(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2019-522949
(P2019-522949A)
(43)公表日　令和1年8月15日(2019.8.15)

(51)Int.Cl.			F I			テーマコード（参考）
H04N	***5/232***	***(2006.01)***	H04N	5/232		5C122
G06T	***7/00***	***(2017.01)***	G06T	7/00	300F	5L096
			G06T	7/00	660A	

審査請求 未請求　予備審査請求 未請求　（全 24 頁）

(21)出願番号　特願2019-520923 (P2019-520923)
(86)(22)出願日　平成29年7月5日 (2017.7.5)
(85)翻訳文提出日　平成31年3月5日 (2019.3.5)
(86)国際出願番号　PCT/US2017/040753
(87)国際公開番号　WO2018/009568
(87)国際公開日　平成30年1月11日 (2018.1.11)
(31)優先権主張番号　62/358,531
(32)優先日　平成28年7月5日 (2016.7.5)
(33)優先権主張国・地域又は機関
米国 (US)

(71)出願人　519005967
ウー・イーチェン
WU, YECHENG
アメリカ合衆国　マサチューセッツ州０２４２０　レキシントン，アップル・ツリー・レーン，５
(71)出願人　519005978
マーティン・ブライアン・ケー.
MARTIN, BRIAN, K.
アメリカ合衆国　ペンシルベニア州１５３１７　マクムーリー，モリー・ドライブ，２３６
(74)代理人　110000028
特許業務法人明成国際特許事務所

最終頁に続く

(54)【発明の名称】ライブ画像キャプチャ中のなりすまし攻撃検出

(57)【要約】
【解決手段】一般に、本明細書に記載の主題の１つの革新的な態様が、コンピュータにより実施される方法で具現化されうる。方法は、撮像される被写体の存在を撮像デバイスによって検出する工程を備える。方法は、さらに、撮像される被写体の第１特徴を撮像デバイスによって測定する工程と、撮像される被写体の第２特徴を撮像デバイスによって測定する工程と、を備える。方法は、さらに、被写体の第１特徴および被写体の第２特徴の少なくとも一方が閾値を超えることをコンピュータデバイスによって判定する工程と、判定に応じて、撮像される被写体がなりすまし被写体または実際の被写体のいずれであるのかをコンピュータデバイスによって示す工程と、を備える。
【選択図】図３

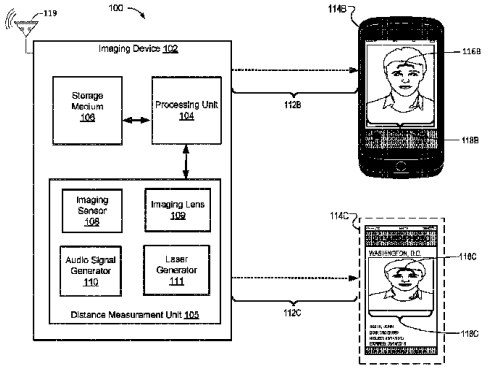

FIG. 3

【特許請求の範囲】
【請求項１】
コンピュータにより実施される方法であって、
撮像される被写体の存在を撮像デバイスによって検出する工程と、
前記撮像デバイスと撮像される前記被写体との間の距離を前記撮像デバイスによって測定する工程と、
コンピュータデバイスによって、前記測定された距離と、前記撮像デバイスの少なくとも１つの特徴とを用いて、撮像される前記被写体の特徴を決定する工程と、
前記被写体の前記特徴が閾値を超えるか否かを前記コンピュータデバイスによって判定する工程と、
撮像される前記被写体がなりすまし被写体および実際の被写体のいずれであるのかを前記コンピュータデバイスによって示す工程と、
を備える、方法。
【請求項２】
請求項１に記載の方法であって、撮像される前記被写体の前記決定された特徴は、前記被写体のサイズである、方法。
【請求項３】
請求項１に記載の方法であって、前記撮像デバイスの前記少なくとも１つの特徴は、
前記撮像デバイスのレンズの焦点距離、
前記撮像デバイスの撮像センサのサイズ、
前記撮像センサの画像ピクセル分解能、および、
ピクセル単位での画像の被写体サイズ、
の内の１つを含む、方法。
【請求項４】
請求項３に記載の方法であって、撮像される前記被写体の前記特徴を決定する工程は、前記撮像デバイスによって検出された画像の幅と、前記撮像センサの幅とを用いる工程を含む、方法。
【請求項５】
請求項４に記載の方法であって、撮像される前記被写体は、人間の顔であり、前記撮像デバイスと前記被写体との間の前記距離は、前記人間の顔の第１瞳孔と前記人間の顔の第２瞳孔との間の距離に基づいて測定される、方法。
【請求項６】
請求項５に記載の方法であって、前記人間の顔の第１瞳孔と前記人間の顔の第２瞳孔との間の前記距離は、前記撮像デバイスによって検出された画像に関連するピクセル単位の距離である、方法。
【請求項７】
コンピュータにより実施される方法であって、
撮像される被写体の存在を撮像デバイスによって検出する工程と、
撮像される前記被写体の第１特徴を前記撮像デバイスによって決定する工程と、
撮像される前記被写体の第２特徴を前記撮像デバイスによって決定する工程と、
前記第１特徴または前記第２特徴を示すパラメータ値が閾値パラメータ値を超えるか否かをコンピュータデバイスによって判定する工程と、
前記パラメータ値が前記閾値パラメータ値を超えるか否かを判定したことに応じて、撮像される前記被写体がなりすまし被写体および実際の被写体のいずれであるのかを前記コンピュータデバイスによって示す工程と、
を備える、方法。
【請求項８】
請求項７に記載の方法であって、前記パラメータ値は、
撮像される前記被写体の画像データに関連するピクセルデータの少なくとも一部の特徴、または、撮像される前記被写体の前記画像データの少なくとも１つの画像領域の色特性

、の内の少なくとも一方を示す、方法。
【請求項９】
請求項８に記載の方法であって、前記パラメータ値が前記閾値パラメータ値を超えるか否かを判定する工程は、
前記ピクセルデータを解析して、１または複数のピクセルが過飽和であるか否かを判定する工程と、
１または複数のピクセルが過飽和であるか否かを判定したことに応じて、過飽和と判定されたピクセルの割合を計算する工程と、
過飽和であると判定されたピクセルの前記割合に基づいて、ピクセル飽和の程度を決定する工程と、
を備える、方法。
【請求項１０】
請求項８に記載の方法であって、過飽和ピクセルの割合が高いほど、撮像される被写体が、なりすまし画像を表示するための電子デバイスである可能性が高いことを示唆する、方法。
【請求項１１】
請求項７に記載の方法であって、撮像される前記被写体の前記第１特徴は、前記被写体のグレア特性、前記被写体の反射特性、もしくは、前記グレア特性および前記反射特性の両方である、方法。
【請求項１２】
請求項８に記載の方法であって、前記被写体は、ディスプレイスクリーンを有する電子デバイスであり、前記電子デバイスは、前記被写体のグレア特性、前記被写体の反射特性、または、前記被写体のフレームに関連する検出可能な属性を備える、方法。
【請求項１３】
請求項７に記載の方法であって、撮像される前記被写体の前記第２特徴は、前記被写体のエッジ特性、前記被写体を描写する画像の背景特性、もしくは、前記被写体の前記エッジ特性および前記被写体を描写する前記画像の前記背景特性の両方である、方法。
【請求項１４】
電子システムであって、
１または複数の処理デバイスと、
動作の実行を引き起こすために前記１または複数の処理デバイスによって実行可能な命令を格納するための１または複数の持続性の機械読み取り可能なストレージデバイスと、
を備え、
前記動作は、
撮像される被写体の存在を撮像デバイスによって検出する動作と、
撮像される前記被写体の第１特徴を前記撮像デバイスによって決定する動作と、
撮像される前記被写体の第２特徴を前記撮像デバイスによって決定する動作と、
前記第１特徴または前記第２特徴を示すパラメータ値が閾値パラメータ値を超えるか否かをコンピュータデバイスによって判定する動作と、
前記パラメータ値が前記閾値パラメータ値を超えるか否かを判定したことに応じて、撮像される前記被写体がなりすまし被写体および実際の被写体のいずれであるのかを前記コンピュータデバイスによって示す動作と、
を含む、電子システム。
【請求項１５】
請求項１４に記載の電子システムであって、前記撮像デバイスは、１または複数の特徴を備え、撮像される前記被写体の第１特徴を決定する動作は、
前記撮像デバイスと、撮像される前記被写体との間の距離を計算する動作と、
前記コンピュータデバイスによって、前記計算された距離と、前記撮像デバイスの少なくとも１つの特徴とに基づいて、撮像される前記被写体の前記第１特徴を決定する動作と、

を含む、電子システム。
【請求項１６】
請求項１５に記載の電子システムであって、撮像される前記被写体の前記第１特徴を決定する動作は、
前記撮像デバイスによって生成された画像の幅を決定する動作と、
前記画像の前記幅および撮像センサの幅に基づいて、撮像される前記被写体の前記第１特徴を決定する動作と、
を含む、電子システム。
【請求項１７】
請求項１６に記載の電子システムであって、撮像される前記被写体は、人間の顔であり、前記撮像デバイスと前記被写体との間の前記距離は、前記人間の顔の第１瞳孔と前記人間の顔の第２瞳孔との間の距離に基づいて測定される、電子システム。
【請求項１８】
請求項１４に記載の電子システムであって、撮像される前記被写体の前記第２特徴を決定する動作は、
画像のデジタル表現に関連する画像ピクセルデータを解析する動作と、
解析する動作に応じて、一部の画像ピクセルの１または複数のパラメータ値を決定する動作と、
パラメータ値に基づいて、撮像される前記被写体の前記第２特徴を決定する動作と、
を含む、電子システム。
【請求項１９】
請求項１４に記載の電子システムであって、撮像される前記被写体の前記第１特徴は、前記被写体のサイズである、電子システム。
【請求項２０】
請求項１４に記載の電子システムであって、撮像される前記被写体の前記第２特徴は、前記被写体のグレア特性、前記被写体の反射特性、もしくは、前記グレア特性および前記反射特性の両方である、電子システム。
【発明の詳細な説明】
【技術分野】
【０００１】
［関連出願の相互参照］
本願は、２０１６年７月５日出願の米国特許出願第６２／３５８，５３１号「ＳＰＯＯＦＩＮＧ　ＡＴＴＡＣＫ　ＤＥＴＥＣＴＩＯＮ　ＤＵＲＩＮＧ　ＬＩＶＥ　ＩＭＡＧＥ　ＣＡＰＴＵＲＥ」の利益を主張し、その出願は、参照によって本明細書に組み込まれる。
【０００２】
本明細書は、一般に、ライブ画像キャプチャ中のなりすまし攻撃の検出に関する。
【背景技術】
【０００３】
個人の本人確認を行うため、制限地域へのアクセス権を提供するため、年齢制限のあるコンテンツの購入を個人に許可するため、もしくは、ネットワーク化されたコンピュータリソースにアクセスする権限を個人に与えるために、物理的なＩＤカード（運転免許証など）が、一般に用いられる。
【発明の概要】
【０００４】
物理的なＩＤカードが、発行プロセス中に発行機関（政府機関または会社など）によってユーザに提供される。発行機関が、ユーザの画像を有するＩＤカードを作成する際、撮像デバイス（カメラまたはスマートフォン／セルラーデバイスなど）による画像の取得またはキャプチャは、１または複数のなりすまし攻撃を受けやすい場合がある。
【０００５】
かかる物理的なＩＤカードは、しばしば、ユーザの身元を識別し、一部の例ではアクセ

ス権または特権をユーザに与えるために用いられるユーザの画像を含む。ライブ画像キャプチャ中に起きるなりすまし攻撃は、特に、かかる画像が、制限地域または機密電子媒体へのユーザアクセス権を提供するＩＤカードまたはデジタルＩＤを作るためにキャプチャされる場合に、物理的セキュリティおよび／またはネットワークセキュリティの文脈で、ユーザ認証を大いに危うくする可能性がある。

【０００６】

一般に、本明細書に記載の主題の１つの革新的な態様が、コンピュータにより実施される方法で具現化されうる。方法は、撮像される被写体の存在を撮像デバイスによって検出する工程を備える。方法は、さらに、撮像デバイスと撮像される被写体との間の距離を撮像デバイスによって測定する工程を備えてよい。さらに、方法は、コンピュータデバイスによって、測定された距離と、撮像デバイスの少なくとも１つの特徴とを用いて、撮像される被写体の特徴を決定する工程を備えてよい。方法は、さらに、被写体の特徴が閾値を超えるか否かをコンピュータデバイスによって判定する工程と、撮像される被写体がなりすまし被写体および実際の被写体のいずれであるのかをコンピュータデバイスによって示す工程と、を備える。

【０００７】

これらおよびその他の実施例は各々、任意選択的に、以下の特徴の内の１または複数を含みうる。例えば、撮像される被写体の決定された特徴は、被写体のサイズであってよい。いくつかの実施例において、撮像デバイスの少なくとも１つの特徴は、撮像デバイスのレンズの焦点距離、撮像デバイスの撮像センサのサイズ、撮像センサの画像ピクセル分解能、および、ピクセル単位での画像上の被写体サイズ、の内の１つを含む。本明細書に記載の主題の一態様において、撮像される被写体の特徴を決定する工程は、撮像デバイスによって検出された画像の幅と、撮像センサの幅とを用いる工程を含む。

【０００８】

別の態様において、撮像される被写体は、人間の顔であり、撮像デバイスと被写体との間の距離は、人間の顔の第１瞳孔と人間の顔の第２瞳孔との間の距離に基づいて測定される。さらに別の態様において、人間の顔の第１瞳孔と人間の顔の第２瞳孔との間の距離は、撮像デバイスによって検出された画像に関連するピクセル単位の距離であってよい。

【０００９】

一般に、本明細書に記載の主題の別の革新的な態様が、コンピュータにより実施される方法で具現化されうる。方法は、撮像される被写体の存在を撮像デバイスによって検出する工程と、撮像される被写体の第１特徴を撮像デバイスによって決定する工程と、撮像される被写体の第２特徴を撮像デバイスによって決定する工程と、を備える。方法は、さらに、第１特徴または第２特徴を示すパラメータ値が閾値パラメータ値を超えるか否かをコンピュータデバイスによって判定する工程を備える。パラメータ値が閾値パラメータ値を超えるか否かを判定したことに応じて、方法は、さらに、撮像される被写体がなりすまし被写体および実際の被写体のいずれであるのかをコンピュータデバイスによって示す工程を備える。

【００１０】

これらおよびその他の実施例は各々、任意選択的に、以下の特徴の内の１または複数を含みうる。例えば、いくつかの実施例において、パラメータ値は、撮像される被写体の画像データに関連するピクセルデータの少なくとも一部の特徴、または、撮像される被写体の画像データの少なくとも１つの画像領域の色特性、の内の少なくとも一方を示す。

【００１１】

いくつかの実施例において、パラメータ値が閾値パラメータ値を超えるか否かを判定する工程は、ピクセルデータを解析して、１または複数のピクセルが過飽和であるか否かを判定する工程と、１または複数のピクセルが過飽和であるか否かを判定したことに応じて、過飽和と判定されたピクセルの割合を計算する工程と、過飽和であると判定されたピクセルの割合に基づいて、ピクセル飽和の程度を決定する工程と、を含む。いくつかの実施例において、過飽和ピクセルの割合が高いほど、撮像される被写体が、なりすまし画像を

表示するための電子デバイスである可能性が高いことを示唆する。いくつかの実施例において、撮像される被写体の第１特徴は、被写体のグレア特性、被写体の反射特性、もしくは、グレア特性および反射特性の両方である。

【００１２】

いくつかの実施例において、被写体は、ディスプレイスクリーンを有する電子デバイスであり、電子デバイスは、被写体のグレア特性、被写体の反射特性、または、被写体のフレームに関連する検出可能な属性を備える。いくつかの実施例において、撮像される被写体の第２特徴は、被写体のエッジ特性、被写体を描写する画像の背景特性、もしくは、被写体のエッジ特性および被写体を描写する画像の背景特性の両方である。

【００１３】

この態様および他の態様の他の実施例は、方法の動作を実行するよう構成された、対応するシステム、装置、および、コンピュータストレージデバイス上にエンコードされたコンピュータプログラムを含む。１または複数のコンピュータのシステムが、動作時にシステムに動作を実行させるシステムにインストールされたソフトウェア、ファームウェア、ハードウェア、または、それらの組み合わせによって、そのように構成されてもよい。１または複数のコンピュータプログラムが、データ処理装置によって実行された時に、その装置に動作を実行させる命令を有することで、そのように構成されてもよい。

【００１４】

添付の図面および以下の説明において、本明細書に記載された主題の１または複数の実施例の詳細について説明する。主題の他の潜在的な特徴、態様、および、利点については、説明、図面、および、特許請求の範囲から明らかになる。

【図面の簡単な説明】

【００１５】

【図１】ライブ画像キャプチャ中のなりすまし攻撃検出のためのシステムの一例を示すブロック図。

【００１６】

【図２】ライブ画像キャプチャ中のなりすまし攻撃検出に用いられる式ならびに１または複数のパラメータを示す図。

【００１７】

【図３】ライブ画像キャプチャ中のなりすまし攻撃検出のためのシステムの一例を示す別のブロック図。

【００１８】

【図４】ライブ画像キャプチャ中のなりすまし攻撃検出のための処理の一例を示すフローチャート。

【００１９】

【図５】ライブ画像キャプチャ中のなりすまし攻撃検出のためのシステムの一例を示す別のブロック図。

【００２０】

【図６】ライブ画像キャプチャ中のなりすまし攻撃検出のための処理の一例を示す別のフローチャート。

【００２１】

様々な図面内の同様の符号は、同様の要素を示す。

【発明を実施するための形態】

【００２２】

一般に、ライブ画像キャプチャ中のなりすまし攻撃の検出のためのシステムおよび方法が開示されている。ネットワークおよび物理的セキュリティの文脈において、なりすましは、例えば、不正ユーザが正規インターネットユーザに似せてインターネットアドレスを偽造するなどして、他者のリソースへアクセスする目的で人を欺こうとすること、と定義されうる。さらに、なりすましは、何らかの不正機能を追加する目的で正常な処理シーケンスの中に挿入されたプログラムによって通信プロトコルをシミュレートする試みも含み

うる。
【００２３】
この文脈内で、記載されている主題は、ライブ画像キャプチャ中のなりすまし攻撃の検出のためのアプローチを含み、ここで、検出は、図１～図４に示すキャプチャされる被写体の距離測定値およびサイズに基づく。本明細書は、さらに、ライブ画像キャプチャ中のなりすまし攻撃の検出のためのアプローチについて記載し、ここで、検出は、図５～図６に示す潜在的ななりすましレンダリングデバイスに関連する画像特性に基づく。
【００２４】
なりすまし攻撃は、一般に、権限のない悪意ある第三者が、コンピュータ環境またはネットワーク環境内の権限を持つ正規ユーザまたはデバイスになりすました時に起きる。なりすまし攻撃は、通例、特定のリソースにアクセスするため、ネットワークホストに攻撃を仕掛けるため、機密データまたはその他のデータを盗むため、マルウェアを拡散するため、または、アクセス制御を迂回するために用いられる。いくつかのシナリオにおいて、なりすましは、攻撃者が、携帯電話、タブレットデバイス、または、ラップトップコンピュータなどのデジタルデバイスを用いて、正規クライアントの静止画像を利用するかまたはビデオを再生する静止画像および／またはビデオ／再生の形態を取りうる。
【００２５】
ライブ画像キャプチャ中のなりすまし攻撃の発生を検出するために、本明細書に記載の技術は、撮像デバイス例のレンズと撮像される被写体（例えば、ユーザ）との間の距離を測定することを含む１または複数のシステムおよび方法を提供する。本明細書に記載のシステムおよび方法は、距離と、撮像デバイス（例えば、カメラ光学系）の少なくとも１つの技術的特徴または技術的特性とを用いて、撮像される被写体のサイズを決定または計算する。測定された距離および決定された被写体のサイズに基づいて、システムおよび方法は、被写体が現実／実際の生身の人間ユーザであるのか、なりすまし攻撃の基礎となる被写体であるのかを判定する。
【００２６】
撮像されている被写体が実際の生身の被写体であるのか、なりすましであるのかを識別して証明することが、信頼される身分証明書の作成および登録の成功に重要なステップである。自動的ななりすまし攻撃検出技術がないために、ほとんどの登録および画像キャプチャ処理が、人間のオペレータを前にして実行される。人間のオペレータの前で実行される画像キャプチャ処理は、オンサイト画像取得システムの動作を管理するために、１または複数の訓練された人材を必要とする。
【００２７】
さらに、画像取得が行われる特定の位置にオペレータが移動する必要もある。これらの要件は、しばしば、資格認定および本人確認プロセスに関連するすべての関係者にとって、時間とコストがかかるものである。さらに、遠隔での資格認定および確認プロセスについては、なりすまし画像またはビデオが実際の人間のユーザの代わりに用いられた場合に、なりすまし攻撃の検出がなければ、潜在的に、権限のない対象者が安全なシステムへのアクセスを認められることになりうる。
【００２８】
図１は、ライブ画像キャプチャ中のなりすまし攻撃検出のためのシステムの一例１００を示すブロック図である。システム１００は、一般に、撮像デバイス１０２を備える。別の実施形態において、撮像デバイス１０２に加えて、システム１００は、さらに、人間のユーザの一例（ユーザ１１４Ａなど）を含んでもよい。いくつかの実施例において、撮像デバイス１０２は、カメラ、ラップトップコンピュータ、デスクトップコンピュータ、セル方式スマートフォンデバイス（例えば、ｉＰｈｏｎｅ（登録商標。以下同じ）、Ｓａｍｓｕｎｇ（登録商標。以下同じ）　Ｇａｌａｘｙ（登録商標。以下同じ）、または、Ａｎｄｒｏｉｄ（登録商標。以下同じ）デバイス）、もしくは、ユーザの画像をキャプチャできる任意のその他の電子デバイスであってよい。
【００２９】

撮像デバイス１０２は、一般に、処理ユニット１０４、ストレージ媒体１０６、および、距離測定ユニット１０５を備える。別の実施形態において、システム１００は、後述する決定および計算の内の１または複数を実行するためのさらなる処理オプションを提供する他の計算リソース／デバイス（例えば、クラウドベースのサーバ）を備えてもよい。

【００３０】

処理ユニット１０４は、ストレージ媒体１０６に格納された命令または別のストレージデバイスに格納された他の命令など、撮像デバイス１０２内で実行するための命令を有するコンピュータプログラムを処理するよう構成される。処理ユニット１０４は、１または複数のプロセッサを備えてよい。ストレージ媒体１０６は、撮像デバイス１０２内に情報を格納する。いくつかの実施例において、ストレージ媒体１０６は、１または複数の揮発性メモリユニットである。いくつかの別の実施例において、ストレージ媒体１０６は、１または複数の不揮発性メモリユニットである。

【００３１】

ストレージ媒体１０６は、フロッピーディスクデバイス、ハードディスクデバイス、光学ディスクデバイス、テープデバイス、フラッシュメモリまたはその他の同様のソリッドステートメモリデバイス、もしくは、ストレージエリアネットワークまたはその他の構成の中のデバイスを含むデバイスのアレイなど、別の形態のコンピュータ読み取り可能な媒体であってもよい。上述のコンピュータプログラムおよび命令は、処理ユニット１０４によって実行されると、以下に詳述するように、処理ユニット１０４に１または複数のタスクを実行させる。

【００３２】

距離測定ユニット（ＤＭＵ）１０５は、一般に、撮像センサ１０８、撮像レンズ１０９、オーディオ信号発生器１１０、および、レーザ発生器１１１を備える。ＤＭＵ１０５は、処理ユニット１０４およびストレージ媒体１０６と協働して、撮像デバイス１０２が人間のユーザ１１４Ａの画像をキャプチャまたは取得する準備をする時に、なりすまし攻撃検出に関連する複数の動作およびタスクを実行する。本明細書で用いられているように、「ユーザ」とは、人間の個人を指しうる。例えば、ユーザは、管轄区域または地方自治体の自動車部門によって発行された運転免許証などの物理的なＩＤカードを求める個人であってよい。他の例において、ＩＤカードは、パスポートなど他のタイプのＩＤ、または、カードに添付されたユーザ１１４Ａの識別画像を有するその他の政府または企業発行のＩＤカードであってもよい。

【００３３】

いくつかの実施例において、ユーザ１１４Ａは、例えば、権限のある代理人が本人確認プログラムに記録を処理するために電子写真／画像を受信してそれに依存するオンライン登録プロセスまたは遠隔フォーム提出プロセスなど、様々な方法を用いるデジタルＩＤプログラムに登録することを望みうる。次いで、デジタルＩＤ管理者が、ＩＤデータベース内にユーザ情報を含むユーザエントリを作成してよい。例えば、ユーザ情報は、電子メールアドレス、ＩＤ番号、ユーザ１１４Ａの電子写真／画像、および、ユーザ１１４Ａに関連するその他のタイプのデモグラフィック情報（例えば、自宅住所）を含みうる。

【００３４】

機密情報にアクセスしようとする悪意あるまたは敵意ある個人または実体は、ユーザ１１４Ａのなりすまし電子写真またはデジタル画像を用いて、デジタルＩＤプログラムを介して不正または詐欺的な登録を行おうとしうる。さらに、悪意ある／敵意あるユーザは、施設へのアクセスを許可する際にユーザ１１４Ａのバイオメトリック情報（顔または虹彩の特徴など）に部分的に依存する物理的セキュリティ手段を回避するために、ユーザ１１４Ａのなりすまし画像を利用しようとしうる。したがって、本明細書は、不正または詐欺的な本人確認に用いられるなりすまし画像を高い信頼性で検出することにより、オンラインまたはリモートでのアイデンティティ登録プロセスの完全性を強化するシステムおよび方法を提供する。

【００３５】

図１を再び参照すると、撮像デバイス１０２は、一般に、ユーザ１１４Ａなどの被写体の画像をキャプチャするよう構成される。図１の実施形態において、ユーザ１１４Ａは、人間の男性または人間の女性に対応する顔および虹彩の特徴を有する生身の人間ユーザである。撮像デバイス１０２は、一般に、撮像される被写体の存在を検知または検出するよう構成される。いくつかの実施例において、撮像デバイス１０２は、デバイスに隣接する被写体の存在を検出するために、従来の被写体検知および検出技術（パッシブまたはアクティブ赤外線センサ、もしくは、周知のモーション検出方法など）を組み込んでよい。様々なその他の関連する被写体検知技術が、撮像される被写体の存在を検出するために用いられてもよい。

【００３６】

ＤＭＵ１０５は、一般に、撮像レンズ１０９（すなわち、実際の撮像デバイス内で用いられる代表的な光学手段）と、撮像される被写体との間の距離を測定するよう構成される。様々な実施例において、撮像される被写体は、生身の男性の人間ユーザ１１４Ａまたは生身の女性の人間ユーザ１１４Ａであってよい。図１の実施形態において、距離１１２Ａは、撮像レンズ１０９とユーザ１１４Ａとの間の測定された距離を示す。撮像デバイス１０２は、測定された距離１１２Ａと、撮像デバイス１０２の少なくとも１つの技術的特徴とを用いて、撮像される被写体の実際のサイズを決定または計算する。いくつかの実施例において、撮像デバイス１０２の少なくとも１つの技術的特徴は、１）撮像レンズ１０９の焦点距離、撮像センサ１０８のサイズ、撮像センサ１０８の画像ピクセル分解能、および、ピクセルでの画像の被写体サイズの内の１つを含む（図２参照）。

【００３７】

撮像される被写体の実際のサイズの決定により、撮像デバイス１０２は、被写体が実際の生身の人間のユーザであるのか、なりすまし攻撃の被写体（例えば、静止画像またはビデオ再生）であるのかを判定できるようになる。撮像デバイス１０２は、撮像される被写体が生身の人間ユーザであるのか、なりすまし攻撃の被写体であるのかに関する判定を、権限のあるシステム管理者に、配信する、信号で知らせる、または、他の方法で通知する信号インジケータ機能（インジケータ１１９）を備えてもよい。１または複数の別の実施形態において、撮像される被写体の実際のサイズは、コンピュータデバイス（クラウドベースのサーバデバイスなど）内で行われる計算に基づいて決定されてよい。様々な実施例において、そのコンピュータデバイスは、処理ユニット１０４およびストレージ媒体１０６によって提供される能力と実質的に同様の処理能力およびストレージ能力を備えうる。

【００３８】

様々な方法が、距離測定のためにＤＭＵ１０５内に配備されて利用されうる。様々な方法は、可聴および不可聴信号の利用、レーザ測距デバイスを備えるためのレーザ信号の利用、画像フレームに関連する測距点の利用、ステレオ撮像と同様の方法で撮像デバイス１０２によって取得された複数の画像の利用、および、撮像デバイス１０２によってサポートされた様々なその他の周知の距離測定方法を含む。一実施例において、可聴または不可聴信号伝達は、一般に、可聴信号または不可聴信号の一方を伝達し、エコー時間を測定し、測定されたエコー値を用いて撮像デバイス１０２までの被写体距離を概算することを含む。

【００３９】

図２は、ライブ画像キャプチャ中のなりすまし攻撃検出に用いられる式ならびに１または複数のパラメータを示す。図２に示すように、ストレージ媒体１０６は、一般に、距離の式１２０、瞳孔距離パラメータ１２２、および、撮像デバイスの特徴１２４を備えてよい。様々な実施例において、式１２０、パラメータ１２２、および、特徴１２４は各々、処理ユニット１０４によってアクセス可能なコンピュータプログラムまたは機械読み取り可能な命令の形態でストレージ媒体１０６内に格納される。

【００４０】

別の実施例において、式１２０、パラメータ１２２、および、特徴１２４は各々、コンピュータデバイス（クラウドベースのサーバデバイスなど）のストレージ媒体内に格納さ

れる。このストレージ媒体において、式１２０、パラメータ１２２、および、特徴１２４は、同様に、コンピュータデバイスの処理ユニットによってアクセス可能なコンピュータプログラムまたは機械読み取り可能な命令の形態で格納される。

【００４１】

上記で簡単に述べたように、様々な方法が、被写体距離測定のために撮像デバイス１０２によって用いられうる。いくつかの実施例において、処理ユニット１０４は、式１２０を用いて、撮像される被写体と撮像デバイス１０２との間の距離を測定する。式１２０は、ＯＤ＝（ＬＦＬ＊ＡＰＤ＊ＩＷ）／（ＩＰＤ＊ＳＷ）と表される。式１２０において、ＬＦＬはレンズ焦点距離、ＡＰＤは実際の瞳孔距離１１６Ａ（図１）、ＩＷは画像幅１１８Ａ（図１）、ＩＰＤは画像瞳孔距離、ＩＳＷは撮像センサ幅（図１のセンサ１０８）である。

【００４２】

上述のように、測定された距離１１２Ａおよび少なくとも１つのデバイス特徴１２４が、撮像される被写体のサイズを決定または計算するために用いられる。いくつかの実施例において、デバイス特徴１２４の各々は、撮像される被写体のサイズを決定または計算するために、測定された距離１１２Ａと共に用いられてよい。特に、測定された距離１１２Ａと共に、被写体のサイズは、撮像デバイスの焦点距離、撮像センサのサイズおよび画像ピクセル分解能、画像上での被写体のサイズ（ピクセル単位）、ならびに、測定された距離を用いて計算されてよい。

【００４３】

様々な実施例において、処理ユニット１０４（または非ローカルコンピュータデバイスの関連処理ユニット）は、計算された被写体サイズを、様々な生身の女性および男性の人間の顔の実例についての１または複数の既知のサイズ範囲と比較するよう構成されてよい。比較により、所定の閾値を上回る（または下回る）サイズの差があった場合、なりすまし攻撃の可能性が、撮像デバイス１０２またはコンピュータデバイスによって検出および示唆される。例えば、写真画像またはビデオが携帯電話のスクリーン上に表示され、撮像デバイス１０２が写真画像またはビデオをキャプチャする準備をしている場合、撮像デバイス１０２を介して表示された顔のサイズは、実際の生身の人間の顔よりもかなり小さい。逆に、比較により、差が所定の範囲内に収まる（すなわち、閾値を上回ることも下回ることもない）場合には、被写体サイズは合理的であると判定され、したがって、生きた人間のユーザであると推定される。

【００４４】

図３は、ライブ画像キャプチャ中のなりすまし攻撃検出のためのシステムの一例を示す別のブロック図である。図３の実施例は、潜在的ななりすまし攻撃が試みられうる別の実施形態を示す。図３の実施形態において、測定される被写体は、被写体１１４Ｂまたは被写体１１４Ｃなどのなりすまし被写体である。上述のように、なりすまし攻撃は、ＩＤカード、もしくは、攻撃者が、携帯電話、タブレットデバイス、または、ラップトップコンピュータなどのデジタルデバイスを用いて、正規クライアントのデジタル静止画像を利用するかまたはビデオを再生する静止画像（被写体１１４Ｃ）および／またはビデオ／再生（被写体１１４Ｂ）の形態を取りうる。

【００４５】

図に示すように、なりすまし攻撃シナリオの一例において、瞳孔距離１１６Ｂおよび１１６Ｃは、生身の人間のユーザの瞳孔距離（図１の距離１１６Ａなど）よりも実質的に短い可能性がある。同様に、画像幅１１８Ｂおよび１１８Ｃは、生身の人間のユーザに関連する幅（図１の画像幅１１８Ａなど）よりも狭い可能性がある。さらに、測定された距離１１２Ｂおよび１１２Ｃも、生身の人間のユーザについて測定された距離１１２Ａと異なりうる。

【００４６】

したがって、処理ユニット１０４（または非ローカルコンピュータデバイスの関連処理ユニット）が、被写体１１４Ｂ／Ｃの計算された被写体サイズを、様々な生身の女性／男

性の人間の顔の１または複数の既知のサイズ範囲と比較すると、比較により、所定の閾値を上回る（または下回る）サイズの差が生じることになる。したがって、なりすまし攻撃が検出される。

【００４７】

さらに、撮像デバイス１０２（または非ローカルコンピュータデバイスの関連処理ユニット）は、撮像される被写体が生身の人間のユーザであるか、なりすまし攻撃被写体であるかの判定を、権限のある管理者に、信号で知らせる、配信する、または、他の方法で通知するために、インジケータ（信号インジケータ１１９など）を作動させてよい。

【００４８】

図４は、ライブ画像キャプチャ中のなりすまし攻撃検出のための処理の一例を示すフローチャートである。処理２００は、ブロック２０２で始まり、各画像フレームについて、撮像デバイス１０２は、撮像される被写体の存在を検出し、これは、生身の人間のユーザ１１４Ａの顔が画像フレーム内にあるか否かを検出することを含む。ブロック２０４で、処理２００は、撮像デバイス１０２が、撮像レンズ１０９と撮像される被写体との間の距離を測定する工程を備える。いくつかの実施例において、測定される被写体は、生身の人間のユーザ１１４Ａである。潜在的ななりすまし攻撃が試みられる別の実施形態において、測定される被写体は、被写体１１４Ｂまたは被写体１１４Ｃなどのなりすまし被写体である。

【００４９】

ブロック２０６で、処理２００は、撮像デバイス１０２（または別のコンピュータデバイス）が、測定された距離と、１または複数のデバイス特徴１２４とを用いて、撮像される被写体の特徴を決定する工程を備える。一実施例において、特徴は、撮像される被写体のサイズである。処理２００は、さらに、特徴すなわち被写体サイズが所定の閾値サイズを超えるか否かを、撮像デバイス１０２または別のコンピュータデバイスのいずれかが判定する工程（ブロック２０８）を備える。

【００５０】

上述のように、一実施例において、処理ユニット１０４または別のデバイスのプロセッサは、計算された被写体サイズを、様々な生身の女性および男性の人間の顔の実例についての１または複数の既知のサイズ範囲と比較してよい。比較により、所定の閾値を上回る（または下回る）サイズの差があった場合、なりすまし攻撃の可能性が検出されうる。ブロック２１０で、処理２００は、撮像される被写体が生身の人間のユーザであるのか、なりすまし攻撃の被写体であるのかの判定を、権限のあるシステム管理者に、（信号インジケータ１１９を介して）示す、伝達する、または、他の方法で通知する工程を備える。

【００５１】

上述のように、図１～図４では、キャプチャされる被写体の距離測定値およびサイズに基づいて、ライブ画像キャプチャ中になりすまし攻撃を検出するためのアプローチを示した。残りの図５～図６は、潜在的ななりすましレンダリングデバイスに関する画像特性に基づいて、ライブ画像キャプチャ中になりすまし攻撃を検出するためのアプローチを示す。

【００５２】

ライブ画像キャプチャ中のなりすまし攻撃の発生を検出するために、以下に記載する技術は、被写体（例えば、人間のユーザまたは物理的デバイス）の画像に関連する１または複数の画像特性を検知または測定するためのシステムおよび方法を含む。いくつかの実施例において、測定される画像特性は、潜在的ななりすましレンダリングデバイスに関連しうる。

【００５３】

測定できる画像特性の例は、画像のグレア、画像の反射、画像背景のバリエーション、画像の形状、および、画像内の被写体が潜在的ななりすましデバイスであることを示唆しうる画像のその他の特徴を含みうる。上述の画像特性の少なくとも１つの測定された検出に基づき、記載されているシステムおよび方法を利用して、撮像される被写体が現実／実

際の生身の人間のユーザであるのか、なりすまし攻撃の基礎となる電子デバイスであるのかを判定することができる。

【００５４】

この文脈において、図５は、ライブ画像キャプチャ中のなりすまし攻撃検出のためのシステムの別の例３００を示すブロック図である。図５の実施例は、図１および図３の実施例にも図示されている対応する符号を有する１または複数の特徴を含みうる。より具体的には、後述する機能に加えて、いくつかの実施例において、システム３００は、図１～図４の実施例を参照して上述したすべての機能も実行するよう構成されうる。したがって、システム１００について上述したいくつかの特徴の記載は、システム３００にも図示されている等価の特徴のために参照できる。

【００５５】

システム３００は、一般に、被写体３０８（例えば、電子デバイス）または人間のユーザ３１０などの被写体例の画像をキャプチャするよう構成された撮像デバイス３０２を備える。いくつかの実施例において、撮像デバイス３０２は、カメラ、ラップトップコンピュータ、デスクトップコンピュータ、セル方式スマートフォンデバイス（例えば、ｉＰｈｏｎｅ、Ｓａｍｓｕｎｇ　Ｇａｌａｘｙ、または、Ａｎｄｒｏｉｄデバイス）、もしくは、電子デバイス３０８の画像または人間のユーザの一例３１０の画像をキャプチャできる任意のその他の電子デバイスであってよい。

【００５６】

撮像デバイス３０２は、一般に、処理ユニット１０４、ストレージ媒体１０６、および、画像特性測定ユニット３０５を備える。別の実施形態において、システム３００は、後述する決定および計算の内の１または複数を実行するためのさらなる処理オプションを提供する他の計算リソース／デバイス（例えば、クラウドベースのサーバ）を備えてもよい。

【００５７】

画像特性測定ユニット（ＩＭＵ）３０５は、一般に、撮像センサ１０８、撮像レンズ１０９、グレア／反射（ＧＲ）検知ロジック３０４、および、エッジ検出／背景（ＥＤＢ）検知ロジック３０６を備える。一般に、ＩＭＵ３０５は、処理ユニット１０４およびストレージ媒体１０６と協働して、なりすまし攻撃の検出に関する複数の演算動作およびタスクを実行する。いくつかの実施例において、演算動作は、撮像デバイス３０２を用いて、潜在的ななりすましデバイス３０８または人間のユーザ３１０などの被写体の画像をキャプチャまたは取得する時に実行される。

【００５８】

ＩＭＵ３０５の１または複数の機能は、キャプチャ／撮像される被写体の１または複数の画像特性を測定または検出するよう構成された演算ロジックまたはソフトウェア命令に対応しうる。いくつかの実施例では、検知ロジック３０４および３０６のためにプログラムされたコードまたはソフトウェア命令が、デバイス３０２に１または複数の機能を実行させるために処理ユニット１０４によって実行されうる。例えば、検知ロジック３０４、３０６のためにプログラムされたコードの実行に応じて、処理ユニット１０４は、デバイス３０２の１または複数のハードウェア検知機能に、画像例の画像特性を検出させることができる。

【００５９】

上述のように、撮像される被写体は、生身の人間のユーザ３１０または潜在的ななりすまし被写体３０８でありうる。図５の実施例において、撮像デバイス３０２は、画像例の検出されたグレア特性、反射特性、もしくは、エッジおよび背景特性を用いて、撮像される被写体がなりすましデバイスであるか否かを判定するよう構成される。いくつかの実施例において、撮像デバイス３０２は、画像内に描かれた被写体の特性に対応する画像の特性を検出または決定するよう構成された１または複数のセンサまたは検知機能を備えてよい。

【００６０】

例えば、デバイス３０２の検知機能は、被写体３０８のグレア特性３１２、被写体３０８の反射特性３１４、被写体３０８のエッジ特性３１６、および／または、被写体３０８の背景特性３１８を検出するよう構成されてよい。いくつかの実施例において、図５では電子デバイスとして図示されているが、被写体３０８は、人間の個人の画像を表示できる様々な被写体でありうる。例えば、被写体３０８は、図３に示した被写体１１４Ｃなど、ＩＤカードまたは静止画像でありうる。

【００６１】

撮像されるアイテムの特性は、アイテムの描写または表現を含むデジタル画像またはライブデジタルレンダリングの解析に基づいて検出されうる。撮像されるアイテムの１または複数の画像特性の検出は、アイテムが実際の生身の人間のユーザ３１０であるか、実際または潜在的ななりすまし攻撃の被写体／デバイス３０８であるのかを、撮像デバイス３０２が判定することを可能にする。

【００６２】

撮像デバイス３０２は、撮像される被写体が生身の人間ユーザであるのか、なりすまし攻撃の被写体であるのかに関する判定を、権限のあるシステムに、配信する、信号で知らせる、または、他の方法で通知する信号インジケータ機能（インジケータ１１９）を備えてもよい。いくつかの実施例において、被写体の特性を決定するデジタル画像または被写体レンダリングの解析は、クラウドベースのサーバデバイスなどのコンピュータデバイスを用いて実行される。いくつかのクラウドベースのサーバデバイスが、処理ユニット１０４およびストレージ媒体１０６の能力と実質的に同様の処理能力およびストレージ能力を備えてもよい。

【００６３】

検知ロジック３０４は、デジタル画像例に関連しうるグレア特性および反射画像特性を検出させるために処理ユニット１０４によって実行される。デジタル画像例は、コンピュータデバイス（例えば、スマートフォンデバイス、ラップトップ、または、コンピュータデバイスのディスプレイ）である被写体３０８、もしくは、ＩＤカード／文書または個人の画像を含むその他の物理的アイテムを含みうる。

【００６４】

グレア特性３１２は、被写体３０８のディスプレイに関連する検出されたグレアに対応しうる。いくつかの実施例において、被写体３０８は、コンピュータデバイス例、または、電子デバイスのディスプレイ／ディスプレイスクリーンである。あるいは、グレア特性３１２は、被写体３０８に対応しうるＩＤカードまたは画像文書の画像に関連する検出されたグレアに対応しうる。例えば、被写体３０８のディスプレイスクリーンまたは基材は、光波が被写体３０８の外面と相互作用することに応じて、光の散乱またはフレアの出現を引き起こしうる検出可能な物理的属性（例えば、ガラス／プラスチックの特徴またはその他のグレアを誘発する特徴）を備えうる。

【００６５】

撮像デバイス３０２は、グレア特性３１２および反射特性３１４を検出するために１または複数のソフトウェア命令を実行する。例えば、デバイス３０２は、検知ロジック３０４を用いて、１または複数の過飽和ピクセルを検出できる。いくつかの実施例において、過飽和ピクセルは、被写体３０８のデジタルレンダリングに関連する画像データに対応しうるか、または、そのデータに対して検出されうるが、人間のユーザ３１０のデジタルレンダリングに関連する画像では検出されない。

【００６６】

１または複数の過飽和ピクセルの検出は、過剰または過度に明るい領域を示すアイテム／被写体の外面部分に対応しうる。特に、１または複数の過飽和ピクセルの検出は、ライブ画像キャプチャセッション中に潜在的ななりすまし攻撃が試みられていることを示唆しうる。例えば、過飽和ピクセルの検出は、電子ディスプレイを覆う外側のガラスレンズに対する光のグレア／反射を表す明度の過剰な領域を示唆しうる。

【００６７】

明度の過剰なこれらの表面領域は、アイテム（例えば、なりすましデバイスの電子ディスプレイを覆う外側のレンズ）の外面と相互作用する環境反射もしくはその他の自然または人工的な光波に基づいて発生しうる。いくつかの実施例において、自然または人工的な光波は、アイテムに反射することによって、アイテムの外面と相互作用する。撮像レンズ１０９を介してデバイス３０２によって、かかる反射を受信することができ、反射に関するピクセルデータを処理および解析することで、アイテムの１または複数の特性を決定できる。

【００６８】

例えば、デバイス３０２は、処理ユニット１０４を用いて、画像およびピクセルデータの解析機能を実行するための検知ロジック３０４を実行することができる。デジタル画像のピクセルデータの解析に応じて、デバイス３０２は、被写体３０８の少なくとも１つのグレア特性３１２または被写体３０８の少なくとも１つの反射特性３１４を検出しうる。例えば、デバイス３０２は、一部のピクセルが過飽和を示唆するか否かを判定することによって、被写体３０８のグレア特性３１２を検出でき、ここで、それらのピクセルは、被写体３０８のデジタル画像を構築するために用いられるものである。

【００６９】

いくつかの実施例において、過飽和は、閾値パラメータ値を超えるピクセル（またはピクセルのセット）のパラメータ値に基づいて決定される。ピクセルのパラメータ値は、デバイス３０８の表面エリアまたは領域の測定された明度に対応しうる。したがって、デバイス３０２は、パラメータ値を用いて、どのピクセルが過飽和であるかを検出または判定し、次いで、過飽和ピクセルに基づいてグレア特性３１２または反射特性３１４を決定できる。

【００７０】

いくつかの実施例において、デバイス３０２は、過飽和であると判定されたピクセルの計算された割合に基づいて、ピクセル飽和の程度を計算または決定する。したがって、デバイス３０２は、なりすまし攻撃検出に面積ベースのピクセル飽和測定値を用いることができ、ここで、過飽和ピクセルの割合が高いと、画像フレームにおいて検出された画像がなりすまし画像である可能性が高いことが示唆される。

【００７１】

いくつかの実施例において、パラメータ値は、デバイス３０８の特定の表面エリアまたは領域の測定された明度を表すために、０．１（低明度）から１．０（高明度）の範囲を取りうる。例えば、第１閾値（例えば、０．６５の明度測定値）を超えるパラメータ値を含むピクセルデータは、被写体３０８のグレア特性３１２が検出されたことを示唆しうる。同様に、第２閾値（例えば、０．８５の明度測定値）を超えるパラメータ値を含むピクセルデータは、被写体３０８の反射特性３１４が検出されたことを示唆しうる。

【００７２】

一般に、ディスプレイデバイスの外面またはレンズで検出されうるグレア特性３１２および反射特性３１４は、生身の人間の顔に関連しうる任意の最小限のグレアおよび反射特性とは異なる。したがって、検出されたグレア特性３１２および反射特性３１４は、例えば、生身の人間ユーザの画像になりすますために電子デバイスが用いられているか否かを高い信頼性で検出するために利用できる。

【００７３】

例えば、撮像される被写体に関連するグレアおよび反射の特徴（例えば、人物の顔または電子デバイスのいずれかの上／周囲での特徴）は、特定のパターンを示しうる。いくつかの実施例において、人間のユーザ３１０のグレアおよび反射の特徴に関するパターンは、撮像されるアイテム／被写体が、なりすましの被写体である可能性があるか、生身の人間である可能性があるかを判定するために、信頼性の高い指標を提供しうる。

【００７４】

光のグレア特徴は、特定のホットスポットパターンも示す場合があり、ここで、ホットスポットは、デバイス３０２の撮像レンズ１０９によって検出可能な特定の赤外（ＩＲ）

光波によって引き起こされうる。いくつかの実施例において、グレアまたはホットスポットのパターンが、電子デバイス（例えば、携帯電話、ラップトップ、または、タブレットコンピュータデバイス）の特定の外部ディスプレイ表面に関連することが知られているグレアまたはホットスポットのパターンと一致しうる。これらの周知の特性は、ストレージ媒体１０６のメモリに格納されてよい。

【００７５】

いくつかの実施例において、処理ユニット３０４は、ストレージ媒体１０６にアクセスして、被写体３０８（または人間のユーザ３１０）について検出されたグレア、反射、または、ホットスポットデータを、既知のグレア、反射、または、ホットスポットデータと比較する。比較に基づいて、デバイス３０２は、撮像されるアイテム／被写体または人物が、生身の人間のユーザであるのか、なりすましデバイス（例えば、タブレットまたはスマートフォン）に表示されている人間のユーザの画像であるのかを判定できる。

【００７６】

検知ロジック３０６は、デジタル画像例に関連しうるエッジおよび背景画像特性を検出させるために処理ユニット１０４によって実行される。上述のように、デジタル画像例は、コンピュータデバイス、ＩＤカード／文書、または、人間のユーザの画像を含む別の物理的アイテムである被写体３０８を含みうる。

【００７７】

エッジ特性３１６は、被写体３０８に対応するコンピュータデバイスのディスプレイまたは筐体に関連する検出されたフレームまたは輪郭に対応しうる。あるいは、エッジ特性３１６は、被写体３０８または被写体１１４Ｃに対応しうるＩＤカードまたは画像文書に関連する検出されたフレームまたは輪郭に対応しうる。例えば、ＩＤカード、ディスプレイスクリーン、電子デバイス筐体、または、被写体３０８の保護ケースは、被写体３０８の外側部分によって規定された物理的なエッジまたは輪郭を含みうる。

【００７８】

エッジ特性３１６は、被写体３０８がコンピュータデバイス例である場合、被写体３０８のディスプレイ、筐体、または、外側に関連する検出されたフレームまたは境界でありうる。あるいは、エッジ特性３１６は、被写体３０８に対応しうるＩＤカードまたは画像文書の画像に関連する検出されたフレームまたは境界でありうる。

【００７９】

撮像デバイス３０２は、エッジ特性３１６および背景特性３０８を検出するために１または複数のソフトウェア命令を実行する。例えば、デバイス３０２は、検知ロジック３０６を用いて、画像内の被写体の１または複数のエッジまたは境界を検出すると共に、画像内の被写体に対する１または複数の背景属性を検出することができる。いくつかの実施例において、エッジまたは境界は、被写体３０８のデジタルレンダリングに関連する画像データに対応しうるか、または、そのデータに対して検出されうるが、人間のユーザ３１０のデジタルレンダリングに関連する画像では検出されない。

【００８０】

境界の検出は、生身の人間のユーザではなく物理的デバイスまたはＩＤ文書であるアイテム／被写体の外面部分によって規定される被写体のフレームに対応しうる。特に、被写体の境界またはフレームの検出は、ライブ画像キャプチャ中に潜在的なりすまし攻撃が試みられていることを示唆しうる。

【００８１】

例えば、デバイス３０２は、処理ユニット１０４を用いて、画像およびピクセルデータの解析機能を実行するための検知ロジック３０６を実行することができる。デジタル画像のピクセルデータの解析に応じて、デバイス３０２は、被写体３０８の少なくとも１つのエッジ特性３１６または被写体３０８の少なくとも１つの背景特性３１８を検出しうる。例えば、デバイス３０２は、一部のピクセルが或る程度の明度の不連続性を示すか否かを判定することによって、被写体３０８のエッジ特性３１６を検出できる。いくつかの実施例において、デバイス３０２は、一部のピクセルが或る程度の明度の不連続性を示すか否

かを判定することによって、被写体３０８のエッジ特性３１６および背景特性３１８を検出し、ここで、不連続性は、画像の検出された色特性に関連するコントラストによって引き起こされうる。

【００８２】

いくつかの実施例において、画像の明度の不連続性および検出された色特性の間のコントラストは、特定の画像データのパラメータ値が閾値パラメータ値を超えることに基づいて決定される。例えば、明度の不連続性は、画像ピクセルデータのピクセルパラメータ値の解析に基づいて決定されてよく、色特性の間のコントラストは、デバイス３０２のＲＧＢ色モデル例によって生成される色パラメータ値の解析に基づいて決定されてよい。

【００８３】

例えば、画像の明度の不連続性に関しては、画像の所与の領域のピクセルパラメータ値を含む画像データを解析して、明度値を決定することができる。デバイス３０２は、明度値を解析して、値のセットの間の差異すなわちデルタが、アイテムすなわち被写体３０８の検出されたエッジまたは境界に対応する明度の不連続性を示唆するか否かを判定することができる。いくつかの実施例において、明度の不連続性は、検出された明度のパラメータ値のセットの間のデルタが閾値デルタを超えた場合に、検出されたエッジまたは境界に対応する。

【００８４】

同様に、画像の色特性の間のコントラストに関しては、画像の所与の領域の色パラメータ値を解析して、色値を決定することができる。デバイス３０２は、色値を解析して、値のセットの間の差異すなわちコントラストが特定の色コントラストを示唆するか否かを判定するができる。特定の色コントラストが、画像の検出された背景に対応しうる。いくつかの実施例において、画像の色特性の間のコントラストは、画像のそれぞれの領域の色値のセットの間のデルタが閾値デルタを超えた場合に、検出された背景に対応する。

【００８５】

例えば、画像の所与の領域の色パラメータ値は、色の差異／コントラストが第１画像領域３２０と第２画像領域３２２との間に存在することを示唆しうる。したがって、デバイス３０２は、第１画像領域３２０と第２画像領域３２２との間に色の差異／コントラストが存在すると決定できる。次いで、デバイス３０２は、決定された色コントラストに基づいて、背景特性３１８を検出できる。例えば、デバイス３０２は、第１画像領域３２０の色値（例えば、０．３１）と、第２画像領域３２２の色値（例えば、０．８３）との間の特定の計算された差／デルタが、閾値デルタ（例えば、０．４）を超えることに基づいて、背景特性３１８を決定することができる。いくつかの実施例において、色値は、デバイス３０２のＲＧＢモデル例によって生成される画像色特性を示すパラメータ値として記述されうる。

【００８６】

一般に、なりすましデバイスまたは関連するなりすまし被写体を含む画像について、エッジ特性３１６および背景特性３１８は、生身の人間の顔の画像に関連しうる任意のささいなフレームまたは境界ならびに任意の色の差異または背景特性とは異なる。したがって、検出されたエッジ特性３１６および背景特性３１８は、例えば、生身の人間ユーザの画像になりすますために電子デバイスが用いられているか否かを高い信頼性で検出するために利用できる。

【００８７】

図６は、ライブ画像キャプチャ中のなりすまし攻撃検出のための処理の一例２２０を示す別のフローチャートである。処理２２０のブロック２２２で、各画像フレームについて、撮像デバイス３０２は、撮像される被写体の存在を検出し、これは、生身の人間のユーザ３１０の顔が画像フレーム内にあるか否かを検出することを含む。ブロック２２４で、処理２２０は、撮像デバイス３０２が、撮像される被写体の第１特徴を決定する工程を備える。いくつかの実施例において、被写体の第１特徴は、被写体のグレア特性、被写体の反射特性の一方または両方に対応する。撮像される被写体は、コンピュータデバイス（例

えば、被写体３０８）、コンピュータデバイスの電子ディスプレイ、ＩＤ文書１１４Ｃ、または、生身の人間のユーザ３１０を含みうる。

【００８８】

ブロック２２６で、処理２２０は、撮像デバイス３０２が、撮像される被写体の第２特徴を決定する工程を備える。いくつかの実施例において、被写体の第２特徴は、被写体のエッジ特性３１６、被写体の反射特性３１８の一方または両方に対応する。被写体の１または複数の特徴は、デバイス３０２が、被写体のデジタル表現を含むデジタル画像の画像データを解析することに基づいて決定されうる。いくつかの実施例において、デバイス３０２は、クラウドベースのコンピュータシステム例に画像データを提供し、クラウドベースのシステムは、画像データを解析して、画像フレーム内に描写された被写体の１または複数の特徴または特性を決定する。

【００８９】

ブロック２２８で、撮像デバイス３０２は、被写体の第１特徴を示す１または複数のパラメータ値が第１閾値パラメータ値を超えるか否か、もしくは、被写体の第２特徴を示す１または複数のパラメータ値が第２閾値パラメータ値を超えるか否かを判定する。 ブロック２３０で、１または複数のパラメータ値が特定の閾値パラメータ値を超えるか否かを判定したことに応じて、デバイス３０２は、撮像される被写体が、なりすまし被写体、すなわち、なりすましデバイスであるのか、または、実際の生身の人間のユーザであるのかを示す。

【００９０】

いくつかの実施例において、撮像される被写体は、デバイス３０２に隣接してローカルに位置する生身の人間のユーザ３１０でありうる。潜在的ななりすまし攻撃が試みられる別の実施形態において、測定される被写体は、被写体１１４Ｂ、被写体１１４Ｃ、または、被写体３０８などのなりすまし被写体である。いくつかの実施例において、デバイス３０２は、クラウドベースのコンピュータデバイスを用いて実行された解析に基づいて、撮像される被写体が、なりすましデバイスであるのか、生身の人間のユーザであるのかを示す。

【００９１】

一般に、ＩＤ文書、シート上の写真、または、電子デバイスなどのアイテムについて、試みられるなりすまし動作は、アイテムをデバイス３０２に掲げて、セルフィーキャプチャを模倣することを含みうる。いくつかの例において、撮像デバイス３０２は、アイテムのデジタル画像／写真をキャプチャできる。キャプチャされた画像は、画像キャプチャ中にアイテムの周囲または背後に現れる検出されたエッジ、フレーム、境界、または、背景特性（各々上述した）を含みうる。別の例において、撮像デバイス３０２は、パラメータ値に基づいてアイテムに関連するグレア、反射、色、または、明度特性（例えば、第１／第２特徴または特性）を検出するよう構成される。

【００９２】

次いで、デバイス３０２は、アイテムに関連する第１／第２特徴（または特性）を示すパラメータ値を、閾値パラメータ値または関連パラメータ値のいずれかと比較できる。比較の結果は、ライブ画像キャプチャ中になりすまし攻撃が試みられているか否かを判定するために用いられる。いくつかの実施例において、ライブ画像キャプチャ中になりすまし攻撃が試みられているか否かを判定するために、複数の画像特性のパラメータ値および閾値の比較が、同時に用いられてもよい。

【００９３】

本明細書に記載した主題および機能的動作の実施形態は、デジタル電子回路、有形で具現化されたコンピュータソフトウェアまたはファームウェア、本明細書に開示した構造およびそれらの構造の等価物を含むコンピュータハードウェア、もしくは、それらの１または複数の組みあわせの中に実装されうる。

【００９４】

本明細書に記載の主題の実施形態は、１または複数のコンピュータプログラム（すなわ

ち、データ処理装置によって実行されるため、または、データ処理装置の動作を制御するための、有形の非一時的なプログラムキャリアにエンコードされたコンピュータプログラム命令の１または複数のモジュール）として実装されてもよい。

【００９５】

代替的または追加的に、プログラム命令は、データ処理装置による実行に向けて適切な受信装置に送信するために情報をエンコードするために生成された人工生成の伝搬信号（例えば、機械生成された電気、光学、または、電磁信号）にエンコードされうる。コンピュータストレージ媒体は、機械読み取り可能なストレージデバイス、機械読み取り可能なストレージ基板、ランダムまたはシリアルアクセスメモリデバイス、もしくは、それらの内の１または複数の組み合わせであってよい。

【００９６】

コンピュータプログラム（プログラム、ソフトウェア、ソフトウェアアプリケーション、モジュール、ソフトウェアモジュール、スクリプト、または、コードとも呼ばれうる、または、記載されうる）は、コンパイルまたは解釈された言語もしくは宣言型言語または手続き型言語など、任意の形態のプログラミング言語で書かれてよく、スタンドアローンプログラムとして、もしくは、モジュール、コンポーネント、サブルーチン、または、計算環境内での利用に適したその他のユニットなど、任意の形態で配備されてよい。コンピュータプログラムは、ファイルシステム内のファイルに対応してよいが、必ずしもその必要はない。

【００９７】

プログラムは、他のプログラムまたはデータを保持するファイルの一部（例えば、マークアップ言語文書に格納された１または複数のスクリプト）、そのプログラム専用の単一のファイル、または、複数の協調的なファイル（例えば、１または複数のモジュール、サブプログラム、または、コードの一部を格納するファイル）に格納されてよい。コンピュータプログラムは、１つのコンピュータ上で実行されるように配備されてもよいし、１つの場所に位置するかまたは複数の場所にわたって分散されて通信ネットワークによって相互接続された複数のコンピュータ上で実行されるように配備されてもよい。

【００９８】

本明細書に記載の処理および論理フローは、１または複数のプログラム可能なコンピュータが、入力データに作用して出力を生成することによって機能を実行するための１または複数のコンピュータプログラムを実行することで実行されうる。処理および論理フローは、専用の論理回路（例えば、ＦＰＧＡ（フィールドプログラマブルゲートアレイ）、ＡＳＩＣ（特定用途向け集積回路）、または、ＧＰＧＰＵ（汎用グラフィクス処理ユニット））によって実行されてもよく、装置は、かかる専用の論理回路として実装されてもよい。

【００９９】

コンピュータプログラムの実行に適したコンピュータは、汎用または専用マイクロプロセッサまたはその両方、もしくは、任意のその他の種類の中央処理装置以下を含む（例えば、基づきうる）。一般に、中央処理装置は、リードオンリーメモリまたはランダムアクセスメモリもしくはその両方から命令およびデータを受信する。コンピュータの基本的な要素は、命令を実行するための中央処理装置、ならびに、命令およびデータを格納するための１または複数のメモリデバイスである。

【０１００】

一般に、コンピュータは、データを格納するための１または複数のマスストレージデバイス（例えば、磁気、光磁気ディスク、または、光学ディスク）をさらに備えるか、もしくは、そこからデータを受信または転送またはその両方を行うように動作可能に接続される。しかしながら、コンピュータは、かかるデバイスを有する必要はない。さらに、コンピュータは、別のデバイス（例えば、いくつかの例を挙げると、携帯電話、パーソナルデジタルアシスタント（ＰＤＡ）、携帯オーディオまたはビデオプレーヤ、ゲーム機、グローバルポジショニングシステム（ＧＰＳ）レシーバ、または、ポータブルストレージデバ

イス（ユニバーサルシリアルバス（ＵＳＢ）フラッシュドライブ））内に内蔵されてもよい。

【０１０１】

コンピュータプログラム命令およびデータを格納するのに適したコンピュータ読み取り可能媒体は、例えば、半導体メモリデバイス（例えば、ＥＰＲＯＭ、ＥＥＰＲＯＭ、および、フラッシュメモリデバイス）；磁気ディスク（例えば、内部ハードディスクまたはリムーバブルディスク）；光磁気光学ディスク；ならびに、ＣＤ－ＲＯＭおよびＤＶＤ－ＲＯＭディスクなど、すべての形態の不揮発性メモリ、媒体、および、メモリデバイスを含む。プロセッサおよびメモリは、専用の論理回路によって補完されてもよいし、そこに組み込まれてもよい。

【０１０２】

ユーザとの相互作用を提供するために、本明細書に記載の主題の実施形態は、ユーザに情報を表示するための表示デバイス（例えば、ＣＲＴ（ブラウン管）またはＬＣＤ（液晶ディスプレイ）モニタなど）と、キーボードと、ポインティングデバイス（例えば、ユーザがコンピュータに入力を提供するためのマウスまたはトラックボール）とを有するコンピュータに実装されてよい。

【０１０３】

他の種類のデバイスが、ユーザとの相互作用を提供するために用いられてもよく；例えば、ユーザに提供されるフィードバックは、任意の形態の感覚フィードバック（例えば、視覚フィードバック、音声フィードバック、または、触覚フィードバック）であってよく；ユーザからの入力は、音響入力、音声入力、または、触覚入力など、任意の形態で受信されてよい。さらに、コンピュータは、ユーザによって用いられるデバイスに対して文書を送受信することによって（例えば、ウェブブラウザから受信した要求に応答して、ユーザのクライアントデバイス上のウェブブラウザにウエブページを送信することによって）ユーザと相互作用できる。

【０１０４】

本明細書に記載の主題の実施形態は、（例えば、データサーバとしての）バックエンドコンポーネント、ミドルウェアコンポーネント（例えば、アプリケーションサーバ）、フロントエンドコンポーネント（例えば、ユーザが本明細書に記載の主題の実施例と相互作用するためのグラフィカルユーザインターフェースまたはウェブブラウザを有するクライアントコンピュータ）、もしくは、１または複数のかかるバックエンド、ミドルウェア、または、フロントエンドコンポーネントの任意の組みあわせを含むコンピュータシステムに実装されてよい。

【０１０５】

システムのコンポーネントは、任意の形態または媒体のデジタルデータ通信（例えば、通信ネットワーク）によって相互接続されうる。通信ネットワークの例は、ローカルエリアネットワーク（ＬＡＮ）およびワイドエリアネットワーク（ＷＡＮ）（例えば、インターネット）を含む。コンピュータシステムは、クライアントおよびサーバを含みうる。クライアントおよびサーバは、一般に、互いに離れており、通例は、通信ネットワークを通して相互作用する。クライアントおよびサーバの関係性は、それぞれのコンピュータ上で実行されて互いにクライアントサーバ関係を有するコンピュータプログラムによって生じる。

【０１０６】

本明細書は、多くの具体的な実施例の詳細を含むが、これらは、どの発明の範囲に対しても請求されうるものの範囲に対しても限定として解釈されるべきではなく、むしろ、特定の発明の特定の実施形態に特有でありうる特徴の記載として解釈されるべきである。別個の実施形態の文脈で本明細書に記載された特定の特徴が、単一の実施形態で組みあわせて実施されてもよい。

【０１０７】

逆に、単一の実施形態の文脈で記載された様々な特徴が、別個にまたは任意の適切な副

組み合わせで複数の実施形態で実施されてもよい。さらに、特徴は、特定の組みあわせで機能するものとして上述され、最初にそのように請求されてもいるが、請求されている組みあわせからの１または複数の特徴が、一部の例において、組みあわせから除外されてもよく、請求されている組みあわせが、副組み合わせまたは副組み合わせの変形例に向けられてもよい。

【０１０８】

同様に、動作は、特定の順序で図示されているが、これは、所望の結果を達成するために、かかる動作が図の特定の順序または順番で実行されること、または、図に示したすべての動作が実行されることを求めると理解されるべきではない。特定の状況では、マルチタスクおよび並列処理が有利でありうる。さらに、上述した実施形態における様々なシステムモジュールおよび構成要素の分離は、すべての実施形態においてかかる分離が必要であると理解されるべきではなく、上述したプログラム構成要素およびシステムは、一般に、単一のソフトウェア製品に統合されてもよいし、複数のソフトウェア製品にパッケージングされてもよい。

【０１０９】

主題の特定の実施形態について記載した。他の実施形態も、以下の特許請求の範囲内にある。例えば、請求項に記載した動作は、異なる順序で実行されても、所望の結果を達成しうる。一例として、添付の図面に示した処理は、所望の結果を達成するために、図に示した特定の順序または順番を必ずしも必要とするわけではない。特定の実施例では、マルチタスクおよび並列処理が有利でありうる。

【図１】

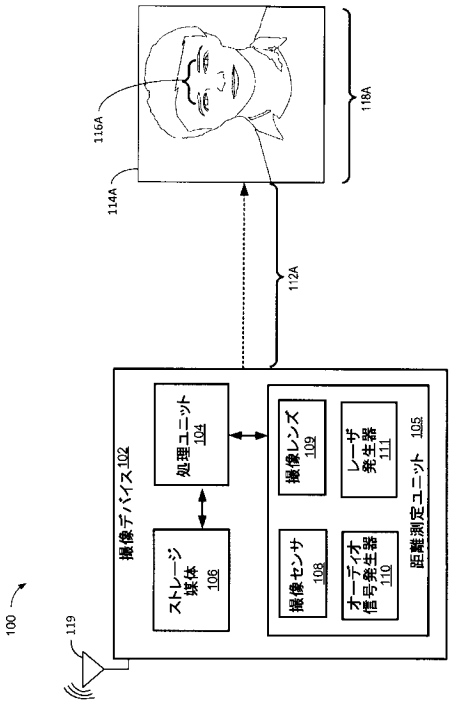

FIG. 1

【図２】

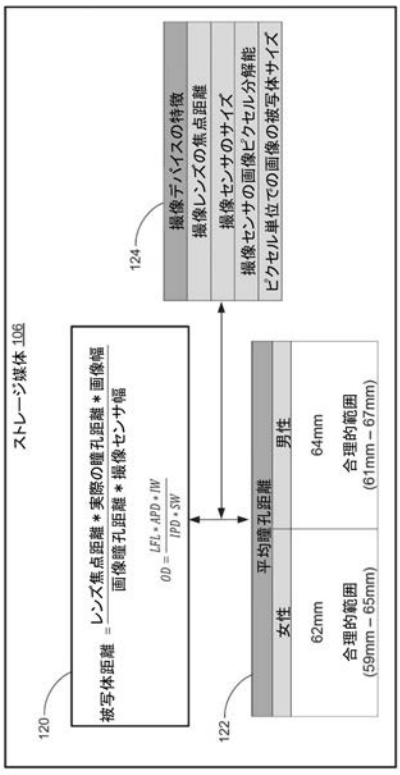

FIG. 2

【図３】

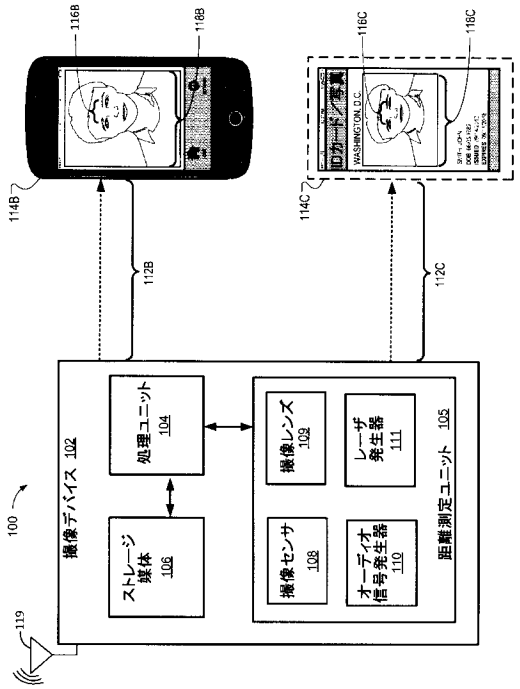

FIG. 3

【図４】

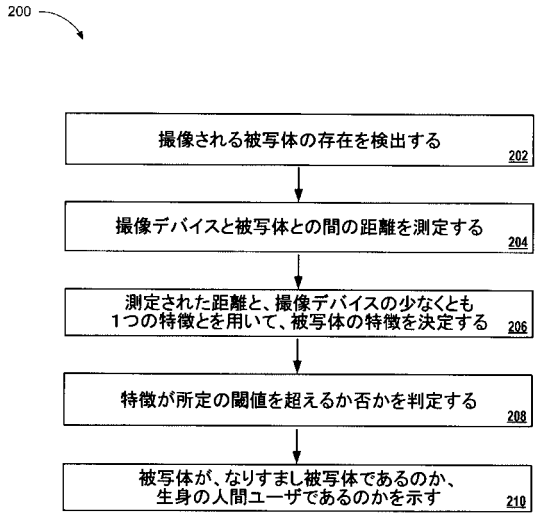

FIG. 4

【図５】

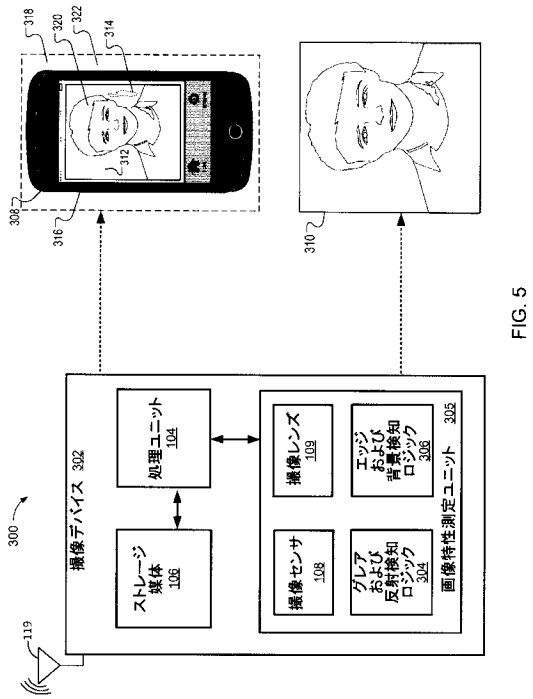

FIG. 5

【図６】

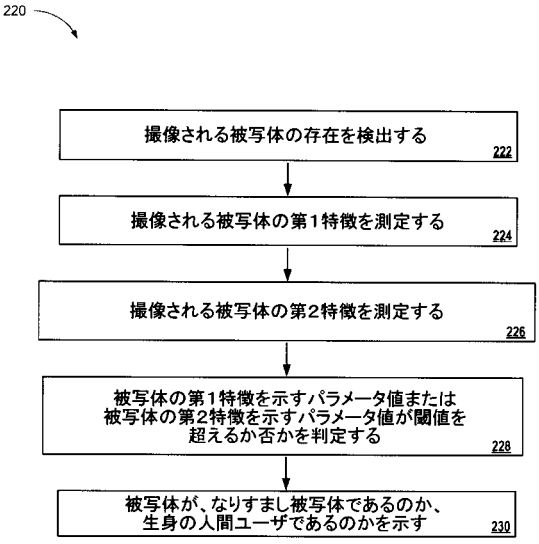

FIG. 6

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2017/040753

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06K 9/00; G06K 9/62; G06T 1/00; G06T 7/00 (2017.01)
CPC - G06K 9/00; G06K 9/00033; G06K 9/00214; G06K 9/00221; G06K 9/00261; G06K 9/00268; G06K 9/00899; G06K 9/62; G06T 1/00; G06T 7/00 (2017.08)

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)
See Search History document

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC - 340/5.830; 340/5.800; 382/103.000; 382/115.000; 382/117.000; 382/118.000; 382/165.000; 382/173.000 (keyword delimited)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
See Search History document

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2016/076912 A1 (INTEL CORPORATION) 19 May 2016 (19.05.2016) entire document	1-4, 7, 8, 11-16, 18-20
---		---
Y		5, 6, 9, 10, 17
Y	US 2016/0125178 A1 (DELTA ID INC.) 05 May 2016 (05.05.2016) entire document	5, 6, 17
Y	US 7,973,838 B2 (MCCUTCHEN) 05 July 2011 (05.07.2011) entire document	9, 10
A	US 2015/0310253 A1 (AGRAWAL et al) 29 October 2015 (29.10.2015) entire document	1-20
A	US 7,502,059 B2 (BARNA) 10 March 2009 (10.03.2009) entire document	1-20
A	US 2014/0049373 A1 (FLASHSCAN3D, LLC) 20 February 2014 (20.02.2014) entire document	1-20
A	US 8,856,541 B1 (GOOGLE INC.) 07 October 2014 (07.10.2014) entire document	1-20
A	US 2016/0148066 A1 (INTEL CORPORATION) 26 May 2016 (26.05.2016) entire document	1-20
A	MENOTTI et al. Deep Representations for Iris, Face, and Fingerprint Spoofing Detection. IEEE Transactions on Information Forensics and Security. Vol. 10, Iss. 4; 864-879, 2015. [retrieved on 22.08.2017]. Retrieved from the Internet. <URL:https://arxiv.org/pdf/1410.1980>. entire document	1-20
A	US 2015/0227781 A1 (NEC CORPORATION) 13 August 2015 (13.08.2015) entire document	1-20

☒ Further documents are listed in the continuation of Box C. ☐ 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
29 August 2017	12 SEP 2017
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, VA 22313-1450 Facsimile No. 571-273-8300	Authorized officer Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2017/040753

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 9,117,109 B2 (NECHYBA et al) 25 August 2015 (25.08.2015) entire document	1-20
A	US 8,317,325 B2 (RAGUIN et al) 27 November 2012 (27.11.2012) entire document	1-20
A	US 8,570,341 B1 (XIE) 29 October 2013 (29.10.2013) entire document	1-20
A	US 9,183,460 B2 (ZHANG et al) 10 November 2015 (10.11.2015) entire document	1-20

Form PCT/ISA/210 (continuation of second sheet) (January 2015)

フロントページの続き

(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,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,IR,IS,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,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT

(72)発明者　ウー・イーチェン
アメリカ合衆国　マサチューセッツ州０２４２０　レキシントン，アップル・ツリー・レーン，５
(72)発明者　マーティン・ブライアン・ケー.
アメリカ合衆国　ペンシルベニア州１５３１７　マクムーリー，モリー・ドライブ，２３６

Ｆターム(参考) 5C122 EA07 FC06 FD03 FE02 FH11 FH14 HA26 HA29 HA88
5L096 DA02 FA59 FA66 FA70 GA38 GA51 JA11