

マルチタッチ操作を利用したリズム認証方式の検討

喜多 義弘¹ 神里 麗葉² 朴 美娘¹ 岡崎 直宣²

概要：スマートフォンなどのモバイル端末の普及に伴い、端末内の個人情報の漏洩が問題視されている。そのため、多くのモバイル端末には画面ロック機能が搭載され、その解除認証に暗証番号やパターンなどの認証方式が利用されている。しかし、既存の認証方式では、認証動作の覗き見や録画・解析する攻撃方法への耐性がないものが多く、認証情報が他人にばれてしまう危険性がある。本研究では、認証の際、画面を見る必要がなく、認証動作を人の目や録画機器の下に曝さないで行うことのできるリズム認証方式に注目し、そこで課題となっていた認証精度の向上を図るための手法について検討する。具体的には、ユーザが画面上を複数の指でタップし、そのタップ情報と自己組織化マップを照合しながらユーザ個人を識別する。複数の指でタップすることで、認証に用いることができる特徴量が増え、それらを有効に利用することで認証精度が向上することを示す。

1. はじめに

近年、BYOD によるビジネスモデルのツールや個人のライフアイテムとして、スマートフォンをはじめとするモバイル端末が普及してきており、端末内の社内情報や個人情報の守秘への意識が高まりつつある [1]。多くのモバイル端末には、他人から端末を操作されないように画面ロック機能が搭載されており、そのロック解除に暗証番号やパターンなどの認証方式が利用されている。しかしながら、人通りの多い場所や公共施設などで画面ロックを解除する際には、第三者や監視カメラなどにより肩越しから認証動作を覗き見られ、認証情報が漏れてしまうこと（以下、覗き見攻撃）が考えられる。

覗き見攻撃への対策として、従来から様々な研究が行われている [2]～[4]。しかし、これらの研究は認証動作をカメラによって覗き見され、認証動作を解析される攻撃（以下、録画攻撃）に対して、十分な耐性を有していない。そのため、利用者が画面を見ながら認証動作を行う以上、その認証画面を録画されていないことが保障されない限り、十分な安全性を確保できない。

録画攻撃対策の先行研究として、自己組織化マップを用いたリズム認証方式 [5], [9] が行われている。この認証方式は、タッチスクリーンをタップし、そのタップのイベント時間を自己組織化マップに入力し、学習・分析によりそ

の類似度に応じて個人認証を行う。そのため、利用者は画面上のタップのみで認証を行うことができるため、鞆やポケットの中などに端末を入れたまま画面を見ずに認証情報を入力でき、認証画面を録画されることはなくなる。しかし、この方式は、タップのイベント時間のみを認証情報にしているため、マルチタッチ操作による指の識別や指間の距離の違いには対応しておらず、認証精度も十分ではない。

そこで本研究では、タップのイベント時間だけでなく、タップした指の識別および指間の距離も自己組織化マップに入力し、マルチタッチ操作への対応と認証精度の向上を図る。タップした指の識別には、タップ点の座標と閾値を用いて最短距離の点同士をクラスタリングし、その集合体によって識別する。また、本人拒否率 (False Reject Rate, 以下, FRR) および他人受入率 (False Accept Rate, 以下, FAR) の低減を考慮し、全ての特徴のうち利用者本人の再現率が高い特徴、および、他人との特徴差が大きい特徴をそれぞれ用いた場合の認証精度についても検証する。

2. 関連研究

2.1 リズム認証

リズム認証とは、連続した入力的时间差を認証情報として用いる認証方法であり、利用者個人の行動的特徴を活かしたバイオメトリクス認証の一つである。リズム認証は、従来からキーボードなどの入力装置を対象とした研究 [6][8] が行われており、現在は、モバイル端末向けにタップ入力を利用した研究が行われている [9]。リズム認証を用いることにより、利用者は認証画面を見ずに、タッチスクリーンへのタップ入力によって認証を行うことができる。その

¹ 神奈川工科大学
Kanagawa Institute of Technology
² 宮崎大学
University of Miyazaki

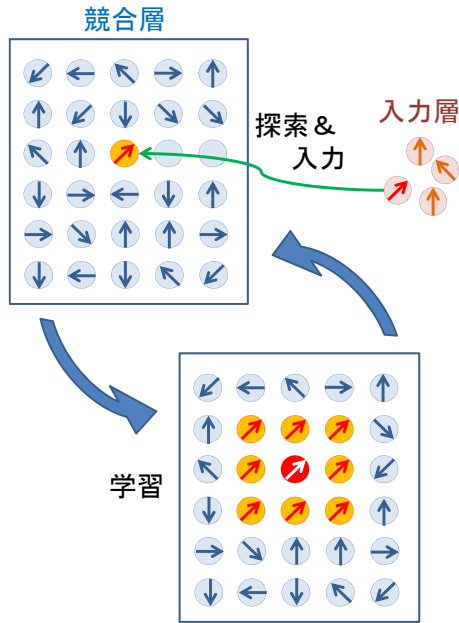


図 1 SOM の基本概念
Fig. 1 Basic concept of SOM

ため、他人や監視カメラに認証画面を露呈することがなくなり、認証情報の漏洩を防ぐことが期待できる。しかし、現在のリズム認証の認証情報は入力的时间差のみであるため、FRR や FAR が増えやすく、認証精度が十分ではない。

そこで認証精度を高めるため、入力的时间差だけでなく、更なる個人の行動的特徴を認証情報として追加することが考えられる。

2.2 自己組織化マップ

自己組織化マップ (Self Organizing Maps, 以下, SOM) とは、競合学習型ニューラルネットワークの一種であり、与えられた入力情報の類似度を 2 次元空間のマップ上での距離で表現するモデルである [10]。

図 1 に、SOM の基本概念を示す。SOM は、入力層と競合層の 2 つの層から成り、入力層には入力ベクトルを持つ複数のノードを、競合層には入力ベクトルと同次元の参照ベクトルを持つ複数のノードを 2 次元空間上に規則的に配置している。入力ベクトル $\vec{i}$ が入力層に与えられたとき、競合層において $\vec{i}$ との内積が最も大きい参照ベクトルを持つノードを、勝利ノードと呼ぶ。勝利ノード v が決定したとき、勝利ノード v とその周辺のノードに対して以下の式 (1)~(3) を適用し、勝利ノードも含むノード n の参照ベクトル $\vec{r}_n$ を入力ベクトル $\vec{i}$ へ近づけるための学習を行う。式において、2 次元空間上での勝利ノードの座標を $L_v = (x_v, y_v)$ 、ノード n の座標を $L_n = (x_n, y_n)$ とする。また、 T は予め設定した学習の総回数、 t は学習回数、 σ は近傍の広がりを表す正規分布の標準偏差に対応した正の定数とする。

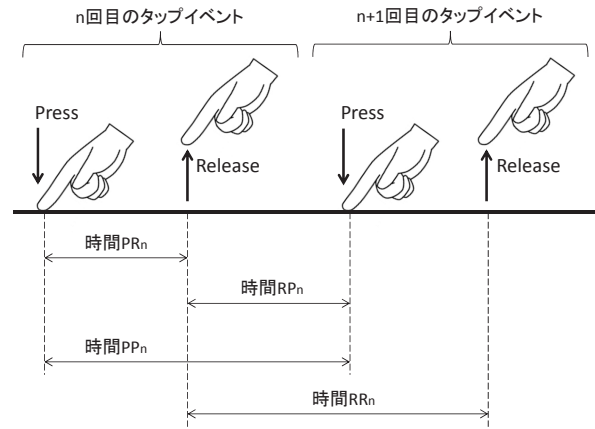


図 2 タップのイベント時間の定義
Fig. 2 Definitions of tap event time

$$\alpha(t) = 1 - \frac{t}{T} \quad (1)$$

$$H_n(t) = \alpha(t) \cdot \exp\left(-\frac{|\vec{L}_n - \vec{L}_v|^2}{2\sigma^2}\right) \quad (2)$$

$$\vec{r}_n(t+1) = \vec{r}_n(t) + H_n(t) \cdot |\vec{i}(t) - \vec{r}_n(t)| \quad (3)$$

これらの式を用いて学習を行うことにより、特徴が似たデータは近い場所に、異なる特徴のデータは遠い場所にマッピングされるため、複数の多次元データを視覚的に解りやすく分類することができる。

SOM の特性を活かしたリズム認証の先行研究 [5], [9] が行われており、認証の判定における SOM の有用性が報告されている。本研究においても認証の判定に SOM を利用し、認証情報の追加または選択により認証精度の向上を目指す。

3. 提案手法

本論文では、従来のリズム認証方式の認証精度の向上とマルチタッチ操作への対応を図るために、タップのイベント時間だけでなく、タップした指の識別および指間の距離も認証情報に追加した認証方法を提案する。以下では、本提案で扱う個人特徴量の定義、クラスタリングによる指の識別、および、SOM を用いた認証方法について述べる。

3.1 個人特徴量の定義

複数回のタップによる一連のリズムを認証情報として登録する。その際、個人を識別するための特徴を定義する必要がある。以下に、個人を特定するための特徴量の定義を示す。また図 2 に、タップのイベント時間の定義を併せて示す。各定義に付加した n は、一連のリズムを入力するために必要とする総タップ数のうち、任意のタップ回を示す。各定義においてタップ操作全体を指す場合は、 n を付加しない。

- n 回目にタップした指 (以下、指 F_n)
- n 回目にタップした点と $n+1$ 回目にタップした点と

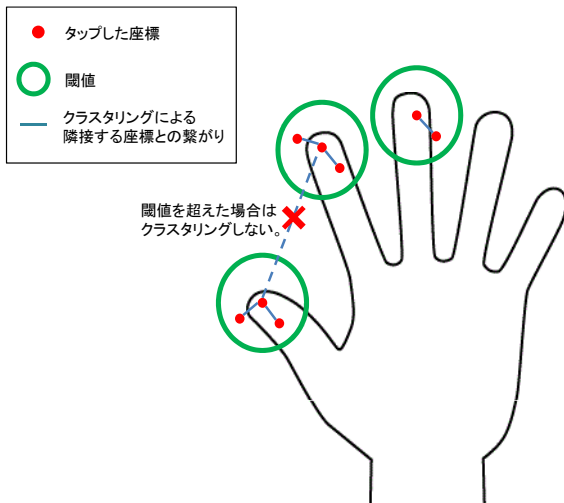


図 3 タップ座標のクラスタリングによる指の識別

Fig. 3 Discrimination of fingers by clustering coordinates of the tap point

の距離（以下、距離 D_n ）

- n 回目にタップしてから指を離すまでの時間（以下時間 PR_n ，図 2 参照）
- n 回目のタップで画面から指を離し， $n+1$ 回目のタップを行うまでの時間（以下，時間 RP_n ，図 2 参照）
- n 回目のタップから $n+1$ 回目のタップまでの時間（以下，時間 PP_n ，図 2 参照）
- n 回目のタップで指を離してから， $n+1$ 回目のタップで指を離すまでの時間（以下，時間 RR_n ，図 2 参照）

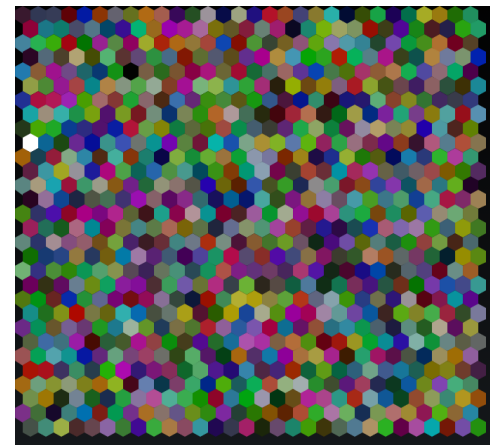
従来のリズム認証方式では，時間 PR および時間 RP のみを認証情報にしていたため，タップの指が異なってもリズムが合っていれば，他人を利用者本人として誤認証することがあり得る．指の識別と指間の距離を認証情報として追加し，タップのイベント時間を細分化することにより，より正確に認証の判定を行うことができる．

3.2 タップ座標のクラスタリングによる指の識別

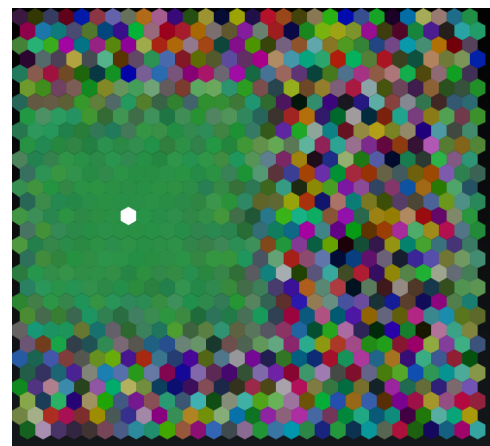
タップした指を識別するために，タップした座標のクラスタリングによって指の識別を行う．図 3 に，タップ座標のクラスタリングによる指の識別について示し，以下では座標のクラスタリングを行う手順を示す．

- (1) 閾値を予め定める．
- (2) タップした点全ての座標 (x, y) を取得する．
- (3) 全ての点に対し，二点間の距離が小さい点同士から順にクラスタリングを行う．
- (4) 二点間の距離が閾値を超えるまで手順 (3) を繰り返す．

この手順により，同一の指でタップされた可能性が高い点同士を 1 つのクラスにまとめることができ，タップした指を識別することができる．指の識別により，複数の指で同時にタップイベントが発生しても，どの指によってタップされたかを判定できるため，マルチタッチ操作へ対



初期状態



学習回数10000回

図 4 SOM の初期状態と学習完了状態

Fig. 4 Initial state and learning completed state of SOM

応することができる．

3.3 SOM を用いた認証方法

モバイル端末の利用者は各端末につき 1 名である場合が多く，複数の利用者で共有することは少ない．そのため，端末の利用者は 1 名であることを想定する．

まず，利用者は認証情報を登録するために，端末のタッチスクリーン上で任意のリズムをタップする．この動作をリズムおよび使用した指の順番は変えずに複数回繰り返す，同一リズムの認証情報を複数個登録する．

次に，登録した認証情報を用いて SOM の学習を行う．図 4 に，SOM の初期状態と学習完了状態を示す．学習回ごとに複数登録した認証情報の中からランダムに 1 つの認証情報を選択し，学習する．学習を一定数以上繰り返し，利用者固有の SOM を作成する．図 4 の下図は，学習回数が 10000 回のときの SOM である．マップ上の白い点は勝利ノードを示す．学習が終了すると，勝利ノードの周りの値が勝利ノードの値に収束しているため，同じ色の近傍領域ができる．また，全ての学習回において勝利ノードの座

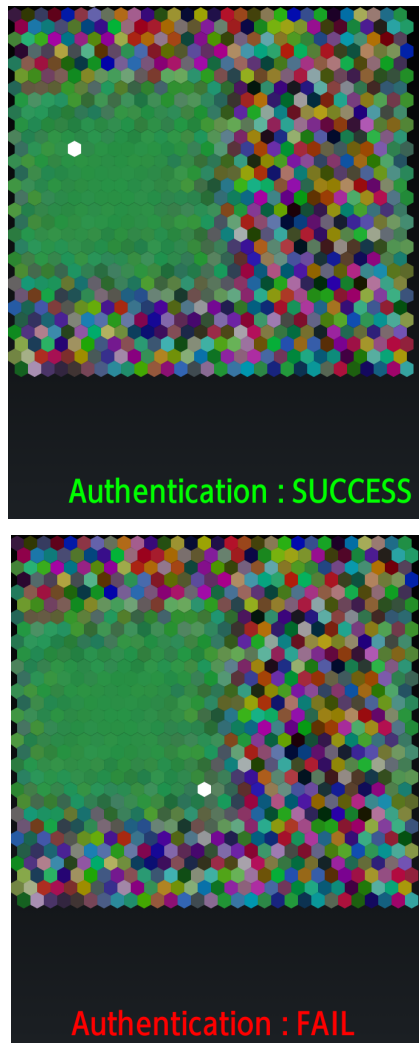


図 5 (上) 認証成功時の SOM / (下) 認証失敗時の SOM
Fig. 5 (Upper)SOM when authentication is success / (Lower)SOM when authentication is fail

標の平均値をとり、その平均値に最も近い座標のノードをマップの重心とする。

画面ロック解除時に、登録したリズムを端末のタッチスクリーン上でタップする。図 5 に、認証成功時または認証失敗時の SOM を示す。マップ内の白い点は入力されたリズムに最も近いノードである。作成した SOM 内において、入力されたリズムに最も近いノードを探し、そのノードとマップの重心になるノードとのユークリッド距離を算出する。そして、ユークリッド距離が予め定めた閾値以内であれば認証成功とし、閾値以上であれば認証失敗とする。

本研究では、認証判定の精度を高めるために、トラス型 SOM[11] を用いる。トラス型 SOM は、マップ端の上下左右を結合したマップであり、近傍領域のばらつきがなく、ノード間のユークリッド距離を正確に導き出すことができる。

4. 評価および考察

4.1 個人特徴量の測定

認証情報の有用性を確かめるために、個人特徴量の測定を行った。被験者は、神奈川工科大学の学生 7 名と宮崎大学の学生 7 名の計 14 名である。

被験者は以下の条件に従い、モバイル端末のタッチスクリーン上で童謡「猫踏んじゃった」の冒頭 4 小節をタップする。タップに使用する指、指の順番、リズムの速さについては被験者の任意とした。試行ごとに 30 秒～1 分程度のブランクを設け、計 5 回の試行回数で実施し、3.1 節で定義した 6 つの個人特徴量の相対的標準偏差を算出した。相対的標準偏差は、データのばらつきを示すための標準偏差を平均値で割った百分率の値であり、尺度や種類が異なる各データのばらつきを相対的に比較することができる。相対的標準偏差 RSD の定義式を、以下に示す。

$$RSD = \frac{SD}{AVE} \times 100 \quad (4)$$

表 1 に、各被験者における特徴量の相対的標準偏差を示す。各被験者および各特徴量の値は、式 (4) の SD に 1 つの特徴に対する試行 5 回分の標準偏差を、 AVE に試行 5 回分の平均値をそれぞれ入れて算出した。表の下部には、各特徴量での相対的標準偏差の平均値を示す。この表により、被験者本人が入力した認証情報のばらつきを確認することができ、値が小さいほどばらつきが小さく、入力が安定している。そのため、相対的標準偏差の値が小さい特徴量を認証判定に用いることにより、FRR の低減を期待することができる。表中の平均値により、値が小さい特徴量は指 F 、距離 D 、時間 PP の 3 つであることから、これら 3 つの特徴量を FRR 低減重視の特徴量とする。

表 2 に、全被験者における特徴量の相対的標準偏差を示す。各特徴量の値は、式 (4) の SD に 1 つの特徴に対する被験者 14 人分の標準偏差を、 AVE に被験者 14 人分の平均値をそれぞれ入れて算出した。この表により、他人が入力した認証情報のばらつきを確認することができ、値が大きいほどばらつきが大きく、他人との差が明確に表れやすい。そのため、相対的標準偏差の値が大きい特徴量を認証判定に用いることにより、FAR の低減を期待することができる。表中の平均値により、値が大きい特徴量は指 F 、距離 D 、時間 RR の 3 つであることから、これら 3 つの特徴量を FAR 低減重視の特徴量とする。

4.2 認証情報の違いによる FRR および FAR の測定

SOM に入力する認証情報による認証精度の違いを確認するために、入力する特徴量ごとに FRR および FAR の測定を行う。従来のリズム認証方式や 4.1 節で定義した特徴量を考慮し、以下の特徴量の組み合わせをそれぞれ入力する。

表 1 各被験者における特徴量の相対的標準偏差

Table 1 Relative standard deviation of characteristic values on each subject

	指 F	距離 D	時間 PR	時間 RP	時間 PP	時間 RR
被験者 1	0.00	7.02	13.58	4.81	7.52	15.14
被験者 2	59.39	32.38	13.63	10.16	11.90	16.02
被験者 3	3.70	13.43	14.19	8.97	10.16	14.88
被験者 4	10.00	14.65	10.99	9.23	11.00	16.12
被験者 5	0.00	6.74	10.97	10.34	12.66	18.39
被験者 6	49.87	21.12	12.15	4.71	6.02	8.35
被験者 7	30.05	6.56	11.54	27.37	34.62	42.41
被験者 8	0.00	8.04	13.74	36.30	13.12	14.06
被験者 9	0.00	10.28	11.79	10.90	8.13	7.82
被験者 10	0.00	5.32	15.58	14.35	7.55	9.89
被験者 11	0.00	9.60	11.99	9.38	7.38	7.00
被験者 12	0.00	10.14	13.08	13.00	9.37	9.58
被験者 13	0.00	9.89	14.39	21.63	11.36	12.76
被験者 14	0.00	4.45	10.58	16.49	8.36	9.34
平均	10.93	11.40	12.73	14.12	11.37	14.41

表 2 全被験者における特徴量の相対的標準偏差

Table 2 Relative standard deviation of characteristic values on all subject

	指 F	距離 D	時間 PR	時間 RP	時間 PP	時間 RR
相対的標準偏差	118.54	28.53	13.53	14.99	18.23	24.38

- 従来のリズム認証方式
時間 PR , 時間 RP
- 全ての特徴量
指 F , 距離 D , 時間 PR , 時間 RP , 時間 PP , 時間 RR
- FRR 低減重視の特徴量
指 F , 距離 D , 時間 PP
- FAR 低減重視の特徴量
指 F , 距離 D , 時間 RR
- FRR および FAR 低減重視の特徴量
指 F , 距離 D , 時間 PP , 時間 RR

まず, 上記の特徴量の組み合わせをそれぞれ入力し, 学習させた SOM5 種類を作成する. 初期マップは 5 種類ともに同じマップを使う. 学習に用いる認証情報は同じ入力者によるタップ情報を 10 種類用意し, それぞれのマップに同じタップ情報を同じ順番で入力する. SOM の大きさは 30×30 (ノード数 900) とし, 学習回数は 10000 回とした. そして, 作成された 5 種類の SOM を用いて, 入力者本人と入力者以外の人それぞれ 20 回ずつ入力し, その認証の成否を確認する. 以上のマップ作成から認証の正否確認までの作業を, 閾値を変更しながら 10 回繰り返し, 入力者本人と入力者以外のそれぞれ計 200 回の試行を対象に, FRR および FAR の測定を行う. 認証の閾値は, 重心ノードからのユークリッド距離でノード 1 個分~10 個分の範囲を, ノード 1 個分ずつ変更する. 認証対象のノードと重心ノードとの距離が閾値以内であれば認証成功とし, 閾

値外であれば認証失敗とする. FRR, FAR, 認証精度の定義式を以下に示す.

$$FRR(\%) = \frac{\text{入力者本人の認証成功数}}{\text{試行回数}} \times 100$$

$$FAR(\%) = \frac{\text{入力者以外の認証成功数}}{\text{試行回数}} \times 100$$

$$\text{認証精度}(\%) = 100 - \frac{FRR + FAR}{2}$$

図 6~図 10 に, それぞれの特徴量の組み合わせを用いた場合の FRR および FAR を示す. 全ての方式において, 閾値がノード 5 個分前後で FRR および FAR とともに低いことが確認できる. そして, FRR と FAR のグラフの交点にあたる等価エラー率 (Equal Error Rate, 以下, EER) は, 従来方式が最も高いことから, 特徴を追加した提案方式により認証精度が向上したと考えることができる.

表 3 に, FRR および FAR を認証精度の定義式に当てはめて算出した, 各特徴量の組み合わせによる認証精度の比較を示す. 従来方式では認証精度が 70%であるのに対し, 全ての特徴量を用いた場合は 85%であり, 従来方式よりも認証精度が向上したことを確認できた. FRR 低減重視, または, FAR 低減重視の方式の場合は, それぞれで FRR または FAR が低減されている傾向があるが, 認証精度については, 全ての特徴量を用いた場合と比べて大きな向上はなかった. そして, FRR および FAR 低減重視の方式の場合は認証精度が 90%であり, 全ての方式の中で最も高い認証精度になった. これにより, FRR および FAR 低減重

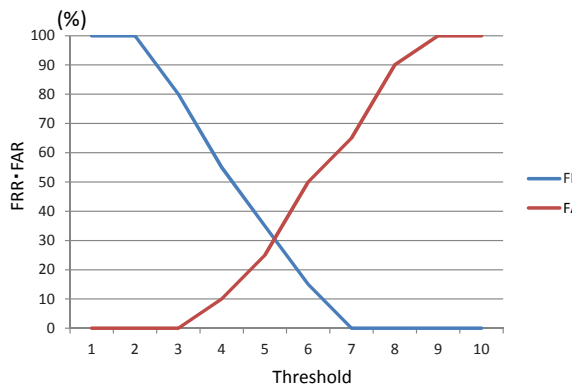


図 6 従来方式を用いた場合の FRR および FAR

Fig. 6 FRR and FAR in the case of using the existing method

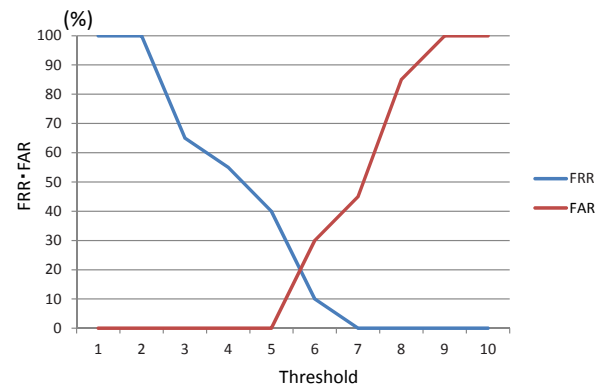


図 9 FAR 低減重視の場合の FRR および FAR

Fig. 9 FRR and FAR in the case of the importance FAR reduction

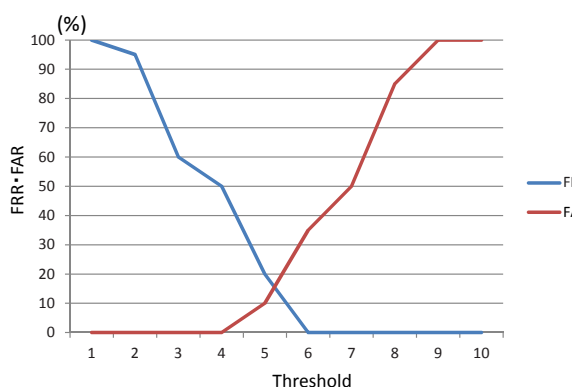


図 7 全ての特徴量を用いた場合の FRR および FAR

Fig. 7 FRR and FAR in the case of using all characteristic values as the authentication information

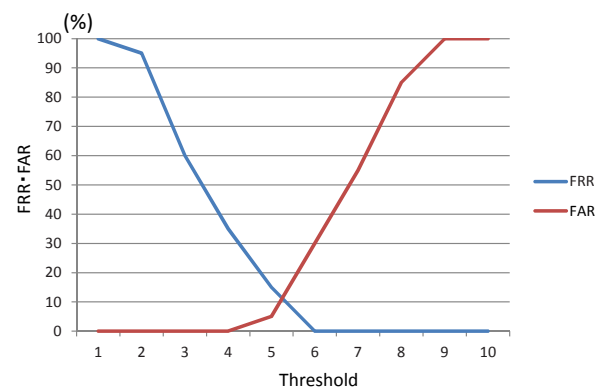


図 10 FRR および FAR 低減重視の場合の FRR および FAR

Fig. 10 FRR and FAR in the case of the importance FRR and FAR reduction

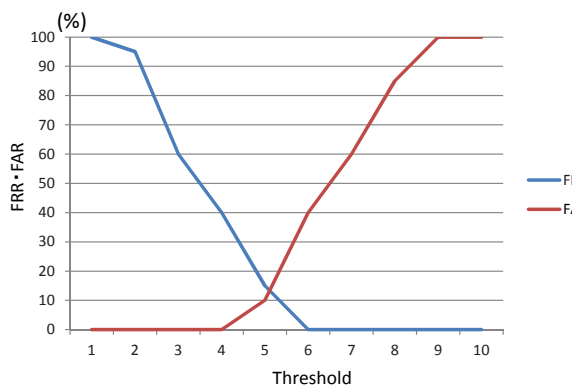


図 8 FRR 低減重視の場合の FRR および FAR

Fig. 8 FRR and FAR in the case of the importance FRR reduction

視の方式の特徴量である、指 F 、距離 D 、時間 PP 、 l_{avg} 、 RR は認証情報として有用であると言える。

しかし、全ての方式において認証精度が 50~90%であることから、認証方式としての実用性は十分ではない。今後、認証精度を更に向上させるべく、SOM の作成方法や認証方法について改良する必要がある。

表 3 特徴量の組み合わせによる認証精度の比較

Table 3 Comparison of authentication accuracy by the combination of characteristic values

	認証精度 (%)
従来方式	70
全ての特徴量	85
FRR 低減重視	87
FAR 低減重視	80
FRR および FAR 低減重視	90

4.3 マルチタッチ操作の活用と問題点

指の識別や指間の距離も認証情報として扱うことにより、マルチタッチ操作を活用した認証入力を行うことができる。マルチタッチ操作により、タップ入力のパターンを増やすことができるため、例えば、端末のスクリーンをタップする音により、リズムを他人に聞かれたとしても、認証情報が全て漏れることがない。

しかし、マルチタッチ操作によって操作が複雑化することにより、利用者の誤操作や誤認証が発生することもある。本提案方式は、マルチタッチ操作に対応できるが、その操作性や利便性についても考慮する必要がある。

5. おわりに

本研究では、タップのイベント時間だけでなく、タップした指の識別および指間の距離も自己組織化マップに入力し、マルチタッチ操作への対応と認証精度の向上を目標としたリズム認証方式について提案をした。タップした指の識別には、タップ点の座標と閾値を用いて最短距離の点同士をクラスタリングし、その集合体によって識別することにより実現できた。

そして、FRR および FAR の低減を考慮し、全ての特徴のうち利用者本人の再現率が高い特徴、および、他人との特徴差が大きい特徴をそれぞれ用いた場合の認証精度についても検証した。その結果、FRR および FAR 低減重視を考慮した、指 F 、距離 D 、時間 PP 、時間 RR の特徴量が認証に有用であることを確認した。

本提案手法によって、リズム認証方式の認証精度向上やマルチタッチ操作への対応が期待でき、覗き見攻撃や録画攻撃により認証情報の漏洩を防止できることが見込まれる。

今後の課題として、認証精度の向上や SOM 作成の実用化を行う必要がある。

参考文献

- [1] “スマートフォン&タブレットの業務利用に関するセキュリティガイドライン,” 日本スマートフォンセキュリティフォーラム (JSSEC), 2012.
- [2] 石塚正也, 高田哲司, “振動機能を応用した携帯端末での個人認証における覗き見攻撃対策手法の提案,” Computer Security Symposium 2013, pp.708-715, 2013.
- [3] 高田哲司, “fakePointer: 映像記録による覗き見攻撃にも安全な認証方式,” 情報処理学会論文誌, Vol.49, No.9, pp.3051-3061, 2008.
- [4] 喜多義弘, 菅井文郎, 朴美娘, 岡崎直宣, 西村広光, 鳥井秀幸, 岡本剛, “STDS 認証方式における録画解析による攻撃への耐性に関する一検討,” 第 12 回情報科学技術フォーラム, RL-002, pp.1-8, 2013.
- [5] 市村亮太, 納富一宏, 斉藤恵一, “覗き見攻撃耐性を考慮したスマートフォンにおけるリズム認証手法,” マルチメディア, 分散, 協調とモバイルシンポジウム (DICOMO2013), pp.230-233, 2013.
- [6] T., Chang, C., Peng, C., Tsai, Y., Chen, and P., Cheng, “Personalized Rhythm Click Based Authentication System Improvement using a Statistical Classifier,” Proceedings of 2nd International Conference on Information Communication and Management (ICICM 2012), pp39-43, 2012.
- [7] T., Chang, C., Tsai, Y., Yang, and P., Cheng, “User Authentication using Rhythm Click Characteristics for Non-Keyboard Devices,” Proceedings of International Conference on Asia Agriculture and Animal, pp.167-171, 2011.
- [8] Jacob, O.W., “TapSongs: Tapping Rhythm-Based Passwords on a Single Binary Sensor,” Proceedings of the 22nd Annual ACM Symposium on User Interface Software and Technology, pp.93-96, 2009.
- [9] 野口敦弘, 納富一宏, 斉藤恵一, “ボタンレスで行うリズム認証手法～ピアノ経験者との比較によるリズムの個人

差検証,” マルチメディア, 分散, 協調とモバイルシンポジウム (DICOMO2012), pp.192-196, 2012.

[10] T. Kohonen., “Self-Organizing Map,” Springer, 2001.

[11] 徳高平蔵, 大北正昭, 藤村喜久郎, “自己組織化マップとその応用,” Springer, 2007.