「テンポ感」を特徴量としたリズム認証の認証精度に関する考察

堀　孝浩 †　　喜多　義弘 ‡　　豊田　健太郎 †　　朴　美娘 †　　岡崎　直宣 ‡2

† 神奈川工科大学
〒 243-0292 神奈川県厚木市下荻野 1030

‡ 東京工科大学
〒 192-0982 東京都八王子市片倉町 1404-1

‡2 宮崎大学
〒 889-2192 宮崎県宮崎市学園木花台西 1-1

あらまし　モバイル端末の画面ロック解除には，パスワードやパターンが一般的であるが，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．そのため我々は，覗き見攻撃への対策として，ユーザが曲に合わせて画面をタップする，リズム認証方式を提案してきた．しかし，認証精度が低いという問題があり，原因として，特徴量の少なさが考えられる．そこで我々は，同一の曲であっても，ユーザによって，1 音毎の間隔，すなわちテンポに特徴があると考え，これを「テンポ感」と定義する．本論文では，ユーザの「テンポ感」を特徴量に追加したときの認証精度への影響を考察する．

Accuracy Improvement with “Tempo” Information on Rhythm Authentication

Takahiro Hori†　　Yoshihiro Kita‡　　Kentaroh Toyoda†　　Mirang Park†
Naonobu Okazaki‡2

†Kanagawa Institute of Technology.
Shimo-Ogino 1030, Atsugi, Kanagawa 243-0292, JAPAN
‡Tokyo University of Technology
Katakura 1404-1, Hachioji, Tokyo 192-0982, JAPAN
‡2 University of Miyazaki
Gakuenkibanadai-Nishi 1-1, Miyazaki 889-2192, JAPAN

Abstract　We generally use password or PIN code to unlock a smartphone but they are vulnerable to so-called shoulder hacking attack. As a countermeasure, we have proposed a rhythm authentication that a user taps screen with pre-defined music. However, the accuracy is not enough for general use. In this paper, we argue that tapped timings should differ by users even if they play same music. We call this feature as ‘tempo’ and show how authentication accuracy improves when adding the tempo information to the conventional features.

1　はじめに

近年，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ってきている [1]．他人による不正使用防止を目的とし，多くのモバイル端末には，画面ロック機能が搭載されている．そのロック解除には，暗証番号，パスワード，PIN などの認証方式が利用されている．しかし，これらの認証方式は，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（以下，覗き見攻撃）可能性が考えられる．

覗き見攻撃への対策として，従来からは様々な研究が行われている [2, 3, 4]．しかし，これらの研究は認証動作をカメラによって録画され，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，ユーザが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 (SOM: Self-Organizing Map) を用いたリズム認証方式が行われている [5, 6, 7]．この認証方式は，各ユーザの想像した楽曲のリズムに合わせてタッチスクリーンをタップし，そのタップ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，ユーザは画面上のタップのみで認証を行うことが可能なため，鞄やポケットの中などに端末を入れたまま認証が行うことができる．これにより，認証画面を録画されることが無くなり，録画攻撃への耐性を得た．

我々も以前に，自己組織化マップを利用したリズム認証方式認証方式 [7] について提案した．しかし，入力する特徴量として，1 タップごとに得られる特徴量のみを使用しているため，一連のテンポを考慮していなかった．

そこで，本論文では，同一の曲であっても，ユーザによって，タップ入力から得られる 1 音毎の間隔，テンポに対するタップ入力のずれに特徴があると考え，これを「テンポ感」と定義する．そして，既存の特徴量に加え，ユーザの「テンポ感」と「指圧」を特徴量として認証情報に加えることで，認証精度への影響，および有用性について考察する．

以下，2 章では関連研究を，3 章では提案方式を，4 章では特性評価を示し，5 章で結論を述べる．

2　関連研究

2.1　覗き見耐性を持つ認証方式

覗き見耐性を持つ認証方式として，アイコンと移動法則を用いた STDS(Secret Tap with Double Shift) 認証方式 [4] がある．

この認証方式は，まずユーザがパスワードとなるアイコンと独自の移動法則を登録する．そして，表示されたアイコン群から登録したアイコンを探し，そこから移動法則に従って移動した先のアイコンをタップすることによって認証を行う．登録したアイコンの位置は認証のたびにランダムに変わるため，覗き見られても登録したアイコンが露呈しない特徴を持つ．これらの認証方式は，覗き見に対して有効であるが，カメラをはじめとする録画機器に対して耐性が十分ではなく，認証動作や端末の画面を複数回録画された場合，認証情報が解析されてしまうことが考えられる．そのため，ユーザが画面を見ながら認証を行う以上，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．そこでユーザが，画面を見ずに認証ができる方式としてリズム認証が提案されている [5, 6, 7]．

2.2　リズム認証

リズム認証とは，ユーザが曲に合わせてキーボード入力や画面タップをし，連続した入力データの時間差を認証情報として用いる認証方法であり，ユーザの行動的特徴を活かしたバイオメトリクス認証の 1 つである．ユーザは自身のイメージした曲のメロディに合わせてキーボード入力や画面タップし，キー入力時間やタップ時間などの特徴量を認証情報としている．

従来のリズム認証は，キーボードなどの入力装置を対象とした研究が行われており，現在では，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．

市村らによって，覗き見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 [5] が提案されている．この認証方式は，スマートフォンを片手に持ち，持った手の親指で画面をタップしたリ

ズムを認証情報にする認証方式である．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．また，ユーザ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るため，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，指の識別を行わないため，認証の際に画面をタップする音が他人に漏れた場合，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できる問題がある．

そこで我々は，これらの問題を解決するために，指の識別，指間情報，および 4 つのタップイベント時間を入力データとしたリズム認証方式 [7] を提案している．また，本人拒否率 (False Rejection Rate，以下，FRR) および他人受入れ率 (False Acceptance Rate，以下，FAR) の低減を考慮し，すべての特徴量のうちユーザ本人の再現率が高い特徴および，他人との特徴量の差が大きい特徴をそれぞれ挙げ，それらの特徴量から成る複数の SOM を用いることにより認証精度の向上を目指した．その結果，FRR および FAR の低減を考慮した SOM を複数用いることによって認証精度を高めることに成功し，特徴量を分類し，FRR および FAR の低減を考慮した複数の SOM を用いることで，認証精度の向上が見込まれることを示した．

2.3 自己組織化マップ

自己組織化マップとは，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 [8]．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 $\vec{i}$ 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 3 つの式を適用し，勝利ノードを含むノード n の参照ベクトル $\overrightarrow{r_n}$ を $\vec{i}$ へ近づ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．

$$
\begin{aligned}
\overrightarrow{r_n}(t+1) &= \overrightarrow{r_n}(t) + H_n(t) \cdot (\vec{t}(t) - \overrightarrow{r_n}(t)) \\
H_n(t) &= \alpha(t) \cdot \exp\left(-\frac{\left|\overrightarrow{L_n} - \overrightarrow{L_v}\right|^2}{2\sigma^2} \right) \\
\alpha(t) &= 1 - \frac{t}{T}
\end{aligned}
$$

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の分布を視覚化することが可能である．また，ある勝利ノードとそれに特徴が似たデータが集合した領域を，以降では近傍領域とする．

SOM の特性を活かしたリズム認証の先行研究が行われており，認証の判定における SOM の有用性が報告されている [5].

3 提案方式

本論文では，同一の曲であっても，ユーザによって，タップ入力から得られる 1 音毎の間隔，テンポに対するタップ入力のずれに特徴があると考え，これを「テンポ感」と定義し，既存の特徴量に加え，ユーザの「テンポ感」と「指圧」を特徴量として認証情報に加えることで，認証精度への影響，および有用性について考察する．

3.1 システムモデル

本認証方式において使用する機器は，ユーザのモバイル端末と，モバイル端末によって得られた認証データを処理するサーバで構成される．

図 1: 認証情報登録および認証の手順

入力情報の分析には，SOM を利用することを想定する．図 1 に，本提案方式のシステムモデルにおける認証情報登録および認証の手順について示す．

サーバで SOM を作成するする理由として，SOM 作成の膨大な処理への対応がある．SOM は，1 つのノードにつき n 次元を扱い，1 つのマップは数千〜数万のノードによって構成されている．それらのノードにつき，探索および学習を数万回行うため，その処理は膨大である．その処理をモバイル端末上で行うには，負荷が大きく，モバイル端末が不安定になることが考えられるため，処理能力が高いサーバで SOM を作成する．

3.2 リズム認証の手順

リズム認証の情報登録は，まず，ユーザがモバイル端末上でタップした認証情報がサーバへ送信され，サーバで SOM を作成する．SOM を作成した後，SOM 情報をモバイル端末へ送信し，登録は完了する．

次にリズム認証の認証時について述べる，まず，ユーザはモバイル端末上をタップしてリズムを入力する．モバイル端末内では，入力情報と SOM とを照合し，入力情報の勝利ノードと近領域の中心とのユークリッド距離を求める．そして，その距離が予め定義した閾値内であるか否かによって認証の成否を判断する．認証が成功した場合は画面ロックを解除し，失敗した場合は，ユーザに対し再度入力を求める．

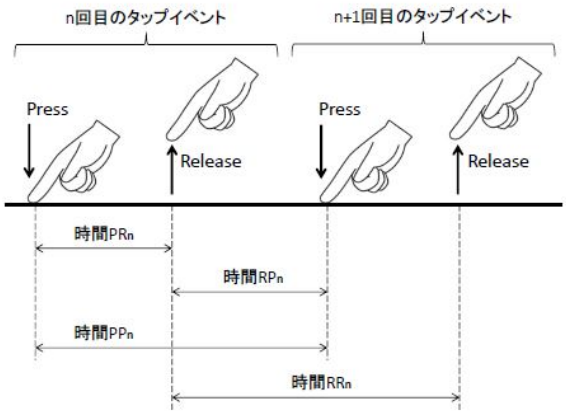

図 2: タップのイベント時間の定義

3.3 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量を定義する必要がある．以下に，9 項目の個人特徴量の定義を示す．また，図 2 に，タップイベント時間の定義を併せておく．

- 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の距離（以下，指間 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）
- n 回目のタップで指を離し，$n+1$ 回目のタップを行うまでの時間（以下，時間 RP_n）
- 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）
- 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})

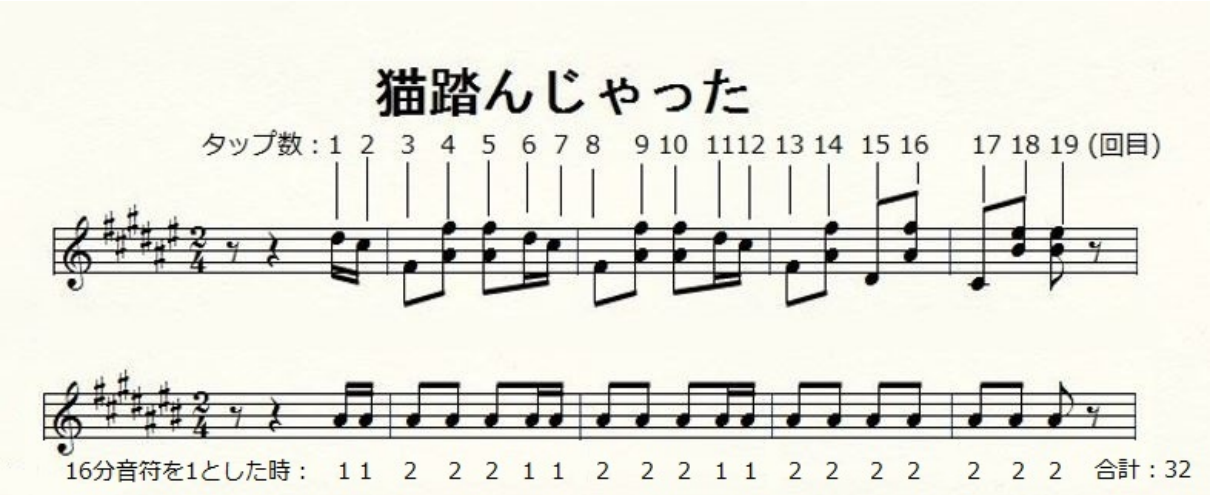

図 3: 「猫踏んじゃった」の楽譜

- n 回目のタップの指圧 (以下，指圧 P_n)
- 楽曲のテンポに対するユーザの時間 PP_n のずれ（以下，誤差 $DifPP_n$）
- 楽曲のテンポに対するユーザの時間 RR_n のずれ (以下，誤差 $DifRR_n$)

3.4 ユーザのテンポ感による特徴

ユーザのタップのテンポ感を計算するにあたり，図 3 の「猫踏んじゃった」の楽譜を参考にする．

図 3 より，この楽曲は，16 分音符が 6 個，8 分音符が 13 個から成っていることがわかる．ここで，冒頭の 16 分音符の音の長さの比を 1 とすると，8 分音符は音の長さが 16 分音符の 2 倍であるため，8 分音符の音の長さの比は 2 となる．これらの比の総和でタップ入力にかかった時間を割ることにより，そのタップしたテンポの 16 分音符の音の長さを求めることができ，この長さを基準値とし，その基準値から実際にタップした時間 PP_n，時間 RR_n を引くと，基準値に対するユーザのタップのずれ，すなわちテンポ感が算出可能である．例えば，算出された数値がプラスならユーザは基準値より早くタップしたことになり，マイナスなら，ユーザは基準値より遅くタップしたことになる．我々はこのタップのずれに個人の特徴があると考え，テンポ感をリズム認証の特徴量として取り入れることを試みる．

時間 PP_n と時間 RR_n を利用する理由は，従来研究 [7] で時間 PP_n は本人再現率が高い特徴量，時間 RR_n は他人との差が大きい特徴量であり，FRR および FAR の低減が期待できる特徴量であるという結果を参考にしている．

4 評価および考察

4.1 使用する曲

実験で使用する曲は童謡「猫踏んじゃった」の冒頭 4 小節，全 19 タップとする．曲を指定する理由としては，ユーザが登録した曲と同じ曲を他人がタップした場合を想定し，誤認証が発生するかを確認するためである．冒頭 4 小節にする理由として，ユーザへの記憶負荷の低減，認証時間を短縮することにより，ユーザビリティを高める狙いもある．また，市村らの研究 [5] により，リズム認証に使用する楽曲は，短い方が高い認証精度になったという実験結果も参考にしている．

表 1: 各被験者における特徴量の相対的標準偏差

	指圧 P	時間 PR	時間 RP	時間 PP	時間 RR	誤差 $DifPP$	誤差 $DifRR$
被験者 1	19.34	31.07	39.16	40.34	39.96	218.22	226.42
被験者 2	17.41	31.68	44.42	34.78	37.04	150.66	194.09
被験者 3	17.41	31.30	44.15	34.18	36.38	154.50	197.49
被験者 4	16.14	32.34	42.36	35.66	36.16	151.38	165.61
被験者 5	15.06	31.93	49.02	36.49	39.05	152.47	202.75
平均	17.07	31.67	44.20	36.29	37.72	165.45	197.27

表 2: 全被験者における特徴量の相対的標準偏差

	指圧 P	時間 PR	時間 RP	時間 PP	時間 RR	誤差 $DifPP$	誤差 $DifRR$
相対的標準偏差	17.28	31.70	44.27	36.17	37.63	168.75	198.59

4.2 FRR および FAR 低減のために有用な特徴量の算出

個人の特徴には，本人再現率が高い特徴と他人との差が大きい特徴がある．それぞれの特徴量を認証情報として利用することにより，本人再現率の高い特徴量は FRR を低減することが期待でき，他人との差が大きい特徴は FAR を低減することが期待できる．従来研究 [7] では，本人再現率が高い特徴と他人との差が大きい特徴を算出し，それらを利用して SOM を複数作ることにより，FRR および FAR 低減に成功した．

そこで，今回新たに追加した特徴量をこれらに分類するために，特徴量の計測を行った．被験者は，神奈川工科大学の学生 5 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 小節をタップした．

- 全体で 5 回の試行を行う．
- タップする指，指の順番，リズムの速さは被験者の任意とする．ただし，それらは全ての試行で一貫し，試行途中での変更は認めない．
- 各試行の合間に 30 秒〜1 分間のブランクを設ける．
- 計測する項目は，3.3 節で定義した項目とし，各項目の相対的標準偏差を算出する．

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 $\sqrt{\sigma^2}$ を平均値 μ で割った百分率であり，尺度や種類の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．各項目のデータを x とし，相対的標準偏差 RSD の定義式を以下に示す．

$$
\begin{aligned}
RSD &= \frac{\sqrt{\sigma^2}}{\mu} \times 100 \\
\sigma^2 &= \frac{1}{5}\sum_{n=1}^{5}(x_n - \mu)^2 \\
\mu &= \frac{1}{5}\sum_{n=1}^{5} x_n
\end{aligned}
$$

指 F，距離 D の相対的標準偏差は，既存研究 [7] で，有用性が報告されているので，今回の実験では算出を省いている．しかし，時間 PR，時間 RP，時間 PP，時間 RR に関しては，今回新たに追加する，誤差 $DifPP$，誤差 $DifRR$ と関連性があると思われるので，算出した．

表 1 に，被験者における特徴量の相対的標準偏差を示す．各値は，試行 5 回分の相対的標準偏差であり，表の下部分には 1 人当たりの平均値を示す．平均値が低いほど，入力が安定して

いることを示し，本人再現率が高いと考えられる．本人再現率が高いということは，FRR を低減できることに結びつく．今回の実験では，指 P は，相対的標準偏差の平均が小さく，本人再現率が高く，FRR の低減が期待できる．しかし，他人との差が少ないので FAR を上げてしまう可能性がある．

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．各値は，項目別の被験者 5 人分の相対的標準偏差である．値が大きいほど，他人との差が大きい特徴となり，FAR を低減できる特徴であると考えられる．表中の値により，時間 RP，誤差 $DifPP$，誤差 $DifRR$ の 3 項目の特徴量は，他人との差が大きく，FAR の低減が期待できる．その中でも，誤差 $DifPP$，誤差 $DifRR$ は他人との差が非常に大きいという結果になった．これは，各ユーザの曲に対するイメージ，音楽経験の有無など様々な要因が影響を与えたと考えられる．

4.3 考察

今回，新たに追加した特徴量，誤差 $DifPP$，誤差 $DifRR$ に関しては，FAR 低減に大きな影響を与えると考えられ，指圧 P に関しては，本人の再現率が高いと考えられる．しかし，指圧 P に関しては，他人との差が表れにくい特徴量という結果にもなったので，今後，特徴量として利用していくかについては，より多くの被験者から取得したデータを解析する必要がある．

5 おわりに

本研究では，従来研究 [7] のリズム認証に，新たに追加した特徴量，指圧 P，誤差 $DifPP$，誤差 $DifRR$ の有用性について考察した．指圧 P は，本人の再現率が高いことが分かったが，他人との差が少なく，FAR を上げてしまう可能性も考えられる．誤差 $DifPP$，誤差 $DifRR$ は，他人との差がとても大きく，認証に利用する特徴量としてはとても有用であると考えられる．しかし，今回の実験では，被験者が少なく，また，試行の回数も少なく，正確なデータを取ることが難しかったので，有用性を調査するには，被験者の人数，試行の回数を増やす必要がある．

今後の課題としては，有用性のあるとされる特徴量が，どれだけ認証精度に影響しているか，また，曲を変更した際の，特徴量の有用性，認証精度などを調査する必要がある．

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] 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

[3] 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対策手法の提案”，Computer Security Symposium 2013，pp.708-715，2013

[4] 喜多義弘，菅井文郎，朴美娘，岡崎直宜，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～楽曲の主旋律を用いた際の認証精度評価～”，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] 喜多義弘，神里麗葉，朴美娘，岡崎直宜，“マルチタッチ操作を利用したリズム認証方式の検討”，モバイルコンピューティング

とユビキタス通信（MBL）研究報告，2014-MBL-70(19)，pp.1-7，2014

[7] 喜多義弘，神里麗葉，朴美娘，岡崎直宜，“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の考察”，マルチメディア，分散，協調とモバイルシンポジウム（DICOMO2014），pp.1011-1018，2014，pp.1005-1010，2014

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

[9] 「猫踏んじゃった」楽譜／総合雑学 http://nue2004.info/music/cat/score.htm (2015-8-24 参照)

[10] Finale NotePad2012 http://www.finalemusic.jp/products/notepad/ (2015-8-24 参照)