利用環境認識型生体認証システムの実環境における性能評価

笠松 祥太朗[1,a)]　山崎 恭[1,b)]

概要：スマートフォンやタブレット PC などのスマートデバイスにおける生体認証では，利用環境の変動がユーザ認証の信頼性に与える影響が大きい．この問題に対する解決策として，「人やモノ，環境などの状況の変化に応じて対応することが可能である」という概念である「コンテキストアウェアネス (Context Awareness)」に基づく，利用環境認識型生体認証システムが提案されている．一方，これまで当該システムの有効性評価はシミュレーション実験により行われており，実際の利用環境では行われていない．そこで，本論文では当該システムを実装したスマートデバイスを用いた実証実験を行い，実環境における有効性を，安全性，利便性，リソース消費の観点から評価した結果について報告する．

キーワード：生体認証システム，スマートデバイス，環境認識，実証実験

Performance Evaluation under Real Environment for Biometric Authentication System Considering Usage Environment

Shotaro Kasamatsu[1,a)]　Yasushi Yamazaki[1,b)]

Abstract: Changes in usage environment have a significant effect on the reliability of biometric authentication on smart devices such as smartphones and tablet PCs. As a solution to this problem, biometric authentication system considering usage environment has been proposed based on the concept of "Context Awareness" which means that it is possible to respond to changes in situations of people, goods, and environments. On the other hand, the effectiveness of the system has been evaluated under simulation experiments but not under actual usage environments. Therefore, in this study, we conduct some demonstration experiments by using a smart device equipped with the above system and evaluate the effectiveness of the system under actual usage environments from the viewpoint of security, convenience, and resource consumption.

Keywords: biometric authentication system, smart device, environment recognition, demonstration experiment

1. はじめに

近年，スマートフォンやタブレット PC などのスマートデバイスの急速な普及に伴い，セキュリティやプライバシーを保護するためのユーザ認証技術が必要不可欠となっている．従来より多くのスマートデバイスにおいて，ユーザ認証方式にパスワードやパターンロックなどが用いられているが，これらのユーザ認証方式では悪意を持った第三者による盗み見や，ユーザ自身によるパスワードの忘却などの問題がある．そこで，忘却の恐れがない顔や指紋といった生体情報をスマートデバイスに搭載されたセンサから取得し，これを認証に利用する生体認証技術が注目されている [1].

一方，スマートデバイスは可搬性に優れているため，様々な環境で利用されることが考えられる．このことから，ス

[1] 北九州市立大学国際環境工学部情報システム工学科，〒 808-0135 福岡県北九州市若松区ひびきの 1-1，Dept. of Information Systems Engineering，The University of Kitakyushu 1-1 Hibikino，Wakamatsu-ku，Kitakyushu，Fukuoka，808-0135，Japan
a) x6531015@eng.kitakyu-u.ac.jp
b) y-yamazaki@kitakyu-u.ac.jp

マートデバイスにおける生体認証では，利用環境の変動がユーザ認証の信頼性に与える影響が大きいことに留意する必要がある．この問題に対する一つの解決策として，「人やモノ，環境などの状況の変化に応じて対応することが可能である」という概念である「コンテキストアウェアネス (Context Awareness)」に基づく，利用環境認識型生体認証システムが提案されている [2]．先行研究 [3] では，生体認証を行う際に参照する情報（以下，テンプレート）を利用環境に応じて生成し，登録時と認証時の利用環境の相違が認証精度に与える影響を評価し，利用環境に則した認証方式を選択することがユーザ認証の信頼性向上に有効であることが報告されている．しかしながら，実際の利用環境（以下，実環境）では生体認証の信頼性に影響を与える要因は多岐にわたると考えられ，提案手法の実環境下での有効性評価は今後の課題として残されている．

そこで，本論文では利用環境認識型生体認証システムをスマートフォンに実装し，これを実環境で利用することにより，提案手法の有効性を安全性，利便性，リソース消費の観点から評価することを目的とする．

2. 利用環境認識型生体認証システム [2][4]

前節で述べたコンテキストアウェアネスに基づく利用環境認識型生体認証システムの概要を図 1 に示す．また，当該システムにおける主要な機能である利用環境の認識，テンプレートの登録と更新，ユーザ認証について詳述する．

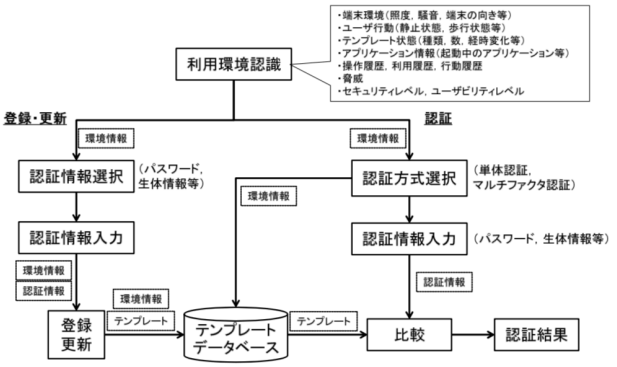

図 1　利用環境認識型生体認証システム

2.1 利用環境の認識

利用環境の認識では，スマートデバイスで取得可能なセンサ情報や，利用履歴，行動履歴などを用いて利用中の環境や状況を認識する．以下，提案手法の中核部分である利用環境認識の各機能について述べる（図 2 参照）．

- 端末環境（照度，騒音，端末の向き等）の認識
  端末に搭載された各種センサを使用し，端末周辺の環境あるいは端末自体の環境を認識する．具体的には，輝度センサで端末周辺の照度を，マイクロフォンで端末周辺の騒音を，ジャイロセンサや加速度センサで端末自体の向きや動きなどを計測する．計測結果は，例えば，端末周辺の騒音が大きい場合，音声を認証情報として使用しないとシステムが判断する際の情報として使用する．

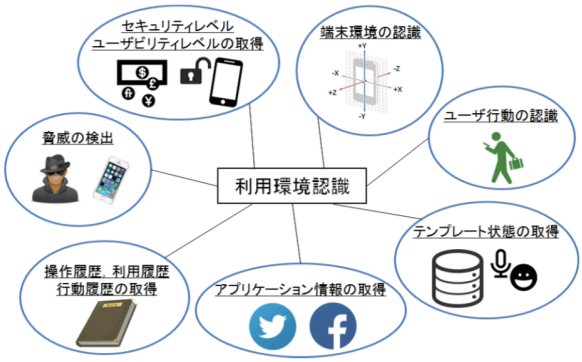

図 2　利用環境認識機能

- ユーザ行動（静止状態，歩行状態等）の認識
  端末に搭載された各種センサを使用し，端末を使用するユーザの行動を認識する．具体的には，加速度センサを使用してユーザが歩行中か否かなどを認識する．認識結果は，例えば，ユーザが歩行中の場合，入力が不安定となる筆記情報を認証情報として使用しないとシステムが判断する際の情報として使用する．
- テンプレート状態（種類，数，経時変化等）の取得
  現在登録されているテンプレートの種類や数，あるいはテンプレート登録時（最終更新時）からの経過時間などの情報を取得する．ここで取得される情報は，例えば，生体情報のテンプレート登録時 (最終更新時) から一定の時間が経過している場合，テンプレートを更新するためにシステムがユーザに生体情報の入力を促すか否かを判断する際の情報として使用する．
- アプリケーション情報（起動中のアプリケーション等）の取得
  ユーザが使用するアプリケーションに関する情報を取得する．用途の一例として，ユーザが通話機能を有するアプリケーションを使用している場合，ユーザの会話音声を継続認証のための情報としてシステムが使用するなどが挙げられる．
- 操作履歴，利用履歴，行動履歴の取得
  端末の操作履歴やアプリケーションの利用履歴，ユーザの行動履歴に関する情報を取得する．ここで取得される情報は，例えば，ユーザが通常と異なる方法で端末を操作したり，普段使用しないアプリケーションを使用したりした場合，システムがユーザに認証を要求するなどの用途に使用する．

- 脅威の検出
  悪意を持つ第三者による端末への脅威を検出する．ここで検出される情報は，例えば，生体情報の一つである顔画像を認証情報として使用する際，認証時に意図的に輝度センサを遮蔽して端末周辺の照度の値を不正に操作しようとする行為などが確認された場合，これを脅威とみなし，システムが顔画像の使用を一時的に中止することを決定する際の情報として使用する．
- セキュリティレベル，ユーザビリティレベルの取得
  あらかじめ設定された個々のアプリケーションに要求されるセキュリティレベルや，ユーザが設定する認証時の利便性に関するレベル（ユーザビリティレベル）に関する情報を取得する．ここで取得される情報は，例えば，端末のロック解除，金銭の授受を伴うアプリケーションにそれぞれ適した認証方式をシステムが決定する際の情報として使用する．

2.2 テンプレートの登録と更新

テンプレートの登録と更新では，ユーザが入力した生体情報を登録し，必要に応じて更新を行う．例として，認証を行う際に利用環境に適したテンプレートが登録されていない場合には，システムがユーザに生体情報の登録を要求する．また，テンプレートの最終更新時刻から一定の時間が経過しているなど，テンプレートの更新が必要であると判断される場合にも，システムはユーザに対してテンプレートの更新を要求する．なお，本論文では便宜的に，ユーザによりシステムに入力された生体情報やそこから得られる特徴量を認証情報と呼称する．

2.3 ユーザ認証

ユーザ認証では，利用環境の認識により得られた環境情報に基づき，システムが適応的に最適な認証方式を選択し，これをユーザに提示する．ユーザはシステムから提示された認証方式に従い認証情報を入力する．システムは，テンプレートとして保存されている生体情報の中から環境情報が最も類似しているテンプレートを抽出し，入力された認証情報と比較を行い認証結果を出力する．

3. 利用環境認識型生体認証システムに関する関連研究

3.1 利用環境に適した認証方式の選択

阿川ら [5] は，使用リソースを考慮したスマートデバイス上での継続認証に関する検討を行っている．この研究では，生体認証を行う際に利用環境に適した認証方式を適応的に選択し，稼働させるセンサを管理することで，スマートデバイスのリソース消費の低減，ならびにシステムの安全性・信頼性低下の抑制が期待されると報告されている．また，顔認証による実験では，認証に適した場合のみカメラを起動させる方式と常時カメラを起動させる方式を比較し，総消費電力，CPU 使用率がともに低減されることが明らかとなっている．一方，スマートデバイスで使用される生体認証は複数存在するため，これらを組み合わせた認証システムにおいてリソースの消費量が低減されるか否かは不明である．したがって，複数の認証方式を用いた生体認証システムにおいて，適切なセンサのみを稼働させることによるリソース消費への影響を評価する必要があると考えられる．

3.2 利用環境に適したテンプレートの生成と選択

岡部ら [3] は，利用環境に適したテンプレートの生成と選択の有効性評価と，環境情報に基づく認証方式選択の検討を行っている．この研究では，テンプレートを利用環境に応じて生成し，登録時と認証時の利用環境の相違が認証精度に与える影響を評価した結果，利用環境に則した認証方式を選択することがユーザ認証の信頼性向上に有効であると報告されている．また，スマートデバイス上の各種センサから取得した環境情報に基づき，顔認証における照明状態，筆者認識における端末の保持状態，話者認識における雑音強度をそれぞれ認識することにより，テンプレートの登録時と認証時の利用環境がどの程度異なるかを推定し，認証方式の選択に活用できることの可能性を示している．一方，これらはシミュレーション実験に基づく報告であり，多様な実環境における有効性の評価は行われていない．したがって，利用環境の認識により得られた情報に基づき認証方式を適応的に選択するアルゴリズムを実装したスマートデバイスを用いた実証実験を行う必要があると考えられる．

4. 提案手法

前節で述べた課題を踏まえ，本論文では複数の認証方式を用いた生体認証システムにおける認証方式の選択手法を提案する．提案手法では，予め各認証方式の認証精度を予備実験により評価し，その結果に基づき認証方式の選択を行う．本論文では，予備実験で認証精度が高い認証方式は実証実験でも認証精度が高いと仮定し，図 3 に示す選択手法を採用した．図 3 では，一例として，認証方式 1，認証方式 2，認証方式 3 の順に認証精度が高い場合の選択手法を示している．認証システムは，環境情報に基づき認証方式 1 の実行に適した利用環境にあるか否かを判定する．ここで，適していると判定された場合は認証方式 1 をユーザに提示し，そうでない場合は認証方式 2 の実行に適した利用環境にあるか否かを判定する．同様に，認証方式 2 の実行が適さない場合は認証方式 3 についての判定を行い，全ての認証方式が実行に適さない環境にあると判定した場合は生体認証によるユーザ認証を中止する．

本論文では，この選択手法の機能を搭載した利用環境認

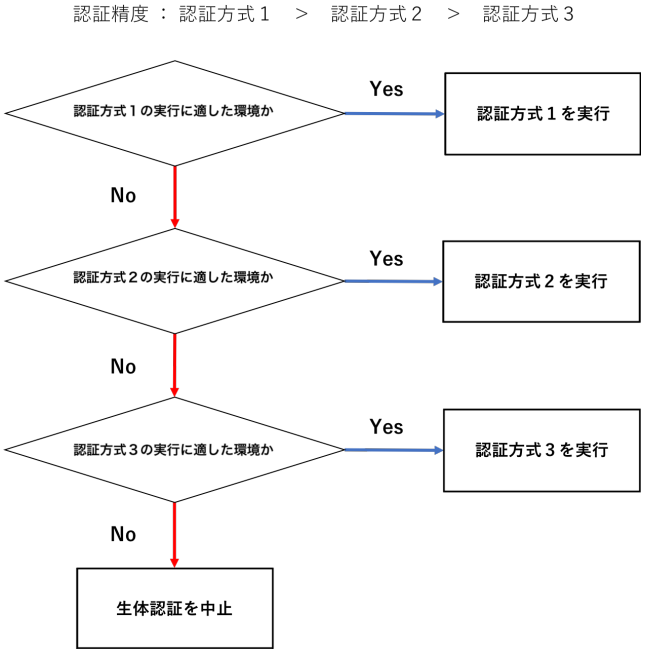

図 3　認証方式の選択

識型生体認証システムをスマートデバイスに実装し，実環境において実証実験を行いその有効性を評価した．また，各認証方式を使用した際のシミュレーション実験と実証実験の認証精度を比較することで提案手法の安全性を評価し，また，実証実験の被験者から収集したアンケートの結果を分析することで提案手法の利便性を評価し，さらに，実証実験中のスマートデバイスの CPU 使用率を測定することで提案手法がリソース消費に与える影響をそれぞれ評価した．

5. 信頼性評価実験

まず，予備実験を行い，当該システムで使用する各認証方式の認証精度を評価した．次に，予備実験の結果を踏まえた信頼性評価実験を行い，実環境における当該システムの有効性を，安全性，利便性，リソース消費の観点から評価した．

5.1 予備実験

5.1.1 実験の概要

認証方式の選択を行う際に使用する各認証方式の認証精度をシミュレーション実験により算出した．なお，認証精度を表す指標として EER（Equal Error Rate）を使用した．

5.1.2 実験の諸元

予備実験の諸元を表 1 に示す．

5.2 実験結果

実験により得られた各認証方式の認証精度を表 2 に示す．

表 2 の結果から，話者認証，顔認証，フリック認証の順に利用環境に適しているか否かを判定することにより，当

表 1　予備実験の諸元

	顔認証	フリック認証	話者認証
使用端末	Apple iPhone6s, MKQP2J/A		
被験者数	10 人		
データ仕様	正面顔画像 (128 × 128 px)	ひらがな文 3 パターン	日本語音声 3 パターン
データ数	10 枚 / 人	3 × 15 回 / 人	3 × 10 回 / 人
入力手段	内蔵カメラ	指	内蔵マイク (16kHz, 16bit)
利用環境	照度：500 ± 50 lx	手で保持	無響室
特徴量	I LBP[6]	x 変位，y 変位，フリック長，フリック曲度，フリック速度，圧力	MFCC(12 次元)[7]
比較スコア	ヒストグラム間のユークリッド距離	ユークリッド距離	DTW[8], ユークリッド距離

表 2　各認証方式における認証精度

認証方式	顔認証	フリック認証	話者認識
EER[%]	5.9	25.4	5.2

該システムの認証精度向上を図ることが期待される．そこで，この予備実験の結果を反映させた認証方式選択手法をスマートデバイスに実装し，以下に述べる信頼性評価実験を行った．

5.3 信頼性評価実験

5.3.1 実験の概要

当該システムの実環境における有効性を評価した．具体的には，同意を得た複数の被験者のスマートデバイスに当該システムを実装し，端末のロックを解除する際に当該システムを用いたユーザ認証を実行してもらった．

5.3.2 実験の諸元

実験の諸元を表 3 に示す．また，各認証方式の認証精度に大きな影響を及ぼすと考えられる環境情報に対し，利用環境に対応したテンプレートの生成を行った（表 4）．今回使用したセンサの特性を以下に述べる．輝度センサは 0〜1.0 の範囲で明るさを取得し，暗い場合は小さな値，明るい場合は大きな値を出力する．加速度センサは端末の x 軸，y 軸，z 軸それぞれの値を-1.0〜1.0 の値で出力する（図 4 参照）．マイクロフォンは雑音強度を取得し，雑音が大きい場合は 0 に近い値を出力する．

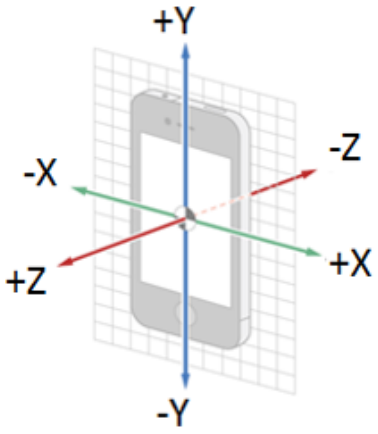

図 4　加速度センサ

表 3　実験の諸元

使用端末	iPhone11Pro，MWC62J/A iPhone11，MWM22J/A iPhoneXs，MTAX2J/A iPhone8，NQ782J/A iPhone7，MNCM2J/A iPhone6s，MKQP2J/A iPhone6s，MKQT2J/A
被験者数	7 人
実験期間	24 時間

表 4　利用環境

顔認証 （使用センサ：輝度センサ）	
明るい場所（明）	輝度：0.35 以上
やや明るい場所（半）	輝度：0.2 以上 0.35 未満
フリック認証 （使用センサ：加速度センサ）	
机上に配置（置）	重力加速度：z 軸の値が-1.0 以下
歩いた状態で手に保持（歩）	ユーザ合成加速度：0.8 以上
止まった状態で手に保持（止）	上記以外
話者認識 （使用センサ：マイクロフォン）	
静かな場所（静）	雑音強度：-30.0 未満
やや雑音がある場所（雑）	雑音強度：-20.0 未満-30.0 以上

5.3.3　実験結果

ユーザ認証に関する実験結果を図 5 に示す．図 5 において，円グラフの中心に記載されている数値は各認証方式の実行回数を表し，同図ではユーザ本人の認証が成功した回数を青色，失敗した回数を橙色で示している．また，Xcode[9] を使用し，実験に使用した端末で，各機能を使用した際の平均 CPU 使用率を計測した結果を図 6 に示す．

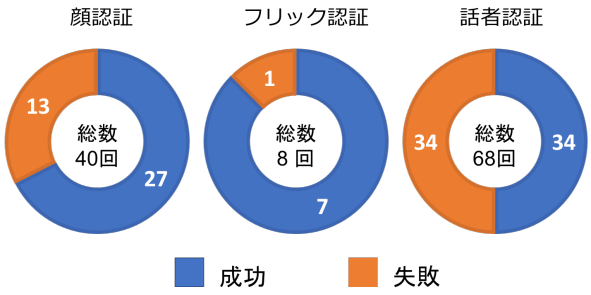

図 5　認証結果

5.3.4　安全性に関する評価

図 5 と表 2 より，予備実験の結果と比較して，当該システムを実環境で利用した際の認証精度が著しく低下していることが明らかとなった．この要因の一つとして，利用環境認識の精度が不十分であったことが考えられる．

まず，話者認証の場合，認証方式を選択する際の利用環境とユーザが話者認証を実行する際の利用環境が一致していない可能性のあることが考えられる．具体的には，本論文における利用環境認識型生体認証システムでは，認証を開始する直前の雑音強度のみを環境情報として利用しているため，認証時に雑音が多く存在している場合でも，雑音が小さい瞬間の環境情報で判定が行われる可能性がある．また，雑音強度では雑音の音量を推定することは可能であるが，雑音の種類を推定することはできないため，同じ雑音強度であっても混入する音が雨や風などの環境音であるのか人の声であるのかにより認証精度は大きく左右されると考えられる．

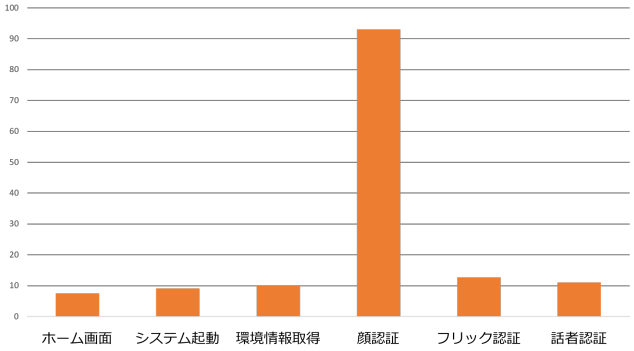

図 6　各機能使用時における CPU 使用率 [%]

また，顔認証の場合，輝度センサから取得される値が同一であっても，顔画像を撮影する際の光の当たり方により，テンプレートと入力情報の間に差異の生じる可能性がある．さらに，利用環境の変化に情報の更新が追いついていない可能性もある．実験に使用した端末は，輝度センサから情報を直接取得することができず，画面の輝度情報により自動的に調整される画面輝度を取得して利用環境の推定を行っている．これにより，屋内から屋外へ移動するなど短時間で利用環境に大きな変動が生じる場合は，利用環境の変化に追従することができず正しい利用環境の推定ができない可能性が考えられる．

一方，フリック認証の場合，認証回数は少ないもののほとんどの場合において本人の認証に成功している．これは，前述の話者認証に使用しているマイクロフォンおよび顔認証に使用している輝度センサから得られる環境情報は，外的要因による変動が大きいのに対し，フリック認証に使用している加速度センサから得られる環境情報は，ユーザの行動に由来する情報であるため，前者と比較してユーザの意識により比較的安定した状態で取得することが可能であり，認証精度への影響が相対的に小さいと考えられる．

以上の結果から，利用環境の変動が少ない安定した条件で行われたシミュレーション実験と，利用環境の変動が大きい多様な利用環境が存在する実環境下で行われた実証実験では，認証精度が必ずしも一致しないことが明らかとなった．この認証精度の差異を減少させるためには，認証

を実行する際の利用環境を高速かつ高精度に認識する手法が必要であると考えられる．

5.3.5 利便性に関する評価

実験後に被験者から報告された当該システムの懸念点は以下のとおりである．

- 周囲に人がいる場合は話者認識を行いたくない．
- 認証を開始するまでどの認証方式を使用するのかが分からないため手間がかかる．
- 何度も連続で認証に失敗することがあり，従来手法よりも時間がかかる．

これらの中で，「周囲に人がいる場合は話者認識を行いたくない」という懸念点は特に注目すべきであると考えられる．なお，回答者以外の被験者の多くが同様の意見を持っていることが判明した．このことは，音声のように周囲に注目されるような認証方式を利用することに対して多くのユーザは消極的であり，その一方，顔認証やフリック認証など周囲に注目される可能性の少ない認証方式を利用することに対しては抵抗が少ないことを示している．以上の結果から，利便性の高いユーザ認証を実現するためには，認証精度や認証時間とともに，ユーザが抵抗なく認証を実行できる手法を検討する必要があると考えられる．

5.3.6 リソース消費に関する評価

図 6 より，ホーム画面の表示やシステム起動の際の CPU 使用率と環境情報取得時の CPU 使用率を比較すると，これらの間の差異は小さく，認証実行時以外に提案手法がリソースの消費に与える影響は小さいことが確認される．一方，顔認証を実行する際は CPU の使用率が上昇するが，これはカメラの起動に起因したものである．カメラの起動は大きくリソースを消費するが，提案手法では顔認証が最適であるとシステムが判定した場合のみカメラが起動されるため，利用環境を問わず顔認証を実行するユーザ認証システムと比較すると，提案手法ではリソースの消費が小さいものと推察される．同様に，提案手法では顔認証以外の認証方式についても必要なセンサのみの稼働により，不要なリソースの消費を抑止することが可能である．以上のことから，提案手法により，リソースに制約のあるスマートデバイスにおいて，リソースの消費を抑えつつ安全性と利便性の高い認証が実現できる可能性のあることが明らかとなった．

6. まとめ

本論文では，コンテキストアウェアネスの概念に基づく利用環境認識型生体認証システムをスマートデバイスに実装し，実環境における有効性を，安全性，利便性，リソース消費の観点から評価した．今後の課題として，実環境での認証精度の向上や高速かつ高精度な利用環境認識手法の検討などが挙げられる．

謝辞

本論文の一部は，JSPS 科研費 JP16K00190 の助成を受けたものです．

参考文献

[1] P.A.Tresadern, C.McCool, N.Poh, P.Matejka, A.Hadid, C.Levy, T.F.Cootes, S.Marcel, “Mobile Biometrics : Combined Face and Voice Verification for a Mobile Platform,” IEEE Pervasive Computing, Vol.12, No.1, pp.79-87, 2013.

[2] 岡部 稜，東 知明，山崎 恭，大木 哲史，“スマートデバイスを用いたコンテキストアウェアネスなマルチファクタ認証システムの実現に向けた一検討，”電子情報通信学会和文論文誌 A, Vol.J99-A, No.12, pp.467-470, 2016.

[3] 岡部 稜，東 知明，山崎 恭，大木 哲史，“スマートデバイスを用いたコンテキストアウェアネスに基づくマルチファクタ認証システム，”電子情報通信学会技術研究報告，Vol.115，No.516，BioX2015-47，pp.37-42，2016.

[4] Yasushi Yamazaki and Tetsushi Ohki, “Toward more secure and convenient user authentication in smart device era,” IEICE TRANS. Inf. & Syst., Vol.E100-D, No.10, pp.2391-2398, 2017.

[5] 阿川 登生，東 知明，山崎 恭，大木 哲史，“使用リソースを考慮したスマートデバイス上での継続認証に関する一検討，”電子情報通信学会技術研究報告，Vol.117，No.236，BioX2017-25，pp.1-6，2017.

[6] H.Jin，Q.Liu，H.Lu，X.Tong，“Face detection using improved LBP under Bayesian framework，”Proc. of Third International Conference on Image and Graphics (ICIG’04)，pp.306-309，2004.

[7] 安藤彰男，“リアルタイム音声認識，” 社団法人電子情報通信学会，2003.

[8] H.Sakoe, S.Chiba, “Dynamic Programming Algorithm Optimization for Spoken Word Recognition,” IEEE Trans. on Acoustics, Speech, and Signal Processing, Vol.ASSP-26,No.1, pp.43-49, 1978.

[9] Apple，“Xcode - Apple Developer，” https://developer.apple.com/jp/xcode/ (参照：2020 年 2 月 21 日).