(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2015-529365
(P2015-529365A)
(43)公表日　平成27年10月5日(2015.10.5)

| (51)Int.Cl. | | F I | | | テーマコード（参考） |
|---|---|---|---|---|---|
| G06T 7/00 | (2006.01) | G06T | 7/00 | 510B | 5B043 |
| G06F 21/32 | (2013.01) | G06T | 7/00 | 300F | 5L096 |
| G06F 21/31 | (2013.01) | G06F | 21/32 | | |
| | | G06F | 21/31 | | |

審査請求 未請求　予備審査請求 未請求　（全 21 頁）

(21)出願番号　特願2015-531210 (P2015-531210)
(86)(22)出願日　平成25年9月5日 (2013.9.5)
(85)翻訳文提出日　平成27年4月9日 (2015.4.9)
(86)国際出願番号　PCT/US2013/058343
(87)国際公開番号　WO2014/039732
(87)国際公開日　平成26年3月13日 (2014.3.13)
(31)優先権主張番号　61/696,820
(32)優先日　平成24年9月5日 (2012.9.5)
(33)優先権主張国　米国 (US)

(71)出願人　515061787
エレメント，インク．
アメリカ合衆国　１００１２　ニューヨーク州　ニューヨーク　エフエル．４　グリーン・ストリート　７２
(74)代理人　100082072
弁理士　清原　義博
(72)発明者　ルカン，ヤン
アメリカ合衆国　０７７８３　ニュージャージー州　リンクロフト　ハワード・コート　１２
(72)発明者　ペロルド，アダム
アメリカ合衆国　１００１４　ニューヨーク州　ニューヨーク　ナンバー２エフ　ウエスト・４番ストリート　２７１

最終頁に続く

(54)【発明の名称】カメラ付きデバイスに関連する生体認証のためのシステム及び方法

(57)【要約】
本発明は全体的に、認証と識別のための生体測定技術の使用に関するものであり、より具体的には、様々なリソースへのアクセスを選択的に容認又は拒否するために、モバイルデバイスなどのコンピュータを介してユーザーを認証及び識別するための、非接触ベースの解決策に関する。本発明において、認証及び／又は識別は、以下の主な工程：（１）ローカル分類器を使用して掌領域を検知する工程；（２）関心領域から特徴を抽出する工程；及び（３）学習プロセスを通じてダイナミックに増大し得る、データベースに保存したユーザーモデルに対するマッチングスコアを計算する工程を含むプロセスを通じて、個人の掌の画像又は画像のセットを使用して行われる。
【選択図】図１

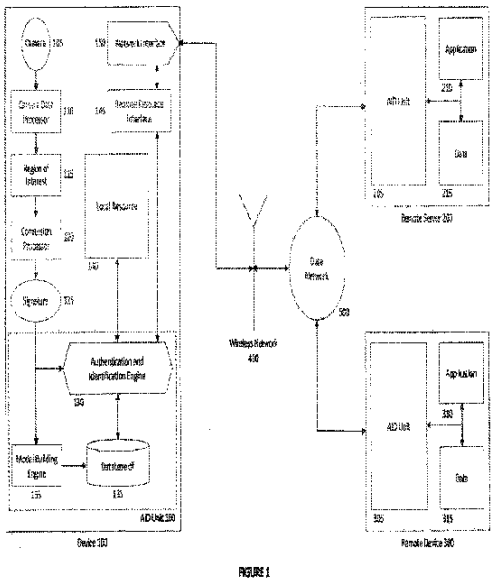


FIGURE 1

【特許請求の範囲】
【請求項１】
適切なコンピュータハードウェア上で実行されるソフトウェアを含むデバイスに関連して利用可能なリソースへの選択的なアクセスを提供するためのシステムであって、該システムは：
（ａ）ヒトの掌紋の少なくとも１つの写真を撮影することができる、前記デバイスに関連する少なくとも１つのカメラ；
（ｂ）物理的に接触することなく掌の関心領域を位置付け且つ分けるためにローカル分類器を使用する検出器モジュール；
（ｃ）ヒトの掌紋の前記対象領域に関連する未加工のピクセルデータを前記掌紋に関連した固有の署名へと変換する、変換プロセッサ；及び
（ｄ）認証及び識別のエンジンであって、該認証及び識別のエンジンは、前記リソースの１以上へのアクセスが、前記固有の署名、及び、複数のユーザーモデルを含む少なくとも１つのデータベースに基づいて認められるべきか否かを定める、認証及び識別のエンジン、
を備えることを特徴とするシステム。
【請求項２】
新たなデータを持つユーザーモデルを改良する学習プロセッサを更に備え、ここで、該学習プロセッサは、前記データベースと、前記認証及び識別のエンジンを増大するために前記掌紋画像を選択的に含む、ことを特徴とする請求項１に記載のシステム。
【請求項３】
前記デバイスはモバイルデバイスである、ことを特徴とする請求項１に記載のシステム。
【請求項４】
前記デバイスはデスクトップデバイスである、ことを特徴とする請求項１に記載のシステム。
【請求項５】
前記デバイスは固定式埋込デバイスである、ことを特徴とする請求項１に記載のシステム。
【請求項６】
前記デバイスは、画像捕捉時に選択的に起動して、関心領域の検知、特徴抽出、及びヒトの掌画像の署名処理に十分な最小限の光を提供する、フラッシュ構成要素を備える、ことを特徴とする請求項１に記載のシステム。
【請求項７】
前記変換プロセッサは、関心領域上のパッチから抽出されるディスクリプタを使用する、ことを特徴とする請求項１に記載のシステム。
【請求項８】
前記ディスクリプタは高次元のスパースベクトルへとコード化される、ことを特徴とする請求項１に記載のシステム。
【請求項９】
前記スパースベクトルは少なくとも１つのグループに溜められる、ことを特徴とする請求項1に記載のシステム。
【請求項１０】
前記署名は、１つのＢａｇ ｏｆ Ｆｅａｔｕｒｅｓ又は複数のＢａｇ ｏｆ Ｆｅａｔｕｒｅｓの表示から計算される、ことを特徴とする請求項１に記載のシステム。
【請求項１１】
前記検出器モジュールは、Ｈａａｒウェーブレット及びＡｄａＢｏｏｓｔアルゴリズムを使用する、ことを特徴とする請求項１に記載のシステム。
【請求項１２】
前記検出器モジュールはサポートベクトルマシンを使用する、ことを特徴とする請求項

１に記載のシステム。
【請求項１３】
前記検出器モジュールは畳み込みニューラル・ネットワークを使用する、ことを特徴と請求項１に記載のシステム。
【請求項１４】
前記ユーザーモデルは、ヒトの掌画像の収集から計算された統計モデルである、ことを特徴とする請求項１に記載のシステム。
【請求項１５】
前記ユーザーモデルはガウス密度モデルである、ことを特徴と請求項１に記載のシステム。
【請求項１６】
前記ユーザーモデルはガウス密度モデルの組み合わせである、ことを特徴とする請求項１に記載のシステム。
【請求項１７】
前記リソースの少なくとも１つはデバイスから離れている、ことを特徴とする請求項１に記載のシステム。
【請求項１８】
前記リソースの少なくとも１つはデバイス上にある、ことを特徴とする請求項１に記載のシステム。
【請求項１９】
前記リソースの前記少なくとも１つはアプリケーションである、ことを特徴とする請求項１に記載のシステム。
【請求項２０】
前記リソースの前記少なくとも１つはデータベースである、ことを特徴とする請求項１に記載のシステム。
【請求項２１】
人の両方の掌紋画像の各々の各署名は、利用可能であれば、ヒトの認証又は識別のために共に利用される、ことを特徴とする請求項１に記載のシステム。
【請求項２２】
掌紋認証又は識別は他の形態と組み合わせられる、ことを特徴とする請求項１に記載のシステム。
【請求項２３】
前記他の形態は、パスコード、セキュリティ質問、指紋認識、顔認識、虹彩認識、手書署名認識、及び他の生体認証並びに非生体認証の形態の１以上を含む、ことを特徴とする請求項２１に記載のシステム。
【請求項２４】
アプリケーションが、１以上のユーザーが１以上のトランザクションを行なうことを選択的に可能にする、ことを特徴とする請求項１に記載のシステム。
【請求項２５】
ヒトの掌のフラッシュ画像及び非フラッシュ画像のシーケンスが、提示された手が手の３Ｄ対象又は２Ｄ表示であるかを定めるための反スプーフィング機構の一部として使用される、ことを特徴とする請求項１に記載のシステム。
【請求項２６】
ヒトの掌の動作中に捕捉した画像データが、提示された手が手の３Ｄ対象又は２Ｄ表示であるかを定めるための反スプーフィング機構の一部として使用される、ことを特徴とする請求項１に記載のシステム。
【請求項２７】
ヒトの掌のフラッシュ画像及び非フラッシュ画像のシーケンス、同様に一連の画像間の時間間隔は、反スプーフィング機構の一部として利用され、認証又は識別のために前に記録した画像のシーケンスを利用しようと相手が試みているかどうかを定める、ことを特徴

とする請求項１に記載のシステム。
【請求項２８】
前に使用したヒトの画像の全ては、認証又は識別のために前に記録した画像のシーケンスを利用しようと相手が試みているかどうかを定める反スプーフィング機構の一部として、新しい画像と比較するために保存される、ことを特徴とする請求項１に記載のシステム。
【請求項２９】
トランザクション情報又は他のデータが、認証又は識別のために設けられる画像シーケンスがトランザクション自体からの情報に一致するかどうかを定める反スプーフィング機構の一部として、画像及び／又はフラッシュパターンのシーケンスのタイミング内に埋め込まれる、ことを特徴とする請求項１に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
＜関連出願への相互参照＞
本出願は、２０１２年９月５日出願の米国仮特許出願第６１／６９６，８２０号の出願日の利益を信頼及び主張するものであり、その全体の開示は、引用により本明細書に組み込まれる。
【背景技術】
【０００２】
＜発明の分野＞
本発明は全体的に、認証と識別のための生体測定技術の使用に関するものであり、より具体的には、様々なリソースへのアクセスを選択的に容認又は拒否するために、モバイルデバイスなどのコンピュータを介してユーザーを認証及び識別するための、非接触ベースの解決策に関する。本発明において、認証又は識別は、以下の主な工程：（１）ローカル分類器を使用して掌領域を検知する工程；（２）関心領域から特徴を抽出する工程；及び（３）学習プロセスを通じてダイナミックに増大し得る、データベースに保存したユーザーモデルに対するマッチングスコアを計算する工程を含むプロセスを通じて、個人の掌の画像又は画像のセットを使用して行われる。
【０００３】
＜関連技術の議論＞
スマートフォン、タブレット、及びノートブックなどのモバイルデバイスが、日常的に多くの人々によって広く取り入れられ、且つ使用されるようになった。これらデバイスは、ますます有力なものとなり、該デバイスで作動する、ますます多くのアプリケーションとサービスを開発者が作成したため、前記デバイスにより我々の日常生活はより豊かなものとなった。これらモバイルデバイスは、それ自体で有力なコンピューティング・プラットフォームを提供するだけでなく、セルサイトへの無線リンクを介して典型的にアクセスされ、その後でインターネットバックボーンに返送される（ｂａｃｋｈａｕｌｅｄ）、リモートプラットフォーム上で利用可能なサービス、アプリケーション、及びデータの事実上無制限のセットに連結性を提供する。これらリモートプラットフォームへのアクセスに加えて、モバイルデバイスはまた、短い且つ長い範囲の無線接続を通じて、他のモバイルデバイスに接続する能力を備える。
【０００４】
恐らく最も重要なことに、これらデバイスの構成部品に関連する費用の削減が進むと共に、これらのデバイスの浸透が絶えず増加していくことで、結果として、より大きな性能で利用可能となる一方で多くのユーザーにとって未だに手頃なままであるデバイスが、もたらされた。例えば、構成部品の費用の削減及びより有力なソフトウェアの開発の結果、相当な数のスマートフォンが現在、約８メガピクセル以上で非常に詳細な写真を撮ることができる、高性能カメラを備える。
【０００５】

モバイルデバイスのコンテキスト、非常に多くの機能性に関連する広範囲の使用、及び非常に多くの異なるリソースと相互に作用するための必要性に生じる、１つの重要な問題は、適用可能なリソースにアクセスする権限が与えられるべき個人又はデバイスのみが実際にアクセスできるように、これらのリソースの各々へのアクセスを制御する必要があるということである。典型的な場合において、リソースのアクセスは、ユーザーＩＤとパスワードなどのテキスト／数字列の入力を通じて制御される。例えば、スマートフォンのユーザーは、自身がデバイス上の任意の機能性にアクセスすることを容認される前に、４桁のコードを入力する必要があり得る。加えて、デバイス上の各ローカルアプリケーション又は他のリソースは、リソースへのアクセスを得る前に１以上のテキスト／数字列を入力することをユーザーに要求する場合がある。この場合、正しいデータ（ユーザーＩＤ、パスワード等）は、デバイスのメモリに保存され得る。代替的に、デバイスから離れて位置づけられるリソース（アプリケーション、データ、通信容量等）へのアクセスのために、ユーザー及び／又はデバイスは、リソースへのアクセスを容認する前に送信データが正確なデータに一致することを次々に確認する、リモートリソースへのテキスト／数字列の正確なセットを送信することを要求される場合がある。

【０００６】

想像されるように、典型的なスマートフォンのユーザーに関して、例えば、認証と識別のための前述の技術には多くの短所が存在する。その１つとして、ＩＤとパスワードがどのように構築されねばならないかに関する必要条件を各々が持つ、非常に多くの異なるアプリケーション、サービス、及び他のリソース用のユーザーＩＤとパスワードを記憶する必要性は、かなり厄介なものであり得、ユーザーは大抵、常習的にアクセスしないリソースのＩＤとパスワードを忘れてしまう。別の欠点は、リソースへのアクセスを制御するためにテキスト／数字列を使用することによるセキュリティ上の懸念が存在する、ということである。例えば、これらの列をハッキングしてリソースへの無許可のアクセスを獲得するために使用され得る、有力なソフトウエアプログラムが存在する。

【０００７】

また、スマートフォンの画面上でパスワードとユーザーＩＤを入力するためにユーザーが指を使用するという、典型的な接触ベースの方法は、セキュリティ上の危険に結び付く。経験を積んだハッカーは大抵、無許可のアクセスを獲得するために、指によって残された油の残留物に基づいて、画面から指紋パターンを「盗む（ｌｉｆｔ）」ことができる。このことは、デバイスをアンロックするために４桁の数字などの短い数字列を入力するという状況では、特に真実である。一旦デバイスがアンロックされると、デバイス上のリソースの多くは、更に確保されず、このことが深刻なセキュリティ上の危険に通じる場合がある。

【０００８】

上に議論された欠点を排除するか減らすために標的とされた１つの解決策は、モバイルデバイスを介して利用可能なリソースへのアクセスを制御する生体測定技術の使用を含む。これら解決策は、幾つかの場合において、上に議論された欠点の幾つかを排除した一方で、前記解決策は未だに、多くの欠点に悩んでいる。例えば、接触ベースの解決策の中には、デバイスセンサー上に自身の指を置くことを、ユーザーに要求するものもあり、該デバイスセンサーは、ユーザーの指紋を捕捉して、その後、ユーザー又はデバイスが１以上のリソースにアクセスするのを可能にするのに十分な一致が存在するかどうかを判定するために、ローカルに（ｌｏｃａｌｌｙ）又は離れて位置付けられた指紋データに対して指紋を一致させるための能力を備える。この場合、上に言及されるように、指紋は、ハッカーによってデバイスセンサーから盗まれ、且つ、その適切な指紋を利用して後に１以上のリソースへの無許可のアクセスを獲得するために使用され得る。これら解決策はまた、典型的に、指紋が一致するかどうかを判定するのに必要な処理を実行する時間が、忙しいユーザーが普段の１日の流れの中でデバイス上の多くの異なるリソースへのアクセスを得ようとする状況では、受け入れられないこともあるという欠点に悩んでいる。

【０００９】

特にユーザー間で共有されたデバイスの場合において、細菌、ウィルス、又は他のバイオ・ハザードの伝達を含む接触ベースの方法に関連する、付加的な健康に関する問題が存在する。当該技術分野で既知であるように、個人の指先、より一般的には個人の手は大抵、人々の間で細菌、ウィルス、又は他のバイオ・ハザードを伝達する主な媒介物の１つである。複数の人々の間で共有される個別デバイスの場合、ユーザーが自分の指先で識別用の文字列をタイプし、又はとりわけ指紋又は掌紋の認識などの接触ベースの生体認証方法を通じて自分を認証又は識別する、認証と識別の接触ベースの方法は、共有の接触媒介物を介して前記バイオ・ハザードを伝達する危険性を引き起こす。

【発明の概要】

【課題を解決するための手段】

【００１０】

このため、本発明の目的は、ユーザー及びデバイスの正確で安全且つ迅速な認証及び識別をサポートすることで、カメラ付きデバイスを通じてアクセス可能なリソースへの選択的なアクセスを提供する、非接触ベースの生体認証システム及び方法を提供することである。

【００１１】

本発明の１つの実施形態において、１以上のリソースへのアクセスを得る条件として自身を識別又は認証することを要求される、前記カメラ付きデバイス（以下、時に便宜上「スマートフォン」と称されるが、前記デバイスは、モバイルデバイス及びデスクトップコンピュータ等の固定式デバイスの両方を含む、カメラ機能を備える全てのデバイスを含むものと理解される）のユーザーは、スマートフォンのカメラを使用して片方又は両方の掌の１以上の連続した写真を撮る。その後、本発明のシステムは、コンピュータビジョン技術を使用して掌紋画像を解析し、掌紋の署名がデータベースに一致することを確認するか（ユーザー認証）、又はデータベース中の多くのモデルの中で一致するユーザーのモデルを見つけ出す（ユーザー識別）。

【００１２】

本発明の更なる特徴及び態様は、添付の図面への言及に関連する、典型的な実施形態の以下の詳述から明白となるであろう。

【図面の簡単な説明】

【００１３】

【図１】好ましい実施形態における本発明のシステムの主な構成要素を描く略図である。

【図２】好ましい実施形態における本発明の方法を示すのに有用なブロック図である。

【図３】本発明の好ましい実施形態に従った、モバイルデバイスと１以上のリモートサーバーとの間の安全な連結性を示す略図である。

【図４】好ましい実施形態における本発明に従った、ユーザー又はデバイスを認証する際の重要な工程を示すフローチャートである。

【図５】好ましい実施形態における本発明に従った、ユーザー又はデバイスを識別する際の重要な工程を示すフローチャートである。

【発明を実施するための形態】

【００１４】

ここで、本発明の様々な典型的な実施形態に対する言及を詳しく行う。典型的な実施形態についての以下の議論は、本明細書に広く開示されるように、本発明を限定するものとしては意図されないことを、理解されたい。むしろ、以下の議論は、本発明の特定の態様及び特徴のより詳細な理解を読者に与えるために提供される。

【００１５】

本発明の実施形態を詳細に記載する前に、本明細書で使用した用語は、特定の実施形態のみについて記載するためのものであり、限定するようには意図されないことを、理解されたい。他に定義されない限り、本明細書で用いる全ての専門用語は、その用語の属する技術分野の当業者によって一般に理解されるものと同じ意味を持つ。本明細書に記載されるものと同様の、又はそれらに等しい任意の方法及び題材が、本発明を実施する際に使用

され得るが、好ましい方法及び材料がここで記載される。本明細書で言及される全ての刊行物は、該刊行物が引用されるものに関連する方法及び／又は題材を開示及び記載するために、引用により本明細書に組み込まれる。本開示は、任意の組み込まれた刊行物と衝突する程度まで統制している。

【００１６】

本明細書及び添付の請求項において使用されるように、単数形「ａ」、「ａｎ」及び「ｔｈｅ」は、文脈が明確に別段の規定をしていない限り、複数の指示対象を含む。故に、例えば、「掌」への言及は、個人の片方又は両方の掌を含み、及び「画像」への言及は、１以上の画像への言及を含む。更に、同義語を使用して記載され得る用語の使用は、それらの同義語の使用を含む。故に、例えば、用語「カメラ」の使用は、対象の画像を得ることができる任意のデバイスを含むと理解される。別の例として、及び上に言及されるように、用語「スマートフォン」は、カメラ機能を備えた全てのデバイスを含む。

【００１７】

好ましい実施形態における本発明の記載が、ここで随伴する。図１に関して、本発明のシステムの重要な構成要素の議論が、これら構成要素の各々が本発明の利点を得るために互いに相互作用するコンテキストと同様に、ここで随伴する。デバイス（１００）は、高画質の写真を撮ることができるカメラを備える任意のデバイスでもよい。好ましくは、デバイス（１００）のカメラはまた、撮影される領域を照らすために選択的且つ急速に起動及び停止することができるフラッシュ素子を含む。前記デバイス（１００）の例は、スマートフォン、タブレットコンピュータ、ノートブック、又は、ユーザーが持ち運ぶことができ、且つ本発明の機能性が有効となるのを可能にするコンピューティング・プラットフォームを提供する他のデバイス、同様に、デスクトップコンピュータ又は様々な固定式埋込デバイスを含む。前記固定式埋込デバイスの例は、フィジカルスペース又は他のリソースへの安全なアクセスを提供する、設備通路（ｆａｃｉｌｉｔｙ　ｅｎｔｒｙｗａｙｓ）又は他の戦略的な位置に固定されるカメラ機器、又は、時間及び随伴（ａｔｔｅｎｄａｎｃｅ）のプロトコルなどの目的のために戦略的な位置に固定されるカメラ機器、同様に他のアプリケーションを含む。必要とされないが、デバイス（１００）はまた、（タッチスクリーンでもある）ビューイングスクリーン（ｖｉｅｗｉｎｇ　ｓｃｒｅｅｎ）、キーパッド、加速度センサー、ＧＰＳ機能、記憶容量、及び中央処理装置（ＣＰＵ）などの様々な他の機能を備え得る。

【００１８】

デバイス（１００）は少なくとも１つのカメラ（１０５）を含み、該カメラは好ましくは、例えば、４メガピクセル、６メガピクセル、又は８メガピクセルなど、２メガピクセル以上の高品質写真を作り出すことができる。カメラデータ処理装置（１１０）は、カメラ（１０５）から画像データを受け取り、それを当該技術分野で既知のように処理して、現在記載されるように本発明に関連して概説される目的を含む様々な方法で使用され得る、写真を表わすピクセルデータを作る。カメラデータ処理装置（１１０）からのデータは、広範囲の画像内に掌の領域を位置付ける役目を果たす関心検知器領域（１１５）に送り込まれ、略同形状の掌領域のマスクを提供する及び異なる発光状態とカメラに対する掌の配向により様々な独立画像を通じて掌上に置くなどのために、高レベルの精密度と整合性で領域を描く。

【００１９】

関心検知器領域（１１５）の１つの実施形態において、関心領域は、分類スコアにより、その後の入力画像の接続構成要素に近隣の掌のピクセルを集める区分工程により、掌及び非掌のピクセルにラベル付けするスライディングウィンドウベースのローカル分類器を使用して、検知される。画像ノイズに対する高レベルの精度とロバスト性が達成され得るのは、相当数の識別力のあるローカル特徴が、強力な分類器を形成する掌の外観の安定特性を捕捉するために典型的な画像の大規模な収集から学習するためである。その結果、訓練した検知器は、様々な手の配向と発光状態により、自由形式で得た入力画像上に関心領域を正確に位置付け、且つ描くことができる。

【００２０】
関心検知器領域（１１５）の１つの実施形態において、Ｈａａｒ Ｗａｖｅｌｅｔｓ ａｎｄ ＡｄａＢｏｏｓｔ（参照例１）に基づくローカル分類器は、ユーザーの手の掌領域において関心領域を検知するために使用される。関心検知器領域（１１５）の別の実施形態において、ｓｕｐｐｏｒｔ ｖｅｃｔｏｒ ｍａｃｈｉｎｅ（参照例２）に基づくローカル分類器は、ユーザーの手の掌領域において関心領域を検知するために使用される。関心検知器領域（１１５）の別の実施形態において、米国特許第５，０６７，１６４号及び第５，０５８，１７９号（参照例３と４）に記載されるものなどの、畳み込みニューラル・ネットワークが、ユーザーの手の掌領域において関心領域を検知するために使用される。

【００２１】
その後、関心検知器領域（１１５）は、個人と別のユーザーを区別するために使用され得る個人の掌領域の特性を表わす画像パッチから署名（１２５）を抽出する役目を果たす、変換プロセッサ（１２０）に、掌領域のマスクを含む画像データを送り、ここで、前記パッチは、掌領域のマスク内の小さなサンプリング窓である。

【００２２】
１つの実施形態において、署名（１２５）は以下のように計算されたベクトルである。第１に、画像中の多くの適切に選択した領域におけるエッジ配向（ｅｄｇｅ ｏｒｉｅｎｔａｔｉｏｎｓ）のヒストグラムが計算される。この計算は、Ｓｃａｌｅ Ｉｎｖａｒｉａｎｔ Ｆｅａｔｕｒｅ Ｔｒａｎｓｆｏｒｍ（ＳＩＦＴ）（例えば、参照例５を参照）、Ｈｉｓｔｏｇｒａｍ ｏｆ Ｏｒｉｅｎｔｅｄ Ｇｒａｄｉｅｎｔｓ（ＨＯＧ）（例えば、参照例６を参照）、及び当該技術分野で既知の他の引用文献など、ローカル画像ディスクリプタを抽出するためのコンピュータビジョンの周知の方法の１つを使用して、実行され得る。第２に、各配向ヒストグラムが、例えば周知のＫ平均法アルゴリズム（Ｋ－ｍｅａｎｓ ｃｌｕｓｔｅｒｉｎｇ ａｌｇｏｒｉｔｈｍ）を使用して、訓練データから計算した多くのプロトタイプと比較される。最終的に、署名ベクトルは、ベクトルの成分ｋが前述のｋ－ｔｈのプロトタイプに相当するように形成される。成分ｋは、ヒストグラムが他の全てのプロトタイプよりもプロトタイプｋに近い、領域の数を含む。この操作の列は、「Ｂａｇ ｏｆ Ｆｅａｔｕｒｅｓ」の表示として参照例において知られている（例えば、参照例７を参照）。本発明の別の実施形態において、複数のＢａｇ ｏｆ Ｆｅａｔｕｒｅｓがローカル領域間の幾何学的関係を維持するために使用され得ることは、現在の教示内容から明らかとなるはずである。

【００２３】
その後、署名（１２５）は、以下に述べられるような本発明の重要なプロセスの多くを示唆する役目を果たす、認証と識別のエンジン（ＡＩＤエンジン）（１３０）に送り込まれる。ＡＩＤエンジン（１３０）は、ユーザーモデル（１３５）のローカルコピーを保存するために、存在する場合にユーザーモデルのデータベースと通信する。故に、デバイス（１００）上にローカルに存在し、且つ、例えばリモートサーバー又はリモートデバイスとの外部通信を必要としないアプリケーション又はサービスの場合、カメラ（１０５）によって得た掌紋画像から結果として生じるユーザー署名は、既知のユーザーモデルと比較され、認証又は識別のためにユーザーモデル（１３５）のデータベースに保存され得る。ユーザーモデルは、モデルを定める画像から得た署名により、個人の掌画像の収集から計算される、統計モデルである。１つの実施形態において、ユーザーモデルは、ユーザーの基準画像から計算した署名の、いわゆるガウス密度モデルから成る。クエリ画像Ｓの署名を与えられると、ユーザーモデルは、マッチングスコアを計算するために使用される。前記署名は、マッチングスコアが以下の場合、ユーザーモデルに一致すると考えられる。

【００２４】

【数１】

$$R = \sum_i \frac{(Si - Mi)^2}{Vi+u}$$

【００２５】

式中、ＭｉとＶｉは、与えられたユーザーの全ての基準画像の署名ベクトルのｉ番目の成分の平均及び変化であり、ｕは小さな定数である。前記署名は、マッチングスコアＲがこのユーザーモデルに関する予め選択した閾値より大きな場合、ユーザーモデルに一致すると考えられる。認証と識別のエンジン（１３０）、モデル構築エンジン（１５５）、及びユーザーモデルのデータベース（１３５）は、ＡＩＤユニット（１６０）を形成する。

【００２６】

署名（１２５）はまた、モデル構築エンジン（１５５）に送り込まれ、最初のユーザー登録中にユーザーモデルを初期化するか、又は、モデルが既に存在する場合にユーザーモデルのデータベース（１３５）に保存されるユーザーモデルを精密化するために前記署名の情報を選択的に組み込む。本発明の１つの実施形態において、モデル構築エンジン（１５５）は、ユーザーの新たな画像から抽出した署名を使用して、前述の平均及び変化、Ｍｉ及びＶｉを更新する。

【００２７】

デバイス（１００）はまた、好ましくは、ＡＩＤエンジン（１３０）と通信するリモートリソースインターフェース（１４５）を備える。リモートリソースインターフェース（１４５）は、デバイス（１００）で実施された認証機能性と識別機能性の間のインターフェースとして機能し、また、それらと同じそれらの機能性が、リモートサーバー及びリモートデバイスなどの外部／リモートリソース上で生じる。故に、例えば、リモートリソースインターフェース（１４５）は、リモートアプリケーションに要求されるように、認証又は識別を調和するリモートサーバー上にあるアプリケーションと相互に作用する。これは、デバイス（１００）を操作するユーザーの認証又は識別、或いはデバイス（１００）自体の認証又は識別のために、外部リソースによる要求を管理する工程、及び応答する工程を含み得る。

【００２８】

リモートリソースインターフェース（１４５）は、認証及び識別の活動に関連するデータを送受信するために、ネットワークインターフェース（１５０）と通信することができる。無線周波数と、同様に、限定されないがＢｌｕｅｔｏｏｔｈ（登録商標）及び他の近距離通信技術を含む他のものを含む、様々な無線通信プロトコルが、使用され得る。本発明の好ましい実施形態において、開放した無線リンク上でデバイス（１００）から往復して通信されるデータは、例えば、本発明の認証及び識別の方法に関連したユーザーデータ及び他のデータが、認証されていない者によって遮断され得る可能性を減らす又は排除する、暗号化及び／又は他の方法の手段により、当該技術分野で既知のように確保される。ネットワークインターフェース（１５０）は典型的に、当該技術分野で既知のような無線周波数トランシーバモジュールを備えており、デバイス（１００）が無線リンクを介してワイヤレスネットワーク（４００）と通信することを可能にする。ワイヤレスネットワーク（４００）は典型的に、デバイス（１００）によって送受信されるデータを、当該技術分野で既知のように再度、データネットワーク（５００）に次々に返送する。

【００２９】

ほんの一例として、本発明は、デバイス（１００）のユーザー又はデバイス（１００）自体が、リモートサーバー、及びアプリケーション、並びにリモートサーバーにある他のリソースによって認証又は識別されることを可能にする。図１に示されるように、リモートサーバー（２００）は、上述の通信路を介してデバイス（１００）と通信することができる。この方法において、及びデバイス（１００）にあるリモートリソースインターフェ

ース（１４５）によって制御されるように、リモートサーバー（２００）にあるＡＩＤユニット（２０５）は、以下により詳しく記載されるように、リモートサーバー（２００）にある又はそれによりアクセス可能な、既知の且つ有効になったユーザーモデルとの比較のために、デバイス（１００）から認証及び識別のデータを要求する且つ受け取ることができる。この認証及び識別の性能は、リモートサーバー（２００）にある１以上のアプリケーション（２１０）、データ（２１５）、及び他のリソースへの選択的なアクセスを提供する。同じ性能はまた、デバイス（１００）に対して離れているデータ又は他のリソースへのアクセスをローカルリソース（１４０）が求める場合と同様に、デバイス（１００）にあるアプリケーション、データ、及び／又は他のリソースを含むローカルリソース（１４０）への選択的なアクセスを提供する場合がある。

【００３０】

本発明の別の実施形態において、上述のような通信は、デバイス（１００）と、１以上のリモートデバイス（３００）との間で生じ得る。リモートデバイス（３００）は、デバイス（１００）と同じ又は異なるデバイスのタイプであり、本発明の教示に従う認証／識別の機能性は、両方に生じ得る。要するに、デバイス（１００）は、例えば、リモートデバイス（３００）上のＡＩＤユニット（３１５）を介してリモートデバイス（３００）にある１以上のアプリケーション（３１０）及び／又はデータ（３１５）にアクセスするために、リモートデバイス（３００）からの認証／識別の要求に応答することができる。しかしまた、リモートデバイス（３００）は、リモートデバイス（３００）がデバイス（１００）にあるリソースにアクセスするために、デバイス（１００）により開始される認証及び識別の要求を受け取り且つ応答することができる。幾つかの場合において、リソースが共有される前に、デバイス（１００）とリモートデバイス（３００）の両方は、他方の認証及び／又は識別を要求することになる。このことは、例えば、デバイス（１００）のユーザーとリモートデバイス（３００）との間の、所望されるセキュア通信のコンテキストにおいて生じ得る。

【００３１】

ここで図２を見てみると、本発明の好ましい実施形態に従ったユーザー／デバイスの認証及び／又は識別の方法が、現在記載されている。最初の議論により、本発明の教示の内容において認証と識別の間の差は、最初に記載される。

【００３２】

認証の場合、ユーザーは、ユーザーＩＤ又はユーザー名の形で身元を提示し、本発明のシステムは、ユーザーが自身で主張するように本人であることを確認する。前記システムはその後、ユーザーの掌の画像から得た署名を、ユーザーモデルのデータベースにおいて対応するモデルと比較する。それらが一致する場合、ユーザーは認証される。それらが一致しない場合、ユーザーは拒絶される。

【００３３】

本発明の教示に従ったユーザー認証のためのフローチャートは、好ましい実施形態において、図４に示される。第１工程として、デバイス（１００）にてユーザーは、デバイス（１００）に自身の名前又は他の識別情報を入力し、又は、ユーザーの身元は既にデバイス（１００）に予めロードされる場合がある。それとは別に、ユーザーは、デバイス（１００）のカメラ（１０５）を使用して、自身の手の掌の写真を撮る。次に、カメラデータ処理装置（１１０）は、画像内の掌領域を判定する、関心検知器領域（１１５）に未加工のピクセルデータを送る。関心検知器領域（１１５）から覆い隠された掌領域は、ユーザーの固有の署名を得る変換プロセッサ（１２０）に送り込まれる。この変換機能は代替的に、リモートリソース上で、又はリモートリソース上で部分的に、及びデバイス（１００）上で部分的に処理され得る。画像化した掌領域とデバイス（１００）との間で直接接触することなく、一般のデジタルカメラを超える任意の特別なハードウェアを必要とすることなくエンドユーザーにより自由形式或いは任意の配向で撮影された、手の高解像度画像を使用して、本発明のシステムは、特徴抽出、ユーザー署名への特徴処理、及び保存したユーザー署名又はユーザーモデルに対するユーザー署名の一致を含む、複数工程のソフト

ウェア解決策を使用して個人を識別し、その中で：（ｉ）１つ又は複数の関心領域が検知され、入力画像から分けられて、外部ピクセルデータを取り除き、且つ掌領域を分離し；（ｉｉ）高次元のスパース特徴ベクトルが画像から抽出され（例えば、参照例８）；（ｉｉ）各画像に関する１つの署名は、近くの特徴ベクトルが、よりコンパクトでロバストな画像表示に溜まるプロセスで作成され；及び、（ｉｖ）複数の画像署名は、各個人のユーザーに関する本人モデルに組み合わされる。

【００３４】

その後、認証と識別のエンジン（１３０）は、ユーザーモデル（１３５）のデータベースで、（以前に示されたユーザー識別データに基づいて）ユーザーのモデルを調べる。この時点で、得られたユーザー署名が、保存されたユーザーモデルと一致する場合、ユーザーは認証され、所望のリソース又はリソースのセットへのアクセスを承認される。代替的に、ユーザー署名とモデルが一致しない場合、その後、ユーザーは、所望のリソース又はリソースのセットへのアクセスを拒否される。調査と一致に関する前述の機能性は代替的に、デバイス（１００）へと遠隔に実行され得る。

【００３５】

識別の場合、ユーザーは、掌紋画像又は画像のセットのみを提示し、認証及び識別のエンジン（１３０）は、掌紋画像から得た署名を、ユーザーモデルのデータベース（１３５）における全てのモデル又はその亜群とを比較する。一致が見出されると、後にユーザーが識別される。一致が見出されなければ、ユーザーは発見されない（ｕｎｋｎｏｗｎ）。

【００３６】

ユーザー識別のためのフローチャートは図５に示される。この場合、認証の場合のように、ユーザーは、自身の手の掌の写真を撮影する。このデータは、カメラデータ処理装置（１１０）によってピクセル形状に再び処理され、画像内の掌領域を判定するために関心検知器領域（１１５）に送られる。関心検知器領域（１１５）から覆い隠された掌領域は、ユーザーの固有の署名を得る変換プロセッサ（１２０）に送り込まれ、その後、ＡＩＤエンジン（１３０）は、得られた署名を、ユーザーモデルのデータベース（１３５）に保存された全てのモデル又はその亜群と比較する。上述の変換及び比較の機能は代替的に、リモートリソース上で、又はリモートリソース上で部分的に、及びデバイス（１００）上で部分的に処理され得る。あらゆる場合も、一致が見出される場合、後にユーザーが識別され、リソース又はリソースのセットへのアクセスが認められ得る。一致が見出されない場合、後にユーザーは識別されず、所望のリソース又はリソースのセットへのアクセスは、認められないことになる。

【００３７】

どのモード（認証又は識別）が使用されるかは、アプリケーションに左右される。一般に、認証は、自身の身元の追加の要因を入力するためにユーザーが取る必要のある余分な工程のため、より高精度であるが低いユーザー体験のレベルを提供する。身元の第２要因は、とりわけ、ユーザーネーム、ユーザーＩＤ、パスワード、固有の従業員ＩＤ、社会保障番号、Ｅメールアドレス、様々な他の生体認証形態などの一般の形態の何れかをとることができる。本発明の１つの実施形態において、身元の第２要因は、個人のもう片方の手の掌紋画像から得た署名であり、個人の両手の掌紋画像又は画像のセットの各々の個人の署名は、認証又は識別のために共に利用される。

【００３８】

上述のそれぞれの場合（認証又は識別）において、デバイス（１００）内にローカルに位置するユーザーモデルのデータベース（１３５）内のモデルに対するユーザー署名の一致の代わりに、デバイス（１００）にて撮影したユーザーの掌の画像又は画像のセットにより作られる署名が、リモートサーバー（２００）又は１以上のリモートデバイス（３００）の何れか或いは両方に位置するデータベースに含まれるモデルに対して、一致され得ることに注目するのが、重要である。この場合、デバイス（１００）のユーザーは典型的に，デバイス（１００）内にローカルに位置するリソースではなく、むしろこれらリモートプラットフォームにある１以上のリソースへのアクセスを求めることになる。一例とし

て、例えば、スマートフォンをアンロックする場合、処理はスマートフォン／デバイス（１００）にてローカルに行われ得るが、一方で、例えばリモートベースのアプリケーションに関連して認証が行われている場合、処理の一部はリモートサーバー（２００）にて行われ、ユーザーモデルは、スマートフォン上でローカルに行われるものとは対照的に、リモートサーバー（２００）に恐らく保存されているものに対して一致する。加えて、ユーザーモデル、署名、及び／又は他の生体認証データは、ＡＩＤユニット（１６０）、（２０５）、（３０５）の何れかの間で同期され、デバイス（１００）、リモートサーバー（２００）、前記デバイス（１００）の無いリモートデバイス（３００）、ユーザーモデル、署名、及び／又は他の生体認証データがローカルに作られるリモートサーバー（２００）又はリモートデバイス（３００）の何れかにて、ローカル認証又は識別を可能にし得ることが、本発明の教示から明らかとならねばならない。

【００３９】

ここで図２に戻ると、本発明の好ましい実施形態において、工程（１）にて、デバイス（１００）を使用して、カメラ（１０５）により（工程（３））、識別されるユーザーの掌の写真を撮る（工程（２））。フラッシュ構成要素（工程（４））が、画像の必要な前処理を提供するためにデバイス（１００）に埋め込まれ得るのは、特に前処理が、関心検出器領域、特徴抽出、及び個人の掌画像の署名処理に十分な最小限の光を提供することに関係する。次に、画像の掌領域は、関心検知器領域（１１５）により覆い隠され（工程（５））、変換プロセッサ（１２０）に送り込まれて（工程（６））、未加工のピクセルを一意に識別可能なユーザー署名、即ち署名（１２５）に変換する。ユーザー署名は、ユーザーの掌紋画像に関連した関連識別情報を含み、ユーザーモデルのデータベース（１３５）又はリモートプラットフォームにあるデータベース等、ユーザーモデルの大規模なデータベースに迅速且つ正確に一致することができる、コンパクト符号である（工程（７））。得られたユーザー署名の１つの利益は、ユーザーモデルのデータベースからユーザーの掌画像を再構築することを本質的に不可能にするということである。工程（８）において、ＡＩＤエンジン（１３０）は、掌画像又は画像のセットからのユーザー署名を、ユーザーモデルのデータベースにおけるものと比較し、適用可能なものとしてユーザーを識別又は認証する。上述の変換及び比較の機能は代替的に、リモートリソース上で、又はリモートリソース上で部分的に、及びデバイス（１００）上で部分的に処理され得る。

【００４０】

ここで図３を見てみると、認証又は識別がリモートリソースに対して達成されている場合、デバイス（１００）と前記リモートリソースの間の通信は好ましくは、当該技術分野で既知であるようなセキュア接続にわたって生じることが、見られ得る。これは、当該技術分野で既知の１以上の技術を備え、例えば、とりわけ強力な暗号化、公開又は秘密鍵暗号、デジタル証明書、及び／又はデジタル署名を含む。

【００４１】

本発明のシステム及び主要な方法が記載された今、認証／識別に関連したスプーフィングを妨げるための様々な方法、同様にリモートリソースによりトランザクション情報をコード化し且つ交換するための新規な方法など、追加の新規な機能について、議論される。

【００４２】

スプーフ保護は、本発明の重要な態様である。前記スプーフ保護は、例えば、認証のために本物の手の代わりに掌の印刷写真を相手が使用するのを妨げる。スプーフ保護に向けられる本発明の１つの新規な態様は、スプーフィングに対するセキュリティを設けるために、ヒトの手の３次元特徴を検知且つ使用する工程を含む。

【００４３】

スプーフ検出の１つの例において、写真と本物の手を区別するために、本発明のシステムは、立て続けに一連の写真を撮影し、カメラフラッシュは、断続的に、及び異なる時間の長さで使用される。フラッシュで撮影された３Ｄ対象（本物の手）の写真は、フラッシュにより作られる特定のハイライト領域と影を備えており、一方で、手の２Ｄ表示（例えば、別のモバイルデバイスの表示画面上に示される掌又は掌画像の印刷写真）における手

の掛り位置（ｏｎ　ｐｏｓｉｔｉｏｎ）は、前記ハイライト領域及び影を示さない。これにより、本発明のシステムは、印刷写真と本物の手を区別するためにフラッシュ写真と非フラッシュ写真との間で作成される、手の上のハイライト領域と影の比較を利用することが、可能となる。このように、認証されたユーザーの掌の写真を偶然獲得した未認証の者は、ローカルリソース又はリモートリソースへの未認証のアクセスを獲得するために前記写真を使用することができない。

【００４４】

本物の手を検知するための更なる方法は、手の３Ｄモデリングを含む。この場合、本発明のシステムは、一連の複数の写真が撮影される間、ユーザーに自身の手を回すように促し得る。真の３Ｄ対象は、各連続画像により手の異なる部分を明らかにし、その一方で２Ｄ対象は常に、異なる歪み具合だけで、手の同じ部分を示す。これにより、本発明のシステムは、印刷写真と本物の手を区別するようになる。同様に、手を回転させる代わりに、ユーザーは、一連の写真が撮影される間、手を閉じて拳にするか、又は手を開くように促され得る。本物の手を手の写真と区別する他の方法も、可能である。

【００４５】

本発明の別の新規な態様は、リプレーアタックが検知され且つ妨げられ得る方法である。この場合、カメラで撮影した画像を送る代わり、モバイルデバイスが、正当なユーザーの本物の手から認証又は識別のためのネットワークへと１以上の一連の前に記録した写真を送るように、相手は、モバイルデバイスを改良する。ここで、相手は、認証したユーザーに気づかれることなく又は撮影を妨げられることなく、認証されたユーザーの手を撮影できると仮定する。これが実際に危険である場合（例えば、認証されたユーザーが眠っている又は無意識の場合）、その後、ユーザーＩＤ又は掌紋画像と無関係のデータの他の形態などの１以上の追加の身元要因がユーザーを認証することを要求されるように、前記システムが使用されることが好ましい。

【００４６】

リプレーアタックを検知及び予防するために、本発明のシステムは、様々な間隔で一連の写真及びフラッシュを出し、即ち前記システムは一連の写真を記録し、フラッシュが切られるものもあれば、フラッシュが付けられるものもある。具体的な写真及びフラッシュオン／オフのシーケンスは、無作為に又は予め定めたシーケンスに従って選択され得、各認証又は識別の要求のために変わることができる。本発明のシステムが、相手が一連の前に記録した写真を使用するかどうかを容易に検知できるのは、写真及びフラッシュのオン／オフのパターンが、モバイルデバイスに実際に送られたものと一致しないためである。

【００４７】

リプレーアタックを検知する別の方法は、前に使用した全ての画像を保存する工程と、新しい画像をデータベースにあるものと比較する工程を含む。２つの異なる掌画像の基礎となるピクセルデータが本質的に、特定の許容レベルと全く同じ又はほぼ同じではないため、前記システムは、いつ前に撮影した画像が再び使用されるのかを検知することができる。リプレーアタックを検知する他の方法も、考えられる。

【００４８】

本発明のまた別の新規な態様は、一連の写真及び／又はフラッシュパターンのタイミング内にトランザクション情報又は他のデータを埋め込む能力である。このタイミングパターンは更に、トランザクション自体に関する情報をコード化するために使用され得る。その後、暗号ハッシュコードが、この情報に適用され得る。ハッシュコードは、結果として生じるコードコンパクト（短い）を作り、及びまた、フラッシュパターンを観察する者が、該コードの本来のコンテンツに関する任意の情報を得ることを妨げる。本発明の１つの実施形態において、画像及び／又はフラッシュパターンのシーケンスのタイミングは、反スプーフィング機構の一部として利用され、認証又は識別のために設けられる画像シーケンスがトランザクション自体からの情報と一致するかどうかを定める。具体的な実施形態は次のものを含み得る：

【００４９】

１．フラッシュパターンによる掌領域の低解像度ビデオ。

【００５０】

２．掌領域の１以上の高解像度スチル画像。

【００５１】

３．高解像度画像がビデオにおけるものと同じ対象に由来するのを確実にするコンピュータビジョン技術。

【００５２】

本発明のシステム及び方法の上記記載に基づいて、様々なアプリケーションが可能であることが、理解され得る。例は、限定されないが、１以上のデバイスへのアクセス、前記デバイスにある又はサーバー上に遠隔に位置する又は他のリモートデバイス上にある１以上のアプリケーションへのアクセス、様々なトランザクションアプリケーション（選挙投票、国家福祉の分配、財政支出など）、及びユーザーの身元の確認を要する他の種類のトランザクションを含む。

【００５３】

要約すると、典型的な実施形態において、本発明は、コンピュータシステム（適切なハードウェアで動くソフトウェアの組み合わせを含む）、コンピュータにより実施される方法、及び下記工程を含むプロセスを通じて個人の掌の画像又は画像のセットを使用する工程を含む、個人の認証又は識別のためのデバイスを提供する：（１）ローカル分類器を使用して掌領域を検知する工程；（２）関心領域から特徴を抽出する工程；及び（３）学習プロセスを通じてダイナミックに増大され得る、データベースに保存されるユーザーモデルに対するマッチングスコアを計算する工程。故に、本発明は、適切なコンピューターハードウェア上で実行されるソフトウェアを含むデバイスに関連して利用可能なリソースへの選択的なアクセスを提供するためのシステムを備え、該システムは次のものを備える：（ａ）ヒトの掌紋の少なくとも１つの写真を撮影することができる、前記デバイスに関連する少なくとも１つのカメラ；（ｂ）物理的に接触することなく掌の関心領域を位置付け且つ分けるためにローカル分類器を使用する検出器モジュール；（ｃ）ヒトの掌紋の前記関心領域に関連する未加工のピクセルデータを前記掌紋に関連した固有の署名へと変換する、変換プロセッサ；及び、（ｄ）認証及び識別のエンジンであって、該認証及び識別のエンジンは、前記リソースの１以上へのアクセスが、前記固有の署名及び複数のユーザーモデルを含む少なくとも１つのデータベースに基づいて認められるべきか否かを定める、認証及び識別のエンジン。前記システムは更に、新たなデータを持つユーザーモデルを改良する学習プロセッサを備え、該学習プロセッサは、前記データベースと、前記認証及び識別のエンジンを増大するために前記掌紋画像を選択的に含む。一実施形態において、前記デバイスはモバイルデバイスであり、一方で他の実施形態において、前記デバイスはデスクトップデバイス又は固定式埋込デバイスである。前記システムは、画像捕捉時に選択的に起動して、関心領域の検知、特徴抽出、及びヒトの掌画像の署名処理に十分な最小限の光を提供する、フラッシュ構成要素を備え得る。一実施形態において、前記システムの変換プロセッサは、関心領域上のパッチから抽出したディスクリプタを使用する。前記ディスクリプタは、少なくとも１つのグループに溜められ得る、高次元のスパースベクトルにコード化され得る。

【００５４】

本発明のシステムは、該システム内で実施される方法の一部として、１つのＢａｇ　ｏｆ　Ｆｅａｔｕｒｅｓ又は複数のＢａｇ　ｏｆ　Ｆｅａｔｕｒｅｓの表示から署名を計算する特徴を備え得る。加えて、前記システムの検出器モジュールは、Ｈａａｒウェーブレット及びＡｄａＢｏｏｓｔアルゴリズムを使用することができる。様々な実施形態において、前記システムは、サポートベクトルマシン又は畳み込みニューラル・ネットワークを使用する検出器モジュールを備える。前記システムのユーザーモジュールは、ヒトの掌画像の収集から計算した統計モデルであり得る。同様に、ユーザーモデルは、ガウス密度モデル、又はガウス密度モデルの組み合わせであり得る。

【００５５】

本発明のシステムは、リソースの少なくとも１つがデバイスから離れるように構成され得る。代替的に、リソースの少なくとも１つはデバイス上にあってもよい。幾つかの実施形態において、リソースの少なくとも１つは、アプリケーション又はデータベースである。

【００５６】

本発明のシステムの実施形態において、ヒトの両方の掌紋画像の各々の各署名は、利用可能であれば、ヒトの認証又は識別のために共に利用される。

【００５７】

本発明のシステムの幾つかの実施形態において、掌紋の認証又は識別は、以下の：パスコード、セキュリティ質問、指紋認識、顔認識、虹彩認識、手書署名認識、及び他の生体認証且つ非生体認証の形態の１以上など、他の形態と組み合わせられる。

【００５８】

本発明のシステムは、アプリケーションにより１以上のユーザーが１以上のトランザクションを行なうことを選択的に許容されるような方法で、実施され得る。

【００５９】

本発明のシステムはまた、ヒトの掌のフラッシュ画像及び非フラッシュ画像のシーケンスの使用を含み、該シーケンスはとりわけ、示された手が手の３Ｄ対象又は２Ｄ表示であるかを定めるための反スプーフィング機構の一部として使用され得る。更に、本発明のシステムは、ヒトの掌の動作中に捕捉した画像データが、示された手が手の３Ｄ対象又は２Ｄ表示であるかを定めるための反スプーフィング機構の一部として使用されるように、実施され得る。幾つかの実施形態において、ヒトの掌のフラッシュ画像及び非フラッシュ画像のシーケンス、同様に一連の画像間の時間間隔は、反スプーフィング機構の一部として利用され、相手が、認証又は識別のために前に記録した画像のシーケンスを利用しようと試みているかどうかを定める。

【００６０】

本発明の幾つかの実施形態において、前に使用したヒトの画像の全ては、相手が、認証又は識別のために前に記録した画像のシーケンスを利用しようと試みているかどうかを定める反スプーフィング機構の一部としての新しい画像と比較するために、コンピューティングデバイスにあるデータベース等に保存される。また更に、特定の実施形態において、本発明のシステムは、トランザクション情報又は他のデータが、認証又は識別のために設けられる画像シーケンスがトランザクション自体からの情報に一致するかどうかを定める反スプーフィング機構の一部として、画像及び／又はフラッシュパターンのシーケンスのタイミング内に埋め込まれるように、実施される。

【００６１】

本発明の特定の実施形態が示され且つ記載されてきた一方で、本明細書における教示に基づき、変更及び改良が本発明及びその広範囲の態様から逸脱することなく行われ得ることは、当業者に明白であろう。

【００６２】

＜引用される参照例＞

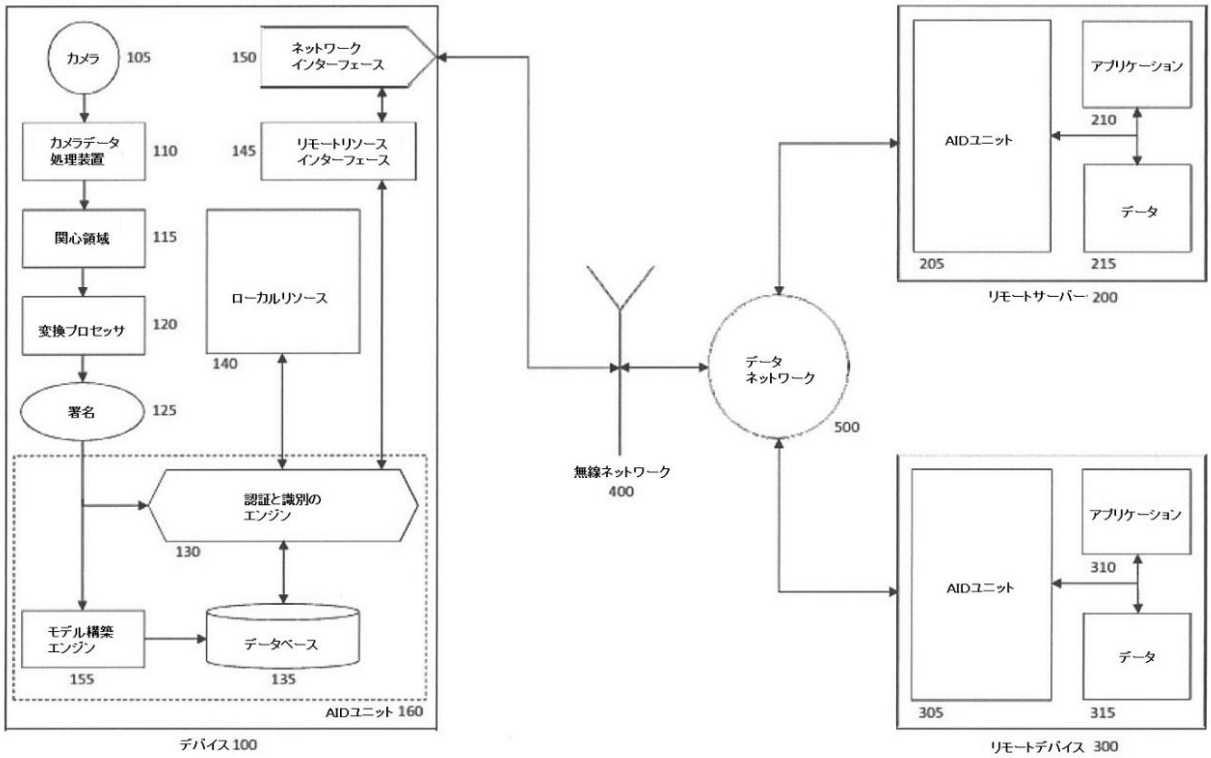
（１）Ｐａｕｌ Ｖｉｏｌａ ａｎｄ Ｍｉｃｈａｅｌ Ｊｏｎｅｓ，Ｒａｐｉｄ Ｏｂｊｅｃｔ Ｄｅｔｅｃｔｉｏｎ ｕｓｉｎｇ ａ Ｂｏｏｓｔｅｄ Ｃａｓｃａｄｅ ｏｆ Ｓｉｍｐｌｅ Ｆｅａｔｕｒｅｓ，Ｐｒｏｃｅｅｄｉｎｇｓ ｏｆ ＩＥＥＥ Ｃｏｍｐｕｔｅｒ Ｖｉｓｉｏｎ ａｎｄ Ｐａｔｔｅｒｎ Ｒｅｃｏｇｎｉｔｉｏｎ，２００１，ｐａｇｅｓ １：５１１－５１８．

（２）Ｃｏｒｉｎｎａ Ｃｏｒｔｅｓ ａｎｄ Ｖｌａｄｉｍｉｒ Ｎ．Ｖａｐｎｉｋ，Ｓｕｐｐｏｒｔ－Ｖｅｃｔｏｒ Ｎｅｔｗｏｒｋｓ，Ｍａｃｈｉｎｅ Ｌｅａｒｎｉｎｇ，２０，１９９５．

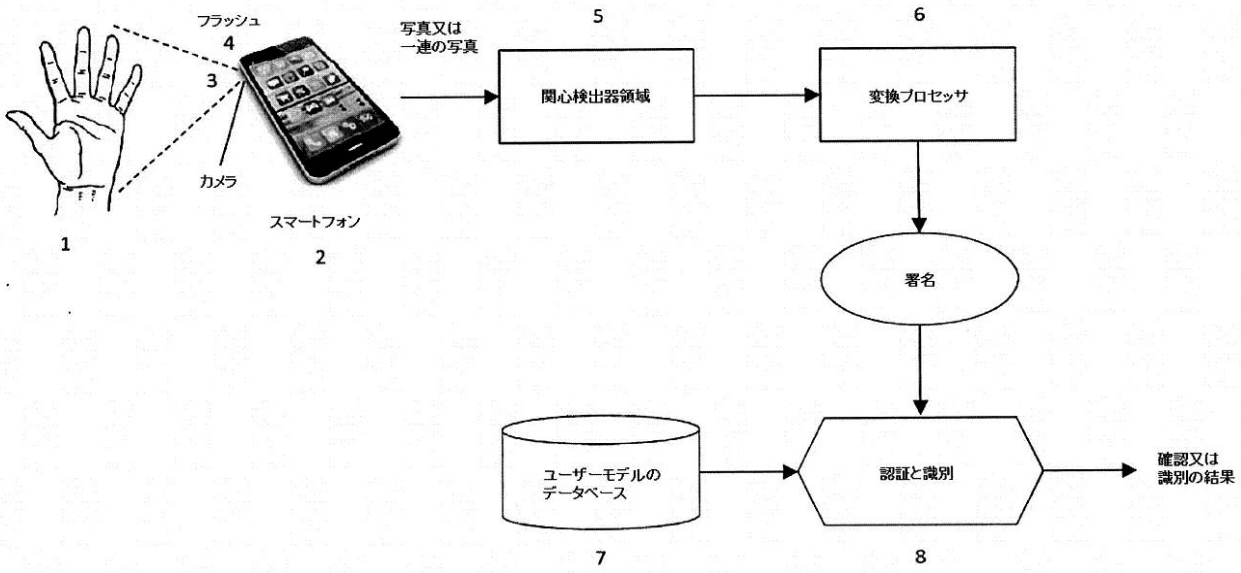
（３）Ｙａｎｎ ＬｅＣｕｎ，Ｌｅｏｎ Ｂｏｔｔｏｕ，Ｙｏｓｈｕａ Ｂｅｎｇｉｏ，Ｐａｔｒｉｃｋ Ｈａｆｆｎｅｒ：Ｇｒａｄｉｅｎｔ－Ｂａｓｅｄ Ｌｅａｒｎｉｎｇ Ａｐｐｌｉｅｄ ｔｏ Ｄｏｃｕｍｅｎｔ Ｒｅｃｏｇｎｉｔｉｏｎ，Ｐｒｏｃｅｅｄｉｎｇ

s of the IEEE, 86(11):2278-2324, November 1998.
(4) Pierre Sermanet, Koray Kavukcuoglu, Soumith Chintala and Yann LeCun: Pedestrian Detection with Unsupervised Multi-Stage Feature Learning, Proc. International Conference on Computer Vision and Pattern Recognition (CVPR'13), IEEE, June 2013.
(5) David G. Lowe, "Distinctive image features from scale-invariant keypoints," International Journal of Computer Vision, 60, 2 (2004), pp. 91-110.
(6) N. Dalal and B. Triggs. Histograms of oriented gradients for human detection. In Proceedings of Computer Vision and Pattern Recognition, 2005.
(7) Y-Lan Boureau, Jean Ponce and Yann LeCun: A theoretical analysis of feature pooling in vision algorithms, Proc. International Conference on Machine learning (ICML'10), 2010.
(8) Yann LeCun, Koray Kavukvuoglu and Clement Farabet: Convolutional Networks and Applications in Vision, Proc. International Symposium on Circuits and Systems (ISCAS'10), IEEE, 2010.

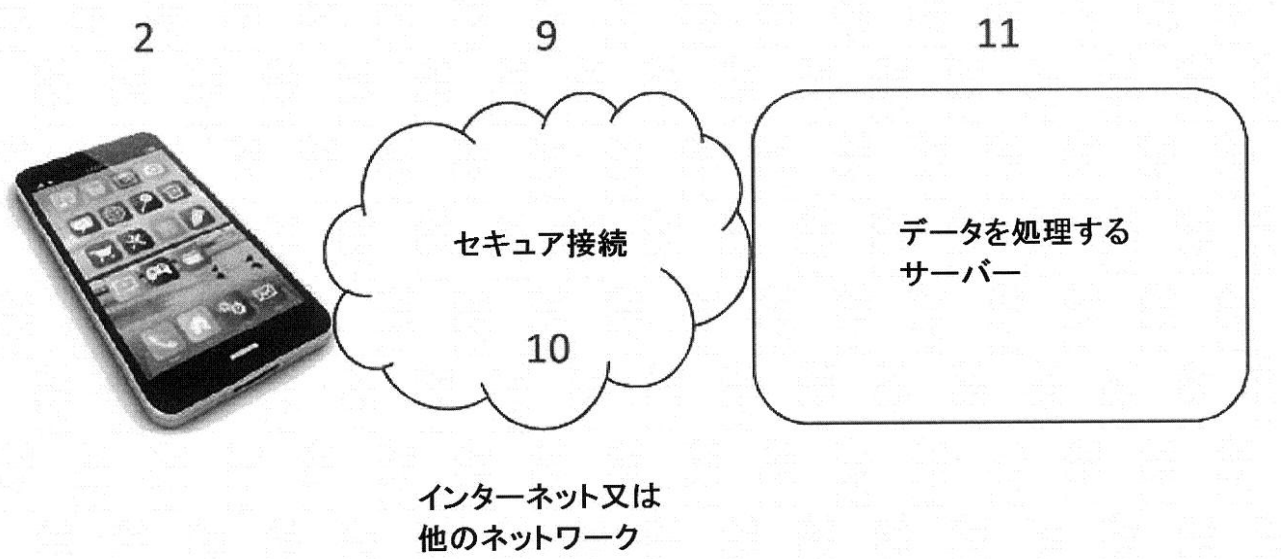
【図１】


カメラ
105
ネットワーク
インターフェース
150
カメラデータ
処理装置
110
リモートリソース
インターフェース
145
関心領域
115
ローカルリソース
140
変換プロセッサ
120
署名
125
認証と識別の
エンジン
130
モデル構築
エンジン
155
データベース
135
AIDユニット 160
デバイス 100
無線ネットワーク
400
データ
ネットワーク
500
AIDユニット
アプリケーション
210
データ
205
215
リモートサーバー 200
AIDユニット
アプリケーション
310
データ
305
315
リモートデバイス 300

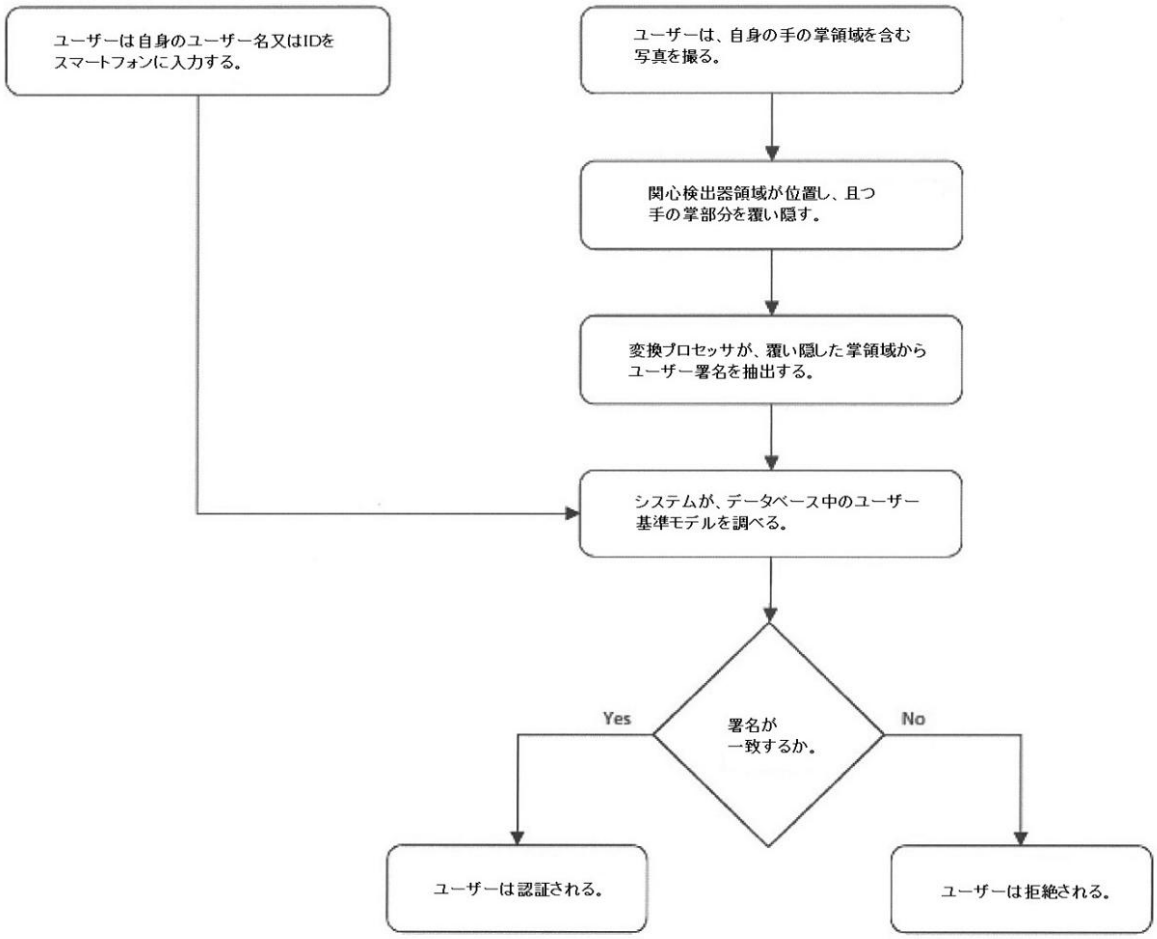
【図２】


フラッシュ
4
3
カメラ
1
スマートフォン
2
写真又は
一連の写真
5
関心検出器領域
6
変換プロセッサ
署名
ユーザーモデルの
データベース
7
認証と識別
8
確認又は
識別の結果

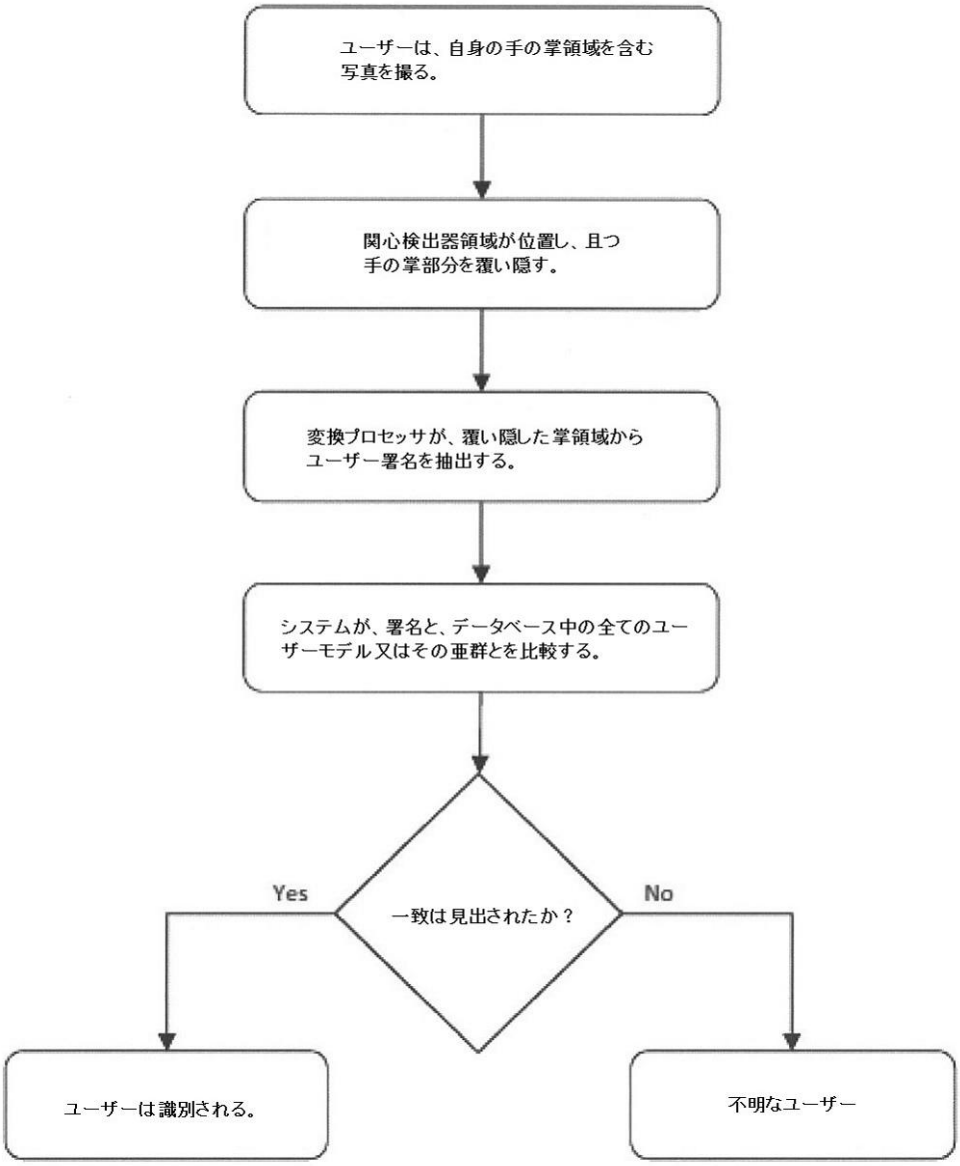
【図３】


2
9
11
セキュア接続
10
データを処理する
サーバー
インターネット又は
他のネットワーク

【図４】


ユーザーは自身のユーザー名又はIDを
スマートフォンに入力する。
ユーザーは、自身の手の掌領域を含む
写真を撮る。
関心検出器領域が位置し、且つ
手の掌部分を覆い隠す。
変換プロセッサが、覆い隠した掌領域から
ユーザー署名を抽出する。
システムが、データベース中のユーザー
基準モデルを調べる。
署名が
一致するか。
Yes
No
ユーザーは認証される。
ユーザーは拒絶される。

【図５】


ユーザーは、自身の手の掌領域を含む
写真を撮る。
関心検出器領域が位置し、且つ
手の掌部分を覆い隠す。
変換プロセッサが、覆い隠した掌領域から
ユーザー署名を抽出する。
システムが、署名と、データベース中の全てのユー
ザーモデル又はその亜群とを比較する。
一致は見出されたか？
Yes
No
ユーザーは識別される。
不明なユーザー

【国際調査報告】

## INTERNATIONAL SEARCH REPORT

International application No.
PCT/US13/58343

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06K 9/00 (2014.01)
USPC - 382/115; 340/5.53, 5.83
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8) Classification(s): G06K 9/00 (2014.01)
USPC Classification(s): 382/115; 340/5.53, 5.83

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
MicroPatent (US-G, US-A, EP-A, EP-B, WO, JP-bib, DE-C,B, DE-A, DE-T, DE-U, GB-A, FR-A); ProQuest, IEEE, Google/Google Scholar; Palm print*, hand print*, biometric* camera*

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | US 8,160,307 B2 (POLCHA, A et al.) 17 April 2012; abstract, figure 11, column 5 lines 19-20, 57-59, and 61-64 column 6 lines 3-5, and 6-13, column 7 lines 6-13, 21-23, 30-31, 46-49, and 50-52, and column 12 lines 6-13 | 1-5, 14, 17-20, and 22-24 |
| Y | | 6-13, 15, 16, 21, 25-29 |
| Y | US 7,660,442 B2 (SWEENEY, L et al.) 09 February 2010; column 3 lines 27-31 | 6 |
| Y | US 8,194,938 B2 (WECHSLER, H et al.) 05 June 2012; column 17 lines 23-26 | 7 |
| Y | US 2011/0229045 A1 (YU, K) 22 September 2011; abstract, paragrah [0013] | 8 and 9 |
| Y | EP 0049039 (KORT, R) 11 July 1984; page 2 lines 36-39 | 9 |
| Y | US 2009/0297032 A1 (LOUI, A) 03 December 2009; abstract | 10 |
| Y | US 2012/0162385 A1 (PARK, J et al.) 28 June 2012; paragraphs [0022] and [0023] | 11 |
| Y | US 2012/0128936 A1 (BAUGHMAN, A) 27 May 2010; abstract | 12 |
| Y | US 8,026,840 B2 (DWELLY, W et al.) 27 September 2011; column 3 lines 4-7 | 13 |
| Y | US 5,450,523 (ZHAO, Y) 12 September 1995; abstract | 15 and 16 |
| Y | US 7,218,761 B2 (MCCLURG, G et al.) 15 May 2007; column 1 lines 18-19 and column 2 lines 25-28 | 21 |
| Y | US 2008/000286 A1 (SUPER, B et al.) 03 January 2008; abstract, paragraphs [0019], [0021], [0024], and [0026] | 25-29 |

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 24 February 2014 (24.02.2014) | 13 MAR 2014 |
| Name and mailing address of the ISA/US<br>Mail Stop PCT, Attn: ISA/US, Commissioner for Patents<br>P.O. Box 1450, Alexandria, Virginia 22313-1450<br>Facsimile No. 571-273-3201 | Authorized officer:<br>Shane Thomas<br>PCT Helpdesk: 571-272-4300<br>PCT OSP: 571-272-7774 |

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ

(72)発明者 ワン，ヤン
アメリカ合衆国 ０８５４０ ニュージャージー州 プリンストン セイヤー・ドライブ ３６
(72)発明者 ワグメアー，セイガー
アメリカ合衆国 １００１４ ニューヨーク州 ニューヨーク ナンバー３シー ジェーン・ストリート ２４

Ｆターム(参考) 5B043 AA04 AA09 BA03 CA10 DA05 EA02 EA05 FA03 FA08 GA02
5L096 BA08 BA18 CA02 FA02 FA39 HA11 HA13 JA03 JA11 KA04