2ZD-05

# AR による PIN 認証システムの開発と評価

朝倉航† 藤川真樹†
工学院大学†

## 1 はじめに

スマートグラスに搭載されているカメラ，透過型ディスプレイ，無線通信機能を利用した業務支援システムがある[1]．当該システムがあらゆる業種・業務で使用されるようになり，勤務時間中にスマートグラスをかける時間が，デスクワークでキーボードやマウスを操作する時間よりも長くなることを想像する．この場合，セキュリティ上の観点（従業員以外の人による目的外使用の防止など）から，スマートグラスの着用者が従業員本人か否かをチェックする機能（本人認証機能）が必要となる．

スマートグラスの本人認証機能は「利便性の向上」をもたらす．たとえば本人であることが認証されており，スマートグラス着用中であれば，タッチレス操作によりフラッパーゲートを通過させることや社用車を運転させたりすることが可能となる．一方で，セキュリティレベルの高い場所に従業員がアクセスしようとしている時には，アクセス制御のためにディスプレイ上に別の本人認証方法を表示することにより「セキュリティの向上」が図れる．

本稿では，スマートグラスに見立てたプロトタイプをベースとして，AR 技術[2]により空中で PIN（Personal Identification Number）を入力できる本人認証システムを開発し，その性能を評価する．

## 2 プロトタイプの構成

### 2.1 概要

プロトタイプの全体図を図 1 に示す．プロトタイプは web カメラ，モニター，アプリケーションから構成される（web カメラとモニターは，それぞれスマートグラスに搭載されているカメラと透過型ディスプレイに見立てる）．

モニターには web カメラが捉えている映像に加えて，PIN を入力するための仮想テンキーをオーバーラップして表示する（これにより web カメラの画角内に手指を入れることで，仮想テンキーを操作できる）．アプリケーションは，入力された PIN の正誤をチェックし，本人か否かを

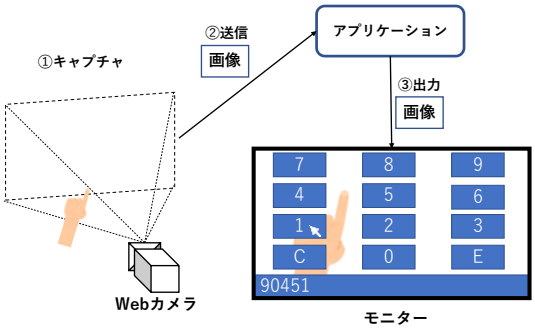


図 1 プロトタイプ全体（概要）

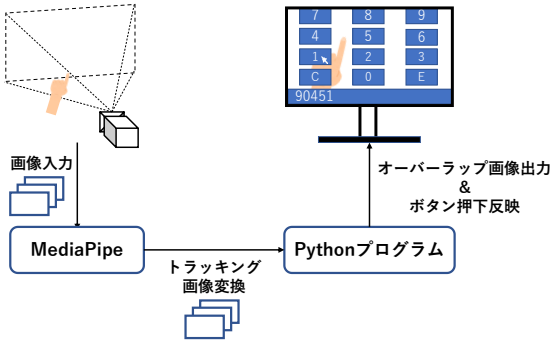


図 2 アプリケーション（概要）

判定する．アプリケーションは PyCharm（Python の統合開発環境），MediaPipe のハンドソリューション，Python 言語，Kivy 言語によって構築される．

### 2.2 パスワード入力の実現方法

アプリケーションの概要を図 2 に示す．アプリケーションは仮想テンキーをモニターに表示するが，同時に web カメラの画角に入った手指を認識し，これらをモニターに表示しつつリアルタイムにトラッキングする（具体的には，人差し指の指先と第 2 関節に注目し，その動きを追跡する）．第 2 関節とモニター上のカーソルが連動し，カーソルが仮想テンキー上の任意のボタン上にある状態で，指先が第 2 関節よりも下に位置したときに，当該ボタンが押下されたものと認識する．

Python プログラムと MediaPipe の関係を概説する．ハンドトラッキングは MediaPipe によって実行される．Python プログラムはトラッキング中の画像を仮想テンキーにオーバーラップさせる形で出力する．また，当該プログラムは指先によって押下されたボタンに対応する数字をテキストとして出力する．出力されたテキスト

---

Development and Evaluation of the AR-based PIN Authentication System
†Wataru Asakura & Masaki Fujikawa, Kogakuin Univ.

を時系列に並べることによりパスワードが形成される．さらに，C ボタンを押下することでテキストを新しいものから 1 つずつ削除するため，パスワード入力時に誤ってボタンを押した場合でも素早い修正が可能となる．

## 3 実験

事前に，実験者が 5 桁の PIN を空中で入力している様子を正面から録画した動画（10 本）を用意する．動画は 2 種類ある．（1 つは実験者が PIN を正確に入力できたものである．もう 1 つは PIN が正確に入力できなかったために C ボタンを押下したか，またはアプリケーションがボタンの押下を検知できなかったために，実験者がボタンを再押下した様子が含まれているものである．前者を「ミスなし」，後者を「ミスあり」と呼ぶ）．実験 1 では，テンキーの配置を図 1 と同じにし，実験 2 ではテンキーの配置をランダムにした．被験者（9 人）は，各動画を視聴する毎にパスワードを推測・回答する．

はじめに実験 1 の結果を表 1 に示す．全体的に見ると「45658」の正答率が 6 割を超える結果となった．これは，(1)「ミスなし」であったために推測が容易であったこと，(2)他のパスワードの入力よりも指の動きが単純（縦と横のみ）であったことが理由として考えられる．

表 1　実験 1 の結果

| | ミスなし | ミスあり |
|---|---|---|
| 数字 | 正答率[%] | 正答率[%] |
| 09172 | 0 | 0 |
| 70341 | 0 | 0 |
| 52134 | 0 | 11.1 |
| 19370 | 0 | 0 |
| 45658 | 66.7 | 0 |
| 79130 | 0 | 22.2 |
| 88499 | 11.1 | 0 |
| 36710 | 0 | 0 |
| 08546 | 0 | 0 |
| 54440 | 0 | 0 |

表 2　実験 2 の結果

| | ミスなし | ミスあり |
|---|---|---|
| 数字 | 正答率[%] | 正答率[%] |
| 06138 | 0 | 0 |
| 12369 | 0 | 0 |
| 77235 | 0 | 0 |
| 53981 | 0 | 0 |
| 93344 | 0 | 0 |
| 24781 | 0 | 0 |
| 80301 | 0 | 0 |
| 32740 | 0 | 0 |
| 68724 | 0 | 0 |
| 49222 | 0 | 0 |

つぎに実験 2 の結果を表 2 に示す．全被験者が「ミスあり」「ミスなし」ともに PIN を見破れなかったことがわかる．これは，テンキーの配置が分かっている実験 1 よりも推測困難になったことが理由として考えられる．

## 4 考察

### 4.1 ユーザビリティ

被験者に対して，プロトタイプのユーザビリティに関するアンケートを実施した．アンケートは 6 つの指標（「操作性」「利便性」「正確性」「効率性」「記憶しやすさ」「主観的満足度」）からなり，これらに基づいて質問紙を作成した．回答者（12 人）は，ユーザの立場からプロトタイプを操作（PIN 入力）したあとに質問紙に回答した．その結果，「利便性」「効率性」「記憶しやすさ」「主観的満足度」の 4 点においては 7 割以上の回答者からポジティブな回答があり，当該指標において有効であることが分かった．一方，「操作性」については 4 割の，「正確性」においては 5 割以上の回答者からネガティブな回答があった．これは，web カメラの映像やアプリケーションがフリーズすることが原因である．このため，「システムの処理を軽くしてフリーズを抑える」という対応を図る予定である．

### 4.2 PIN を推測困難にする方法

仮想テンキーよりも PIN の推測を困難にする方法として，金庫の解錠に用いられるダイヤルをディスプレイ上に表示することを提案する．「攻撃者はディスプレイに表示されるダイヤルを視認できない」と仮定した場合，ダイヤルの数字や回転度合いを推測するのは困難である．なお，セキュリティレベルに応じてダイヤルの位置や個数を変化させることにより，PIN 推測の難易度を調整できる．

## 5 まとめ

著者は，AR 技術により空中で PIN を入力できるプロトタイプの開発と評価を行った．PIN 入力は，指先をハンドトラッキングすることによって実現できる．プロトタイプは，テンキーの配置がランダムであれば PIN の推測は困難であり，6 つのうちの 4 つの指標を満足している．

参考文献

[1] 森田健太郎，長田剛典，佐藤健哉，“指動作認識を利用したスマートグラス上のユーザインターフェイス操作”，“マルチメディア，分散協調とモバイルシンポジウム 2016 論文集”，2016 巻，pp.866-871，July 2016.
[2] Dieter Schmalstieg，Tobias Höllerer，AR の教科書，マイナビ出版，東京，2018.