

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

**特許第6722272号
(P6722272)**

(45) 発行日 令和2年7月15日(2020.7.15)

(24) 登録日 令和2年6月23日(2020.6.23)

(51) Int.CI.

F 1

G06T 7/00 (2017.01)
G06F 21/32 (2013.01)
A61B 3/113 (2006.01)
A61B 5/1171 (2016.01)

GO6T 7/00 510D
 GO6F 21/32
 A61B 3/113
 A61B 5/1171 300

請求項の数 2 (全 14 頁)

(21) 出願番号 特願2018-506086 (P2018-506086)
 (86) (22) 出願日 平成28年4月18日 (2016.4.18)
 (65) 公表番号 特表2018-517998 (P2018-517998A)
 (43) 公表日 平成30年7月5日 (2018.7.5)
 (86) 國際出願番号 PCT/US2016/028090
 (87) 國際公開番号 WO2016/168814
 (87) 國際公開日 平成28年10月20日 (2016.10.20)
 審査請求日 平成31年4月17日 (2019.4.17)
 (31) 優先権主張番号 62/148,501
 (32) 優先日 平成27年4月16日 (2015.4.16)
 (33) 優先権主張国・地域又は機関
米国(US)

早期審査対象出願

(73) 特許権者 517361546
 トビー エーピー
 アメリカ合衆国、ヴァージニア 2204
 6, フォールズ チャーチ, ノース ワシ
 ントン ストリート 510, スイート
 200
 (74) 代理人 100137969
 弁理士 岡部 肇昭
 (74) 代理人 100104824
 弁理士 梶場 仁
 (72) 発明者 スコゲ, モーテン
 スウェーデン, ストックホルム 182
 53, ダンダイド, 7ティーアール, カー
 ルスロヴァーゲン 2ディー

最終頁に続く

(54) 【発明の名称】凝視情報を使用するユーザの識別および／または認証

(57) 【特許請求の範囲】

【請求項 1】

デバイスのユーザを認証するためのシステムであって、前記システムは、
 ユーザの少なくとも一部の少なくとも1つの画像を取り込むための第1の画像センサと

、前記第1の画像センサによって取り込まれた少なくとも1つの画像に少なくとも部分的に基づいて、前記ユーザの眼に関する情報を判定する判定ユニットと、

前記ユーザの前記眼に関する前記情報を用いて前記ユーザを認証するための認証ユニットと、

プロファイルユニットであって、

前記認証ユニットによって認証される前記ユーザに基づく視標追跡較正プロファイルをロードし、前記視標追跡較正プロファイルは、光軸に対する前記ユーザの前記眼の眼窩の間、または前記眼窩と前記ユーザの前記眼の角膜曲率の間のオフセットを記憶し、

ログインプロシージャの一部として、前記視標追跡較正プロファイルおよび前記判定ユニットによって判定された凝視情報を用いて、ログインプロシージャを実行し、

前記ログインプロシージャは、

1つ以上の仮想オブジェクトを提示し、

前記判定ユニットから、前記1つ以上の仮想オブジェクトを見るときの前記眼の特性を定義する前記凝視情報を受信し、

前記視標追跡較正プロファイルからの眼の情報で前記眼の前記特性を確認し、

10

20

前記ログインプロシージャの完了後に、前記ユーザの前記眼を追跡することの一部として前記判定ユニットによって判定される将来の凝視情報を、前記視標追跡較正プロファイルに少なくとも部分的に基づいて変更する、プロファイルユニットを備える、システム。

【請求項 2】

デバイスのユーザを認証するためのシステムであって、前記システムは、ユーザの少なくとも一部の少なくとも1つの画像を取り込むための第1の画像センサと、

前記第1の画像センサによって取り込まれた少なくとも1つの画像に少なくとも部分的に基づいて、前記ユーザの眼に関する情報を判定する判定ユニットと、

前記ユーザの前記眼に関する前記情報を用いて前記ユーザを認証するための認証ユニットと、

前記ユーザの認証に基づいてユーザプロファイルをロードするためのプロファイルユニットであって、

前記認証ユニットによって認証される前記ユーザに基づく視標追跡較正プロファイルをロードし、前記視標追跡較正プロファイルは、光軸に対する前記ユーザの前記眼の眼窩の間、または前記眼窩と前記ユーザの前記眼の角膜曲率の間のオフセットを記憶し、

ログインプロシージャの一部として、前記視標追跡較正プロファイルおよび前記判定ユニットによって判定された凝視情報を用いて、ログインプロシージャを実行し、

前記ログインプロシージャは、

1つ以上の仮想オブジェクトを提示し、

前記判定ユニットから、前記1つ以上の仮想オブジェクトを見るときの前記眼の特性を定義する前記凝視情報を受信し、

前記視標追跡較正プロファイルからの眼の情報で前記眼の前記特性を確認し、

前記ログインプロシージャの完了後に、前記ユーザの前記眼を追跡することの一部として前記判定ユニットによって判定される将来の凝視情報を、前記視標追跡較正プロファイルに少なくとも部分的に基づいて変更する、プロファイルユニットを備え、

前記ユーザプロファイルが、コンピュータ上で動作するコンピュータアプリケーションの動作に影響を及ぼす、システム。

【発明の詳細な説明】

【技術分野】

【0001】

関連出願の相互参照

[0001]本出願は、2016年4月16日に提出された米国仮特許出願第62/148,501号“IDENTIFICATION OR AUTHENTICATION OF A USER USING GAZE INFORMATION”的優先権を主張し、その開示の全体は、全ての目的のために、本明細書に完全に記載されているかのように、参照により本明細書に組み込まれる。

【0002】

[0002]本発明は、一般に、ユーザからの凝視情報を使用するユーザ識別および/またはユーザの認証のためのシステムおよび方法に関し、特に、ユーザがそのような凝視情報を使用してデバイスにログインすることを可能にするシステムおよび方法に関する。

【背景技術】

【0003】

[0003]現代のコンピューティングでは、セキュリティは非常に重要である。コンピューティングデバイスの移動性とパワーが向上するにつれて、複数のユーザがますます多くのデバイスを使用している。したがって、複数のユーザを正確に識別して、デバイスにログインさせることが最も重要である。

【0004】

10

20

30

40

50

[0004]従来の識別および認証システムは、パスワードまたはパスフレーズ認証などの単純なメカニズムに依存している。これは、システムがユーザ名および／またはパスワードの両方の正確な構文を記憶しておく能力に依存しているため面倒である。多くの場合、ユーザは、様々なシステムのための潜在的に異なるユーザ名とパスワードを覚えておく必要がある。さらに、そのような情報は、場合によっては、ユーザから学習され、抽出され、コピーされ、そうでなければ取得されて、そのユーザとして不正にログインされる可能性がある。

【0005】

[0005]ユーザがコンピューティングデバイスにログインすることを可能にするために、他の形式の識別および認証を使用することが以前から提案されている。例えば、多くのコンピューティングデバイスは、現在、デバイスのログインを容易にするためにユーザの指紋をスキャンするための指紋センサを備える。そのようなシステムの問題点は、ユーザが指先をある時間感知表面上にしばらく保持しなければならないことであり、したがって、感知表面または指の汚れおよび他の障害物などのさらなる問題により、システムが正確に機能しなくなる可能性がある。

【0006】

[0006]さらに、代替的な認証技術として網膜走査技術が提案されている。これらのシステムでは、ユーザの網膜は、カメラなどによってスキャンされ、保存された網膜プロファイルと照合され、それにより、正しいユーザがコンピューティングデバイスにログインすることを可能にする。このシステムでは、スキャン中にユーザが依然として静止している必要があるため、システムが機能しない可能性もある。

【発明の概要】

【発明が解決しようとする課題】

【0007】

[0007]網膜スキャンおよび他の顔面スキャンシステムは、人またはその眼の写真をスキャンするなどの方法によってだまされる可能性もある。したがって、生きた人物としてユーザを認証し、デバイスのログインを可能にする改良されたシステムが必要とされている。

【0008】

[0008]さらに、第三者によって観察されている場合であっても、ユーザに対して個別であり、ユーザがコンピューティングデバイスを使用して認証することを可能にする非接触ログインプロセッサーが必要である。

【課題を解決するための手段】

【0009】

[0009]一実施形態では、デバイスのユーザを認証するためのシステムが提供される。本システムは、第1の画像センサと、判定ユニットと、認証ユニットとを含むことができる。第1の画像センサは、ユーザの少なくとも一部の少なくとも1つの画像を取得するためのものとすることができます。判定ユニットは、第1の画像センサによって取り込まれた少なくとも1つの画像に少なくとも部分的に基づいて、ユーザの眼に関する情報を判定するためのものとすることができます。認証ユニットは、ユーザの眼に関する情報を使用してユーザを認証するためのものとすることができます。

【0010】

[0010]他の実施形態では、デバイスのユーザを認証するための方法が提供される。本方法は、第1の画像センサを用いてユーザの少なくとも一部の少なくとも1つの画像を取り込むステップを含むことができる。本方法はまた、第1の画像センサによって取り込まれた少なくとも1つの画像に少なくとも部分的に基づいてユーザの眼に関する情報を判定することを含むことができる。本方法は、ユーザの眼に関する情報を使用してユーザを認証するステップをさらに含むことができる。

【0011】

[0011]別の実施形態では、デバイスのユーザを認証する方法のための命令を記憶した非

10

20

30

40

50

一時的機械可読媒体が提供される。本方法は、第1の画像センサを用いてユーザの少なくとも一部の少なくとも1つの画像を取り込むステップを含むことができる。本方法はまた、第1の画像センサによって取り込まれた少なくとも1つの画像に少なくとも部分的に基づいてユーザの眼に関する情報を判定することを含むことができる。本方法は、ユーザの眼に関する情報を使用してユーザを認証するステップをさらに含むことができる。

【0012】

[0012]本発明は添付図面と関連して説明される。

【図面の簡単な説明】

【0013】

【図1】デバイスのユーザを認証するための本発明の一実施形態の1つのシステムのブロック図である。10

【図2】デバイスのユーザを認証するための本発明の一実施形態の1つの方法のブロック図である。

【図3】本発明の装置またはシステムの少なくとも一部に使用することができる、または本発明の方法の少なくとも一部を実施することができる、例示的なコンピュータシステムのブロック図である。

【発明を実施するための形態】

【0014】

[0016]以下の説明は、例示的な実施形態のみを提供するものであり、本開示の範囲、適用性、または構成を限定するものではない。むしろ、例示的な実施形態についての以下の説明は、当業者に、1つまたは複数の例示的な実施形態を実現するための可能な説明を提供する。本明細書に記載された本発明の精神および範囲から逸脱することなく、要素の機能および配置に様々な変更を加えることができることが理解される。20

【0015】

[0017]以下の説明では、実施形態の完全な理解を提供するために特定の詳細が与えられる。しかしながら、当業者には、これらの具体的な詳細なしに実施形態を実施できることができ理解されるであろう。例えば、本明細書で説明する任意の所与の実施形態において、その実施形態の任意の特定の詳細は、その実施形態の全ての意図されるバージョンに存在しても存在しなくてもよい。同様に、一実施形態に関して説明される任意の詳細は、本明細書で説明する他の実施形態の任意の潜在的なバージョンに存在しても存在していなくてもよい。さらに、本発明の回路、システム、ネットワーク、処理、周知の回路、処理、アルゴリズム、構造、技術、および他の要素は、実施形態を不明瞭にすることを避けるために不必要な詳細なしに論じる可能性がある。30

【0016】

[0018]「機械可読媒体」という用語は、携帯型または固定記憶装置、光学記憶装置、無線チャネル、ならびに命令および／またはデータを記憶、格納、または搬送することができる他の様々な媒体を含むが、これらに限定されない。コードセグメントまたは機械実行可能命令は、プロシージャ、関数、サブプログラム、プログラム、ルーチン、サブルーチン、モジュール、ソフトウェアパッケージ、クラス、または命令、データ構造、もしくはプログラムステートメントの任意の組み合わせを表すことができる。コードセグメントは、情報、データ、引数、パラメータ、またはメモリ内容を渡すおよび／または受け取ることによって、別のコードセグメントまたはハードウェア回路に結合することができる。情報、引数、パラメータ、データなどは、メモリ共有、メッセージパッシング、トーカンパッシング、ネットワーク送信などを含む任意の適切な手段を介して渡され、転送され、または送信され得る。40

【0017】

[0019]さらに、本発明の実施形態は、手動または自動のいずれかで少なくとも部分的に実施することができる。手動または自動実装は、機械、ハードウェア、ソフトウェア、ファームウェア、ミドルウェア、マイクロコード、ハードウェア記述言語、またはそれらの任意の組み合わせの使用を通して実行されるか、または少なくとも支援され得る。ソフト50

ウェア、ファームウェア、ミドルウェア、またはマイクロコードで実装される場合、必要なタスクを実行するプログラムコードまたはコードセグメントは、機械可読媒体に格納することができる。プロセッサは、必要なタスクを実行することができる。

【0018】

[0020]いくつかの実施形態では、ユーザを認証するためのシステムが提供され、システムは、凝視判定デバイスからの情報を利用する。例示的な実施形態では、凝視判定デバイスは、T o b i i (www.tobi.com) または他のサプライヤから市販されているシステムなどの赤外線ベースの視標追跡デバイスである。また、バーチャルリアリティまたは拡張リアリティヘッドセットなどのウェアラブルシステムに組み込まれた視標追跡デバイスを使用することも可能にすることができる。10

【0019】

[0021]広義には、本発明の実施形態は、以下の方法、すなわち、(1)画像センサまたは視標追跡デバイスからの情報を使用して、デバイスの前面に存在するユーザを確認すること、(2)ユーザが顔認識に基づいてデバイスの適切なユーザであることを検証し、ならびに / もしくは凝視および / または眼の情報を受信および分析することによってデバイスの適切なユーザとしてユーザの検証を強化すること、および(3)前のステップからの情報に基づいてユーザを認証することにより、ユーザを認証するシステムに関する。

【0020】

[0022]画像センサによって取り込まれた画像は、ユーザの眼のみで構成されている可能性もあり、ユーザの顔などの余分な情報をさらに含んでいる可能性もある。本発明の明確な目的は、視標追跡デバイスによって捕捉され得る任意の情報の使用を可能にすることである。この情報には、眼の開き、眼の位置、眼の向き、および頭の向きが含まれるが、これらに限定されない。ユーザの顔を含む画像は、ユーザを識別するために、当業者によって容易に理解されるような顔認識アルゴリズムを使用して分析することができる。20

【0021】

[0023]さらに、取り込まれた画像が生きている人に関係していると判定することが有利であるだろう。いくつかの実施形態によれば、これを行う方法の1つは、ユーザの角膜から反射された赤外光の存在について、取り込まれた画像を分析することとできる。赤外線ベースの視標追跡デバイスを使用することにより、ユーザの眼の角膜上に、適切に構成された画像センサを用いて取り込むことができる光が存在し得る。30

【0022】

[0024]取り込まれた画像が生きている人に関するかどうかを判定するさらなる方法は、一連の取り込まれた画像をチェックすることであろう。この一連の取り込まれた画像は、ユーザの凝視点が静的であるか否かを判定するために分析することができる。静止していない凝視点は、一般に生きている人間を示す。本分析は、マイクロサッカードを含む、サッカードおよび / または固定などの、生きている眼の既知の動きを探して特定することさえもできる。

【0023】

[0025]取り込まれた画像が生きている人間に関係するかどうかを判定するさらなる方法は、異なる光源が作動されている間に取り込まれた画像を比較することであろう。例えば、画像センサと同軸に配置された赤外線光源が作動する間に取り込まれた画像は、いわゆる明るい瞳孔効果を有することができ、画像センサと非同軸に配置された赤外線光源が作動する間に取り込まれた画像は、いわゆる暗い瞳孔効果を有する。明るい瞳孔と暗い瞳孔画像との比較を行って、瞳孔の存在を判定することができる。このようにして、偽の瞳孔をシステムに提供することは困難であろう。40

【0024】

[0026]システムが、ユーザが生きており、そのユーザを識別したと判定すると、任意選択的に、人の両眼の少なくとも一方の特徴を定義する個人較正プロファイルをロードすることができる。この較正プロファイルは、ユーザの判定された凝視方向を変更するために使用することができ、例えば、較正プロファイルは、ユーザからの判定された全ての凝視

10

20

30

40

50

方向に適用される標準オフセットを提供することができる。あるいは、較正プロファイルは、ユーザの眼の特性に関するデータ、例えば、眼の光軸に対する眼窩のオフセットまたは眼の角膜曲率に関するデータを含むことができる。次いで、ユーザは、システムにログインすることを望むことを示すディスプレイ上のインジケータを凝視することができ、例えば、「ログイン」を示すボタン、小さな眼の捕捉アイコンなどが適している。

【0025】

[0027]さらなる改善策では、較正プロファイルは、瞳孔間距離、瞳孔サイズ、瞳孔サイズ変動、明るい瞳孔コントラスト、暗い瞳孔コントラスト、および角膜半径などのさらなる情報を含むことができる。この情報は、ユーザが生存しているかどうかを判定するために、較正プロファイルに予め存在していてもよく、または分析時に較正プロファイルに組み込まれっていてもよい。ログイン（認証）プロシージャを実行するために、ユーザは、システムの構成に応じて次のいずれかを実行することができる。10

【0026】

[0028]第1の実施形態では、所定の順序で表示された一連の画像またはテキストを見て、原則的にパターンを凝視する。このパターンは、システムのセットアップ段階中など、以前にユーザによって定義され、割り当てられ、または選択されている。以前に定義されたパターンと現在検出されたパターンとの比較を使用して、ユーザが認証されたかどうかを判定することができる。

【0027】

[0029]第2の実施形態では、移動物体、場合によっては、一連の移動物体の中の単一の移動物体を眼で追う。特定の移動物体は、システムのセットアップ段階中にユーザによって予め定義され、割り当てられ、または選択され、表示された他の物体ではなくその物体をユーザの眼が追った場合にデバイスへのログインを可能にする。20

【0028】

[0030]第3の実施形態では、一連の移動物体の中で所定の順序（システムのセットアップ段階中にユーザが定義、割り当て、または選択した予め定義された順序）で異なる移動物体を凝視する。

【0029】

[0031]第4の実施形態では、所定の物体、画像、または画像の一部（システムのセットアップ段階中にユーザによって定義され、割り当てられ、または選択された所定の物体、画像、または画像の一部）に固定する。30

【0030】

[0032]一連の凝視動作における特定の点は、ユーザの視線が各点上にある時間の点から定義することができる。さらに、シーケンスを完了するのに要した総時間は、シーケンスが正当であるか否かを決定する決定ポイントとして使用することもできる。

【0031】

[0033]ログインプロシージャを開始するための「リセット」機能を含むことが望ましく、これは、ユーザが凝視しなければならない画面上に表示されたアイコンなどとすることができます、そうでなければ、ユーザがログインプロシージャを開始したがっているとシステムに示すために他の方法で作動させることができる。40

【0032】

[0034]本発明のさらなる改良では、「パニック」認証モードをユーザが定義することができる。このモードでは、ユーザは通常の認証シーケンスとは異なる認証シーケンスを設定することができる。この代替シーケンスが入力された場合、コンピューティングデバイスは、表示された機能および情報（銀行口座情報および機密情報など）を制限することなどによってその機能を変更することができ、またはそのコンピューティングデバイスは、警察などの事前に指定された緊急連絡先または信頼できる連絡先と連絡を取ることができる。この連絡は、電子メール、電話、またはテキストメッセージなどを介したものとすることができる。

【0033】

10

20

30

40

50

[0035]前述の認証プロシージャは、コンピューティングデバイスの動作、またはコンピューティングデバイス上で実行されるサービスの識別および／または認証のために使用することができる。例えば、本明細書に記載された識別および認証プロシージャは、ウェブサイトおよびアプリケーションなどを有するユーザを認証するのに適している。

【0034】

[0036]既知の較正プロファイルを有することは、ログインプロシージャには有用であるが、必須ではない。較正プロファイルがロードされていない場合、凝視パターンを画像の既知のレイアウトに一致させるために、いくつかの異なる静的物体ならびに／もしくは1つまたは複数の移動物体の間の凝視パターンを比較することが可能である。いくつかの実施形態では、凝視パターンを同時に使用して、デバイスの較正を作成することができる。

10

【0035】

[0037]いくつかの実施形態では、本システムは、複数の照明源を有する視標追跡デバイスを備えることができる。本システムは、様々な照明源が作動している間に画像が取り込まれるよう視標追跡デバイスを動作させることができ、これにより、取り込まれた画像内の陰影に変化が生じる。この影画像は、より正確な顔認識のためにユーザの顔をモデル化するために使用することができる。この実施形態のさらなる利点は、印刷された画像などの平面画像を使用して実際の人物を偽装することを困難にすることである。これは、そのような印刷画像上の影が証明源の変化に基づいて変化しないためである。

【0036】

[0038]いくつかの実施形態では、3次元頭部姿勢情報を画像センサによって取り込むことができる。この頭部姿勢情報は、一連の画像にわたって変化し、人物が画像センサによって捕捉され、顔認識アルゴリズムによって使用されることを保証するために使用することができる。

20

【0037】

[0039]いくつかの実施形態では、システム内の視標追跡デバイスは、2つ以上の画像センサを備えることができる。2つ以上の画像センサを使用して画像を取り込むことによって、当業者に理解されるように距離マップを作成することができる。この距離マップは、ユーザを識別するために使用することができ、このユーザに対して個別であるとすることができます。取り込まれた画像内のユーザの存在を偽装することをより困難にする。

【0038】

[0040]あるいは、2つ以上の画像センサを使用して画像を取り込むことによって、距離マップを作成する必要無く、人物が単一の時点で複数の角度から撮像されることを確実にし、これらの画像を前記人物の顔および／または少なくとも一方の眼の特定の態様を表す予め記録されたモデルと照合することによって、2つ以上の（おそらく既知の）視点からの画像を使用することができ、したがって、取り込まれた画像内のユーザの存在を偽装することをより困難にすることができます。さらなる改良として、ユーザが認証されてシステムにログインすると、デバイスは、システムのユーザが以前に認証されたのと同じユーザであることを保証するためのプロシージャを定期的に実行することができる。このプロシージャは、取り込まれた画像または一連の取り込まれた画像内のユーザを、認証されたユーザの識別情報と比較するために、本明細書に記載されたものを含むことができる。デバイスのユーザが認証されたユーザではないことをシステムが検出した場合、システムは、以下の動作、すなわち、ユーザに通知する、デバイス上のアプリケーションを閉じる、デバイスの表示からアイテムを削除する、デバイスからログアウトする、デバイスをシャットダウンする、および／または別のシステムもしくは個人に通知メッセージを送信する、の1つまたは複数を実行することができる。

30

【0039】

[0041]いくつかの実施形態では、本明細書に記載のシステムおよび方法のいずれかを使用して、デバイスではなく特定のアプリケーションまたはプログラムにログインすることができる。例えば、MMORPG (Massively Multiplayer Online Roleplaying Game) では、ユーザは、遊ぶことによってコン

40

50

ピュータ／仮想キャラクタの能力および特性を高めるために多大な時間と労力を費やす。本発明は、MMORPG内のキャラクタの所有者または許可されたオペレーターを認証するために使用することができる。もちろん、本発明の実施形態は、任意の形態のゲームまたは他の任意のソフトウェアに適合することができる。

【0040】

[0042]本発明の実施形態は、ユーザの識別と前記ユーザが前記システムの許可されたユーザであるという認証を必要とする任意のシステムでの使用に適しているであろう。そのようなシステムの例には、コンピュータ、ラップトップ、タブレット、携帯電話、従来の地上電話、車両、機械、安全な通路、バーチャルリアリティヘッドセット、および拡張現実ヘッドセットなどが含まれるが、これらに限定されない。

10

【0041】

[0043]本発明のいくつかの実施形態では、認証プロシージャは、バーチャルリアリティまたは拡張現実環境において実行することができる。この環境では、ヘッドセットなどを介して2次元またはシミュレートされた3次元フォーマットでユーザ物体に提示することが可能である。次いで、ユーザは、例えば2次元またはシミュレートされた3次元空間において、環境内の静止物体または移動物体を凝視することによってログインプロシージャを実行することができる。あるいは、ユーザは、環境内の異なる深さの物体に焦点を合わせることができます。ユーザは、ユーザが一意のログインシーケンスとして凝視したいシークエンスまたは物体を定義することができる。後でシークエンスを使用して、デバイスは（本明細書で前述したように）ユーザを認証することができる。

20

【0042】

[0044]いくつかの実施形態では、他のモダリティを凝視と組み合わせて、固有のログインプロシージャを作成することを可能にすることができる。これらのモダリティは、キーボード、マウス、またはタッチパッドもしくはタッチスクリーンなどのタッチベースの接触装置を含むことができる。さらに、モダリティは、3Dジェスチャ、音声、頭部姿勢、またはボタンなどの特定の機械的入力部を含むことができる。ユーザは、同時に別のモダリティを定めながら、ディスプレイ上の特定の物体を凝視すること、または仮想現実／拡張現実環境内で凝視することを必要とするプロシージャを定義することができる。例えば、ユーザは、特定のパスフレーズを話している間、および／または特定のジェスチャを実行している間に、物体を凝視することができる。

30

【0043】

[0045]いくつかの実施形態では、ユーザが生きていることを判定するために、本明細書のシステムは、ユーザの瞳孔の一方または両方の拡張をトリガするイベントを生成することができます。例えば、ディスプレイが非常に暗い状態から非常に明るい状態に、またはその逆に切り替わる可能性がある場合、ユーザの瞳孔の取り込まれた画像を分析して、瞳孔が光強度の変化に反応したかどうかを判定することができる。さらに、イベントのシークエンス、タイプ、またはタイミングが、定期的にまたはセッション間で変更される可能性があり、誰かがシステムをだまし／迂回しようとしている場合に、それを説明することにより困難にする可能性がある。

【0044】

[0046]ユーザのプロファイル、認証プロシージャ、および識別情報などは、コンピュティングデバイス上にローカルに格納され、暗号化されてもよく、またはリモート格納されてローカルデバイスに転送されてもよい。ユーザの画像を取り込む凝視追跡デバイスなどのデバイスは、誰かが認証のためにシステムに予め取り込まれた画像を導入することができる回避策が不可能であるという点で安全でなければならない。

40

【0045】

[0047]本発明のさらなる実施形態では、ユーザの識別は、コンピュータシステムによって収集された他のデータと組み合わせることができる。例えば、視標追跡デバイスなどを使用することによって、本発明によるシステムは、ユーザの注意の対象を判定し、これをユーザの識別情報と組み合わせることができる。説明のために、システムは、以下の方法

50

、すなわち、(a)本発明に従ってユーザが識別され、(b)ユーザの注意の対象が、ユーザの凝視パターンが記録されるのと同時に画面上に表示される情報を反映したデータと組み合わされるユーザの凝視パターンを実行することによって、派生および記録され、(c)ユーザの識別情報がユーザの注意の対象と組み合わされ注意データを定義すること、で機能することができる。

【0046】

[0048]この注意データは、コンピュータシステム上にローカルに、またはリモートサーバ上にリモートに格納することができる。注意データは、同一または異なるユーザの注意データと組み合わせて、情報に対する注意の代表的な見解を判定することができる。

【0047】

[0049]さらに説明するために、本発明のこの実施形態を、可能性のある用途に関連して説明する。視標追跡デバイスを備えたコンピュータシステムは、前述したように、ユーザの凝視に基づいて識別および認証を可能にする。ユーザが識別され、認証されると、視標追跡デバイスは、画面に表示される情報に関連してユーザの凝視方向を判定する。例えば、情報は広告であってもよい。この広告に対するユーザの凝視の要素は、システムによって記録され、要素は、凝視の日時、滞在時間、サッカード方向、および頻度などを含む。これらの要素は、ユーザのIDと識別情報と組み合わされ、システムによって記憶される。ストレージは、コンピュータシステム上にローカルに存在するか、またはインターネットなどを介してリモートサーバに送信される。これは、同じ場所、異なる場所、または異なる広告内の同じ広告について、何度も繰り返すことができる。情報は、広告だけでなく、画像、テキスト、ビデオ、およびウェブページなどを含むことができる、コンピュータシステムによって表示することができる任意の形態とすることができます。

【0048】

[0050]情報の少なくとも2つの項目、または少なくとも2人のユーザからデータが一旦収集される。情報を照合して、代表的なビューを提示することができる。例えば、ユーザの識別情報、すなわち、年齢、性別、および場所などの関連情報を知ることによって、本発明は、様々な情報について「15～19歳の男性の休憩時間」などのレポートを生成することができる。当業者は、ユーザの識別情報と、そのユーザの注意の対象とを組み合わせることによって、情報の多くの組み合わせを収集し、記憶し、分析し、報告することができることを容易に認識するであろう。

【0049】

[0051]本発明のさらなる改良では、本発明によるシステムは、ユーザがコンピューティングデバイスを操作できるように、ユーザを識別および/または認証するために視標または凝視追跡デバイスを利用することができる。認証されると、システムは、凝視追跡デバイスによって取り込まれた情報を連続的に監視し、コンピューティングデバイスの前で認証されたユーザ以外の人の存在について前記情報をチェックすることができる。別人がコンピューティングデバイスの前にいる場合、システムは、一部の情報を、コンピューティングデバイスによって不明瞭にさせるか、または表示させなくすることができる。少なくとも1人の別の個人の識別情報を知る必要はなく、別人がいるという事実だけで十分であろう。このようにして、認証されたユーザ以外の人物がコンピューティングデバイスを見ている場合に、銀行口座情報などの機密情報を隠蔽して保護することができる。認証されたユーザは、ソフトウェアオーバーライドを通じてこの機能を無効にするか、または本発明もしくは任意の他の既知の識別および認証プロシージャを使用して追加の人物を識別および認証することを選択することができる。

【0050】

[0052]本発明は、頭の動き、まばたきの頻度、サッカードなどの眼の動き、眼の開放度、瞳孔の直径、眼の向き、および頭の向きを含むがこれらに限定されない行動的バイオメトリクスを識別および収集することができる。この情報は、ユーザの識別および認証中に収集することができ、また、ユーザがコンピューティングデバイスを使用している間も継続して収集することができる。この情報の一部または全部は、後でユーザを識別し認証す

10

20

30

40

50

るためのプロファイルの形式で保存することができる。

【0051】

[0053]さらに、本発明によれば、ユーザがコンピューティングデバイスで識別および認証され、そのユーザがコンピューティングデバイスから遠ざかると、コンピューティングデバイスに戻ったときにユーザを再認証する必要が生じる可能性がある。これを実施するために、認証されたユーザが再認証を返さない場合、再認証が必要であるが、時間が超過された場合、再認証が必要となる期間を定義することができる。さらに、システムは、以前に記述された行動バイオメトリックを使用して戻ってきたユーザを識別することができ、システムが新しいユーザを認証されたユーザと異なる識別情報または認識されない識別情報として識別する場合、再認証プロシージャに従わなければならない。

10

【0052】

[0054]関連して、ユーザが本発明に従って識別および認証され、ユーザが所定の期間、コンピューティングデバイスの使用を中止すると、コンピューティングデバイスは「ロック」モードに入ることができる。コンピューティングデバイスのロックを解除するには、移動物体を追うことなどの簡単な手順を使用することができる。

【0053】

[0055]本発明のさらなる改良では、システムは、ユーザの状態を判定するために凝視追跡装置によって収集された情報を使用することができる。例えば、システムは、ユーザの環境における明るさのレベル、コンピューティングデバイスのディスプレイから放射される明るさのレベルを判定し、ユーザの予想される瞳孔サイズを計算することができる。また、システムは、代わりに、特定のユーザの瞳孔サイズに関する履歴情報を使用してもよい。次いで、システムは、ユーザの瞳孔サイズに基づいてユーザの精神状態を判定することができる。例えば、拡大された瞳孔は、驚いた状態もしくは興奮した状態、または心変わりさせる者が存在することすらも示すことができる。

20

【0054】

[0056]凝視または眼の情報への本発明の任意の言及は、場合によっては、ユーザの頭部に関する情報に置き換えてよい。例えば、解像度はそれほど高くない可能性が高いが、頭の向き情報のみを使用してユーザを識別し、認証することが可能である可能性がある。これは、さらに、ユーザの顔の表情、まばたき、ウィンク様の動作などに及ぶ可能性がある。

30

【0055】

[0057]本発明は、画像センサを備える視標追跡デバイスを有するコンピューティングデバイスを参照して説明されているが、そのようなシステムは多くの形態で存在することが理解されるべきである。例えば、視標追跡デバイスは、ディスプレイまたはコンピューティングデバイスを直接的に制御するために必要な全ての計算能力を含むことができる。例えば、視標追跡デバイスは、本発明で要求される必要なアルゴリズム判定の全部または一部を実行することができる特定用途向け集積回路（ASIC）を含むことができる。

【0056】

[0058]図1は、デバイスのユーザを認証するための本発明の一実施形態の1つのシステム100のブロック図である。上述したように、システムは、第1の画像センサ110、第2の画像センサ120、判定ユニット130、認証ユニット140、プロファイルユニット150、および（ユーザが認証されようとしている）デバイス160を含むことができる。構成要素間の通信チャネルは、様々な構成要素の間の線として示されているが、当業者であれば、構成要素間の他の通信チャネルが存在し、この特定の例では示されない可能性があることを理解されよう。

40

【0057】

[0059]図2は、デバイスのユーザを認証するための本発明の一実施形態の1つの方法200のブロック図である。上述のように、本方法は、ステップ210において、第1の画像センサで画像を取り込むステップを含むことができる。ステップ220では、第2の画像センサで画像を取り込むことができる。ステップ230では、画像からユーザの眼に関

50

する情報を判定することができる。ステップ240では、前に取得した情報および判定に基づいて、ユーザが生きているかどうかを判定することができる。ステップ250では、前に取得した情報および判定に基づいて、ユーザを認証するかどうかを判定することができる。ステップ260において、ユーザプロファイルは、ユーザの認証に基づいてロードすることができる。

【0058】

[0060]図3は、本発明の実施形態を実施することができる例示的なコンピュータシステム300を示すブロック図である。この例は、本明細書で説明するシステムまたは装置のいずれかの機能を提供するために、全体的に、部分的に、または様々な変更を伴って使用され得るようなコンピュータシステム300を示す。例えば、視標追跡デバイスの様々な機能は、単に例として、凝視追跡および顔面特徴の識別などを含み、コンピュータシステム300によって制御することができる。10

【0059】

[0061]コンピュータシステム300は、バス390を介して電気的に結合することができるハードウェア要素を備えるように示される。ハードウェア要素は、1つまたは複数の中央処理装置310、1つまたは複数の入力装置320（例えば、マウス、キーボードなど）、ならびに1つまたは複数の出力装置330（例えば、表示装置、プリンタなど）を含むことができる。コンピュータシステム300はまた、1つまたは複数の記憶装置340を含むことができる。一例として、記憶装置340は、プログラム可能および／またはフラッシュ更新可能とすることができる、ディスクドライブ、光記憶装置、ランダムアクセスメモリ（RAM）および／または読み出し専用メモリ（ROM）などのソリッドステート記憶装置とすることができます。20

【0060】

[0062]コンピュータシステム300は、コンピュータ可読記憶媒体リーダ350、通信システム360（例えば、モデム、ネットワークカード（無線または有線）、赤外線通信デバイス、Bluetooth（登録商標）デバイス、セルラ通信デバイスなど）、ならびに上記のようなRAMおよびROM装置を含むワーキングメモリ380とをさらに含むことができる。いくつかの実施形態では、コンピュータシステム300は、デジタル信号プロセッサおよび／または専用プロセッサなどを含むことができる処理加速ユニット370も含むことができる。30

【0061】

[0063]コンピュータ可読記憶媒体リーダ350はさらに、コンピュータ可読情報を一時的および／またはより永続的に含むためのリモート、ローカル、固定、および／またはリムーバブル記憶装置プラス記憶媒体を包括的に表すコンピュータ可読記憶媒体に（および、任意選択的に、記憶装置340と組み合わせて）接続することができる。通信システム360は、データが上記のネットワーク、システム、コンピュータ、および／または他の構成要素と交換されることを可能にすることができます。

【0062】

[0064]コンピュータシステム300はまた、オペレーティングシステム384および／または他のコード388を含む、ワーキングメモリ380内に現在位置するものとして示されるソフトウェア要素を備えることができる。コンピュータシステム300の代替実施形態は、上述のものから数多くの変形を有し得ることを理解されたい。例えば、カスタマイズされたハードウェアを使用してもよく、および／または特定の要素がハードウェア、ソフトウェア（アプレットなどのポータブルソフトウェアを含む）、またはその両方で実装されてもよい。さらに、ネットワーク入力／出力デバイスおよびデータ取得デバイスなどの他のコンピューティングデバイスへの接続もまた起こる可能性がある。40

【0063】

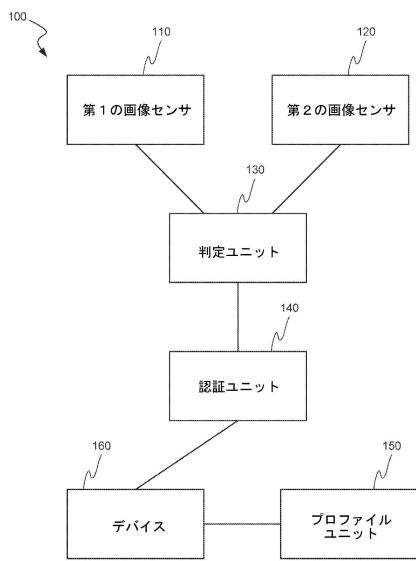
[0065]コンピュータシステム300のソフトウェアは、本明細書で説明されるアーキテクチャの様々な要素の機能のいずれかまたは全てを実装するためのコード388を含むことができる。例えば、システム300などのコンピュータシステムに記憶され、および／50

または実行されるソフトウェアは、上述したような視標追跡デバイスおよび／または本発明の他の構成要素の機能を提供することができる。これらの構成要素のいくつか上でソフトウェアによって実現可能な方法については、詳細に上記した。

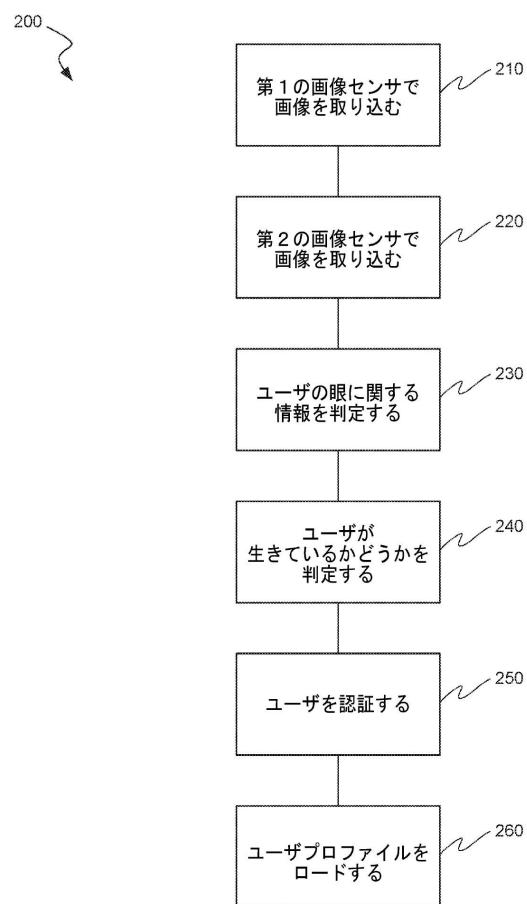
【 0 0 6 4 】

[0066]本発明は、明瞭化および理解のために詳細に記載されている。しかしながら、添付の特許請求の範囲の範囲内である種の変更および修正を実施できることは理解されよう。

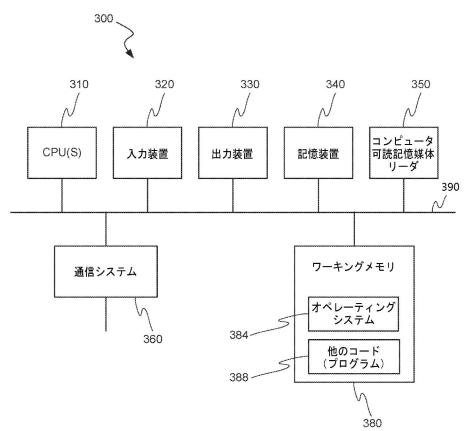
【 図 1 】



【 図 2 】



【図3】



フロントページの続き

(72)発明者 ハインツ , リチャード
スウェーデン , ストックホルム 182 53 , ダンダイド , 7ティーアール , カールスロヴァー
ゲン 2ディー

(72)発明者 ジエンソン , ヘンリック
スウェーデン , ストックホルム 182 53 , ダンダイド , 7ティーアール , カールスロヴァー
ゲン 2ディー

(72)発明者 ヴェンストレム , アンダース
スウェーデン , ストックホルム 182 53 , ダンダイド , 7ティーアール , カールスロヴァー
ゲン 2ディー

(72)発明者 ジョージ 斯ヴァン , アーランド
スウェーデン , ストックホルム 182 53 , ダンダイド , 7ティーアール , カールスロヴァー
ゲン 2ディー

(72)発明者 エルヴェスジエ , ジョン
スウェーデン , ストックホルム 182 53 , ダンダイド , 7ティーアール , カールスロヴァー
ゲン 2ディー

審査官 新井 則和

(56)参考文献 特開2015 - 013031 (JP, A)
特表2014 - 534655 (JP, A)
特開2008 - 198028 (JP, A)
米国特許出願公開第2014 / 0313129 (US, A1)

(58)調査した分野(Int.Cl. , DB名)

G 06 T 7 / 00
A 61 B 3 / 113
A 61 B 5 / 1171
G 06 F 21 / 32