L-021

スマートフォンでのキーストロークダイナミクスにおける特徴量抽出の検討

A study of Feature Extraction for Keystroke Dynamics on Smartphone

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じ価値を持ち始めている．従って，スマートフォンを盗難にあった際の個人情報漏洩や不正使用のリスクは大きい．

不正アクセスへのセキュリティ対策としては，パスワードによるシステムロック機能がある．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バイオメトリクス（生体認証）を用いたシステムロック手法が検討されている．

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．通常のキーストロークダイナミクスはパソコンのキーボード入力を対象としている．我々はこれまで，キーボード入力によるキーストロークダイナミクスについて，識別を向上させる手法の研究を行なってきた [1]．しかし，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ダイナミクスの研究へのニーズが高まると考えられる．

そこで本研究では，スマートフォンを対象としたキーストロークダイナミクスを扱う．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，システムロック手法として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 [2]．これに対し本研究では，我々がキーボードを対象に行なってきた，非定型な異なる文書の入力からでも個人を認証する非定型文入力の認証可能性を検討する．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．

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．

Fig.1 Flick input on smartphone

本研究では，我々のこれまでのキーストロークダイナミクスの研究をベースに，被験者 21 名による非定型文の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．

2 キーストロークダイナミクス手法

キーストロークダイナミクス手法は他のバイオメトリクスと同様にデータ収集，前処理，特徴量抽出，識別手法，判定により認証を行う．

2.1 キーストロークデータ収集

キーボードによるキーストロークダイナミクスは，あるキーを押す，離す，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．本稿ではフリック 1 文字入力時の状態（押す（press），離す（release）），各状態イベントの時間，座標 (x, y)，押下圧を取得する．

2.2 特徴量抽出

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 [3] 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

* 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

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加え，3 種類の測度を扱う．Fig.2 左図は，ひらがな 1 文字のフリック時間（f_time）及び押した（タップ）時の圧力（押下圧:p_pressure）である．また右図は，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（f_angle）である．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．得られた各測度を 0 ~ 1 の範囲に規格化する．

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，各測度の平均値（xxx.ave: xxx=f_time, p_pressure, f_angle）と標準偏差（xxx.sd）を特徴量とする．

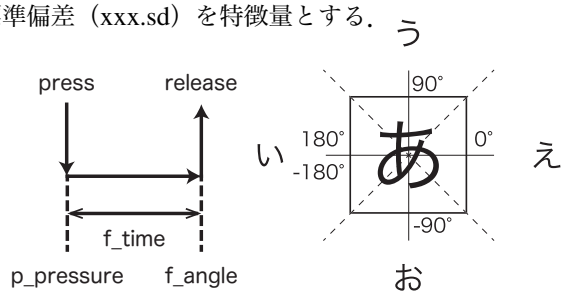

Fig.2 Keystroke measurements. (left): flick time (f_time) and pressing Pressure (p_pressure) of each hiragana letter, (right): direction of flicking (f_angle)

2.3 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 [1] に押下圧とフリック角度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．

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

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：フリック角度の平均値と標準偏差）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．

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

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

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：フリック角度の平均値と標準偏差）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 名の被験者は自分が使い慣れているスマートフォン端末で実験を行う．

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用いた（Fig.3）．入力文書は「不思議の国のアリス」の日本語訳 [4] から 1 文書あたりひらがな 310 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.4 である．

本研究の評価には，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，評価を行う 1 対 N 方式を用いる．識別率評価には 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，次式より識別率を求める．

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

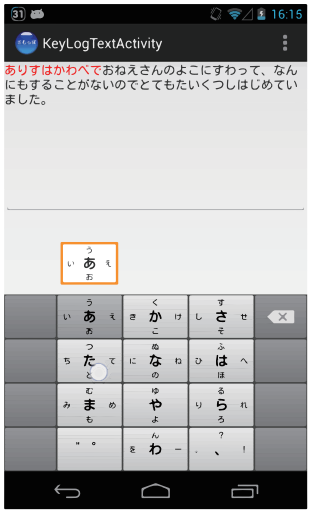

Fig.3　Screenshot of interface of keystroke data collecting system

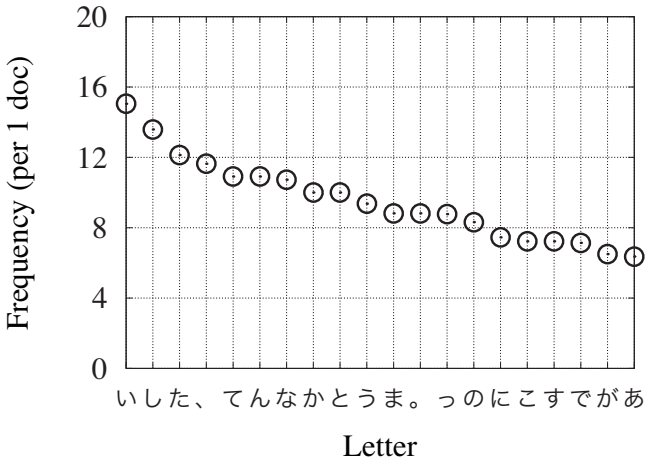

Fig.4　Frequency of each hiragana letter per document

4　実験結果

各特徴量がどの程度になるのかの目安として，フリック方向を対するフリック時間の平均値と標準偏差を Fig.5 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が Fig.6 である．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．またフリック角度の場合を Fig.7 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．

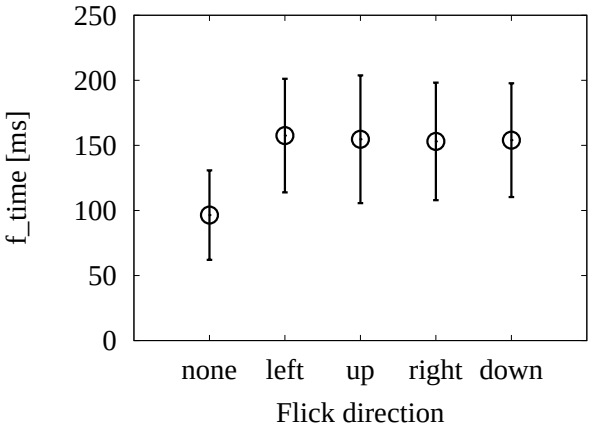

Fig.5　Average and standard deviation values of duration times of filck

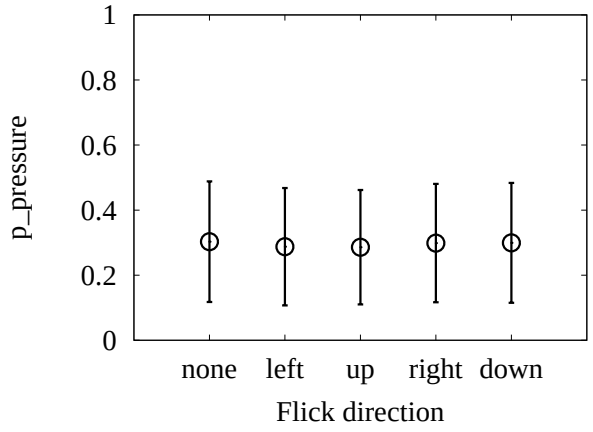

Fig.6　Average and standard deviation values of pressing pressures

次に各特徴量の中から識別率を上げる特徴量について調べる．Fig.8 にそれぞれの特徴量の識別率を WED 法，AD 法および WED+AD 法の場合について示す．まず WED+AD 法が一番識別率が高いことが確認できる．また各特徴量のみの識別では最大で 80 [%] 程度であるので，これらの特徴量を組み合わせることにより識別率の向上を図る．各測度の平均値は識別率に大きく寄与するが，標準偏差は寄与が少ない．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．

特徴量を組み合わせた識別率の入力文字数依存性を

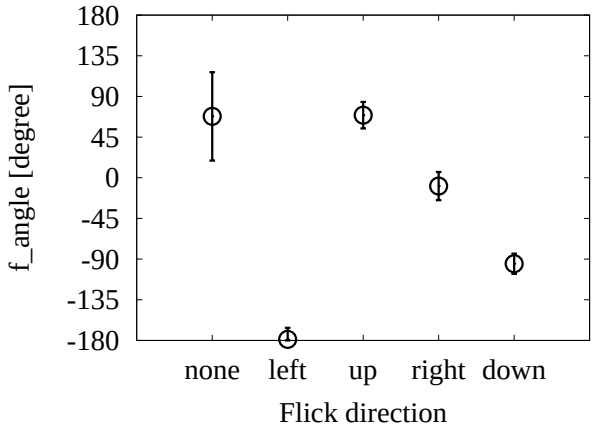

Fig.7 Average and standard deviation values of angles of flick

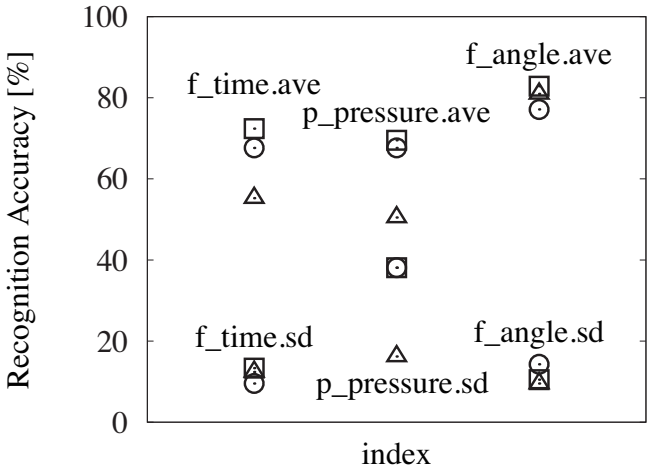

Fig.8 Recognition accuracy of individual features (□:WED+AD, ○:WED, △:AD)

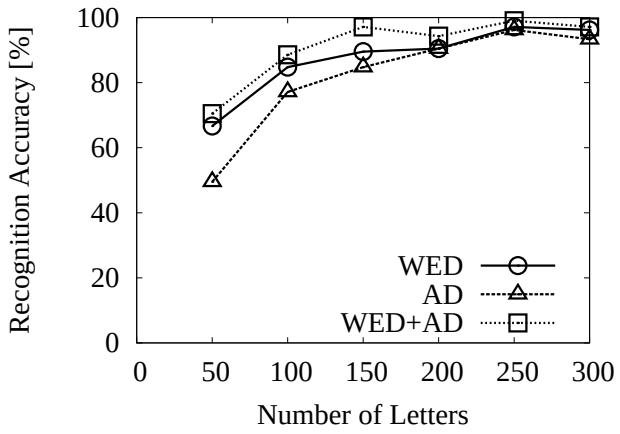

Fig.9 Dependence of recognition accuracy on number of hiragana letters

Fig.9 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 310 文字程度のひらがなを入力しているが，150 文字程度入力すれば識別率は 97 [%] となり，識別が可能なレベルに達することが判明した．

5 おわりに

本研究では非定型な長文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．

また本研究では，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．統一した端末による実験についても検討を行ったが，多くのユーザは様々な性能の端末を持っているので本実験のほうが実用的であると考えた．また様々なセンサーを用いた個人認証を議論する際，出力結果が機種に依存することは避けられない．本研究では，スマートフォンの機種依存も考慮したキーストロークダイナミクスを研究する．すなわちどのような機種のスマートフォンを持っているかということも本人の特性のひとつとして扱う．ただし，今後統一機種による実験との比較を通して，機種依存性についても定量的な評価を行いたい．

謝辞

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] 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)

[2] N. L. Clarke and S. M. Furnell: Advanced user authentication for mobile devices, Computer & Security, Vol. 26, No. 2, pp. 109-119 (2007)

[3] 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)

[4] 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）