(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)公表番号
特表2024-527263
(P2024-527263A)
(43)公表日　令和6年7月24日(2024.7.24)

(51)国際特許分類			FI			テーマコード（参考）
G06F	*21/32*	*(2013.01)*	G06F	21/32		5B043
G06T	*7/00*	*(2017.01)*	G06T	7/00	510F	5L096
G06V	*40/16*	*(2022.01)*	G06V	40/16	A	
G06V	*10/82*	*(2022.01)*	G06T	7/00	350C	
			G06V	10/82		

審査請求　未請求　予備審査請求　未請求　（全26頁）　最終頁に続く

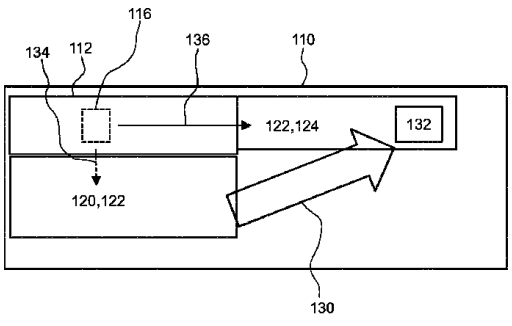
(21)出願番号　特願2023-577596(P2023-577596)
(86)(22)出願日　令和4年6月14日(2022.6.14)
(85)翻訳文提出日　令和6年2月15日(2024.2.15)
(86)国際出願番号　PCT/EP2022/066188
(87)国際公開番号　WO2022/263452
(87)国際公開日　令和4年12月22日(2022.12.22)
(31)優先権主張番号　21179598.4
(32)優先日　令和3年6月15日(2021.6.15)
(33)優先権主張国・地域又は機関
欧州特許庁(EP)
(81)指定国・地域　AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),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,
最終頁に続く

(71)出願人　517267802
トリナミクス ゲゼルシャフト ミット ベシュレンクテル ハフツング
ドイツ、６７０６３ ルートヴィッヒスハーフェン アム ライン、インドゥストリーシュトラーセ ３５
(74)代理人　100100354
弁理士　江藤 聡明
(74)代理人　100167106
弁理士　倉脇 明子
(74)代理人　100194135
弁理士　山口 修
(74)代理人　100206069
弁理士　稲垣 謙司
(74)代理人　100185915
最終頁に続く

(54)【発明の名称】　モバイルデバイスのユーザ認証方法

(57)【要約】
モバイルデバイス（１１０）のユーザを認証する方法が提案される。この方法は以下のステップ：
a) （１１４）前記モバイルデバイス（１１０）の少なくとも１つのカメラ（１１２）を使用することによって、顔の少なくとも１つの第１画像（１１６）を画像化するステップと；
b) （１１８）前記モバイルデバイス（１１０）のプロセッサ（１２２）の通常の実行環境（１２０）に前記第１画像（１１６）を提供し、前記プロセッサ（１２２）の信頼できる実行環境（１２４）に前記第１画像（１１６）を提供するステップと；
c) （１２６）前記通常の実行環境（１２０）において少なくとも１つのトレーニングされたモデルを使用して前記第１画像（１１６）を分析し、それによって画像情報を含む多次元ベクトルを決定するステップと；
d) （１２８）以下の顔認証ステップ：
di) （１３０）前記多次元ベクトルを前記信頼できる実行環境（１２４）に提供し、
dii) 少なくとも１つのデコーダ（１３２）を使用す

FIG.2



【特許請求の範囲】
【請求項１】
以下のステップを含む、モバイルデバイス（１１０）のユーザ認証方法であって：
a) （１１４）前記モバイルデバイス（１１０）の少なくとも１つのカメラ（１１２）を使用することによって、顔の少なくとも１つの第１画像（１１６）を画像化するステップと；
b) （１１８）前記第１画像（１１６）を前記モバイルデバイス（１１０）のプロセッサ（１２２）の通常の実行環境（１２０）に提供し、及び前記第１画像（１１６）を前記プロセッサ（１２２）の信頼できる実行環境（１２４）に提供するステップと；
c) （１２６）前記通常の実行環境（１２０）において少なくとも１つのトレーニングされたモデルを使用して前記第１画像（１１６）を分析し、それによって画像情報を含む多次元ベクトルを決定するステップと；
d) （１２８）顔認証ステップであって、以下のステップ：
di) （１３０）前記多次元ベクトルを前記信頼できる実行環境（１２４）に提供するステップと、
dii) 少なくとも１つのデコーダ（１３２）を使用することによって、前記信頼できる実行環境（１２４）において前記多次元ベクトルから第２画像を決定するステップと、
diii) 前記第１画像（１１６）と前記第２画像を比較するステップであって、前記第１画像と前記第２画像が同一の場合、前記多次元ベクトルを実証するステップと；
div) 前記多次元ベクトルが実証された場合、前記実証された多次元ベクトルは、前記信頼できる実行環境（１２４）において保存されたユーザの顔の多次元ベクトルと比較されるステップであって、前記多次元ベクトルと前記保存されたユーザの顔の多次元ベクトルが同一の場合、前記ユーザは認証されるステップと、
を含む顔認証ステップと、
を含む、方法。
【請求項２】
前記信頼できる実行環境（１２４）は、前記通常の実行環境（１２０）から分離された実行環境である、請求項１に記載の方法。
【請求項３】
前記信頼できる実行環境（１２４）は、物理的分離、ハードウェアロジックベースの分離、又は暗号的分離方法の１つ以上によって、前記通常の実行環境（１２０）から分離される、請求項２に記載の方法。
【請求項４】
前記信頼できる実行環境（１２４）は、少なくとも１つのセキュリティ機能を備え、少なくとも１つのセキュリティ要件を満たす、請求項１～３のいずれか１項に記載の方法。
【請求項５】
前記第１画像（１１６）は、通常パス（１３４）を介して前記通常の実行環境（１２０）に提供され、前記通常パス（１３４）は、前記通常の実行環境（１２０）及び／又は前記信頼できる実行環境（１２４）内でソフトウェアによるアクセスを許可するように構成される、請求項１～４のいずれか１項に記載の方法。
【請求項６】
前記第１画像（１１６）は、セキュアパス（１３６）を介して前記信頼できる実行環境（１２４）に提供され、前記セキュアパス（１３６）は、前記第１画像（１１６）が前記通常の実行環境（１２０）内で任意のソフトウェアによって導出及び／又は変更されることを防止するように構成される、請求項１～５のいずれか１項に記載の方法。
【請求項７】
前記第２画像を決定することは、前記多次元ベクトルから前記ユーザの顔の画像を再構築するデコーダ（１３２）を含む、請求項１～６のいずれか１項に記載の方法。
【請求項８】
前記トレーニングされたモデルは、少なくとも１つの顔認識モデルを含む、請求項１～

７のいずれか１項に記載の方法。
【請求項９】
前記トレーニングされたモデルは、少なくとも１つの畳み込みニューラルネットワークを含む、請求項１～８のいずれか１項に記載の方法。
【請求項１０】
ステップc)における分析（１２６）は、前記第１画像（１１６）のフィルタリング及び畳み込みのうちの１つ以上を含む、請求項９に記載の方法。
【請求項１１】
ユーザの認証方法であって、前記方法は、請求項１～１０のいずれか１項に記載のモバイルデバイス（１１０）のユーザを認証するための方法を実施することを含み、前記方法は、信頼できる実行環境（１２４）がプロセスステップを許可するための信号を出力することをさらに含み、前記プロセスステップは、支払い、文書への署名、前記モバイルデバイス（１１０）へのアクセス、アプリケーションの有効化のうちの１つ以上を含む、方法。
【請求項１２】
コンピュータ又はコンピュータネットワーク上で実行されたときに、コンピュータ又はコンピュータネットワークに認証方法に関する請求項１～１１のいずれか１項に記載のユーザの認証方法を完全に又は部分的に実施させるように構成されたモバイルデバイス（１１０）のユーザの認証のためのコンピュータプログラムであって、前記コンピュータプログラムは、認証方法に関する請求項１～１１のいずれか１項に記載のユーザ認証方法の少なくともステップa)～d)を実施及び／又は実行するように構成されている、コンピュータプログラム。
【請求項１３】
前記コンピュータ又はコンピュータネットワーク上で実行されたときに、コンピュータ又はコンピュータネットワークに、請求項１１に記載のユーザの認証方法を完全に又は部分的に実行させるように構成されたモバイルデバイス（１１０）のユーザを認証するためのコンピュータプログラム。
【請求項１４】
コンピュータ又はコンピュータネットワークによって実行されたときに、認証に関連する方法を参照する請求項１～１１のいずれか１項に記載の方法の少なくともステップa)～d)を実行させる、及び／又は請求項１１に記載のユーザの認証方法を実行させる命令を含む、コンピュータ可読記憶媒体。
【請求項１５】
少なくとも１つのカメラ（１１２）と少なくとも１つのプロセッサ（１２２）とを備えるモバイルデバイス（１１０）であって、前記モバイルデバイス（１１０）は、認証方法を参照する請求項１～１１のいずれか１項に記載の方法の少なくともステップa)～d)を実行させる、及び／又は請求項１１に記載の認証方法を実施するように構成される、モバイルデバイス（１１０）。
【請求項１６】
支払い、文書への署名のうちの１つ以上のための、請求項１５に記載のモバイルデバイス（１１０）の使用。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、モバイルデバイスのユーザを認証する方法、認証のための方法、モバイルデバイス及びモバイルデバイスの様々な使用に関する。本発明による装置、方法及び使用は、具体的には、例えば、日常生活、セキュリティ技術、ゲーミング、交通技術、生産技術、芸術、文書又は技術目的のためのデジタル写真又はビデオ撮影などの写真撮影、安全技術、情報技術、農業、作物保護、メンテナンス、化粧品、医療技術、又は科学の様々な分野において採用され得る。ただし、他の適用も可能である。

【背景技術】
【０００２】
信頼できる実行環境（ＴＥＥ）技術の使用は、スマートフォンやタブレットコンピュータなどのモバイルデバイスで使用されることが知られている（例えば、en.wikipedia.org/wiki/Trusted_execution_environmentを参照）。しかし、モバイルデバイスのプロセッサの信頼できる実行環境は、メインプロセッサ、特に通常の実行環境と比較して、計算能力及びメモリ容量が限られている。
【０００３】
モバイルデバイスは、多くの場合セキュリティが必要な幅広いアプリケーションで使用されている。例えば、モバイルデバイスは支払いに使用され得る。支払いプロセスを承認するために、ユーザの身元は、通常、カメラに記録された顔を使用して確認される。ニューラルネットワークは、顔分析に使用され、指定された基準に基づいてユーザの身元を明らかにするために使用され得る。その結果に基づいて、支払いプロセスが承認され得る。この共有は、モバイルデバイスのプロセッサの通常の安全でない環境で改ざんされ得る。しかし、計算能力とメモリ容量が限られているため、信頼できる実行環境で顔認証（facial authentication）及び／又は認識（recognition）を実行することは不可能である。非セキュアな通常の実行環境で画像分析を実施すると、ユーザの顔の記録が、例えば修正などに、アクセス可能な状態にさらされる可能性があり、したがって、セキュリティ上の問題がある。
【０００４】
US2021/173916A1は、ダイナミックチャレンジパスフレーズデータオブジェクトの生成に関する様々な実施形態におけるシステム、デバイス、方法、及びコンピュータ可読媒体を記載している。この方法は、互いに排他的な個人の構造化データレコードのセットを表す複数のデータレコードクラスタを確立することと、データレコードクラスタの確立に対する各特徴データフィールドの決定された寄与値に基づいて複数の特徴データフィールドをランク付けすることと、ランク付けされた複数の特徴データフィールドを使用して、複数の特徴データフィールドの第１及び第２特徴データフィールドを識別することとを含む。この方法は、ダイナミックチャレンジパスフレーズデータオブジェクトを生成することであって、第１又は第２特徴データフィールドは、ステートメント文字列部分を確立するために使用されるダイナミックチャレンジパスフレーズデータオブジェクトを生成することを含み、第１又は第２特徴データフィールドの残りの１つは、質問文字列部分及び正解応答文字列を確立するために使用される。
【０００５】
US2019/205518A1は、顔に基づいてユーザを認証又は識別するためにモバイルデバイスで使用される方法を記載している。本方法は、モバイル装置の信頼できる実行環境において、ユーザの連続する画像フレームに対応する生体認証顔サンプルのシーケンスを取得することと、信頼できる実行環境において、テスト生体認証顔サンプルを含む修正シーケンスを生成するように、シーケンス内の生体認証顔サンプルの一部を修正又は置換することとを含む。この方法は、修正されたシーケンスをモバイル装置のリッチ実行環境に送信することと、リッチ実行環境において分類器を使用して生体認証顔サンプルの少なくとも一部分を分類し、分類された生体認証顔サンプルごとに、一連の中間出力と分類結果を生成することとを含む。本方法はまた、分類された生体認証顔サンプルごとに、中間出力又は分類結果の少なくとも一部、及び／又は、中間出力のダイジェストを、信頼できる実行環境に送信することを含む。本方法はさらに少なくとも１つのテスト生体認証顔サンプルについて、信頼できる実行環境において、中間出力及び／又は結果及び／又はダイジェストの少なくとも一部を検証することを含む。
【０００６】
CN105138973Aには、顔認証方法と装置が記載されている。この方法は、以下の：あらかじめ多層分類ネットワークジョイントトレーニングが行われた多層深度畳み込みネットワークを用いて、認証対象の顔画像と顔画像テンプレートから、複数レベルの特徴ベ

クトルを順次抽出するステップと；複数レベルの特徴ベクトルを、統一された次元線形マッピングマトリックスを介して、統一次元特徴ベクトルに順次マッピングするステップと；統一された次元特徴ベクトルを直列結合特徴ベクトルに連結するステップと；結合特徴ベクトルに対して線形次元削減マッピング行列を通じて次元削減マッピングを行うステップと；線形判別分析を通じて余弦値を絶対値で正規化し、得られた認証対象の顔画像の特徴ベクトルと顔画像テンプレートの特徴ベクトルに対して比較と認証を行うステップとを含む。

【発明の概要】

【発明が解決しようとする課題】

【０００７】

したがって、本発明の目的は、既知の装置及び方法の上述の技術的課題に対する装置及び方法を提供することである。具体的には、本発明の目的は、セキュリティを強化したモバイルデバイスのユーザの認証を可能にする装置及び方法を提供することである。

【課題を解決するための手段】

【０００８】

この問題は、独立特許請求項の特徴を備えた本発明によって解決される。個別に又は組み合わせて実現することができる本発明の有利な展開は、従属請求項及び／又は以下の明細書及び詳細な実施形態に示されている。

【０００９】

以下で使用される場合、「有する」、「備える」、又は「含む」という用語、又はそれらの任意の文法上の変形は、非排他的な方法で使用される。したがって、これらの用語は、これらの用語によって導入された特徴の他に、この文脈で説明されている実体にさらなる特徴が存在しない状況と、１つ以上のさらなる特徴が存在する状況の両方を指し得る。一例として、「ＡはＢを有する」、「ＡはＢを備える」、及び「ＡはＢを含む」という表現は、Ｂ以外にＡに他の要素が存在しない状況（つまり、Ａは専らかつ排他的にＢから構成される状況）と、Ｂに加えて、１つ以上の要素、例えば要素Ｃ、要素ＣとＤ、又はさらに要素などが実体Ａに存在する状況の双方を指し得る。

【００１０】

さらに、「少なくとも１つ」、「１つ以上」という用語、又は、特徴もしくは要素が１回以上存在し得ることを示す同様の表現は、典型的には、それぞれの特徴又は要素を導入するときに１回だけ使用されることに留意されたい。以下では、ほとんどの場合、それぞれの特徴又は要素を参照するときに、「少なくとも１つ」又は「１つ以上」という表現は、それらの特徴又は要素が１回以上現れ得るという事実にもかかわらず、繰り返されないことに留意されたい。

【００１１】

さらに、以下で使用される場合、「好ましくは」、「より好ましくは」、「特に」、「より特に」、「具体的に」、「より具体的に」という用語、又は、同様の用語は、代替の可能性を制限することなく、任意の特徴に関連して使用される。したがって、これらの用語によって導入される特徴は、任意の特徴であり、いかなる意味でも特許請求の範囲を限定することを意図するものではない。本発明は、当業者であれば認識するように、代替的特徴を用いて実施することができる。同様に、「本発明の一実施形態では」又は同様の表現によって導入される特徴は、本発明の代替の実施形態に関するいかなる制限もなく、本発明の範囲に関するいかなる制限もなく、及び、そのような方法で導入される特徴を本発明の他の任意の又は非任意の特徴と組み合わせる可能性に関するいかなる制限もなく、任意の特徴であることが意図されている。

【００１２】

本発明の第１の態様では、モバイルデバイスのユーザを認証する方法が開示される。

【００１３】

本明細書で使用される「モバイルデバイス」という用語は、広義の用語であり、当業者にとって通常で慣用的な意味を与えられるべきであり、特別な意味又はカスタマイズされ

た意味に限定されるべきではない。この用語は、具体的には、限定されることなく、モバイル電子装置、より具体的には携帯電話又はスマートフォンなどのモバイル通信装置を指し得る。追加的に又は代替的に、モバイルデバイスは、タブレットコンピュータ又は他のタイプのポータブルコンピュータを指し得る。

【００１４】

本明細書で使用される「ユーザ」という用語は、広義の用語であり、当業者にとって通常で慣用的な意味を与えられるべきであり、特別な意味又はカスタマイズされた意味に限定されるべきではない。この用語は、具体的には、限定されることなく、モバイルデバイスを使用する人を指し得る。ユーザは、モバイルデバイスの所有者及び／又はその他の権限を有する者であってよい。

【００１５】

本明細書で使用される「認証」という用語は、広義の用語であり、当業者にとって通常で慣用的な意味を与えられるべきであり、特別な意味又はカスタマイズされた意味に限定されるべきではない。この用語は、具体的には、限定されることなく、ユーザの身元を検証することを指し得る。具体的には、認証は、ユーザを他の人間又は物体から区別すること、特に、許可されたアクセスと許可されていないアクセスとを区別することを含むことができる。認証は、それぞれのユーザの身元を検証すること、及び／又はユーザに身元を割り当てることを含むことができる。認証は、例えば、支払いプロセスを実施するための認証のための少なくとも１つの認証ユニットなどの他のデバイス又はユニットに対して、身元情報を生成及び／又は提供することを含むことができる。身元情報は、認証によって証明されることができる。例えば、身元情報は、少なくとも１つの身元トークンであってよく、及び／又はそれを含むことができる。認証に成功した場合、モバイルデバイスのカメラによって記録された顔の画像がユーザの顔の画像であることが検証され、及び／又はユーザの身元が検証される。

【００１６】

この方法は以下のステップ：

a) モバイルデバイスの少なくとも１つのカメラを使用することによって、顔の少なくとも１つの第１画像を画像化するステップと；

b) 第１画像をモバイルデバイスのプロセッサの通常の実行環境に提供し、及び第１画像をプロセッサの信頼できる実行環境に提供するステップと；

c) 通常の実行環境において少なくとも１つのトレーニングされたモデルを使用して第１画像を分析し、それによって画像情報を含む多次元ベクトルを決定するステップと；

d) 顔認証ステップであって、以下のステップ：

di) 多次元ベクトルを信頼できる実行環境に提供するステップと、

dii) 少なくとも１つのデコーダを使用することによって、信頼できる実行環境において多次元ベクトルから第２画像を決定するステップと、

diii) 第１画像と第２画像を比較するステップであって、第１画像と第２画像が同一の場合、多次元ベクトルを検証するステップと；

div) 多次元ベクトルが検証された場合、検証された多次元ベクトルは、信頼できる実行環境において保存されたユーザの顔の多次元ベクトルと比較されるステップであって、多次元ベクトルと保存されたユーザの顔の多次元ベクトルが同一の場合、ユーザは認証されるステップと、

を含む顔検証ステップと、

を含む。

【００１７】

方法ステップは、所定の順序で実施されてもよいし、異なる順序で実施されてもよい。さらに、列挙されていない１つ以上の追加の方法ステップが存在してもよい。さらに、方法ステップの１つ、１つより多く、又は、すべてさえも、繰り返し実施されてよい。

【００１８】

本明細書で使用される「カメラ」という用語は、広義の用語であり、当業者にとって通

常で慣用的な意味を与えられるべきであり、特別な意味又はカスタマイズされた意味に限定されるべきではない。この用語は、具体的には、限定されることなく、空間的に分解された一次元、二次元、さらには三次元の光学データ又は情報を記録又はキャプチャするように構成された少なくとも１つの画像要素を有する装置を指し得る。一例として、カメラは、画像を記録するように構成された少なくとも１つのＣＣＤチップ及び／又は少なくとも１つのＣＭＯＳチップなどの少なくとも１つのカメラチップを備えてよい。例えば、カメラは、以下で詳細に説明するように、少なくとも３つのカラーピクセルを備えるカラーカメラであってよい。カメラはカラーＣＭＯＳカメラであってよい。例えば、カメラは白黒ピクセルとカラーピクセルを含んでよい。カラーピクセルと白黒ピクセルは、カメラの内部で組み合わされてよい。カメラは、少なくとも１つのカラーカメラと、白黒ＣＭＯＳなど少なくとも１つの白黒カメラを備えることができる。カメラは、少なくとも１つの白黒ＣＭＯＳチップを備えることができる。カメラは一般に、ピクセルなどの画像センサの一次元又は二次元アレイを備えることができる。

【００１９】

カメラは、少なくとも１つのカメラチップ又は画像チップに加えて、１つ以上の光学要素、例えば１つ以上のレンズなどのさらなる要素を含んでいてよい。一例として、カメラは、カメラに対して固定的に調整された少なくとも１つのレンズを有する固定焦点カメラであってよい。あるいは、しかし、カメラは自動又は手動で調整され得る１つ以上の可変レンズを備えていてよい。しかし、他のカメラも可能である。

【００２０】

本明細書で使用される「画像化」という用語は、広義の用語であり、当業者にとって通常で慣用的な意味を与えられるべきであり、特別な意味又はカスタマイズされた意味に限定されるべきではない。この用語は、具体的には、限定されることなく、カメラを使用することによって少なくとも１つの画像をキャプチャ及び／又は生成及び／又は決定及び／又は記録することを指し得る。画像化は、単一の画像及び／又は一連の画像などの複数の画像をキャプチャすることを含んでよい。例えば、画像化は、ビデオ又はムービーのような一連の画像を連続的に記録することを含んでよい。画像化は、ユーザの動作によって開始されてよく、又は、例えば、視野内及び／又はカメラの視野の所定のセクタ内に少なくとも１つの物体が存在することが自動的に検出されると、自動的に開始されてよい。画像化は、モバイルデバイスのプロセッサによってサポートされてよい。

【００２１】

本明細書で使用される場合、限定されることなく、「画像」という用語は、具体的には、カメラチップのピクセルなどカメラからの複数の電子読み取り値など、カメラを使用することによって記録されるデータに関し得る。第１画像は、カメラを使用することによって画像化された初期画像であってよい。第１画像は、生(raw)の画像データを含んでよく、又は前処理された画像であってよい。例えば、前処理は、生画像データに少なくとも１つのフィルタ、及び／又は少なくとも１つの背景補正、及び／又は少なくとも１つの背景減算を適用することを含んでよい。第１画像は、顔を含むシーンを含んでよい。前処理は、顔検出の実施及び／又は関心領域の選択のうちの１つ以上を含んでよい。関心領域は、手動で決定されてよく、又は第１画像内の特徴を認識することなどによって自動的に決定されてよい。

【００２２】

本明細書で使用される「プロセッサ」という用語は、広義の用語であり、当業者にとって通常で慣用的な意味を与えられるべきであり、特別な意味又はカスタマイズされた意味に限定されるべきではない。この用語は、具体的には、限定されることなく、コンピュータ又はシステムの基本動作を実施するように構成された任意の論理回路、及び／又は一般に、計算もしくは論理動作を実施するように構成された装置を指し得る。特に、プロセッサは、コンピュータ又はシステムを駆動する基本命令を処理するように構成されることができる。一例として、プロセッサは、少なくとも１つの算術論理ユニット（ＡＬＵ）、数学コプロセッサ又は数値コプロセッサなどの少なくとも１つの浮動小数点ユニット（ＦＰ

Ｕ）、複数のレジスタ、具体的にはＡＬＵにオペランドを供給して動作結果を記憶するように構成されたレジスタ、ならびにＬ１及びＬ２キャッシュメモリなどのメモリを備えることができる。特に、プロセッサはマルチコアプロセッサであってよい。具体的には、プロセッサは、中央処理装置（ＣＰＵ）であってよく、又はそれを備えてよい。追加的に又は代替的に、プロセッサは、マイクロプロセッサであってよく、又はそれを備えてよく、したがって、具体的には、プロセッサの要素は、１つの単一の集積回路（ＩＣ）チップに含まれてもよい。追加的に又は代替的に、プロセッサは、１つ以上の特定用途向け集積回路（ＡＳＩＣ）及び／又は１つ以上のフィールドプログラマブルゲートアレイ（ＦＰＧＡ）及び／又は１つ以上のテンソル処理ユニット（ＴＰＵ）及び／又は専用の機械学習最適化チップなどの１つ以上のチップであってよく、又はそれらを備えてよい。プロセッサは、具体的には、例えばソフトウェアプログラミングなどによって、１つ以上の評価動作を実施するように構成され得る。

【００２３】

本明細書で使用される「実行環境」という用語は、広義の用語であり、当業者にとって通常で慣用的な意味を与えられるべきであり、特別な意味又はカスタマイズされた意味に限定されるべきではない。この用語は、具体的には、限定されることなく、アプリケーションの実行をサポートするように構成されたファシリティを提供するハードウェア及びソフトウェアコンポーネントのセットを指し得る。実行環境は、グローバルプラットフォームテクノロジー(GlobalPlatform Technology)、TEEシステムアーキテクチャ(TEE System Architecture)、バージョン1.2、公開リリース2018年11月、ドキュメント参照：GPD_SPE_009、又はwww.qualcomm.com/media/documents/files/guard-your-data-with-the-qualcomm-snapdragon-mobile-platform.pdf、又はwww.arm.com/why-arm/technologies/trustzone-for-cortex-a/tee-reference-documentationniに記載されているように設計されることができる。具体的には、実行環境は、少なくとも１つのハードウェア処理ユニットと、少なくとも１つのメモリ、特に揮発性メモリ及び不揮発性メモリと、ハードウェア処理ユニットと他のハードウェアリソースとの間の接続と、周辺インターフェースとを備えることができる。

【００２４】

本明細書で使用される、リッチ実行環境（Rich Execution Environment）とも呼ばれる「通常の実行環境」という用語は、広義の用語であり、当業者にとって通常で慣用的な意味を与えられるべきであり、特別な意味又はカスタマイズされた意味に限定されるべきではない。通常の実行環境は、グローバルプラットフォームテクノロジー(GlobalPlatform Technology)、TEEシステムアーキテクチャ(TEE System Architecture)、バージョン1.2、公開リリース2018年11月、ドキュメント参照：GPD_SPE_009、又はwww.qualcomm.com/media/documents/files/guard-your-data-with-the-qualcomm-snapdragon-mobile-platform.pdf又は、www.arm.com/why-arm/technologies/trustzone-for-cortex-a/tee-reference-documentationに記載されているように設計されることができる。「通常の実行環境」という用語は、具体的には、限定されることなく、少なくとも１つのデバイスオペレーティングシステム（ＯＳ）及び／又はリッチオペレーティングシステム（リッチＯＳ）と、デバイスのその他すべてのコンポーネント、特に少なくとも１つのシステムオンチップ（ＳｏＣ）、他のディスクリートコンポーネント、ファームウェア、及びＯＳ及び／又はリッチＯＳを実行、ホスト、及びサポートするように構成されたソフトウェアとを含むプロセッサの実行環境を指し得る。ＳｏＣは、そのすべてのコンポーネントが単一の集積回路に含まれる電子システムであってよい。通常の実行環境は、モバイルデバイスに含まれる信頼できる実行環境及びセキュアエレメント（ＳＥ）を除外してよい。具体的には、通常の実行環境は、信頼できる実行環境の外側にあるすべてのものであってよい。通常の実行環境は、特に、サイズ及びＯＳ及び／又はリッチＯＳの必要性に起因して、信頼できる実行環境のハードウェアの外側の実行環境で実行されてよい。通常の実行環境は、信頼できる実行環境と比較して物理的なセキュリティ境界がはるかに低い可能性がある。したがって、通常の実行環境は

信頼されていないと考えられ得る。しかし、内部的な信頼構造が通常の実行環境に存在し得る。

【００２５】

本明細書で使用される「信頼できる実行環境（Trusted Execution Environment：ＴＥＥ）」という用語は、広義の用語であり、当業者にとって通常で慣用的な意味を与えられるべきであり、特別な意味又はカスタマイズされた意味に限定されるべきではない。信頼できる実行環境は、グローバルプラットフォームテクノロジー(GlobalPlatform Technology)、ＴＥＥシステムアーキテクチャ(TEE System Architecture)、バージョン1.2、公開リリース2018年11月、ドキュメント参照：GPD_SPE_009、又はwww.qualcomm.com/media/documents/files/guard-your-data-with-the-qualcomm-snapdragon-mobile-platform.pdf、又はwww.arm.com/why-arm/technologies/trustzone-for-cortex-a/tee-reference-documentationに記載されているように設計されることができる。「信頼できる実行環境」という用語は、具体的には、限定されることなく、少なくとも１つのセキュリティ機能を備え、少なくとも１つのセキュリティ要件を満たす実行環境を指し得る。信頼できる実行環境は、信頼できる実行環境内の資産を一般的なソフトウェア攻撃から保護するように構成され得る。信頼できる実行環境は、プログラムがアクセスできるデータ及び機能に関する厳格なセーフガードを定義するように構成され得る。信頼できる実行環境は、定義された一連の脅威に抵抗するように構成されることができる。信頼できる実行環境を実装するための複数の技術が知られており、達成されるセキュリティレベルはそれに応じて変化し得る。具体的には、信頼できる実行環境は、source.android.com/compatibility/11/android-11-cdd#7_3_10_biometric_sensorsに記載されているようなセキュリティ要件を満たし得る。ＴＥＥは、特に、生体認証ベースの認証又は登録が行われている間、ＴＥＥの外部で、カメラフレームが読み取られたり変更されたりすることを防止するモードで、カメラを作動させ、又はＴＥＥへのセキュアチャネルを持つチップを作動させることができる。ＲＧＢシングルカメラソリューションの場合、カメラフレームは、登録のためのプレビューなどの操作をサポートするために、ＴＥＥの外部で読み取ることができるが、それでも変更されることはできない。ＴＥＥは、ＴＥＥのコンテキスト外で、プロセッサの一部への、識別可能な生体認証データ又はそこから派生するデータ（埋め込みデータなど）への暗号化されていないアクセスを許可してはならない。ＴＥＥは、オペレーティングシステム又はカーネルの侵害によって、データが直接注入されてユーザとして誤って認証できないように、セキュア処理パイプラインを有することができる。ＴＥＥは、ハードウェアに支援されたキーストアの実装を有することができる。ＴＥＥは、ＴＥＥ又はＴＥＥとのセキュアチャネルを備えたチップの外部で取得、読み取り、又は改ざんできないように、すべての識別可能なデータを暗号化し、暗号的に認証することができる。ＴＥＥは、ユーザに既存のデバイスクレデンシャルを確認させたり、又は、例えばＴＥＥによって保証された(secured)ＰＩＮ及び／又はパターン及び／又はパスワードなど、新しいデバイスクレデンシャルを追加させたりすることによって、トラストチェーンを最初に確立することなく、新しい生体認証を追加することを防止することができる。

【００２６】

信頼できる実行環境は、通常の実行環境から分離された実行環境であってよい。信頼できる実行環境は、物理的分離、ハードウェアロジックベースの分離、又は暗号的分離方法の１つ以上によって、通常の実行環境から分離されることができる。具体的には、信頼できる実行環境は、ＴＥＥ常駐ブートソフトウェア又はランタイムソフトウェアによって構成可能なＴＥＥシステムハードウェアを介して、電子アクセス制御によって、通常の実行環境から分離され得る。

【００２７】

本明細書で使用される第１画像を「提供する」という用語は、広義の用語であり、当業者にとって通常で慣用的な意味を与えられるべきであり、特別な意味又はカスタマイズされた意味に限定されるべきではない。この用語は、具体的には、限定されることなく、カ

メラによって記録された画像データをモバイルデバイスのプロセッサ、特に通常の実行環境及び信頼できる実行環境に転送することを指し得る。第１画像は、通常パス（regular path）を介して通常の実行環境に提供されてよい。通常パスは、信頼されないパスであってもよい。通常パスは、通常の実行環境及び／又は信頼できる実行環境内でソフトウェアによるアクセスを許可するように構成されてよい。第１画像は、セキュアパスを介して信頼できる実行環境に提供されてよく、セキュアパスは、第１画像が通常の実行環境内の任意のソフトウェアによって導出及び／又は変更されることを防止するように構成されてよい。

【００２８】

第１画像の分析は、通常の実行環境で実施される。このため、第１画像の分析に高い計算能力とメモリ容量が利用され得る。

【００２９】

ステップc)における分析は、第１画像のフィルタリング及び畳み込みのうちの１つ以上を含むことができる。トレーニングされたモデルは、少なくとも１つの顔認識モデルを含むことができる。第１画像の分析は、ＦａｃｅＮｅｔなどの顔認識システムを使用することによって実施されることができる。したがって、顔認識システムは、フロリアン・シュロフ(Florian Schroff)，ドミトリー・カレニチェンコ(Dmitry Kalenichenko)，ジェームズ・フィルビン(James Philbin)，「ＦａｃｅＮｅｔ：顔認識とクラスタリングのための統合埋め込み（FaceNet：A Unified Embedding for Face Recognition and Clustering）」，arXiv:1503.03832に記載されるように設計され得る。

【００３０】

本明細書で使用される「トレーニングされたモデル」という用語は、広義の用語であり、当業者にとって通常で慣用的な意味を与えられるべきであり、特別な意味又はカスタマイズされた意味に限定されるべきではない。この用語は、具体的には、限定されることなく、少なくとも１つのトレーニングデータセットでトレーニングされた数学的モデルを指し得る。トレーニングされたモデルは、追加のトレーニングデータに基づいて再トレーニング及び／又は更新されることができる。トレーニングされたモデルは、機械学習を使用することによってトレーニングされることができる。本明細書で使用される「機械学習」という用語は、広義の用語であり、当業者にとって通常で慣用的な意味を与えられるべきであり、特別な意味又はカスタマイズされた意味に限定されるべきではない。この用語は、具体的には、限定されることなく、自動的なモデル構築のため、特にモデルのパラメータ化のために人工知能（ＡＩ）を使用する方法を指し得る。トレーニングされたモデルは、機械学習、深層学習、ニューラルネットワーク、又は他の形態の人工知能のうちの１つ以上を使用することによってパラメータ化され得る。トレーニングされたモデルは、トレーニングデータの記録を使用してトレーニングされてよい。トレーニングデータの記録は、トレーニング入力データ及び対応するトレーニング出力データを含むことができる。トレーニングデータの記録のトレーニング出力データは、同じトレーニングデータの記録のトレーニング入力データを入力として与えられたときにモデルによって生成されると予想される結果であり得る。この予想される結果と、アルゴリズムによって生成された実際の結果との間の偏差は、「損失関数」によって観察され、評価され得る。この損失関数は、モデルのパラメータを調整するためのフィードバックとして使用されることができる。例えば、すべてのトレーニング入力データをモデルに入力し、その結果を対応するトレーニング出力データと比較したときに得られる損失関数の値を最小化するという最適化目標でパラメータを調整することができる。このトレーニングの結果は、「グラウンドトルス」としてトレーニングデータの比較的少数の記録が与えられると、モデルは、何桁も多い入力データの記録数に対してその仕事をうまく実施できるようになる。したがって、モデルは少なくとも１つのアルゴリズムとモデルパラメータを含むことができる。モデルのパラメータは、少なくとも１つの人工ニューラルネットワークを使用することによって生成されることができる。

【００３１】

トレーニングされたモデルは、少なくとも１つの畳み込みニューラルネットワークを含むことができる。例えば、畳み込みニューラルネットワークは、M. D. Zeiler及びR. Fergus, 「畳み込みネットワークの視覚化と理解（Visualizing and understanding convolutional networks）, CoRR, abs/1311.2901, 2013、又はC. Szegedyら、「畳み込みを深くする（Going deeper with convolutions）」、 CoRR, abs/1409.4842, 2014に記載されているように設計されてよい。顔認識システムのための畳み込みニューラルネットワークに関する詳細については、フロリアン・シュロフ(Florian Schroff), ドミトリー・カレニチェンコ(Dmitry Kalenichenko), ジェームズ・フィルビン(James Philbin), 「ＦａｃｅＮｅｔ：顔認識とクラスタリングのための統合埋め込み（FaceNet：A Unified Embedding for Face Recognition and Clustering）」, arXiv:1503.03832を参照されたい。

【００３２】

トレーニングデータとして、画像データベースからラベル付けされた画像データを使用することができる。具体的には、ラベル付き顔は、G. B. Huang、M. Ramesh、T. Berg、及びE. Learned-Miller、「Labeled faces in the wild：制約のない環境での顔認識を研究するためのデータベース（A database for studying face recognition in unconstrained environments）」, テクニカルレポート 07-49, マサチューセッツ大学, Amherst, 2007年10月、2011年にCVPRのIEEE Conf.でWolf, T. Hassner, and I. Maoz「背景の類似性が一致した制約のないビデオでの顔認識（Face recognition in unconstrained videos with matched background similarity）」で説明されているようなYoutube（登録商標）Facesデータベース、又はGoogle（登録商標）表情比較データセット（Facial Expression Comparison dataset）の１つ以上を使用することができる。畳み込みニューラルネットワークのトレーニングは、フロリアン・シュロフ(Florian Schroff), ドミトリー・カレニチェンコ(Dmitry Kalenichenko), ジェームズ・フィルビン(James Philbin), 「ＦａｃｅＮｅｔ：顔認識とクラスタリングのための統合埋め込み（FaceNet：A Unified Embedding for Face Recognition and Clustering）」, arXiv:1503.03832に記載されているように実施され得る。

【００３３】

トレーニングされたモデルを使用したステップc）における分析の出力は、多次元ベクトルであってよい。多次元ベクトルは、埋め込み、具体的には、第１画像の低次元表現であってよい。トレーニングされたモデルへの入力として第１画像から多次元ベクトルを決定することは、フロリアン・シュロフ(Florian Schroff), ドミトリー・カレニチェンコ(Dmitry Kalenichenko), ジェームズ・フィルビン(James Philbin), 「ＦａｃｅＮｅｔ：顔認識とクラスタリングのための統合埋め込み（FaceNet：A Unified Embedding for Face Recognition and Clustering）」, arXiv:1503.03832に記載されているように実施される。具体的には、トレーニングされたモデルは、第１画像から128個の数値のベクトルを決定することができる。多次元ベクトルのエントリは、画像化された顔の特徴であってよい。画像情報は、多次元ベクトルに埋め込まれ、及び／又はマッピングされ得る。画像情報は、第１画像を特徴付け及び／又は定義する第１画像の任意のパラメータであってよい。画像情報は、人物の顔の類似性を検証するために他の画像情報との比較を可能にする情報であってよい。

【００３４】

多次元ベクトルは信頼できる実行環境に提供される。多次元ベクトルの提供は、通常の実行環境と信頼できる実行環境との間の少なくとも１つのインターフェースを使用することによって、特に、信頼できる実行環境から通常の実行環境へのアクセスによって実施されることができる。

【００３５】

信頼できる実行環境において、多次元ベクトルからの第２画像は、少なくとも１つのデコーダを使用することによって決定される。第２画像は、多次元ベクトルから再構築され

た画像であってよい。第２画像を決定することは、デコーダが多次元ベクトルからユーザの顔の画像を再構築することを含んでよい。本明細書で使用される「デコーダ」という用語は、広義の用語であり、当業者にとって通常で慣用的な意味を与えられるべきであり、特別な意味又はカスタマイズされた意味に限定されるべきではない。この用語は、具体的には、限定されることなく、埋め込みから、特に多次元ベクトルから画像を再構築するように構成された、信頼できる実行環境の少なくとも１つの要素を指し得る。このようなデコーダ及びその動作原理は、例えばpapers.nips.cc/paper/2014/file/a14ac55a4f27472c5d894ec1c3c743d2-Paper.pdfに記載されているように、当業者には一般的に知られている。

【００３６】

本方法は、第１画像と第２画像とを比較することを含む。比較は、信頼できる実行環境においてプロセッサによって実施されてよい。比較は、第１画像と第２画像の少なくとも１つの特徴、特に複数の特徴を比較することを含んでよい。比較に使用される特徴は、予め定義されていてよい。第１画像の特徴と第２画像の特徴は同一の画像データに基づいているが、特徴は異なるアルゴリズムを使用することによって生成されている。特に、多次元ベクトルによって含まれる特徴は、上述の顔認識アルゴリズムによって決定された。多次元ベクトルは、ＴＥＥにも保存されている第１画像から決定された。追加的又は代替的に、第１画像と第２画像は、例えばピクセル単位の類似性尺度で比較されてよい。第１画像と第２画像が同一である場合、多次元ベクトルが検証される。本明細書で使用される「同一」という用語は、広義の用語であり、当業者にとって通常で慣用的な意味を与えられるべきであり、特別な意味又はカスタマイズされた意味に限定されるべきではない。この用語は、具体的には、限定されることなく、少なくとも許容範囲内で同一であることを指し得る。第１画像と第２画像は、±３０％、好ましくは±１０％、より好ましくは±５％の許容範囲内で同一であると考えられてよい。

【００３７】

多次元ベクトルが検証された場合、検証された多次元ベクトルは、信頼できる実行環境に保存されたユーザの顔の多次元ベクトルと比較される。そうでない場合、手順は中断及び／又は再開され得る。多次元ベクトルと保存されたユーザの顔の多次元ベクトルが同一の場合、ユーザは認証される。ユーザの顔の多次元ベクトルは、ＴＥＥの少なくとも１つのメモリに保存され得る。上記で概説したように、埋め込みは、例えばスカラー積を使用することによって、互いに比較可能な顔特徴の数学的表現を記述する。

【００３８】

非セキュアな通常の実行環境で画像分析を実施すると、通常の実行環境の計算能力とメモリ容量をすべて活用することができる。信頼できる実行環境に保存された第１画像と比較することにより、通常の実行環境で得られた画像分析の結果を証明することで、セキュリティを強化したユーザの認証が可能になる。

【００３９】

さらなる態様では、ユーザの認証方法が開示される。本方法は、本発明によるモバイルデバイスのユーザを認証するための方法を実施することを含む。本方法はさらに、信頼できる実行環境がプロセスステップを認証するための信号を出力することを含む。プロセスステップは、支払い、文書への署名、モバイルデバイスへのアクセス、ＢｉｏｍｅｔｒｉｃＰｒｏｍｐｔ及び/又はＦＩＤＯ２　ＡＰＩなどのアプリケーションの有効化（source.android.com/security/biometric/measureを参照）のうち１つ以上を含む。

【００４０】

本明細書で使用される「認証」という用語は、広義の用語であり、当業者にとって通常で慣用的な意味を与えられるべきであり、特別な意味又はカスタマイズされた意味に限定されるべきではない。この用語は、具体的には、限定されることなく、さらなるプロセスステップを実行する許可をユーザに付与するプロセスを指し得る。

【００４１】

詳細、オプション、定義については、前述の方法を参照されたい。

【００４２】
さらなる態様は、コンピュータ又はコンピュータネットワーク上で実行されたときに、コンピュータ又はコンピュータネットワークに本発明によるユーザ認証のための方法を完全に又は部分的に実施させるように構成されたモバイルデバイスのユーザ認証のためのコンピュータプログラムであって、該コンピュータプログラムは、本発明による認証のための方法の少なくともステップa)～d)を実施及び／又は実行するように構成される。同様に、コンピュータ可読記憶媒体が開示されており、これは、プログラムがコンピュータ又はコンピュータネットワークによって実行されると、コンピュータ又はコンピュータネットワークに、上記で開示された実施形態のいずれか１つ及び／又は以下でさらに詳細に開示される実施形態のいずれか１つによるなど、本発明による認証のための方法を実施させる命令を含む。本明細書で使用される「コンピュータ可読記憶媒体」という用語は、具体的には、コンピュータ実行可能命令が格納されたハードウェア記憶媒体などの非一時的データ記憶手段を指し得る。コンピュータ可読データキャリア又は記憶媒体は、具体的には、ランダムアクセスメモリ（ＲＡＭ）及び／又はリードオンリーメモリ（ＲＯＭ）などの記憶媒体であってよく、又はそれらを含んでよい。
【００４３】
したがって、具体的には、上記に示したような方法ステップa）～d）の１つ、複数、又はさらにすべてを、コンピュータ又はコンピュータネットワークを使用することによって、好ましくはコンピュータプログラムを使用することによって、実施することができる。
【００４４】
本明細書でさらに開示され提案されるのは、プログラムがコンピュータ又はコンピュータネットワーク上で実施されるときに、本明細書に包含される実施形態の１つ以上において本発明による方法を実行するためのプログラムコード手段を有するコンピュータプログラム製品である。具体的には、プログラムコード手段は、コンピュータ可読データキャリア上及び／又はコンピュータ可読記憶媒体上に保存され得る。
【００４５】
本明細書でさらに開示及び提案されているのは、コンピュータ又はコンピュータネットワーク、例えばコンピュータ又はコンピュータネットワークのワーキングメモリ又はメインメモリにロードされた後、本明細書に開示された実施形態の１つ以上による方法を実行することができる、記憶されたデータ構造を有するデータキャリアである。
【００４６】
本明細書でさらに開示され提案されるのは、１つ以上のプロセッサによって実施されると、１つ以上のプロセッサに、本明細書で開示される実施形態の１つ以上による方法を実行させる命令を含む、非一時的なコンピュータ可読媒体である。
【００４７】
本明細書でさらに開示され提案されるのは、プログラムがコンピュータ又はコンピュータネットワーク上で実行されたときに、本明細書で開示される実施形態の１つ以上による方法を実施するために、機械可読キャリアに格納されたプログラムコード手段を有するコンピュータプログラム製品である。本明細書で使用される場合、コンピュータプログラム製品とは、取引可能な製品としてのプログラムを指す。製品は、一般に、紙形態、又はコンピュータ可読データキャリア上及び／又はコンピュータ可読記憶媒体上など、任意の形態で存在することができる。具体的には、コンピュータプログラム製品は、データネットワークを介して配布され得る。
【００４８】
さらに、本明細書で開示及び提案されているのは、本明細書で開示される実施形態の１つ以上による方法を実施するための、コンピュータシステム又はコンピュータネットワークによって読み取り可能な命令を含む変調データ信号である。
【００４９】
具体的には、本明細書でさらに開示されるのは：

－　少なくとも１つのプロセッサを含むコンピュータ又はコンピュータネットワークであって、該プロセッサが、本明細書に記載の実施形態の１つによる方法を実施するように適合されている、コンピュータ又はコンピュータネットワークと、
－　データ構造がコンピュータ上で実行されている間に、本明細書で記載された実施形態の１つによる方法を実施するように適合された、コンピュータにロード可能なデータ構造と、
－　コンピュータプログラムであって、該プログラムがコンピュータ上で実行されている間、本明細書に記載の実施形態の１つによる方法を実施するように適合されている、コンピュータプログラムと、
－　コンピュータプログラムであって、該コンピュータプログラムがコンピュータ又はコンピュータネットワーク上で実行されている間に、本明細書で説明される実施形態の１つによる方法を実施するためのプログラム手段を含む、コンピュータプログラムと、
－　コンピュータプログラムであって、先行する実施形態によるプログラム手段を備え、該プログラム手段は、コンピュータ可読記憶媒体に格納されている、コンピュータプログラムと、
－　記憶媒体であって、データ構造が記憶媒体に記憶されており、該データ構造が、コンピュータ又はコンピュータネットワークのメインストレージ及び／又はワーキングストレージにロードされた後に、本明細書に記載の実施形態の１つによる方法を実施するように適合されている、記憶媒体と、
－　プログラムコード手段を有するコンピュータプログラム製品であって、該プログラムコード手段は、該プログラムコード手段がコンピュータ又はコンピュータネットワーク上で実行された場合に、本明細書に記載の実施形態の１つによる方法を実施するように、記憶媒体に記憶され得るか、又は記憶媒体に記憶されている、コンピュータプログラム製品と、
である。

【００５０】

本発明のさらなる態様では、モバイルデバイスのユーザを認証するためのコンピュータプログラムが開示される。コンピュータプログラムは、プログラムがコンピュータ又はコンピュータネットワークによって実行されるとき、コンピュータ又はコンピュータネットワークに、上記で開示された実施形態のいずれか１つ及び／又は以下でさらに詳細に開示される実施形態のいずれか１つによるような、本発明による認証方法を実施させる命令を含んでいる。同様に、プログラムがコンピュータ又はコンピュータネットワークによって実行されるとき、コンピュータ又はコンピュータネットワークに、上記で開示された実施形態のいずれか１つ及び／又は以下でさらに詳細に開示される実施形態のいずれか１つによるような、本発明による認証方法を実施させる命令を含む、コンピュータ可読記憶媒体が開示される。

【００５１】

さらなる態様では、モバイルデバイスが開示される。モバイルデバイスは、少なくとも１つのカメラと少なくとも１つのプロセッサとを備える。モバイルデバイスは、例えば、上記で開示された実施形態のいずれか１つ及び／又は以下でさらに詳細に開示される実施形態のいずれか１つによる、本発明による認証方法の少なくともステップａ）～ｄ）を実施するため、及び／又は本発明による認証方法を実施するために構成される。詳細、オプション、及び定義については、上述した方法を参照されたい。

【００５２】

本発明のさらなる態様においては、上記で与えられた又は以下でさらに詳細に与えられる１つ以上の実施形態などによる、本発明によるモバイルデバイスの使用が、１つモバイルデバイス支払い、文書への署名、ＢｉｏｍｅｔｒｉｃＰｒｏｍｐｔ及び／又はＦＩＤＯ２　ＡＰＩ（source.android.com/security/biometric/measureを参照）などからなる群から選択される使用目的のために、提案される。

【００５３】

全体として、本発明の文脈において、以下の実施形態が好ましいと考えられる：
実施形態１．　以下のステップを含む、モバイルデバイスのユーザ認証方法であって：
a) 前記モバイルデバイスの少なくとも１つのカメラを使用することによって、顔の少なくとも１つの第１画像を画像化するステップと；
b) 前記第１画像を前記モバイルデバイスのプロセッサの通常の実行環境に提供し、及び前記第１画像を前記プロセッサの信頼できる実行環境に提供するステップと；
c) 前記通常の実行環境において少なくとも１つのトレーニングされたモデルを使用して前記第１画像を分析し、それによって画像情報を含む多次元ベクトルを決定するステップと；
d) 顔認証ステップであって、以下のステップ：
di) 前記多次元ベクトルを前記信頼できる実行環境に提供するステップと、
dii) 少なくとも１つのデコーダを使用することによって、前記信頼できる実行環境において前記多次元ベクトルから第２画像を決定するステップと、
diii) 前記第１画像と前記第２画像を比較するステップであって、前記第１画像と前記第２画像が同一の場合、前記多次元ベクトルを実証するステップと；
div) 前記多次元ベクトルが実証された場合、前記実証された多次元ベクトルは、前記信頼できる実行環境において保存されたユーザの顔の多次元ベクトルと比較されるステップであって、前記多次元ベクトルと前記保存されたユーザの顔の多次元ベクトルが同一の場合、前記ユーザは認証されるステップと、
を含む顔認証ステップと、
を含む、方法。
【００５４】
実施形態２．　前記信頼できる実行環境は、前記通常の実行環境から分離された実行環境である、先行する実施形態に記載の方法。
【００５５】
実施形態３．　前記信頼できる実行環境は、物理的分離、ハードウェアロジックベースの分離、又は暗号的分離方法の１つ以上によって、前記通常の実行環境から分離される、先行する実施形態に記載の方法。
【００５６】
実施形態４．　前記信頼できる実行環境は、少なくとも１つのセキュリティ機能を備え、少なくとも１つのセキュリティ要件を満たす、先行する実施形態のいずれか１つに記載の方法。
【００５７】
実施形態５．　前記第１画像は、通常パスを介して前記通常の実行環境に提供され、前記通常パスは、前記通常の実行環境及び／又は前記信頼できる実行環境内でソフトウェアによるアクセスを許可するように構成される、先行する実施形態のいずれか１つに記載の方法。
【００５８】
実施形態６．　前記第１画像は、セキュアパスを介して前記信頼できる実行環境に提供され、前記セキュアパスは、前記第１画像が前記通常の実行環境内で任意のソフトウェアによって導出及び／又は変更されることを防止するように構成される、先行する実施形態のいずれか１つに記載の方法。
【００５９】
実施形態７．　前記第２画像を決定することは、前記多次元ベクトルから前記ユーザの顔の画像を再構築するデコーダを含む、先行する実施形態のいずれか１つに記載の方法。
【００６０】
実施形態８．　前記トレーニングされたモデルは、少なくとも１つの顔認識モデルを含む、先行する実施形態のいずれか１つに記載の方法。
【００６１】
実施形態９．　前記トレーニングされたモデルは、少なくとも１つの畳み込みニューラ

ルネットワークを含む、先行する実施形態のいずれか１つに記載の方法。
【００６２】
実施形態１０．　ステップc)における分析は、前記第１画像のフィルタリング及び畳み込みのうちの１つ以上を含む、先行する実施形態に記載の方法。
【００６３】
実施形態１１．　ユーザの認証方法であって、前記方法は、先行する実施形態のいずれか１つに記載のモバイルデバイスのユーザを認証するための方法を実施することを含み、前記方法は、前記信頼できる実行環境がプロセスステップを許可するための信号を出力することをさらに含み、前記プロセスステップは、支払い、文書への署名、前記モバイルデバイスへのアクセス、アプリケーションの有効化のうちの１つ以上を含む、方法。
【００６４】
実施形態１２．　コンピュータ又はコンピュータネットワーク上で実行されたときに、コンピュータ又はコンピュータネットワークに認証方法に関する先行する実施形態のいずれか１つに記載のユーザの認証方法を完全に又は部分的に実施させるように構成されたモバイルデバイスのユーザの認証のためのコンピュータプログラムであって、前記コンピュータプログラムは、認証方法に関する先行する実施形態のいずれか１つに記載のユーザ認証方法の少なくともステップa)～d)を実施及び／又は実行するように構成されている、コンピュータプログラム。
【００６５】
実施形態１３．　前記コンピュータ又はコンピュータネットワーク上で実行されたときに、コンピュータ又はコンピュータネットワークに、実施形態１１に記載のユーザの認証方法を完全に又は部分的に実行させるように構成されたモバイルデバイスのユーザを認証するためのコンピュータプログラム。
【００６６】
実施形態１４．　コンピュータ又はコンピュータネットワークによって実行されたときに、認証に関連する方法を参照する先行する実施形態のいずれか１つに記載の方法の少なくともステップa)～d)を実行させる、及び／又は実施形態１１に記載のユーザの認証方法を実行させる命令を含む、コンピュータ可読記憶媒体。
【００６７】
実施形態１５．　少なくとも１つのカメラと少なくとも１つのプロセッサとを備えるモバイルデバイスであって、前記モバイルデバイスは、認証方法を参照する先行する実施形態のいずれか１つに記載の方法の少なくともステップa)～d)を実行させる、及び／又は実施形態１１に記載の認証方法を実施するように構成される、モバイルデバイス。
【００６８】
実施形態１６．　支払い、文書への署名のうちの１つ以上のための、先行する実施形態に記載のモバイルデバイスの使用。
【図面の簡単な説明】
【００６９】
本発明のさらなる任意選択の詳細及び特徴は、従属請求項と関連して続く好ましい例示的な実施形態の説明から明らかである。この文脈において、特定の特徴は、孤立した形で、又は他の特徴と組み合わせて実施され得る。本発明は、例示的な実施形態に限定されるものではない。例示的な実施形態は、図に概略的に示されている。個々の図における同一の参照数字は、同一の要素又は同一の機能を有する要素、あるいは、機能に関して互いに対応する要素を指す。
【図１】モバイルデバイスのユーザを認証する方法の実施形態を示す図である。
【図２】本発明によるモバイルデバイスの一実施形態を示す図である。
【発明を実施するための形態】
【００７０】
実施形態の詳細な説明：
図１は、モバイルデバイス１１０のユーザを認証する方法の一実施形態のフローチャー

トを示す。モバイルデバイス１１０は、モバイル電子装置、より具体的には携帯電話又はスマートフォンなどのモバイル通信装置であり得る。追加的に又は代替的に、モバイルデバイス１１０は、タブレットコンピュータ又は他のタイプのポータブルコンピュータをも指し得る。

【００７１】

ユーザは、モバイルデバイス１１０を使用する人であってよい。モバイルデバイス１１０の一実施形態が図２に非常に概略的に示されている。ユーザは、モバイルデバイス１１０の所有者及び／又はその他の権限を有する人であってよい。認証は、ユーザを他の人間又は物体から区別すること、特に、許可されたアクセスと許可されていないアクセスとを区別することを含むことができる。認証は、それぞれのユーザの身元を検証すること、及び／又はユーザに身元を割り当てることを含むことができる。認証は、例えば、支払いプロセスを実行するための認証のために少なくとも１つの認証ユニットを他のデバイス又はユニットへなど、例えば他のデバイス又はユニットに対して、身元情報を生成及び／又は提供することを含むことができる。身元情報は、認証によって証明されることができる。例えば、身元情報は、少なくとも１つの身元トークンであってよく、及び／又はそれを含むことができる。認証に成功した場合、モバイルデバイス１１０のカメラ１１２によって記録された顔の画像がユーザの顔の画像であることが検証され、及び／又はユーザの身元が検証される。

【００７２】

この方法は以下のステップ：

a) （参照番号１１４で示される）モバイルデバイス１１０の少なくとも１つのカメラ１１２を使用することによって、顔の少なくとも１つの第１画像１１６を画像化するステップと；

b) （参照番号１１８で示される）第１画像１１６をモバイルデバイス１１０のプロセッサ１２２の通常の実行環境１２０に提供し、及び第１画像１１６をプロセッサ１２２の信頼できる実行環境１２４に提供するステップと；

c) （参照番号１２６で示される）通常の実行環境１２０において少なくとも１つのトレーニングされたモデルを使用して第１画像１１６を分析し、それによって画像情報を含む多次元ベクトルを決定するステップと；

d) （参照番号１２８で示される）顔認証ステップであって、以下のステップ：

di) （図２の矢印１３０で示される）多次元ベクトルを信頼できる実行環境１２４に提供するステップと、

dii) 少なくとも１つのデコーダ１３２を使用することによって、信頼できる実行環境１２４において多次元ベクトルから第２画像を決定するステップと、

diii) 第１画像１１６と第２画像を比較するステップであって、第１画像１１６と第２画像が同一の場合、多次元ベクトルを検証するステップと；

div) 多次元ベクトルが検証された場合、検証された多次元ベクトルは、信頼できる実行環境１２４において保存されたユーザの顔の多次元ベクトルと比較されるステップであって、多次元ベクトルと保存されたユーザの顔の多次元ベクトルが同一の場合、ユーザは認証されるステップと、

を含む顔検証ステップと、

を含む。

【００７３】

カメラ１１２は、空間的に分解された一次元、二次元、さらには三次元の光学データ又は情報を記録又はキャプチャするように構成された少なくとも１つの画像要素を有する装置を指し得る。一例として、カメラ１１２は、画像を記録するように構成された少なくとも１つのＣＣＤチップ及び／又は少なくとも１つのＣＭＯＳチップなどの少なくとも１つのカメラチップを備えてよい。例えば、カメラ１１２は、以下で詳細に説明するように、少なくとも３つのカラーピクセルを備えるカラーカメラであってよい。カメラ１１２はカラーＣＭＯＳカメラであってよい。例えば、カメラ１１２は白黒ピクセルとカラーピクセ

ルを含んでよい。カラーピクセルと白黒ピクセルは、カメラの内部で組み合わされてよい。カメラは、少なくとも１つのカラーカメラと白黒ＣＭＯＳなどの少なくとも１つの白黒カメラを備えることができる。カメラ１１２は、少なくとも１つの白黒ＣＭＯＳチップを備えることができる。カメラ１１２は一般に、ピクセルなどの画像センサの一次元又は二次元アレイを備えることができる。

【００７４】

第１画像１１６は、カメラ１１２を使用することによって画像化された初期画像であってよい。第１画像１１６は、生の画像データを含んでよく、又は前処理された画像であってよい。例えば、前処理は、生画像データに、少なくとも１つのフィルタ、及び／又は少なくとも１つの背景補正、及び／又は少なくとも１つの背景減算を適用することを含んでよい。第１画像は、顔を含むシーンを含んでよい。前処理は、顔検出の実施及び／又は関心領域の選択のうちの１つ以上を含んでよい。関心領域は、手動で決定されてよく、又は第１画像内で特徴を認識することなどによって自動的に決定されてよい。第１画像１１６の前処理は、カメラ１１２によって、及び／又はモバイルデバイス１１０のプロセッサ１２２によって実施されてよい。

【００７５】

通常の実行環境１２０は、グローバルプラットフォームテクノロジー(GlobalPlatform Technology)、TEEシステムアーキテクチャ(TEE System Architecture)、バージョン1.2、公開リリース2018年11月、ドキュメント参照：GPD_SPE_009、又はwww.qualcomm.com/media/documents/files/guard-your-data-with-the-qualcomm-snapdragon-mobile-platform.pdf、又はwww.arm.com/why-arm/technologies/trustzone-for-cortex-a/tee-reference-documentationに記載されているように設計されることができる。通常の実行環境１２０は、少なくとも１つのデバイスオペレーティングシステム（ＯＳ）及び／又はリッチオペレーティングシステム（リッチＯＳ）と、プロセッサ１２２の他のすべてのコンポーネント、特に少なくとも１つのシステムオンチップ（ＳｏＣ）、他のディスクリートコンポーネント、ファームウェア、及びＯＳ及び／又はリッチＯＳを実行、ホスト、及びサポートするように構成されたソフトウェアとを含むプロセッサの実行環境であってよい。ＳｏＣは、そのすべてのコンポーネントが単一の集積回路に含まれる電子システムであってよい。通常の実行環境１２０は、モバイルデバイスに含まれる任意の信頼できる実行環境及びセキュアエレメント（ＳＥ）を除外することができる。具体的には、通常の実行環境１２０は、信頼できる実行環境の外側のすべてであってよい。通常の実行環境１２０は、特に、サイズ及びＯＳ及び／又はリッチＯＳの必要性に起因して、信頼できる実行環境のハードウェアの外側の実行環境で実行されてよい。通常の実行環境１２０は、信頼できる実行環境と比較して物理的セキュリティ境界がはるかに低い場合がある。したがって、通常の実行環境１２０は信頼されていないと考えられ得る。しかし、内部的な信頼構造が通常の実行環境１２０に存在する可能性がある。

【００７６】

信頼できる実行環境１２４は、グローバルプラットフォームテクノロジー(GlobalPlatform Technology)、TEEシステムアーキテクチャ(TEE System Architecture)、バージョン1.2、公開リリース2018年11月、ドキュメント参照：GPD_SPE_009、又はwww.qualcomm.com/media/documents/files/guard-your-data-with-the-qualcomm-snapdragon-mobile-platform.pdf、又はwww.arm.com/why-arm/technologies/trustzone-for-cortex-a/tee-reference-documentationniに記載されているように設計されることができる。信頼できる実行環境１２４は、少なくとも１つのセキュリティ機能を備え、少なくとも１つのセキュリティ要件を満たす実行環境であってよい。信頼できる実行環境１２４は、信頼できる実行環境１２４内の資産を一般的なソフトウェア攻撃から保護するように構成され得る。信頼できる実行環境１２４は、プログラムがアクセスできるデータ及び機能に関する厳格なセーフガードを定義するように構成され得る。信頼できる実行環境１２４は、定義された一連の脅威に抵抗するように構

成されることができる。信頼できる実行環境を実装するための複数の技術が知られており、達成されるセキュリティレベルはそれに応じて変化し得る。具体的には、信頼できる実行環境１２４は、source.android.com/compatibility/11/android-11-cdd#7_3_10_biometric_sensorsに記載されているようなセキュリティ要件を満たし得る。ＴＥＥ１２４は、特に、生体認証ベースの認証又は登録が行われている間、ＴＥＥ１２４の外部でカメラフレームが読み取られたり変更されたりすることを防止するモードで、カメラ１１２を作動させ、又は、ＴＥＥ１２４へのセキュアチャネルを持つチップを作動させることができる。ＲＧＢシングルカメラソリューションの場合、カメラフレームは、例えば登録のためのプレビューなどの操作をサポートするために、ＴＥＥ１２４の外部で読み取ることができるが、それでも変更することはできない。ＴＥＥ１２４は、識別可能な生体認証データ又はそこから派生するデータ（埋め込みデータなど）に対する、ＴＥＥ１２４のコンテキスト外のプロセッサの一部への暗号化されていないアクセスを許可してはならない。ＴＥＥ１２４は、オペレーティングシステム又はカーネルの侵害によって、データが直接注入されてユーザとして誤って認証されないように、セキュア処理パイプラインを有することができる。ＴＥＥ１２４は、ハードウェアに支援されたキーストアの実装を有することができる。ＴＥＥ１２４は、すべての識別可能なデータを暗号化し、暗号的に認証することで、ＴＥＥ１２４又はＴＥＥ１２４とのセキュアチャネルを備えたチップの外部で取得、読み取り、又は改ざんできないようにすることができる。ＴＥＥ１２４は、ＴＥＥ１２４によって保証された(secured)ＰＩＮ及び／又はパターン及び／又はパスワードなど、既存のデバイスクレデンシャルをユーザに確認させたり、又は新しいデバイスクレデンシャルを追加させたりすることによって、トラストチェーンを最初に確立することなく、新しい生体認証を追加することを防止することができる。

【００７７】

信頼できる実行環境１２４は、通常の実行環境１２０から分離された実行環境であってよい。信頼できる実行環境１２４は、物理的分離、ハードウェアロジックベースの分離、又は暗号的分離方法の１つ以上によって、通常の実行環境１２０から分離されることができる。具体的には、信頼できる実行環境１２４は、ＴＥＥ常駐ブートソフトウェア又はランタイムソフトウェアによって構成可能なＴＥＥシステムハードウェアを介した電子アクセス制御によって、通常の実行環境１２０から分離され得る。

【００７８】

第１画像１１６は、通常パス１３４を介して通常の実行環境１２０に提供されてよい。通常パス１３４は、信頼されないパスであってもよい。通常パス１３４は、通常の実行環境１２０及び／又は信頼できる実行環境１２４内でソフトウェアによるアクセスを許可するように構成されてよい。第１画像１１６は、セキュアパス１３６を介して信頼できる実行環境１２４に提供されてよく、セキュアパス１３６は、第１画像１１６が通常の実行環境１２０内で任意のソフトウェアによって導出及び／又は変更されることを防止するように構成されてよい。

【００７９】

第１画像１１６の分析は、通常の実行環境１２０で実施される。このため、第１画像１１６の分析に高い計算能力とメモリ容量が利用され得る。

【００８０】

ステップc)における分析は、第１画像１１６のフィルタリング及び畳み込みのうちの１つ以上を含むことができる。トレーニングされたモデルは、少なくとも１つの顔認識モデルを含むことができる。第１画像の分析は、ＦａｃｅＮｅｔなどの顔認識システムを使用することによって実施されることができる。したがって、顔認識システムは、フロリアン・シュロフ(Florian Schroff)，ドミトリー・カレニチェンコ(Dmitry Kalenichenko)，ジェームズ・フィルビン(James Philbin)，「ＦａｃｅＮｅｔ：顔認識とクラスタリングのための統合埋め込み（FaceNet：A Unified Embedding for Face Recognition and Clustering）」，arXiv:1503.03832に記載されるように設計され得る。

【００８１】

トレーニングされたモデルは、少なくとも１つの畳み込みニューラルネットワークを含むことができる。例えば、畳み込みニューラルネットワークは、M. D. Zeiler及びR. Fergus, 「畳み込みネットワークの視覚化と理解（Visualizing and understanding convolutional networks）, CoRR, abs/1311.2901, 2013、又はC. Szegedyら、「畳み込みを深くする（Going deeper with convolutions）」、 CoRR, abs/1409.4842, 2014に記載されているように設計されてよい。顔認識システムのための畳み込みニューラルネットワークに関するさらなる詳細については、フロリアン・シュロフ(Florian Schroff), ドミトリー・カレニチェンコ(Dmitry Kalenichenko), ジェームズ・フィルビン(James Philbin), 「ＦａｃｅＮｅｔ：顔認識とクラスタリングのための統合埋め込み（FaceNet：A Unified Embedding for Face Recognition and Clustering）」, arXiv:1503.03832を参照されたい。

【００８２】

トレーニングデータとして、画像データベースからラベル付けされた画像データを使用することができる。具体的には、ラベル付き顔は、G. B. Huang、M. Ramesh、T. Berg、及びE. Learned-Miller、「Labeled faces in the wild：制約のない環境での顔認識を研究するためのデータベース（A database for studying face recognition in unconstrained environments）」, テクニカルレポート 07-49, マサチューセッツ大学, Amherst, 2007年10月、2011年にCVPRのIEEE Conf.でWolf, T. Hassner, and I. Maoz「背景の類似性が一致した制約のないビデオでの顔認識（Face recognition in unconstrained videos with matched background similarity）」で説明されているようなYoutube（登録商標）Facesデータベース、又はGoogle（登録商標）表情比較データセット（Facial Expression Comparison dataset）の１つ以上を使用することができる。畳み込みニューラルネットワークのトレーニングは、フロリアン・シュロフ(Florian Schroff), ドミトリー・カレニチェンコ(Dmitry Kalenichenko), ジェームズ・フィルビン(James Philbin), 「ＦａｃｅＮｅｔ：顔認識とクラスタリングのための統合埋め込み（FaceNet：A Unified Embedding for Face Recognition and Clustering）」, arXiv:1503.03832に記載されているように実施され得る。

【００８３】

トレーニングされたモデルを使用したステップc）における分析の出力は、多次元ベクトルであってよい。多次元ベクトルは、埋め込み、具体的には、第１画像の低次元表現であってよい。トレーニングされたモデルへの入力として第１画像から多次元ベクトルを決定することは、フロリアン・シュロフ(Florian Schroff), ドミトリー・カレニチェンコ(Dmitry Kalenichenko), ジェームズ・フィルビン(James Philbin), 「ＦａｃｅＮｅｔ：顔認識とクラスタリングのための統合埋め込み（FaceNet：A Unified Embedding for Face Recognition and Clustering）」, arXiv:1503.03832に記載されているように実行される。具体的には、トレーニングされたモデルは、第１画像から128個の数値のベクトルを決定することができる。多次元ベクトルのエントリは、画像化された顔の特徴であってよい。画像情報は、多次元ベクトルに埋め込まれ、及び／又はマッピングされ得る。画像情報は、第１画像１１６を特徴付け及び／又は定義する第１画像１１６の任意のパラメータであってよい。画像情報は、人物の顔の類似性を検証するために他の画像情報との比較を可能にする情報であってよい。画像情報は、埋め込みを使用して第１画像１１６の再構築を可能にする情報であってよい。

【００８４】

多次元ベクトルは信頼できる実行環境１２４に提供される。多次元ベクトルの提供は、通常の実行環境１２０と信頼できる実行環境１２４との間の少なくとも１つのインターフェースを使用することによって、特に、信頼できる実行環境１２４から通常の実行環境１２０へのアクセスによって実施されることができる。

【００８５】

信頼できる実行環境１２４において、多次元ベクトルからの第２画像は、少なくとも１

つのデコーダ１３２を使用することによって決定される。第２画像は、多次元ベクトルから再構築された画像であってよい。第２画像を決定することは、多次元ベクトルからユーザの顔の画像を再構築するデコーダ１３２を含んでよい。デコーダ１３２は、埋め込みから、特に多次元ベクトルから画像を再構築するように構成された、信頼できる実行環境１２４の少なくとも１つの要素であってよい。このようなデコーダ１３２及びその動作原理は、例えばpapers.nips.cc/paper/2014/file/a14ac55a4f27472c5d894ec1c3c743d2-Paper.pdfに記載されているように、当業者には一般的に知られている。

【００８６】

本方法は、第１画像１１６と第２画像とを比較することを含む。比較は、信頼できる実行環境においてプロセッサ１２０によって実施されてよい。比較は、第１画像１１６と第２画像の少なくとも１つの特徴、特に複数の特徴を比較することを含んでよい。比較に使用される特徴は、予め定義されていてよい。第１画像１１６の特徴と第２画像の特徴は同一の画像データに基づいているが、特徴は異なるアルゴリズムを使用することによって生成されている。特に、多次元ベクトルによって含まれる特徴は、上述の顔認識アルゴリズムによって決定された。多次元ベクトルは、ＴＥＥにも保存されている第１画像から決定された。追加的又は代替的に、第１画像１１６と第２画像は、例えばピクセル単位で類似性尺度で比較されてよい。第１画像と第２画像が同一である場合、多次元ベクトルが検証される。

【００８７】

多次元ベクトルが検証された場合、検証された多次元ベクトルは、信頼できる実行環境１２４において保存されたユーザの顔の多次元ベクトルと比較される。そうでない場合、手順は中断及び／又は再開され得る。多次元ベクトルと保存されたユーザの顔の多次元ベクトルが同一である場合、ユーザは認証される。ユーザの顔の多次元ベクトルは、ＴＥＥ１２４の少なくとも１つのメモリに保存され得る。上記で概説したように、埋め込みは、例えばスカラー積を使用することによって、互いに比較可能な顔特徴の数学的表現を記述する。

【００８８】

多次元ベクトルが検証された場合、検証された多次元ベクトルは、信頼できる実行環境において保存されたユーザの顔の多次元ベクトルと比較される。そうでない場合、手順は中断及び／又は再開され得る。多次元ベクトルと保存されたユーザの顔の多次元ベクトルが同一の場合、ユーザは認証される。ユーザの顔の多次元ベクトルは、ＴＥＥの少なくとも１つのメモリに保存され得る。上記で概説したように、埋め込みは、例えばスカラー積を使用することによって、互いに比較可能な顔特徴の数学的表現を記述する。

【００８９】

図１にさらに示されるように、認証方法の実施に続いて、認証ステップを実施してよい。信頼できる実行環境１２４は、プロセスステップを認証するための信号を出力することができる（参照番号１３８で示される）。プロセスステップは、支払い、文書への署名、モバイルデバイス１１０へのアクセス、ＢｉｏｍｅｔｒｉｃＰｒｏｍｐｔ及び/又はＦＩＤＯ２　ＡＰＩなどのアプリケーションの有効化（source.android.com/security/biometric/measureを参照）のうち１つ以上を含む。

【００９０】

非セキュアな通常の実行環境１２０で画像分析を実施すると、通常の実行環境１２０の計算能力とメモリ容量をすべて活用することができる。信頼できる実行環境１２４に保存された第１画像１１６と比較することにより、通常の実行環境１２０で得られた画像分析の結果を証明することで、セキュリティを強化したユーザの認証が可能になる。

【符号の説明】

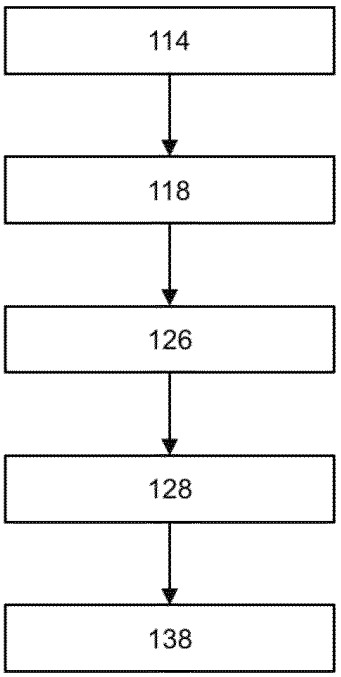
【００９１】

１１０　モバイルデバイス
１１２　カメラ
１１４　画像化

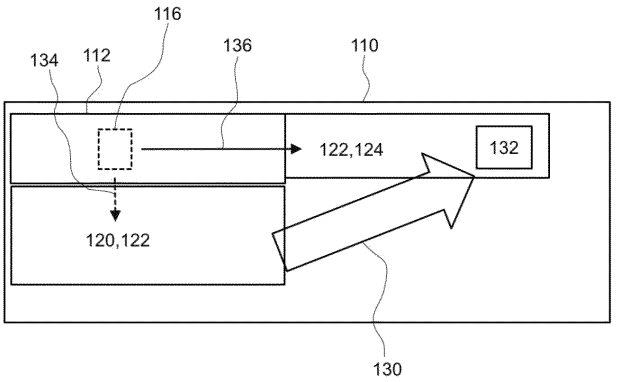
１１６　第１画像
１１８　第１画像の提供
１２０　通常の実行環境
１２２　プロセッサ
１２４　信頼できる実行環境
１２６　第１画像の分析
１２８　ステップd)
１３０　多次元ベクトルの提供
１３２　デコーダ
１３４　通常パス
１３６　セキュアパス
１３８　プロセスステップを認証するための信号の出力

【図面】

【図１】



【図２】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2022/066188

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/32 G06F21/53
ADD.

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)
G06F

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)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2021/173916 A1 (ORTIZ EDISON U [CA] ET AL) 10 June 2021 (2021-06-10) paragraphs [0005], [0037], [0047], [0151], [0182] - [0192], [0195], [0205] - [0219], [0231] - [0233], [0265] paragraphs [0296] - [0297], [0303], [0315], [0329] - [0340], [0353], [0356] - [0361]	1-16
X	US 2019/205518 A1 (MOULIN FRANCOIS [CH] ET AL) 4 July 2019 (2019-07-04) paragraphs [0012], [0014] - [0028], [0031] - [0039]	1-16
X	CN 105 138 973 A (BEIJING TECHSHINO TECHNOLOGY CO LTD) 9 December 2015 (2015-12-09) paragraphs [0007] - [0014]; claims 1-3	1-16

-/--

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* 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
5 September 2022	13/09/2022

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Betz, Sebastian

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2022/066188

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	GUANGCAN MAI ET AL: "On the Reconstruction of Face Images from Deep Face Templates", ARXIV.ORG, CORNELL UNIVERSITY LIBRARY, 201 OLIN LIBRARY CORNELL UNIVERSITY ITHACA, NY 14853, 2 March 2017 (2017-03-02), XP081311815, DOI: 10.1109/TPAMI.2018.2827389 section 1, Introduction; section 2.3 GAN for Face Image Generation; section 3.2 NbNet for Face Image Reconstruction	1-16
A	US 2011/222744 A1 (KIM HONG-IL [KR] ET AL) 15 September 2011 (2011-09-15) paragraphs [0012] - [0014], [0027] - [0029], [0034], [0036] - [0037]	1-16

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2022/066188

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2021173916 A1	10-06-2021	NONE	
US 2019205518 A1	04-07-2019	NONE	
CN 105138973 A	09-12-2015	NONE	
US 2011222744 A1	15-09-2011	KR 20110101675 A	16-09-2011
		US 2011222744 A1	15-09-2011

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

(51)国際特許分類	ＦＩ	テーマコード（参考）
	Ｇ０６Ｔ　7/00　６６０Ａ	

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,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IQ,IR,IS,IT,JM,JO,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,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,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,ZW

弁理士　長山 弘典

(72)発明者　シック，フリードリヒ
ドイツ、６７０６３ ルートヴィッヒスハーフェン アム ライン、インドゥストリーシュトラーセ３５

(72)発明者　シレン，ペーター
ドイツ、６７０６３ ルートヴィッヒスハーフェン アム ライン、インドゥストリーシュトラーセ３５

(72)発明者　グティール，ベンヤミン
ドイツ、６７０６３ ルートヴィッヒスハーフェン アム ライン、インドゥストリーシュトラーセ３５

(72)発明者　シンドラー，パトリク
ドイツ、６７０６３ ルートヴィッヒスハーフェン アム ライン、インドゥストリーシュトラーセ３５

(72)発明者　ブトフ，ディミトリ
ドイツ、６７０６３ ルートヴィッヒスハーフェン アム ライン、インドゥストリーシュトラーセ３５

(72)発明者　プレディガー，マルク
ドイツ、６７０６３ ルートヴィッヒスハーフェン アム ライン、インドゥストリーシュトラーセ３５

Ｆターム（参考）　5B043　AA09 BA04 CA09 CA10 DA05 FA02 FA03 GA01
5L096　AA02 AA06 BA08 BA18 CA14 DA02 HA11 KA04

【要約の続き】

ることによって、前記信頼できる実行環境（１２４）において前記多次元ベクトルから第２画像を決定し、

diii) 前記第１画像（１１６）と前記第２画像を比較し、前記第１画像と前記第２画像が同一の場合、前記多次元ベクトルを実証するステップであって；

div) 前記多次元ベクトルが実証された場合、前記実証された多次元ベクトルは、前記信頼できる実行環境（１２４）に保存されたユーザの顔の多次元ベクトルと比較され、前記多次元ベクトルと前記保存されたユーザの顔の多次元ベクトルが同一の場合、前記ユーザは認証されること、

を含む顔認証ステップと、

を含む。

【選択図】図２