

明 細 書

発明の名称：

ゲート装置、認証システム、ゲート制御方法及び記憶媒体

技術分野

[0001] 本発明は、ゲート装置、認証システム、ゲート制御方法及び記憶媒体に関する。

背景技術

[0002] 顔認証を用いたサービスの普及が始まっている。例えば、空港における各種手続き（例えば、チェックイン、荷物預け入れ、セキュリティチェック等）に顔認証の適用が始まっている。顔認証を用いたサービスはゲート装置を用いて提供されることが多い（特許文献 1、2 参照）。

[0003] 例えば、特許文献 1 には、簡易な構成で、ウォークスルー顔認証の利便性を維持しながら、未認証者の不正通行を防止可能とする、と記載されている。特許文献 1 に開示された顔認証システムは、画像取得手段と、記憶手段と、顔照合手段と、認可手段と、を備える。画像取得手段は、認証領域を撮影して入力画像を順次取得する。記憶手段は、予め登録された利用者の登録顔画像を記憶する。顔照合手段は、入力画像から抽出された人物の顔画像と登録顔画像とを照合し、当該人物が前記利用者であることを認証する。認可手段は、入力画像における認証された人物を示す領域の大きさが所定以上のとき、当該人物の通行を許可する。特許文献 1 に開示された顔認証システムは、顔認証により正規利用者と認証されたとしても、その認証者がカメラから離れた位置にいる場合は通行許可せず、認証者のカメラ側への接近を検出した時点で通行を許可する。

先行技術文献

特許文献

[0004] 特許文献 1：特開 2015-001790 号公報

特許文献 2：特開 2019-133364 号公報

発明の概要

発明が解決しようとする課題

- [0005] 特許文献１に開示されたように、カメラの前に利用者を立ち止まらせることなく、ウォーキングペースで利用者を撮影して顔認証を行う認証方式がある。ウォーキングペースの顔認証を行う場合、エリアセンサを用いて、ゲート装置前方の所定のエリアに利用者が到達したことを検知する。所定のエリアに利用者が到達したことが検知されると、認証処理が始まる。
- [0006] ここで、認証対象者をカメラの前に立ち止まらせることなく撮影するためには、エリアセンサの検知範囲を延伸することが望ましい。しかし、エリアセンサの検知範囲を延伸すると、最終的にはゲート装置を通過しない利用者の顔画像を用いた認証処理が実行される可能性が高くなる。利用者の認証に成功したことを契機にゲートが開くと、認証に成功していない第三者によるゲート通過を許す可能性がある。
- [0007] この点、特許文献１に開示された顔認証システムは、認証者がゲート装置の近くに位置していることを画像処理（人の大きさが所定値以上か否かを判定する画像処理）にて判定している。しかし、人の大きさ（身長）は個人差が大きく、画像処理を利用した人物の位置判定手法ではゲートが正しいタイミングで開く保証がない。例えば、背の高い利用者はゲート装置から遠い位置にいてもゲート装置に近づいていると判定される傾向が強くなり、上記第三者によるゲート通過の余地がある。
- [0008] 本発明は、認証されていない利用者の通過を防止することに寄与する、ゲート装置、認証システム、ゲート制御方法及び記憶媒体を提供することを主たる目的とする。

課題を解決するための手段

- [0009] 本発明の第１の視点によれば、認証エリアに存在する認証対象者の生体情報を取得する、取得部と、前記取得された生体情報を含む認証要求をサーバ装置に送信する、認証要求部と、自装置への進入者を検出するためのセンサを用いて前記進入者を検出すると共に、前記進入者と前記認証対象者が同一

人物か否かを判定する、判定部と、前記サーバ装置による認証が成功し、且つ、前記進入者と前記認証対象者が同一人物である場合に、前記認証対象者が通過できるようにゲートを制御する、ゲート制御部と、を備える、ゲート装置が提供される。

[0010] 本発明の第2の視点によれば、複数のシステム利用者それぞれの生体情報を記憶し、前記複数の生体情報を利用した認証処理を実行する、サーバ装置と、前記サーバ装置と接続されたゲート装置と、を含み、前記ゲート装置は、認証エリアに存在する認証対象者の生体情報を取得する、取得部と、前記取得された生体情報を含む認証要求を前記サーバ装置に送信する、認証要求部と、自装置への進入者を検出するためのセンサを用いて前記進入者を検出すると共に、前記進入者と前記認証対象者が同一人物か否かを判定する、判定部と、前記サーバ装置による認証が成功し、且つ、前記進入者と前記認証対象者が同一人物である場合に、前記認証対象者が通過できるようにゲートを制御する、ゲート制御部と、を備える、認証システムが提供される。

[0011] 本発明の第3の視点によれば、ゲート装置において、認証エリアに存在する認証対象者の生体情報を取得し、前記取得された生体情報を含む認証要求をサーバ装置に送信し、自装置への進入者を検出するためのセンサを用いて前記進入者を検出すると共に、前記進入者と前記認証対象者が同一人物か否かを判定し、前記サーバ装置による認証が成功し、且つ、前記進入者と前記認証対象者が同一人物である場合に、前記認証対象者が通過できるようにゲートを制御する、ゲート制御方法が提供される。

[0012] 本発明の第4の視点によれば、ゲート装置に搭載されたコンピュータに、認証エリアに存在する認証対象者の生体情報を取得する処理と、前記取得された生体情報を含む認証要求をサーバ装置に送信する処理と、自装置への進入者を検出するためのセンサを用いて前記進入者を検出すると共に、前記進入者と前記認証対象者が同一人物か否かを判定する処理と、前記サーバ装置による認証が成功し、且つ、前記進入者と前記認証対象者が同一人物である場合に、前記認証対象者が通過できるようにゲートを制御する処理と、を実

行させるためのプログラムを記憶する、コンピュータ読取可能な記憶媒体が提供される。

発明の効果

[0013] 本発明の各視点によれば、認証されていない利用者の通過を防止することに寄与する、ゲート装置、認証システム、ゲート制御方法及び記憶媒体が提供される。なお、本発明の効果は上記に限定されない。本発明により、当該効果の代わりに、又は当該効果と共に、他の効果が奏されてもよい。

図面の簡単な説明

[0014] [図1]一実施形態の概要を説明するための図である。
[図2]第1の実施形態に係る認証システムの概略構成の一例を示す図である。
[図3]第1の実施形態に係るゲート装置の外観の一例を示す図である。
[図4]第1の実施形態に係るゲート装置の平面図の一例を示す図である。
[図5]第1の実施形態に係るゲート装置の処理構成の一例を示す図である。
[図6]認証要求の一例を示す図である。
[図7]第1の実施形態に係るゲート装置の動作の一例を示すフローチャートである。
[図8]第1の実施形態に係るサーバ装置の処理構成の一例を示す図である。
[図9]利用者データベースの一例を示す図である。
[図10]第1の実施形態に係る認証システムの動作の一例を示すシーケンス図である。
[図11]第2の実施形態に係るゲート装置の動作の一例を示すフローチャートである。
[図12]ゲート装置のハードウェア構成の一例を示す図である。
[図13]認証要求の一例を示す図である。
[図14]認証要求の一例を示す図である。

発明を実施するための形態

[0015] はじめに、一実施形態の概要について説明する。なお、この概要に付記した図面参照符号は、理解を助けるための一例として各要素に便宜上付記した

ものであり、この概要の記載はなんらの限定を意図するものではない。また、特段の釈明がない場合には、各図面に記載されたブロックはハードウェア単位の構成ではなく、機能単位の構成を表す。各図におけるブロック間の接続線は、双方向及び単方向の双方を含む。一方向矢印については、主たる信号（データ）の流れを模式的に示すものであり、双方向性を排除するものではない。なお、本明細書及び図面において、同様に説明されることが可能な要素については、同一の符号を付することにより重複説明が省略され得る。

[0016] 一実施形態に係るゲート装置１００は、取得部１０１と、認証要求部１０２と、判定部１０３と、ゲート制御部１０４と、を備える（図１参照）。取得部１０１は、認証エリアに存在する認証対象者の生体情報を取得する。認証要求部１０２は、取得された生体情報を含む認証要求をサーバ装置に送信する。判定部１０３は、自装置への進入者を検出するためのセンサを用いて進入者を検出すると共に、進入者と認証対象者が同一人物か否かを判定する。ゲート制御部１０４は、サーバ装置による認証が成功し、且つ、進入者と認証対象者が同一人物である場合に、認証対象者が通過できるようにゲートを制御する。

[0017] ゲート装置１００は、認証エリアに到達した利用者の生体情報を取得し、当該取得された生体情報を用いた認証処理をサーバ装置に依頼する。サーバ装置による認証処理と並行して、ゲート装置１００は、自装置の内部エリア（ゲート装置１００の本体により囲まれたエリア）に進入する利用者を検出する。その際、ゲート装置１００は、進入者の検出に、例えば、通過センサのような確実性の高い手段を用いるので、確実な検出（進入者の検出）が行われる。ゲート装置１００は、認証に成功した利用者が進入したと判定した場合に、ゲートを開く。その結果、認証されていない利用者がゲートを通過することが防止できる。

[0018] 以下に具体的な実施形態について、図面を参照してさらに詳しく説明する。

[0019] [第１の実施形態]

第 1 の実施形態について、図面を用いてより詳細に説明する。

[0020] 図 2 は、第 1 の実施形態に係る認証システムの概略構成の一例を示す図である。図 2 を参照すると、認証システムは、複数のゲート装置 10-1 ~ 10-3 と、サーバ装置 20 と、を含む。

[0021] 以降の説明において、ゲート装置 10-1 ~ 10-3 を区別する特段の理由がない場合には、単に「ゲート装置 10」と表記する。図 2 に示す構成は例示であって、ゲート装置 10 の台数等を限定する趣旨ではない。認証システムは、少なくとも 1 台以上のゲート装置 10 を含んでいればよい。

[0022] ゲート装置 10 とサーバ装置 20 は、有線又は無線の通信手段により通信が可能に構成されている。サーバ装置 20 は、ゲート装置 10 と同じ建物内に設置されていてもよいし、ネットワーク（クラウド）上に設置されていてもよい。

[0023] ゲート装置 10 は、例えば、空港や駅に設置される装置である。ゲート装置 10 は、利用者の通行を制御する。ゲート装置 10 は、サーバ装置 20 による認証が成功した利用者（以下、認証成功者と表記する）の通行を許可する。ゲート装置 10 は、サーバ装置 20 による認証が行われていない利用者や認証に失敗した利用者（以下、認証失敗者と表記する）の通行を許可しない。以降の説明において、サーバ装置 20 による認証が行われていない利用者を「未認証者」と表記する。

[0024] サーバ装置 20 は、認証処理を行う装置である。具体的には、サーバ装置 20 は、ゲート装置 10 を通過できる利用者（システム利用者）の生体情報を記憶する。サーバ装置 20 は、ゲート装置 10 から取得した生体情報と予め記憶された生体情報を用いた認証処理を実行し、認証結果（認証成功、認証失敗）をゲート装置 10 に通知する。

[0025] ゲート装置 10 は、認証結果が「認証成功」、且つ、認証成功者が自装置の内部エリアに進入していると判定した場合にゲートを開き、認証対象者の通過を許可する。換言すれば、ゲート装置 10 は、サーバ装置 20 から「認証成功」を受信したとしても、認証成功者が自装置の内部エリアに進入して

いなければゲートを開くことはない。

[0026] 利用者の生体情報には、例えば、顔、虹彩の模様（パターン）といった個人に固有な身体的特徴から計算されるデータ（特徴量）が例示される。あるいは、利用者の生体情報は、顔画像、虹彩画像等の画像データであってもよい。利用者の生体情報は、利用者の身体的特徴を情報として含むものであればよい。

[0027] 続いて、第１の実施形態に係る認証システムに含まれる各装置の詳細について説明する。以降の説明では、生体情報として利用者の「顔画像」を例にとり説明を行う。

[0028] [ゲート装置]

図３は、第１の実施形態に係るゲート装置１０の外観の一例を示す図である。

[0029] 図３を参照すると、ゲート装置１０は、顔認証モジュール１１を備えている。顔認証モジュール１１は、ゲート装置１０の本体に取り付けられている。顔認証モジュール１１は、カメラ１２を備える。なお、ゲート装置１０の「本体」とは、ゲート装置１０の中心をなす構造体であり、床と接触し、顔認証モジュール等が取り付けられた部材である。

[0030] 顔認証モジュール１１は、調光用のＬＥＤ（Light Emitting Diode）（図示せず）、ディスプレイ１３を備える。ゲート装置１０は、調光用のＬＥＤを用いて利用者の顔画像取得時における環境（利用者に照射される光）を制御する。ゲート装置１０は、ディスプレイ１３を用いて、利用者に対して必要なメッセージ等を通知する。例えば、ゲート装置１０は、サーバ装置２０による認証結果（認証成功、認証失敗）に関する表示を行う。

[0031] ゲート装置１０は、ディスプレイ１４を備える。ゲート装置１０は、ディスプレイ１４を用いて、利用者に対して必要なメッセージ等を通知する。例えば、ゲート装置１０は、サーバ装置２０による認証結果（認証成功、認証失敗）に関する表示を行う。あるいは、ゲート装置１０は、スピーカー（図示せず）を用いて必要なメッセージを利用者に通知してもよい。

- [0032] ゲート装置 10 は、エリアセンサ 15 を備える。エリアセンサ 15 は、ゲート装置 10 の前方に設定された所定エリア（図 3 にて点線で囲まれたエリア）に人が存在するか否かを検出するためのセンサである。エリアセンサ 15 は、赤外線を利用したセンサ（所謂、人感センサ）を用いて構成することができる。
- [0033] ゲート装置 10 は、エリアセンサ 15 からの検出信号に基づき上記所定エリアに人が存在することを確認すると、カメラ 12 を制御し、画像データを取得する。以降の説明において、エリアセンサ 15 が人の存在を検出するエリアを「認証エリア」と表記する。ゲート装置 10 は、認証エリアに人が存在することを検出すると、当該認証エリアに所在する利用者を撮像する。
- [0034] ゲート装置 10 は、ゲート内センサ 16 を備える。ゲート内センサ 16 は、自装置（ゲート装置 10）の内部に人が進入したことを検出するためのセンサである。ゲート内センサ 16 には、例えば、光の送信デバイスと受信デバイスにより構成されたセンサ（所謂、光を用いた通過センサ）を利用できる。例えば、光の送信デバイスと受信デバイスのそれぞれが対向するように設置される（本体の内壁に 2 つのデバイスが設置される）。送信デバイスは、光を常時送信し、受信デバイスは、当該送信された光を受信する。ゲート装置 10 は、受信デバイスが光を受信できなかった場合に、ゲート装置 10 の内部に人が進入したと判定する。なお、図 3 では、ゲート内センサ 16 を構成する 2 つのデバイスのうち一方のデバイスを図示している。ゲート内センサ 16 は、人の進行方向に略等間隔に複数対設けられても良い。
- [0035] ゲート装置 10 は、ゲート 17 を備える。ゲート装置 10 は、認証エリアに利用者が存在することを確認すると、利用者の顔画像を取得する。ゲート装置 10 は、取得した画像から特徴量（生体情報）を生成し、当該生成した特徴量を含む認証要求をサーバ装置 20 に送信する。ゲート装置 10 は、サーバ装置 20 による認証に成功し、且つ、認証成功者が自装置に進入していると判定された場合に、ゲート 17 を開く。ゲート装置 10 は、認証成功者がゲート 17 を通過した後に、ゲート 17 を閉じる。

- [0036] ゲート 17 の方式は、特に限定されるものではなく、例えば、通路の片側又は両側から設けられたフラPPERが開閉するフラPPERゲート、3本バーが回転するターンスタイルゲート等である。
- [0037] 顔認証モジュール 11 は、利用者がゲート装置 10 に向かって歩いてくる方向に対して所定の角度傾けて設置されている。図 4 は、ゲート装置 10 の上方から当該装置を見下ろした場合を示す図（平面図）である。
- [0038] 図 4 に示すように、顔認証モジュール 11 は、利用者が歩いてくる方向（ゲート 17 に対して垂直な方向）に対して角度 θ 傾けて設置されている。なお、角度 θ は、カメラ 12 が認証エリア内の利用者 U を撮像可能となるように選択（調整）される。
- [0039] 角度 θ を小さくするとゲート装置 10 の近傍しか撮像できず、顔画像を用いた認証処理が終了する前に利用者がゲート装置 10 の内部に進入する可能性がある。この場合、利用者は認証処理が終了するまで立ち止まって待機する必要があり快適なウォークスルーが実現できているとは言えない。対して、角度 θ を大きくするとゲート装置 10 の遠方まで撮像できるようになる。この場合、快適なウォークスルーの実現には有利であるが、自装置に向かって歩いていない利用者まで認証してしまう可能性がある。例えば、図 2 の例では、ゲート装置 10-1 に向かって歩いていない利用者をゲート装置 10-1 が撮像し、サーバ装置 20 に認証を要求してしまう。このように、角度 θ が大きすぎると、無駄な認証処理が発生する可能性がある。システムの管理者、運用者は、上記のような顔認証モジュール 11 の設定角度 θ に起因する利害得失を考慮し、最適な角度を決定するのが望ましい。なお、発明者らが鋭意検討した結果、角度 θ は 30°～60°の範囲から選択されるのが望ましいことが判明した。
- [0040] 図 5 は、第 1 の実施形態に係るゲート装置 10 の処理構成（処理モジュール）の一例を示す図である。図 5 を参照すると、ゲート装置 10 は、通信制御部 201 と、認証対象者検出部 202 と、生体情報取得部 203 と、認証要求部 204 と、進入者判定部 205 と、ゲート制御部 206 と、メッセー

ジ出力部 207 と、記憶部 208 と、を含む。

- [0041] 通信制御部 201 は、他の装置との間の通信を制御する手段である。具体的には、通信制御部 201 は、サーバ装置 20 からデータ（パケット）を受信する。また、通信制御部 201 は、サーバ装置 20 に向けてデータを送信する。通信制御部 201 は、他の装置から受信したデータを他の処理モジュールに引き渡す。通信制御部 201 は、他の処理モジュールから取得したデータを他の装置に向けて送信する。このように、他の処理モジュールは、通信制御部 201 を介して他の装置とデータの送受信を行う。
- [0042] 認証対象者検出部 202 は、認証エリアの認証対象者（認証処理の対象となる利用者）を検出する手段である。認証対象者検出部 202 は、エリアセンサ 15 からの検出信号に基づき認証エリアに存在する人（利用者）を検出する。認証対象者検出部 202 は、エリアセンサ 15 の出力が「認証エリアに利用者あり」を示す場合、その旨を生体情報取得部 203 に通知する。
- [0043] 生体情報取得部 203 は、認証エリアに存在する認証対象者の生体情報を取得する手段である。生体情報取得部 203 は、認証対象者検出部 202 から「認証エリアに利用者あり」に係る通知を取得すると、カメラ 12 を制御し、認証エリアに所在する利用者を撮像する。
- [0044] 生体情報取得部 203 は、得られた画像から顔画像（顔領域）の抽出を試みる。例えば、生体情報取得部 203 は、CNN（Convolutional Neural Network）により学習された学習モデルを用いて、画像データの中から顔画像（顔領域）を抽出する。あるいは、生体情報取得部 203 は、テンプレートマッチング等の手法を用いて顔画像を抽出してもよい。
- [0045] 顔画像が抽出できた場合、生体情報取得部 203 は、当該顔画像から特徴量（複数の特徴量からなる特徴ベクトル）を生成する。具体的には、生体情報取得部 203 は、取得した顔画像から特徴点を抽出する。なお、特徴点の抽出処理に関しては既存の技術を用いることができるのでその詳細な説明を省略する。例えば、生体情報取得部 203 は、顔画像から目、鼻、口等の特徴点として抽出する。その後、生体情報取得部 203 は、特徴点それぞれの

位置や各特徴点間の距離を特徴量として計算し、複数の特徴量からなる特徴ベクトル（顔画像を特徴づけるベクトル情報）を生成する。

[0046] 生体情報取得部203は、生成した特徴量（特徴ベクトル）を認証要求部204に引き渡す。

[0047] 認証要求部204は、認証対象者の認証処理をサーバ装置20に要求する手段である。認証要求部204は、生体情報取得部203から取得した特徴量（生体情報）を含む認証要求を生成し、サーバ装置20に送信する。

[0048] 例えば、認証要求部204は、自装置の識別子（以下、ゲート識別子と表記する）、特徴量等を含む認証要求を生成する（図6参照）。なお、ゲート識別子には、ゲート装置10のMAC（Media Access Control）アドレスやIP（Internet Protocol）アドレスを用いることができる。

[0049] また、認証要求部204は、認証要求をサーバ装置20に送信する際、当該要求に含まれる特徴量を進入者判定部205に引き渡す。

[0050] 認証要求部204は、認証要求に対するサーバ装置20からの応答を受信する。認証要求部204は、サーバ装置20からの応答（認証成功、認証失敗）をゲート制御部206に引き渡す。

[0051] 進入者判定部205は、自装置（ゲート装置10）への進入者を検出するためのゲート内センサ16を用いて進入者を検出すると共に、進入者と認証対象者が同一人物か否かを判定する手段である。進入者判定部205は、ゲート内センサ16の出力を監視（ポーリング）する。ゲート内センサ16の出力が「内部に進入者あり」を示す場合、進入者判定部205は、当該進入者と認証対象者が一致するか否かを判定する。具体的には、進入者判定部205は、生体情報取得部203と同様に、カメラ12を制御し、顔画像を取得する。進入者判定部205は、得られた顔画像から特徴量（進入者の特徴量）を計算する。

[0052] 進入者判定部205は、当該計算した特徴量（進入者の特徴量）と認証要求部204から取得した特徴量（認証対象者の特徴量）が実質的に一致するか否かを判定する。具体的には、進入者判定部205は、上記2つの特徴量

間の類似度を計算する。当該類似度には、カイ二乗距離やユークリッド距離等を用いることができる。なお、距離が離れているほど類似度は低く、距離が近いほど類似度が高い。進入者判定部205は、類似度が所定の値以上の場合に、2つの特徴量は実質的に一致（進入者と認証対象者は同一人物）と判定する。

[0053] このように、進入者判定部205は、光を用いた通過センサ（ゲート内センサ16）からの検出信号に基づき進入者を検出する。その後、進入者判定部205は、2つの特徴量（進入者の特徴量、認証対象者の特徴量）を用いた1対1照合を実施する。当該1対1照合（進入者の生体情報と認証対象者の生体情報を用いた1対1照合）により、進入者と認証対象者が同一人物か否かが判定される。

[0054] 進入者判定部205は、進入者と認証対象者が同一人物であると判定した場合、その旨をゲート制御部206に通知する。

[0055] ゲート制御部206は、ゲート装置10が備えるゲート17を制御する手段である。ゲート制御部206は、サーバ装置20の認証結果が「認証成功」、且つ、進入者と認証対象者が同一人物である場合に、ゲート17を開く。換言すれば、ゲート制御部206は、上記条件（認証成功、進入者と認証対象者が同一人物）が満たされなければ原則としてゲート17を開くことはない。ゲート制御部206は、距離センサ等を用いて通行が許可された利用者がゲート17を通過した後にゲート17を閉じる。

[0056] メッセージ出力部207は、利用者に通知するメッセージを出力する手段である。メッセージ出力部207は、ディスプレイ13、14やスピーカー等を用いて必要なメッセージを利用者に通知する。

[0057] 記憶部208は、ゲート装置10の動作に必要な情報を記憶する手段である。

[0058] 図7は、第1の実施形態に係るゲート装置10の動作の一例を示すフローチャートである。

[0059] ゲート装置10は、認証エリアに認証対象者が存在するか否かを検出する

(ステップS 1 0 1)。認証対象者が検出されないと(ステップS 1 0 1、N o 分岐)、ゲート装置1 0はステップS 1 0 1の処理を繰り返す。

[0060] 認証対象者が検出されると(ステップS 1 0 1、Y e s 分岐)、ゲート装置1 0は、認証エリアに位置する利用者(認証対象者)を撮像し、顔画像を取得する(ステップS 1 0 2)。

[0061] ゲート装置1 0は、顔画像から特徴量を計算する(ステップS 1 0 3)。

[0062] ゲート装置1 0は、当該計算された特徴量を含む認証要求をサーバ装置2 0に送信し、当該認証要求に対する応答(認証結果)を受信する(ステップS 1 0 4)。

[0063] ゲート装置1 0は、自装置の内部に進入者が存在するか否かを判定する(ステップS 1 0 5)。進入者の検出処理を開始して所定時間経過しても進入者が検出できないと(ステップS 1 0 5、N o 分岐)、ゲート装置1 0はステップS 1 0 9に係る処理を実行する。

[0064] 所定期間の間に進入者が検出されると(ステップS 1 0 5、Y e s 分岐)、ゲート装置1 0は、進入者と認証対象者が同一人物か否かを判定する(ステップS 1 0 6)。進入者と認証対象者が同一人物でなければ(ステップS 1 0 6、N o 分岐)、ゲート装置1 0はステップS 1 0 9に係る処理を実行する。

[0065] 進入者と認証対象者が同一人物であれば(ステップS 1 0 6、Y e s 分岐)、ゲート装置1 0は、サーバ装置2 0から取得した認証結果が「認証成功」であるか否かを判定する(ステップS 1 0 7)。認証結果が「認証失敗」であれば、ゲート装置1 0はステップS 1 0 9に係る処理を実行する。なお、ステップS 1 0 7に係る処理は、ステップS 1 0 5に係る処理の前に実行されても良いことは勿論である。

[0066] 認証結果が「認証成功」であれば、ゲート装置1 0は、ゲート1 7を開門する(ステップS 1 0 8)。ゲート装置1 0は、ゲート開門条件(認証成功、且つ、進入者と認証対象者が同一人物)が満たされる場合に、認証対象者が通過できるようにゲート1 7を制御する。その際、ゲート装置1 0は、認

証対象者の認証に成功した旨をディスプレイ 13、14 に表示してもよい。

[0067] 上記条件が満たされない場合（ステップ S105、S106、S107 のいずれかにおいて N o 分岐）、ゲート装置 10 は、エラー処理を実行する（ステップ S109）。具体的には、所定期間の間に進入者を検出できない場合（ステップ S105、N o 分岐）、ゲート装置 10 は、サーバ装置 20 から取得した認証結果を破棄する。進入者と認証対象者が異なる場合（ステップ S106、N o 分岐）、ゲート装置 10 は、その旨をディスプレイ 13、14 に表示する。サーバ装置 20 による認証に失敗した場合（ステップ S107、N o 分岐）、ゲート装置 10 は、その旨をディスプレイ 13、14 に表示する。

[0068] [サーバ装置]

図 8 は、第 1 の実施形態に係るサーバ装置 20 の処理構成（処理モジュール）の一例を示す図である。図 8 を参照すると、サーバ装置 20 は、通信制御部 301 と、利用者登録部 302 と、認証部 303 と、記憶部 304 と、を含む。

[0069] 通信制御部 301 は、他の装置との間の通信を制御する手段である。具体的には、通信制御部 301 は、ゲート装置 10 からデータ（パケット）を受信する。また、通信制御部 301 は、ゲート装置 10 に向けてデータを送信する。通信制御部 301 は、他の装置から受信したデータを他の処理モジュールに引き渡す。通信制御部 301 は、他の処理モジュールから取得したデータを他の装置に向けて送信する。このように、他の処理モジュールは、通信制御部 301 を介して他の装置とデータの送受信を行う。

[0070] 利用者登録部 302 は、ゲート装置 10 を通過できる利用者（システム利用者）をシステム登録する手段である。利用者登録部 302 は、任意の手段を用いてゲート装置 10 を通過できる利用者の生体情報（例えば、顔画像）を取得する。

[0071] 例えば、ゲート装置 10 が空港に設置された装置の場合、システム利用者は、航空会社の WEB（ウェブ）ページや空港に設置されたキオスク端末を

用いて生体情報や個人情報（氏名、旅券番号等）をサーバ装置20に入力する。あるいは、ゲート装置10が駅の改札に設置された装置の場合、システム利用者は、鉄道会社等のWEBページや駅に設置された端末から生体情報、個人情報等をサーバ装置20に入力する。

[0072] 利用者登録部302は、顔画像を取得した場合には、当該顔画像から特徴量を計算する。利用者登録部302は、システム利用者の生体情報（例えば、顔画像から計算された特徴量）を「利用者データベース」に登録する。利用者登録部302は、必要に応じて、システム利用者を識別する利用者ID（Identifier）や個人情報（例えば、氏名、国籍、性別等）と生体情報に対応付けて利用者データベースに登録する（図9参照）。図9に示す利用者データベースは例示であって、他の項目が生体情報（特徴量）と対応付けて記憶されていてもよい。例えば、「顔画像」が利用者データベースに登録されていてもよい。

[0073] 認証部303は、ゲート装置10から受信した認証要求を処理する手段である。具体的には、認証部303は、認証要求に含まれる生体情報（特徴量）を照合対象に設定し、利用者データベースに登録された生体情報との間で照合処理を行う。

[0074] より具体的には、認証部303は、認証要求から取り出した特徴量を照合対象に設定し、利用者データベースに登録されている複数の特徴量との間で1対N（Nは正の整数、以下同じ）照合を実行する。

[0075] 認証部303は、照合対象の特徴量（特徴ベクトル）と登録側の複数の特徴量それぞれとの間の類似度を計算する。認証部303は、類似度が所定の値以上の特徴量が利用者データベースに登録されていれば「認証成功」に設定する。認証部303は、類似度が所定の値以上の特徴量が利用者データベースに登録されていなければ「認証失敗」に設定する。

[0076] また、認証部303は、利用者データベースに登録された複数の特徴量のうち、照合対象の特徴量との間の類似度が所定の値以上、且つ、最も類似度が高い特徴量を特定する。認証部303は、当該特定された特徴量に対応す

る利用者IDや個人情報を必要に応じて、他のモジュールやゲート装置10に送信する。例えば、ゲート装置10が空港に設置された装置であれば、認証部303により特定された情報（氏名、旅券番号等）を用いて手続きの進捗（チェックイン通過、セキュリティチェック通過等）が管理される。例えば、ゲート装置10が駅の改札に設置された装置であれば、上記特定された情報を用いて料金の精算処理等が行われる。

[0077] 記憶部304は、サーバ装置20の動作に必要な各種情報を記憶する。記憶部304には、利用者データベースが構築される。

[0078] 図10は、第1の実施形態に係る認証システムの動作の一例を示すシーケンス図である。なお、図10の動作に先立ち、システム利用者の登録は予め行われているものとする。

[0079] ゲート装置10は、認証エリアに所在する認証対象者を検出する（ステップS01）。なお、ゲート装置10は、認証対象者を検出した際、認証処理が実行中であることを利用者が認識できるような対応をしてもよい。例えば、ゲート装置10は、認証対象者の顔画像をディスプレイ13、14に表示してもよい。あるいは、ゲート装置10は、認証エリアからゲート装置10の内部エリアに進入するように促すメッセージや記号（例えば、矢印等）をディスプレイ13、14に表示してもよい。

[0080] ゲート装置10は、認証対象者（認証エリアに所在する利用者）の生体情報を取得し、生体情報を含む認証要求をサーバ装置20に送信する（ステップS02）。

[0081] サーバ装置20は、認証要求に含まれる生体情報と、利用者データベースに登録された生体情報と、を用いた認証処理を実行する（ステップS11）。

[0082] サーバ装置20は、認証結果（認証成功、認証失敗）をゲート装置10に送信する（ステップS12）。

[0083] ゲート装置10は、サーバ装置20の認証処理と並行して認証対象者が自装置に進入したか否かを判定する（進入者の検出；ステップS03）。

- [0084] ゲート装置 10 は、ゲート 17 を開門するための条件（ゲート開門条件）が満たされているか否かを確認する（ステップ S04）。具体的には、ゲート装置 10 は、認証成功、且つ、進入者と認証対象者が同一人物か否かを確認する。
- [0085] ゲート装置 10 は、ゲート開門条件が満たされていれば、ゲート 17 を開門する（ステップ S05）。
- [0086] 以上のように、第 1 の実施形態に係る認証システムは、認証エリアに到達した利用者の生体情報を取得し、当該取得された生体情報を用いた認証処理を実行する。また、認証処理と並行して、ゲート装置 10 は、自装置に進入する利用者を検出する。その際、ゲート装置 10 は、進入者の検出に「通過センサ」のような確実性の高い手段を用いるので、利用者の身長等に影響されない確実な検出（進入者の検出）が行われる。ゲート装置 10 は、認証に成功した利用者が進入したと判定した場合に、ゲート 17 を開く。その結果、第 1 の実施形態に係る認証システムでは、認証成功者がゲート装置 10 の内部に到達したタイミングでゲート 17 を開くことができ、認証されていない利用者の通過を防止すると共に、快適なウォークスルーを実現できる。
- [0087] [第 2 の実施形態]
- 続いて、第 2 の実施形態について図面を参照して詳細に説明する。
- [0088] 第 1 の実施形態では、認証対象者がゲート装置 10 の内部に進入した場合にゲート 17 を開門する場合について説明した。しかし、当該対応では認証に成功していない第三者（認証失敗者、未認証者）が認証対象者と一緒にゲート 17 を通過できる余地がある。
- [0089] 第 2 の実施形態では、認証対象者と一緒に、第三者がゲート 17 を通過することを防止する認証システムについて説明する。即ち、第 2 の実施形態では、認証成功者がゲート装置 10 を通過することに乗じて他の第三者もゲート装置 10 を通過する「共連れ」を防止することを説明する。
- [0090] 第 2 の実施形態に係る認証システムの構成は第 1 の実施形態と同一とすることができるので図 2 に相当する説明を省略する。また、第 2 の実施形態に

係るゲート装置１０、サーバ装置２０の処理構成も第１の実施形態と同一とすることができるので、その説明を省略する。以下、第１及び第２の実施形態における相違点を中心に説明する。

[0091] 第２の実施形態に係るゲート装置１０の進入者判定部２０５は、ゲート内センサ１６の検出信号に基づく検出結果が「内部に進入者あり」の場合、カメラ１２を制御して進入者を撮像する。進入者判定部２０５は、取得した画像に２以上の顔画像が含まれている場合、「共連れ発生」と判断する。

[0092] 進入者判定部２０５は、共連れ発生を検出すると、その旨をゲート制御部２０６に通知する。

[0093] ゲート制御部２０６は、共連れが発生している場合、ゲート１７を開門しない。即ち、第２の実施形態に係るゲート開門条件は「認証成功、認証対象者と進入者が同一人物、及び共連れなし」となる。

[0094] 図１１は、第２の実施形態に係るゲート装置１０の動作の一例を示すフローチャートである。図７と図１１に示すフローチャートにおいて同じ処理については同じ符号（ステップ）を付し重複する説明を省略する。

[0095] 進入者を検出すると（ステップＳ１０５、Ｙｅｓ分岐）、ゲート装置１０は画像を解析することで共連れが発生しているか否かを判定する（ステップＳ１１０）。共連れが発生していれば（ステップＳ１１０、Ｙｅｓ分岐）、ゲート装置１０は、エラー処理を実行する（ステップＳ１０９）。例えば、ゲート装置１０は、共連れを検出した旨と共に、共連れ者は外部にできるようにメッセージを出力する。

[0096] エラー処理の実行後、ゲート装置１０は、改めて進入者の検出（ステップＳ１０５）、共連れ発生の検出（ステップＳ１１０）等の処理を行ってもよい。

[0097] 共連れが発生していなければ（ステップＳ１１０、Ｎｏ分岐）、ゲート装置１０は、ステップＳ１０６以降の処理を実行する。

[0098] [第２の実施形態に係る変形例]

上述のように、ゲート装置１０は、共連れ発生を検出すると、所定のメッ

セージ（例えば、共連れ者は外部にでることを促すメッセージ）を出力するのが望ましい。さらに、ゲート装置１０は、進入者判定部２０５が撮像した画像データの解析結果に応じて出力するメッセージを変更してもよい。

[0099] 具体的には、進入者判定部２０５は、ゲート内センサ１６の検出信号に基づいて進入者を撮像する。進入者判定部２０５は、得られた画像データに２以上の顔画像が含まれるか否かを判定する。２以上の顔画像が含まれる場合、進入者判定部２０５は、当該画像データに認証対象者の顔画像が含まれるか否かを判定する。例えば、進入者判定部２０５は、認証要求部２０４から取得した特徴量と実質的に一致する特徴量を持つ顔画像が画像データに含まれるか否かを判定する。

[0100] 進入者判定部２０５は、判定結果をメッセージ出力部２０７に通知する。

[0101] 画像データに２以上の顔画像が含まれ、且つ、認証対象者の顔画像が含まれる場合は、認証対象者と共に第三者（共連れ者）がゲート装置１０の内部に進入していることを示す。この場合、メッセージ出力部２０７は、共連れ者は外部に出ることを促すメッセージを出力する。例えば、メッセージ出力部２０７は、「後ろの人は下がってください」といったようなメッセージを出力する。

[0102] 画像データに２以上の顔画像が含まれ、且つ、認証対象者の顔画像が含まれない場合は、ゲート装置１０への進入者（２以上の進入者）はゲート１７を通過することはできない。このような場合、メッセージ出力部２０７は、２以上の進入者はゲート装置１０の外部に出ることを促すメッセージを出力する。例えば、メッセージ出力部２０７は、「ゲート内の全ての人は下がってください」といったようなメッセージを出力する。

[0103] このように、メッセージ出力部２０７は、画像データに認証対象者の顔画像が含まれるか否かに応じて、出力するメッセージを変更してもよい。即ち、ゲート装置１０は、進入者を撮像して得られる画像データを解析し、その結果に応じて出力するメッセージを変更してもよい。

[0104] 以上のように、第２の実施形態に係る認証システムでは、ゲート装置１０

は、進入者を含む画像データを取得すると共に、取得された画像データに2以上の顔画像が含まれるか否かを判定する。ゲート装置10は、画像データに2以上の顔画像が含まれる場合に「共連れ発生」と判断する。即ち、ゲート装置10は、画像データに2以上の顔画像が含まれない場合に、認証対象者が通過できるようにゲート17を制御する。その結果、認証対象者と一緒に第三者がゲート17を通過することを防止できる。

[0105] 続いて、認証システムを構成する各装置のハードウェアについて説明する。図12は、ゲート装置10のハードウェア構成の一例を示す図である。なお、顔認証モジュール11、カメラ12等については既に説明を行っているので図12にはこれらの要素を図示していない。

[0106] ゲート装置10は、プロセッサ311、メモリ312、入出力インターフェイス313及び通信インターフェイス314等を備える。上記プロセッサ311等の構成要素は内部バス等により接続され、相互に通信可能に構成されている。

[0107] 但し、図12に示す構成は、ゲート装置10のハードウェア構成を限定する趣旨ではない。ゲート装置10は、図示しないハードウェアを含んでもよいし、必要に応じて入出力インターフェイス313を備えていなくともよい。また、ゲート装置10に含まれるプロセッサ311等の数も図12の例示に限定する趣旨ではなく、例えば、複数のプロセッサ311がゲート装置10に含まれていてもよい。

[0108] プロセッサ311は、例えば、CPU (Central Processing Unit)、MPU (Micro Processing Unit)、DSP (Digital Signal Processor) 等のプログラマブルなデバイスである。あるいは、プロセッサ311は、FPGA (Field Programmable Gate Array)、ASIC (Application Specific Integrated Circuit) 等のデバイスであってもよい。プロセッサ311は、オペレーティングシステム(OS; Operating System)を含む各種プログラムを実行する。

[0109] メモリ312は、RAM (Random Access Memory)、ROM (Read Only M

emory)、HDD(Hard Disk Drive)、SSD(Solid State Drive)等である。メモリ312は、OSプログラム、アプリケーションプログラム、各種データを格納する。

[0110] 入出力インターフェイス313は、図示しない表示装置や入力装置のインターフェイスである。表示装置は、ディスプレイ14とすることができる。入力装置は、ディスプレイ14と一体となったタッチパネルでもよい。

[0111] 通信インターフェイス314は、他の装置と通信を行う回路、モジュール等である。例えば、通信インターフェイス314は、NIC(Network Interface Card)等を備える。

[0112] ゲート装置10の機能は、各種処理モジュールにより実現される。当該処理モジュールは、例えば、メモリ312に格納されたプログラムをプロセッサ311が実行することで実現される。また、当該プログラムは、コンピュータが読み取り可能な記憶媒体に記録することができる。記憶媒体は、半導体メモリ、ハードディスク、磁気記録媒体、光記録媒体等の非トランジエント(non-transitory)なものとすることができる。即ち、本発明は、コンピュータプログラム製品として具現することも可能である。また、上記プログラムは、ネットワークを介してダウンロードするか、あるいは、プログラムを記憶した記憶媒体を用いて、更新することができる。さらに、上記処理モジュールは、半導体チップにより実現されてもよい。

[0113] なお、サーバ装置20もゲート装置10と同様に構成可能であり、その基本的なハードウェア構成はゲート装置10と相違する点はないので説明を省略する。

[0114] ゲート装置10は、コンピュータを搭載し、当該コンピュータにプログラムを実行させることでゲート装置10の機能が実現できる。また、ゲート装置10は、当該プログラムによりゲート制御方法を実行する。

[0115] [変形例]

なお、上記実施形態にて説明した認証システムの構成、動作等は例示であって、システムの構成等を限定する趣旨ではない。

- [0116] 本願開示のゲート装置 10 の適用先は特に限定されない。例えば、本願開示のゲート装置 10 の適用先（設置場所）として「空港」が例示される。具体的には、空港にて行われる生体認証を用いた審査システムを担う装置の一部としてゲート装置 10 が用いられてもよい。当該審査システムでは、チェックイン時に本人確認（撮影顔画像とパスポートに記載された顔画像が一致するか否かの確認）が行われ、顔データ（顔画像または特徴量）、フライト情報及びパスポート情報が対応付けられて記憶される。本人確認が終了すると、生体認証にて審査を行うためのトークンが生成される。空港内の各種審査エリア（例えば、保安検査場）に本願開示のゲート装置 10 が設置され、ゲート装置 10 はチェックイン時に登録された顔画像と自装置にて撮像した顔画像を照合することで、利用者を認証する。
- [0117] 上記実施形態では、ゲート装置 10 からサーバ装置 20 に顔画像から生成された特徴量に係る生体情報が送信される場合について説明した。しかし、ゲート装置 10 からサーバ装置 20 に「顔画像」そのものが生体情報として送信されてもよい。サーバ装置 20 は、取得した顔画像から特徴量を生成し、認証処理（1 対 N 照合）を実行してもよい。なお、顔画像そのものがサーバ装置 20 に送信された場合であっても、ゲート装置 10 は、顔画像から生成された特徴量を用いて認証対象者と進入者の同一性を判定する。
- [0118] 上記実施形態では、認証対象者と進入者の同一性に関する判定はゲート装置 10 にて実行されているが、当該判定はサーバ装置 20 にて実行されてもよい。この場合、ゲート装置 10 は、内部エリアへの進入者の生体情報を取得し、サーバ装置 20 に送信する。サーバ装置 20 は、認証要求に含まれる生体情報と上記進入者の生体情報を照合し、認証対象者と進入者の同一性を判定すればよい。
- [0119] 上記実施形態では、ゲート内センサ 16 を用いて進入者の検出を行っているが、カメラ 12 から得られる画像を解析することで進入者の検出が行われてもよい。
- [0120] 上記実施形態では、ゲート装置 10 が認証要求をサーバ装置 20 に送信し

、サーバ装置 20 が当該要求を処理する、所謂、クライアントサーバシステムについて説明した。しかし、サーバ装置 20 にて実行される認証処理はゲート装置 10 にて実行されてもよい。即ち、サーバ装置 20 の一部又は全部の機能はゲート装置 10 にて実現されてもよい。

[0121] 上記実施形態では、カメラ 12 は単眼のカメラであることを前提としているが、カメラ 12 は、奥行方向を測定できるデプスカメラ（ステレオカメラ）であってもよい。この場合、ゲート装置 10 は、エリアセンサ 15 に代えてステレオカメラから得られる画像を用いて認証エリアの認証対象者を検出してもよい。具体的には、ゲート装置 10 は、ステレオカメラから得らえる 2 枚の画像を解析（視差を利用した解析）し、顔認証モジュール 11 を基準とした利用者（認証対象者）の位置を計算する。ゲート装置 10 は、当該計算された位置が予め定めた認証エリア内であれば、「認証対象者あり」と判断する。

[0122] あるいは、ゲート装置 10 は、ステレオカメラを利用して複数の進入者（認証対象者、共連れ者）の位置関係を正確に把握してもよい。ゲート装置 10 は、進入者の位置に基づいて共連れ発生に伴うメッセージを変更してもよい。例えば、ゲート装置 10 は、認証対象者の後ろに共連れ者（認証失敗者、未認証者）が続いている場合には、「後ろの人はゲートから出てください」といったメッセージを出力する。対して、ゲート装置 10 は、共連れ者の後ろに認証対象者が続いている場合には、「前の人はゲートから出てください」といったメッセージを出力する。

[0123] 上記実施形態では、ゲート装置 10 への進入者を検出した際に得られた画像データに 2 以上の顔画像が含まれる場合には「共連れ発生」と判断される場合について説明した。しかし、共連れが発生していない場合（顔認証モジュール 11 の設置状況等により共連れが発生していない場合）でも、1 枚の画像データに 2 以上の顔画像が含まれる可能性がある。ゲート装置 10 は、画像データに含まれる顔画像（顔領域）のサイズを利用し、共連れの誤判定を防止してもよい。例えば、ゲート装置 10 は、画像データに含まれる顔領

域のサイズや目間の距離が所定値よりも小さい場合には、そのような顔領域を無視して共連れ発生の判断を行う。

[0124] あるいは、顔認証モジュール 11 に設置されたカメラ 12 とは異なるカメラを用いて共連れ発生が検出されてもよい。即ち、共連れの誤判定が起きないような角度等に「共連れ検出用のカメラ」が設置され、ゲート装置 10 は当該カメラから得られる画像データを用いて共連れ発生の検出を行ってもよい。

[0125] 上記実施形態では、認証エリアに 1 人の利用者が存在する場合を前提としている。しかし、実際には、認証エリアに複数の利用者が存在する場合も考えられる。つまり、1 枚の画像データに複数の認証対象者が写ることも想定される。この場合、ゲート装置 10 は、複数の認証対象者それぞれについて認証要求をサーバ装置 20 に送信してもよいし、複数の認証対象者に関する 1 つの認証要求をサーバ装置 20 に送信してもよい。前者の場合、1 台のゲート装置 10 から送信される認証要求を区別するため、認証要求を区別する ID（認証 ID）を認証要求に含めるのが望ましい（図 13 参照）。後者の場合、1 つの認証要求に含まれる各特徴量（生体情報）を区別するため、認証対象者の ID（認証対象者 ID）と対応する特徴量の組を認証要求に含めるのが望ましい（図 14）。サーバ装置 20 は、認証 ID や認証対象者 ID を用いて認証結果（認証成功、認証失敗）をゲート装置 10 に通知する。

[0126] 複数の認証対象者についての認証を同時に（並行して）サーバ装置 20 に要求した場合には、ゲート装置 10 は、共連れ判定の基準を変更するのが望ましい。例えば、2 人の認証対象者について認証要求をサーバ装置 20 に送信した場合、ゲート装置 10 は、進入者が 2 人であって当該 2 人の進入者が共に認証対象者であれば、ゲート 17 を開門する。この場合、ゲート装置 10 は、画像データに 3 以上の顔画像が含まれる場合に「共連れ発生」と判断してもよい。

[0127] ゲート装置 10 は、取得する画像（顔画像；生体情報）の目的に応じて調光用の LED の制御を変更してもよい。例えば、ゲート装置 10 は、認証エ

リアの認証対象者を撮像する場合と自装置への進入者を撮像する場合で光度を変更してもよい。

[0128] 複数のゲート装置 10 が連動、連携して動作してもよい。具体的には、サーバ装置 20 は、一のゲート装置 10 から取得した認証要求に対する応答を他のゲート装置 10 にも送信してもよい。例えば、図 2 の例では、ゲート装置 10-1 から取得した認証要求に対する認証結果がゲート装置 10-1 ~ 10-3 のそれぞれに送信されてもよい。この場合、ゲート装置 10-1 にて検出された認証対象者がゲート装置 10-2 に向かったとしても（ゲート装置 10-2 に進入しても）、当該認証対象者はゲート装置 10-2 を通過することができる。なお、この場合、ゲート装置 10-1 が生成した認証対象者の生体情報は、ゲート装置 10-1 から他のゲート装置 10-2、10-3 に送信される。あるいは、サーバ装置 20 から認証対象者の生体情報が他のゲート装置 10-2、10-3 に送信されてもよい。

[0129] ゲート装置 10 とサーバ装置 20 の間のデータ送受信の形態は特に限定されないが、これら装置間で送受信されるデータは暗号化されていてもよい。顔画像や当該顔画像から算出される特徴量は個人情報であり当該個人情報を適切に保護するためには、暗号化されたデータが送受信されることが望ましい。

[0130] ゲート装置 10 は、例えば、既存の施設の限られたスペースに設置することも想定される。この場合、ゲート装置 10 を通過する人の進行方向におけるゲート装置 10 の長さは、一般的な顔認証ゲートの長さである 2~3 メートルに比べて短い約 1.5 メートルとすることができ、ゲート 17 までの距離を例えば 96 センチメートル（成人男性の歩幅の 1 歩半に相当）とすることができ、ゲート装置 10 の長さを約 1.5 メートルとした場合、進行方向における認証エリアの長さは、約 30 センチメートルから 60 センチメートルとするのが好ましい。

[0131] 上記説明で用いた流れ図（フローチャート、シーケンス図）では、複数の工程（処理）が順番に記載されているが、実施形態で実行される工程の実行

順序は、その記載の順番に制限されない。実施形態では、例えば各処理を並行して実行する等、図示される工程の順番を内容的に支障のない範囲で変更することができる。

[0132] 上記の実施形態は本願開示の理解を容易にするために詳細に説明したものであり、上記説明したすべての構成が必要であることを意図したものではない。また、複数の実施形態について説明した場合には、各実施形態は単独で用いてもよいし、組み合わせて用いてもよい。例えば、実施形態の構成の一部を他の実施形態の構成に置き換えることや、実施形態の構成に他の実施形態の構成を加えることも可能である。さらに、実施形態の構成の一部について他の構成の追加、削除、置換が可能である。

[0133] 上記の説明により、本発明の産業上の利用可能性は明らかであるが、本発明は、空港や駅等に設置される認証システムなどに好適に適用可能である。

[0134] 上記の実施形態の一部又は全部は、以下の付記のようにも記載され得るが、以下には限られない。

[付記 1]

認証エリアに存在する認証対象者の生体情報を取得する、取得部と、
前記取得された生体情報を含む認証要求をサーバ装置に送信する、認証要求部と、

自装置への進入者を検出するためのセンサを用いて前記進入者を検出すると共に、前記進入者と前記認証対象者が同一人物か否かを判定する、判定部と、

前記サーバ装置による認証が成功し、且つ、前記進入者と前記認証対象者が同一人物である場合に、前記認証対象者が通過できるようにゲートを制御する、ゲート制御部と、

を備える、ゲート装置。

[付記 2]

前記判定部は、前記進入者の生体情報を取得し、前記進入者の生体情報と前記認証対象者の生体情報を用いた 1 対 1 照合により、前記進入者と前記認

証対象者が同一人物か否かを判定する、付記 1 に記載のゲート装置。

[付記 3]

前記判定部は、前記進入者を含む画像データを取得すると共に、前記取得された画像データに 2 以上の顔画像が含まれるか否かを判定し、

前記ゲート制御部は、前記画像データに 2 以上の顔画像が含まれない場合に、前記認証対象者が通過できるように前記ゲートを制御する、付記 1 又は 2 に記載のゲート装置。

[付記 4]

前記画像データに 2 以上の顔画像が含まれる場合には所定のメッセージを出力する、出力部をさらに備える、付記 3 に記載のゲート装置。

[付記 5]

前記出力部は、前記画像データに前記認証対象者の顔画像が含まれるか否かに応じて、前記出力される所定のメッセージを変更する、付記 4 に記載のゲート装置。

[付記 6]

前記取得部は、前記認証対象者の顔画像を取得し、

前記認証要求部は、前記認証対象者の顔画像から生成された特徴量を含む前記認証要求を前記サーバ装置に送信する、付記 1 乃至 5 のいずれかに記載のゲート装置。

[付記 7]

前記判定部は、光を用いた通過センサからの検出信号に基づき前記進入者を検出する、付記 1 乃至 6 のいずれかに記載のゲート装置。

[付記 8]

前記認証エリアの前記認証対象者を検出する、検出部をさらに備える、付記 1 乃至 7 のいずれかに記載のゲート装置。

[付記 9]

前記検出部は、赤外線を利用した人感センサからの検出信号に基づき前記認証対象者を検出する、付記 8 に記載のゲート装置。

[付記 10]

複数のシステム利用者それぞれの生体情報を記憶し、前記複数の生体情報を利用した認証処理を実行する、サーバ装置と、

前記サーバ装置と接続されたゲート装置と、

を含み、

前記ゲート装置は、

認証エリアに存在する認証対象者の生体情報を取得する、取得部と、

前記取得された生体情報を含む認証要求を前記サーバ装置に送信する、認証要求部と、

自装置への進入者を検出するためのセンサを用いて前記進入者を検出すると共に、前記進入者と前記認証対象者が同一人物か否かを判定する、判定部と、

前記サーバ装置による認証が成功し、且つ、前記進入者と前記認証対象者が同一人物である場合に、前記認証対象者が通過できるようにゲートを制御する、ゲート制御部と、

を備える、認証システム。

[付記 11]

ゲート装置において、

認証エリアに存在する認証対象者の生体情報を取得し、

前記取得された生体情報を含む認証要求をサーバ装置に送信し、

自装置への進入者を検出するためのセンサを用いて前記進入者を検出すると共に、前記進入者と前記認証対象者が同一人物か否かを判定し、

前記サーバ装置による認証が成功し、且つ、前記進入者と前記認証対象者が同一人物である場合に、前記認証対象者が通過できるようにゲートを制御する、ゲート制御方法。

[付記 12]

ゲート装置に搭載されたコンピュータに、

認証エリアに存在する認証対象者の生体情報を取得する処理と、

前記取得された生体情報を含む認証要求をサーバ装置に送信する処理と、
自装置への進入者を検出するためのセンサを用いて前記進入者を検出する
と共に、前記進入者と前記認証対象者が同一人物か否かを判定する処理と、
前記サーバ装置による認証が成功し、且つ、前記進入者と前記認証対象者
が同一人物である場合に、前記認証対象者が通過できるようにゲートを制御
する処理と、

を実行させるためのプログラムを記憶する、コンピュータ読取可能な記憶
媒体。

[0135] なお、引用した上記の先行技術文献の各開示は、本書に引用をもって繰り
込むものとする。以上、本発明の実施形態を説明したが、本発明はこれらの
実施形態に限定されるものではない。これらの実施形態は例示にすぎないとい
うこと、及び、本発明のスコップ及び精神から逸脱することなく様々な変
形が可能であるということは、当業者に理解されるであろう。即ち、本発明
は、請求の範囲を含む全開示、技術的思想にしたがって当業者であればなし
得る各種変形、修正を含むことは勿論である。

符号の説明

- [0136] 10、10-1～10-3、100 ゲート装置
- 11 顔認証モジュール
 - 12 カメラ
 - 13 ディスプレイ
 - 14 ディスプレイ
 - 15 エリアセンサ
 - 16 ゲート内センサ
 - 17 ゲート
 - 20 サーバ装置
 - 101 取得部
 - 102、204 認証要求部
 - 103 判定部

- 104、206 ゲート制御部
- 201、301 通信制御部
- 202 認証対象者検出部
- 203 生体情報取得部
- 205 進入者判定部
- 207 メッセージ出力部
- 208、304 記憶部
- 302 利用者登録部
- 303 認証部
- 311 プロセッサ
- 312 メモリ
- 313 入出力インターフェイス
- 314 通信インターフェイス