フリック入力による日本語非定型文のキーストローク認証

Keystroke Dynamics with Flick Input on Smartphone in Japanese Free Text Typing

泉将之 * 佐村敏治 † 西村治彦 ‡
Masayuki IZUMI Toshiharu SAMURA Haruhiko NISHIMURA

1 はじめに

スマートフォンは単なる電話機能だけでなく，データベース機能，マルチメディア機能，高度コミュニケーション機能，バンキング機能等多機能性を持った携帯端末である．最近のスマートフォンの普及は著しく，販売シェアは数年で携帯電話を追い越すであろう．そしてスマートフォン自体が身分証明書や手帳を持つことと同等の価値を持ち始めている．従って，スマートフォンの盗難にあった際の個人情報漏洩や不正使用のリスクは極めて大きい．

不正アクセスへのセキュリティ対策としては，パスワードを用いたロック機能がある．しかし，数文字程度のパスワードでは総当りによる解除が可能になる．そこで指紋や顔，キーストローク等の身体的，行動的特性を利用した生体認証 (バイオメトリクス) を用いたセキュリティ対策が検討されている．

キーストローク認証（キーストロークダイナミクス）とは行動的生体認証の一種であり，キーストロークデータに個人特有のパターンが含まれているという性質を利用している．多くのキーストローク認証はパソコンのキーボード入力を対象としている [1]．更にキーストローク認証の研究は 2 種類に分類できる．ひとつは利用者がログイン時に入力するパスワード（定型語）に対して，文字や数字列だけでなく，入力時のキーストロークデータも認証に利用しようとするものである [2–6]．もうひとつは非定型な異なる文章の入力からでも個人の特徴を抽出し，それによって認証に結び付けようとするものである [7–18]．我々はこれまで後者について識別を向上させる手法の研究を行なってきた．

今後スマートフォンの普及により，タッチパネルにおけるキーストローク認証の研究へのニーズが高まると考えられる．またスマートフォンのセンサー情報を利用することで，キーボードでは得られなかった新しい特徴量を導入することが可能となっている．スマートフォン端末での日本語入力には，キーを長押しし，指先をフリックした方向のひらがな文字を入力する「フリック入力」がある（Fig.1）．従来の携帯電話端末の日本語文字入力方法であるトグル入力に比べ，素早い入力が可能になるだけでなく，指への負担も少ないとされるため，若年層を中心に多く利用されている．また，Android や iPhone 等のほとんどのプラットフォームで利用することができる．

そこで本研究では，スマートフォンでのフリック入力を対象としたキーストローク認証を扱う．これまでのスマートフォンのキーストロークに関わるの研究の多くはパスワードのような定型語（パスフレーズ）による認証可能性を議論している [19–23]．これに対し本研究では，我々のこれまでのキーストローク認証の研究を基礎とし，被験者 21 名による非定型文入力データを対象として，スマートフォンによるフリック入力を行う際の個人認証可能性について検討する [24]．応用として，メールや Twitter，e-learning 等のなりすましを検出でき，システムをロックしたり，通信会社に通報するなどの新しいセキュリティシステムへの適用が期待できる．

Fig.1 Flick input on smartphone

2 キーストローク認証手法

Fig.2 は，本論文で提案するスマートフォンによるキーストローク認証システムの識別（Identification）及び照合（Authenticaion）過程である．本システムには，2 つのモードが存在する．1 つはプロファイル登録（Enrollment）モードであり，もう 1 つが認証（Identification, Authenticaion）モードである．

プロファイル登録モードは，Fig.2 の実線で示す流れである．フリック入力時にバックグランドでスマートフォンのセンサーが動作し，キーストロークデータとして収集する．次にキーストロークデータから特徴量を抽出し，プロファイル文書をデータベースに登録する．

認証モードは，Fig.2 の破線で示す流れである．プロ

* 明石工業高等専門学校専攻科 機械・電子システム工学専攻
Advanced Cource of Mechanical and Electoronic System Engineering, Akashi National College of Technology
† 明石工業高等専門学校電気情報工学科
Department of Electrical and Computer Engineering, Akashi National College of Technology
‡ 兵庫県立大学 応用情報科学研究科
Graduate School of Applied Informatics, University of Hyogo

ファイル登録モードと同様に，未知入力者からキーストロークデータを収集し，特徴量を抽出し，認証対象の未知文書を生成する．この未知文書と，事前にデータベースに登録されている登録プロファイル文書とを比較することにより，入力者の識別及び照合を行う．そして，入力者が登録者であると認証された場合は，入力者の未知文書を登録プロファイルとして新たにデータベースに追加する．一方，登録者に該当しないと判定されれば，スマートフォンの通信会社へ通報したり，当該入力者を強制的にログアウトさせるなどの措置を行う．

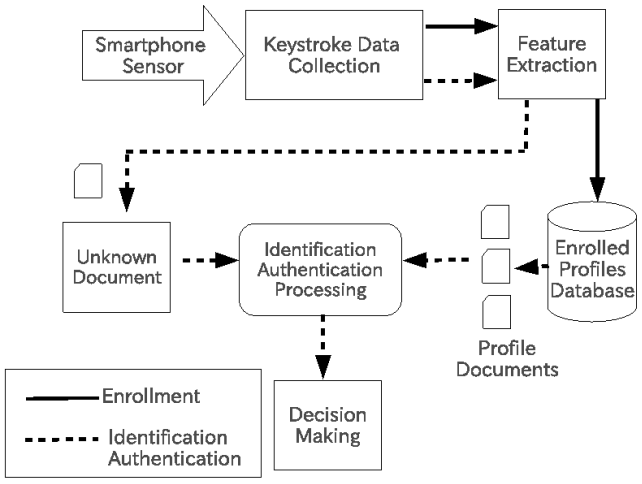

Fig.2　Identification and authentication process of keystroke dynamics on smartphone

Fig.5 に記録されたキーストロークデータ例を示す．第 1 フィールドに入力文字，第 2 フィールドにフリックの状態（0:押す，1:離す，2:保持），第 3 フィールドにキーイベントの x 座標，第 4 フィールドにキーイベントの y 座標，第 5 イールドにキーイベントの圧力，第 6 フィールドにキーイベントの時刻が UNIX 時間（ミリ秒単位）が記録される．

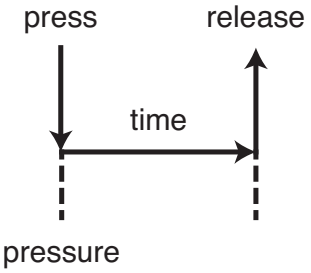

Fig.3　Keystroke measurements of flick time

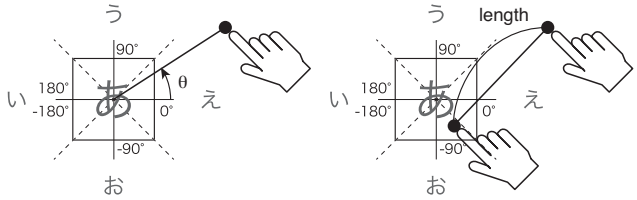

Fig.4　Keystroke measurements. (left): direction of flicking (angle), (right): length of flicking (length)

2.1　キーストロークデータと特徴量抽出

キーボードによるキーストローク認証は，キーの文字，キーの押離，キーイベント時間しか計測できなかった．しかし，スマートフォンでは各種センサーが搭載されているため，多くの測度を取得することが可能である．

ひらがなの入力に着目すると，従来のキーボードによる入力ではローマ字入力を対象にしていたため，母音以外のひらがな 1 文字では 2 文字分の特徴量を得ることができたが，フリック入力はひらがな 1 文字で 1 文字分の特徴量しか得られない．実際に我々は文献 [24] でひらがな 1 文字のフリック時間のみを特徴量測度として扱ったが，キーボード入力の場合のような有意な結果を得ることはできなかった．

そこで本研究では，スマートフォンのセンサーによる特徴量を追加して，次の 4 種類の測度を扱う．まずひらがな 1 文字のフリック時間（time）及び押した（タップ）時の圧力（押下圧:pressure）である（Fig.3）．次にフリック時の方向であり，押離イベントの座標とキーの中心から得られるフリック角度（angle）である（Fig.4 左図）．右方向（0°）へのフリックを “right”，上方向（90°）へのフリックを “up” 等とし，押しただけの場合を “none” とする．得られた各測度のデータを 0 ~ 1 の範囲に規格化する．最後にフリック開始からフリック終了までのフリック距離（length）である（Fig.4 右図）．

```
た,0,144.31952,742.15796,0.08627451,1355760908517
た,2,142.18935,742.15796,0.08627451,1355760908571
た,2,140.05917,742.15796,0.08627451,1355760908593
た,2,127.81065,746.4294,0.08627451,1355760908624
た,2,96.92307,758.1758,0.08627451,1355760908625
た,2,91.59763,761.37933,0.08627451,1355760908626
た,2,88.40237,762.4472,0.08627451,1355760908642
た,2,86.27219,764.5829,0.08627451,1355760908653
た,1,86.27219,764.5829,0.08627451,1355760908680
```

Fig.5　Illustration of keystroke data

各文字の出現回数による下限閾値を N_{TH} = 3 回，フリック時間の上限閾値を T_{TH} = 450 ms とし，各ひらがな文字に対して 1 文書中に出現する測度の平均値（xxx.ave: xxx=time, pressure, angle, length）と標準偏差（xxx.sd）を特徴量とする．

2.2　識別手法

識別手法として，重みつきユークリッド距離（WED:Weighted Euclidean Distance）法と Array Disorder（AD）法，両手法を組み合わせた手法である WED+AD 法について述べる．各手法は，我々の手法 [16] に押下圧，フリック角度，フリック距離を追加したものである．

重みつきユークリッド距離（WED）法は，対象者 A の 1 番目のプロファイル文書 $docA1$ と未知文書 $docUK$ 間

の WED 距離を次式で与える．

$$WED(docA1, docUK) = \sqrt{\frac{1}{4}\sum_{\beta=0}^{3}\frac{1}{m}\sum_{\alpha=1}^{m}\frac{1}{n_\alpha}\sum_{i=1}^{n_\alpha}\left(k_{\alpha(i),\beta} - r_{\alpha(i),\beta}\right)^2} \quad (1)$$

ここで，α はひらがな文字の特徴量，m は特徴量の全種類数を表す．$\alpha(i)$ は α の i 番目の文字を表し，n_α は α で比較される文字の総数である．$r_{\alpha(i),\beta}$ が $docA1$ における文字 $\alpha(i)$ の特徴量 β（$\beta = 0$:フリック時間，1:押下圧，2:フリック角度, 3:フリック長さの各平均値と標準偏差）を表し，$k_{\alpha(i),\beta}$ は $docUK$ における文字 $\alpha(i)$ の特徴量 β を表す．

Array Disorder（AD）法 [8] は，入力文書と未知文書のそれぞれにおいて，各文字を特徴量値に基づき順位付けしたときの不揃度を評価する．$docA1$ と $docUK$ との不揃度を次式で与える．

$$AD(docA1, docUK) = \frac{1}{4}\sum_{\beta=0}^{3}\frac{1}{m}\sum_{\alpha=1}^{m}\frac{1}{\omega(n_\alpha)}\sum_{i=1}^{n_\alpha}\left(\left|rk_{\alpha(i),\beta} - rr_{\alpha(i),\beta}\right|\right) \quad (2)$$

$$\omega(n_\alpha) = \begin{cases} \frac{n_\alpha^2}{2} & (n_\alpha : \text{偶数}) \\ \frac{n_\alpha^2 - 1}{2} & (n_\alpha : \text{奇数}) \end{cases}$$

ただし，α，m，n_α，w_p は式 (1) と同じ変数である．$rr_{\alpha(i),\beta}$ は $docA1$ における文字 $\alpha(i)$ の特徴量 β（$\beta = 0$:フリック時間，1:押下圧，2:フリック角度, 3:フリック距離の各平均値と標準偏差）の順位を表し，$rk_{\alpha(i),\beta}$ は $docUK$ における文字 $\alpha(i)$ の特徴量 β の順位である．

WED 法では特徴量値の差の大きさという絶対的な距離を評価するのに対し，AD 法では特徴量の順位パターン差という相対的な距離をそれぞれ用いている．そこで，性質の異なるこれら 2 つの手法を組み合わせることにより，更なる認証率の向上を図る．WED+AD 法による距離を次式に示す．

$$WED + AD(docA1, docUK) = WED(docA1, docUK) + AD(docA1, docUK) \quad (3)$$

判定には最近傍決定則を用いる．未知文書と各プロファイルの文書間の比較により，最小値を与えるプロファイル文書の入力者を未知文書の入力者とみなす．今，ある被験者 A の入力文書が 5 つ（$docA1$~$docA5$）あるとする．本識別手法では，その中の 1 つ（例えば $docA1$）を未知文書とし，残りの 4 つの文書と他の被験者の入力文書（5 × 人数）を比較し，距離が最も近い登録者を未知文書の所有者とみなす．

3 実験

3.1 実験方法

提案手法の有効性を検証するため，スマートフォンを用いた実証実験を行う．17 歳〜21 歳の高専学生男女からなる 21 名の被験者は各自が使い慣れているスマートフォン端末で実験に参加する．本研究ではプロファイル文書数を 5 文書と設定した．これはキーボードを用いた我々の先行研究との比較のためである．

キーストロークデータの収集には Android 端末向けのフリック入力アプリケーションを開発した（Fig.6）．入力文書は「不思議の国のアリス」の日本語訳 [25] から 1 文書あたりひらがな 300 文字程度を切り出したものを使用した．表示画面に入力文書がひらがなで提示され，1 文字ずつフリック入力するたびに正しければ赤い字に変化する．1 文書あたりの 1 文字ひらがなの平均出現頻度を降順に 20 個まで示したのが Fig.7 である．150 文字入力では 4 回程度のひらがな文字が多く登場するが，300 文字程度になると頻度は倍増し 8 回を越すひらがな文字も多く出現する．

Fig.6 Screenshot of interface of keystroke data collecting system

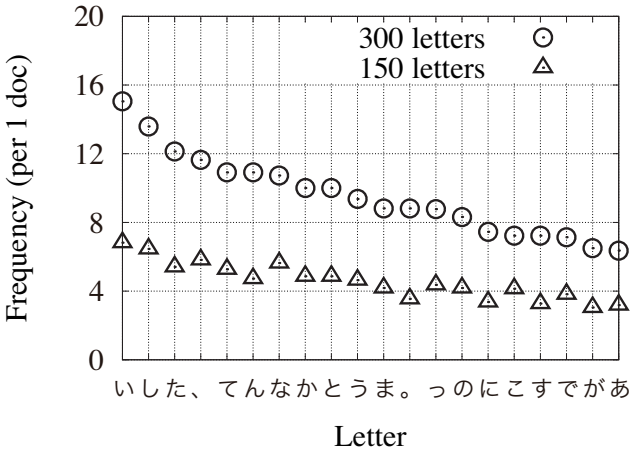

Fig.7 Frequency of each hiragana letter per document

3.2 評価方法

認証方法には識別（Identification）と照合（Authentication）があるため，評価方法もそれぞれにより異なる．

まず，N 人のプロファイル文書の入力者のうち，未知文書 $docUK$ の所有者が誰であるかの識別（Identification）を行う方式について述べる（本方式は 1 対 N 方式ともよばれる）．評価には leave-one-out クロスバリデーション法を採用する．leave-one-out クロスバリデーション法では，実験対象である全てのプロファイル文書から 1 つ取り出し，それを未知文書として評価する．残りの文書をプロファイル文書として未知文書との比較をそれぞれ行い，前述の各識別手法で求めた特徴量の距離が最小の文書を探す．取り出したプロファイル文書の所有者と識別された被験者が一致したときに識別成功，不一致の場合は識別失敗とする．これを全てのプロファイル文書に対して行い，評価指標として次式の識別率を求める．

$$\frac{\text{識別成功数} \times 100}{\text{(1 人あたりのプロファイル数)} \times \text{(被験者数)}} \ [\%] \quad (4)$$

次に，未知文書 $docUK$ の入力者が宣言された正規のユーザであるかの照合（Authentication）を行う方式について述べる（本方式は 1 対 1 方式ともよばれる）．

評価には，Gunetti と Picardi の方法 [8] を用いて導出する．今，ある被験者（例えば A）のプロファイル文書が 5 つ（$A1 \sim A5$）あったとする．未知文書（$docUK$）と各プロファイル文書との識別関数 $d(docUK, docA1)$, $d(docUK, docA2)$, $\cdots$ を求める．識別関数は，WED 法，AD 法，WED+AD 法の各距離に対応する．まず，各被験者ごとの識別関数の平均距離を求める，

$$md(UK, A) = [d(docUK, docA1) + d(docUK, docA2) + \cdots + d(docUK, docA5)] / 5 \quad (5)$$

次に入力者 A の全文書の識別関数の平均距離 $m(A)$ を次の式で示す．

$$m(A) = [d(docA1, docA2) + d(docA1, docA3) + \cdots + d(docA(N-1), docAN)] / {}_N\mathrm{C}_2 \quad (6)$$

次の条件を満たすとき未知文書 $docUK$ の入力者を A とみなす．

1. 入力者 A と未知文書 $docUK$ との平均距離 (5) 式（$md(UK, A)$）は他の入力者との平均距離に対して最短である
2. (2-i) $md(UK, A) < m(A)$ が成り立つか，
   (2-ii) 入力者 A の $md(UK, A)$ の次に小さい $md(UK, X)$ の入力者 X に対して，
   $md(UK, A) - m(A) \leq md(UK, X) - md(UK, A)$
   が成り立つ

評価指標として本人が他人としてみなされる確率である本人拒否率（FRR: False Rejectin Rate）と未登録ユーザを含む他人ユーザが宣言されたユーザとしてみなされる確率である他人受け入れ率（FAR: False Acceptance Rate）とを用いる．

FRR の評価は次の手順で行う．leave-one-out クロスバリデーション法と同様に全実験対象文書から 1 つ取り出して，それを未知文書 $docUK$ とする．上記の条件 1，2 を満たす対象者が未知文書の入力被験者と一致すれば認証成功とし，そうでなければ認証失敗 (false rejection）とみなす．この試行を $M \times N_{doc}$ 回繰り返し，FRR = (Number of false rejections/$(M \times N_{doc})) \times 100$ により FRR を求める．

一方，FAR の評価は次の手順で行う．FAR で扱う未知文書 $docUK$ は外部からの侵入者が入力したものとして扱う．全実験対象文書からある対象者の 1 文書を未知文書 $docUK$ として取り出したときに，その対象者を未登録者として扱うために，全実験対象文書からその対象者の他の文書を取り除く．そして，残りの全対象文書と未知文書とで上記の条件 1, 2 を満たす対象者が出現するか調べる．対象者が出現すれば認証失敗（false acceptance）となり，満たさなければ未登録者による外部からの侵入とみなされて認証成功となる．1 回の試行で $(M-1)$ 人が攻撃に耐えたことになるため，試行を $M \times N_{doc}$ 文書について繰り返すことで，FAR = (number of false acceptance/$((M \times N_{doc}) \times (M-1))) \times 100$ により FAR を求める．

多くの文献が評価指標に FRR と FAR とが等しい等誤り率（EER: Equal Error Rate）を導入している．本論文では上記の条件 2 を以下のように変更し，パラメータ k $(0 < k < 1)$ を導入する．

(2-i)’ $md(UK, A) < m(A)$ が成り立つか，

(2-ii)’ 入力者 A の $md(UK, A)$ の次に小さい $md(UK, X)$ の入力者 X に対して，

$md(UK, A) < m(A) + k\,[md(UK, X) - m(A)]$

が成り立つ

パラメータ k を $0 < k < 1$ で変化させて，FRR と FAR が等しい値を EER とする．

3.3 実験結果

各特徴量がどの程度の測定量になるのかの目安を示す．フリック方向を対するフリック時間（time）の平均値と標準偏差を Fig.8 に示す．フリックしないで押離する（“none”）時間はフリックする時間より短く（100 ms 程度），フリックする場合は 150 ms 程度であることがわかる．フリック方向ごとの押下圧（pressure）が Fig.9 である．押下圧は 0~1 に規格化されている．フリック方向への依存性は見られない．ただし，機種によっては押下圧を計測できずに全て 1 になったり 0 になったりする場合があるが，それらの機種は図には除外している．またフリック角度（angle）の場合を Fig.10 に示す．被験者全員が正しい方向にフリックできていることが確認できる．Fig.11 はフリック長さ（length）の平均値と標準偏差である．単位の dp（dip: density-independent pixel）は解像度に依存しない pixel の単位である．通常であれば機種により長さが異なってくるが，dp で表示することにより，160 dpi の端末を基準にした長さに変換を行う．

次に．Fig.12 に各特徴量の識別率を WED 法，AD 法および WED+AD 法の場合について示す．まず全体を通して WED+AD 法が一番識別率が高い (length.ave が顕著) ことが確認できる．また各測度の平均値は識別率に大き

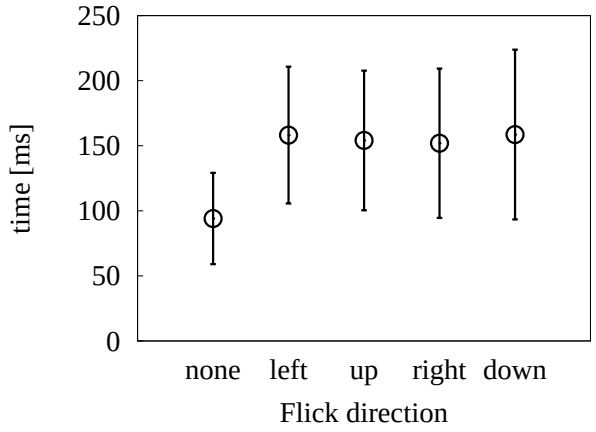

Fig.8　Average and standard deviation values of duration times of filck

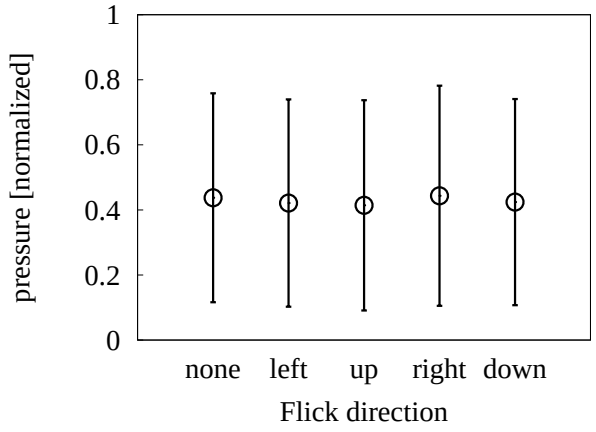

Fig.9　Average and standard deviation values of pressing pressures

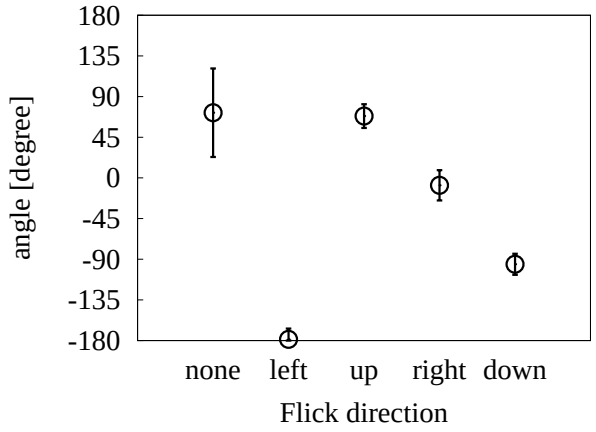

Fig.10　Average and standard deviation values of angles of flick

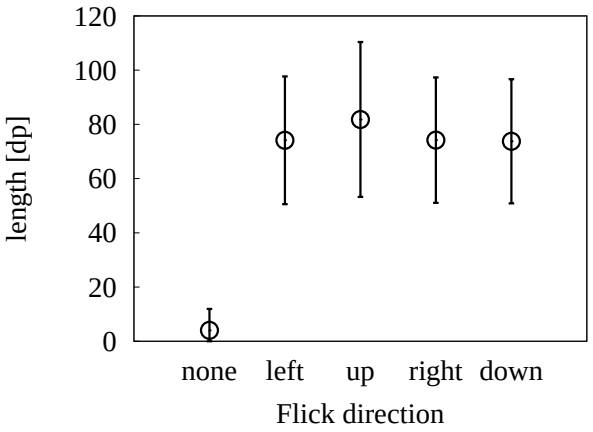

Fig.11　Average and standard deviation values of length of flick

く寄与する (80 % 前後) が，標準偏差は寄与が少ない (40 % 未満)．そこで，式 (1) と式 (2) には各測度の標準偏差は含めないこととした．

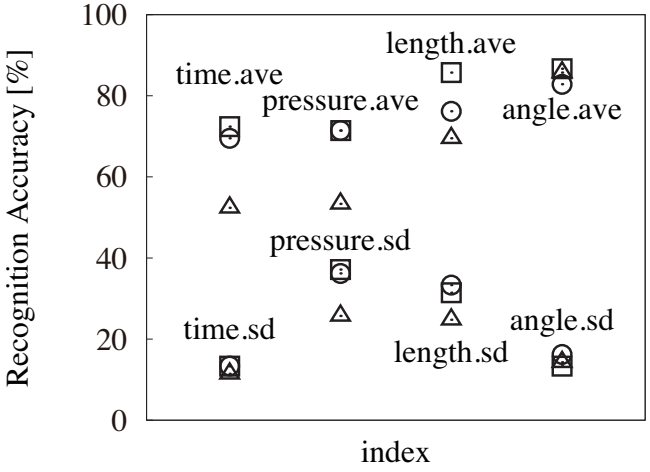

Fig.12　Recognition accuracy of individual features (□:WED+AD, ◯:WED, △:AD)

識別（Identification）認証の場合の識別率の入力文字数依存性を Fig.13 に示す．WED+AD 法が一番識別率が高いことがわかる．今回の実験では 300 文字程度のひらがなを入力しているが，100 文字程度の入力で識別率は 96 % となり，識別が可能なレベルに達することが判明した．

一方，照合（Authentication）認証では，本人拒否率（FRR）の入力文字依存性を Fig.14 に，他人受入率（FAR）を Fig.15 に示す．300 文字程度入力すると，FRR~ 1 %，FAR~0.5% となるが，100 文字程度でも FRR~2%，FAR~0.85% と十分に照合が可能であることが確認できる．また等誤り率（EER）を求めるため，節 3.2 で述べた k パラメータを導入して FRR と FAR の変化を示したのが Fig.16 である．FRR は 1% の場合は本人が他人として誤る回数が 1 回だけのため，$k > 0.5$ で FRR= 0 となる．EER は 0.7 ~ 1% 程度であることが示される．

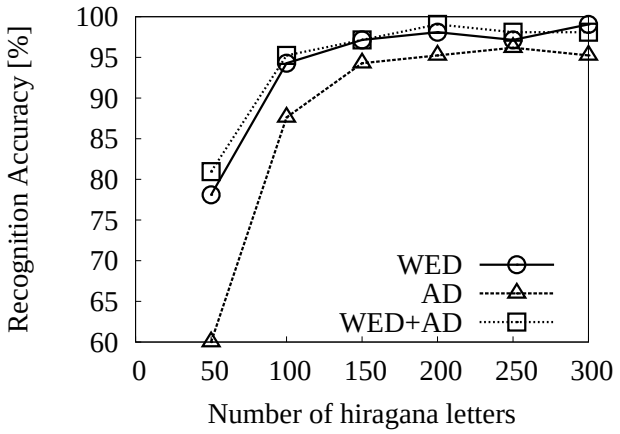

Fig.13　Dependence of recognition accuracy on the number of hiragana letters

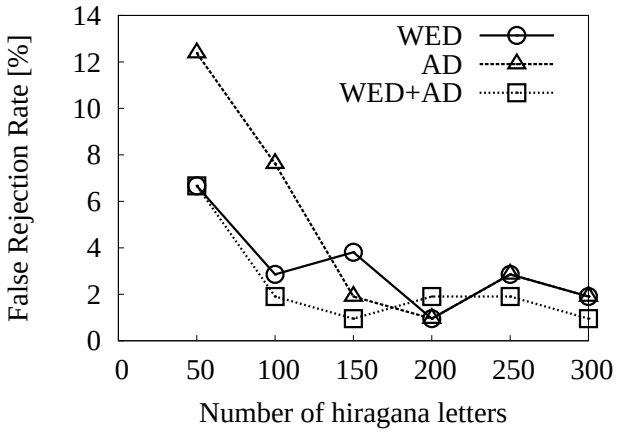

Fig.14　Dependence of FRR on the number of hiragana letters

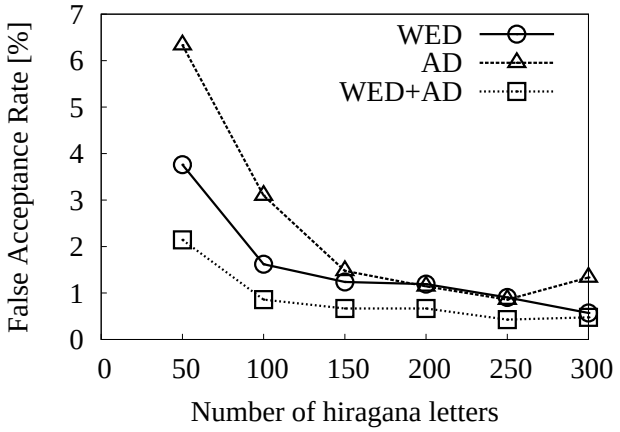

Fig.15　Dependence of FAR on the number of hiragana letters

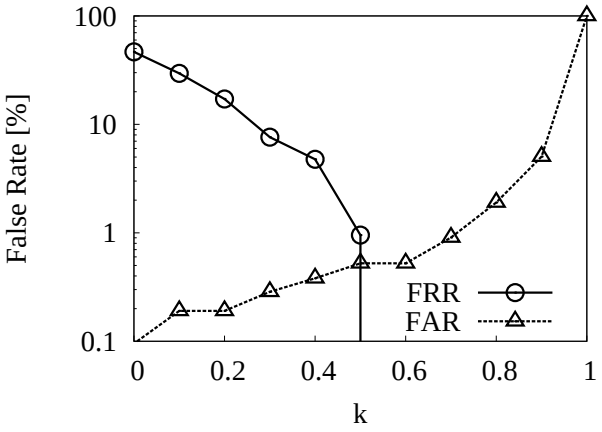

Fig.16　Dependence of FRR and FAR on k parameter in the case of 150 hiragana letters

本実験での文字の出現回数下限閾値 N_{TH}，および文字の打鍵時間上限閾値 T_{TH} の設定の妥当性について言及する．本論文では出現回数の下限閾値を 3 回（$N_{TH} = 3$）と設定した．Fig.17 に出現回数閾値 N_{TH} への識別率の依存性を示す．入力文字数が 300 文字程度のときは出現回数閾値 N_{TH} はあまり影響を及ぼさないが，150 文字のときは 4 文字を超えると識別率が急激に低下する．これは Fig.7 からわかるように $N_{TH} \sim 4$ 程度になると 1 文書あたりの有効ひらがな種数が極端に減ってくることが原因である．以上から本研究での $N_{TH} = 3$ の設定に問題はないと考えられる．

さらに，打鍵時間閾値 T_{TH} への識別率の依存性についても調べた．Fig.18 に示すように識別率は打鍵時間閾値にあまり依存しないことがわかる．打鍵時間閾値 $T_{TH} = 450$ ms と設定したが，1 文字のみの特徴量を対象としている場合にはあまり認証精度に影響はない．

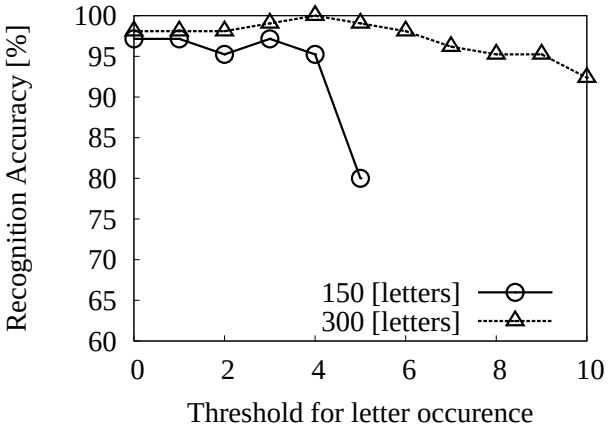

Fig.17　Dependence of Recognition accuracy on threshold for letter occurence N_{TH}

Table 1　Related studies

	password	# of training participants	# of training samples	classifier	EER[%]
Clarke and Furnell [19]	4 digit	30	30	Neural Net	9–16
	11 digit	30	30	Neural Net	5–13
	6 character	30	30	Neural Net	15–21
Saevance and Bhatarakosol [20]	10 digit	10	20	KNN	1
Campisi et al. [21]	10 character	30	6	Statistical	13
Hwang et al. [22]	4 digit	25	5	Statistical	4
Chang et al. [23]	3–6 thumbnails	100	5	Statistical	6.9

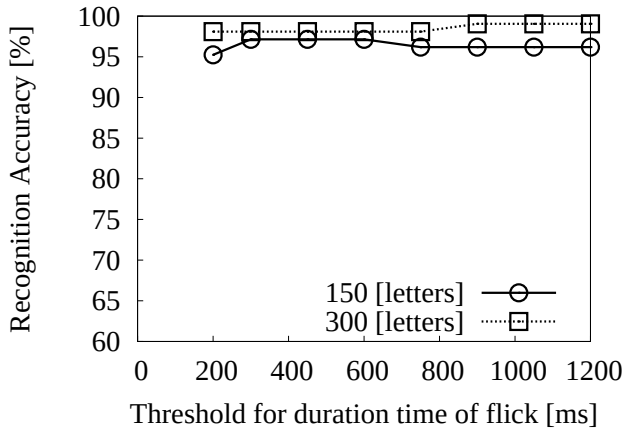

Fig.18　Dependence of Recognition accuracy on threshold for duration time of flick T_{TH}

3.4　関連研究との対比

モバイル端末による非定型文入力に対するキーストローク認証の研究は，我々の知る限りにおいてまだほとんど行われていない．そこでモバイル端末により PIN（Personal identification number）やパスワードを入力した場合の関連研究を Table 1 に示す．特徴量の点で我々の研究アプローチに近いのは Saevance と Bhatarakosol [20] と Chan ら [23] の研究であり，キーストローク時間だけでなく押下圧も特徴量に考慮している．多くの研究が EER は数 % 程度であることから我々の研究結果の優位性をみることができた．

4　おわりに

本研究では非定型な文章のフリック入力時のキーストロークデータから個人識別を行う手法について検討した．具体的にはひらがな 1 文字に関するフリック時間に加えて，通常のキーボードでは測定できない押下圧やフリック角度も特徴量とし，識別の向上に寄与する特徴量を確認し，それらによる評価指標を構成した．今後更に識別率を向上させる特徴量について検討を進めたい．

本研究では，現実的な状況への第一段階のアプローチとして，各被験者が日頃使い慣れているスマートフォン端末で実験を実施した．すなわち，各自の使用スマートフォンの機種は問わず包括的に特徴抽出を行った．今後，各自の機種変更（交換）を行った場合や統一機種による場合の実験を実施し，それらの結果との比較を通して，機種依存性の程度についても定量的な評価を行いたい．

謝辞

本論文作成にあたりお世話になった松原慶朋氏や実験の実施にあたり尽力を尽くしていただいた吉次優氏に謝意を表します．本研究の一部は日本学術振興会の科学研究費補助金（24500101）の助成を受けたものである．

参考文献

[1] S. Banerjee and D. Woodard, "Biometric authentication and identification using keystroke dynamics: A survey," Journal of Pattern Recognition Research, 7, pp. 116-139 (2012)

[2] R. Joyce and G. Gupta: Identity authentication based on keystroke latencies,*Communication of the ACM*, 33-2, pp.168-176(1990)

[3] 粕川，森，小松，赤池，角田: 打鍵データに基づく個人認証システムと改良, 情報処理学会論文誌，33-5, pp.728-735 （1992）

[4] 佐村，高岡，柴田，西野，小高，小倉: 打鍵データの特性を生かした個人認証システム，福井工業大学研究紀要，第二部, No. 29, pp.305-312 （1999）

[5] 小谷, 法岡, 堀井: テンキーパネルを用いた打鍵認証システムの構築と評価，ヒューマンインタフェース学会論文誌，7-1，pp.149-156 （2005）

[6] 金子: ハミング距離似のフィルタリングを用いたキーストロークダイナミクスによるパスワード強化，電子情報通信学会技術研究報告， CAS, 回路とシステム 111(242), pp.43-48 （2011）

[7] F. Monrose and A. Rubin: Keystroke dynamics as a biometric for authentication, Future Generation Computer Systems, 16, pp.351-359 (2000)

[8] D. Gunetti and C. Picardi: Keystroke Analysis of Free Text, ACM Trans. Inf. Syst. Secur.，8-3，pp.312-347 (2005)

[9] 倉橋，田中，小松: スコアの累積値を用いたキーストロークダイナミクスによる個人認証手段，電子情報通信学会技術研究報告，IE，106-244，pp.35-40 (2006)

[10] 片岡，宮本，青木，泉: キーストロークの統計情報を利用した個人認証手法の提案，電子情報通信学会技術研究報告，SEC，107-140，pp.23-30 （2007）

[11] 佐村，西村: 非定型な日本語文入力におけるキーストロークダイナミクス識別，システム制御情報学会論文誌，22-4，pp.145-153 （2009）
[12] C.C. Tappert, M. Villani, and S. Cha: Keystroke Biometric Identification and Authentication on Long-Text Input, Behavioral Biometrics for Human Identification: Intelligent Applications, IGI global, pp.342-367 (2009)
[13] 佐村，西村: 日本語非定型文入力のキーストロークデータに基づく個人識別ハイブリッドモデル，計測自動制御学会論文集，Vol.46，No.11．pp.676-684（2010）
[14] T. Samura and H. Nishimura: Keystroke Dynamics for Individual Identification in Japanese Free Text Typing, SICE JCMSI, Vol. 4, No. 2, pp.172-176 (2011)
[15] 平岡，佐村，西村: 日本語自由文書入力におけるキーストローク認証，第 10 回情報科学技術フォーラム (FIT2011)，第 4 分冊，RL-005，pp.19-24 （2011）
[16] T. Samura and H. Nishimura: Personal Identification and Authentication Based on Keystroke Dynamics in Japanese Long-Text, in Continuous Authentication based on Biometrics: Data,Models, and Metrics, I. Traore et al.(Eds.), IGI Global, pp.212-231 (2011)
[17] 櫻井，宮本，青木，岩田，汐崎: ニューラルネットワークを用いたキーストローク特徴によるユーザ認証，電子情報通信学会技術研究報告， IT, 情報理論 110（442）, pp.213-220（2011）
[18] Y. Matsubara, T. Samura and H. Nishimura: Robustness of Keystroke Dynamics against Changing in Input and Recognition Conditions for Japanese Atypical Text, Proc. of ISTS2012, pp.103-106 (2012)
[19] N. L. Clarke, S. M. Furnell: Advanced user authentication for mobile devices, Computer & Security, Vol. 26, No. 2, pp. 109-119 (2007)
[20] H. Saevance, P. Bhatarakosol: User authentication using combination of behavioral biometrics over the touchpad action like touch screen of mobile device, Proc. of ICCEE 2008, Computer and Electrical Engineering, pp.82-86 (2008)
[21] P. Campisi, E. Majorana, M. L. Bosco, A. Neri: User authentication using keystroke dynamics for celluar phones, IET Signal Processing, 3, pp. 333-341 (2009)
[22] S. Hwang, S. Cho, S. Park: Keystroke dynamics based authentication for mobile devices, Computers & Security, 28, pp. 85-93 (2009)
[23] T. Y. Chang, C. J. Tsai, J. H. Lin: A graphical-based password keystroke dynamics authentication system for touch screen handheld mobile devices, Journal of Systems and Software, 85, pp. 1152-1165 (2012)
[24] 佐村，西村:スマートフォン端末の日本語入力キーストロークによる個人認証，第 55 回システム制御情報学会研究発表講演会講演論文集，pp. 189-190（2012）
[25] プロジェクト杉田：不思議の国のアリス（翻訳：山形浩生），http://www.genpaku.org/alice01/alice01j.html （2013.06.27 accessed）