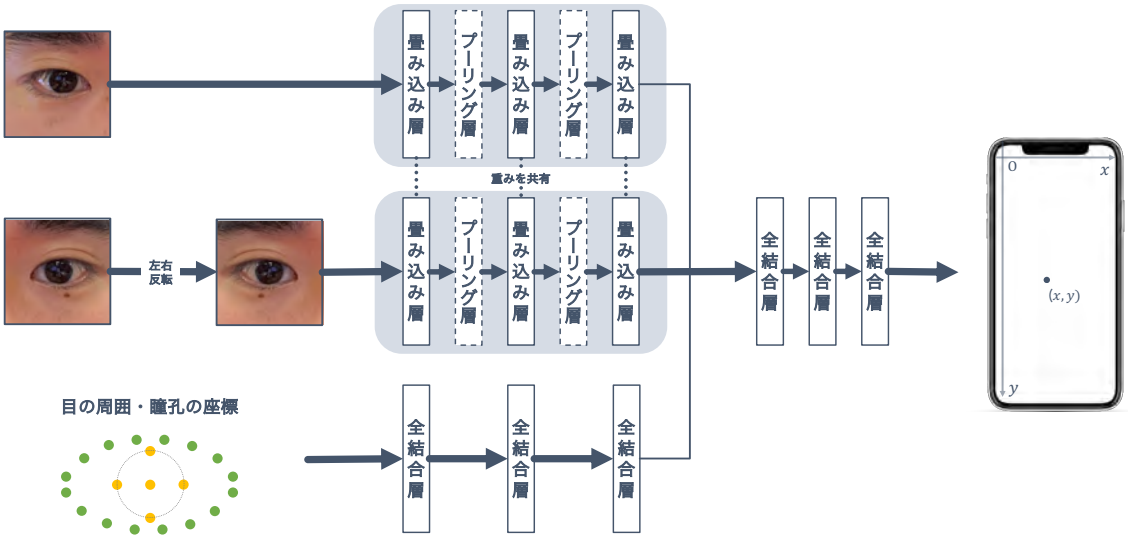


図 4.6: 深層学習モデルの概要図．入力は，左右の目の画像と，目の周囲の座標（16 点 × XY 座標 × 左右）及び瞳孔の座標（5 点 × XY座標 × 左右）である．学習を効率化するために左の目の画像は左右反転し，畳み込み層の重みを共有する．出力は画面上のユーザの視点座標である．

4.3.2 深層学習モデルの構築

深層学習モデルの構築には，Valliappan ら [VDS+20] や Krafka ら [KKK+16] のモデルを参考にした．モデルの概要を図 4.6 に示す．本モデルは，ユーザの左右の目の画像と目の周囲の座標 16 点，瞳孔の座標 5 点を入力として，スマートフォンの画面内の標準化された視点座標（[0,1]）を出力する．左右の目の画像はそれぞれ 3 層の畳み込み層にて処理されるが，計算時間短縮のために左右の目で重みを共有する．この時，左目の画像は左右反転された状態にて入力される．目の周囲の座標及び瞳孔の座標については，3 層の全結合層によって処理され，畳み込み層の出力と結合する．最後に，結合された出力を 3 層の全結合層によって処理し，最終的な出力とする．

一般的に，深層学習は大量の学習データを必要とする．しかしながら，HCI 分野において大量のデータを用意することは多大な労力を必要とする．大量の学習データの収集なしにて，高い精度を達成する手法の一つとして転移学習 [Pra93] がある．予め対象のデータと似た大量のデータを用いて事前学習させ，その後に対象のデータを用いて最適化を行う．大規模データセットとして，スマートフォンのフロントカメラからの画像およびそれに対応するユーザの視点座標を含む GazeCapture[KKK+16] データセットを利用した．前処理として，GazeCapture データセットの画像に対して，目の周囲の座標及び瞳孔の座標の取得する．目の周囲の座標

[3] https://www.tensorflow.org/
[4] https://www.tensorflow.org/lite/api_docs?hl=ja

及び瞳孔の座標の取得は，MediaPipe の Iris Landmark Model[AVG+20] を利用した．また，目の周囲の座標をもとに，左右の目の画像のクロップを行い，左目の画像に関しては左右反転を行った．前処理により得られた目の周囲の座標及び瞳孔の座標と左右の目の画像をもとに，事前学習を行った．事前の学習に利用したハイパパラメータは，Valliappan ら [VDS+20] と同じ値を利用した．

4.3.3 モデルの最適化とキャリブレーション

GazeCapture データセットによって事前学習されたモデルを利用し，iPhone 11 Pro を利用した視線追跡システムに最適化させる．後述の 5 章の予備実験にて，収集した 145,800 フレームの画像データ（図 4.5 右の軌跡を注視し続けたときのデータ）を利用して，追加学習を行った．学習済みのモデルの出力をユーザへ最適化するために，前節 4.2.4 のキャリブレーションと同様に回帰モデルであるサポートベクタマシン（SVR）を利用する．キャリブレーションに利用するデータも同様に図 4.5 における 4 角の点データである．回帰分析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．

4.4 ラップトップにおける視線推定システムの実装

ラップトップコンピュータにおける視線推定システムの実装は，Irisbond 社の開発した商用の視線追跡デバイスである Hiru[5]（図 4.7）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，16 点）を必要とする．

図 4.7: Hiru（画像は Irisbond 社による）

Hiru はディスプレイ下部に設置され，PC とは USB にて接続された（図 4.8）．Hiru デバイスと目の距離は推奨距離である 35 cm − 80 cm にて，利用した．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，視線推定システムは Windows 上にて実装

[5]https://www.irisbond.com/en/producto/hiru/

図 4.8: Hiru を接続した様子

された．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．Hiru は注視判定が行われると，画面内における注視位置を 2 次元座標系にて出力する．出力された注視点を認証システムの入力として利用する．

第5章　予備実験

4 章にて実装した視線推定システムを利用し，以下の目的にて，予備実験を行った．

- ARKit を利用した視線推定システムの精度調査
- 深層学習を利用した視線追跡システムの精度調査
- 提案手法の認証実行時のユーザの特性を調査

本章では，提案手法を実装する上での各種パラメータの決定および視線追跡を行うために実施した予備実験について述べる．

5.1　参加者及び実験環境

実験参加者は，9 名（P1–P9，21–24 歳，平均年齢 22.9 歳）であり，普段からスマートフォンを使用している大学生及び大学院生であった．被験者の内 1 名がコンタクトレンズ，2 名が眼鏡を着用していた．

実験は屋内の蛍光灯下にて行われた．使用したデバイスは，TrueDepth カメラの搭載された iPhone 11 Pro[1]である．被験者は，椅子に座り，顔とスマートフォンの位置を固定された状態にて，実験に参加した．

5.2　タスク

被験者のタスクは，3 種類あり，サンプルデータ収集・シークレット登録・認証実行である．視線追跡精度の検証を行うためのサンプルデータ収集セッションでは，被験者は緑色の点を見続けるタスクを行う．図 5.1 左の 15 点が 1 点ごとランダムな順番にて 2 秒間ずつ表示される（*Dots*）．続いて，図 5.1 右のように円，四角形，ジグザグを描くように 30 秒間表示される（*Pursuit*）．被験者は表示される緑色の点を見続ける．次に，シークレット登録セッションでは，被験者は画像内に表示された特徴点から指示された個数の特徴点を指定する．その後，指定した特徴点の注視する順番を決定する．これにより，認証に利用するシークレットが登録される．最後に，認証実行セッションでは，被験者はランダムに表示される 6 枚の画像に対して，登録したシークレットにて特徴点を注視する．認証実行後，被験者は正しく認

[1] https://support.apple.com/kb/SP805?locale=ja_JP

証が行われたか質問され，正しく認証された場合には次の画像へ，認識されなかった場合には同じ画像で成功するまで認証を行う．上記 3 セッションを 1 セットとし，特徴点の数を 1，2，3 において，それぞれ 3 セットずつ実施する．

図 5.1: キャリブレーションに利用する点（左），軌跡（右）

5.3 結果

実験により，サンプルデータ収集セッションにおいて，$60_{\text{フレーム}} \times 2_{\text{秒}} \times 15_{\text{点}} \times 3_{\text{回}} \times 3_{\text{セット}} \times 9_{\text{人}} = 145,800_{\text{フレーム}}$（*Dots*），$60_{\text{フレーム}} \times 30_{\text{秒}} \times 2_{\text{種類}} \times 3_{\text{回}} \times 3_{\text{セット}} \times 9_{\text{人}} = 291,600_{\text{フレーム}}$（*Pursuit*），シークレット登録セッションにおいて，$3_{\text{特徴点数}} \times 3_{\text{セット}} \times 9_{\text{人}} = 81_{\text{種類のシークレット}}$，認証実行セッションにおいて，$6_{\text{枚の画像}} \times 3_{\text{特徴点数}} \times 3_{\text{セット}} \times 9_{\text{人}} = 486_{\text{回の実行}}$ が得られた．

5.3.1 視線追跡精度評価

ARKit を利用した視線推定システムの精度

サンプルデータ収集セッションの *Dots* において得られたデータを利用し，視線追跡精度の評価を行った．図 5.1 左における 1，3，13，15 の点を訓練データ，残りをテストデータとして，検証を行ったところ，xy それぞれにおいて RMSE は（44.82 pt, 62.28 pt）となった．

深層学習を利用した視線追跡システムの精度

サンプルデータ収集セッションの *Dots* において得られたデータを利用し，視線追跡精度の評価を行った．図 5.1 左における 1，3，13，15 の点を訓練データ，残りをテストデータとし

て，検証を行ったところ，xy それぞれにおいて RMSE は（35.50 pt, 91.82 pt）となった．

比較分析結果

どちらの RMSE においても，x 座標よりも y 座標の方が大きい結果となった．要因としては，デバイスの位置が顔よりも下に存在したために，取得できた画像自体が歪んでいたことや，さらに下に視線を動かすことが難しかったことが挙げられる．これらは，デバイスの位置が顔よりも下に存在する場合におけるデータをより多く収集し，学習データとして利用することにより実際の使用環境に合わせたより精度の高い結果を得られると考えられる．

ARKit を利用した視線推定システムの誤差距離は 76.7 pt，深層学習を利用した視線追跡システムの誤差距離は 97.5 pt であった．したがって，ARKit を利用した視線推定システムを採用する．精度結果から，画面サイズ 812 pt × 385 pt（iPhone 11 Pro）の場合，幅 44.82 pt，高さ 62.28 pt の重ならない長方形を 21 個含むことができる．この場合，TPS は $\log_2 21^4 \approx 17.6$ となり，少ない特徴点数においても十分な堅牢性を維持することができる（例えば， 4 桁の PIN は $13.3 \approx \log_2 10^4$，4 桁のパスワードは $20.7 \approx \log_2 64^4$）．認証にかかる時間を短くするためには，シークレットに含む特徴点数はできるだけ少ない方が好まれる．

5.3.2 特徴点

予備実験において，収集されたシークレットに含まれる特徴点のヒストグラムを図 5.2 に示す．鼻や背，尾，のどといった左右の概念を持たない特徴点が多く選択していることが確認された．これらは，ユーザが分かりやすく，覚えやすい点であり，近い距離にある点（左右の目や足）を避けた結果だと考えられる．この結果は，シークレットに選択する特徴点に偏りが生じてしまい，攻撃者の推測攻撃に対して脆弱性を与える可能性を示唆している．この懸念を解決するためには，左右の概念を持たない特徴点のみを含む画像や，全ての特徴点間の距離が一定以上離れている画像を利用することが考えられる．

5.3.3 正答率

ARKit を利用した視線推定システムにおいて，登録したシークレットとユーザが実際に注視した特徴点の正答率は，シークレットに含まれる特徴点の数ごとに，1 点の時 88.9%，2 点の時 81.5%，3 点の時 81.5%であった．また，特徴点それぞれにおける正答率は 84.7%である．この時の特徴点ごとの混同行列を図 5.3 に示す．左右の要素を持つ特徴点同士の混同が多く見られる．これは画像内において，左右の要素を持つ特徴点同士の位置が近くなっていることによる誤認識とユーザが左右の特徴点を混同してしまい間違った点を見ている誤実行によるものであると推測される．

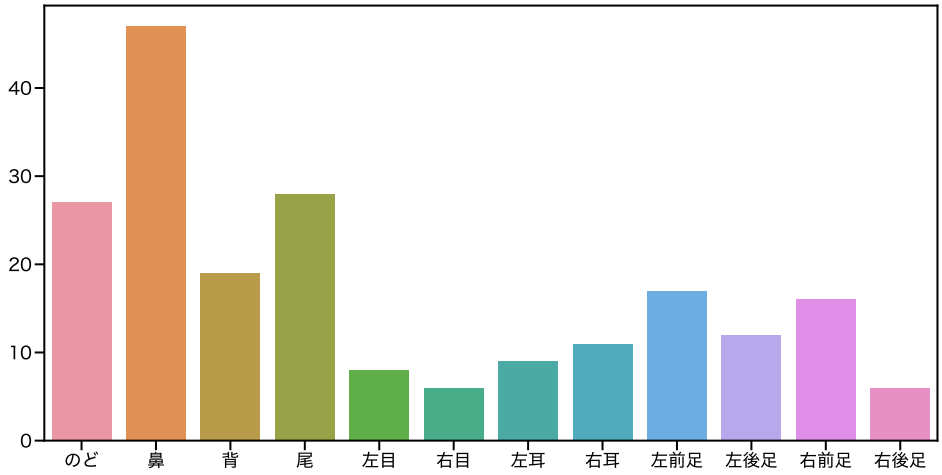


図 5.2: シークレットに含まれる特徴点のヒストグラム

5.3.4 実行時間

ARKit を利用した視線推定システムにおいて，本認証に要する実行平均時間は，シークレットに含まれる特徴点ごとに，1 点の時 1.749 秒，2 点の時 2.487 秒，3 点の時 3.464 秒となった．実行時間は特徴点の数に比例しており，より少ない特徴点数にて堅牢性を維持することにより非常に短時間にて実行可能な認証の実現が可能となる．

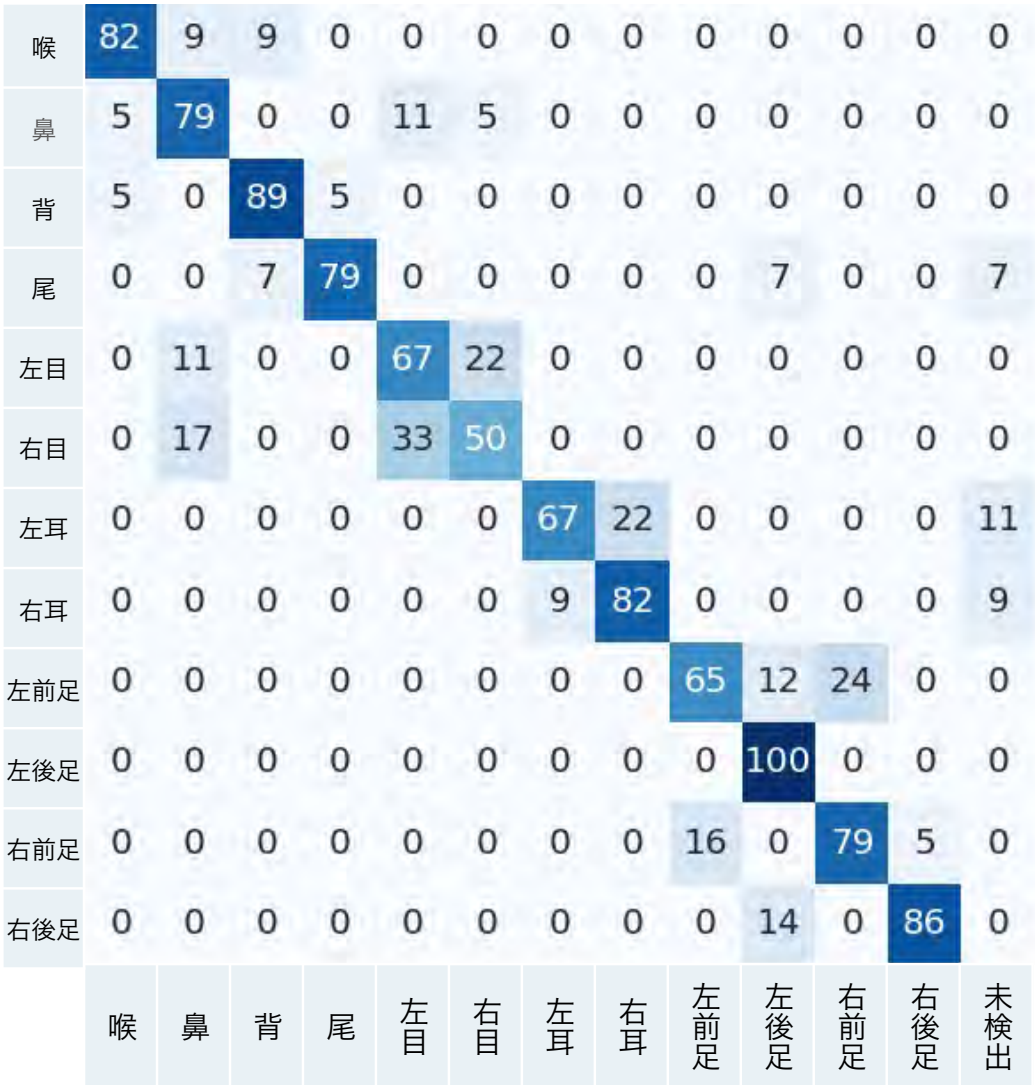


図 5.3: 特徴点ごとの検出結果の混同行列

第6章　認証システムの実装

本章では，3 章にて提案した認証システムのプロトタイプの実装について述べる．予備実験の結果を基に実装した「認証インタフェース」と「認証アルゴリズム」について説明したのちに，認証システムの実装を実現する上で，必要であった「画像と特徴点データ」について述べる．今回は認証システムのプロトタイプとして実装しており，ユーザの登録したシークレットと視線によって入力されたシークレットのマッチングを行うアプリケーションとして実現した．

6.1　実装環境

本認証システムは，スマートフォンとラップトップコンピュータ上にて実装される．視線認識システムと同様に，スマートフォンは iPhone 11 Pro を利用し，Swift を利用して実装された．ラップトップコンピュータは Windows PC（Intel Core i9-10900K CPU @3.70GHz，GeForce RTX 3090，32GB Memory，15inch Display）を利用した．また，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．

6.2　認証インタフェース

ユーザは以下の手順に従って認証を行う．

登録 ユーザは画面に表示された画像中の青い点からタッチ入力（スマートフォン），マウス選択（ラップトップコンピュータ）にて複数の特徴点を選択し，注視する順番をシークレットとして登録する（図 3.2，3.3(A)(B)）．

認証 ユーザはランダムに表示された画像において，登録された順番にシークレットに対応する特徴点を注視する（図 3.2，3.3(C)(D)）．青い点は認証時には表示されない．

ユーザは，図 3.2（スマートフォン），3.3（ラップトップコンピュータ）の画面上にて，登録と認証を行うことができる．例えば図 3.2，3.3A では犬が表示され，シークレットに利用できる特徴点が青い点にて表示されている．ユーザは，「右耳，左前足，鼻，尻尾」の 4 つの特徴点をシークレットとして選択する（図 3.2，3.3B）．この時，登録した特徴点の名称が画面に表示され確認することができる．

認証時には，異なる動物の画像がランダムに表示され（図 3.2CD），ユーザは登録したシークレットに従って対応する特徴点を注視することにより，認証毎に異なる視線位置にてデバ

イスのロックを解除する．注視のたびにフィードバックをユーザに提示し，注視が検知されたことを明確にする．スマートフォンユーザには，振動を，ラップトップユーザには，効果音を提示した．また，認証時の画像を一定時間（30 秒）表示し，ユーザが画面を横にスライドさせた時及び一定時間経過した時に画像を変更する．また，攻撃者が何度も認証を試みることを防ぐために，認証に 5 回（スマートフォンの一般的なリトライ回数）失敗すると 30 秒間認証を無効化する．

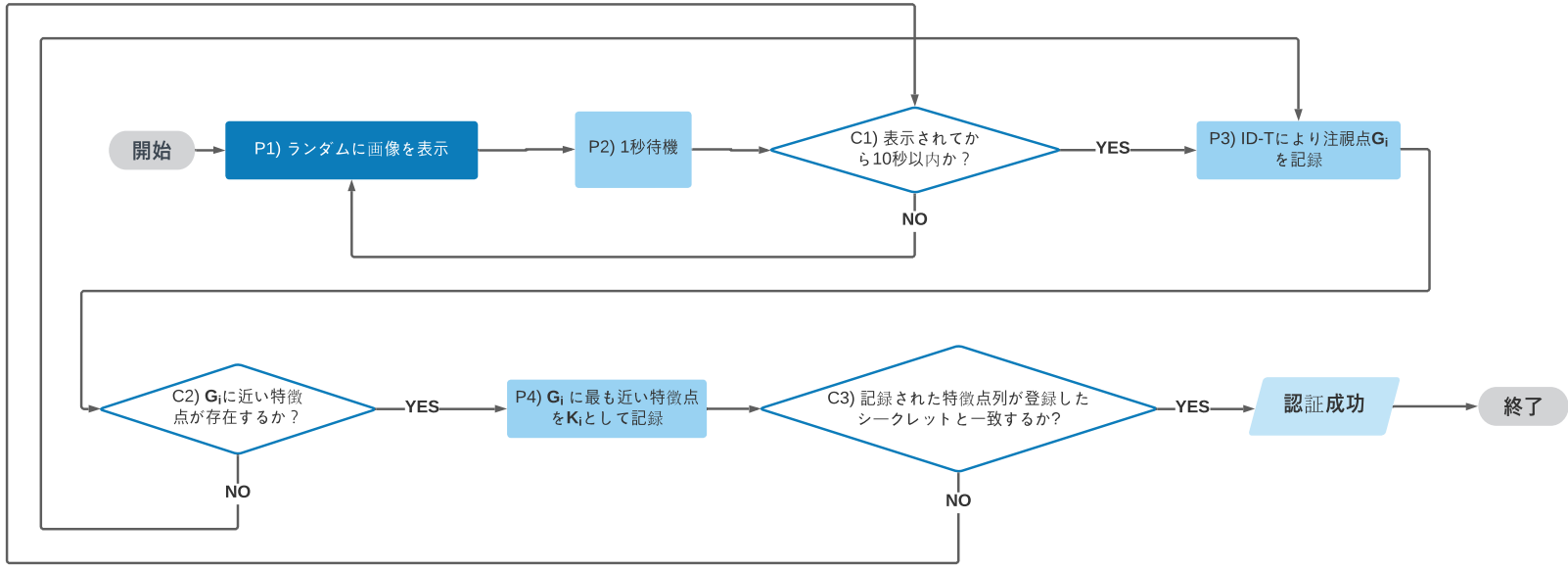


図 6.1: 認証アルゴリズム

6.3 認証アルゴリズムの実装

図 6.1 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）．認証システムはユーザの視線追跡位置をシステムの入力として利用する．この時，ミダスタッチ問題を抑制するために，画像が表示されてから 1 秒間は注視を検出しない（P2）．注視の検出を開始すると，注視された特徴点列がシークレットと一致するか判定される．一致していた場合は，認証成功となる．画像を表示してから一定時間経過すると画像が更新される（C1）．失敗回数が 5 回になると，認証に使用できない画像（類似画像でない画像）を 30 秒間表示する．

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選択し，選択した特徴点列とシークレットを照合する必要がある．ユーザの注視点を取得するために，Dispersion-Threshold Identification (I-DT) algorithm [SG00] を利用した．ウィンドウ幅（$T = 700\,\mathrm{ms}$），標準偏差閾値（th_{gaze}=10 pt）に設定した．システムは，I-DT により検出されたユーザの注視点（G_i）を記録し（P3），続いて，注視点から一定範囲内（$G_x - d_x \leq K_x \leq G_x + d_x \wedge G_y - d_y \leq K_y \leq G_y + d_y$）に存在する特徴点（$K_i$）を記録する（C2）．ここで，一定範囲には，視線追跡システムの RMSE よりも大きい範囲を指定する．複数の特徴点が検出された場合，注視点に最も近い特徴点を記録する（P4）．注視された特徴点が記録されると，記録された特徴点列（$[K_1, \ldots]$）と登録されたシークレットを比較し，特徴点とその順番が完全に一致した時に限り，認証成功とする（C3）．一致しない場合は，一定時間が経過する，もしくはユーザにより画像が変更されるまで，認証を継続する．

6.4 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，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 [CTF+19] 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 つ（*Two eyes, Throat, Nose, Withers, Two Earbases, Tailbase, Four Elbows, Four Knees, and Four Paws*）の種類の特徴の位置が記録されている（図 6.2）．これらの特徴点の中でも，*Four Elbows and Four Knees* は，他の点との距離が違すぎたため省略し，7 つの特徴（計 12 点）を利用した．

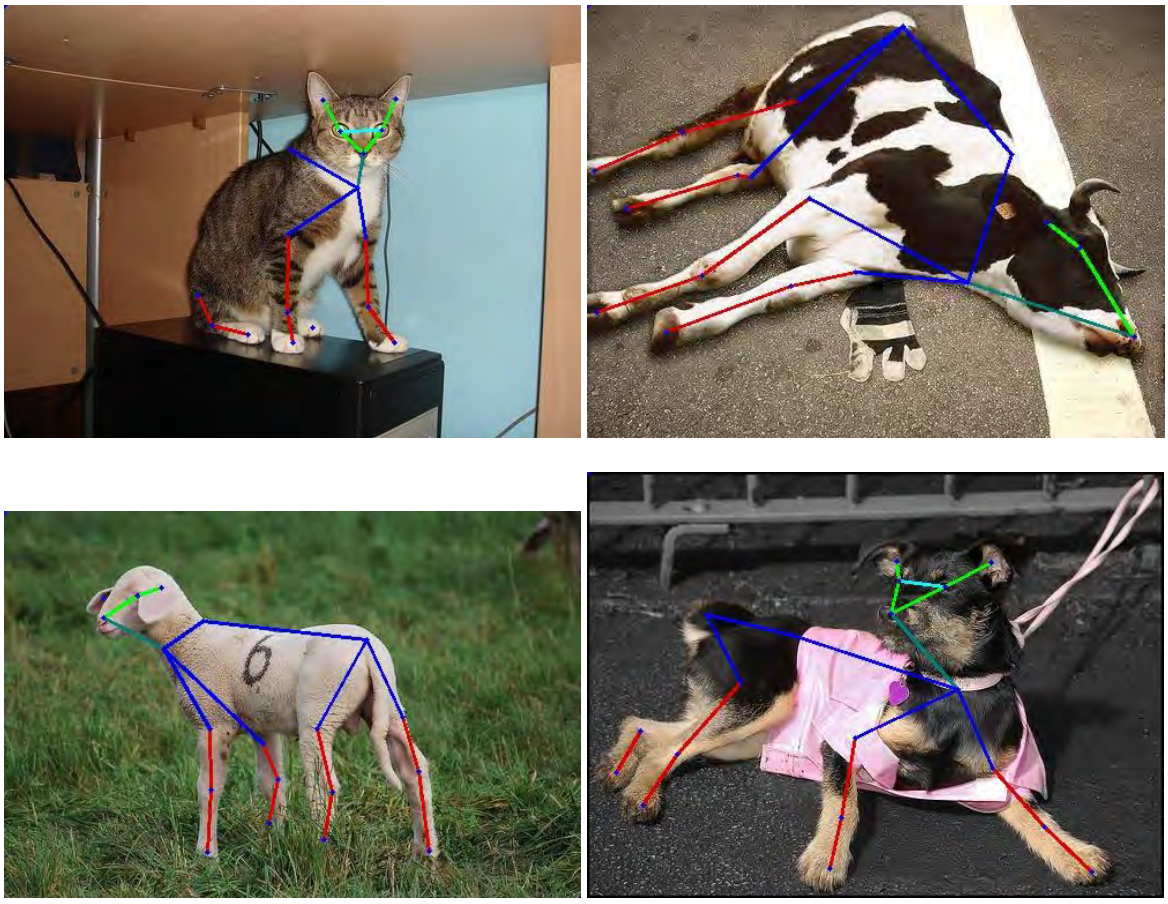


図 6.2: Animal-Pose Dataset に含まれる画像と特徴点例（画像は元論文 [CTF+19] を引用）.

第7章　評価実験

本章では，提案手法の実現可能性を調査するために実施した評価実験について述べる．初めに，「スマートフォンにおける認証システムの評価」について述べ，次に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」について述べる．最後に，攻撃者に対してどれだけ堅牢であるかを評価するために実施した「攻撃実験」について述べる．

7.1　スマートフォンにおける認証システムの評価

スマートフォンにおける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．

7.1.1　参加者及び実験環境

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大学生であった．被験者の内 3 名がコンタクトレンズ着用しており，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．被験者は，椅子に座り，顔とスマートフォンの位置を固定された状態にて，実験に参加した．

7.1.2　タスクと実験手順

被験者のタスクは，シークレット登録と認証実行である．シークレット登録タスクでは，被験者は画像内に表示された特徴点から 4 点の特徴点をタッチ入力にて指定し，その順番をシークレットとして登録する．認証実行セッションでは，被験者はランダムに表示される画像に対して，登録したシークレットにて特徴点を注視する．上記 2 つのタスクを 5 回繰り返すことを 1 セットとし，4 セット実施する．それぞれのセットの初めに，被験者はキャリブレーションを実施した．実験終了時に，被験者は表 7.1 に示されるアンケートに 5 段階のリッカード尺度にて回答する．

7.1.3　結果

実験の結果，$5_{\text{execution}} \times 4_{\text{sets}} \times 5_{\text{persons}} = 100_{\text{executions}}$ のデータが得られた．また，アンケート結果を表 7.1 に示す．

表 7.1: アンケートの内容と回答

No.	質問と回答	平均	標準偏差
Q1	本認証の実行は容易であったか 1: 難しい 5: 易しい	4.2	0.84
Q2	本認証を実行した時に，疲労感はあったか 1: 感じなかった 5: 感じた	3.6	1.14
Q3	本認証を使いたいか 1: 使いたくない 5: 使いたい	4.4	0.89

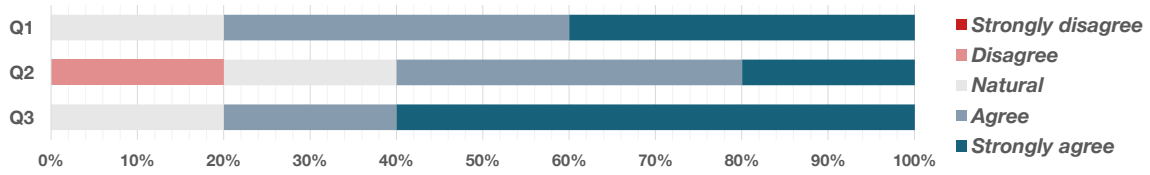


図 7.1: アンケート結果（スマートフォン）

認証の受入率は，86.0%であった．ここで，認証の受入率とはユーザが正しく入力したときに認証システムが認証成功とした割合である．被験者ごとの認証されるまでに実行した回数を図 7.2 に示す．1 回のリトライで 95%の認証が成功した．Microsoft の認証システムの一つである Windows Hello の受入率の要件として，95%（理論値，実測においては 90%）以上である [1]ことが求められているため，提案手法の受入率を向上させる必要がある．特に，左と右の混同が受入率に強く影響していると考えられる．これは，左右の要素を持つ特徴点が近接していることによる誤認識と，ユーザが左右の特徴点を混同して注視することによる誤入力が原因として考えられる．

誤認識に対処するためには，視線追跡精度を向上させる必要がある．今回の実験は，ARKit を利用した視線追跡手法を用いていたが，深層学習を利用した視線追跡手法を導入することにより更なる改善が見込まれる．また，視線追跡の RMSE に基づいて，近すぎる特徴点の選択を無効化することでも対処できると考えられる．誤入力に対処するために，風景画像や，人物の集合写真等の左右の特徴が少なく，複数の対象が存在する画像データセットを利用することが挙げられる．

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

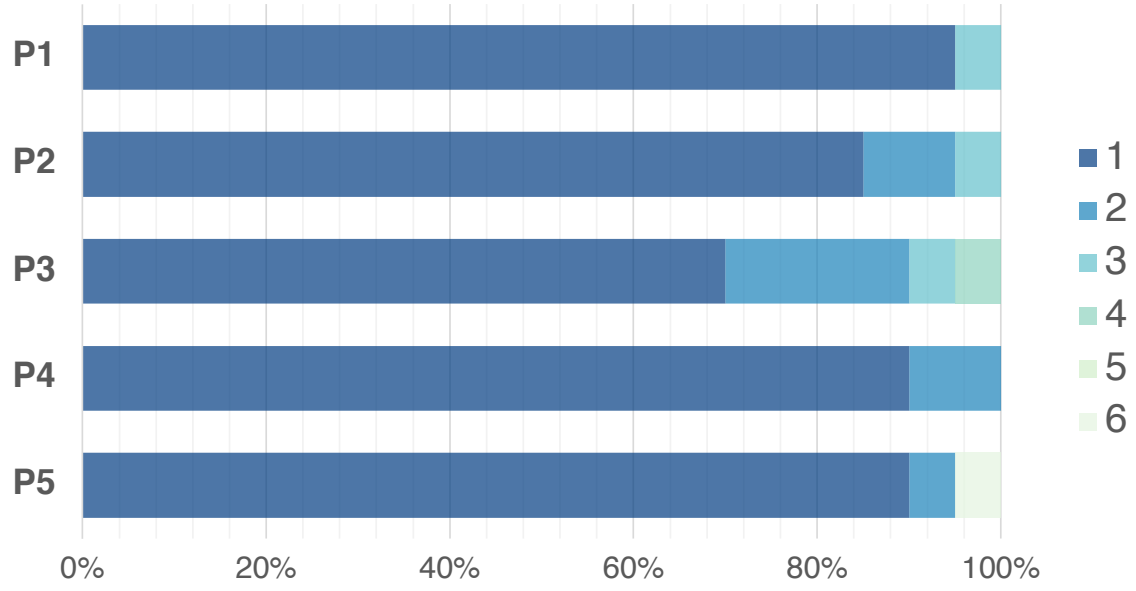


図 7.2: 試行回数（スマートフォン）

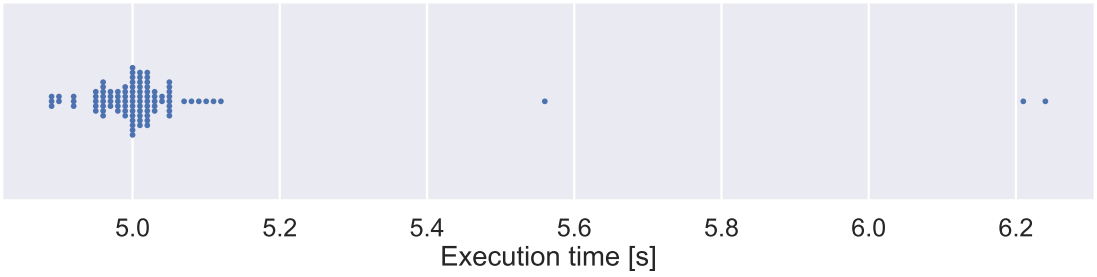


図 7.3: 実行時間（スマートフォン）

認証の平均実行時間は，5.03 s（SD=0.186 s，VAR=0.0345）であった．認証の実行時間は，非常に短い範囲に分布しており（図 7.3），分散も小さいことから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．予備実験を考慮すると，認証の実行時間は注視検出に必要な一定時間と特徴点の数の積におおよそ従うことがわかる．

アンケートの項目とそれぞれの結果を表 7.1，各ユーザの結果を図 7.1 に示す．本手法の全体的な印象は好意的であったが，認証実行時に疲れを感じている被験者も存在した．これは，視線を利用した操作に慣れていないため引き起こされたと考えられる．一方で，「思ったよりもスムーズに認証できてよかった」，「スクリーンセーバーが表示されているように見えるだ

表 7.2: ユーザコメント（原文）

被験者	コメント
P1	点の数はちょうど良い，パスワードはできるだけ離れた点を使った， 面白かった，思っていたよりもスムーズに実行できた
P2	点の数はもっと増やした方が安全そう， 近い点を使わないようにした
P3	点の数をもっと減らしてほしい，わかりやすい点（鼻，尾）を入れた， パソコンの方が使いやすそう
P4	使いやすかった，点の数も違和感がなかった， なるべく離れていて，ある程度の規則性を持って決めた（左右の足を斜めにとか）
P5	点の数が自由でもいいのかなって思った， 深く考えずに決めた，結果として近すぎる点がないようになっていた気がする， 縦長の画像の方がやりやすい？

けなので安心できる」といった好意的なコメントも存在した．また，シークレットに利用する特徴点の選択基準として，鼻や尻尾といった「わかりやすい」特徴点を選択し，選択画面において近くに表示されていた特徴点は選択しなかったと報告された．

7.2 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

スマートフォンに搭載されている画面とは異なる画面サイズのデバイスにおける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．

7.2.1 参加者及び実験環境

実験参加者は，3 名（P1–P3，21–22 歳，平均年齢 21.3 歳，男性 3 人女性 1 名）であった．被験者の内 2 名がコンタクトレンズ着用しており，残り 1 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．使用したデバイスとして，ラップトップコンピュータは Alienware 15 R3，視線追跡デバイスは Hiru を利用した．被験者は，椅子に座り，実験に参加した．

7.2.2 タスクと実験手順

被験者のタスクは，シークレット登録と認証実行である．シークレット登録タスクでは，被験者は画像内に表示された特徴点から 4 点の特徴点をタッチ入力にて指定し，その順番をシークレットとして登録する．認証実行セッションでは，被験者はランダムに表示される画像に対して，登録したシークレットにて特徴点を注視する．上記 2 つのタスクを 5 回繰り返すこ

とを 1 セットとし，4 セット実施する．それぞれのセットの初めに，被験者はキャリブレーションを実施した．実験終了時に，被験者は表 7.3 に示されるアンケートに 5 段階のリッカード尺度にて回答する．

表 7.3: アンケートの内容と回答

No.	質問と回答	平均	標準偏差
Q1	本認証の実行は容易であったか 1: 難しい 5: 易しい	4.3	0.47
Q2	本認証を実行した時に，疲労感はあったか 1: 感じなかった 5: 感じた	1.7	0.47
Q3	本認証を使いたいか 1: 使いたくない 5: 使いたい	4.3	0.47

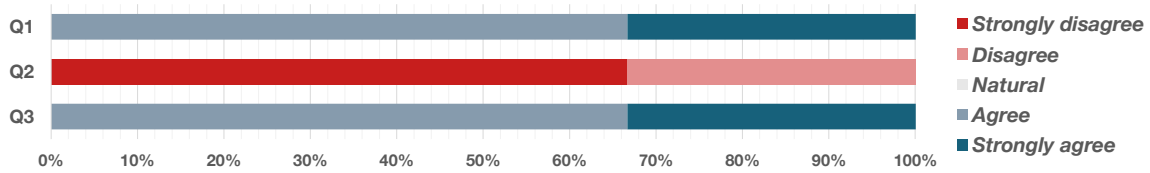


図 7.4: アンケート結果（ラップトップコンピュータ）

7.2.3 結果

実験の結果，$5_{\text{execution}} \times 4_{\text{sets}} \times 3_{\text{persons}} = 60_{\text{executions}}$ のデータが得られた．また，アンケート結果を表 7.3 に示す．

認証の受入率は 96.7%であった．被験者ごとの認証されるまでに実行した回数を図 7.5 に示す．1 回のリトライで 100%の認証が成功した．

スマートフォンにおける実行と比較して，受入率，試行回数の観点で良い結果を得ることができた．これは，画面が広いことにより画像内の特徴点同士の距離が遠いことによって，特徴点の選択が正確になったためと考えられる．しかしながら，実行時間においてはラップトップコンピュータの方が長い結果となった．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．これらは画面サイズに依存しているため，画面に表示する画像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．

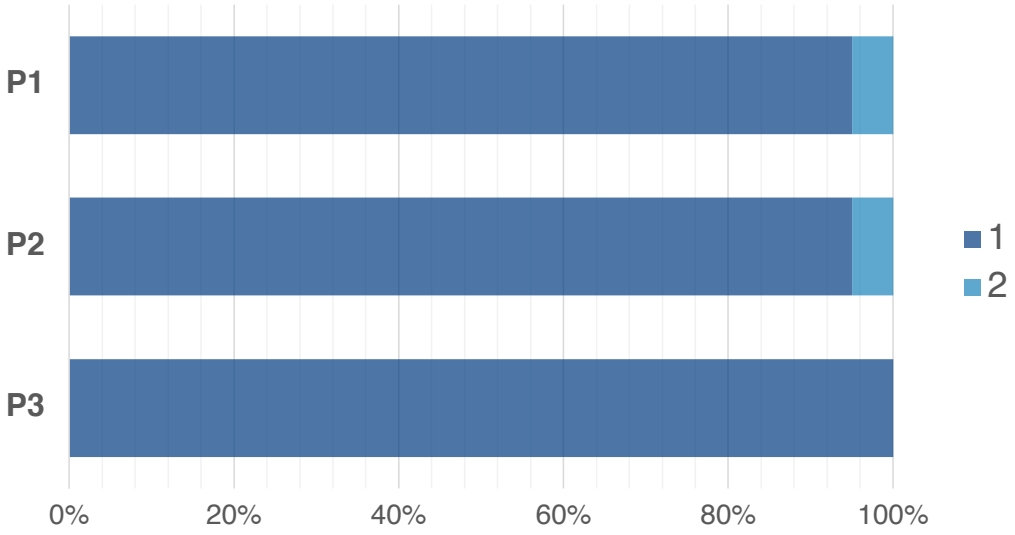


図 7.5: 試行回数（ラップトップコンピュータ）

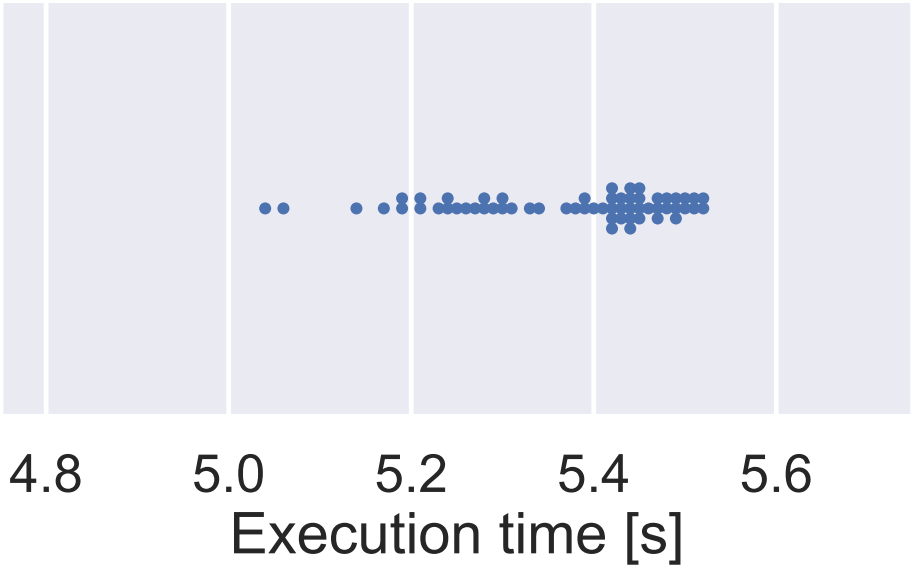


図 7.6: 実行時間（ラップトップコンピュータ）

7.3 攻撃実験

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．

7.3.1 参加者及び実験環境

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．被験者の内 3 名がコンタクトレンズ着用しており，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．

本実験において，認証を実行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，5 章の予備実験及び 7.1 節の評価実験において，被験者の正面，顔の高さに設置されたカメラにより撮影した（図 7.7）．収集したビデオは，181 個のシークレットであり，シークレットに含まれる特徴点の数ごとに 12 個ずつランダムに抽出したものを実験にて利用した．

7.3.2 タスクと実験手順

被験者のタスクは，ランダム攻撃とシークレット再現と観察攻撃である．ランダム攻撃タスクでは，被験者は何も情報がない状態にて，シークレット毎に 5 回ロック解除を試みる．この時，被験者は事前に認証手法については理解しており，その他の情報は与えられない．シークレット再現タスクでは，ユーザの認証時の目の動きから入力しているシークレットが再現できるかを調査するために，認証実行をしているユーザの正面から撮影した映像から，シークレットを再現してもらう．この時，被験者は，実行者がパスワードを解除しているときの目の動きのビデオ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された．観察攻撃タスクでは，ユーザの認証時の目の動きから入力しているシークレットを解読し，認証を突破することが可能であるかを調査するために，認証実行をしているユーザの正面から撮影した映像から，ロック解除を試みてもらうこの時，シークレット再現タスクと同様に，映像は何度でも見ることができ，ノート等の使用が許可された．．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毎に 1 回ずつ実施することを 1 セットとし，4 セット実施する．ランダム攻撃タスクと観察攻撃タスクの初めに，被験者はキャリブレーションを実施した．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）を被験者に質問している．

7.3.3 結果

実験の結果，ランダム攻撃にて $16_{\text{シークレット}} \times 5_{\text{回}} \times 5_{\text{人}} = 80_{\text{回の攻撃}}$，シークレット再現にて $16_{\text{シークレット}} \times 5_{\text{人}} = 80_{\text{回の再現}}$，観察攻撃にて $16_{\text{シークレット}} \times 5_{\text{回}} \times 5_{\text{人}} = 80_{\text{回の攻撃}}$ が行われた．全ての攻撃の結果を表 7.4 に示す．実験後に被験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
- 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・確信度を表 7.5–7.15 に示す．ランダム攻撃，シークレット再現，観察攻撃全てにおいて，シークレット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 点以上のシークレットにおいては一度も突破されることは存在しなかった．また，シークレット再現，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て攻撃していないことがわかる．

表 7.4: 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	-
シークレット再現	2.50%	2	1.18 (SD = 0.41)
観察攻撃	2.25%	9	1.11 (SD = 0.32)

特徴点ごとに突破された回数を図 7.8 に示す．右前足や背，尾の特長点が多く解読されていることが確認できる．実際に解読されたシークレットについて内容を確認したところ，特定の実行者が行った一回の実行に関して 4 回攻撃が突破されていたことがわかった．

図 7.7: 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.

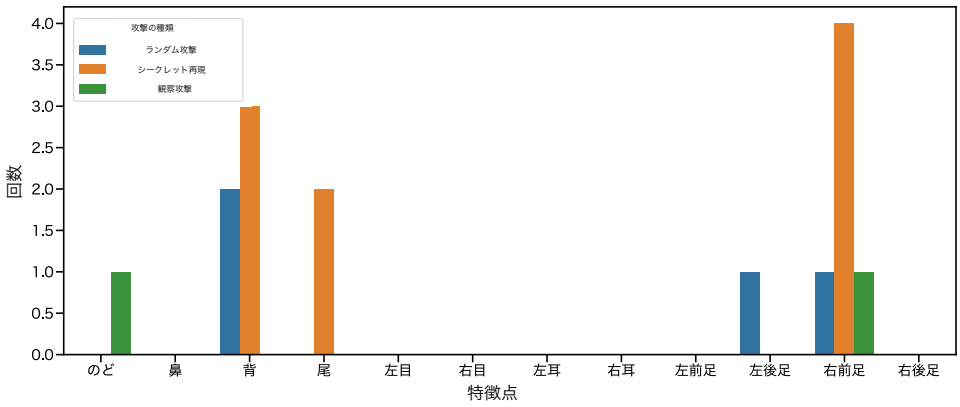


図 7.8: 攻撃され突破された特徴点

表 7.5: 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 7.6: 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 7.7: 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 7.8: 実行者ごとの結果（ランダム攻撃）

攻撃者	突破回数
1	0
2	0
3	-
4	0
5	0
6	0
7	2
8	2
9	-

表 7.9: 特徴点数ごとの結果（シークレット再現）

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 7.10: 攻撃者ごとの結果（シークレット再現）

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 7.11: 実行者ごとの結果（シークレット再現）

攻撃者	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 7.12: 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 7.13: 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 7.14: 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☒☒☒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 7.15: 実行者ごとの結果（観察攻撃）

攻撃者	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	8	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	-	-

第8章　議論と今後の課題

本章では，予備実験，認証システムの実装，評価実験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．

8.1　誤認識と誤入力

予備実験及び評価実験の結果から，提案手法には誤認識と誤入力の懸念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，視線追跡精度及び ID-T のパラメータ調整不足によるものだと考えられる．視線追跡の誤差よりも短い距離に存在する特徴点が含まれてしまい，システムが間違った特徴点を検出してしまうことへの対策としては，

- 視線追跡精度を向上させる
- 近すぎる特徴点を選択できないようにする
- シークレット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

ことが考えられる．また，ID-T のパラメータについては，必要な注視時間よりも早く視線を動かしてしまうことや，注視判定された後に視線を留まらせてしまったことによる二重入力が発生していたため，より多くの被験者実験を通して最適な注視判定時間や，標準偏差閾値を再度調整する必要がある．

ユーザがシークレットに登録した特徴点ではない特徴点を入力してしまったことによる誤入力は，ユーザがシークレット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．これは，左右の要因を持つ特徴は画像として表示される際に鏡像反転しており，シークレットを登録する際に左右を混同してしまうといった被験者のコメントが存在した．したがって，左右の要因を持つ特徴を削除する，もしくは，左右の要因を持つ特徴を持つ画像群を利用しない（例えば，人の顔や，物体自体を特徴とする画像）ことが挙げられる．

8.2　使用感

アンケートの結果及びコメントから，ユーザは，提案手法の容易さ及び使用したさに関して非常に好意的であることがわかった．疲労を感じるユーザも存在したが，視線による操作

に慣れていないことが原因として挙げられているため，長期間における学習効果についても検証する必要がある．また，スマートフォンよりもラップトップコンピュータのようなある程度の大きさを持った画面における使用の方がアンケート結果が良好であったことから画面サイズも使用感に影響していると考えられる．画面サイズが大きくなることにより，特徴点の選択において正確性が高まることが想定されるため，特徴点の誤入力の観点においてユーザへ不快感を与える可能性が少なくなる．ただし，大きくなりすぎると実行時間が増大する可能性があるため，表示する画像サイズについては比較実験を行う必要がある．

8.3 認証の実行時間と堅牢性

認証はデバイス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求められる．予備実験及び評価実験の結果から，認証時間はシークレット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，シークレットに含まれる特徴点の数を可能な限り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．しかしながら，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．7.3 節により示されたように，特徴点を 1 点だけ含むシークレットの場合，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．一方で，2 点以上の場合，計 400 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，シークレット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，今回の攻撃実験は被験者 5 人であったため，より多くの人数を採用して堅牢性を確かめる必要がある．

8.4 他者からの攻撃に対する堅牢性

前節でも述べたようにシークレット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，突破されたシークレット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．同じ実行者の別のシークレット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シークレット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．

今回の認証アルゴリズムにおいて，入力の終了を定義しておらず，攻撃者が 3 点の入力をしようとした時に，前方の 1 点，もしくは 2 点が一致していた時，つまり，入力が前方部分一致していた場合に，認証が突破されてしまう懸念が存在する．この問題に対処するために，注視判定を行なった後に次の注視を行うまでの間の時間にタイムアウトを設けることにより入力終了条件を追加することができる．これにより，シークレットに含む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，入力終了後に待ち時間が発生してしまうため，認証の実行時間を伸ばしてしまう要因となる．システム自体の堅牢性と使用感のトレードオフを考慮すると，本人以外には絶対に解除されてはいけないシステ

ムに対しては十分なタイムアウトを設け，堅牢にし，堅牢性よりも日々の使用感や認証速度が重視されるシステムに関してはタイムアウトを短くする，もしくはタイムアウトを設けないといったコンテキストに応じた条件分けが必要となると考えられる．

8.5 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，単純な動物の画像を含む公開データセットの Animal-Pose Dataset を利用した．本提案手法は類似画像とそれぞれの画像内の特徴点位置が含んでいれば適用できるため，ユーザ自前の画像に対しても利用可能である．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 [MMC+18, TPL20, CMB+20, FWN+14, MMDB21, CTF+19] を利用することにより，特徴点の位置を算出することができる．しかしながら，ユーザの画像は認証システムとしての安全性を満たす数の特徴点を含んでいるか，特徴点ごとの距離は離れているかといった懸念が存在する．そのため，利用できる画像群の要件定義を行い，要件を満たさない画像に対しては利用できなくするといった対策が必要となる．

現在利用している「特徴」は画像内の特徴であるが，デバイス自体の特徴（画面の角や端，中央）といった情報も認証時には共通の特徴となるため，これらを特徴として取り入れることによりより複雑なシークレットを生成し，攻撃者が解読できないようにすることができるようになる可能性がある．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」の追加はシークレットを複雑にし，攻撃者に対する堅牢性を得られる可能性があるが，一方でユーザのシークレットの記憶性や，実行容易性を損なう恐れがあるため，導入する際には，被験者実験を通して使用感を調査する必要がある．

また，更なる発展として，動画に対しても適用できると考えられる．例えば，アクアリウムのような複数の魚が泳いでいるような映像を利用し，特定の魚を見る順序をシークレットとして利用することにより，特徴点の場所を完全に流動的にすることができ，更なる堅牢性を得られる可能性がある．

第9章　結論

本論文において，画像内の特徴点を鍵とする視線入力によ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シークレットとして登録し，ランダムに表示される類似画像に対して，登録したシークレットに従って対応する特徴点を注視することによりデバイスのロックを解除する．

これを実現するために，スマートフォン及びラップトップコンピュータにおける視線追跡システムを設計及び実装し，その性能を調査するための予備実験を行った．結果として，更なる追跡精度の向上は求められるが，プロトタイプとして十分な精度を持つことがわかった．続いて，予備実験の結果をもとに，提案手法の認証システムの実装を行った．

評価実験では，実装したプロトタイプの認証システムを用いて，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，認証の受入率が 86.0%，96.7%（一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，注視検出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ることが確認され，シークレットに含む特徴点数が 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．攻撃実験では，無作為な攻撃及び，認証実行時のユーザの目の動きを観察して攻撃のどちらにおいても，シークレットに含まれる特徴点の数が 1 点の時にはごく少数突破されているが，2 点以上の時に一度も突破されないことがわかった．このことから，シークレットに含む特徴点の数を 2 点以上のできるだけ小さな値にすることにより短時間かつ堅牢な認証を実現できる可能性がある．

今後の課題として，視線追跡精度を要因とする誤認識と画像の特徴のの左右混同による誤入力があることが確認されたため，対処する必要がある．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，より大人数での被験者実験を行い実行容易性とともに安全性を調査する必要がある．また，今回実装したプロトタイプシステムは基礎的な設計のみであり，ユーザ保有の画像の利用や動画の利用，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．

謝辞

本研究を進めるにあたり，高橋伸准教授，志築文太郎教授，川口一画助教には多大なご助力を賜り，深く感謝を申し上げます．特に，高橋伸准教授には，研究の方針や内容，論文の書き方など研究活動において数多くのご意見やご指導をいただきました．重ねて感謝いたします．

インタラクティブプログラミング研究室の皆様には，研究における様々なご助力をいただきました．特に UBIQUITOUS チームの皆様には，チームゼミを始め，実装や論文時の添削など多くのご支援をいただきました．感謝いたします．さらに，昨年度修了生である鈴木雄太郎さんには，メンターとして指導していただき，研究の方針や実装，論文の執筆において多くのご助力をいただきました．深く感謝いたします．

最後に，研究室生活を支えてくださった家族，友人，学生生活にてお世話になった皆様にお礼申し上げます．

参考文献

[AFKC+12] P. N. Ali Fahmi, Elyor Kodirov, Deok-Jai Choi, Guee-Sang Lee, A. Mohd Fikri Azli, and Shohel Sayeed. Implicit authentication based on ear shape biometrics using smartphone camera during a call. In *2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pp. 2272–2276. Institute of Electrical and Electronics Engineers, October 2012.

[Agr20] Harsh Agrawal. How hackers hack your accounts password & ways to avoid being hacked. `https://shoutmetech.com/how-hackers-hack/`, July 2020. Accessed: 2022-1-6.

[AIPH18] Hassoumi Almoctar, Pourang Irani, Vsevolod Peysakhovich, and Christophe Hurter. Path word: A multimodal password entry method for ad-hoc authentication based on digits' shape and smooth pursuit eye movements. In *Proceedings of the 20th ACM International Conference on Multimodal Interaction*, ICMI '18, pp. 268–277, New York, NY, USA, October 2018. Association for Computing Machinery.

[App21a] Apple, inc. ARAnchor - augmented reality - apple developer. `https://developer.apple.com/documentation/arkit/aranchor`, 2021. Accessed: 2022-1-11.

[App21b] Apple, inc. ARFaceAnchor - augmented reality - apple developer. `https://developer.apple.com/documentation/arkit/arfaceanchor`, 2021. Accessed: 2022-1-11.

[App21c] Apple, Inc. ARKit - augmented reality - apple developer. `https://developer.apple.com/jp/augmented-reality/arkit/`, 2021. Accessed: 2020-12-17.

[App21d] Apple, Inc. Face ID - apple. `https://support.apple.com/en-us/HT208108`, September 2021. Accessed: 2022-1-11.

[AVG+20] Artsiom Ablavatski, Andrey Vakunov, Ivan Grishchenko, Karthik Raveendran, and Matsvei Zhdanovich. Real-time pupil tracking from monocular video for digital puppetry. June 2020.

[AYM18] Mahdieh Abbaszadegan, Sohrab Yaghoubi, and I. Scott MacKenzie. TrackMaze: A comparison of Head-Tracking, Eye-Tracking, and tilt as input methods for mobile games. In *Human-Computer Interaction. Interaction Technologies*, pp. 393–405. Springer International Publishing, 2018.

[BAS12] Andreas Bulling, Florian Alt, and Albrecht Schmidt. Increasing the security of gaze-based cued-recall graphical passwords using saliency masks. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '12, pp. 3011–3020, New York, NY, USA, May 2012. Association for Computing Machinery.

[BCVO12] Robert Biddle, Sonia Chiasson, and P. C. Van Oorschot. Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys*, Vol. 44, No. 4, September 2012.

[BS00] Sacha Brostoff and M. Angela Sasse. Are passfaces more usable than passwords? a field trial investigation. In *People and Computers XIV — Usability or Else!*, pp. 405–424. Springer London, 2000.

[BZL+13] Cheng Bo, Lan Zhang, Xiang-Yang Li, Qiuyuan Huang, and Yu Wang. SilentSense: silent user identification via touch and movement behavioral biometrics. In *Proceedings of the 19th annual international conference on Mobile computing & networking*, MobiCom '13, pp. 187–190, New York, NY, USA, September 2013. Association for Computing Machinery.

[CMB+20] Grigorios G. Chrysos, Stylianos Moschoglou, Giorgos Bouritsas, Yannis Panagakis, Jiankang Deng, and Stefanos Zafeiriou. P–nets: Deep polynomial neural networks. In *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 7323–7333, June 2020.

[CSZZ15] Yimin Chen, Jingchao Sun, Rui Zhang, and Yanchao Zhang. Your song your way: Rhythm-based two-factor authentication for multi-touch mobile devices. In *2015 IEEE Conference on Computer Communications (INFOCOM)*, pp. 2686–2694. Institute of Electrical and Electronics Engineers, April 2015.

[CTF+19] J. Cao, H. Tang, H. Fang, X. Shen, Y. Tai, and C. Lu. Cross-Domain adaptation for animal pose estimation. In *2019 IEEE/CVF International Conference on Computer Vision (ICCV)*, pp. 9497–9506. Institute of Electrical and Electronics Engineers, October 2019.

[CVR+14] Dietlind Helene Cymek, Antje Christine Venjakob, Stefan Ruff, Otto Hans-Martin Lutz, and Matthias Roetting. Entering PIN codes by smooth pursuit eye movements. *Journal of Eye Movement Research*, Vol. 7, No. 4, pp. 1–11, August 2014.

[CYLWWF+15] Andrew Lim Chee Yeung, Bryan Lee Weng Wai, Cheng Hao Fung, Fiza Mughal, and Vahab Iranmanesh. Graphical password: Shoulder-surfing resistant using falsification. In *2015 IEEE 9th Malaysian Software Engineering Conference (MySEC)*, pp. 145–148. Institute of Electrical and Electronics Engineers, December 2015.

[DACJR05] Antonella De Angeli, Lynne Coventry, Graham Johnson, and Karen Renaud. 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, July 2005.

[DKA19] Heiko Drewes, Mohamed Khamis, and Florian Alt. DialPlates: enabling pursuits-based user interfaces with large target numbers. In *Proceedings of the 18th International Conference on Mobile and Ubiquitous Multimedia*, MUM '19, New York, NY, USA, November 2019. Association for Computing Machinery.

[DLDH09] Alexander De Luca, Martin Denzel, and Heinrich Hussmann. Look into my eyes! can you guess my password? In *Proceedings of the 5th Symposium on Usable Privacy and Security*, No. 7 in SOUPS '09, pp. 1–12, New York, NY, USA, July 2009. Association for Computing Machinery.

[DLWD07] Alexander De Luca, Roman Weiss, and Heiko Drewes. Evaluation of eye-gaze interaction methods for security enhanced PIN-entry. In *Proceedings of the 19th Australasian conference on Computer-Human Interaction: Entertaining User Interfaces*, OZCHI '07, pp. 199–202, New York, NY, USA, November 2007. Association for Computing Machinery.

[DLWHA08] Alexander De Luca, Roman Weiss, Heinrich Hußmann, and Xueli An. Eyepass - eye-stroke authentication for public terminals. In *Proceedings of the 2008 CHI Extended Abstracts on Human Factors in Computing Systems*, CHI EA '08, pp. 3003–3008, New York, NY, USA, April 2008. Association for Computing Machinery.

[DMR04] Darren Davis, F. Monrose, and M. Reiter. On user choice in graphical password schemes. In *Proceedings of the 13th Conference on USENIX Security Symposium*, Vol. 13 of *SSYM '04*, USA, August 2004. USENIX Association.

[DPM+15] Sourav Kumar Dandapat, Swadhin Pradhan, Bivas Mitra, Romit Roy Choudhury, and Niloy Ganguly. ActivPass: Your daily activity is your password. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, pp. 2325–2334, New York, NY, USA, April 2015. Association for Computing Machinery.

[EBFK09] Katherine M. Everitt, Tanya Bragin, James Fogarty, and Tadayoshi Kohno. A comprehensive study of frequency, interference, and training of multiple graphical passwords. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '09, pp. 889–898, New York, NY, USA, April 2009. Association for Computing Machinery.

[EI08] Ali Mohamed Eljetlawi and Norafida Ithnin. Graphical password: Prototype usability survey. In *2008 International Conference on Advanced Computer Theory and Engineering*, pp. 351–355. Institute of Electrical and Electronics Engineers, December 2008.

[FLU+19] Eira Friström, Elias Lius, Niki Ulmanen, Paavo Hietala, Pauliina Kärkkäinen, Tommi Mäkinen, Stephan Sigg, and Rainhard Dieter Findling. Free-Form gaze passwords from cameras embedded in smart glasses. In *Proceedings of the 17th International Conference on Advances in Mobile Computing & Multimedia*, MoMM2019, pp. 136–144, New York, NY, USA, December 2019. Association for Computing Machinery.

[FNS19] Rainhard Dieter Findling, Le Ngu Nguyen, and Stephan Sigg. Closed-Eye gaze gestures: Detection and recognition of Closed-Eye movements with cameras in smart glasses. In *Advances in Computational Intelligence*, IWANN 2019, pp. 322–334, Cham, Switzerland, May 2019. Springer International Publishing.

[FWN+14] Shaojing Fan, Rangding Wang, Tian-Tsong Ng, Cheston Y.-C. Tan, Jonathan S. Herberg, and Bryan L. Koenig. Human perception of visual realism for photo and Computer-Generated face images. *ACM Transactions on Applied Perception*, Vol. 11, No. 2, pp. 1–21, July 2014.

[GVA20] Robert Greinacher and Jan-Niklas Voigt-Antons. Accuracy assessment of ARKit 2 based gaze estimation. In *Human-Computer Interaction. Design and User Experience*, pp. 439–449. Springer International Publishing, 2020.

[GWR+12] Payas Gupta, Tan Kiat Wee, Narayan Ramasubbu, David Lo, Debin Gao, and Rajesh Krishna Balan. HuMan: Creating memorable fingerprints of mobile users. In *2012 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pp. 479–482. Institute of Electrical and Electronics Engineers, 2012.

[HDLS+15] Alina Hang, Alexander De Luca, Matthew Smith, Michael Richter, and Heinrich Hussmann. Where have you been? using location-based security questions for fallback authentication. In *Proceedings of the 11th Symposium On Usable*

Privacy and Security (SOUPS 2015), pp. 169–183, Ottawa, July 2015. USENIX Association.

[HHFM17] Daniel Hintze, Philipp Hintze, Rainhard D. Findling, and René Mayrhofer. 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, June 2017.

[Jac90] Robert J. K. Jacob. What you look at is what you get: eye movement-based interaction techniques. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '90, pp. 11–18, New York, NY, USA, March 1990. Association for Computing Machinery.

[Jac91] Robert J. K. Jacob. The use of eye movements in human-computer interaction techniques: what you look at is what you get. *ACM Transactions on Information and System Security*, Vol. 9, No. 2, pp. 152–169, April 1991.

[JGK+03] Wayne Jansen, Serban Gavrila, Vlad Korolev, Rick Ayers, and Ryan Swanstrom. Picture password: A visual login technique for mobile devices. Technical Report 7030, National Institute of Standards and Technology Interagency Report, Gaithersburg, MD, July 2003.

[KAB18] Mohamed Khamis, Florian Alt, and Andreas Bulling. The past, present, and future of gaze-enabled handheld mobile devices: survey and lessons learned. In *Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services*, MobileHCI '18, pp. 1–17, New York, NY, USA, September 2018. Association for Computing Machinery.

[KAR+20] Christina Katsini, Yasmeen Abdrabou, George E. Raptis, Mohamed Khamis, and Florian Alt. The role of eye gaze in security and privacy applications: Survey and future HCI research directions. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, pp. 1–21, New York, NY, USA, April 2020. Association for Computing Machinery.

[KGBW07] Manu Kumar, Tal Garfinkel, Dan Boneh, and Terry Winograd. Reducing shoulder-surfing by using gaze-based password entry. In *Proceedings of the 3rd symposium on Usable privacy and security*, SOUPS '07, pp. 13–19, New York, NY, USA, July 2007. Association for Computing Machinery.

[KHZ+17] Mohamed Khamis, Mariam Hassib, Emanuel Von Zezschwitz, Andreas Bulling, and Florian Alt. GazeTouchPIN: protecting sensitive data on mobile devices using secure multimodal authentication. In *Proceedings of the 19th ACM International*

Conference on Multimodal Interaction, ICMI '17, pp. 446–450, New York, NY, USA, November 2017. Association for Computing Machinery.

[KKK+16] K. Krafka, A. Khosla, P. Kellnhofer, H. Kannan, S. Bhandarkar, W. Matusik, and A. Torralba. Eye tracking for everyone. In *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 2176–2184. Institute of Electrical and Electronics Engineers, June 2016.

[KPR16] Rajesh Kumar, Vir V. Phoha, and Rahul Raina. Authenticating users through their arm movement patterns. Vol. abs/1603.02211, pp. 1–25. Cornell University, March 2016.

[Kuc06] Andreas Kuckertz. Strategies of competition in the bank card business. *Technovation*, Vol. 26, No. 7, p. 820, July 2006.

[LTN+19] Camillo Lugaresi, Jiuqiang Tang, Hadon Nash, Chris McClanahan, Esha Uboweja, Michael Hays, Fan Zhang, Chuo-Ling Chang, Ming Guang Yong, Juhyun Lee, Wan-Teh Chang, Wei Hua, Manfred Georg, and Matthias Grundmann. MediaPipe: A framework for building perception pipelines. In *Proceedings of the 3rd Workshop on Computer Vision for AR/VR at IEEE Computer Vision and Pattern Recognition (CVPR) 2019*. Institute of Electrical and Electronics Engineers, June 2019.

[ML07] Wendy Moncur and Grégory Leplâtre. Pictures at the ATM: exploring the usability of multiple graphical passwords. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '07, pp. 887–894, New York, NY, USA, April 2007. Association for Computing Machinery.

[MMC+18] Alexander Mathis, Pranav Mamidanna, Kevin M. Cury, Taiga Abe, Venkatesh N. Murthy, Mackenzie Weygandt Mathis, and Matthias Bethge. DeepLabCut: markerless pose estimation of user-defined body parts with deep learning. *Nature Neuroscience*, Vol. 21, No. 9, pp. 1281–1289, September 2018.

[MMDB21] Olga Moskvyak, Frederic Maire, Feras Dayoub, and Mahsa Baktashmotlagh. Semi-supervised keypoint localization. In *Proceedings oh the 9th International Conference on Learning Representations (ICLR)*. OpenReview, January 2021.

[MRRT17] Ivan Martinovic, Kasper Rasmussen, Marc Roeschlin, and Gene Tsudik. Authentication using pulse-response biometrics. *Communications of the ACM*, Vol. 60, No. 2, pp. 108–115, January 2017.

[NWL+16] Natalia Neverova, Christian Wolf, Griffin Lacey, Lex Fridman, Deepak Chandra, Brandon Barbello, and Graham Taylor. Learning human identity from motion patterns. *IEEE Access*, Vol. 4, pp. 1810–1820, 2016.

[PLH17] Alexandra Papoutsaki, James Laskey, and Jeff Huang. SearchGazer: Webcam eye tracking for remote studies of web search. In *Proceedings of the 2017 Conference on Conference Human Information Interaction and Retrieval*, CHIIR '17, pp. 17–26, New York, NY, USA, March 2017. Association for Computing Machinery.

[PPC21] Joonbeom Park, Seonghoon Park, and Hojung Cha. GAZEL: Runtime gaze tracking for smartphones. In *2021 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pp. 1–10. Institute of Electrical and Electronics Engineers, March 2021.

[Pra93] Lorien Y. Pratt. Discriminability-Based transfer between neural networks. In S. J. Hanson, J. D. Cowan, and C. L. Giles, editors, *Proceedings of the 5th International Conference on Neural Information Processing Systems*, Vol. 5 of *NIPS '92*, pp. 204–211, San Francisco, CA, USA, November 1993. Morgan Kaufmann Publishers Inc.

[PSL+16] Alexandra Papoutsaki, Patsorn Sangkloy, James Laskey, Nediyana Daskalova, Jeff Huang, and James Hays. Webgazer: scalable webcam eye tracking using user interactions. In *Proceedings of the Twenty-Fifth International Joint Conference on Artificial Intelligence*, IJCAI'16, pp. 3839–3845. AAAI Press, July 2016.

[RH09] Räihä, Kari-Jouko and Heikkilä, Henna. Speed and accuracy of gaze gestures. *Journal of Eye Movement Research*, Vol. 3, No. 2, pp. 1–14, November 2009.

[RPTH17] Vijay Rajanna, Seth Polsley, Paul Taele, and Tracy Hammond. A gaze Gesture-Based user authentication system to counter Shoulder-Surfing attacks. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, CHI EA '17, pp. 1978–1986, New York, NY, USA, May 2017. Association for Computing Machinery.

[Sam21] 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.

[San04] Marie Sandström. *Liveness Detection in Fingerprint Recognition Systems*. PhD thesis, Linköping University, Linköping Sweden, June 2004.

[SDHS15] Nathan Shone, Chelsea Dobbins, William Hurst, and Qi Shi. Digital memories based mobile user authentication for IoT. In *2015 IEEE International Conference*

on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, pp. 1796–1802. Institute of Electrical and Electronics Engineers, October 2015.

[SG00] Dario D. Salvucci and Joseph H. Goldberg. Identifying fixations and saccades in eye-tracking protocols. In *Proceedings of the 2000 symposium on Eye tracking research & applications*, ETRA '00, pp. 71–78, New York, NY, USA, November 2000. Association for Computing Machinery.

[SK19] Syed W. Shah and Salil S. Kanhere. Recent trends in user authentication – a survey. *IEEE Access*, Vol. 7, pp. 112505–112519, 2019.

[SMB10] Mojtaba Sepasian, Cristinel Mares, and Wamadeva Balachandran. Liveness and spoofing in fingerprint identification: issues and challenges. In *Proceedings of the 4th WSEAS international conference on Computer engineering and applications*, CEA'10, pp. 150–158, Stevens Point, Wisconsin, USA, January 2010. World Scientific and Engineering Academy and Society (WSEAS).

[SZZZ14] Jingchao Sun, Rui Zhang, Jinxue Zhang, and Yanchao Zhang. TouchIn: Sightless two-factor authentication on multi-touch mobile devices. In *2014 IEEE Conference on Communications and Network Security*, pp. 436–444. Institute of Electrical and Electronics Engineers, October 2014.

[TMSA13] Julie Thorpe, Brent MacRae, and Amirali Salehi-Abari. Usability and security evaluation of GeoPass: a geographic location-password scheme. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, No. Article 14 in SOUPS '13, pp. 1–14, New York, NY, USA, July 2013. Association for Computing Machinery.

[TPL20] Mingxing Tan, Ruoming Pang, and Quoc V. Le. EfficientDet: Scalable and efficient object detection. In *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 10778–10787, Seattle, WA, USA, June 2020. Institute of Electrical and Electronics Engineers.

[VDS+20] Nachiappan Valliappan, Na Dai, Ethan Steinberg, Junfeng He, Kantwon Rogers, Venky Ramachandran, Pingmei Xu, Mina Shojaeizadeh, Li Guo, Kai Kohlhoff, and Vidhya Navalpakkam. Accelerating eye movement research via accurate and affordable smartphone eye tracking. *Nature Communications*, Vol. 11, No. 1, p. 4553, September 2020.

[VHCR20] Simon Voelker, Sebastian Hueber, Christian Corsten, and Christian Remy. HeadReach: Using head tracking to increase reachability on mobile touch devices.

In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, pp. 1–12, New York, NY, USA, April 2020. Association for Computing Machinery.

[VHH+20] Simon Voelker, Sebastian Hueber, Christian Holz, Christian Remy, and Nicolai Marquardt. GazeConduits: Calibration-Free Cross-Device collaboration through gaze and touch. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, pp. 1–10, New York, NY, USA, April 2020. Association for Computing Machinery.

[WWB+05] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. PassPoints: design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies*, Vol. 63, No. 1-2, pp. 102–127, July 2005.

[XEZ+15] Pingmei Xu, Krista A. Ehinger, Yinda Zhang, Adam Finkelstein, Sanjeev R. Kulkarni, and Jianxiong Xiao. TurkerGaze: Crowdsourcing saliency with webcam based eye tracking. April 2015.

[XYL+20] Zhihua Xia, Chengsheng Yuan, Rui Lv, Xingming Sun, Neal N. Xiong, and Yun-Qing Shi. 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, April 2020.

[YLX15] Junshuang Yang, Yanyan Li, and Mengjun Xie. MotionAuth: Motion-based authentication for wrist worn smart devices. In *2015 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pp. 550–555. Institute of Electrical and Electronics Engineers, March 2015.

[YSW19] Chengsheng Yuan, Xingming Sun, and Q. M. Wu. Difference co-occurrence matrix using BP neural network for fingerprint liveness detection. *Soft Computing*, Vol. 23, No. 13, pp. 5157–5169, July 2019.

[ZBHW14] Nan Zheng, Kun Bai, Hai Huang, and Haining Wang. You are how you touch: User verification on smartphones via tapping behaviors. In *2014 IEEE 22nd International Conference on Network Protocols*, pp. 221–232. Institute of Electrical and Electronics Engineers, October 2014.

[ZYK+18] Xiang Zhang, Lina Yao, Salil S. Kanhere, Yunhao Liu, Tao Gu, and Kaixuan Chen. 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, September 2018.

著者論文リスト

本論文に関する論文

本論文の主内容は，下記の論文にて公表済みである．

査読付き国際会議論文

1. Yuki Yamato and Shin Takahashi. 2021. Gaze-Based Authentication Method Using Graphical Passwords Featuring Keypoints. In Proceedings of the 33rd Australian Conference on Human-Computer Interaction (OzCHI '21), ACM, New York, NY, USA. to appear.

その他論文

査読付き国際会議論文

1. Yuki Yamato, Yutaro Suzuki, Kodai Sekimori, Buntarou Shizuki, and Shin Takahashi. 2020. Hand Gesture Interaction with a Low-Resolution Infrared Image Sensor on an Inner Wrist. In Proceedings of the International Conference on Advanced Visual Interfaces (AVI '20). ACM, New York, NY, USA, Article 58, 5 pages.

2. Yutaro Suzuki, Kodai Sekimori, Yuki Yamato, Yusuke Yamasaki, Buntarou Shizuki, and Shin Takahashi. A Mouth Gesture Interface Featuring a Mutual-Capacitance Sensor Embedded in a Surgical Mask. 2020 In Proceedings of The 22nd International Conference on Human-Computer Interaction (HCI International 2020). Springer. Multimodal and Natural Interaction, 154–165.

3. Yuki Yamato, Yutaro Suzuki, and Shin Takahashi. 2021. FGFlick: Augmenting Single-Finger Input Vocabulary for Smartphones with Simultaneous Finger and Gaze Flicks. In Proceedings of 18th IFIP TC 13 International Conference on Human-Computer Interaction − INTERACT 2021, Springer. LNCS 12936, pp. 421–425.

4. Takumi Kitagawa, Yuki Yamato, Buntarou Shizuki, and Shin Takahashi. 2019. A Viewpoint Control Method for 360° Media Using Helmet Touch Interface. In Proceedings of the Sym-

posium on Spatial User Interaction (SUI '19). ACM, New York, NY, USA, Article 33, 2 pages.