Vol.2013-ICS-170 No.8
2013/3/11

圧縮性特徴量を用いたフリーストローク個人認証方式 PRDC-FDPA

田嶋 良明[†1,a)]　渡辺 俊典[†1]　古賀 久志[†1]

概要：近年，スマートフォンは世界的に普及してきている．一般的にスマートフォンのセキュリティロックは 4 桁の暗証番号か 9 点のロックパターンが用いられている．これらに対し，生態的特徴を用いた個人認証の研究はいくつか存在するが，それらは各々に対応した学習機構等を必要とし汎用性は低い．本論文では，データの圧縮性に基づいた統一的学習分類機構によりタッチパネルでのフリーストロークベースの個人認証を可能とする手法を提案する．

1. はじめに

近年，スマートフォンは従来型の携帯電話に代わる通信手段として世界的に普及してきている．スマートフォンは他者との連絡手段としてだけでなく，重要な機密情報の保存や，それらへのネットワークを通したアクセスなどへも用いられることがあり，以前と比較して保護すべき情報は格段に増加している．

スマートフォンのセキュリティロックは，一般的に 4 桁の暗証番号か，9 つの点をあらかじめ設定した順序で 4 つ以上なぞるロックパターンか，スクリーンキーボードによる英数字パスワードが用いられている．しかし，これらは入力の最中に後ろから覗かれるだけでパスワードがわかってしまい，決して重要な情報を保護するものとしてセキュリティが十分であるとは言えない．

従来のセキュリティロックに対し，個人の動作の生体的特徴を追加してセキュリティを強固にする研究がよく行われている．しかしこれらの個人認証は，各々に対応した動作特徴の取得と比較が必要となり，それぞれの固有の学習機構が用いられる．よって新しいセキュリティロックの出現時に，それらの学習機構を再利用することはできず汎用性は低い．

本研究では，従来のセキュリティロックのこの問題に対して，より汎用性の高いタッチパネルを用いたフリーストローク入力による個人認証手法 PRDC-FDPA (Pattern Representation Scheme using Data Compression - Free Drawing Personal Authentication) を提案する．これはスマートフォンのタッチパネルを用いて自由に文字や絵などを描写し，指の位置，移動方向，速度，空中滞在時間等を符号化しこれを圧縮特徴量を用いて分類を行う簡明かつ汎用性の高い方式である．PRDC-FDPA を用いるとフリーのパスストローク対して全て同じ学習機構を用いた学習が可能となる．

[†1] 現在，電気通信大学 大学院 情報システム学研究科
Presently with The University of Electro- Communications
[a)] tajima@sd.is.uec.ac.jp

2. 基本構想

ここでは，既存のセキュリティロックと，その生体特徴を用いた個人認証の問題点を述べ，それを解決するための本研究のアプローチを述べる．

2.1 既存のセキュリティロック

一般的にスマートフォンに用いられている端末起動時のセキュリティロックは 4 桁の暗証番号と 9 点のロックパターンと英数字のパスワードの 3 種類である．

4 桁の暗証番号は，スマートフォンに限らず，クレジットカードや，従来型の携帯電話にも用いられており，実社会で広く利用されている．この 4 桁の暗証番号は，使い勝手は非常に良いが，スマートフォンのパスワードを他の認証のパスワードと同じ数字にしている人も多くパスワード流出時のリスクが非常に高い．逆に 4 桁の暗証番号での認証を各々別の数字にしていた場合，他の数字と混同してしまう可能性が高く，使いづらくなる．

ロックパターンは，Android 端末で多く用いられており，画面に表示された 9 つの点を 4 点以上を含むようになぞるパスワードである．パターン数は理論上は 389112 通りあり，大変堅牢なロックである．また，使い勝手もよく，文字列のパスワードのように他の認証手法に用いられていない

のでパスワードが流出した場合でも他の認証に使用されるリスクは低い．しかし，ユーザーには実際には 4 点か 5 点を用いた簡単なパスワードが使用され易い．この場合，認証の瞬間を後ろから覗かれるとパスワードがわかったり，タッチパネルに残る指油の跡を見るだけでパスワードが推測できたりするなど，脆弱性がある．

英数字のパスワードは，4 桁の暗証番号同様実社会で広く利用されている．ただ，スマートフォンにおいては，タッチパネル上に表示された擬似キーボードを用いての入力になるため，ボタンが小さく入力ミスが多くなり，非常に使い勝手が悪い．また，4 桁の暗証番号同様にパスワード流出時のリスクが高い．

2.2 生体特徴を用いた個人認証

以上から，既存のセキュリティロックには良い点もあるが，問題点が多数存在する．

これらの問題点，特に他者にパスワードが漏れてしまったときのために，個々人の動作の生体的特徴を分析してセキュリティをより強固にする研究が存在する．

4 桁の暗証番号のキーストロークダイナミクス（ボタンとボタンの間の時間や，ボタンを押している時間等の行動的特徴を利用した認証技術）による認証の研究 [1] では，個人認証の性能の指標となる EER(Equal Error Rate：本人拒否率と他人受容率が等しくなるときのエラー率．低いほど性能が良い) は 8.5% となっている，しかしながらこの研究は従来型の携帯電話端末 (Nokia5110) を用いてデータを取得し，認証の計算等は PC 上で行っているため，端末のみでの学習や認証は出来ていない．

ロックパターンの点領域を触っている時間と点と点の間の時間を行動的特徴として認証に用いた研究 [2] では，EER は 13.8% となっている．しかし，この研究で用いられたパスワードは 6 点を含むように設定しており，複雑なものが多い．しかし実際にユーザーが使用するパスワードは 4 点や 5 点の簡単な場合が多く，その場合にはさらに結果が悪くなると考えられる．

タッチパネル上に表示された擬似的なスクリーンキーボードを用いたキーストロークダイナミクスの研究 [3] では，EER が 2% と非常に良いが，この 2% を達成するためには 250 字以上の入力が必要で，アプリケーションとしては入力が多すぎる．また，スマートフォンの狭いタッチパネルでのスクリーンキーボード入力となり，使い勝手が非常に悪く，誤入力も多い．

2.3 既存のセキュリティロックとその個人認証の問題点

以上から，既存のセキュリティロックとその個人認証の問題点をまとめると以下のようになる．

問題点 1 ユーザーは複雑なパスワードを用いない場合が多い．

問題点 2 パスワードの種類が有限であり，推測しやすい．

問題点 3 各々の認証のアルゴリズムは手法に強く依存しており汎用性は低い．

まず問題点 1 と 2 に関しては上記で述べた生体特徴を用いた個人認証によりある程度のセキュリティ強化は見込めるものの，いずれにせよパスワードが流出しやすく，そのパスワードを何度か入力するとセキュリティは突破される．特に 4 桁の暗証番号や，英数字パスワードはそれ自体の流出によるリスクが非常に高い．

また，問題点 3 に関しては，認証手法毎に入力データの処理法が異なるため手法の汎用性が低く，多種のセキュリティロックを有するスマートフォンがあると，内部にそれぞれ固有の生体特徴を用いた個人認証アルゴリズムを必要とし，スマートフォンの内部容量を圧迫してしまいかねない．

2.4 本研究のアプローチ

2.4.1 フリーストロークのパスワード

§2.3 で述べた問題に対して, 本研究ではユーザーにパスワードとしてタッチパネルを用いた文字や絵等のフリーストローク入力をさせて，認証を行うこととした．これによって，たとえ簡易なパスワードを設定したとしてもそのパスワードは理論上無限にあり，文字なのか絵なのかも推測しにくくなることを利用し，問題点 1,2 に対処することにした．また，指の油を見てパスワードを推測する方法は，ロックパターンのように決まった点しかタッチしないという弱点を利用している反面，フリーストロークの場合は指の空中滞在状況も認証に利用できるので推測は難しくなると考えられる．

2.4.2 汎用的な学習機構

問題点 3 にもあるように，従来の生体特徴を用いた個人認証においては，登録データと入力データの比較アルゴリズムが方式毎に異なり汎用性は低い．

そこで本研究では，4 桁の暗証番号やロックパターン，英数字入力を全てフリーストローク入力とみなし，フリーストローク入力に対して生体特徴を用いた個人認証を行う方式を提案する．このため，提案手法は既存のセキュリティロックの全てに対応できる汎用的な学習・認証機構となると考えられる．

3. 入力ストローク列の圧縮性を利用した認証機構

ここではまず提案手法である PRDC-FDPA の概要を流れ図で示し，フリーストローク入力で取得されるデータの扱い方を各手法の詳細な説明の中で述べる．

3.1 分類手法の概要

ここでは，ユーザーのフリーストローク入力から取得し

た時空間特徴を符号化して分類し認証する PRDC-FDPA の概要を説明する．このアルゴリズムは入力されたストロークの時間情報と空間情報に対し，詳細に各々のデータを記録済みのストロークデータと比較していくのではなく，ストローク全体を 1 つのテキストデータにし，テキスト間の類似度から分類を行う．

図 1 が PRDC-FDPA のアルゴリズムの流れ図である．

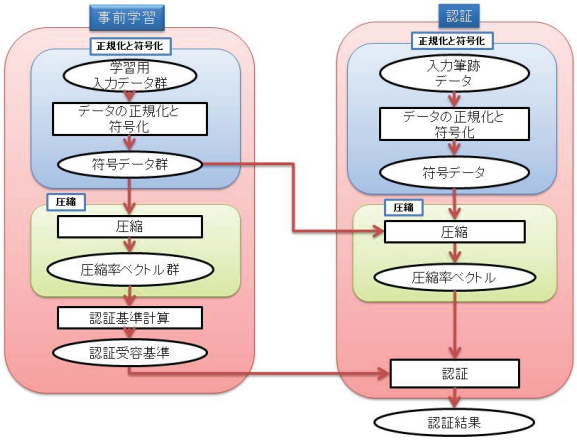

図 1　PRDC-FDPA

大別して事前学習と認証の 2 つのフェーズを持っている．事前学習フェーズでは，ユーザーから事前に学習データを取得し認証受容基準を作成し，認証フェーズではそれに対して入力データが認証受容基準の中に入っているかどうかの判定を行う．

各処理の詳細については以下順次述べていく．

3.2　データの取得

ユーザーには，パスストロークを数種類用意してもらい，それらの軌跡データとその座標の時間データ，そして指が離れてから次のタッチまでの空中滞在時間を取得する．

図 2 が取得されるデータの例である．

```
45.85625 124.73958 0.0↓
45.85625 124.73958 10.0↓
46.853123 124.73958 20.0↓
46.853123 124.73958 30.0↓
49.84375 123.74166 40.0↓
55.825 121.745834 50.0↓
65.79375 119.75 60.0↓
65.79375 119.75 70.0↓
79.75 117.754166 80.0↓
94.703125 115.75833 90.0↓
-1.0 -1.0 100.0↓
-1.0 -1.0 110.0↓
-1.0 -1.0 120.0↓
-1.0 -1.0 130.0↓
-1.0 -1.0 140.0↓
-1.0 -1.0 150.0↓
-1.0 -1.0 160.0↓
167.47499 129.72917 170.0↓
167.47499 129.72917 180.0↓
167.47499 129.72917 190.0↓
167.47499 129.72917 200.0↓
167.47499 129.72917 210.0↓
167.47499 129.72917 220.0↓
167.47499 129.72917 230.0↓
```

図 2　取得されるデータ

これは，それぞれ左から X 座標，Y 座標，時間となっている．途中の座標が-1.0 となっているところが空中滞在時間である．

ここで，取得されたデータは CPU やタッチパネルの性能上，XY 座標がまばらとなっており，同じ動作をしても途中の座標が異なったりなど様々な問題があり，単純に時間ごとに座標を比較する手法は適切とは言えない．

そこでこれらを符号化し，符号テキスト間の類似度を見ることによって分類を行うこととした．これによって途中に多少のノイズが入ってもロバスト性を持った分類が可能となる．

3.3　データの符号化

本研究でに用いるデータは，軌跡の XY 座標，座標点での時間，空中滞在時間である．

タッチパネルを図 3 のように分割し，それぞれに英数字を与え，符合化器とする．これによって XY 座標のアスキー文字への符号化が行われる．符号化区画を細かくしすぎるとタッチしようとした場所と実際に符号化される文字の違いが生じるため，スマートフォンのボタン入力の大きさ程度に区切った．

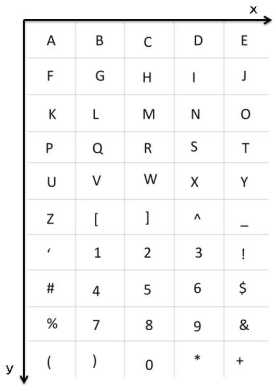

図 3　位置（x,y）の符号化

しかし，これだけではタッチした場所の情報しか取れていない．さらに，どの向きにどれくらいの速さで動いたかのデータを取得するため図 4 に示す符合化器も同時に用いた．

これは直前の座標からどちらの方向にどれだけ動いたかを符号化している．まったく動かなければ「a」，水平右方向にゆっくり動いた場合は「c」が出力され，速く動いた場合は「k」が出力される．

取得している空中滞在時間は 10ms ごとに「o」を出力するようにした．これによって，長い時間空中にとどまったあとにまたタッチをした場合，テキストに「o」がたくさん出力され，空中滞在が短い場合とは異なるテキストとなる．

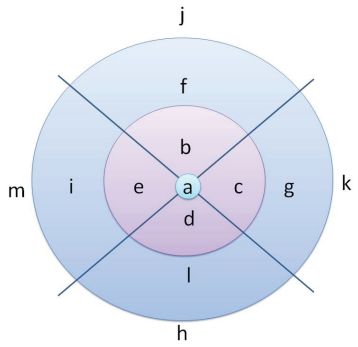

図 4　方向と速さの符号化

以上よりデータの大まかな特徴を符号化テキストとして表すことができ，これらの類似度からデータの分類を行うことによって，厳密な比較が難しい時空間特徴量を用いたフリーストローク入力の認証を行うことができると期待される．

3.4 PRDC

次に，符号化データの類似度判定についての説明に移る．

データの分類には，データの圧縮性特徴量を用いた分類手法，PRDC [4] [5] を用いている．

A,B ふたつのテキストがあった時，テキスト A を圧縮する際に作られた圧縮辞書を用いてテキスト B を圧縮した結果が高圧縮であれば，テキスト A とテキスト B は類似していると判断する．n 個の圧縮辞書を用いて任意のテキストを n 次元の圧縮率ベクトルとして特徴表現することが容易にできる．

3.4.1 圧縮率ベクトル

PRDC は入力テキストを圧縮率ベクトルという形で特徴表現する．図 5 で圧縮率ベクトルについて説明する．まず様々なテキスト群 T = [t_1, t_2, ⋯, t_n] を用意し，各テキストを圧縮する際に得られる圧縮辞書群 D = [d_1, d_2, ⋯, d_n] を基底辞書とする．入力テキストが与えられた時，各基底辞書で圧縮すると，n 個の出力が得られる．各出力テキスト長を入力テキスト長で割ったものを圧縮率ベクトルとする．

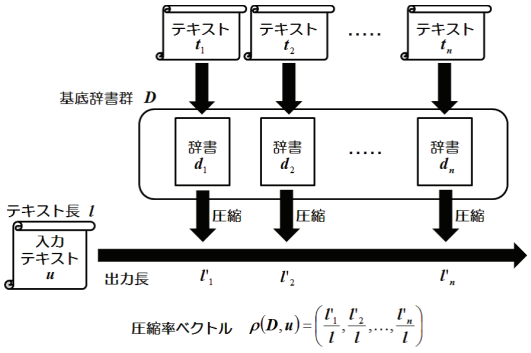

図 5　圧縮率ベクトルの計算

例えば，図 6 は A, B, C という 3 個のテキストがあった時，圧縮辞書 d_1 と d_2 を用いてそれらの特徴を 2 次元の圧縮率ベクトルで数値化し，圧縮率空間上に写像した例である．ここで空間上のベクトル間の距離を見ると，A は C よりも B の方が近い位置にあるので，B に対して A は C よりも類似性が高いと言える．これがデータ圧縮を用いて多様なファイルを特徴付け，分類・検索を行う PRDC の原理である．

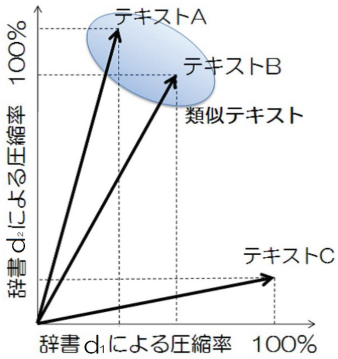

図 6　圧縮率ベクトルによるテキストの特徴表現

3.4.2 LZW 圧縮アルゴリズム

PRDC で用いる辞書式圧縮方式として LZ 符号方式 [7] のバリエーションの 1 つである LZW 方式 [8] を用いる．LZ 符号方式には様々なバリエーションが存在するが，J. Ziv と A. Lempel が 1977 年に発表した LZ77 [9] が最初である．

LZ77 は情報源がどのような統計的性質を持っているかを知らなくても，記号長が長くなるについれて平均符号長がエントロピーに収束するという点で，理想的な符号化を行う事ができる．しかし LZ77 も完璧ではなく，有限長のバッファ中の記号列を辞書として利用する為，符号化する記号の直前の記号列しか参照する事ができないという問題点がある．この問題点を解決した LZ78 が 1978 年に発表された．LZ78 は LZ77 を改良した手法と言うよりも，LZ77 とは似て非なる別の手法と言った方が適切であり，LZ77 の問題点を解決しただけでなく，圧縮/展開が高速でプログラム化が容易という優れた特徴を持っている．そして，LZW は LZ78 の中間符号語のフォーマットにおける無駄な文字を取り除くことで圧縮性能を向上させている．

3.4.3 認証受容基準の作成

PRDC における入力データ群のクラス分類は圧縮率ベクトルをクラスタリングすることで可能である．クラスタ分離面を機械学習法によって決定することで認証基準を作ることができる．しかし本研究では，できる限り少数の教示データのみでの学習を実現するためにこの方式を用いない．

具体的には，学習データの一部を圧縮してできた圧縮辞書群を基底辞書群とし，他の学習データを圧縮して圧縮率ベクトル群を作成する．作成された圧縮率ベクトル群を各次元に射影し，その平均・標準偏差を算出し，平均から標

準偏差の 2 倍の距離以内を認証受容基準とした．

3.5 パスストロークの組み合わせ方式

今回用いたデータの符号化と PRDC による分類は，ストロークの類似度を部分ストローク集合の類似度で計量するという特徴がある．このため，ノイズには強くなるが，ストローク曲線間の距離比較などの能力は低い．

そこで本研究ではユーザーがセキュリティの強固さをより強く求めた場合にも対応できるように，パスストロークの組み合わせによる認証方式を提案する．これは，本来 1 つのパスストロークで認証を行うところを，2 つのパスストロークを 1 つのペアとし 2 つとも成功したら 1 回の認証成功とする．これを 2 回行い，どちらかで認証成功したらセキュリティロックの認証成功とする，といったように，パスストロークを組み合わせて認証を行う方式である．この場合，1 つのパスストロークでの本人認証失敗率を p，他者のなりすまし成功率を q とすると，上記の 2 つのストロークの 2 回認証による組み合わせ方式を用いると，

$$\text{本人失敗率} : (1-(1-p)^2)^2$$

$$\text{他人成功率} : (q^2)*2$$

となる．

4. 実験

PRDC-FDPA の有用性を確認する為の各種の実験を行った．Google のモバイル端末のプラットフォーム Android でアプリケーションを実装し，データを取得した．実験に使用した端末は以下となっている．

端末名： L-04C
OS： Android 2.2
CPU： Qualcomm MSM7227
RAM： 512MB
ディスプレイ解像度： HVGA(320*480)

また，具体的な実験項目は以下の通りである．

(1) 使用するパスストローク形式の検討
(2) 符号化方式の検討
(3) 個人認証としての利用可能性確認

実験にはそれぞれ 3 種類のパスストロークを用い，各 30 回ずつ入力し，最初の 4 回を練習用データとして捨て，5 回目を圧縮してできた辞書を基底辞書とし，残りのデータを圧縮してできた圧縮率ベクトルを比較している．

なお，実験結果として表示している図や表の x,y,z は，それぞれ x が 1 つ目のパスストロークの基底辞書で圧縮してできる圧縮率，y が 2 つ目のパスストロークの基底辞書で圧縮してできる圧縮率，z が 3 つ目のパスストロークの基底辞書で圧縮してできる圧縮率である．

4.1 使用するパスストローク形式の検討

フリーストロークによる認証では，4 桁の暗証番号やロックパターン等と違い，論理マッチングによってパスワードが合っているかどうかの判定をすることができない．よってまずはユーザーが実際に用いると想定される簡単なパスストロークを用いて入力ストロークがそれぞれ別々のパスストロークとして識別されているかどうかを，3 次元の圧縮率ベクトルの gnuplot による視覚化によって確認する．

また，類似したパスストローク（1 と i など）を入力した場合にも，識別可能かどうかを確認する．

これらに関する実験を行い，PRDC-FDPA によってどの程度の識別が可能かの確認を行い，問題点があった場合それに対する検討も行う．

4.1.1 簡単なパスストローク

スマートフォンは普段から持ち歩く端末であり，日常的に認証を行うため，セキュリティロックのパスワードは簡単なものに設定する場合が多い．

このことからパスストロークとして「○」,「T」,「い」を用いて，提案手法の PRDC-FDPA がどの程度の識別ができるのかの確認を行った．

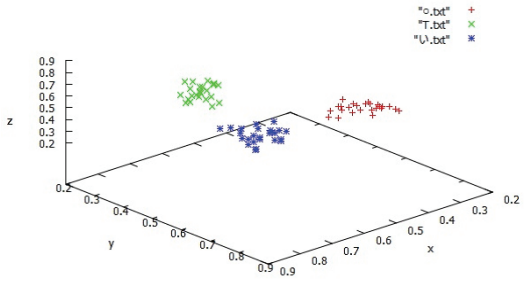

図 7 「○」,「T」,「い」によってできた圧縮率ベクトル

図 7 からわかるように，分類結果は良好である．

4.1.2 類似したパスストローク

次に，3 種類のパスストロークが似た形状の場合どうなるかの実験を行った．今回用いたパスストロークは「1」,「i」,「I」である．

図 8 が結果の圧縮率ベクトルである．

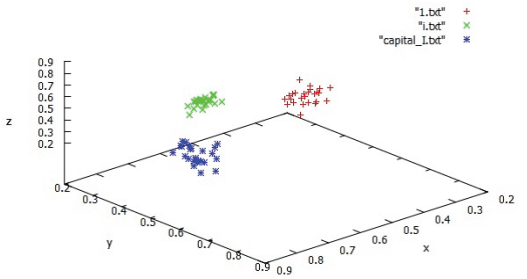

図 8 「1」,「i」,「I」によってできた圧縮率ベクトル

この程度の形状の類似したストロークは識別が可能であることがわかる．これは，軌跡の形状はほぼ同じに思えるが，実際の動作は「1」は 1 画だけなのに対し，「i」は 2 画，「I」は 3 画であることによるストロークの空中滞在状況の違いが識別に貢献していると考えられる．

4.1.3 パスストロークの考察

以上の実験で，普段よく使われる短いストロークのパスワードの識別はできていることがわかった．

4.2 符号化方式の検討

本研究では空間特徴と時間特徴を利用するため，位置，方向・速度，空中滞在時間の 3 種類の符号化を行っている．これらの符号化方式が妥当かどうかを，各々の符号化方式を用いない場合との比較によって確認する．§4.1.1 で用いたデータにそれぞれ符号化方式を 1 つずつ除いた場合，以下のような圧縮率ベクトル群となる．

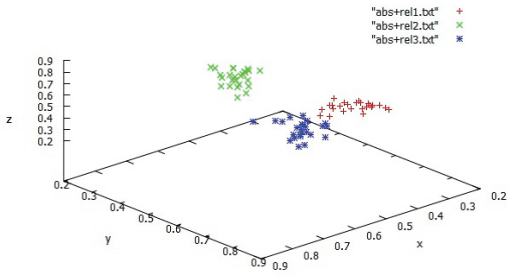

図 9 （位置，方向・速度）の符号化

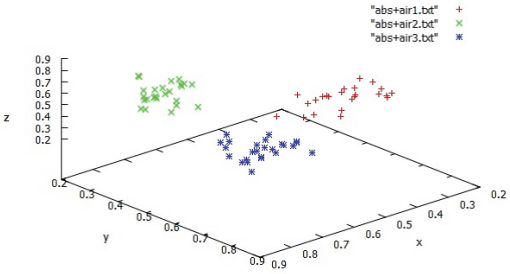

図 10 （位置，空中滞在時間）の符号化

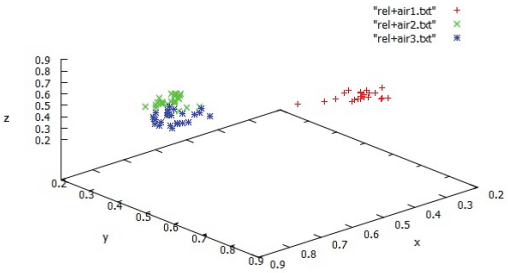

図 11 （方向・速度，空中滞在時間）の符号化

図 9 と図 11 では，異なる圧縮率ベクトル群の分布が重なっているところがあり，ストロークの識別がはっきりとできていないことがわかる．

また，図 10 では，ストロークの識別は出来ているものの，分布が非常にばらついており，これを用いて認証基準を作成した場合，他者のなりすましを容易に成功させてしまうと考えられる．

よって，位置，方向・速度，空中滞在時間の全ての符合化器を用いるのがベストであると考えられる．

4.3 個人認証としての利用可能性の確認

個人認証として用いる場合，同じパスワードを入力した場合でも他者との違いが出てくることが重要となってくる．

本実験は，異なる 5 人の被験者に「○」，「T」，「い」をそれぞれ 30 回ずつ入力してもらい，そのうち 15 回ずつを学習データとして認証受容基準を作成し，残りの 10 回ずつを認証用データとし，この実験を行った．

4.3.1 実験結果

最初に本人の学習データで作成された認証基準においての認証成功率を出した．

表 1 各人の与えた学習データ下での本人の認証成功率

被験者	A	B	C	D	E	平均
成功率	56.7%	80.0%	86.7%	86.7%	70.0%	76.0%

表 1 を見るとわかるが，それぞれ良い認証成功率を得られたと思われる．しかしながら被験者 A に関してはあまり良い結果は得られなかった．これに関しては §4.3.2 で考察する．

次にそれぞれの学習データと基底辞書を用いて，他者の認証データの圧縮率ベクトルを算出して認証を行い，どの程度他者のデータを異データとして識別できるかを確認した．

表 2 がそれぞれの他者のなりすまし認証成功率である．

表 2 各人の与えた学習データ下での他者のなりすまし認証成功率

	他者の認証入力					
本人	A	B	C	D	E	平均
A	-	0%	6.7%	0%	0%	1.7%
B	46.7%	-	26.7%	36.7%	43.3%	38.3%
C	53.3%	46.7%	-	56.7%	36.7%	48.3%
D	10.0%	16.7%	50.0%	-	63.3%	35.0%
E	3.3%	13.3%	3.3%	10.0%	-	7.5%
平均						26.1%

被験者 A は自身の入力に対してもあまり認証が成功しなかったが，他者の入力に対してはもなりすまし認証を許していない．B,C,D は他人から高い確率でなりすまし認証を

許している．よって単一ストロークは個人認証には弱いと言える．

4.3.2 個人認証としての考察

被験者 A の本人成功率

表 1 の被験者 A のデータに関してであるが，これはおそらくパスストローク入力の練習回数や学習回数の少なさが起因していると考えられる．というのは，被験者 A のデータを詳しく見ると，特に 2 つ目のパスストローク（T）に対しての入力が，前半と後半で少しずつ変化しているのが見て取れたからである．

表 3 被験者 A の「T」の学習データの圧縮率ベクトルの平均と標準偏差

	x	y	z
平均	0.68	0.34	0.68
標準偏差	0.01	0.02	0.02

表 4 被験者 A の「T」の認証データの圧縮率ベクトルの平均と標準偏差

	x	y	z
平均	0.71	0.37	0.66
標準偏差	0.02	0.04	0.04

表 3 と表 4 を見るとわかるが，学習のデータと認証のデータでは圧縮率に違いが生じていることがわかる．また，標準偏差を見ても，学習データは非常にばらつきの少ないデータであるのに対し，認証データには多少ばらつきがでている．これはおそらく，被験者 A が何度か入力を行っている内に，入力に慣れ，速さや軌跡に多少の違いが生じてきたのではないかと考える．よって，この問題には学習データを取得する前の練習回数を増やすのが効果的だろうと考える．

熟練度と他者の認証成功率

§4.3.1 の実験では，全員が他者のパスストロークを知っているという最悪の事態を想定してデータを取得している．実際にはパスストロークを知らない場合が多く，表 2 の 26.1% を過大に悲観視すべきではない．

今回実験に協力したもらった 5 人のうち，被験者 B と被験者 C は普段はスマートフォンを使用しておらず，タッチパネルでの操作も慣れていない．被験者 B と被験者 C のデータを見ると他の被験者よりも標準偏差が大きく，データの幅が広いことがわかった．このため他者の認証を許しやすく，結果が悪いものとなってしまった．したがって，被験者 B と被験者 C に関しては，スマートフォンでの操作に慣れるともう少し良い結果となると予想され，これに関しても被験者 A の本人成功率に関する考察同様，練習回数を多く取ることによって解決が見込めると考える．

4.4 パスストロークの組み合わせ方式による改良

単一ストローク入力の場合，本人の失敗率が 24% ，他人のなりすまし成功率が 26.1% となり，個人認証方式としてはあまり良い結果とは言えない．

そこで，§3.5 で述べたパスストロークの組み合わせを用いることによって性能の向上を図る．

今回の実験結果を 2 つのパスストロークのペアによる 2 回認証の組み合わせ方式に当てはめると，

$$\text{本人失敗率} : (1-(1-0.24)^2)^2 = 0.176$$

$$\text{他人成功率} : (0.261^2) * 2 = 0.136$$

より，本人失敗率が 17.6% ，他人成功率が 13.6% となり，性能は向上する．

5. まとめ

5.1 結論

タッチパネルを用いたフリーのパスストロークに対し，入力データを符号化しその圧縮特徴を用いた分類による個人認証方式，PRDC-FDPA を提案した．本方式では，入力はスマートフォンのタッチパネルを用いてフリーのパスストロークを入力してもらい，そのときの指の座標や動き，タッチ間の指が空中にある時間等を符号化し，テキストとする．そして PRDC を用いて，テキストを圧縮してできた圧縮率特徴ベクトルによる類似度判定を行う．最後に学習データでできた圧縮率ベクトルを各次元に射影し，その平均と標準偏差を出し，平均を中心とし，標準偏差の 2 倍の範囲を認証基準とし，入力データがその中に入ったかどうかによる認証を行う．

実験により，単一ストロークでの本人の認証成功率は 76% ，他者のなりすまし成功率は 26.1% を得た．2 ストロークを 2 回，計 4 回入力する組み合わせ方式では，本人失敗率は 17.6% ，他人成功率は 13.6% となる．実用には様々の改良が必要であるが，簡単な仕組みで多様なフリーストロークを受理できることから，有望な結果が得られたと考える．

5.2 今後の課題

今回は，ユーザーが使用する可能性の高い簡単なストロークを中心として，原理レベルでの提案と検証を行った．

多様なフリーストロークを簡単な仕組みで認証できる汎用性があるが，入力ストロークの許容長や類似度判定方式など，今後の検討課題は多く残されている．

謝辞

本研究は，文科省科研費補助金基盤研究 (C)(# 2250122, 2010) の支援を受けて実施した．

参考文献

[1] Clarke, N.L, Furnell, S, "Authenticating mobile phone users using keystroke analysis," *International Journal of Information Security (IJIS)*, Vol.6, number 1, pp. 1-14, 2007.

[2] Julio Angulo, Erik Wastlund, "Exploring Touch-screen Biometrics for User Identification on Smart Phones," *in Proceedings of IFIP International Summer School 2011*, 2011.

[3] Zahid, S, Shahzad, M, Khayam, S, Farooq, M, "Keystroke-based user identification on smart phones," *Recent Advances in Intrusion Detection, Lecture Notes in Computer Science*, vol. 5758, pp. 224-243, 2009.

[4] T.Watanabe, K.Sugawara, and H.C. Park.: *A new universal media featuring scheme using data compression*, *Proc. Int'l Conf. on Media Futures*, pp. 261–264, 2001.

[5] T. Watanabe, K. Sugawara, and H. Sugihara, "new pattern representation scheme using data compression," *IEEE Trans. PAMI*, vol. 24, no. 5, pp. 579-590, 2002.

[6] A. Macedonas, D. Besiris, G. Economou, and S. Fotopoulos, "Dictionary based color image retrieval," *JVC & IR*, vol. 19, no. 7, pp. 464–470, 2008.

[7] A. Lempel and J. Ziv, "On the complexity of finite sequences," *IEEE Trans. IT*, vol. 22, no. 1, pp. 75–81, 1976.

[8] T. A. Welch, "A technique for high-performance data compression," *Computer*, vol. 17, no. 6, pp. 8–19, 1984.

[9] A. Lempel and J. Ziv, "A universal algorithm for sequential data compression," *IEEE Trans. IT*, vol. 223, no. 3, pp. 337–343, 1977.