

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B1)

(11) 特許番号

特許第6134875号
(P6134875)

(45) 発行日 平成29年5月24日(2017.5.24)

(24) 登録日 平成29年4月28日(2017.4.28)

(51) Int.CI.

G06F 21/32 (2013.01)

F 1

G06F 21/32

請求項の数 36 外国語出願 (全 28 頁)

(21) 出願番号 特願2017-13383 (P2017-13383)
 (22) 出願日 平成29年1月27日 (2017.1.27)
 (62) 分割の表示 特願2015-83696 (P2015-83696)
 の分割
 原出願日 平成20年9月9日 (2008.9.9)
 審査請求日 平成29年2月24日 (2017.2.24)
 (31) 優先権主張番号 60/995,200
 (32) 優先日 平成19年9月24日 (2007.9.24)
 (33) 優先権主張国 米国(US)

早期審査対象出願

(73) 特許権者 503260918
 アップル インコーポレイテッド
 アメリカ合衆国 95014 カリフォル
 ニア州 クパチーノ インフィニット ル
 ープ 1
 (74) 代理人 100076428
 弁理士 大塚 康徳
 (74) 代理人 100115071
 弁理士 大塚 康弘
 (74) 代理人 100112508
 弁理士 高柳 司郎
 (74) 代理人 100116894
 弁理士 木村 秀二
 (74) 代理人 100130409
 弁理士 下山 治

最終頁に続く

(54) 【発明の名称】電子デバイスに組み込まれた認証システム

(57) 【特許請求の範囲】

【請求項 1】

方法であって、タッチ感知式ディスプレイと前記タッチ感知式ディスプレイに統合されている指紋センサとを有する電子デバイスにおいて、前記タッチ感知式ディスプレイに統合されている前記指紋センサの位置の視覚的インジケーションを含むロック画面を前記タッチ感知式ディスプレイに表示することと、前記ロック画面に表示されたグラフィカル要素とのインタラクションを含むタッチ入力を前記タッチ感知式ディスプレイで検出することと、前記ロック画面に表示された前記グラフィカル要素との前記インタラクションを含む前記タッチ入力の間に、前記タッチ感知式ディスプレイに統合されている前記指紋センサを用いて前記入力が受け取られる際にユーザの識別情報を検出することと、前記タッチ感知式ディスプレイに統合されている前記指紋センサを用いて検出された前記識別情報に基づいて前記ユーザを認証することと、前記タッチ感知式ディスプレイに統合されている前記指紋センサで検出された前記識別情報に基づいて前記ユーザを認証することに応じて、前記タッチ感知式ディスプレイでの前記ロック画面の表示をロック解除済ユーザインターフェースの表示で置き換えることと、を有する方法。

【請求項 2】

10

20

前記指紋センサは、前記タッチ感知式ディスプレイの他の領域よりも高密度の容量センサを有する、請求項 1 に記載の方法。

【請求項 3】

前記指紋センサの位置の前記視覚的インジケーションを表示することは、前記ロック画面で前記指紋センサの輪郭を強調することを含む、請求項 1 に記載の方法。

【請求項 4】

前記指紋センサの前記輪郭は、前記ユーザが前記指紋センサへ適切な指紋を提供するのが困難であるとの判定に従って一時的に強調される、請求項 3 に記載の方法。

【請求項 5】

前記ロック画面に表示される前記グラフィカル要素は、前記指紋センサ上へ動かすための指の移動の方向を視覚的に示す、請求項 1 に記載の方法。

10

【請求項 6】

前記指紋センサは、前記タッチ感知式ディスプレイのディスプレystack の下にある、請求項 1 に記載の方法。

【請求項 7】

前記指紋センサは、前記タッチ感知式ディスプレイのディスプレystack の既存の構成要素を含む、請求項 1 に記載の方法。

【請求項 8】

前記指紋センサは、前記タッチ感知式ディスプレイの前記指紋センサの位置で静止した指の入力から前記識別情報を取得するように構成されている 2 次元指紋センサである、請求項 1 に記載の方法。

20

【請求項 9】

前記指紋センサは、容量センサと、光学センサと、ソナーセンサと、高周波センサと、脈拍検出センサと、熱センサとのうちの 1 つ以上のタイプの組み合わせを含む、請求項 1 に記載の方法。

【請求項 10】

前記指紋センサは、前記グラフィカル要素が前記タッチ感知式ディスプレイに表示される位置で前記タッチ感知式ディスプレイに統合されている、請求項 1 に記載の方法。

【請求項 11】

前記指紋センサは、前記タッチ感知式ディスプレイの他の領域と比較して異なるタイプの容量センサアレイを有する、請求項 1 に記載の方法。

30

【請求項 12】

前記ロック解除済ユーザインタフェースは、複数のアプリケーション起動アイコンを含む、請求項 1 に記載の方法。

【請求項 13】

電子デバイスであって、

タッチ感知式ディスプレイと、

前記タッチ感知式ディスプレイに統合されている指紋センサと、

1 つ以上のプロセッサと、

コンピュータ命令を備えるメモリであって、前記コンピュータ命令は、前記 1 つ以上のプロセッサによって実行された場合に、前記デバイスに、

40

前記タッチ感知式ディスプレイに統合されている前記指紋センサの位置の視覚的インジケーションを含むロック画面を前記タッチ感知式ディスプレイに表示することと、

前記ロック画面に表示されたグラフィカル要素とのインタラクションを含むタッチ入力を前記タッチ感知式ディスプレイで検出することと、

前記ロック画面に表示された前記グラフィカル要素との前記インタラクションを含む前記タッチ入力の間に、前記タッチ感知式ディスプレイに統合されている前記指紋センサを用いて前記入力が受け取られる際にユーザの識別情報を検出することと、

前記タッチ感知式ディスプレイに統合されている前記指紋センサを用いて検出された前記識別情報に基づいて前記ユーザを認証することと、

50

前記タッチ感知式ディスプレイに統合されている前記指紋センサで検出された前記識別情報に基づいて前記ユーザを認証することに応じて、前記タッチ感知式ディスプレイでの前記ロック画面の表示をロック解除済ユーザインタフェースの表示で置き換えることとを行わせる電子デバイス。

【請求項 1 4】

前記指紋センサは、前記タッチ感知式ディスプレイの他の領域よりも高密度の容量センサを有する、請求項 1 3 に記載のデバイス。

【請求項 1 5】

前記指紋センサの位置の前記視覚的インジケーションを表示することは、前記ロック画面で前記指紋センサの輪郭を強調することを含む、請求項 1 3 に記載のデバイス。

10

【請求項 1 6】

前記指紋センサの前記輪郭は、前記ユーザが前記指紋センサへ適切な指紋を提供するのが困難であるとの判定に従って一時的に強調される、請求項 1 5 に記載のデバイス。

【請求項 1 7】

前記ロック画面に表示される前記グラフィカル要素は、前記指紋センサ上へ動かすための指の移動の方向を視覚的に示す、請求項 1 3 に記載のデバイス。

【請求項 1 8】

前記指紋センサは、前記タッチ感知式ディスプレイのディスプレystackの下にある、請求項 1 3 に記載のデバイス。

20

【請求項 1 9】

前記指紋センサは、前記タッチ感知式ディスプレイのディスプレystackの既存の構成要素を含む、請求項 1 3 に記載のデバイス。

【請求項 2 0】

前記指紋センサは、前記タッチ感知式ディスプレイの前記指紋センサの位置で静止した指の入力から前記識別情報を取得するように構成されている 2 次元指紋センサである、請求項 1 3 に記載のデバイス。

【請求項 2 1】

前記指紋センサは、容量センサと、光学センサと、ソナーセンサと、高周波センサと、脈拍検出センサと、熱センサとのうちの 1 つ以上のタイプの組み合わせを含む、請求項 1 3 に記載のデバイス。

30

【請求項 2 2】

前記指紋センサは、前記グラフィカル要素が前記タッチ感知式ディスプレイに表示される位置で前記タッチ感知式ディスプレイに統合されている、請求項 1 3 に記載のデバイス。

【請求項 2 3】

前記指紋センサは、前記タッチ感知式ディスプレイの他の領域と比較して異なるタイプの容量センサアレイを有する、請求項 1 3 に記載のデバイス。

【請求項 2 4】

前記ロック解除済ユーザインタフェースは、複数のアプリケーション起動アイコンを含む、請求項 1 3 に記載のデバイス。

40

【請求項 2 5】

命令を備える非一時的でありコンピュータで読み取り可能な媒体であって、前記命令は、タッチ感知式ディスプレイと前記タッチ感知式ディスプレイに統合されている指紋センサとを有する電子デバイスによって実行された場合に、前記デバイスに、

前記タッチ感知式ディスプレイに統合されている前記指紋センサの位置の視覚的インジケーションを含むロック画面を前記タッチ感知式ディスプレイに表示することと、

前記ロック画面に表示されたグラフィカル要素とのインタラクションを含むタッチ入力を前記タッチ感知式ディスプレイで検出することと、

前記ロック画面に表示された前記グラフィカル要素との前記インタラクションを含む

50

前記タッチ入力の間に、前記タッチ感知式ディスプレイに統合されている前記指紋センサを用いて前記入力が受け取られる際にユーザの識別情報を検出することと、

前記タッチ感知式ディスプレイに統合されている前記指紋センサを用いて検出された前記識別情報に基づいて前記ユーザを認証することと、

前記タッチ感知式ディスプレイに統合されている前記指紋センサで検出された前記識別情報に基づいて前記ユーザを認証することに応じて、前記タッチ感知式ディスプレイでの前記ロック画面の表示をロック解除済ユーザインタフェースの表示で置き換えることと

を行わせる媒体。

【請求項 26】

10

前記指紋センサは、前記タッチ感知式ディスプレイの他の領域よりも高密度の容量センサを有する、請求項 25 に記載の媒体。

【請求項 27】

前記指紋センサの位置の前記視覚的インジケーションを表示することは、前記ロック画面で前記指紋センサの輪郭を強調することを含む、請求項 25 に記載の媒体。

【請求項 28】

前記指紋センサの前記輪郭は、前記ユーザが前記指紋センサへ適切な指紋を提供するのが困難であるとの判定に従って一時的に強調される、請求項 27 に記載の媒体。

【請求項 29】

20

前記ロック画面に表示される前記グラフィカル要素は、前記指紋センサ上へ動かすための指の移動の方向を視覚的に示す、請求項 25 に記載の媒体。

【請求項 30】

前記指紋センサは、前記タッチ感知式ディスプレイのディスプレystack の下にある、請求項 25 に記載の媒体。

【請求項 31】

前記指紋センサは、前記タッチ感知式ディスプレイのディスプレystack の既存の構成要素を含む、請求項 25 に記載の媒体。

【請求項 32】

30

前記指紋センサは、前記タッチ感知式ディスプレイの前記指紋センサの位置で静止した指の入力から前記識別情報を取得するように構成されている 2 次元指紋センサである、請求項 25 に記載の媒体。

【請求項 33】

前記指紋センサは、容量センサと、光学センサと、ソナーセンサと、高周波センサと、脈拍検出センサと、熱センサとのうちの 1 つ以上のタイプの組み合わせを含む、請求項 25 に記載の媒体。

【請求項 34】

前記指紋センサは、前記グラフィカル要素が前記タッチ感知式ディスプレイに表示される位置で前記タッチ感知式ディスプレイに統合されている、請求項 25 に記載の媒体。

【請求項 35】

40

前記指紋センサは、前記タッチ感知式ディスプレイの他の領域と比較して異なるタイプの容量センサアレイを有する、請求項 25 に記載の媒体。

【請求項 36】

前記ロック解除済ユーザインタフェースは、複数のアプリケーション起動アイコンを含む、請求項 25 に記載の媒体。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、内蔵認証システムを備えた電子デバイスに関する。

【背景技術】

【0002】

50

電子デバイス、特に携帯型電子デバイスは、個人情報を格納するために用いられる。例えば、ユーザは、ユーザが用いる連絡先、電子メール、カレンダー情報、文書、および、その他の情報を格納するために、携帯電話、PDA、スマートフォン、または、その他の電子デバイスを用いてよい。この情報は、必ずしも秘密にしなくてもよいが、ユーザは、情報の少なくとも一部を他人に利用できなくするよう望んでもよい。許可されていない人物がユーザの個人情報にアクセスし閲覧することを防ぐ方法の1つとして、デバイス機能を有効にする前、または、デバイスリソースにアクセスする前に、パスワードまたはパスコードの提供を電子デバイスのユーザに要求する方法が挙げられる。例えば、電子デバイスは、デバイスのホームスクリーン（例えば、スプリングボード）またはメニューを表示する前に、4つの数字または4つの文字のPINを入力するよう、ユーザに要求してよい。別の例として、ユーザの指紋を検出するためまたはユーザの網膜を走査するための付属デバイスをデバイスに接続することによって、ユーザが、デバイスへのアクセス権を受ける前に、承認された指紋または網膜を最初に示さなければいけないようにしてよい。10

【0003】

これらの方法は両方とも有効でありうるが、パスワードまたはパスコードに基づくアクセス制限は、パスワードまたはパスコードを知っている他のユーザがいない限りは、効果的である。パスワードまたはパスコードが知られると、制限メカニズムは、効果がなくなりうる。また、パスワードまたはパスコードを忘れて、許可ユーザがデバイスにアクセスできなくなる場合もある。さらに、ユーザに指紋を提供するまたは網膜スキャンを受けるよう要求することは、ユーザがデバイスにアクセスできるまでに求めるステップを増やすため、時間がかかり、ユーザにとって煩わしい場合がある。この方法は、パスワードまたはパスコードの入力よりも安全であるが、ハードウェア（例えば、必要なスキャナ、検出器、または、リーダ）のコストと時間がかかる。したがって、例えば、ユーザがデバイスをオンにする、ロック解除する、または、起動する時に、デバイスが迅速かつシームレスにユーザを認証するように、生体認証および他の認証メカニズムを実装した電子デバイスを提供することが望ましい。20

【発明の概要】

【0004】

電子デバイスのユーザを認証するための方法、電子デバイス、および、コンピュータ読み取り可能な媒体が提供されている。一部の実施形態において、電子デバイスは、ユーザをシームレスに認証しうる。電子デバイスは、ユーザから入力を受信してよく、その入力は、電子デバイスの入力メカニズムによって提供される。電子デバイスは、ユーザが、入力メカニズムの中またはその近傍に組み込まれた1または複数のセンサから入力を提供する時に、識別情報を検出してよい。電子デバイスは、検出した識別情報を、デバイスのライブラリに格納されている識別情報と比較することによって、ユーザを認証してよい。例えば、センサは、ユーザの皮膚の特長、または、ユーザの皮下の特長を検出するためのセンサを含んでよい。センサは、タッチスクリーン、ボタン（例えば、キーボードまたはマウスのボタン）、入力メカニズム近傍のデバイスの筐体（例えば、キーボードの近くのラップトップ筐体）、または、任意の他の適切な位置の少なくとも一ヵ所に組み込まれてよい。30

【0005】

一部の実施形態において、電子デバイスは、デバイスの検知素子に対して位置合わせするようユーザに指示することなく、ユーザが検知素子に対して位置合わせされていることを決定してよい。例えば、検知素子は、センサの検知領域が、電子デバイスを操作する際に予期されるユーザの位置を含むように配置されてよい。センサは、検知素子を用いて、ユーザの1または複数の生体属性（例えば、顔または眼の特長）を検出してよい。例えば、センサは、デバイスのディスプレイに隣接したカメラまたは光学センサを備えてよい。次いで、ユーザは、検出された生体属性を、電子デバイスに格納された、または、電子デバイスがアクセスできる生体属性のライブラリと比較することによって認証されてよい。

【0006】

50

40

50

40

一部の実施形態において、電子デバイスは、ユーザによって選択されたオプションの共通の属性に基づいて、ユーザを認証してもよい。電子デバイスは、ユーザによる選択のために、いくつかの選択可能なオプションを表示してよく、オプションのサブセット（一部）のユーザ選択を受信してよい。次いで、電子デバイスは、選択されたオプションの一部または全部に共通する1または複数の属性を特定してよい。属性は、例えば、サイズ、色、輪郭、網掛けパターン、形状、他のオプションとの配列、他のオプションに対する位置、オプションのソース、または、任意の他の適切な属性の内の少なくとも1つを含んでよい。次いで、電子デバイスは、特定された属性に基づいてユーザを認証してよい。例えば、ユーザが、特定のユーザに関連づけられた属性を共有する形状をすべて選択した場合、電子デバイスは、そのユーザを認証してよい。

10

【0007】

一部の実施形態において、電子デバイスは、デバイスが受信した入力のパターンに基づいて、ユーザを認証してもよい。電子デバイスは、ユーザによって提供される複数の入力を検出するセンサを備えてよい。例えば、センサは、ユーザによって提供された入力を受信する入力メカニズムを備えてよい。別の例として、センサは、電子デバイスの動き、または、電子デバイスとの接触を検出する加速度計またはジャイロスコープを備えてよい。電子デバイスは、検出した入力のパターンを特定し、特定したパターンを、メモリに格納されたパターンと比較して、ユーザを認証するよう動作してよい。パターンは、時間的パターン（例えば、連続する入力の間の遅延に関するパターン）、視覚的パターン（例えば、ユーザが選択したいくつのオプションの属性、または、ユーザが提供した入力に関するパターン）、または、これらの組み合わせを含みうる。ユーザを認証すると、電子デバイスは、制限された電子デバイスリソースへのアクセスをユーザに提供してよい。

20

【図面の簡単な説明】

【0008】

【図1】本発明の一実施形態による認証システムと共に使用するための電子デバイスの一例を示す概略図。

【図2】本発明の一実施形態に従って、電子デバイスのディスプレイスクリーンの一例を示す概略図。

【図3】本発明の一実施形態に従って、ユーザに認証を指示するためのディスプレイスクリーンの一例を示す図。

30

【図4】本発明の一実施形態に従って、ユーザがデバイスリソースにアクセスする前に、ユーザに認証を指示するためのディスプレイスクリーンの一例を示す概略図。

【図5A】本発明の実施形態に従って、ユーザ認証に応答して提供された異なるユーザに関連づけられたディスプレイスクリーンの例を示す概略図である。

【図5B】本発明の実施形態に従って、ユーザ認証に応答して提供された異なるユーザに関連づけられたディスプレイスクリーンの例を示す概略図である。

【図5C】本発明の実施形態に従って、ユーザ認証に応答して提供された異なるユーザに関連づけられたディスプレイスクリーンの例を示す概略図である。

【図6】本発明の一実施形態に従って、ユーザの指紋を検出するための電子デバイスのディスプレイの一例を示す概略図。

40

【図7】本発明の一実施形態に従って、ユーザの指紋を検出するための電子デバイスの別の例を示す概略図。

【図8A】本発明の一実施形態に従って、ユーザの手紋を検出するための電子デバイスの一例を示す概略図。

【図8B】本発明の一実施形態に従って、ユーザの手紋を検出するための電子デバイスの一例を示す概略図。

【図9】本発明の一実施形態に従って、ユーザの手紋を検出するための電子デバイスの一例を示す概略図。

【図10】本発明の一実施形態に従って、ユーザの皮膚の下の特徴を検出するセンサを有するデバイスの一例を示す概略図。

50

【図11】本発明の一実施形態に従って、ユーザの顔の特徴を検出するためのセンサを有する電子デバイスの一例を示す概略図。

【図12】本発明の一実施形態に従って、ユーザの眼の特徴を検出するためのセンサを有する電子デバイスの一例を示す概略図。

【図13】本発明の一実施形態に従って、視覚的パターンを提供するためのディスプレイの一例を示す概略図。

【図14】本発明の一実施形態に従って、視覚的パターンを提供するためのディスプレイの一例を示す概略図。

【図15】本発明の一実施形態に従って、ユーザを認証するための方法の一例を示すフローチャート。

10

【発明を実施するための形態】

【0009】

電子デバイスのリソースへのアクセスを制限するための認証システムを有する電子デバイスが提供されている。例えば、デバイスに格納されたまたはデバイスから利用できるファイルまたはデータへのアクセスなど、任意の適切な電子デバイスリソースへのアクセスが制限されてよい。別の例として、特定のアプリケーション（例えば、特定のユーザが購入したアプリケーション、または、管理者タスクまたは管理者特権と関連づけられたアプリケーション）へのアクセスが制限されてもよい。さらに別の例として、ユーザが認証されるまで、個人設定（例えば、表示されるオプション、背景画像、または、アプリケーションに用いるアイコン）へのアクセスが制限されてもよい。

20

【0010】

任意の適切な認証システムが実装されてよい。一部の実施形態において、認証システムは、ユーザの生体特徴または属性を検出するためのシステムを備えてよい。例えば、電子デバイスは、指紋、手紋（hand print）、掌紋、指関節紋（knuckle print）、血管パターン、または、任意のその他の適切なユーザの皮膚の一部もしくは皮下の一部など、ユーザの皮膚の特徴または皮下の特徴に基づいて、ユーザを検出および認証するシステムを備えてよい。別の例として、電子デバイスは、ユーザの眼または顔の特徴もしくはユーザの眼（眼球）の動きに基づいて、ユーザを検出および認証するシステムを備えてもよい。さらに別の例として、電子デバイスは、ユーザの外耳道の特徴、ユーザに関連した匂い、ユーザのDNA、または、ユーザに関連した任意のその他の適切な生体属性もしくは情報を検出するシステムを備えてもよい。

30

【0011】

一部の実施形態において、認証システムは、ユーザによって提供される視覚的または時間的な入力パターンに基づいてユーザを特定するシステムを備えてよい。例えば、電子デバイスは、視覚的なパターンを形成するいくつかの選択可能なオプションまたは図形を表示してよい。ユーザは、認証のために、表示されたオプションから任意の適切な所定のサブセット（一部）を選択してよい。例えば、ユーザは、共通する所定の属性（例えば、サイズ、色、形状、または、輪郭）を有する1または複数のオプションを選択してよい。別の例として、ユーザは、ディスプレイの所定の領域に配置された1または複数のオプションを（例えば、選択するオプションの属性とは無関係に）選択してもよい。ユーザは、同時に、逐次的に、または、これらの組み合わせとして、オプションを選択してよい。

40

【0012】

別の例として、ユーザは、特定のペースまたは特定のパターンで、一連の入力を提供してもよい。例えば、ユーザは、特定の遅延（例えば、2つの選択の間の中斷）を伴って、オプションを選択してよい。あるいは、ユーザは、所定の時間的パターンに従って、デバイスのセンサ（例えば、加速度計またはジャイロスコープ）で検出される入力を提供してもよい。デバイスは、デバイスまたはデバイスに隣接した領域をタッピングしたり特定の方法でデバイスを動かしたりすることによって引き起こされる振動から入力を検出するなど、入力を検出するための任意の適切な方法で検出してよい。

【0013】

50

電子デバイスは、例えば、生体認証システムおよびパターンに基づく認証システム、いくつかの生体認証システム、または、いくつかのパターンに基づくシステムなど、任意の適切な組み合わせの認証システムを提供してよい。一部の実施形態において、異なるリソースに異なる認証システムを関連づけてよく、その結果、ユーザは、特定の制限されたリソース（例えば、プライベートまたは個人情報）に最終的にアクセスする前に、いくつかのシステムに認証情報を提供しうる。電子デバイスは、どの認証システムを組み合わせるかを選択するために任意の適切な方法を用いてよい。例えば、ユーザが、いくつかの認証システムを特定のリソースと関連づけてもよいし、あるいは、電子デバイスが、自動的に（例えば、デフォルトとして）特定の認証システムを特定のリソースに割り当ててもよい。

10

【0014】

図1は、本発明の一実施形態による認証システムと共に使用するための電子デバイスの一例を示す概略図である。電子デバイス100は、プロセッサ102、ストレージ104、メモリ106、通信回路108、入力／出力回路110、認証システム112、および、電源114を備えてよい。一部の実施形態において、電子デバイス100の構成要素の内の1または複数を組み合わせたり省略したりしてもよい（例えば、ストレージ104およびメモリ106を組み合わせる）。一部の実施形態において、電子デバイス100は、図1に示した構成要素に一体化されていないまたは備えられていない他の構成要素（例えば、ディスプレイ、バス、または、入力メカニズム）を備えてもよいし、図1に示した構成要素を複数備えてもよい。簡単のために、図1には各構成要素について1つだけ図示している。

20

【0015】

プロセッサ102は、電子デバイス100の動作および実行を制御する任意の処理回路を備えてよい。例えば、プロセッサ100は、オペレーティングシステムアプリケーション、ファームウェアアプリケーション、メディア再生アプリケーション、メディア編集アプリケーション、または、任意の他のアプリケーションを実行するために用いられてよい。一部の実施形態において、プロセッサは、ディスプレイを駆動し、ユーザインターフェースから受信した入力を処理してよい。

【0016】

ストレージ104は、例えば、ハードドライブ、ソリッドステートドライブ、フラッシュメモリ、ROMのような永久メモリ、任意の他の適切なタイプの記憶素子、または、それらの任意の組み合わせなど、1または複数の記憶媒体を含んでよい。ストレージ104は、例えば、メディアデータ（例えば、音楽ファイルおよびビデオファイル）、（例えば、デバイス100に機能を実装するための）アプリケーションデータ、ファームウェア、ユーザプリファレンス情報データ（例えば、メディア再生設定）、認証情報（例えば、許可ユーザに関連づけられたデータのライブラリ）、ライフスタイル情報データ（例えば、食べ物の好み）、エクササイズ情報データ（例えば、エクササイズ監視装置で取得した情報）、取引情報データ（例えば、クレジットカード情報などの情報）、無線接続情報データ（例えば、電子デバイス100が無線接続を確立することを可能にしうる情報）、定期購読情報データ（例えば、ユーザが加入するポッドキャスト、テレビ番組、または、その他のメディアを把握する情報）、連絡先データ（例えば、電話番号および電子メールアドレス）、カレンダー情報データ、および、任意の他の適切なデータまたはこれらの任意の組み合わせを格納しうる。

30

【0017】

メモリ106は、キャッシュメモリ、RAMなどの半永久メモリ、および／または、データを一時的に格納するために用いられる1または複数の異なるタイプのメモリを含みうる。一部の実施形態において、メモリ106は、電子デバイスアプリケーションを動作させるために用いるデータ、または、ストレージ104に格納されうる任意の他のタイプのデータを格納するために利用可能である。一部の実施形態において、メモリ106およびストレージ104は、単一の記憶媒体として組み合わされてもよい。

40

50

【0018】

通信回路108は、デバイス100が、任意の適切な通信プロトコルを用いて、1または複数のサーバまたはその他のデバイスと通信することを可能にすることができる。電子デバイス100は、異なる通信ネットワークを用いていくつかの通信動作を同時に実行するため、複数の通信回路108を備えてもよいが、図が複雑になることを避けるために図1には1つしか図示していない。例えば、通信回路108は、Wi-Fi(例えば、802.11プロトコル)、イーサーネット(登録商標)、Bluetooth(登録商標)(Bluetooth SIG社の商標)、無線周波数システム、セルラーネットワーク(例えば、GSM(登録商標)、AMPS、GPRS、CDMA、EV-DO、EDGE、3GSM、DECT、IS-136/TDMA、iDEN、LTE、または、任意の他の適切なセルラーネットワークまたはプロトコル)、赤外線、TCP/IP(例えば、TCP/IP層の各層で用いられるプロトコルのいずれか)、HTTP、BitTorrent、FTP、RTP、RTSP、SSH、ボイスオーバーIP(VoIP)、任意の他の通信プロトコル、または、それらの任意の組み合わせをサポートしてよい。
10

【0019】

入力/出力回路110は、アナログ信号およびその他の信号をデジタルデータに変換(および、必要であればエンコード/デコード)するよう動作してよい。一部の実施形態において、入力/出力回路は、デジタルデータを任意の他のタイプの信号に変換してもよく、その逆を行うこともできる。例えば、入力/出力回路110は、(例えば、マルチタッチスクリーンからの)物理接触入力、(例えば、マウスまたはセンサからの)物理的な動き、(例えば、マイクロホンからの)アナログ音声信号、または、任意の他の入力を受信して変換してよい。デジタルデータは、プロセッサ102、ストレージ104、メモリ106、または、電子デバイス100の任意の他の構成要素に供給し、また、そこから受信することができる。入力/出力回路110は、電子デバイス100の単一の構成要素として、図1に示されているが、複数の入力/出力回路を電子デバイス100に備えてもよい。
20

【0020】

電子デバイス100は、入力/出力回路110にユーザが入力を提供することを可能にする任意の適切なメカニズムまたは構成要素を備えてよい。例えば、電子デバイス100は、例えば、ボタン、キーパッド、ダイヤル、クリックホイール、または、タッチスクリーンなど、任意の適切な入力メカニズムを備えてよい。一部の実施形態において、電子デバイス100は、静電容量式検知メカニズムまたはマルチタッチ静電容量式検知メカニズムを備えてよい。いくつかの検知メカニズムは、2004年7月10日に出願された同時係属している本願出願人の米国特許出願第10/902,964号「*Gestures for Touch Sensitive Input Device*」、および、2005年1月18日に出願された米国特許出願第11/028,590号「*Mode-Based Graphical User Interfaces for Touch Sensitive Input Device*」に記載されており、両方とも本明細書に全体が組み込まれる。
30

【0021】

一部の実施形態において、電子デバイス100は、例えば、1または複数のオーディオ出力などの出力デバイスに関連する専用の出力回路を備えてもよい。オーディオ出力は、電子デバイス100に内蔵された1または複数のスピーカ(例えば、モノラルスピーカまたはステレオスピーカ)、または、電子デバイス100と遠隔接続されたオーディオ構成要素(例えば、有線または無線で通信デバイスと接続できるヘッドセット、ヘッドホン、または、イヤホン)を含んでよい。

【0022】

一部の実施形態において、I/O回路110は、ユーザに可視表示を提供するディスプレイ回路(例えば、スクリーンまたは投影システム)を備えてよい。例えば、ディスプレイ回路は、電子デバイス100に組み込まれたスクリーン(例えば、LCDスクリーン)
50

を備えてよい。別の例として、ディスプレイ回路は、移動可能なディスプレイ、または、電子デバイス 100 から離れた面にコンテンツの表示を提供するための投影システム（例えば、ビデオプロジェクタ）を備えててもよい。一部の実施形態において、ディスプレイ回路は、デジタルメディアデータをアナログ信号に変換するためにコーダ / デコーダ（コーデック）を備えてよい。例えば、ディスプレイ回路（または、電子デバイス 100 内のその他の適切な回路）は、ビデオコーデック、オーディオコーデック、または、任意のその他の適切なタイプのコーデックを備えてよい。

【 0 0 2 3 】

また、ディスプレイ回路は、ディスプレイドライバ回路、ディスプレイドライバを駆動するための回路、または、その両方を含みうる。ディスプレイ回路は、プロセッサ 102 の指示を受けて、コンテンツ（例えば、メディア再生情報、電子デバイスに実装されたアプリケーションのアプリケーション画面、継続中の通信動作に関する情報、入ってくる通信要求に関する情報、または、デバイス操作画面）を表示するよう動作してよい。10

【 0 0 2 4 】

認証システム 112 は、デバイス 100 のユーザを特定する入力を受信または検出する任意の適切なシステムまたはセンサを備えてよい。例えば、認証システム 112 は、皮膚のパターンを検知するメカニズム、ユーザの顔のパターン、眼の特徴（例えば、網膜）、または、静脈パターンに基づいてユーザを特定するための光学システム、または、任意の他のユーザ特有の生体特徴または属性を検出するための任意の他のセンサを備えてよい。20
別の例として、認証システム 112 は、ユーザを特定する秘密または機密の入力（例えば、デバイス上でのジェスチャ、または、ディスプレイ上のオブジェクトまたは色を特定のパターンで触ること、など）を受信するよう動作してもよい。さらに別の例として、認証システム 112 は、ユーザによるデバイスの特定の動きまたは振動を検出するよう動作してもよい。認証システム 112 は、電子デバイス 112 の任意の他の構成要素（例えば、ディスプレイまたはカメラ）に一体化または内蔵されてもよく、また、電子デバイスの様々なセンサ（例えば、加速度計または近接センサ）によって検出されたイベントを利用してもよい。一部の実施形態において、複数種類の認証システムが、電子デバイスに組み込まれたり実装されたりしてよい。

【 0 0 2 5 】

一部の実施形態において、電子デバイス 100 は、制御プロセッサ 102、ストレージ 104、メモリ 106、通信回路 108、入力 / 出力回路 110、認証システム 112、および、電子デバイスに備えられた任意の他の構成要素とのデータのやり取り、または、それら構成要素の間でのデータのやり取りのためのデータ転送バスを提供するバスを備えてよい。30

【 0 0 2 6 】

メモリまたはストレージに格納されたデータまたは情報への不正アクセスを防ぐために、電子デバイスは、ユーザを特定し、要求されたリソースへのアクセスを許可するよう、認証システムに指示してよい。電子デバイスは、任意の電子デバイスリソースへのアクセスを提供する前に、認証を要求してよい。一部の実施形態において、電子デバイスは、異なるアプリケーション、または、異なるアプリケーションに関連づけられた異なるデータまたはファイルへのアクセスを提供する前に、異なるレベルの認証を要求してもよい。例えば、電子デバイスは、アプリケーションまたはデータへのアクセスを提供する前に、いくつかの認証システムを満たすようにユーザに要求してよい（例えば、パスコードなどの第 1 または初期認証に加えて、生体認証などを用いる第 2 認証を、デバイスのロック解除に利用する）。

40

【 0 0 2 7 】

図 2 は、本発明の一実施形態に従って、電子デバイスのディスプレイクリーンの一例を示す概略図である。ディスプレイクリーン 200 は、ユーザが電子デバイスをロック解除したことに応答して表示されてよい。ディスプレイクリーン 200 は、様々なデバイス機能にアクセスするための選択可能なオプション 210 を備えてよい。例えば、各オ50

プション 210 は、電子デバイスで利用可能な異なるアプリケーションと関連づけられてよい。別の例として、各オプションは、ユーザが利用可能な特定のデータまたはファイルと関連づけられてもよい。電子デバイスは、ディスプレイ 200 にアクセスするための認証を要求してもよいし要求しなくてもよい。例えば、ディスプレイ 200 は、ユーザが利用可能な基本的またはデフォルトのアプリケーションを含んでよい。別の例として、ディスプレイ 200 は、すべてのユーザが利用可能なデフォルトの機能を含んでもよい。

【0028】

一部の実施形態において、1 または複数のアプリケーションが、1 または複数のユーザの個人的なデータまたはリソースへのアクセスを提供したり利用したりしてよい。例えば、それぞれ、電話およびメールのアプリケーションと関連づけられたオプション 212 および 214 は、電子デバイスのすべてのユーザには関連づけられていない個人のアカウントまたは連絡先を含んでよい。かかるアプリケーションへのアクセス、または、かかるアプリケーションを介して利用可能な個人的または秘密の機能またはリソースへのアクセスを提供する前に、電子デバイスは、ユーザに認証を要求してよい。一部の実施形態において、アプリケーションのデフォルトの機能は、認証なしに利用可能であってもよい（例えば、すべてのユーザが電話をかけることができるが、連絡先リストにはアクセスできない）。

10

【0029】

図 3 は、本発明の一実施形態に従って、ユーザに認証を行わせるディスプレイスクリーンの一例を示す図である。ディスプレイスクリーン 300 は、認証プロトコルによって制限されたリソース（例えば、情報またはアプリケーション）にアクセスするための命令をユーザから受信したことに応答して表示されてよい。ディスプレイスクリーン 300 は、選択されたリソースに関連づけられた情報 310 を含んでよい。認証前には、無許可ユーザがリソースを閲覧することを防ぐために、情報 310 は、不鮮明になっていてよいし、ビューから隠されてもよい（例えば、特定のフィールドのエントリが取得不可能になってよい）。一部の実施形態において、ディスプレイスクリーン 300 は、ユーザが認証されるまで情報を含まなくてもよい。

20

【0030】

ディスプレイスクリーン 300 は、要求されたリソースにアクセスする前にユーザが認証を行うよう指示する通知 320 を備えてよい。通知 320 は、ポップアップ、オーバーレイ、新たなディスプレイスクリーン、または、ユーザに指示を提供するための任意の他の適切なタイプのディスプレイを含みうる。通知 320 は、例えば、ユーザが認証を行う方法など、任意の適切な指示を含んでよい（例えば、使用すべき特定の認証システムを指定する指示など）。例えば、通知 320 は、指紋の提供、または、所定の視覚的または時間的パターンに適合する入力の提供をユーザに指示してよい。ユーザが適切に認証されると、電子デバイスは、ユーザが識別できるように情報 310 を表示し、選択されたリソースに関連づけられた選択可能オプションまたはその他の機能を有効にしてよい。

30

【0031】

一部の実施形態において、ユーザは、電子デバイスをロック解除する前に（例えば、デバイスの任意のリソースにアクセスする前に）、認証を要求されてよい。図 4 は、本発明の一実施形態に従って、ユーザがデバイスリソースにアクセスする前に、ユーザに認証を指示するためのディスプレイスクリーンの一例を示す概略図である。ディスプレイスクリーン 400 は、ディスプレイのロックを解除するためのオプション 410 を備えてよい。例えば、オプション 410 は、スクリーンの一部を横切って（横断して）ドラッグされるスライダを備えてよい。別の例として、オプション 410 は、ユーザが選択すべきオプションまたは一連のオプション（例えば、いくつかのキーを同時または連続的に押す、または、ディスプレイスクリーン 400 のいくつかの領域に触れる、など）を備えてもよい。

40

【0032】

ディスプレイスクリーン 400 は、デバイスリソースにアクセスする前に、認証を受けるようユーザに指示する通知 420 を含んでよい（例えば、情報およびアプリケーション

50

を起動するホームスクリーン）。通知 420 は、例えば、ポップアップ、オーバーレイ、新たなディスプレイスクリーン、または、ユーザに指示を提供するための任意の他の適切なタイプのディスプレイなど、任意の適切なタイプの通知を含みうる。電子デバイスは、例えば、ユーザがデバイスのスイッチを入れた時（例えば、その後ディスプレイスクリーン 400 を見る時）、第 1 の認証なしにユーザがデバイスリソースへのアクセスを試みたことに応じて（例えば、エラーメッセージとして）、ユーザによるヘルプの要求に応じて、または、任意のその他の適切な時点など、任意の適切な時に通知 420 を表示してよい。通知 420 は、例えば、ユーザが認証を行う方法、許可ユーザのリスト、または、任意のその他の適切な情報など、任意の適切な指示を含んでよい。

【0033】

ユーザが適切に認証されると、電子デバイスは、認証されたユーザに関連づけられたオプション（例えば、特定のユーザが購入したアプリケーションのオプション）を表示してよい。一部の実施形態において、電子デバイスは、以前には利用できなかったリソースまたはコンテンツ（例えば、電話または電子メールアプリケーションの連絡先リストまたは以前のメッセージ、など）へのアクセスを提供してよい。図 5A ないし C は、本発明の実施形態に従って、ユーザ認証に応答して提供された異なるユーザに関連づけられたディスプレイスクリーンの例を示す概略図である。ディスプレイスクリーン 500A は、いくつかのオプション 510A を備えてよい。表示されたオプションは、電子デバイスのデフォルトまたは基本的なディスプレイに共通するいくつかのオプションを含んでよい（例えば、ディスプレイスクリーン 500A は、図 2 のディスプレイスクリーン 200 とオプションを共有している）。ディスプレイスクリーン 500A は、特定の認証済みユーザにだけ利用可能な追加のアプリケーションまたはリソースのためのいくつかのオプション 512A を備えてよい。例えば、ディスプレイスクリーン 510A は、ゲーム、システム、および、メディアアプリケーションのための追加のオプション 512A を備えてよい。

【0034】

ディスプレイスクリーン 500B は、ユーザに利用可能なリソースまたはアプリケーションのためのオプション 510B を備えてよい。一部の実施形態において、オプション 510B は、デフォルトスクリーンのオプションと完全に異なるものであってよい（例えば、ディスプレイスクリーン 500B は、図 2 のディスプレイスクリーン 200 とオプションを共有しない）。ディスプレイスクリーン 500B は、オプション 510B に関連づけられたアプリケーションまたはリソースを特定するラベルを含まないよう、さらにカスタマイズされてよい。

【0035】

ディスプレイスクリーン 500C は、ユーザに利用可能なリソースまたはアプリケーションのためのオプション 510C を備えてよい。一部の実施形態において、他のディスプレイスクリーンと同じリソースのためのオプション 510C が、異なるアピアランス（例えば、異なるアイコン）を有してもよい。例えば、図 5C において、メール、時計、写真、Y o u T u b e（登録商標）、および、電卓アプリケーションのために表示されているオプションは、図 5A のディスプレイスクリーン 500A に表示されるオプションと異なっていてよい。ディスプレイスクリーン 500C は、カスタムすなわち個人用の背景 512C（例えば、異なる背景画像）を、さらに備えてよい。一部の実施形態において、ディスプレイスクリーン 500C は、（例えば、ドック 512B に配置されるオプション 510B と異なり）、いくつかのオプション 510C を固定位置に維持するためのドックまたはその他の機能を備えなくてもよい。

【0036】

一部の実施形態において、電子デバイスは、認証済みユーザのアイデンティティに基づいて、異なる範囲の電子デバイスリソースへのアクセスを提供してよい。例えば、電子デバイスが複数のユーザによって利用されている場合（例えば、同一家族の両親と子供たち）、ユーザは、リソースのすべてではなく一部を共有してよい（例えば、すべてのユーザが家族の連絡先リストにアクセスできるが、他の家族の電子メールにはアクセスできない

10

20

30

40

50

)。別の例として、電子デバイスのユーザは、ユーザのグループまたは階層に体系化されてもよい。いくつかのリソースが、特定のユーザに関連づけられる代わりにまたはそれに加えて、ユーザのグループまたは階層に関連づけられてよい。特定のユーザがグループの一員として認証および特定されると、電子デバイスは、そのグループに関連づけられたりソース（例えば、共通または供用の連絡先、供用の通信、または、供用の文書）、および、特定のユーザに関連づけられたリソース（例えば、個人的な連絡先、電子メールアカウント、および、通話リスト）へのアクセスを、そのユーザに提供してよい。

【0037】

電子デバイスは、特定のリソースを1または複数の認証システムと関連づけてよい。例えば、ユーザは、リソースを特定し、保護またはセキュリティの命令を（例えば、適切なオプションを選択することによって）提供してよい。ユーザは、さらに、リソースへのアクセスを提供する前に、満たすべき1または複数の認証システムを選択してよい。リソースが供用ではない（例えば、すべてのユーザに利用可能なままであるデフォルトのアプリケーションまたはファイルではない）場合、または、リソースがユーザによって作成または購入された場合、電子デバイスは、選択されたリソースを1または複数の選択された認証システムと関連づけてよい。あるいは、ユーザが十分な特権を有する（例えば、管理者である）場合、任意のリソースが、1または複数の選択された認証システムを用いて保護されてもよい。

【0038】

電子デバイスは、ユーザが電子デバイスをロック解除または操作するたびに、ユーザに認証を要求しなくてもよい。一部の実施形態において、電子デバイスは、ユーザが認証された状態を特定の期間だけ維持してよい。例えば、一旦認証が済むと、電子デバイスは、ユーザが認証された時間から10時間、制限されたリソースにユーザがアクセスすることを許容してよい。別の例として、電子デバイスは、ユーザの最後の命令を受信した後またはスタンバイモードに入った後、特定の期間だけユーザの認証を保持（例えば、入力後30分間認証を保持）してもよい。電子デバイスが認証情報を保持する期間の長さは、デバイスまたはユーザによって設定されてよく、認証情報によって保護される特定のタイプまたはリソースに基づいてよい（例えば、ユーザの個人的な連絡先よりも、特定のユーザが購入したゲームへのアクセスについては認証期間が長くてよい）。ユーザがデバイスを操作するたびに電子デバイスが認証を要求しなくともよいため、電力消費を節約することができる。

【0039】

電子デバイスは、デバイスリソースへの不正アクセスを防ぐために任意の適切なタイプの認証システムを用いてよい。一部の実施形態において、電子デバイスは、ユーザ特有の皮膚のパターンに基づいた認証システムを備えてよい。例えば、電子デバイスは、ユーザの指紋、手紋、掌紋、指關節紋、または、ユーザに特有な任意の他の適切な紋理または皮膚の特徴を検出する認証システムを備えてよい。認証システムは、ユーザに特有な皮膚のパターンまたは特徴を検出するセンサを備えてよい。

【0040】

センサは、ユーザの皮膚に特有な特徴またはパターンを検出するための任意の適切なタイプのセンサを含んでよい。例えば、センサは、ユーザの皮膚の特徴を検出する光学スキヤナを含みうる。光学センサは、電荷結合素子、または、センサ（例えば、電荷結合素子）によって受光した光を記録する任意の他の適切な受光素子（例えば、ダイオード）のアレイを備えてよい。例えば、電荷結合素子が受光素子アレイを備える場合、光学センサは、アレイの各受光素子について、特定の受光素子が受光した光を表すピクセルを記録するよう動作してよい。各ピクセルの値は、ピクセルに関連づけられたユーザの皮膚の特定の部分（例えば、隆線または谷線）のセンサからの距離を反映しうる。記録されたピクセルは、電子デバイスが許可ユーザに関連づけられた画像のライブラリと比較できる画像（例えば、ユーザの皮膚の特定の部分の画像など）を形成しうる。

【0041】

10

20

30

40

50

別の例として、センサは、ユーザの皮膚の特徴を検出する容量センサを含んでもよい。容量センサは、セルのアレイを含む1または複数のチップを備えてよく、各セルは、絶縁層によって隔てられた少なくとも2つの導体板を備えてよい。センサは、チップの各セルの少なくとも2つの導体板の間の電圧を変化させる反転増幅器に接続されてよい。ユーザの指がセルアレイ上に置かれると、センサは、各セルの容量値の違い（例えば、谷線の下のセルは隆線の下のセルよりも低い容量値を有する）に基づいて、谷線（例えば、指紋の谷線）の置かれたセルと隆線（例えば、指紋の隆線）の置かれたセルを区別するよう動作しうる。チップの各セルで検出された容量値を用いて、センサは、電子デバイスが利用できる画像または表現のライブラリと比較可能な画像または表現を、センサに置かれた皮膚について生成しうる。

10

【0042】

認証システムは、例えば、画像（例えば、印刷した画像）または3次元構造（例えば、ポリマ铸造物）を認証システムのセンサに近接させることによって、無許可ユーザが許可ユーザの皮膚パターンをまねることを防止する任意の適切な対応策を備えてよい。例えば、認証システムは、光学および容量センサの組み合わせ、ソナーまたは高周波センサ、ユーザの脈拍を検出するセンサ、センサに触れた物体の温度を決定する熱センサ（例えば、温度が人間の皮膚温度の予測の範囲内にあるか否かを判定するため）、または、任意のその他の適切な対応策を備えてよい。

【0043】

センサは、任意の適切な方法を用いて、ユーザの皮膚の特徴を検出するよう動作しうる。一部の実施形態において、センサは、ユーザの皮膚がセンサ上で移動された時に、ユーザの皮膚の特徴を検出するよう動作してよい。例えば、センサは、ユーザの指がセンサ上でスライドまたは回転した時にユーザの指の特徴を検出する一次元センサすなわち固定センサ（stagnant sensor）（例えば、一列の検知素子）を備えてよい。センサは、ユーザの皮膚の特徴の正確な表現を提供するために、ユーザの皮膚を動かすべき方向を有してよい。例えば、センサは、指の軸に沿ってまたは指の軸に直交に指先を動かすよう、ユーザに要求してよい。

20

【0044】

一部の実施形態において、センサは、皮膚がセンサ上で動かないよう保持された時に、ユーザの皮膚の特徴を検出するよう動作してもよい。例えば、センサは、指がセンサの上で静止している時にユーザの指の特徴を検出する2次元センサすなわち移動センサを備えてよい。センサは、静止したユーザの指の下で規則的なペースまたは速度で動くよう動作してもよいし、（例えば、ユーザの指がセンサ上で動く状態で）ある時点のユーザの指の瞬間的または略瞬間的な二次元表現を検出するよう動作してもよい。二次元センサは、一次元センサと違って、ユーザが規則的または一様なペースでセンサ上で皮膚を移動されることには依存しないので、二次元センサを用いることにより、ユーザの皮膚特徴のより正確な表現を提供できる。

30

【0045】

センサは、電子デバイス内の任意の適切な位置に配置されてよい。一部の実施形態において、センサは、ユーザが電子デバイスを操作する時または操作し始める時に、ユーザの皮膚の適切な部分を検出するよう動作できるように配置されてよい。センサの位置は、検出すべきユーザの皮膚の部分（例えば、指、手、または、掌）によって異なってよい。図6は、本発明の一実施形態に従って、ユーザの指紋を検出するための電子デバイスのディスプレイの一例を示す概略図である。ディスプレイ600は、電子デバイスのロックを解除するようユーザに指示するスクリーン602を備えてよい。例えば、スクリーン602は、ブロック610に指を置いてトラック612に沿って指をドラッグすることによって、トラック612に沿ってブロック610をスライドさせて電子デバイスのロックを解除するよう、ユーザに指示する矢印を有するブロック610を備えてよい。

40

【0046】

ロック解除処理中にユーザを認証するために、ディスプレイ600は、トラック612

50

に沿ってディスプレイ内にセンサ620を備えてよい。例えば、センサ620は、ディスプレイスタック（例えば、容量検知素子、光源、および、ディスプレイ面を備えうるディスプレイスタック）内に組み込まれてよい。別の例として、センサ620は、ディスプレイスタックの下に配置されてもよい。さらに別の例として、センサ620は、ディスプレイスタックの既存の構成要素を含んでもよい（例えば、タッチスクリーンディスプレイのディスプレイスタックは、容量センサを備えうる）。かかる例において、認証システムは、ユーザの皮膚の隆線と谷線を区別するのに十分な解像度を有する（例えば、タッチスクリーンディスプレイの）ディスプレイスタックの容量検知素子の検出出力を用いてよい。一部の実施形態において、ディスプレイスタックの容量検知素子は、ディスプレイの特定の部分を用いた認証を可能にするために、いくつかのタイプまたは密度の容量検知素子を備えてよい（例えば、トラック612の少なくとも一部に沿ったディスプレイスタックには、認証のために非常に精細な検知素子を用いて、ディスプレイ600の残りの領域にはあまり精細でない検知素子を用いる）。

【0047】

一部の実施形態において、センサ620は、ディスプレイ600内で見えないように、電子デバイスに埋め込まれてよい。例えば、センサ620は、ユーザが指紋スキャナを見ることができないように、ディスプレイ600上に組み立てられ、印刷され、または、直接エッティング（例えば、ガラス上にエッティング）されてよい。ユーザがセンサ620に適切な指紋を提供するのが困難な場合、ディスプレイ600は、認証の際にユーザを支援するために、センサ620の輪郭を強調してよい（例えば、センサ620の上に位置するアイコン上に指を置くよう指示するアイコンを表示する、など）。

【0048】

図7は、本発明の一実施形態に従って、ユーザの指紋を検出するための電子デバイスの別の例を示す概略図である。電子デバイス700は、ユーザが電子デバイス700に入力を提供するために作動させうる入力メカニズム710および712を備えてよい。例えば、入力メカニズム710は、キーボードを含んでよく、入力メカニズム712は、タッチパッドまたはトラックパッドを含んでよい。ただし、電子デバイス700と遠隔接続された入力メカニズム（例えば、有線または無線マウス）など、任意の他の入力メカニズムが、電子デバイス700で用いられてもよいことを理解されたい。

【0049】

リソースへの安全なアクセスを提供するために、電子デバイス700は、ユーザを特定するためにユーザの指紋の特徴を検出する少なくとも1つのセンサ720を備えてよい。シームレスなユーザ体験を提供するために、センサ720は、入力メカニズム710および712の少なくとも一方の中または下に組み込まれてよい。一部の実施形態において、入力メカニズム710は、ユーザが電子デバイス700に入力を提供するために押下しうる複数の別個のキーを備えうるため、1または複数のキーに内蔵されたセンサ720を備えてよい。例えば、光学または容量センサは、ユーザが指をキーに置いた（例えば、ユーザの人差し指を「F」または「J」キーに置いた）時に、センサがユーザを認証するためにユーザの指先の特徴を検出できるように、キーの上面に配置されてよい。ユーザの指がキーの上に置かれている間にユーザを認証するために、二次元すなわち移動センサが、用いられ得る。

【0050】

センサ720は、電子デバイスにおいてユーザが押下しうる任意のボタンまたはその他の物理的入力の中、近傍、または、裏側に配置されてもよい。例えば、センサ720は、携帯型メディアプレーヤまたは携帯電話のホームボタン（例えば、図8Bのボタン812）の背後に配置されてよい。センサ720は、外部のカバーまたは表面（例えば、ガラスまたはプラスチック表面）と、スイッチまたは電子回路に作用する機械的構成要素との間に配置されてよい。例えば、指紋検知メカニズムが、透明な表面の下に組み込まれてよく、そうすれば、検知メカニズムは、その表面を介して、ユーザの指紋の隆線および谷線を検出することができる。一部の実施形態においては、透明な表面を追加しなくてもよい（

例えば、検知メカニズムが、ユーザが指を置くことのできる表面を備える場合)。

【0051】

一部の実施形態において、入力メカニズム712は、パッドの一部または全体の下に組み込まれたセンサ720を備えてよく、そうすれば、(例えば、ディスプレイ715上のインジケータを動かすために)ユーザが入力メカニズム712上に指を置いた時に、センサ720がユーザを認証するためにユーザの指の特徴を検出することができる。センサ720は、ユーザがパッドを横切って指を移動させた時にユーザを認証する一次元センサであってもよいし、ユーザの指をパッド上で静止させた時(例えば、ユーザが最初に指をパッドの上に置いた時)にユーザを認証する二次元センサであってもよい。センサ720は、認証のためにユーザが入力メカニズム712の特定の部分の上に指を置く必要がないように、入力メカニズム712の表面全体を網羅してよい。電子デバイス700は、ユーザが十分に検出可能な入力を提供するのを支援するために、例えば、強調表示、ディスプレイ上の指示、または、任意のその他の適切な方法を用いて、各センサ720の位置を特定するよう動作してよい。一部の実施形態において、任意の他の適切な入力メカニズム(例えば、ボタン、ホイール、キー、または、スクリーン)が、ユーザの指紋の特徴をシームレスに検出するセンサ720を備えてよい。10

【0052】

図8Aおよび8Bは、本発明の一実施形態に従って、ユーザの手紋を検出するための電子デバイスの一例を示す概略図である。電子デバイス800は、ディスプレイ810を保持する筐体802を備えてよい。筐体802は、電子デバイスの構成要素を保護するために、電子デバイス800の背面(例えば、ディスプレイ810を備えない側の表面)を実質的に構成してよい。ユーザが電子デバイス800を持つ時、ユーザの手830は、図8Bに示すように、ディスプレイ810が見えるように、筐体802の周りで凹状にされてよく、その時、少なくともユーザの掌832が背面804に触れるよう配置される。電子デバイス800は、背面804内に組み込まれユーザの掌または手の特徴を検出するセンサ820を備えてよい。背面802(または、ディスプレイ810の表面と反対側にある電子デバイスの任意の表面)にセンサ820を配置することにより、センサ820は、ユーザが電子デバイス800を持った時に、ユーザを認証することができる。センサ820は、二次元センサを備えてよく、それにより、電子デバイス800は、背面804に触れて手を移動またはスライドさせるようユーザに要求することなく、ユーザをシームレスに認証することがきる。20

【0053】

図9は、本発明の一実施形態に従って、ユーザの手紋を検出するための電子デバイスの一例を示す概略図である。電子デバイス900は、ユーザがデバイスに入力を提供するための入力メカニズム910を備えてよい。入力メカニズム910は、ユーザの指が入力メカニズム910の上に置かれた時に、ユーザの掌および手首が筐体912の上に置かれるまたはその上方に伸びるように、配置されてよい。電子デバイス900は、デバイスのユーザを認証するために、筐体912内に組み込まれたまたは筐体912上に配置された1または複数のセンサ920を備えてよい。センサ920は、ユーザが、入力メカニズム910を操作するために筐体912の上にユーザの手を置いた時に、ユーザの手、掌、または、手首がセンサ920に対して位置合わせされるように、配置されてよい。センサ920は、ユーザの手が筐体912の上に置かれた時に、例えば、二次元センサを用いて、ユーザの皮膚の特徴を検出するよう動作してよい。30

【0054】

一部の実施形態において、認証システムは、代替的または追加的に、ユーザの皮膚の下の特徴を検出する検知メカニズムを備えてよい。例えば、認証システムは、ユーザの静脈、動脈、毛包の分布パターン、または、検出可能なユーザの皮下の任意の他の適切な特徴を検出するセンサを備えてよい。センサは、例えば、電子デバイスの表面上に配置された光学センサ(例えば、カメラ)など、任意の適切なタイプのセンサを含みうる。センサは、電子デバイスの使用中に、ユーザの皮膚の任意の適切な部分の下の特徴を検出するよ4050

う配置されてよい。例えば、センサは、ユーザの指、手、手首、腕、顔、または、任意の他の適切な領域の皮膚の下の特徴を検出するよう配置されてよい。

【0055】

図10は、本発明の一実施形態に従って、ユーザの皮膚の下の特徴を検出するセンサを有するデバイスの一例を示す概略図である。電子デバイス1000は、筐体1012の一部の上に配置された、または、筐体1012の一部にわたって拡がる入力メカニズム1010を備えてよい。入力メカニズム1010は、使用時に、ユーザの手および手首が（例えば、入力メカニズム1010の上ではなく）筐体1012の上に配置されるように構成されてよい。電子デバイス1000は、ユーザの皮膚の下の特徴を検出するセンサ1020を備えてよい。例えば、センサ1020は、ユーザの手首付近のユーザの静脈パターンを検出する光学センサを含みうる。センサ1020は、例えば、入力メカニズム1010を用いて入力を提供するためにユーザの手を配置した時にユーザの手首がセンサ1020に近接しうるように、筐体1012の上に配置または中に組み込まれる、など、電子デバイス1000の任意の適切な表面に配置されてよい。かかる配置によると、ユーザがデバイス1000を操作する間に、ユーザの皮膚の下の特徴（例えば、ユーザの手首付近の静脈パターン）を検出することによって、シームレスなユーザ認証を行うことができる。10

【0056】

一部の実施形態において、認証システムは、代替的または追加的に、ユーザの顔の特徴を検出するセンサを備えてもよい。例えば、認証システムは、ユーザの顔がセンサと向かい合うように配置された時に、ユーザの顔の1または複数の顕著な特徴によって放射または反射される放射線を検出するセンサを備えてよい。センサは、任意の適切な種類の放射線を検出するよう動作してよい。例えば、センサは、光センサ（例えば、カメラ）、赤外線センサ、紫外線センサ、スキヤニングレーザ、超音波センサ（例えば、ソナー）、または、所望の放射線（例えば、特定の範囲の放射線周波数または周期を持つもの）を検出する任意の他の適切なセンサを含みうる。20

【0057】

認証システムは、ユーザの顔の任意の適切な要素を検出するよう動作してよい。例えば、認証システムは、ユーザの頭部、鼻、口、耳、頬骨、あご、または、ユーザの顔の任意の他の属性の相対的な位置およびサイズを解析することにより、顔を特定しうる。別の例として、認証システムは、ユーザの顔の特徴の曲面または深さ（例えば、眼窩、あご、または、鼻の輪郭）を取り込んで解析するために、三次元認証システムを用いてユーザの顔の特徴を特定してもよい。さらに別の例として、認証システムは、（例えば、皮膚テクスチャ解析を用いて）ユーザの皮膚に特有の線、パターン、または、染みを検出してよい。認証を向上または円滑化するために、これらの方法を併用してもよい。30

【0058】

ユーザの顔の特徴を検出するためのセンサは、電子デバイスの任意の適切な場所に配置されてよい。一部の実施形態において、センサは、別の目的で電子デバイスに提供されたカメラまたは他のセンサ（例えば、チャットのための内蔵ウェブカメラ）を含んでもよい。図11は、本発明の一実施形態に従って、ユーザの顔の特徴を検出するためのセンサを有する電子デバイスの一例を示す概略図である。電子デバイス1100は、ユーザが電子デバイスリソースに対して閲覧またはアクセスを行うためにディスプレイ1110の方を向いた時に、ユーザの顔およびユーザの顔における対象となる特徴が、センサ1120に對して（例えば、センサ1120の視野内に）位置が合いうるよう、ディスプレイ1110に隣接して配置されたセンサ1120を備えてよい。センサ1120と對向したユーザの顔の検出に応答して、電子デバイス1100は、ユーザの顔の特徴を捉えて解析するようセンサ1120に指示し、解析された特徴を許可ユーザに関連づけられた特徴のライブラリと比較してよい。許可ユーザが検出された場合、電子デバイス1100は、制限されたコンテンツ1112をディスプレイ1110に表示したり、コンテンツへのアクセスを提供したりしてよい。40

【0059】

一部の実施形態において、認証システムは、代替的または追加的に、ユーザの眼の属性に基づいて、ユーザを認証するセンサを備えてもよい。例えば、センサは、ユーザの網膜、虹彩、または、網膜血管を走査して、ユーザに特有のパターンを検出するよう動作してもよい。センサは、光（例えば赤外線など）を放射する光源を備えてよく、その光は、ユーザの眼によって反射され、レンズまたは光学センサによって検出される。センサは、受信した光を解析して、許可ユーザの眼のライブラリと比較することができるユーザの眼の表現を作成する。

【0060】

別の例として、センサは、代替的または追加的に、例えば、ユーザの網膜、虹彩、血管、または、ユーザの眼の任意の他の特徴の位置および動きを追跡することにより、ユーザの眼の動きを検出するよう動作してもよい。電子デバイスリソースへのアクセスをユーザに提供する前に、電子デバイスは、許可ユーザによって設定された所定の眼の動きを検出するようセンサに指示してよい。例えば、各許可ユーザは、センサを見つつ、特定の方法で（例えば、上、下、左、右、瞬き、瞬き、など）眼を動かすことにより、眼の動きの流れを作成してよい。デバイスのユーザが所定の眼の動きと適合するように眼を動かした場合に、電子デバイスは、デバイスのロックを解除したり、制限されたリソースへのアクセスを提供したりしてよい。

10

【0061】

センサは、例えば、ユーザの眼と向かい合うデバイスのディスプレイまたはその他の部分に隣接する位置など、デバイスの任意の適切な位置に配置されてよい（例えば、ユーザの眼の特徴からユーザを認証するのに利用できる図11のセンサ1120と同様の位置）。図12は、本発明の一実施形態に従って、ユーザの眼の特徴を検出するためのセンサを有する電子デバイスの一例を示す概略図である。電子デバイス1200は、ユーザが電子デバイスリソースに対して閲覧またはアクセスを行うためにディスプレイ1210の方を向いた時に、ユーザの眼が、センサ1220に対して（例えば、センサ1220の視野内に）位置合わせされうるように、ディスプレイ1210に隣接して配置されたセンサ1220を備えてよい。センサ1220を用いて、電子デバイス1200は、ユーザを認証し、制限されたデバイスリソースへのアクセスを提供するために、ユーザの眼の特徴または動きを検出してよい。一部の実施形態において、センサ1220は、（例えば、図11のセンサ1120のように）ユーザの顔の特徴に基づいてユーザを認証するよう実装してもよい。

20

【0062】

一部の実施形態において、認証システムは、声の属性または質に基づいて、ユーザを認証するよう動作してもよい。例えば、認証システムは、特定の声の高さまたは声紋を検出するよう動作してよい。認証システムは、文字列に依存してもよいし（例えば、ユーザは、「私の声が私のパスワード」など、認証のための特定のフレーズを言わなければならない）、文字列に依存しなくてもよい（例えば、ユーザの認証のために、任意の適切な言葉を言えばよい）。一部の実施形態において、認証システムは、認証のために秘密のパスワードを言うようユーザに要求してよく、そうすれば、そのユーザのパスワードを知っていることと、そのユーザの声の高さを有することの両方を要求して、適切な認証を行うことができる。認証システムは、例えば、マイクロホンなど、ユーザを認証するための任意の適切な構成要素を備えてよい。一部の実施形態において、マイクロホンは、主に別の目的（例えば、電話通信またはビデオ会議）に用いられてもよい。

30

【0063】

一部の実施形態において、他のタイプの認証システムが用いられてもよい。一部の実施形態において、認証システムは、外耳道の形からユーザを特定して認証するよう動作してよい。例えば、認証システムは、ユーザの外耳道の特有な特徴（例えば、形および長さ）を検出するセンサ（例えば、光学センサ、レーダー、または、ソナー）を備えてよい。例えば、センサは、（例えば、デバイスが電話である場合には）デバイスのスピーカの近くに配置されてよい。一部の実施形態において、認証システムは、ユーザに特有の匂いに基

40

50

づいてユーザを特定するよう動作してもよい。例えば、認証システムは、ユーザの皮膚または汗腺の匂いに特有の属性を検出するセンサを備えてよい。センサは、例えば、入力デバイスの場所またはその近傍（例えば、ユーザがデバイスに触れる場所）など、デバイス上の任意の適切な場所に配置されてよい。

【0064】

一部の実施形態において、認証システムは、DNA配列に基づいて、ユーザを特定するよう動作してもよい。例えば、認証システムは、ユーザのDNAを有する細胞を（例えば、ユーザの皮膚または口から）取得するプロセッサに接続されたセンサを備え、特定のDNA配列が存在するか否かを判定してよい。DNA配列の長さまたは変異は、適切な認証を提供しつつ認証処理を十分に速やかに実行できるように選択されてよい（例えば、DNA鎖全体を解析する必要はない）。センサは、例えば、ユーザが触れうる入力メカニズムまたはその他の構成要素上、または、その近傍など、デバイス上の任意の適切な場所に配置されてよい。10

【0065】

電子デバイスは、任意の適切な方法を用いて、許可ユーザを反映する生体情報を取得してよい。例えば、ユーザが特定のデバイスリソースに対して用いるよう認証システムを選択すると、電子デバイスは、ライブラリに格納すべき生体情報（例えば、指紋、眼の走査結果、または、DNA配列）を提供するようユーザに指示してよい。電子デバイスは、例えば、視覚的な合図、聴覚的な合図を用いる方法、および、認証システムのセンサの位置を強調または特定する方法など、任意の適切な方法を用いて、生体情報入力を提供するようユーザに指示してよい。取得されてライブラリに格納された生体情報は、ユーザが認証を試みる時に取り出され、ユーザによって提供された生体情報と比較されてよい。提供された生体認証情報がライブラリに格納された情報（例えば、要求されたリソースに関連づけられた情報）と適合する場合、電子デバイスは、制限されたリソースへのアクセスを提供してよい。一部の実施形態において、同様の方法を用いて、非生体認証情報を受信してもよい。20

【0066】

一部の実施形態において、認証システムは、代替的または追加的に、ユーザに電子デバイスリソースへのアクセスを提供するために、生体パラメータを要求しなくてもよい。非生体認証システムは、生体認証システムよりも容易に破られる場合もあるが、非常に効果的で安全なものもある。一部の実施形態において、認証システムは、キーまたはトークンが電子デバイスから特定の距離の範囲内にあるとの検出に応答して、電子デバイスリソースへのアクセスを提供してよい。例えば、ユーザは携帯電話およびコンピュータを有してよい。一方または両方のデバイスは、それらのデバイスが互いに特定の範囲内にあることを検出するための回路を備えてよい（例えば、ユーザがポケットに携帯電話を入れてコンピュータを使うためにデスクに座った時に認証されうるように5フィートの範囲など）。デバイスが互いに近接していると判定した場合、一方または両方のデバイスのリソースが利用可能になってよい。この方法は、ユーザが携帯型デバイスを持ち続けうることを利用しつつ、据え付け型のデバイスへのアクセスを保護するのに特に有効である。本実施形態および他の実施形態の詳細は、2007年6月27日に出願された同時係属している本願出願人の米国特許出願第11/823,656号（代理人整理番号104677-0059-101、P4884US1）に記載されている。3040

【0067】

一部の実施形態において、電子デバイスは、ユーザによって提供される特定の一連の入力に基づいて、ユーザを認証してもよい。例えば、電子デバイスは、電子デバイスによって提供された視覚的パターンと対応する入力を提供するようユーザに要求してよい。図13および図14は、本発明の一実施形態に従って、視覚的パターンを提供するためのディスプレイの一例を示す概略図である。ディスプレイ1300は、オプションすなわち図形1312の分布1310を備えてよい。ディスプレイ1400は、オプションすなわち図形1412の分布1410を備えてよい。図形1312および1412の各々は、異なる

50

網掛けパターン（例えば、異なる線方向）、単色または多色、形状または輪郭、サイズ（例えば、周囲長または面積）、表示された他の図形との近さまたは相対位置、他の形状との配列（例えば、4つの黄色の図形を選択すると直線を形成する、など）、ソース（例えば、特定のアルバムまたはライブラリの写真を示す図形）、または、任意のその他の適切な特徴を有してよい。分布1310または1410は、例えば、複数の一様に分布した図形（例えば、20の一様に分布した図形1310）、または、見かけ上不規則な分布の図形（例えば、任意に分布した形1410）など、任意の適切な数および分布の図形を含んでよい。

【0068】

認証を行うために、ユーザは、表示された図形すなわちオプションから任意の適切なサブセットを（例えば、入力メカニズムまたはその他のセンサによって検出された通りに）選択してよい。サブセットは、1または複数の属性を共有する一部またはすべての図形を含みうる。例えば、ユーザは、特定の色である一部またはすべての図形（例えば、黄色を含む図形すべて）を選択してよい。別の例として、ユーザは、同じ輪郭を有する一部またはすべての図形（例えば、すべての正方形）を選択してもよい。さらに別の例として、ユーザは共通する特定の属性を有する一部またはすべての図形（例えば、5つの辺を持つ図形すべて、または、デバイスが格納する特定のアルバムに関連づけられた写真を表す図形すべて）を選択してもよい。さらにまた別の例として、ユーザは、特定の分布の色を含む一部またはすべての図形（例えば、青い部分に隣接して赤い部分を含む図形）を選択してもよい。（青い図形を上から2つ、および、正方形を下から2つ選択するなど、上述の例を組み合わせたものも含め）任意の適切な基準または属性が、表示された図形の特定のサブセットを選択するために用いられてよい。

10

【0069】

任意の適切な数の図形すなわちオプションが、認証のために選択すべきサブセットに関連づけられてよい。例えば、かかる図形の数は、表示された図形の総数に関連してよい（例えば、表示された図形の20%を選択する、など）。別の例として、かかる図形の数は、（例えば、ユーザが片手ですべての図形を同時に選択できるように）5以下、または、（ユーザが両手ですべての図形を同時に選択できるように）10以下など、決まった数であってもよい。かかる図形の数は、セキュリティを最適化するように選択されてもよい（例えば、どの図形を選択すべきかを容易には推測できないほど十分な数の図形を要求する、など）。

20

【0070】

ユーザは、任意の適切な方法を用いて、サブセットに含まれる図形を選択してよい。マルチタッチディスプレイが提供されている場合、認証システムは、認証に用いる図形すべてを同時に選択するようユーザに要求してよい。別の例として、認証システムは、ユーザが、認証に用いられる図形を順次選択することを許容してもよい。図形は、任意または特定の順序（例えば、上から下、または、左から右）で選択されてよい。さらに別の例として、認証システムは、一筆書きの入力で（例えば、ディスプレイにわたって指をドラッグして）、許可されたサブセットの図形だけを選択するようユーザに要求してもよい。サブセットに含まれる図形を選択するための任意の他の適切な方法を用いてもよい。

30

【0071】

（例えば、表示されたキーパッドを用いて数字のパスコードを入力する場合と同様に）、ディスプレイ上の同じ相対位置に表示された図形をユーザに毎回選択させることを避けるために、電子デバイスは、認証のために選択すべき図形の分布を変更してもよい。次いで、ユーザは、認証を行うために、認証プロトコルに関連づけられた属性を共有する図形を特定してよい。ユーザがデバイスリソースにアクセスするたびに、認証に用いられる図形の位置が変化しうるため、選択された図形の全体的な分布をユーザの肩越しに見た人物が、認証のために同じ分布で図形を選択することはできない（例えば、縞模様の図形が、デバイスの同じ領域に分布されなくてもよい）。

40

【0072】

50

無許可ユーザが適切な図形サブセットを推測することを防ぐために、認証のために図形を選択する試みを失敗した後には、電子デバイスは、表示された図形の分布を変更させてもよいし、図形を変化させてもよい（例えば、異なる色または輪郭を用いる、など）。電子デバイスは、適切な図形サブセットを選択する試みに特定の回数失敗した後に、デバイスをロックしてよい。ロックされると、ユーザは、デバイスを再度有効にするためにデバイスをホストに接続する（例えば、携帯型デバイスを据え付け型デバイスに接続する）必要があつてもよいし、デバイスを再度有効にするために別の認証システム（例えば、生体認証システムなど）を用いる必要があつてもよい。

【0073】

一部の実施形態においては、特定の図形を選択するのではなく、ユーザは、スクリーンの所定の部分に位置する図形を単に選択してもよい。例えば、ユーザは、実際に表示されている図形と無関係に、いくつかの図形位置に1または複数の指を置いてよい。別の例として、ユーザは、電子デバイスに表示された特定の図形上に1または複数の指を置いて、表示されている図形と無関係に、所定の方法で1または複数の指を動かしてもよい（例えば、1または複数の指をスライドしてよい）。さらに別の例として、ユーザは、ディスプレイの所定の位置に配置されたいいくつかの図形を連続的に選択してもよい（例えば、所定のパターンを形成するように特定の位置の図形を選択する、など）。一部の実施形態において、電子デバイスは、ユーザが1または複数の指を用いて1または複数のパターンをその上に描きうる空白または一様なディスプレイ画面を提供してもよい。かかる方法は、表示された図形で視覚的に引きつけることにより、無許可ユーザを混乱させたり注意をそらしたりすることができる。

【0074】

一部の実施形態において、電子デバイスは、代替的または追加的に、ユーザから受信した入力の時間的パターンに基づいて、ユーザを認証してもよい。例えば、ユーザは、認証のために、特定の速度で特定の回数の入力を提供してよい。電子デバイスは、任意の適切な方法を用いて入力を検出してよい。例えば、電子デバイスは、デバイスの入力メカニズムを用いて提供された入力（例えば、タッチスクリーンが受けた入力）を検出してよい。別の例として、電子デバイスは、デバイスの適切なセンサ（例えば、加速度計）によって検出された動き、接触、振動、または、その他の衝撃から入力を検出してよい。かかる方法において、ユーザは、デバイスの任意の部分（または、デバイスが置かれているテーブルなど、デバイスと接触する物体）をタップ（たたく）してよく、デバイスのセンサが、それらのタップを検出して、許可された時間的パターンに対応しているか否かを判定する。さらに別の例として、電子デバイスは、デバイスのセンサ（例えば、加速度計またはジャイロスコープ）を用いて、特定の方法（例えば、2回振った後に回転させる、など）で動かされたことを検出してよい。正確な時間的パターンの検出に応答して、電子デバイスは、制限されたリソースへのアクセスを提供してよい。

【0075】

一部の実施形態において、認証システムは、認証のための時間的パターンおよび視覚的パターンを組み合わせてもよい。例えば、ユーザは、或る特定の速度（例えば、最初の2つの図形を素早く、次いで、休止した後に、最後の2つを同時に選択）で、特定の表示された図形を選択するよう要求されてよい。別の例として、ユーザは、最初に適切な図形を選択し、次いで時間的パターンの入力を提供するよう要求されてもよい。さらに別の例として、ユーザは、1または複数の図形を選択し、デバイスを動かす（例えば、デバイスを振る）よう要求されてもよい。任意の他の適切な組み合わせの入力が、認証のために要求されてもよい。

【0076】

電子デバイスは、任意の適切な方法を用いて、許可ユーザに対して視覚的または時間的パターンを設定してよい。一部の実施形態において、ユーザが、特定のデバイスリソースへのアクセスを制限するために時間的または視覚的パターンを用いると選択した場合、電子デバイスは、時間的または視覚的パターンを提供または選択するようユーザに指示して

10

20

30

40

50

よい。例えば、電子デバイスは、ユーザがパターンを形成するために選択できる図形の属性（例えば、色または輪郭）のリストを提供してよい。別の例として、電子デバイスは、表示された図形を選択するか時間的パターンを提供するようユーザに指示して、受信した入力からパターンを抽出または特定してもよい。電子デバイスは、ユーザが、意図的に行つたこと、および、選択したパターンを記憶していることを保証するために、パターンを受け付ける前に複数回提供するようユーザに指示してもよい。

【0077】

電子デバイスは、任意の適切な数およびタイプの認証システムを備えてよい。例えば、電子デバイスは、上述の認証システムまたは認証方法内の1つ、複数、または、すべてを備えてよい。様々なリソースへのアクセスが、1または複数の認証システムを用いて制限されてよく、用いられる認証システムは、ユーザが選択または設定してよい。一部の実施形態において、特定の制限されたリソースへのアクセスが提供される前に、複数の認証システムが連続的に用いられてもよい。10

【0078】

図15は、本発明の一実施形態に従って、ユーザを認証するための方法の一例を示すフローチャートである。処理1500は工程1502で始まる。工程1504で、電子デバイスは、デバイスのユーザを特定してよい。例えば、電子デバイスは、ユーザに関連づけられたユーザ名またはパスワードを受信してよい。別の例として、電子デバイスは、認証システムを用いて認証情報を受信し、受信した認証システムからユーザを特定してもよい。電子デバイスは、例えば、ユーザがデバイスを操作する時に認証情報をシームレスに取得できるように認証システムのセンサを配置することによって、ユーザからの明示的な入力を要求することなく、認証情報を自動的に受信しうる。別の例として、センサは、ユーザがセンサの視野すなわち検知領域内に入るとすぐに、ユーザの属性の特徴を検出するよう動作してもよい。一部の実施形態において、処理1500は、工程1502から工程1506に直接移行してもよい。20

【0079】

工程1506で、電子デバイスは、制限されたリソースへのアクセス要求が受信されたか否かを判定してよい。例えば、電子デバイスは、ユーザが、特定のユーザに関連づけられたデータ（例えば、連絡先リストまたは他の個人情報）にアクセスするための命令を提供したか否かを判定してよい。別の例として、電子デバイスは、ユーザが、制限されたアプリケーション（例えば、管理者などの特定の階層のユーザに制限されたアプリケーション、または、特定のユーザが購入したアプリケーション）にアクセスするための命令を提供したか否かを判定してもよい。制限されたリソースにアクセスするための命令を受信していないと、電子デバイスが判定した場合、処理1500は、工程1506に戻って、ユーザから受ける入力を監視し続けてよい。30

【0080】

一方、工程1506で、制限されたリソースにアクセスするための命令を受信したと、電子デバイスが判定した場合、処理1500は、工程1508に進んでよい。工程1508で、電子デバイスは、特定されたユーザがリソースへのアクセスを許可されているか否かを判定してよい。例えば、電子デバイスは、ユーザが、制限されたリソースにアクセスするのに適切な認証情報を提供したか否かを判定してよい。電子デバイスは、例えば、通常の使用中に認証情報を取得できるように、デバイスに認証センサを内蔵することによって、ユーザの知るところなく、適切な認証情報を取得してよい。特定されたユーザが許可されていないと、電子デバイスが判定した場合、処理1500は、工程1510に進んでよい。工程1510で、電子デバイスは、認証を行うようユーザに指示してよい。例えば、電子デバイスは、認証システム（例えば、上述の認証システムのいずれか）に認証情報を提供するようユーザに指示してよい。一部の実施形態において、電子デバイスは、ユーザによる複数の入力を検出し、それらの入力が、許可ユーザに関連づけられたパターンを有しているか否か、または、許可ユーザに関連づけられた属性を共有しているか否かを判定してよい（例えば、ユーザが、許可ユーザの属性またはパターンに対応する適切な入力4050

を提供したか否かを判定する、または、入力の属性またはパターンが、許可ユーザに関連づけられた属性またはパターンと適合するか否かを判定する)。次いで、処理 1500 は、ユーザが適切な認証情報を提供したか否かを判定する工程 1508 に戻ってよい。

【0081】

一方、工程 1508 で、ユーザが許可されていると、電子デバイスが判定した場合、処理 1500 は、工程 1512 に進んでよい。工程 1512 で、電子デバイスは、要求された制限されたリソースへのアクセスをユーザに提供してよい。例えば、電子デバイスは、個人データへのアクセスまたはユーザに固有のアプリケーションへのアクセスをユーザに提供してよい。次いで、処理 1500 は、工程 1514 で終了してよい。

【0082】

上述の本発明の実施形態は、限定ではなく例示の目的としたものであり、本発明は、以下の特許請求の範囲によってのみ限定される。

【要約】

本発明は、デバイスリソースへのアクセスを制限するための内蔵認証システムを備えた電子デバイスに関する。認証システムは、ユーザの生体情報を検出する 1 または複数のセンサを備えてよい。センサは、生体情報を提供するためのステップを実行するようユーザに要求することなく、ユーザがデバイスを操作した時に、センサが適切な生体情報を検出できるように、デバイスに配置されてよい(例えば、デバイス筐体の別個の部分に指紋センサを設けるのではなく、入力メカニズム内に指紋センサを組み込む)。一部の実施形態において、認証システムは、ユーザを認証するために視覚的または時間的な入力パターンを検出するよう動作してよい。認証に応答して、ユーザは、制限されたファイル、アプリケーション(例えば、ユーザが購入したアプリケーション)、または、設定(例えば、連絡先または保存したゲームプロファイルなどのアプリケーション設定)にアクセスできるようになる。

【図 1】

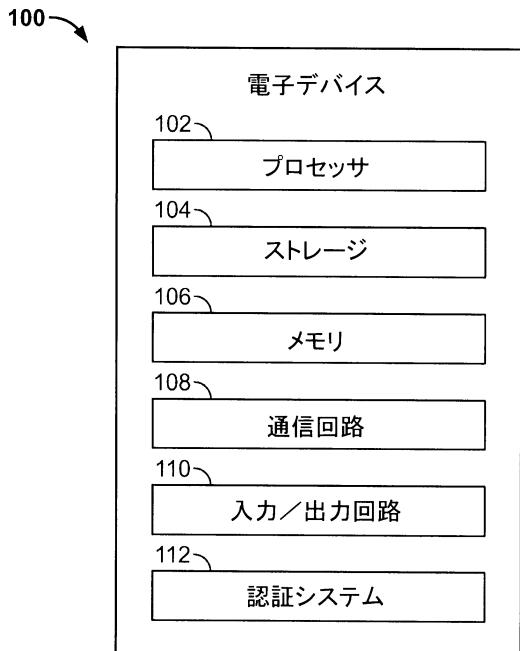


FIG. 1

【図 2】

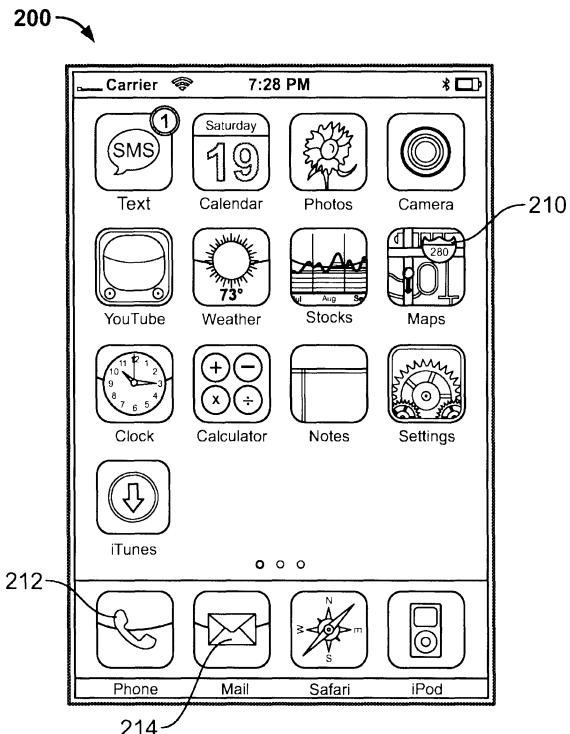
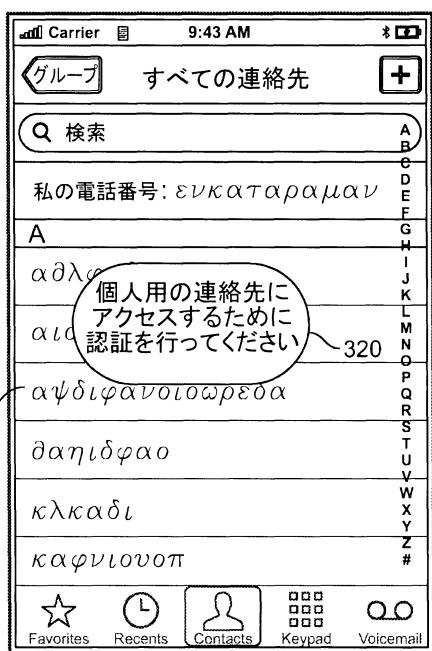


FIG. 2

【図3】

300



310

FIG. 3

【図4】

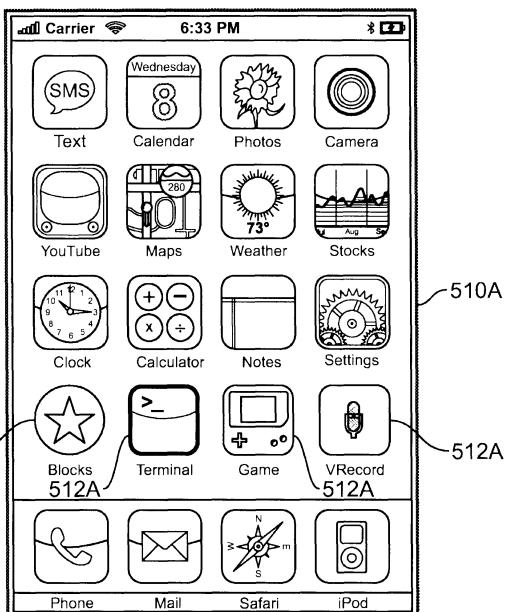
400

420
410

FIG. 4

【図5A】

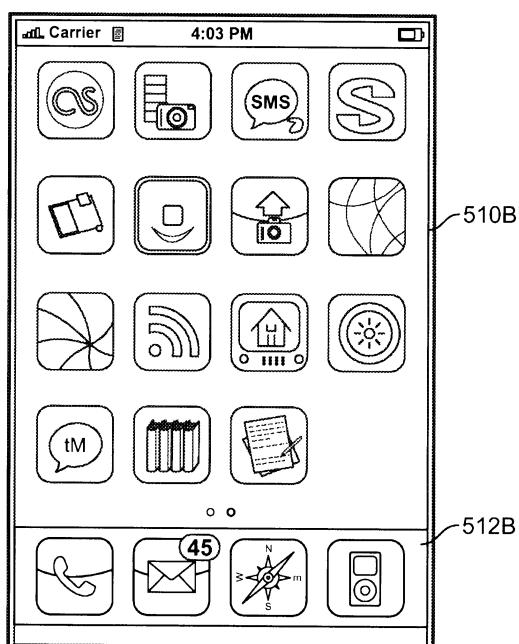
500A



512A

【図5B】

500B



512A

FIG. 5A

FIG. 5B

【図 5 C】

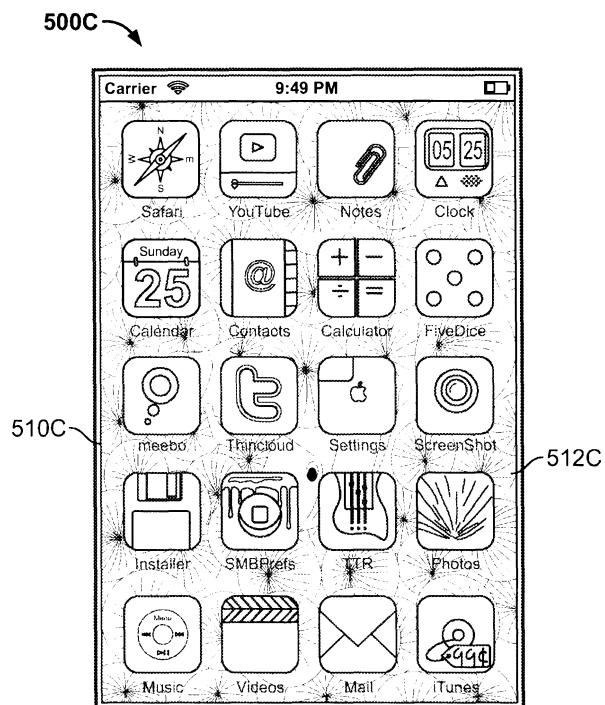


FIG. 5C

【図 6】

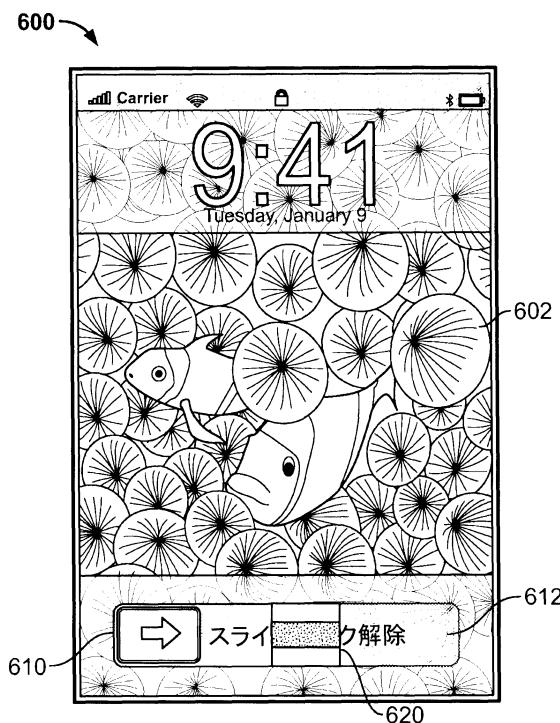


FIG. 6

【図 7】

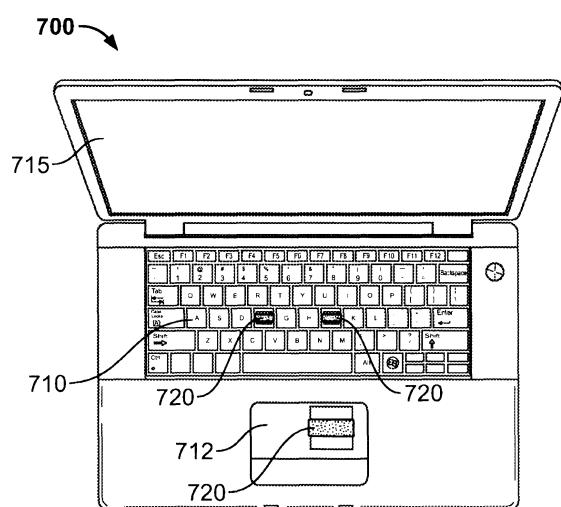


FIG. 7

【図 8 A】

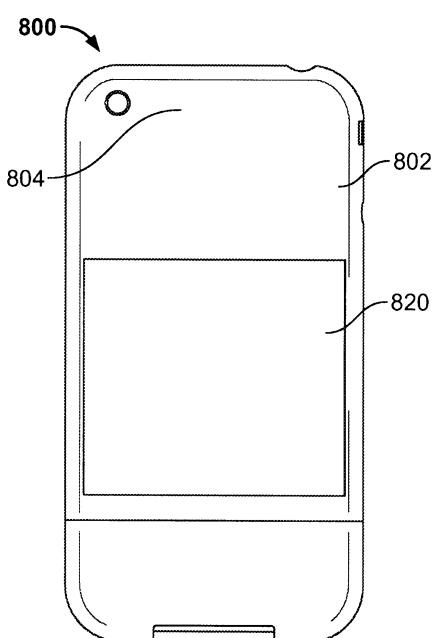
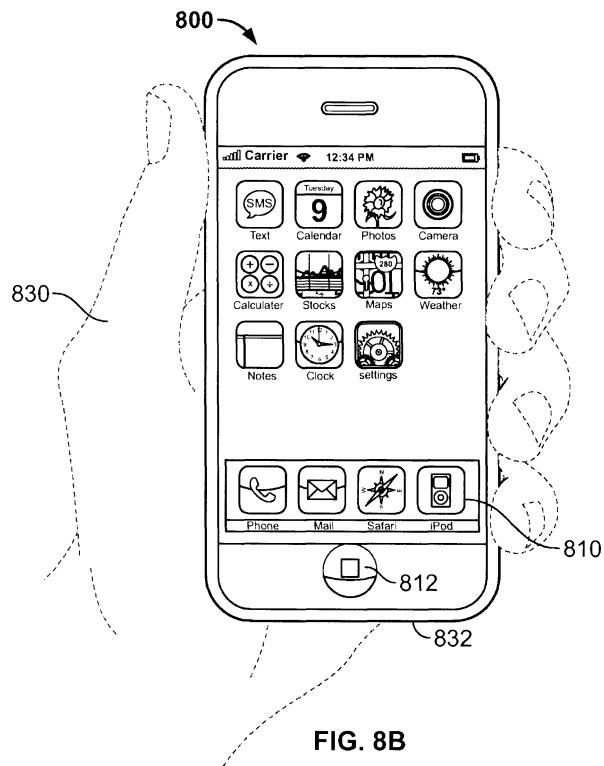


FIG. 8A

【図 8B】



【図 9】

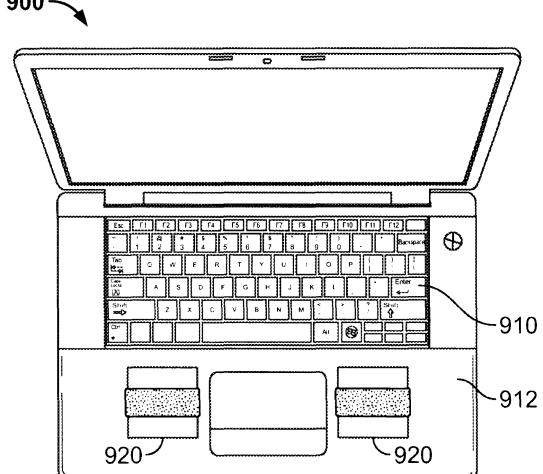
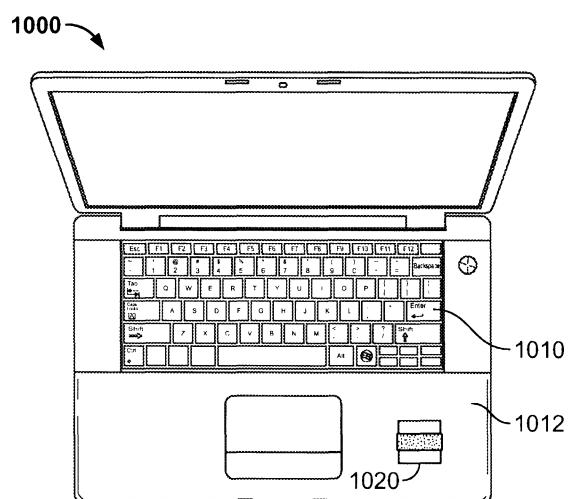


FIG. 9

FIG. 8B

【図 10】



【図 11】

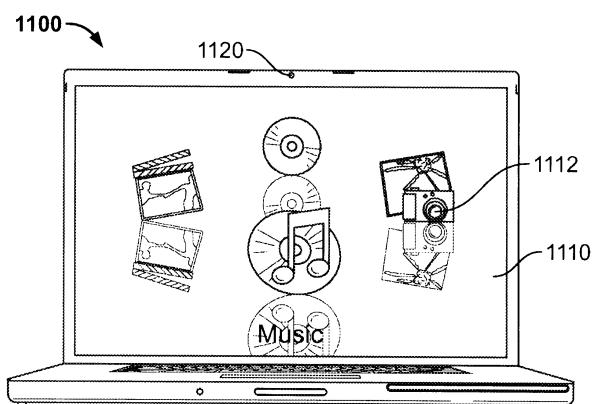


FIG. 11

FIG. 10

【図12】

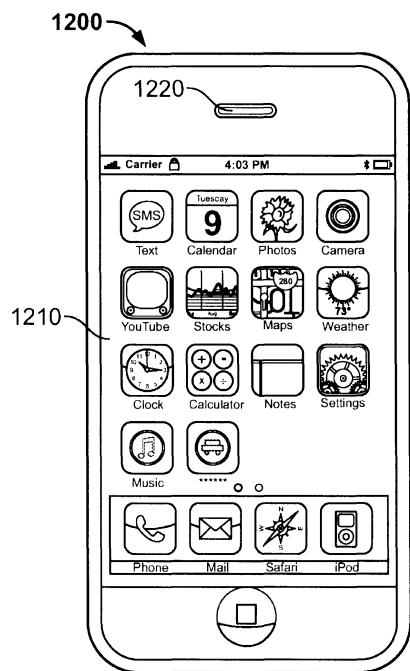


FIG.12

【図13】

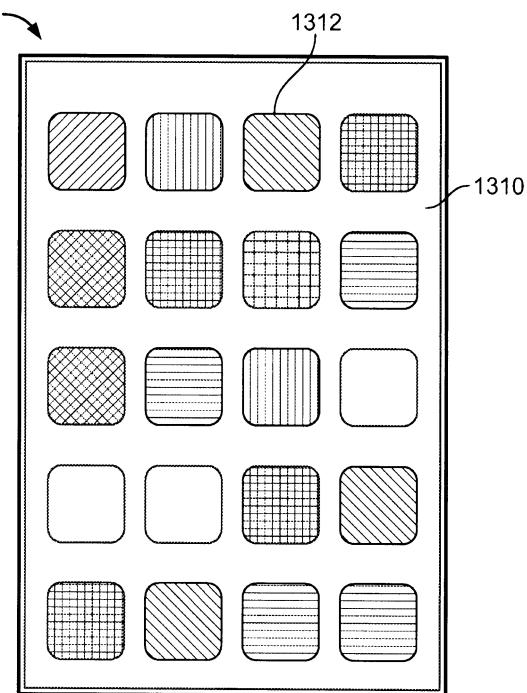


FIG.13

【図14】

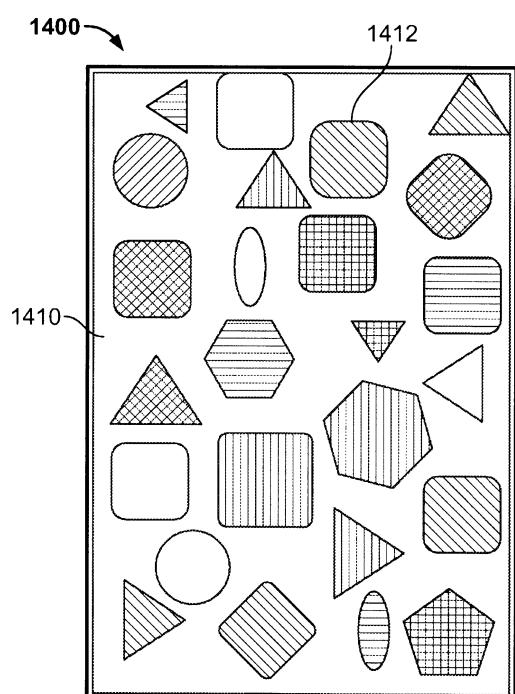


FIG.14

【図15】

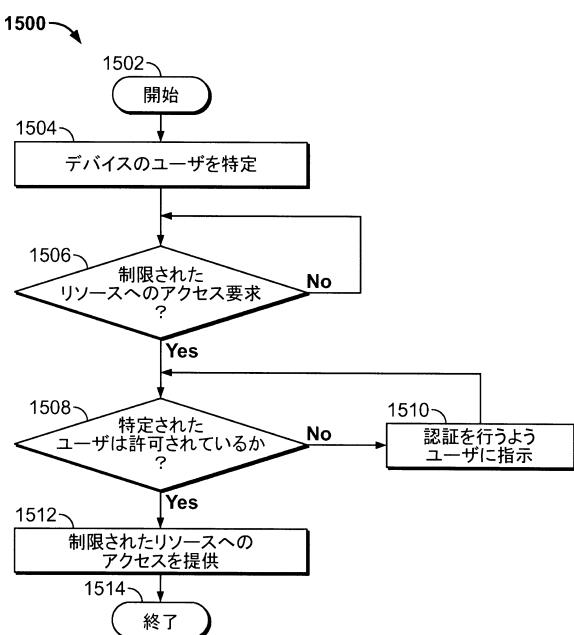


FIG. 15

フロントページの続き

(74)代理人 100134175
弁理士 永川 行光

(72)発明者 ファデル・アンソニー
アメリカ合衆国 カリフォルニア州 95014 クパチーノ, インフィニット・ループ, 1

(72)発明者 ホッジ・アンドリュー
アメリカ合衆国 カリフォルニア州 95014 クパチーノ, インフィニット・ループ, 1

(72)発明者 シェル・スティーブン
アメリカ合衆国 カリフォルニア州 95014 クパチーノ, インフィニット・ループ, 1

(72)発明者 カバレロ・ルーベン
アメリカ合衆国 カリフォルニア州 95014 クパチーノ, インフィニット・ループ, 1

(72)発明者 ドログスカー・ジェシー リー
アメリカ合衆国 カリフォルニア州 95014 クパチーノ, インフィニット・ループ, 1

(72)発明者 ザデスキー・スティーブン
アメリカ合衆国 カリフォルニア州 95014 クパチーノ, インフィニット・ループ, 1

(72)発明者 サンフォード・エメリー
アメリカ合衆国 カリフォルニア州 95014 クパチーノ, インフィニット・ループ, 1

審査官 宮司 卓佳

(56)参考文献 特開2000-315118 (JP, A)
特開2006-085559 (JP, A)
特開2004-313459 (JP, A)
国際公開第2007/076210 (WO, A1)
米国特許出願公開第2006/0224645 (US, A1)

(58)調査した分野(Int.Cl., DB名)

G 06 F 21 / 30 - G 06 F 21 / 46