

Leap Motion を用いた生体認証アプリケーションの開発

井川 征士¹ 堂園 浩^{1,a)}

概要: 現在タッチパネルを用いた入力方式が主流だが、近年新たな方式としてモーションセンシングというユーザー・インターフェースが注目を集めている。そこで本研究では、近年問題となっているセキュリティの分野に注目し、バイOMETRICSの分野において最も偽造が難しい行動的特徴を取り込んで、モーションセンサーデバイスの一つである Leap Motion を用いた生体認証を行うアプリケーションの開発を行った。

キーワード: 携帯端末, セキュリティ, 認証

Development of the Biometrics Authentication Application using Leap Motion

IGAWA SEIJI¹ DOUZONO HIROSHI^{1,a)}

Abstract: New user interface called the motion sensing that uses the device of the non-contact type unlike the conventional touch screen method attracts its attention. In this research, the application to perform biometrics authentication using Leap Motion which is one of the motion sensor devices is developed. It perform biometrics authentication using feature points of the traces moving fingers.

Keywords: portable terminal, security, authenticate

1. はじめに

近年、一般的に普及しているスマートフォンやタブレットといった端末は、キーボードやマウスなどのデバイスを用いた操作ではなく、タッチパネルによる接触型のタッチスクリーン方式が幅広く利用されている。ところが、近年になって従来の接触型の入力方式とは異なる、非接触型のデバイスであるモーションセンサーデバイスを用いたモーション・センシングという新たな U・I (ユーザー・インターフェース) が注目を集めている。U・I とは、利用者 (ユーザー) とコンピューターとの入出力のやり取りを行うものを指す。キーボードやマウスがそれらに該当する。モーションセンサーデバイスは非接触型のデバイスなので、

手術室のような医療の現場や飲食店の厨房といった衛生面の配慮が求められる場面で期待されている。これらのデバイスは今後携帯端末に標準搭載される可能性があり、将来的にコンシューマ市場の拡大も考えられる。そこで本研究では、モーションセンサーデバイスの一つである「Leap Motion」を用いた生体認証を行うアプリケーションの開発を行った。

2. モーションセンサーデバイス

2.1 Leap Motion

「Leap Motion」は、2012年にアメリカの Leap Motion 社から発売された「手」や「指」の動きを検知することが可能なセンサーデバイスである。その外観は図 1 に示す。マウスや画面タッチ操作を用いらずに操作が可能で、大きさも 10 × 13 × 76 mm と小型で手元で操作することを想定している。原理として、図 2 を見ると分かるが 3 基の赤外線照射 LED と 2 基の赤外線カメラで構成されている。

¹ 佐賀大学 大学院 工学系研究科 先端融合工学専攻
saga university graduate school
graduate school of science and engineering
department of advanced technology fusion

^{a)} douzono@cc.saga-u.ac.jp



図 1 Leap Motion
Fig. 1 Leap Motion



図 2 内部構造
Fig. 2 The internal structure

赤外線 LED で照射されたオブジェクト（指や手）を 2 基の赤外線カメラで撮影し、画像解析を行うことで現実空間のオブジェクトの位置を特定し、画面上に 3D 表示することが可能である。検知可能な範囲は半径約 50cm、中心角 110 度の空間を 1/100mm 単位で動作を認識する。両手と 10 本の指をそれぞれ独立して同時に認識し、手や指の動きを三次元的にモーションキャプチャを行えるだけでなく、スワイプやタップといったジェスチャーも捉えることが可能である。[1] このように人間にとって直感的でかつ自然に操作可能な仕組みや方法を用いた U・I を NUI (ナチュラルユーザーインターフェース) と呼ばれている。

2.2 Kinect

「Leap Motion」と類似した技術を用いたセンサーで「Kinect」というデバイスがある。「Kinect」とは、マイクロソフト社から発売されたジェスチャーと音声認識によって操作が可能なデバイスである。Leap Motion 同様、物理的なコントローラーを必要とせず、ユーザーの動きを読み取ってモーションキャプチャを行う。ジェスチャー検出には、「Light Coding」と呼ばれる方式を用いている。この方式は、図 3 を参照してもらえると分かるように、赤外線プロジェクターから無数の赤外線ドットを照射し、物体に当たった時のドットパターンの勾配の変化量を読み取る。

2.3 Leap Motion と Kinect の違い

Leap Motion と Kinect のデバイスの違いを表したもの



図 3 Kinect
Fig. 3 Kinect

表 1 Leap Motion と Kinect の違い

Table 1 A difference between Leap Motion and Kinect of Table

	Kinect	Leap Motion
視野角	vertical 43°	150°
	horizontal 57°	
有効距離	0.4 ~ 3m (Near)	
	0.8 ~ 4m (Normal)	2.5 ~ 60cm
精度	1mm	1/100mm
	4 ~ 10m (far)	
計測方式	Light Coding 方式	赤外線カメラ

を表 1 に示す。Kinect は 1 m 以上離れた距離を測定することに優れており、Leap Motion は最大射程が 60cm と短い。その反面、認識精度は 1/100mm と Leap Motion の方が約 100 倍近く優秀で、検出スピードも非常に高速である。また、カラーカメラやマイクといったものを搭載していない分 Kinect よりも非常に小型で安価である。[2] 今回の研究目的は生体認証を行うことなので、精度が低くわざわざ端末から離れて認証を行う必要もない。したがって、本研究ではセンサーデバイスの中では比較的安価で小型な Leap Motion を使用した。

3. 生体認証について

3.1 バイオメトリクス研究の現状

現代社会において、最も使用されているセキュリティ方式はパスワードを用いた認証が一般的である。しかし、パスワードを用いた認証の場合パスワードを盗み見られたり、ツールを用いることで突破されるという事態が問題となっている。セキュリティとして脆弱性を持つパスワード認証に代わるものとして台頭してきたのが、「バイオメトリクス」と呼ばれる指紋や声帯といった身体的特徴、筆跡や瞬きといった行動的特徴を用いた認証である。セキュリティという観点からのバイオメトリクスの利点は、パスワード等の文字や数字を記憶する必要がなく、もし他のユーザーから覗き込まれてそれらの情報が流出するということが少ない。また、ユーザー本人が鍵ということから、IC カードや IC チップを搭載したものを携帯する必要がなく、紛失の危険性もなくなる。しかし、キーとなるデバイスを持ち歩く必要がない反面、生体認証を行うためのセンサーを用いる必要があり、コストと運用の問題が生じる。コストを

抑えると、それに比例して精度が落ちるのが一般的で、認証を行うセンサーによっては現段階では小型化が難しいものもある。また、認証における「厳格さ」を求めると本人拒否率 (FFR) が高くなってしまい、逆に「厳格さ」を緩めると今度は他人受入率 (FAR) が上がりセキュリティとして問題が起こる。現在の生体認証の技術では、指紋を用いた認証の場合ゼラチンでできた人口皮膚やプリンターで指紋を印刷した濡紙で偽装することができ、ちょっとした汚れや傷があると FFR が上がることもある。また、顔認証の場合だと本物の顔と写真との区別が難しく、光の加減や周囲の環境によって認証が左右されてしまう。[3] このように二律背反のジレンマを抱えているのがバイオメトリクス研究の現状である。

3.2 タッチスクリーン方式との比較

現在普及しているスマートフォンやタブレットといった携帯端末はキーボードやマウスといったインターフェースを必要とせずタッチパネルと呼ばれる画面を直接接触することで指やペンの位置を認識することができるデバイスである。これにより、わざわざキーボードの位置を記憶したりすることなく、誰にでも直感的に操作することが可能となった画期的な技術である。この技術を用いた認証方法が研究されている。身体的特徴を用いた様々な認証の問題点は既に述べたが、こちらはもう一つの行動的特徴を用いる方法である。こちらが筆跡パターンを盗み見られたとしても、ユーザーが書くときの癖や筆速パターンまでも模倣するのは容易ではないが、身体的特徴よりも FAR は高いと推測できる。ところが、認証にタッチパネルを用いるので、接触面と指やペンの間で摩擦が生じるため精度がデバイスによって依存してしまう。しかし、本研究で用いる Leap Motion は空間で認証を行うため、接地面は存在せずこれらの問題を気にする必要がないという利点がある。

4. アプリケーションの開発

4.1 開発環境

ソフトウェアは公式でサポートされている開発に必要な開発キットである「Leap Motion SDK (Software Development Kit)」を使い、アプリケーションの開発を行った。この SDK に合わせて、本実験で使用した OS は「Windows 8.1」、開発言語は「Processing」を用いた。Processing の他にも C++、C#、Java、JavaScript、Python、Unity といった言語にも対応している。OS は Mac OS や Linux にも対応している。Processing の特徴として、Java をベースにプログラミングを行うことが可能で、エディタが内蔵されているため環境設定も容易である。また、Windows、Mac、Linux のクロスプラットフォームで開発可能で、マウス以外のカメラやマイクなどのデバイスを入力インターフェースとして扱うことができるという利点がある。Processing

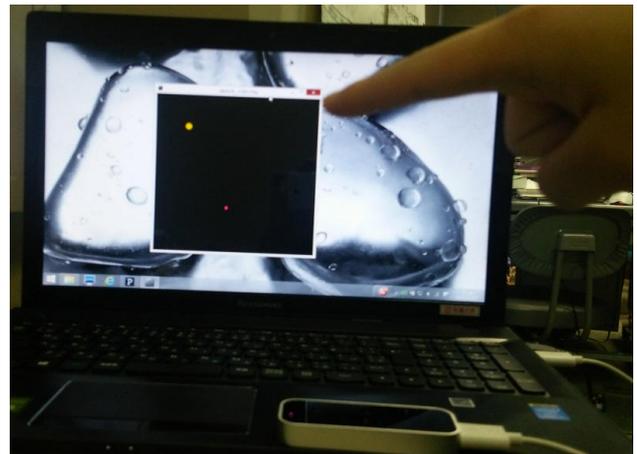


図 4 システムの外観

Fig. 4 The appearance of the system

用の開発ライブラリが一般向けに公開されており、今回は GitHub で公開されている「LeapMotionP5」を利用した。[4]

4.2 システムの外観

今回の実験で作製した生体認証を行うシステムの外観を図 4 に示す。ノート PC 上に置かれたマッチ箱サイズの小型なセンサーが Leap Motion である。そのセンサーの上に指をかざすことで仮想的な座標空間を構築し、Leap Motion で計測した距離等のデータ置き換えることで現実空間における指の位置座標を推測する。

4.3 データ取得

アプリケーションを起動させるとまず 500×500 のマップが表示される (図 5 参照)。このマップ上では一番左上の座標を $(0,0)$ とおき、一番右下を $(500,500)$ とおく。Leap Motion 上に指をかざすとマップ上に指の座標を表すポイントが映る。そのポイントに合わせて、マップ上の基準点となる目印の付いた座標 $(100,100)$ に指を動かし、その基準点に触れると認証が始まる。データの取得は 30fps、つまり 1 秒間に 30 回のデータ更新を行い、終了までの座標や筆速等のデータを記録する。一筆書きで書き終わったら何かボタンを押すとデータ取得は一旦終了となる。

4.4 認証

取得したデータを元に今度は認証を行っていく。まず、図 7 に示すような始点と終点だけが表示されたマップが表示される。この段階では、図に始点と終点が見えるようになっているが、最終的にはどちらか分からないようにする予定である。データ取得のときと同様に、指をかざすとポイントが表示されるので、始点もしくは終点の位置に合わせて指を動かすと認証が始まる。この時点で終点の位置から始めてしまうとこの時点ユーザー本人ではないと認識し、

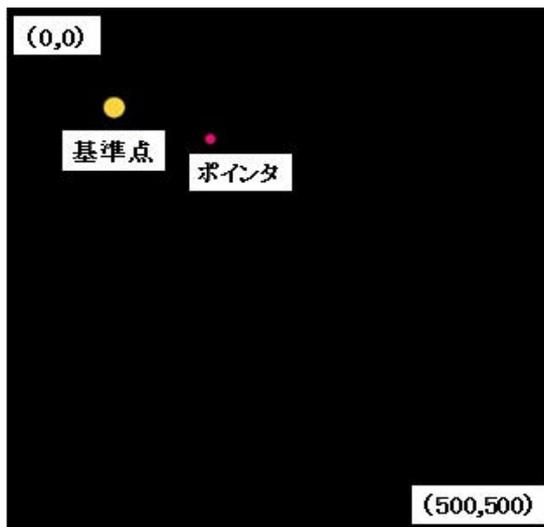


図 5 表示画面
Fig. 5 The display screen

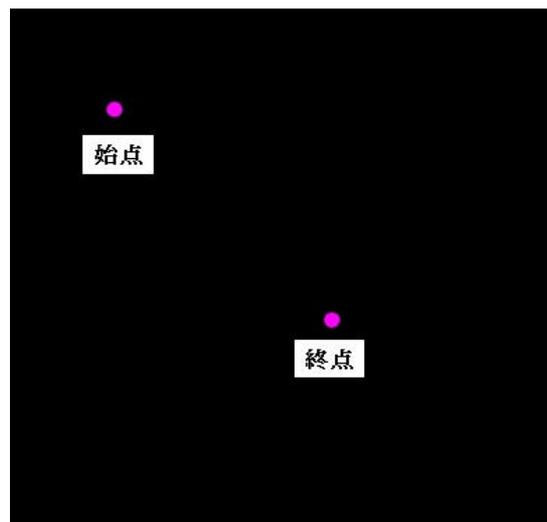


図 7 認証画面
Fig. 7 The authentication screen

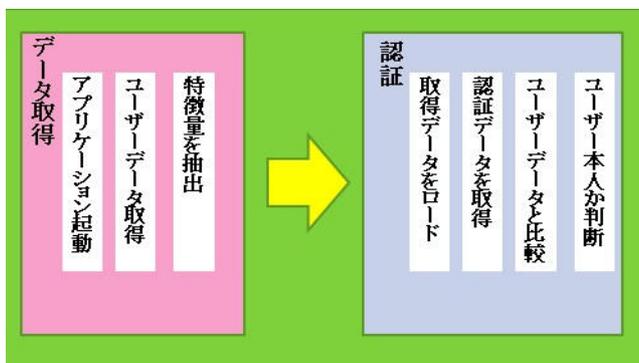


図 6 システムの全体図
Fig. 6 The general view of the system

認証終了時つまり終点から始点まで一筆書きで書き終わった時点で警告を出す。ただし、始点の場所が異なっていることは教えない。始点から筆測のデータを取得し、終点まで書き終わったら今度は認証前に行ったデータ取得時の値と比較を行っていく。比較して近似していった結果、保存したデータを類似性が見当たらなければユーザー本人ではないと認識し警告を出す。類似しているならば、ユーザー本人と認識し認証成功とする。

4.5 実験結果

認証の精度向上のためプログラム内部を書き換えており、現在試行錯誤しているため実験結果は当日示す。

5. 終わりに

現段階では二次元座標を用いて指の位置座標を検出し、そのデータを元に特徴点の検出を行った。しかし、Leap Motion は空間上で描画するため直感的に操作し難く、認証の際に再現することが困難であった。また、認証時に常に腕を上げておく必要があるため、ユーザーへの負担が大

きい。そのため、認証を行う際本人拒否率が高くなる可能性もあり、そうするとセキュリティとして問題があるので考慮する必要がある。今後は更なる精度の向上とユーザーの負担を考慮した認証に加えて、指の関節の位置や長さのデータを検出し、三次元座標上で指の位置座標を読み取りながら認証を行うアプリケーションの開発を行っていく予定である。

謝辞 本研究を行うにあたって、日ごろから丁寧かつ親切なご指導、ご鞭撻いただきました堂蘭浩准教授並びに諸先生方に厚くお礼を申し上げます。また、本研究にあたって御助言、御協力いただいたグループF研究室の学部生、先輩方の皆様に深く感謝いたします。

参考文献

- [1] 中村 薫 (2014): Leap Motion プログラミングガイド, 工学社
- [2] 茂出木裕也 (2013): モーションセンサーで組み込み機器はどう変わる?: モーションセンサーデバイスとは何か, <http://monoist.atmarkit.co.jp/mn/articles/1309/19/news011.html>, 2014年1月28日アクセス
- [3] Serge Malenkovich (2013): 生体認証の問題点, <http://blog.kaspersky.co.jp/biometric-authentication/1425/>, 2014年2月6日アクセス
- [4] 蜜葉 優 (2013): PC 制御 UI の最先端 Leap アプリ開発入門: Processing や JavaScript で Leap Motion を動かす, <http://www.atmarkit.co.jp/ait/articles/1309/30/news016.html>, 2014年1月28日アクセス