

加速度とボタン操作を用いた個人認証方式に関する検討

染谷大介[†] 長谷川まどか[†] 田中雄一[†] 加藤茂夫[†]

我々はこれまでに、腕振り動作による個人認証方式の1つとして、腕を振る動作と端末付属のボタンを押下/解放する動作を組み合わせた、成りすましが困難な個人認証方式を提案した。しかし、ユーザの動作の経時変化を十分に考慮しておらず、経時によって本人拒否率が增大する問題があった。そこで本研究では、より新しいユーザの動作特徴を反映させる手法および、動作の種類に依存せずに認証成功率を調整するためのパラメータに関する検討を行った。

A Study on Authentication Using Acceleration and Button Operation

Daisuke Someya[†] Madoka Hasegawa[†] Yuichi Tanaka[†]
and Shigeo Kato[†]

In our preceding study, we proposed a multimodal authentication method using a drawing movement and a pattern of pressing/releasing a button while a user is holding a small handheld terminal with an acceleration sensor and buttons. However, this method was over sensitive to the slight differences of movements, because once a user registered a master data, the system used the same master data for all authentications and did not consider variation and change of user's movement with time. In this paper, we study on a method for updating the master data in our multimodal authentication system. This method is able to reflect the user's latest movement characteristic and is effective to reduce the false rejection rate.

1. はじめに

携帯電話などの小型端末に保存された個人情報の漏洩対策として、現在、パスワードや指紋認証などが主流である。しかし、安全性を重視すると、複雑で長いパスワードを端末上の数字ボタンなどで入力することになり、使い易さの面で改良の余地がある。また、指紋は、万一漏洩すると変更ができないことや、心理的な抵抗を持つユーザも少なくないため、より使い易い認証方式が望まれている。この問題の解決策の一つとして、ユーザにとって認証動作が容易な腕振り動作による個人認証方式[1][2]が提案されているが、動作を第三者に覗き見られた場合、成りすまされる可能性がある。そこで我々は、腕振り動作に加えて、携帯端末のボタンの押下/解放の動作を組み合わせた、成りすましが頑健なマルチモーダル個人認証方式を提案し、検討を進めている[3]。しかし、これまでの検討では、ユーザの動作の経時変化に十分に対応できておらず、経時によってユーザの動作が登録時の動作から変化し、登録時の動作との相違が大きくなると本人拒否率が增加するという問題点と、動作によって最適な閾値制御パラメータが違うために、システム側で本人拒否率と成りすまし成功率のバランスを調整することが困難という問題点があった。そこで本稿では、ユーザの動作の経時変化に対応するために、マスターデータの更新方法と動作の種類に依存しない閾値制御パラメータに関する検討を行い、本人拒否率と成りすまし成功率の検証を行ったので報告する。

2. 加速度とボタン操作による個人認証

2.1 本方式の概要

近年、センサ類を用いて個人の行動的特徴を抽出し、個人認証や、動作の識別を行うインターフェースの研究が行われている[1]-[7]。

本方式は、ユーザが加速度センサを内蔵した端末を手に持ち、ユーザがあらかじめ決めた何らかの図形を空中に描く動作を用いて認証を行う方式である。認証に使用する装置は、携帯端末に内蔵された加速度センサと、端末付属のボタンなので、携帯端末への実装が容易であるという点が利点として挙げられる。描画動作時のユーザの腕の振り方、手首のひねり等の個人の動作特徴を加速度データとして取得する。そして、ユーザがあらかじめ登録した加速度データとのマッチングを行い、マッチングにより得られる相違度をもとに認証を行う。また、認証動作時にユーザは携帯端末のボタンを押下/解放する動作を、腕を振る動作とともに行い、ボタンを押していた区間を認証動作の動作区間とする。生成される加速度データの例を図1に示す。

[†] 宇都宮大学大学院工学研究科
Graduate School of Engineering, Utsunomiya University

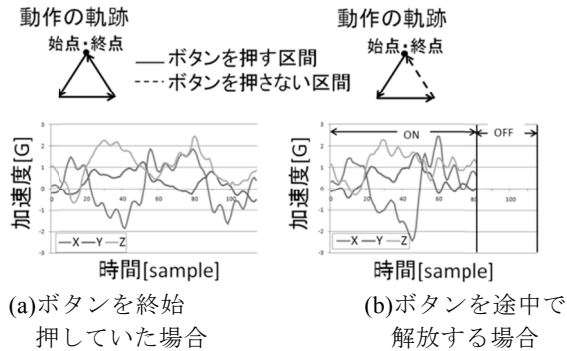


図 1. 加速度データの生成の例

ボタンの押下/解放の動作を認証に用いることにより、図 1 のように認証の動作区間をユーザが任意に決定できる。つまり、同じ軌跡を描く動作であっても、ボタンを押す区間を変えることで異なった加速度データパターンが生成される。さらに、認証時には、ボタンの押下/解放のパターンの照合も行う。つまり、認証時には腕振り動作だけでなく、端末のボタンを押す区間の再現も必要となる。よって、認証動作すべてを動作区間とする方式と比べ、動作の一部を囲とする工夫をユーザが施すことが可能であり、他者が認証を行う場合との相違度を大きくできるため、成りすましが困難になると考えられる。

2.2 相違度の算出法

本方式では、加速度データ間の相違度を算出するためのマッチングに DP マッチングを用いる。DP マッチングは毎回の動作の微小な揺らぎを吸収したマッチングが可能な手法である。マッチングを行う 2 つの加速度データをそれぞれ A, B とし、両者の相違度を算出する手順を図 2 に示す。

毎回の認証時に、ユーザが同じ動作を同じ速度で行うことは難しいため、マッチングを行う 2 つの加速度データの速度差を吸収するために加速度の正規化を行う。本方式では、A, B それぞれの絶対値の最大値を 1 として正規化する。

次に距離尺度に加速度ベクトル間のユークリッド距離を用いて DP マッチングを行う。ここで加速度データ A における i 番目 ($i=1 \sim I$) の加速度ベクトルと加速度データ B における j 番目 ($j=1 \sim J$) の加速度ベクトル間のユークリッド距離を式(1)のように $d(i, j)$ と表す。このとき、 I, J は A, B それぞれのデータの系列長である。そして、式(3)を漸化式の初期値として式(2)を順次計算し、式(4)の DP マッチング距離 $D(A, B)$ を算出する。これにより算出された $D(A, B)$ が加速度データ間の相違度となる。

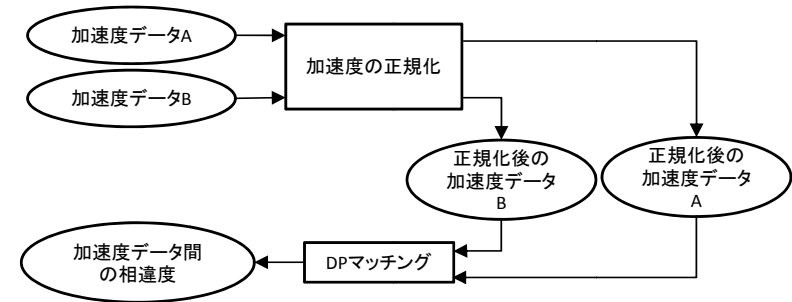


図 2. 加速度データ間の相違度算出の流れ

$$d(i, j) = \sqrt{(Ax_i - Bx_j)^2 + (Ay_i - By_j)^2 + (Az_i - Bz_j)^2} \quad (1)$$

$$g(i, j) = \min \begin{bmatrix} g(i-1, j) + d(i, j) \\ g(i-1, j-1) + 2d(i, j) \\ g(i, j-1) + d(i, j) \end{bmatrix} \quad (2)$$

$$g(1, 1) = 2d(1, 1) \quad (3)$$

$$D(A, B) = \frac{g(I, J)}{I + J} \quad (4)$$

2.3 マスタデータ登録時の処理の流れ

まず、ユーザは事前に自分の決めたタイミングでボタンを押下/解放しながら図形を空中に描画する認証動作を N 回行い、加速度データを登録する。この複数の加速度データをマスタデータ M_k ($k=1, 2, \dots, N$) とする。

ユーザの動作の登録後、システムはマスタデータの中から、取得した加速度データとのマッチングに最適な代表マスタデータ M_m を決定する。次に、認証の成否判定に用いる閾値 T を式(5)により算出する。

$$T = \mu_m + a\sigma_m \quad (5)$$

ここで、 μ_m は代表マスタデータ M_m と $N-1$ 個の他のマスタデータとの相違度の平均値、 σ_m はその標準偏差、 a は閾値制御パラメータである。

代表マスタデータ M_m の決定法は種々考えられ、これまでの検討(文献[3])では、マスタデータの重心に最も近いマスタデータを代表マスタデータ M_m としていた。この代表マスタデータの算出式を式(6)に示す。

$$M_m = \arg \min_{M_k} \sum_{l=1}^N D^2(M_k, M_l) \quad (k \neq l) \quad (6)$$

ここで、 $M_k (k=1,2,\dots,N)$ は N 個のマスターデータのうち k 番目のデータを表し、 $D(M_k, M_l)$ は着目するマスターデータ M_k とその他のマスターデータ $M_l (l \neq k)$ との相違度を表す。

さらに今回の検討では、式(7)のように、 N 個のマスターデータのうち、時系列でみて最も新しいマスターデータを代表マスターデータ M_m とした場合についても検討を行った。

$$M_m = M_N \quad (7)$$

これは、ユーザが現在行っている動作に含まれる個人の動作特徴は、より新しい加速度データに多く含まれていると考えられるためである。

2.4 認証の流れ

認証フェーズの流れを図3に示す。まず、ユーザは自分の認証動作を行い、システムは動作から得られる加速度データ C とボタンの押下/解放のパターン P を取得する。次に、ボタンの押下/解放のパターン P の照合を行い、一致しない場合はその時点で認証失敗と判断する。 P が一致した場合は、さらに、代表マスターデータ M_m と取得した加速度データ C との相違度を算出し、相違度が閾値 T よりも小さい場合に認証成功と判定する。

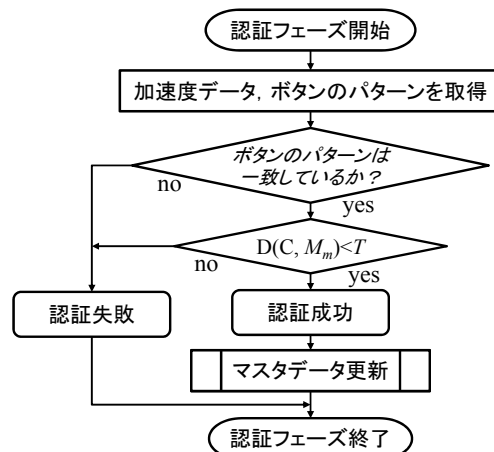


図3. 認証フェーズの流れ

3. マスターデータの更新方法

石原らの方式[1]では、マスターデータが更新されるたびに、複数あるマスターデータの中から代表マスターデータの決定を行っている。また、松尾らの方式[2]では、代表マスターデータと認証時の加速度データとの合成を行い、両データの特徴を併せ持った1つの代表マスターデータを作成している。いずれの方式においても、マスターデータの更新を行うことで、より新しいユーザの腕振りの動作特徴を捉えた加速度データをマスターデータとすることができ、本人拒否率を減少させることができることが分かっている。そこで、本方式でもマスターデータの更新を行い、より新しい加速度データを取り入れる手法の検討を行った。以下では、その方法を説明する。

3.1 マスターデータの更新条件

マスターデータの更新は、認証が成功した場合にのみ行うものとする。代表マスターデータを式(6)で決定する場合は、認証成功時のデータをマスターデータに追加し、最も古いものを削除することで常に N 個のマスターデータを保持する。また、代表マスターデータを式(7)で決定する場合は、代表マスターデータを認証成功時のデータで更新するだけでよい。

ただし、マスターデータを更新しても、閾値の再計算は行わない。これは以下の理由による。もし、認証を1回行ってから、次の2回目の認証までの時間間隔が短いと、動作の正確な再現が容易であるため各加速度データ間の相違度が小さくなる。このとき閾値の再計算も行うとすると、閾値 T は極端に小さくなる。これは、以後継続して正確な動作再現を要求することを意味する。しかし、その次の認証までの時間間隔が長いと、一般にユーザの動作に変化が生じるため、一旦閾値 T が極端に小さくなった後は、認証に成功することが非常に難しくなる。このため、閾値 T の算出は動作登録時のみとし、同じ閾値を継続して認証の成否判定に使用する。

4. 閾値制御パラメータの調整

我々のこれまでの検討では、本人拒否率(False Rejection Rate : FRR)と第三者による成りすましの成功率(False Acceptance Rate : FAR)をともに低くすることができる閾値を見出すため、閾値制御パラメータ a を実験的に調整し、等誤り率(Equal Error Rate : EER)が最小となる場合の調査を行ってきた。しかし、毎回動作に揺らぎが生じるユーザと、毎回ほぼ同じ動作を行えるユーザが存在し、最適なパラメータは登録動作(およびユーザ)によって異なるという結果が得られており、本人拒否率と成りすまし成功率を共に最小化するパラメータ決定の自動化が課題であった。

そこで今回の検討では、あらかじめ数種類の認証動作を代表的な動作とみなし、そのマスターデータ間の相違度の標準偏差と、EERとなるときの閾値制御パラメータ a を求め、これらの相関図から近似曲線を作成する。そして、この近似曲線を用いること

により、実際に登録されたマスタデータ間の相違度の標準偏差から、その動作の認証に使用する閾値を決定する方法の検討を行った。以下では、相関図の作成と閾値の算出法について詳説する。

4.1 相関図の作成

マスタデータ間の相違度の標準偏差と各被験者の EER の相関図の作成方法について説明する。マスタデータ間の相違度の標準偏差は、初期の動作登録時のマスタデータを用いて算出する。まず、登録されたマスタデータ $M_k(k=1,2,\dots,N)$ の中から近似曲線算出のための代表マスタデータ M_a を決定する。ここでは、近似曲線算出時の代表マスタデータ M_a と認証時の代表マスタデータ M_m は異なる方法で決定することを想定して異なる変数で表しているが、同一の方法で決定することも可能である。

次に、この近似曲線算出用代表マスタデータ M_a と他のマスタデータ $M_l (M_l \neq M_a)$ との相違度 $D(M_a, M_l)$ の標準偏差 σ_a を求める。

この相違度の標準偏差 σ_a と EER となるときの閾値制御パラメータ a を各認証動作について実験的に求め、両者の相関図を作成する。次に、相関図のプロット点の近似曲線を求める。得られた近似曲線の例を図 4 に示す。

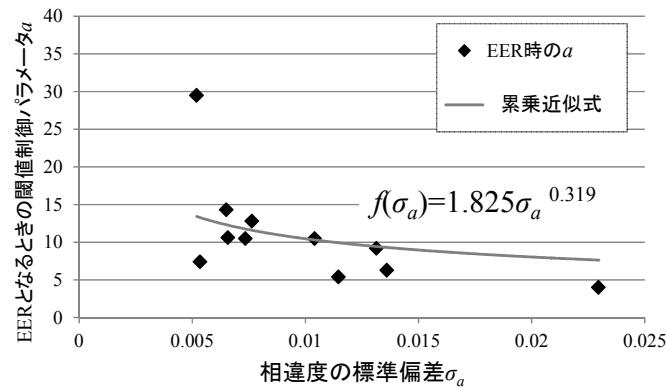


図 4.作成される近似曲線の例

4.2 閾値の算出法

次に、閾値の決定法を説明する。まず、登録されたマスタデータについて、認証用代表マスタデータとの相違度の平均 μ_m と分散 σ_m および、近似曲線算出用代表マスタデータとの相違度の標準偏差 σ_a を求める。次に、算出した近似曲線 $f(\sigma_a)$ を用いて、式 (8) より、EER になると予想される閾値を求める。

$$T = \mu_m + b\sigma_m \cdot f(\sigma_a) \quad (8)$$

ここで、 $f(\sigma_a)$ は、標準偏差 σ_a を入力とし、EER になると予想される閾値制御パラメータを出力する関数である。また、 b は近似曲線を使用した閾値決定方法における閾値制御パラメータであり、この値を変動させることにより閾値をさらに細かく制御する。

5. 実験

本人認証実験と成りすまし実験を行い、提案方式における FAR, FRR, および、EER を測定した。さらに、この実験結果をもとにマスタデータ間の標準偏差と EER となる場合の閾値制御パラメータ a との相関図から近似曲線を作成し、実験で取得した加速度データに対して新たに閾値を算出することで EER の測定シミュレーションを行う。

5.1 実験環境

本実験では加速度センサとボタンを内蔵した端末として、Wii リモコン®を使用する。実験機器の仕様を表 1 に示す。動作区間の指定には、図 5 に示す端末背面のボタンを使用した。

表 1. 実験機器の仕様

機器名	Wii リモコン
加速度のレンジ	X,Y,Z 各軸 ±3G
サンプリングレート	100Hz

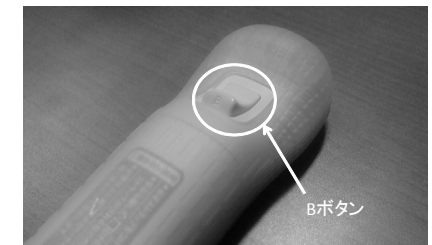


図 5. 認証動作区間の指定に使用するボタン

実験の手順を以下に示す。本人認証実験の被験者は 20 代男性 12 名、実験期間は 5 日間である。まず、1 日目に被験者が任意の同じ動作を 5 回行うことで、自分の鍵となる動作の登録を行う。このとき、腕振りの動作は同じで、ボタンの押下/解放の動作を施す場合とそうでない場合の 2 種類の動作を登録する。そして、実験期間中は毎日各人の登録した 2 種類の動作で各 5 回ずつ認証を行った。したがって、各被験者から得られる計 50 回分の認証データを使用して、それぞれの認証動作の FRR を測定する。

また、成りすまし実験では、本人認証実験の被験者のマスタデータに対し成りすましを試みる。成りすましの被験者は本人認証実験の被験者とは別の 20 代男性 18 名である。1 人の被験者が成りすましを試みる対象は 4 人分の動作である。各対象あたり、ボタンの押下/解放の有無で 2 種類の動作がある。動作ごとの認証試行回数は 5 回とした。したがって、1 人当たり計 40 回成りすましを試行することで FAR を測定する。成りすまし被験者には、実験の前に、成りすまし対象が描画した図形の情報を事前に

与えるとともに、動作を正面から撮影した映像を納得するまで見る機会を与えた。ただし、ボタンの操作パターンの情報は与えない。なお、両実験ともに、認証動作は全て被験者の利き手でいった。被験者は全員右利きである。

5.2 実験結果

まず、ボタンの押下/解放を行う工夫の有無、および、マスターデータの更新の有無について比較を行った結果を図6に示す。認証用代表マスターデータは、時系列で最近登録されたマスターデータ(式(7))を使用した。また、閾値は閾値制御パラメータ a を実験的に変化させ、各閾値での FAR, FRR の測定を行った。閾値制御パラメータ a の刻み幅は 0.1 とし、 a を 0 から 19.9 まで変化させた。凡例の"非更新"はマスターデータの更新を行わなかったことを意味し、"ボタン不使用"は認証動作時にボタンの押下/解放を行う工夫を施さないことを意味している。図中の FRR, FAR は全員の平均値である。また、図中の矢印は EER, すなわち $FRR=FAR$ となる箇所を表している。図より、マスターデータの更新を行い、かつ、加速度データとボタンの押下/解放を組合せた方法が最も EER が低いことが分かる。

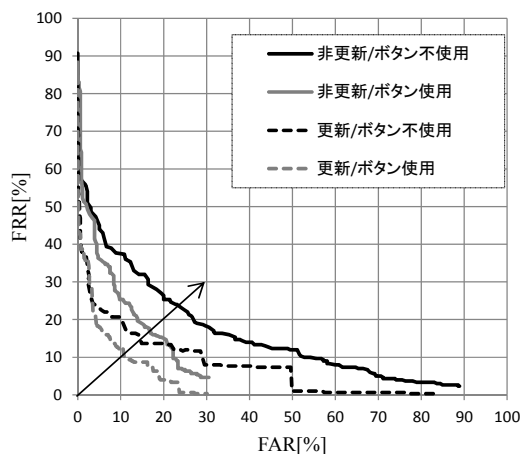


図 6. 実験結果の ROC 曲線

次に、得られた認証時のデータから相関図と近似式を作成し、新たに算出した閾値を用いて EER の測定シミュレーションを行った。ここでは、認証用代表マスターデータには時系列で最近登録されたマスターデータ(式(7))を使用し、閾値算出用代表マスターデータにはマスターデータの重心に最も近いマスターデータ(式(6))を使用した。なお、近似の方法は累乗近似を用いた。閾値制御パラメータ b の刻み幅を 0.01 とし、 b を 0 から 1.99 まで変化させ、各場合における FAR, FRR を測定した結果を図7に示す。図中の

実線は閾値の決定に近似式を利用した場合であり、破線は閾値を全て実験的に決定した場合である。また、図6、図7の EER をまとめたものを表2に示す。これらの結果から、ボタンを使用するマルチモーダル認証において、マスターデータの更新を行い、かつ、近似曲線を使用して閾値を計算することで EER をさらに減少させることができていることが分かる。

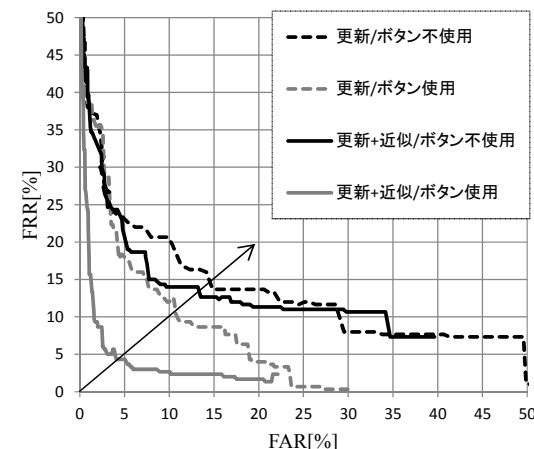


図 7. 閾値の決定法の比較

表 2. 各認証方式の EER [%]

ボタンの使用	マスターデータの更新		
	非更新	更新	更新+累乗近似 (提案方式)
ボタン不使用	23.6	14.6	13.4
ボタン使用有	16.6	10.7	4.3

次に、被験者が登録した認証動作の例を図8に示す。図8では、被験者はひらがなの“お”を描いており、実線部がボタンを押しながら動作を行った部分(認証に使用するデータの取得区間)、破線部がボタンを押さずに認証動作を行った部分(動作中の囿となる区間)を表している。図8では破線部は2箇所あるので、この動作では囿となる動作が2回含まれている。

また、ボタンを使用するマルチモーダル認証について、認証動作中の囿となる動作

の割合と各被験者の EER の相関を求めた結果を図 9 に示す。EER は、マスタデータの更新を行う場合の結果を使用した。また、図 9 の横軸は、全動作区間に対する ㊦となる動作区間の割合であり、ボタンを使用せず全区間でサンプリングした場合のサンプル数とボタン押下区間のみでサンプリングした場合のサンプル数の比率から求めた。12 人の被験者のうち、動作中の ㊦の回数を 1 回とした被験者は 9 人、2 回とした被験者は 3 人であった。図 9 より、㊦区間を 2 回とした被験者は、1 回の被験者と比べ、EER が特に低くなっていることが分かる。また、認証動作中の ㊦の区間が占める割合が大きい方が、EER が低い傾向があることが分かる。これは、㊦区間の数や ㊦の区間の長さが増大するほど、成りすまし被験者が認証動作中のボタンを押すタイミングや区間を正確に判別することが困難になるため FAR が低くなり、結果として EER が低下したためだと考えられる。なお、今回の実験で使用したボタンは 1 個のみであるが、使用するボタンの数を増やすことで成りすましがより困難になると予想される。ただし、ユーザにとっての使い易さも低下する可能性があるため今後の検証が必要である。

また、提案方式において全被験者の平均 FRR と平均 FAR から求めた EER は 4.3% であったのに対し、被験者ごと FRR と FAR の EER の平均は 2.1% であったため、各被験者の動作に対応した閾値の算出法にはさらなる検討の余地がある。加えて、今回は 12 種類の動作を用いて相関図を作成したが、より多くのデータから相関図を作成したほうが、より汎用性の高い近似曲線を作成できる可能性があると考えられる。

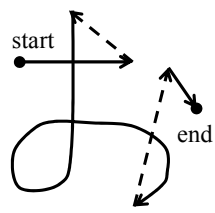


図 8. 認証動作の例

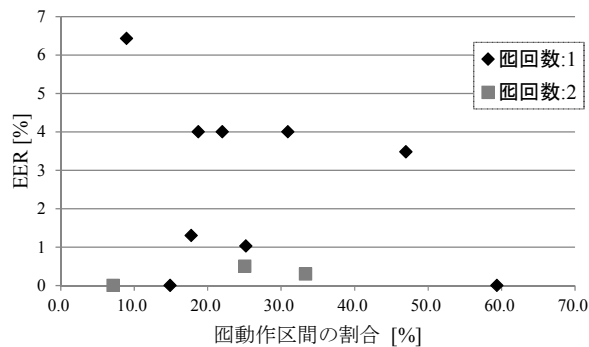


図 9. ㊦となる動作の量と各被験者の EER との関係

6. おわりに

本稿では、加速度センサと携帯端末に付属したボタンの操作を併用したマルチモーダル個人認証についての検討を行った。実験より、加速度だけでなく、ボタン操作を

加えたマルチモーダル個人認証を行うことで FAR を低減させ、結果として EER を改善できることが確認できた。また、マスタデータの更新を行い、さらに、実験により得られた加速度データを用いて最適な閾値を算出することにより被験者の動作毎の EER のばらつきを抑制し、動作の種類に依存しない閾値制御パラメータ b によって FAR, FRR の調整を行うことができた。

しかし、閾値制御パラメータ b を用いて算出した閾値によって求めた結果と、各被験者の EER の平均値との間にはまだ差があり閾値の算出法にはまだ改善の余地があると思われる。また、今回実験で用いた動作は肩を支点とした動作で、どこでも行えるような動作ではないことから、汎用性が高いとは言い難い。

今後の課題として、閾値の算出法のさらなる検討と、より簡単な動作を行った場合の認証精度の検証が挙げられる。

謝辞

本研究の一部は科学研究費補助金基盤(C)(22500105)の助成を受けたものである。

参考文献

- 1) 石原進, 太田雅敏, 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, Dec. 2005.
- 2) 松尾賢治, 奥村文教, 橋本真幸, 小池淳, 久保田彰, 羽鳥好律, “腕の振りに基づく生体認証とテンプレート更新による経時変化の抑制,” 電子情報通信学会論文誌, Vol.J91-B, No.6, pp.695-705, June 2008.
- 3) 染谷大介, 田中雄一, 長谷川まどか, 加藤茂夫, “腕振り動作による個人認証方式に関する検討,” 画像電子学会第 38 回年次大会予稿集, P-2, June 2010.
- 4) Kresimir Delac, Mislav Grgic, “A Survey of Biometric Recognition Methods,” 46th International Symposium Electronics in Marine, 2004.
- 5) Paul Keir, Jocelyn Elgoyhen, Martin Naef, John Payne, Martyn Homer, Paul Anderson, “Gesture-recognition with Non-referenced Tracking,” 3DUI, pp.151-158, 3D User Interfaces (3DUI'06), 2006.
- 6) J. Liu, L. Zhong, J. Wickramasuriya, V. Vasudevan, “User Evaluation of Lightweight User Authentication with a Single Tri-Axis Accelerometer,” in Proc. ACM Int. Conf. Human Computer Interaction with Mobile Devices and Services (MobileHCI '09), Sep. 2009.
- 7) A. Zaharis, A. Martini, P. Kikiras, and G. Stamoulis, “User Authentication Method and Implementation Using a Three-Axis Accelerometer,” Mobile Lightweight Wireless Systems: Second International ICST Conference, Mobilight 2010, pp.192-202, May 2010.