Vol.2021-MBL-101 No.13
Vol.2021-ITS-87 No.13
2021/12/7

顔認証動作の特徴を用いたスマートフォンの顔認証手法

小野寺晃希[1]　鈴木孝幸[1]　清原良三[1]

概要：COVID-19 の流行によって，感染防止の観点から外出先でのマスク着用時におけるスマートフォンの顔認証が容易に利用できなくなった．顔認証を行うためにマスクを一時的に外す，あるいは下げることで認証可能であるが，ウイルス感染の可能性が上昇するため推奨できない．マスクを着用していない状態の顔認証では，顔全体を認証に利用できるが，マスクを着用した状態の顔認証では顔の大部分が覆われて隠れてしまうため，本人受け入れ率が減少，あるいは他人受け入れ率が上昇すると予測できる．そこで，マスクで隠れていない目の部分の特徴と，顔認証を行う際の動作から得られる端末の加速度や角度の特徴を組み合わせることでマスクを着用した状態でマスクを着用していない状態と同じように顔認証を行えるシステムを提案する．本論文では，提案手法を実際に評価するため，あらかじめ登録したマスクで覆われていない目の部分の顔画像データとスマートフォンのフロントカメラに映った目の部分を特徴点マッチングを行うことで顔の類似度計算を行い，マスクの影響で欠損した状態の顔画像でどの程度の精度が得られるかを検証した．今後は，顔認証を行う動作から得られる加速度データを用いた機械学習結果の検証を行い，本人認証に有効か検証する．

1. はじめに

スマートフォンをはじめとした携帯端末の普及率は年々増加しており，2019 年度における世帯別スマートフォン保有率は 83.4%と 8 割を超え，人々の生活に欠かせないものとなってきている．対して 2019 年度における世帯別 PC 保有率は 69.1 %とスマートフォンの利用者が上回っている [1]．PC はデスクトップ型やノート PC などの種類があり，持ち歩いたその場で簡単に利用できない特性を持つ．

しかしスマートフォンは持ち運びが容易であることと，持ち歩いたその場で簡単に利用できる特性から強固なセキュリティ対策を講じる必要がある．またスマートフォンには数多くの個人情報やビジネスなどにかかわる重要な情報が蓄積されていることや金銭の授受などの重大な手続きを行うことができることからも，他人の不正利用を防ぐ手段が日々模索されている．

現在のスマートフォンの本人認証手法には，数値や英単語を組み合わせるパスコード認証や，9 つの点から 4 つ以上を選び一筆書きで結ぶパターン認証，指紋・顔などの身体的特徴を用いる生体認証などが存在する．生体認証である指紋認証や顔認証は身体的特徴を用いているためユーザがパスワードを打たなくていいことや，パターンを記憶する必要がないことによってユーザビリティが高い．また端末以外の機械を使用しないことで紛失の恐れがないことや，パスワードを盗み見られることがないことからも安全で利用しやすく、近年では生体認証が多くのスマートフォンで実装されている．

しかし，昨今の COVID-19 の影響で人々はマスクを着用した生活を余儀なくされるようになったことにより，以前まで利用できていた顔認証がマスクによる顔情報の欠損によって利用が困難になった．この問題に対して多くの企業がマスクを着用した状態で顔認証を行えるシステムを開発している．例としてはオフィスに設置される入退室管理システムなどである [2]．しかしこれらシステムはスマートフォン向けに開発されたわけではなく，要求されるスペックがスマートフォンとは異なるためスマートフォン利用者は依然として不便さを被っている．

マスクを外さずにスマートフォンのロックを解除できる仕組みとして，Apple は自社で開発しているスマートフォンである iPhone で iOS14.5 のバージョンから同社のウェアラブル端末である AppleWatch と連携することでマスクを着用した状態でスマートフォンのロックを解除する機能を追加した．しかしウェアラブル端末が必要なことから所持していないユーザは依然不利益を被っている状態が続いている．またマスクを着用していれば本人以外でもスマートフォンのロックが解除可能である [3].

そこで，本論文では生体認証のようにユーザが数値やパターンを記憶することなく，スマートフォンのみで，マス

[1] 神奈川工科大学
Kanagawa Institute of Technology

クを着用した状態でもマスクを着用していない状態と同じように，特別な操作をすることなく，同精度の顔認証を行えるシステムを提案する．具体的には，顔認証のために動かす操作の行動特性と，マスクで隠れてない部分の情報を組み合わせる手法を提案する．

2. 関連研究

これまでにも本人認証に関する研究は様々行われている．認証方式は大きくは以下の 3 つの方式に分けられる．

- 所持情報認証
- 生体認証
- 知識情報認証

多くの場合は，この中の 2 点を組み合わせる多要素認証を採用している．スマートフォンの場合は，所持していることと，生体情報または知識情報の認証のどちらかを組み合わせていることになる．自動車の場合は，キーを所持しているだけでの認証であり，個人情報が含まれるかどうかの違いや，持ってるだけで悪意を持った利用ができるどうかの違いなどに依存すると考えられる．

これらの中でも生体認証はその精度が問題であり，数多くの研究が実施されている．また知識情報認証は，盗み見など知識の盗難に弱い側面があり，注意喚起を含んだ対策の研究が実施されてきた．本論文では，生体情報の認証に関する関連研究および実用化されている技術を中心に紹介しその課題を整理する．

富士通 (株) ではマスク非着用の顔画像にマスクを付加した画像を生成し，学習させることで，マスク着用時でも非着用時と同等レベルの精度を得ることができた．様々な色や柄，形のマスクに対応するため，多様なタイプのマスクを付加し，マスクを外すことなく認証でき，マルチ認証が衛生的に使うことができるようにしたと発表している [4]．

日本電気 (株) ではマスク着用を検出してマスクで覆われていない目の周辺の特徴を捉えて照合を行う Bio-IDiom と呼ぶ生体認証のシステムを開発し公表している同社はこのシステムでマスク着用時で認証率 99.9%以上の精度を実現している．しかしどちらのシステムもスマートフォン向けに開発されていないことが課題である [5]．

世界でも，米国国立標準技術研究所 (NIST:National Institute of Standards and Technology) も FRVT(Face Recognition Verification Test) で，マスク付きでのアルゴリズムのテストを行うなど重要性が認識されている [6]．

しかし，スマートフォンで解決できる手法ではない．そこで行動といった動作の特徴と組み合わせる手法を検討することとした．

行動認証は人間の動きの習性を機械学習で解析，学習し本人認証を行うものである．石原らの提案 [7] は，手に持った携帯端末の動きから個人的な動作特徴を抽出することによって認証を行うものである．この手法は端末に搭載された加速度センサから加速度を抽出し，端末を動かす速度やタイミングなどを特徴とし本人認証に利用する．手首のひねりや回転などの微妙な動きは肉眼でとらえることが難しく，たとえ他人に認証動作を見られたとしても，なりすましによって不正利用される危険性は低い．

今野らの提案 [8] はスマートフォンをポケットにしまった状態で歩行することで得られる継続的な加速度データを認証に用い，利用する際に自動的に端末のロックを解除する手法である．この手法は日常的に無意識に行っている歩行動作を認証に利用するため，ユーザが認証に覚える要素がないことや他人からのなりすましの危険性が低いことにより高い精度を誇っている．しかし実験では屋内の平坦かつ直線状の廊下であったことから，天候や地形，人の混雑度，その日の体調により認証精度が低くなることが考えられる．

そこで組み合わせる手法に関する基礎検討として，我々の研究グループでも，加速度データから本人認証に有効である特徴について検証，評価している [9]．加速度データで本人認証に有効である特徴は最大値後の最大傾き値であり，データをいくつかのクラスタ群に分け，どこのグループに属するかの結果を返す手法が有効であると導いた．また，生体認証を複数組み合わせることで，精度を向上するといった研究も実施されており [10]，有効な手法だと考えられる．そこで，本論文ではスマートフォンでの実現手法を提案し，その基礎的な評価を行うこととした．

3. 提案手法

本論文ではスマートフォン単体でマスクを着用した状態で，かつジェスチャーなどの特別な動作をすることなく顔認証を行えるシステムを提案する．

具体的には，マスクで覆われていない目の部分の画像データを端末のストレージに登録しておき，登録されている画像データとスマートフォンのフロントカメラに映った目の部分を特徴点マッチングを行うことで顔の類似度計算を行う．加速度の類似度計算については，学習データとして何度か加速度を計測し端末に登録しておく．端末を身体の側面から顔の前に運び，顔認証を行う際の動作から加速度や角度を抽出し，機械学習を行う．この 2 つの計算を組み合わせることで本人認証を行う．処理の概要を**図 1** に示す．また，**図 2** に提案手法のフローチャートを**図 3** に動作イメージを示す．このように個々の認証アルゴリズムにおいて評価値を計算し，トータルでの再度評価を行う．

ここで，顔認証で評価を行い，その認証をパスしたものについてのみ，動作での認証を行う方式と，個々の評価を別に行うトータルで評価を行う方式の複数が考えられる．ここでは，その検討を行ったことを目的に基礎実験を行うこととする．

Vol.2021-MBL-101 No.13
Vol.2021-ITS-87 No.13
2021/12/7

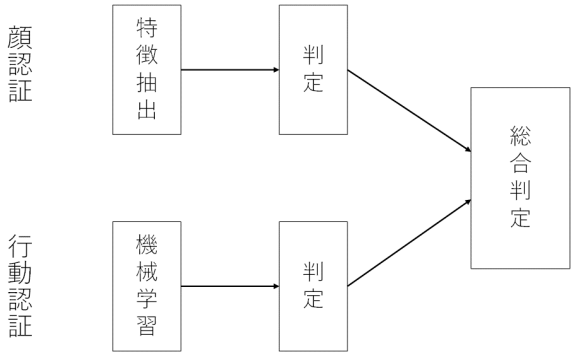

図 1 提案手法の概要

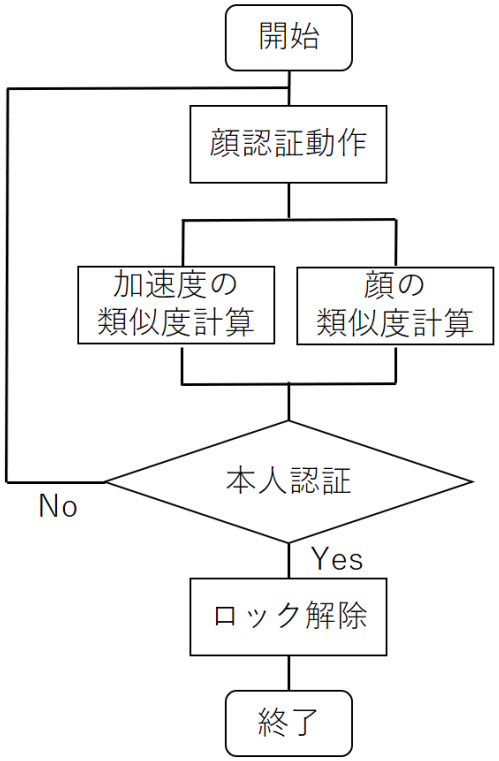

図 2 提案手法のフローチャート

3.1 顔認証処理

顔の特徴点抽出また特徴点マッチングにはオープンソースのコンピューター・ビジョン・ライブラリである OpenCV[11](Open Source Computer Vision Library) に実装されている画像の特徴点を検出する手法でである AKAZE[12] を用いる．AKAZE は，特徴点抽出と特徴量記述を行う手法である．AKAZE は SIFT[13] や SURF[14] などのほかの手法と比べ処理速度が速く，オブジェクトのスケール変化，回転，照明変化にロバスト性を持っている．AKAZE を用いた特徴点マッチングのイメージ図を図 **4** に

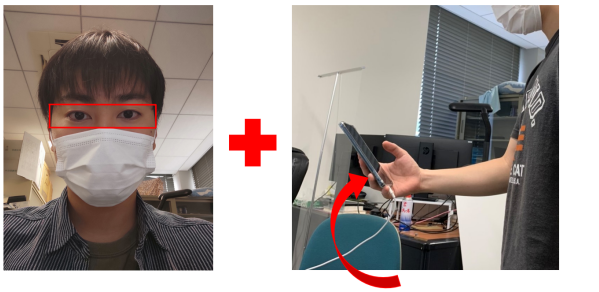

図 3 提案手法の動作イメージ

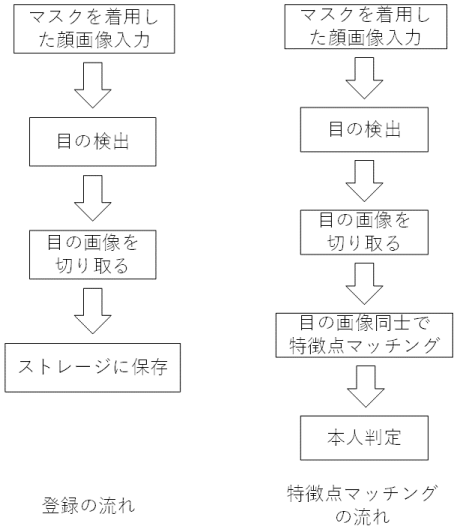

図 4 特徴点マッチングのイメージ

図示する．特徴点マッチングでは目の同じ位置同士が対応することが重要である．

3.2 動作認証処理

加速度データは Android スマートフォンに搭載された加速度センサから取得することとする．加速度センサのデータを取得し，取得した加速度データをもとに機械学習を行う．機械学習には Python のライブラリである scikit-learn[15] を用い，分類アルゴリズムである SVM によって類似度を計算する．端末を顔の前に持って来た時の加速度データの例を図 **5** に示す．

4. 基礎実験

本論文で示した提案を評価するため Python で特徴点マッチングのプログラムを作成し実験を行った．被験者は同大学の男子学生 5 名と女子学生 1 名である．**表 1** に被験者 6 人の情報を示す．また特徴点マッチングを行う際に精度に影響を及ぼすと考えられる眼鏡を着用しているのは被験者 C と被験者 E である．実験の準備として男子学生 5 名に 2 回，正面を向いた状態の顔が映った動画を 10 秒程

Vol.2021-MBL-101 No.13
Vol.2021-ITS-87 No.13
2021/12/7

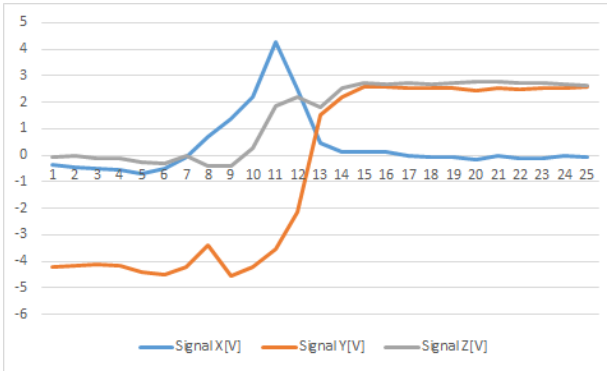

図 5　端末の加速度データ

表 1　被験者 6 人の情報

被験者	性別	眼鏡着用有無
A	男	無
B	男	無
C	男	有
D	男	無
E	男	有
F	女	無

度撮影してもらった．女子学生には 1 回，正面を向いた状態の顔が映った動画を 10 秒程度撮影してもらった．

特徴点マッチングを行い本人認証を行う流れを**図 6** に示す．目の画像同士で特徴点マッチングを行うため，マスクを着用した顔画像から両目を検出し，その部分の切り取りを行うことで両目のみの画像を取得する．端末にあらかじめ登録しておく目の画像もこの手法でストレージに保存し，本人認証を行う際，目の画像を切り取ることで，目の画像同士の特徴点マッチングを行うことができる．両

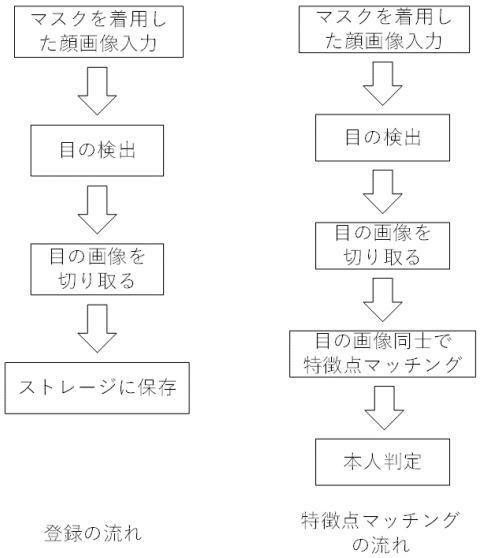

図 6　特徴点マッチングの流れ

表 2　男子学生 5 名の FAR,FRR

被験者	FAR	FRR
A	4%	0%
B	7%	0%
C	0%	0%
D	4%	1%
E	0%	24%

表 3　女子学生の FAR,FRR

被験者	FAR	FRR
F	2%	2%

目の検出には OpenCV の Haar-Cascades[16] を利用した．Haar-Cascades とは，カスケード分類器という検出したい物体が対象物かを判別するために基準となるファイルを用いて対象物を検出する機械学習の一つの手法である．カスケード分類器は顔や目などを検出できる学習済みファイルが事前に用意されている．今回は用意された両目を検出できるカスケード分類器を用いて実験を行った．

撮影してもらった動画を 1 フレームごとに分割し Haar-Cascades を行うことで，男子学生それぞれ 200 枚，女子学生は 100 枚の両目のみの画像データを取得することができた．男子学生は 100 枚を登録データとしてストレージに保存しておき，残りの 100 枚を入力データとして実験を行った．女子学生は 50 枚をストレージに保存しておき，残りの 50 枚を入力データとして実験を行った．実験結果として男性の他人受入れ率 FAR と本人拒否率 FRR を**表 2** に示す．女子学生である被験者 F に関しては FAR を評価するため，インターネット上に公開されている東洋人顔画像データセット [17] から女性の顔画像 100 枚を利用し，結果を**表 3** に示す．

5.　考察

表 2, 表 3 の実験結果より，眼鏡を着用している被験者 C，E は FAR が 0%となっていることがわかる．これは眼鏡を着用していない，または，違う色，形の眼鏡を着用している人物が認証を行ったとき，特徴点の距離が遠くなることで認証が失敗するからだと考えられる．このことから同じ眼鏡，または似た色，形の眼鏡を着用した人物が認証を行ったとき認証が通ってしまう可能性があると考えられる．同じ眼鏡を着用した際の実験も今後行う必要性がある．ほかの被験者の FAR は 2〜7%となっており，最も高かった被験者 B は 7%と大体 10 回に 1 回他人を受け入れる結果となった．これは両目のみでは認証に利用できる特徴点が少ないからだと考えられる．

FRR に関しては，被験者 A〜D は 0%や 1%であるが，

被験者 E は 24%と高い結果となった．これは明度の違いによるものだと考えられる．被験者 E の特徴点マッチングで比較した目の画像を**図 7** に示す．左の画像は全体的に暗いのに対し，右の画像は照明が当たり全体的に明るいことがわかる．0%となった被験者 A の目の画像は図 4 のようにやや右が明るく見えるが大きな明度の違いは見られない．このことから，極端な明度の差がある場合，FRR が大きくなると考えられる．対策として，特徴点マッチングで比べる画像同士の明度を均一化するなどの手法が考えられる．

また表 3 から画像データセットを用い，100 枚の様々な目の画像で FAR を検証した. 結果，FAR は 2%であったがデータセットの画像は様々な環境や顔の角度から撮影されたものであり，ほとんどの画像で認証は失敗したが，1 回認証に成功してしまった．似た明度や目の特徴点が近いものが誤って認証を通ってしまうと考えられる．FRR は 2%という結果となった．女子学生は画像データが男子学生より少なかったため，男子学生より FRR はやや高くなったと考えられる．このことから，データ数が多くなれば精度は上がることが分かった．しかしデータ数が増えれば増えるほど処理に時間がかかるため，本人認証時に処理時間がかかりすぎないデータ数を探す必要がある．

マスクを着用していない顔認証ではほぼ 100%の精度であるのに対し，両目のみの顔認証では数パーセントの確率で認証が通らないことが分かった．また，明るすぎる画像で特徴点マッチングを行ったとき FRR が上がったことにより極端な明度が精度に影響することが分かった．FAR についても被験者 6 名のうち最大で 7%他人を受け入れてしまった．今回の実験では，被験者 6 名の全員に正面を向いた顔を撮影してもらったため，顔の角度をつけた場合は，今回の実験結果より精度が下がることが考えられる．角度が違う場合も FAR また FRR が高くならない対策や，今後行う予定である，端末の加速度による本人認証を組み合わせることで，精度を落とさないようにする必要がある．

6. おわりに

本論文では，マスクで覆われていない顔の特徴である両目と顔認証を行う際の動作から得られる端末の加速度や角度の特徴を組み合わせることでマスクを着用した状態でマスクを着用していない状態と同じように顔認証を行えるシステムを提案した．提案手法を実際に評価するため，あらかじめ登録したマスクで覆われていない目の部分の顔画像データとスマートフォンのフロントカメラに映った目の部分を特徴点マッチングを行うことで顔の類似度計算を行い，マスクの影響で欠損した状態の顔画像でどの程度の精度が得られるかを検証した．結果としてマスクを着用していない状態の顔認証には及ばないが，FAR を 10%未満，FRR を 1 名を除き 2%以下という結果になった．

今後は，提案手法を実際に利用した場合の精度を確認するため，顔認証を行う際の動作から得られる端末の加速度や角度の特徴を組み合わせる実験を行う．そのために加速度データの取得，また，SVM などの機械学習を行う予定である．

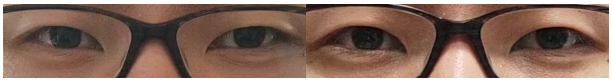

図 7 被験者 E の比較した両目の画像

参考文献

[1] 総務省,”令和 2 年版　情報通信白書　情報通信機器の保有状況,” https://www.soumu.go.jp/johotsusintokei/whitepaper/ja /r02/html/nd252110.html, (2021/10/06 Accessed).
[2] SECUREAIOfficeBase, https://secureinc.co.jp/aioffice/, (2021/11/02 Accessed).
[3] apple 社,”マスクやサングラスの着用時に Apple Watch で iPhone のロックを解除する,” https://support.apple.com/ja-jp/HT212208, (2021/11/01 Accessed).
[4] 富士通 (株),”非接触でクリーンなマルチ生体認証技術を開発,” https://pr.fujitsu.com/jp/news/2021/01/21.html, (2021/11/01 Accessed).
[5] 日本電気 (株),”Bio-IDiom Services,” https://jpn.nec.com/biometrics/services/index.html, (2021/11/01 Accessed).
[6] NIST,”FRVT Face Mask Effects,” https://pages.nist.gov/frvt/html/frvt_facemask.html, (2021/11/01 Accessed).
[7] 石原進，太田正敏，行方エリキ，水野忠則．”端末自体の動きを用いた携帯端末向け個人認証,” 情報処理学会論文誌，Vol.46,No.12,pp.2997-3007(2005).
[8] 今野慎介，中村嘉隆，白石陽，高橋修, ”複数のウェアラブルセンサを用いた歩行動作による本人認証法の精度向上,” 情報処理学会論文誌，Vol.57,No.1,pp.109-122(2016).
[9] 檜垣敦士，鈴木孝幸，清原良三,”個人の認証動作の特徴を用いたマスク着用時における本人認証手法の提案,”第 28 回マルチメディア通信と分散処理ワークショップ論文集，pp.242-245(2020).
[10] 妹尾尚一郎, 厚井裕司, 貞包哲男, 中谷直司, 馬場義昌, 鹿間敏弘,”生体認証によるネットワーク個人認証システム,” 情報処理学会論文誌，Vol.44, No.4, pp.1111-1120(2003).
[11] OpenCV, https://opencv.org/, (2021/11/01 Accessed).
[12] Pablo F, Alcantarilla, Jesus Nuevo, Adrien Bartoli,“Fast Explicit Diffusion for Accelerated Features in Nonlinear Scale Spaces”, BMVC, (2013), pp.13.1-13.11.
[13] David G. Lowe,“Distinctive Image Features from Scale-Invariant Keypoints”, IJCV,pp.91-110, (2004).
[14] Herbert Bay1, Tinne Tuytelaars2, Luc Van Gool12,“SURF: Speeded Up Robust Features”, CVPR, pp.346-359, (2008).
[15] scikit-learn, https://scikit-learn.org/stable/, (2021/11/01 Accessed).
[16] P. Viola and M. Jones, ”Rapid object detection using a boosted cascade of simple features,” Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition. CVPR 2001, (2001).
[17] The AFAD Dataset,https://afad-dataset.github.io/, (2021/11/01 Accessed).