第4回バイオメトリクスと認識・認証シンポジウム
2014年11月25日～26日（産業技術総合研究所）

自己組織化マップを利用したリズム認証における個人分類手法の提案

Proposal of Personal Classification Method for Rhythm Authentication using Self-Organizing Map

喜多義弘 † 朴美娘 † 岡崎直宣 ‡
† 神奈川工科大学
‡ 宮崎大学

Yoshihiro KITA† Mirang PARK† Naonobu OKAZAKI‡
†Kanagawa Insutitute of Technology
‡University of Miyazaki

アブストラクト 携帯端末に搭載されている画面ロック機能には，暗証番号やパターンなどの認証方式が用いられている．しかし，これらの認証方式は，第三者からの覗き見攻撃に対して脆弱である．我々は以前より覗き見攻撃への対策として，自己組織化マップを利用したリズム認証方式を提案してきた．しかしながら，対応できる人数に限りがあった．そこで本論文では，より実用的な認証を目指して，キーストローク認証と自己組織化マップによる分類手法を組み合わせた，リズム認証に適した個人分類手法について提案し，その実用性について考察を行う．この個人分類手法により，多人数において個人を識別でき，実用性や安全性が向上することが期待される．

1 はじめに

近年の携帯端末には，他人による不正使用の防止を目的として，個人認証を利用した画面ロック機能が搭載されている．その個人認証には，PIN，パスワード，パターン認証などが様々な認証方式が用いられているが，これらの認証方式は安全性が低い．特に覗き見攻撃に対して耐性がないため，人通りの多い場所で第三者や監視カメラなどにより肩越しから覗き見られ，認証情報が漏れてしまうことが考えられる．

覗き見攻撃対策の一つとして，自己組織化マップ（Self-Organizing Maps，以下，SOM）を用いたリズム認証方式 [1], [2] 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たイベント時間を SOM に入力し，学習および分析により登録情報と入力情報との類似度に応じて個人認証を行う．これにより，利用者は鞄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，認証画面を覗き見られることはなくなる．我々も以前に，マルチタッチ操作に対応したリズム認証方式 [3], [4] について提案した．マルチタッチ操作により，扱う認証情報が増え，認証精度が従来よりも向上した．しかし，SOM を用いた認証判定に対応できる利用者数に限りがあるため，多人数向けの個人認証には対応できない問題が出てきた．

そこで本研究では，多人数向けの個人認証に対応するため，パスワード認証とリズム認証を組み合わせた認証方式について提案する．具体的には，タップ数およびタップする指の順番をパスワードとするパスワード認証である程度の人数にまで本人候補を絞り込み，その候補から既存のリズム認証方式によって本人の認証を行う認証方式を提案する．また，SOM による認証判定を，2 点間の距離による判定から類似するノードによる判定へ変更することにより，1 つの SOM を用いてより多くのユーザを識別することを目指す．

2 関連研究

2.1 リズム認証方式

リズム認証方式とは，連続した入力の時間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．

納富らによって，シングルタップ操作によるリズム認証方式 [1], [2] が提案されている．この方式は，使用する指に関わらず，タップしたリズムを認証情報にする認証方式である．この方式は SOM 利用しており，タップのイベント発生時間および終了時間を入力データにしている．リズムのみであるため，画面が小さいモバイル端末でも適用しやすい利点がある．しかし，指の識別は行わないため，認証の際に画面をタップする音を他人が聞くことで，認証情報であるリズムが漏れ，他人が同様のリズムでタップすることで画面ロックを解除されてしまうこと

が考えられる．

我々は以前に，マルチタップ操作を利用したリズム認証方式 [3], [4] を提案した．この認証方式は，認証方式 [2] を基に，タップのイベント時間による特徴量を追加し，さらに指の識別や指間の距離など計 6 項目の入力データから SOM を作成し，その SOM を認証に利用した方式である．指の識別や指間の距離も特徴として加えることにより，ユーザ本人と他人との区別がつきやすくなり，従来のリズム認証方式よりも認証精度が向上した．

2.2 自己組織化マップ

自己組織化マップ（Self-Organizing Maps: 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 [5], [6].

SOM は入力層と競合層の 2 つの層から成る．入力層には入力ベクトルが割り当てられたノードを，競合層には入力ベクトルと同次元の参照ベクトルを割り当てられた，2 次元空間上で規則的に配置したノードをそれぞれ持つ．まず，入力ベクトル $\overrightarrow{i}$ が入力層に与えられたとき，競合層において $\overrightarrow{i}$ との内積が最も大きい参照ベクトルを持つノードを探索する．この探索により特定したノードを，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，勝利ノードを含むノード n の参照ベクトル $\overrightarrow{r_n}$ を $\overrightarrow{i}$ 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 $L_v = (x_v, y_v)$，近傍半径 θ 内のノード 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．

$$\overrightarrow{r_n}(t+1) = \overrightarrow{r_n}(t) + H_n(t) \cdot (\overrightarrow{i}(t) - \overrightarrow{r_n}(t)) \quad (1)$$

$$H_n(t) = \alpha(t) \cdot exp(-\frac{|\overrightarrow{L_n} - \overrightarrow{L_v}|^2}{2\sigma^2}) \quad (2)$$

$$\alpha(t) = 1 - \frac{t}{T} \quad (3)$$

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．また，ある勝利ノードとそれに特徴が似たデータとが集合した領域を，以降では近傍領域とする．

3 提案手法

本論文では，多人数向けの個人認証に対応するため，パスワード認証とリズム認証を組み合わせた認証方式について提案する．以下では，本研究で用いるパスワード認証方式とリズム認証方式について述べる．

3.1 タップ数および指の順番をパスワードとしたパスワード認証

リズム認証は，特定のリズムをタップすることによって認証を行う．リズムやタップする指の順番は，ユーザによって異なるため，これらの情報をパスワードとして扱うことを提案する．既存のリズム認証方式では，指の識別情報をイベント時間や指間の距離とともに SOM への入力情報にしている．本提案では，指の識別情報を SOM の入力情報から分離し，この識別情報を用いて指の順番を特定する．

指の識別情報は各タップ点の距離によって決定するため，画面上の 2 点をタップした指は同じかどうかを判断でき，具体的にどの指でタップしたかは特定できない．これにより，タップした指の順番で識別できるユーザ数 u は，タップ数を t，タップに使用する指の最大数を m とすると，以下の式によって求めることができる．

$$u = m^t \quad (4)$$

例えば，ユーザは任意のリズムを登録できることを想定し，片手で操作することを考慮してタップする指は 3 本，リズムの長さは 2 小節程度を想定し，タップ数を 10 打と仮定する．このときに識別できるユーザの最大数は式 (4) より，$3^{10} = 59,049$ 人となる．

これにより，本提案手法によって多人数のユーザを識別可能であることと考えられる．

3.2 多人数に対応した SOM を用いたリズム認証

前節において，タップする指の順番をパスワードとするパスワード方式によって多人数のユーザを識別可能であることを述べた．しかし，現実社会においてほとんどのユーザは使いやすい指使いをし，その指使いは共通であることが多い．そのため，指の順番だけでは多人数のユーザを識別することは難しい．

そこで，同じリズムかつ同じ指の順番のユーザを SOM によって分類し，個人認証を行う．以下に，SOM に入力する情報を示す．

- タップのイベント時間（図 1 参照）
  - 時間 PR_n

    n 回目の画面タップ（Press）から指を画面から離すまで（Release）の時間
  - 時間 RP_n

    n 回目の Release から $n+1$ 回目の Press までの時間

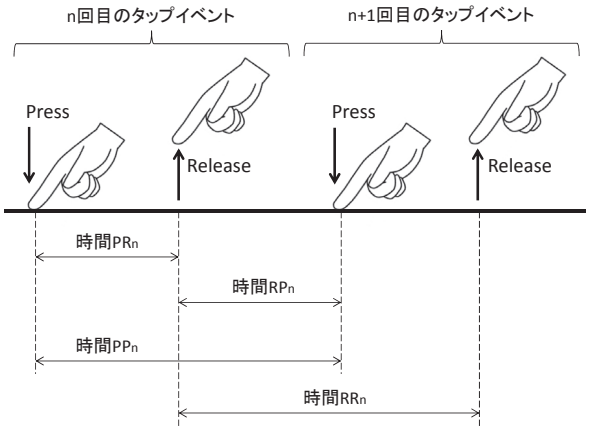

図 1: タップのイベント時間の定義

  - 時間 PP_n

    n 回目の Press から $n+1$ 回目の $Press$ までの時間

  - 時間 RR_n

    n 回目の Release から $n+1$ 回目の $Release$ までの時間

- 指間の距離 D_n

  n 回目のタップをした指と $n+1$ 回目のタップをした指との距離

- タップの圧力 P_n

  n 回目のタップをした指の画面押下圧力

これらの 6 種の情報をタップごとに計測し，ベクトル化して SOM へ登録する．SOM の作成方法は，2.2 節で述べた一般的な SOM の作成方法と同様である．

従来のリズム認証では，勝利ノードをユーザ本人の登録情報とし，認証時の入力情報をマッピングした際に勝利ノードと入力情報のノードとの 2 点間の距離によって認証判定を行っていた．しかし，複数のユーザを登録する場合，各ユーザの近傍領域が重複しないようにマッピングする必要があるため，1 つの SOM 内に少数のユーザしか登録できない問題があった．

そこで本提案での認証判定には，入力情報のノードに最も近い勝利ノードがユーザ本人の勝利ノードか否かによって判定する方法を用いる．具体的には，まずユーザの認証情報登録時に，各ユーザの勝利ノードが重複しないように，SOM 上にマッピングする．ベクトル化した認証情報を SOM に登録する際，最も類似したベクトルを持つノードをその登録者の勝利ノードにするが，他の登録者の勝利ノードと重複する場合は，次点で類似したノードを勝利ノードにする．次に認証時において，ベクトル化した入力情報に最も類似したノードを探索し，そのノードに最も近い勝利ノードの登録者と入力者とを比較する．このとき，登録者と入力者が一致していれば認証成功とし，していなければ認証失敗とする．提案手法によって，各ユーザの近傍領域の重複を許可することにより，より多くのユーザを管理できると考えられる．

この手法において注意すべき点は，予め入力者を固定してから認証入力を行う点である．入力者を固定していなければ，登録者との比較を行うことができない．そのため，タップする前にユーザ選択を行う必要がある．

4 評価および考察

4.1 SOM による複数のユーザの識別可能性についての評価

提案手法により，1 つの SOM 上で複数のユーザを識別することが可能かどうかを確認するために，被験者 5 人を対象に以下の実験を行った．

1. 童謡「猫ふんじゃった」のリズムで，全被験者が同じ指使いでタッチスクリーン上をタップする．
2. 手順 1 で得た各被験者のタップ情報を登録情報として，以下の条件に沿って SOM を作成する．
   - 各被験者の勝利ノードが重複しないようにマッピングする．
   - 各被験者の近傍領域の重複は許可する．
   - トーラス型 SOM[5] を利用し，学習回数は 30,000 回，学習の範囲である近傍領域は勝利ノードからノード 2 個分を半径とする．
3. 再び各被験者は手順 1 と同様にタップし，これを 30 回繰り返す．
4. 各被験者 30 回分のタップ情報を入力情報として，各入力情報のベクトルに最も近い参照ベクトルを持つノード上にマッピングする．マッピングされたノードを入力情報のノードとする．

図 2 に，SOM 上での入力情報のマッピング例を示す．本実験の SOM は，100 個の六角形のノードを 10×10 で蜂の巣状に敷き詰めた形になっており，1 つのノードには前述した 6 種のタップ情報をベクトル化したデータを含む．SOM 上の「User 番号 : 色名」を記述したノードは，各被験者の勝利ノードである．そして，色の点はその色に該当する被験者の入力情報であり，それらの点をマッピングしているノードは入力情報のノードである．

図 2 より，各被験者の勝利ノードの周辺に同じ色の入力情報が集まっていることが確認できる．これにより，入力

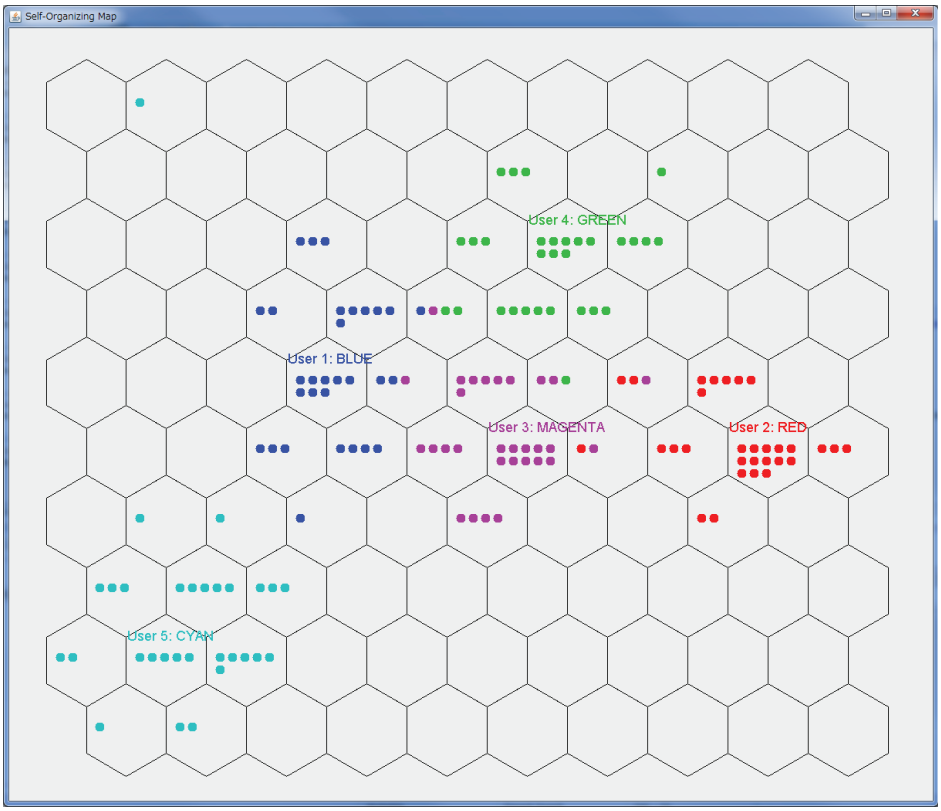

図 2: SOM 上での入力情報のマッピング例

情報の多くは被験者ごとに分類できるため，1 つの SOM で複数のユーザを識別することが可能であると考えられる．

しかし，同じノード内に複数の被験者の入力情報が含まれていたり，複数の勝利ノードからの距離が等しいノードに入力情報が含まれていたりする．これらの入力情報のノードから被験者を特定することは困難であるため，認証精度が低下することが考えられる．

4.2 複数のユーザへの実用性についての考察

本提案手法により，複数のユーザから特定のユーザを識別できるかどうかについて考察する．

本提案では，タップする指の順番をパスワードとするパスワード方式とリズム認証方式を組み合わせている．パスワード方式については，同じリズムであっても識別可能な最大ユーザ数は，3.1 節の式 (4) によって求めることができる．

4.1 節の実験で使用した，童謡「猫ふんじゃった」を例に考察する．この曲の 4 小節分のタップ数は，19 タップである．片手で入力することを考慮し，使用する指は 3 本とする．このとき、識別可能なユーザの最大数は，$3^{19} = 1,162,261,467$ 人となる．

しかし現実的には，よく利用されるタップする指のパターンはある程度絞り込まれる．例として，よく利用されるタップする指のパターン数を 100 パターンと仮定する．このとき，10,000 人のユーザから 1 人のユーザを特定するとき，同じパターンのユーザは，$10,000/100 = 100$ 人であると考えられ，この 100 人をリズム認証によって識別する必要がある．100 人を識別するには，SOM の規模を大きくすることにより対応できるが，その分だけ学習時間が増え，実用的な時間で SOM を作成することが困難になると考えられる．

5 おわりに

本論文では，多人数向けの個人認証に対応するため，パスワード認証とリズム認証を組み合わせた認証方式について提案した．具体的には，タップ数およびタップする指の順番をパスワードとするパスワード認証である程度の人数にまで本人候補を絞り込み，その候補から既存のリズム認証方式によって本人の認証を行う．さらに SOM での認証判定については，従来の勝利ノードと入力情報のノードとの距離で判定するのではなく，複数の勝利ノードから最も近い勝利ノードのユーザとの成否判定を行うことにより，SOM において複数のユーザを識別することを提案した．

実験による評価によって，多人数のユーザから特定のユーザを識別できることが確認できたが，認証精度が低

いという問題点も出てきた．しかし，パスワード認証によって多人数のユーザに対応できることから，本提案手法により多人数のユーザに対応した認証が可能であることが期待できる．

今後の課題として，SOM による認証判定を改良することにより，認証精度を高くすることが挙げられる．

参考文献

[1] 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.

[2] 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.

[3] 喜多義弘，神里麗葉，朴美娘，岡崎直宣，“自己組織化マップを利用したリズム認証方式とその認証精度に関する考察，”マルチメディア，分散，協調とモバイルシンポジウム（DICOMO2014），pp.1011-1017，2014.

[4] 喜多義弘，朴美娘，岡崎直宣，“ユーザの慣れによる認証精度の低下を考慮したリズム認証方式の提案，”コンピュータセキュリティシンポジウム（CSS2014），pp.1034-1041，2014.

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

[6] 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.