一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
ET2018-62 (2018-11)

e-Testingにおける時系列画像推定による顔認証の検討

川又　泰介†　　赤倉　貴子††

† 東京理科大学大学院工学研究科，東京都葛飾区新宿 6-3-1
†† 東京理科大学工学部，東京都葛飾区新宿 6-3-1
E-mail: †4417701@ed.tus.ac.jp, ††akakura@rs.tus.ac.jp

あらまし　Web 上で試験を行う e-Testing は時空間の制約なく受験が可能という利点がある一方で，試験中の不正行為が容易に発生しうるという問題がある．そこで，試験中のなりすまし受験を防止するために顔画像を用いた受験者認証法が提案されている．しかし，登録情報を参照して入力情報を評価するという従来の生体認証では，受験者の姿勢変動に対応できないという課題が存在する．そこで本稿では，試験中における顔の変動に着目した認証法について報告する．システムを実環境に近い状況で使用した結果，試験中における受験登録者間の入れ替わりに関しては 75%程度の精度であったが，非受験登録者については 90%程度の割合で検知できることが明らかになった．
キーワード　e-Testing，替え玉受験，生体情報，受験者認証

Discussion of a facial authentication method using estimation of time series facial image in e-Testing

Taisuke KAWAMATA† and Takako AKAKURA††

† Graduate School of Engineering, Tokyo University of Science, 6–3–1, Niijuku, Katsushika-Ku, Tokyo, 125–8585 Japan
†† Faculty of Engineering, Tokyo University of Science, 6–3–1, Niijuku, Katsushika-Ku, Tokyo, 125–8585 Japan
E-mail: †4417701@ed.tus.ac.jp, ††akakura@rs.tus.ac.jp

Abstract　One problem in e-testing is cheating easily by impersonation. In our previous work, a facial authentication was proposed for e-testing. Traditional biometrics identify a student with comparing pre-registered with input information, but this procedure cannot authenticate any students who often tend to write the posture during e-Testing. Therefore, we report the authentication focused on the variation of face pose with the machine learning. As a result of the evaluation, the accuracy of examinated authentication method is about 90% and we found the proposed method is useful for an unknown attacker.
Key words　e-testing, proxy test-taking, biometrics, examinee authentication

1. 研 究 背 景

少子高齢化が進む近年の日本において，高等教育機関における社会人の学び直しに注目が集まっている [1]．最近では通信制の高等教育機関も充実し，在宅で教育を受けることも可能となってきた．このことから，通信制の教育機関や，放送大学での学び直しを図る社会人が増加してきている [1]．通信制教育では，e-Learning システムを用いて講義を受講し，場合によっては Web 上で試験を実施する e-Testing なども用いられることから，学習における時空間的な制約の多い社会人でも教育を受けることが可能となる．しかしながら，単位認定試験などのハイステークステストにおいて，e-Testing は必ずしも許容されるものではない．e-Testing では，試験実施者が受験者の受験環境を統制することが困難であり，アメリカでは実際に大学の e-Testing において替え玉受験が発生した例も存在する [2]．これら不正行為を防止する取り組みとして，サイバー大学などでは，Web カメラを用いて試験開始時に生体認証を行い，試験中はカメラで取得した画像から監督者が目視で認証する方法が採用されていた [3]．しかし人力に頼った方法は，人件費や不正検知基準の客観性，試験時と監督時の同期が求められるなど，様々な問題が生じる．そのため，e-Testing 中の受験者を継続的に認証できるシステムの開発が必要である．

e-Testing 中における不正行為を防止するための手法として，橋本ら [4] の研究があげられる．橋本らは e-Testing におけるなりすまし防止のための生体認証（以下受験者認証と呼称）の要件として，(a) 継続性：受験中の継続的な本人確認が可能，(b) 透過性：受験を阻害しない，(c) 同一性：解答者と被認証者が同一であることを確認可能，(d) 耐攻撃性：情報の偽造が一般的に困難，という 4 つの要素を挙げている．また，これらの要件を満たす方法として，カメラデバイスを用いたペンの持ち方認証を提案した．この手法は，訓練された強いなりすまし攻撃に対しても十分な精度で認証することが可能であった．しかし，実際の e-Testing では，受験者の心理状態などによってペンの持ち方などが変化する可能性がある．そのため，実環境下ではペンの把持特徴だけでなく，別の特徴量の組み合わせによるマルチモーダル認証も検討する必要がある．

複数の生体認証を組み合わせた受験者認証システムとして，Agulla ら [5] は顔追跡と顔認証を受講者に適用することで受講中のなりすましや離退席を検知するシステムを開発した．この研究では，講義中の照明変動や受講者の姿勢変化によって顔画像処理が失敗しやすいという課題に対して，顔認証に失敗した場合には，指紋や音声を用いた認証を学習者に要求することで解決を図った．しかし，要求型の認証法は橋本ら [4] の挙げる透過性を満たさないという課題がある．

透過性を満たす受験者認証法として林ら [6] は，事前に登録した文字と試験時にペンタブレットを用いて入力された文字を比較することで，問題ごとに受験者認証を行うモデルが提案されている．筆記認証の中でも筆圧などの動的変動情報は耐攻撃性に優れているが，一方で多肢選択式の e-Testing では，筆記認証のタイミングが解答入力時に限定されるため，継続性を持った認証法と組み合わせる必要がある．

一方で，著者らはこれまでに，講義映像の視聴や e-Testing 中における受験者の入れ替わりに着目した画像認証について検討してきた [7] [8]．これらは従来の生体認証において行われてきた事前登録情報と入力情報の比較ではなく，入力情報同士の比較を行うことで，試験中の異常検知を行う方法論であった．しかしながら，頬杖や思案などによる顔姿勢の変動により，依然として認証精度が低いという課題が残されている．

以上より，先行研究で開発された受験者認証は，受験者認証の要件 [4] を満足していない，もしくは認証精度が低いという課題がある．そこで本稿では，先行研究 [?] における入力情報同士の比較に着目する．ただし，先行研究の方法はあくまで「受験前半の受験者」と「後半の受験者」が同一人物であることを認証する方法であり，「事前登録者」と「受験者」が同一人物であることを保証できないという点では，セキュリティ上の問題がある．この点について，本研究では「登録中の顔の変動」と「試験中の顔の変動」に大きな差がないと仮定し，顔の相対的な変動情報を認証する方法論について検討する．本稿では，登録中のある時点における顔情報から別の時点の顔情報を求める写像関数を求め，その写像関数を試験中に適応した際の認証精度について評価した結果を報告する．

2. 方　法　論

本章では，本稿にて想定する e-Testing 環境について説明し，その状況下で行う認証手順を説明する．本章の最後では，方法論を評価するための実験概要について述べる．

2.1 認証の手順

図 1 に，本稿で扱う受験者認証の手順を示す．生体認証は事前登録時と認証時で処理が異なるが，正面画像の取得，前処理，特徴抽出のプロセスは共通している．

まず，登録時の処理について説明する．受験希望者は，教育機関が指定した期間中に自身の正面画像を複数件提出する．サーバは正面画像を受信すると，正面画像から顔画像を抽出し，色調変換やサイズの調整を行う．その後，正規化された顔画像から特徴ベクトルを抽出し，データベースに登録する．

次に，受験中の処理について説明する．受験者は受験開始時に本人確認を行った後，受験を開始する．受験中は継続的に Web カメラで受験者を撮影し，Web カメラで取得した受験者の正面画像は，試験中数秒ごとにサーバへ送信される．以降は登録時と同様に，サーバは画像を受信すると画像から顔領域を探索する．検出に失敗した場合は検出失敗を示す応答を行う．成功した場合は，顔領域から特徴ベクトルを抽出する．

一般的には，受験中に取得した特徴量をデータベースの登録情報と比較し，顔類似度を算出して閾値比較により本人判定を行う．ただし，登録特徴（テンプレート）と入力特徴を単純に比較したとしても，登録時と入力時の姿勢の違いにより，受験者本人を他人として拒否する誤りが発生することが受験者認証では多発してきた [7]．そこで本稿では，ある時間内における顔の変動に着目している．具体的には，ある受験者の特徴量が入力された場合，その受験者の別時間における特徴量を出力する写像空間を求める．特に，本稿での具体的な実装では t 時点の顔から $t+1$ 時点の顔を推定していることになる．試験中は，その関数に特徴量を入力し，出力を求める．この際，受験者が一貫して同一人物であれば，関数の推定値と実測値は一致するはずである．仮に受験者がある時点で入れ替わった場合，推定値と実測値の誤差が大きくなると考えられる．以降の節で，具体的な実装法について述べる．

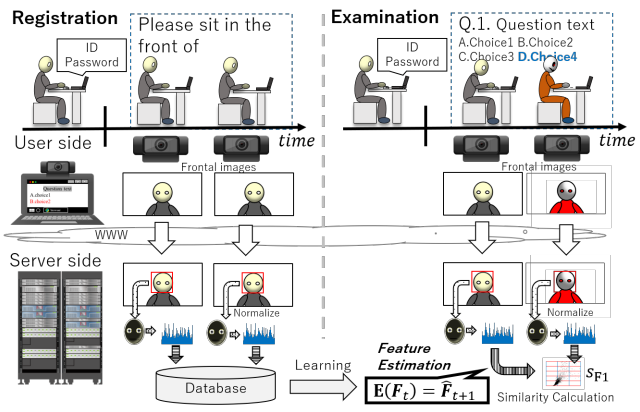

図 1　受験者認証の手順

2.2 具体的な実装

実装した方法は，グレースケールの顔画像ベクトルについて，t 時点でのベクトルを t+1 時点のベクトルに写像する関数をニューラルネットワーク（以下 NN）で求めるというものである．まず正規化については，Viola and Jones [9] の提案した手法で顔を検出し，顔画像をグレースケール化し，サイズを統制する．特徴量の抽出は行わず，顔画像の輝度値が格納されたベクトルを用いる．その顔ベクトルが受験者ごとに時系列順に保存されているとし，NN で t+1 推定器を作成する．

図 2 に，推定器の構造および学習手順を示す．推定器は入力層・隠れ層・出力層を持つ一般的な全結合型の NN である．この構造は著者の事前分析によって決定したものであり，大いに改善の余地がある．事前分析においては，線形識別よりも非線形識別（多層 NN）のほうが精度が高かったが，隠れ層を 1 つ以上設けても精度が変わらなかったことがこの構造の理由である．推定器の結合強度は，受験登録者の登録顔画像をすべて用いて行う．入力をある受験者 j における t 時点での顔画像ベクトル，出力を受験者 j の $t+1$ 時点の顔画像ベクトルとし，それぞれの二乗誤差を最小にするよう確率的最急降下法を適用した．ここで，入力層-隠れ層間の重みの初期値は単位行列を与え，各バイアスは 0，活性化関数は線形を与えた．これは，同一人物間の顔の輝度変動が各ピクセルごとに対応しているという仮説に基づく．隠れ層-出力層間の重みは乱数で設定し，出力化は構造のスパース性と輝度値の範囲から正規化線形関数とした．

本人である尤もらしさ（尤度）は，推定値 $\hat{F}_{t+1}$ と真値 F_t の 2 乗誤差で求める．この距離を基に，受験者が本人か，もしくは入れ替わりが発生したか否かを決定する．ただし，この方法論における認証精度および閾値は不明であるため，本稿では実験によりデータを取得し，認証精度および誤り率について考察する．

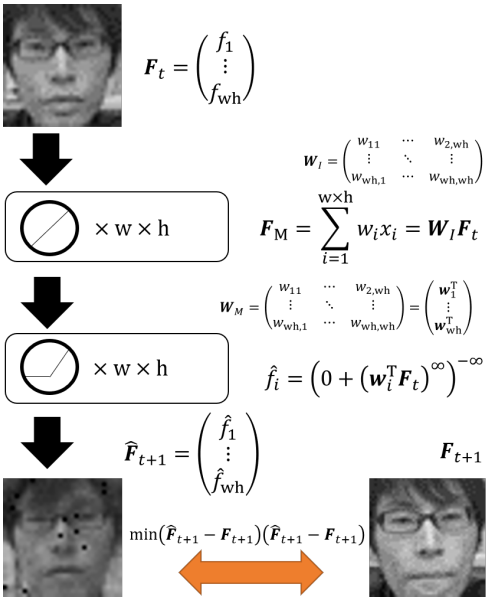

図 2　推定器の構造

2.3 実験概要

本方法について，評価する点は 2 点である．1 つは，ある受験登録者が別の受験登録者になりすまして受験した場合の精度，2 つ目は，未知の攻撃者がある受験者になりすました場合の状況下での精度である．以降で，前者を入れ替わり検知，後者を攻撃者検知と呼ぶ．

入れ替わり検知の評価については，著者らが実験で取得したデータを用いた．被験者は男性 9 名，女性 1 名である．男性 9 名中 5 名は眼鏡を着用している．被験者にはまず顔情報を登録してもらい，登録日とは別日に受験をしてもらった．

攻撃者検知については，前述のデータを正規受験者のデータとし，攻撃者のデータは田中ら [10] の取得したものうち，9 名分のデータを用いた．被験者は男性 5 名，女性 2 名である．男性 5 名中 1 名は眼鏡を着用している．

認証精度の評価は，本人拒否率 (FRR: False Rejection Rate) と他人受入率 (FAR: False Acceptance Rate)，等誤率 (EER: Equal Error Rate) を用いた [11]．FAR と FRR は閾値の変化に対してトレードオフの関係にあることから，FAR と FRR が等しくなる最適閾値における誤り率 EER が認証精度の評価に用いられる．

3. 実験結果

誤り率曲線を図 3 に示す．「Exchange」は入れ替わり検知における誤り率を，「Attacker」は攻撃者検知における誤り率を示す．

これを見ると，入れ替わり検知の評価としては EER=26% と，先行研究 [7] と比較して低い値であった．ただし，出力された推定画像を著者が視認したところ，推定されている顔に大きな誤りは見当たらなかった．このことから，顔自体は推定できているが，尤度（誤差）の計算方法に改善の余地がみられた．

一方で，攻撃者検知に関しては EER=10%であった．このことから，受験登録者のモデルに含まれていない攻撃者に対して，ある程度の有効性が期待できる．ただし，閾値の問題もあるが，攻撃者の検知を想定した場合の FRR は，入れ替わりにおける FRR よりも高いことが図 3 の左上からわかる．このような傾向は先行研究 [7] にもみられたことから，依然として受験者認証における FRR の改善は課題である．

次に，FRR について考察する．図 4 は，受験者本人が一貫して受験していた場合の推定値と真値の類似度（=誤差の反数）を，時系列グラフで表したものである．これを見ると，8 秒の時点で尤度が高く，23 秒の時点で尤度が低くなっている．そこで，推定された顔画像を可視化した．その一部を図 5 に示すが，著者のサンプルでは試験全体を通してほぼ 8 秒時点の顔と同様の顔画像が得られているが，23 秒周辺では顔の角度が右上向きに若干変化している．登録時の顔は図 6 に示すように，大抵が左図のような正面向き，稀に右図のようになっているため，学習されたモデルもその向きを再現するようになっている．そのため，図 5 の 23 秒時の推定画像は左側の眼鏡が消失している．

以上の結果より，顔画像の変動を用いて認証する場合，事前に取得したモデルにない行動が発生すると拒否判定が発生する

ことがわかった．このことはモデル外の攻撃者に対しては有効であるが，受験者の行動によっては正しく顔が推定できない場合も存在する．そのため，登録時における受験者の行動を試験時に近づけるような処理が必要である．

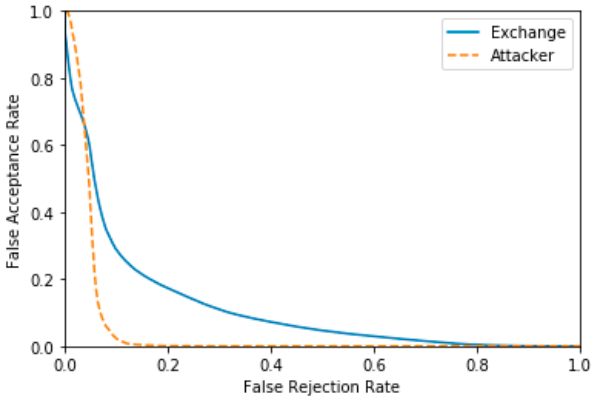

図 3　ROC 曲線

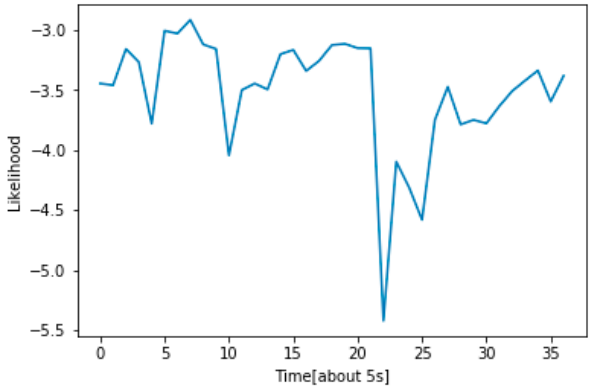

図 4　尤度の時系列推移

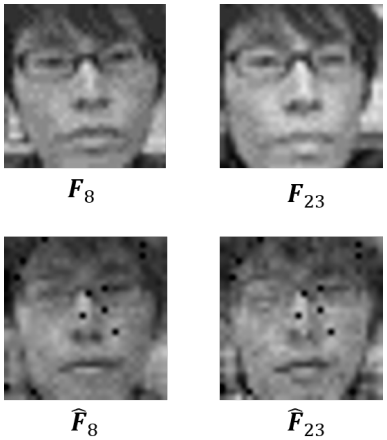

図 5　推定された顔画像と真の顔画像

図 6　登録顔画像

4. 総　　括

e-Testing は受験における時間的・空間的な制約を緩和することが可能である一方，試験中のなりすましやカンニングが容易であるという問題点が存在する．そこで本研究では，なりすましの防止に焦点を当て，受験者の顔画像を用いた受験者認証法に着目した．方法論として，ある受験者の顔が入力された場合，その受験者の別時点での顔を出力するような関数をニューラルネットワークにより求め，性能を評価した．その結果，従来法と同様に FRR については課題が残るものの，モデルに含まれない未知の攻撃者に対しては有効である可能性が示唆された．

今後の課題として，サンプルを増加する必要がある．被験者数ももちろんのこと，各受験者が取り得る行動についても多くのデータを取得する必要がある．また，今回は推定に用いる情報に顔の輝度値のみを用いたが，例えば顔の検出位置や，他の入力機器などを合わせることでより受験者の行動推定を行える可能性がある．他に，本稿において用いた実装はあくまで基礎的なものである．本稿の方法に近い手法として，畳み込みオートエンコーダを用いた異常検知が挙げられる．具体的な実装も理論はそれらに近いが，局所特徴量の計算を単位行列による初期値で賄っている点，出力が入力と同一の情報でない点などが違いとして挙げられる．今回の方法のほか，畳み込みオートエンコーダを用いた手法についてが今後の課題である．

文　　献

[1] “大学等における社会人の実践的・専門的な学び直しプログラムに関する検討会，”文部科学省，http://www.mext.go.jp/b_menu/shingi/chousa/koutou/065/index.htm，参照 Aug. 3, 2018.

[2] J. A. Wollack, J. J. Fremer, “Handbook of Test Security, ” Routledge, 2013.

[3] 川原洋，“遠隔教育における単位認定のための個人認証，”メディア教育研究，vol.7，no.1，pp57-63，2010.

[4] 橋本侑樹，村松大吾，小方博之，“替え玉防止に向けたペン持ち方認証法におけるなりすまし耐性の強化，”信学論（A），vol.J96-A，no.12，pp.769-779，Feb. 2013.

[5] E. Agulla, E. Rúa, J. Castro, D. Jiménez, and L. Rifón, “Multimodal biometrics-based student attendance measurement in learning management systems,” 11th IEEE International Symposium on Multimedia, pp.699-704, New York City, Dec. 2009.

[6] 林大介，赤倉貴子，“e-Testing におけるタブレット PC とオンライン筆記情報を用いた筆記認証法の提案，”日本教育工学会論文誌，vol.42 (Suppl.)，2018（採録決定）．

[7] 川又泰介，石井隆稔，赤倉貴子，“e-Learning における入力顔情報を用いた参照情報の逐次更新による受講者認証，”信学論（D），vol.J101-D，no.4，pp.725-728，Apr. 2018. DOI:10.14923/transinfj.2017JDL8018

[8] 川又泰介，石井隆稔，赤倉貴子，“e-Testing 受験者の正面画像を用いた試験中の入れ替わり検知，”信学技報，ET2017-53，Nov. 2017.

[9] P.Viola, M.Jones, “Rapid object detection using a boosted cascade of simple features,” Proc Of Computer Vision and Pattern Recognition, vol.1, pp.511-518, 2001. DOI: 10.1109/CVPR.2001.990517

[10] 田中佑典，吉村　優，東本崇仁，赤倉貴子，“e-Testing におけるなりすまし防止のための顔画像を利用した個人認証，”信学論，vol.J98-D，no.1，pp.174-177，Jan. 2015.

[11] 半谷精一郎，“バイオメトリクス教科書～原理からプログラミングまで～，”コロナ社，東京，2012.