L-021

空中筆記動作で認証するための筆記者モデルの検討

Writer Model for Authentication in the Aerial Writing Operation

青木 康祐 †　　中井 満 †

Kosuke Aoki　Mitsuru Nakai

1. はじめに

加速度センサ・角速度センサを内蔵した筆記具を持ち，空中に文字を書く動作でユーザを認証・識別する研究が行われている [1][2]．既報 [3] では登録時に筆記したテキストとは異なる文字でも認証ができるテキスト独立型の手法について発表した．一般的に，登録したテキストを忘れなければユーザが決めた文字列で登録・認証を行うテキスト依存型の手法の方が高い認証精度が得られる．そこで本研究では，テキスト依存型の認証に適したユーザのモデル化について検討する．

2. 空中筆記者認証の原理

2.1 空中筆記の加速度・角速度パターン

加速度・角速度センサを内蔵したデバイスを筆記具として用いる．今回は，Nintendo Wii リモコンを使用した．図 1（左）に示す通り，xz 平面が筆記面，y 軸がペン先方向である．図 1（右）のように空中に文字を書き，筆記動作の信号を 10 ミリ秒間隔でサンプリングする．時刻 t の加速度 $\vec{a_t} = (a_x, a_y, a_z)$ と角速度 $\vec{\omega_t} = (\omega_x, \omega_y, \omega_z)$ を合わせた 6 次元の信号を $\vec{o_t}$ として，筆記時間長 T の信号 $O = \vec{o_1}\vec{o_2}\vec{o_3}\ldots\vec{o_T}$ を筆記パターンとする．加速度信号 $\vec{a_t}$ には重力加速度が加わっているので，筆記パターンの平均加速度を減算してバイアス成分を除去する．また，同じ筆記者でも筆記するたびに筆記信号の振幅が異なるので，加速度信号と角速度信号のそれぞれの大きさの平均が 1 になるように正規化する．

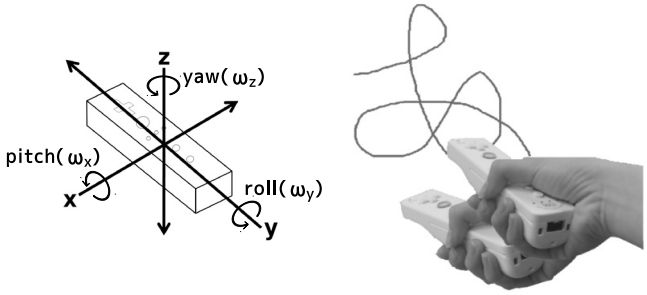

図 1: 筆記具の座標系と空中筆記の様子（筆跡は見えない）

2.2 テキスト依存型の筆記者認証システム

筆記者認証を本人か他人かの 2 クラスの識別問題と捉え，ベイズ識別によって本人である確率が閾値以上のときに本人と認証する．既報 [3] では，テキスト独立型の認証システムについて説明した．ここでは，テキスト依存型のシステムについて説明する．図 2 に空中筆記者認証システムの構成を示す．ユーザが登録する時にはユーザが任意に選んだテキストを書き，2 節で述べたパターン O から本人の確率モデルを学習する．モデル化については次節で説明する．他人モデルは事前に大勢から収集したサンプルを用いて学習しておく．認証時には，ユーザが登録したテキストを書き，本人モデルからの出力確率 $P(O|$ 本人$)$，他人モデルからの出力確率 $P(O|$ 他人$)$，および事前確率 $P($本人$)$， $P($他人$)$ から事後確率 $P($本人$|O)$ を計算する．

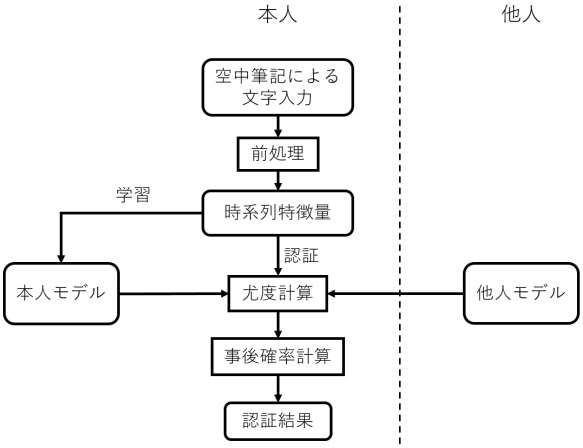

図 2: 筆記者認証システムの構成

2.3 筆記者モデル

本人モデル，および他人モデルは，それぞれ 1 個の HHM（Hidden Markov Model）でモデル化する． HMM は，複数の状態（定常信号源）を遷移することで，時系列信号を生成するモデルである．筆記者認証で用いる筆記パターンは時系列の特徴量であるので，HMM が適していると考えられる．本研究では，連続分散型の HMM を用い状態遷移の型，状態数，出力確率密度関数を表す正規分布の混合数について検討した．

テキスト独立型の場合のモデル化

テキスト独立型の認証法では登録に使用したテキストと認証に使用するテキストが異なるので，筆跡（ここでは加速度信号）を直接比較することはできない．そこで，筆記全体の加速度の分布を GMM (Gaussian mixture model) でモデル化する方法が考えられる．既報 [3] では， GMM を持つ状態間を全結合で遷移可能な ergodic 型 HMM （図 3（左））でモデル化した．このモデル化では個々の状態はその筆記者に見られるプリミティブな動作（癖）を表し，状態の遷移系列が筆記したテキストを表している．したがって，状態数は比較的少なくて済み，先行研究 [3] では 5 状態 3 混合でモデル化した．

†富山県立大学, Toyama Prefectural University.

テキスト依存型の場合のモデル化

登録と認証に同じテキストを使うテキスト依存型の認証では，ergodic 型 HMM において，ある決められた状態遷移のみが高い確率で起こるものと考えられる．すなわち，この状態遷移系列を直列に並べた left-to-right 型の HMM （図 3（右））になると考えられる．このモデルでは状態の先頭から順に，書き始めから書き終わりまでの筆跡を表している．なお，筆記中に同じ動作が複数回あったとしても異なる状態を割り当てなければならないので，ergodic 型のモデルと比べて，多くの状態数が必要になる．予備実験により，テキストを筆記する時系列の長さ T に対して，$T/20$ 個の状態でモデル化することにした．また，各状態に割り当てられる筆跡は大きく変わらないと考えて，混合数は 1 とした．

なお，認証を破ろうと他人が筆記する場合，テキストの内容（文字種）も長さ（文字数）も異なるので，他人モデルはこれを考慮してモデル化しなければならない．まず，何を書かれるか分からないので，想定するすべての文字種を用いて，1 文字分の left-to-right 型のモデルを学習する．このとき，状態に割り当てられる筆跡の種類が多いので，混合数を 3 とした．また，何文字書かれるか分からないので，1 文字の最終状態から，先頭状態に遷移することで，任意の長さのテキストに対処する．

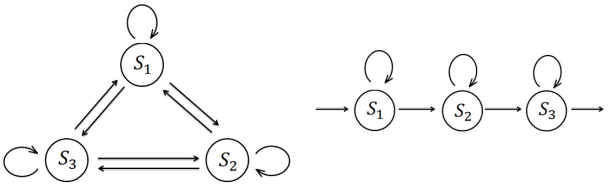

図 3: ergodic 型 HMM(左) と left-to-right 型 HMM(右) の構造

3. 筆記者認証実験

3.1 HMM の遷移型による比較

テキスト依存型の認証のもとで，left-to-right 型 HMM と ergodic 型 HMM の比較実験を行った．筆記者 30 名のデータから，20 名を登録者，10 名を詐称者に選んだ．登録者のうちの 1 名を本人としたときに，残りの 19 名を他人モデルの学習に用いた．本人を交代して，20 通りの交差確認を行った．実験ではテキスト長 n が 1 ～ 10 文字の場合について，それぞれ比較した．

実験の状況は，まず，ユーザが登録するときは，n 文字のテキストを選び，3 回書いて本人モデルを学習した．認証するときは，同じテキストを 1 回書いて本人か否かを識別した．次に，他人が認証を破ろうとする場合，今回はテキスト長が n 文字であることを知っているがテキスト内容は知らず，ランダムに n 文字書くことにした．これを本人については登録者を交代しながら合計 1,000 回，他人については合計 100,000 回試行した．なお，実験では実際にテキストを筆記したのではなく，30 人が筆記した 46 文字 300 セットから組み合わせて生成した．

本人と判定する確率閾値を変化させ，本人拒否率と他人受入率が等しくなる等誤り率を表 1 に示す．どちらの HMM でも，テキストが長いほど等誤り率が低くなり， left-to-right 型の HMM でモデル化した方が高い認証精度が得られた．

表 1: テキストの長さと等誤り率 [%] の関係

テキスト長	1	2	3	4	5	6	7	8	9	10
left-to-right	8.6	3.8	2.8	2.4	1.9	1.5	0.8	0.9	5.3	13.7
ergodic	36.0	5.2	4.1	3.4	2.0	2.4	2.0	2.1	2.4	2.0

表 2: 本人拒否率 [%] の変化（$n = 5$）

	覚えている→忘れている
left-to-right	1.9 → 79.5
ergodic	2.0 → 19.0

表 3: 他人受入率 [%] の変化（$n = 5$）

	知らない→知られた
left-to-right	1.9 → 11.6
ergodic	2.0 → 4.5

3.2 状況の変化による認証精度の変化

以下の 2 つの状況における認証精度を調査した．

状況 1. ユーザが登録したテキストを忘れた場合の本人拒否率

状況 2. 登録したテキストを他人に知られた場合の他人受入率

実験はテキストの長さが 5 文字の場合に限った．状況 1 については本人が登録した文字以外のテキストをランダムに合計 10,000 回試行した．状況 2 については他人が知ったテキストを合計 10,000 回試行した．状況 1 の結果を表 2，状況 2 の結果を表 3 に示す．これらの状況においては，ergodic 型の方が比較的頑健であることが分かった．

4. まとめ

テキスト依存型の認証に適した HMM の検討として，left-to-right 型 HMM と ergodic 型 HMM を比較した．本人がテキストを忘れず，また他人に知られていない状況では left-to-right 型の HMM を用いた方が認証精度が良い．しかし，本人がテキストを忘れたり，他人に知られたりすることを想定した場合には ergodic 型の方が認証精度が良いことが分かった．

謝辞 本研究は JSPS 科研費 24500151 の助成を受けて行った．

参考文献

[1] 行方 他，“携帯端末の動きによる個人認証手法の評価,” 情報処理学会 CSS（2004-11）
[2] 中井，山崎，大坪，“空中手書き文字の認識と筆記者の識別に関する検討,” 信学総大，AS-3-10（2014-3）
[3] 青木，中井，“空中筆記者識別のための学習用文字セットの検討,” 第 14 回情報科学技術フォーラム（2015-9）