

明 細 書

発明の名称：

認証装置、認証方法、認証システムおよびプログラム

技術分野

[0001] 本開示は、認証装置、認証方法、認証システムおよびプログラムに関する。

背景技術

[0002] 顔認証によって、駅や空港などに設置されるゲート装置を通過する人の入退出を管理する技術が知られている。例えば、特許文献1には、ゲート装置に進入する進入者が所持する無線タグから送信された識別子に対応して登録される顔特徴量に基づいて、進入者の顔認証を行うことが可能なゲート装置が開示されている。

先行技術文献

特許文献

[0003] 特許文献1：特許第6816821号公報

発明の概要

発明が解決しようとする課題

[0004] ところで、将来的に顔認証に対応するゲート装置を含む認証システムが、利用者が多い駅等に展開される場合、その認証システムの登録者が膨大な数となる可能性がある。登録者数が増大すると、顔の特徴が類似する登録者も増大するため、ゲート装置への進入者の顔認証において誤認証するおそれがある。

[0005] 顔認証に対応するゲート装置では、進入者が認証処理のための特別な装置を用いなくとも通過できることがメリットであるが、上記のように、顔の特徴だけで認証を行う場合、認証精度に一定の限界があるので、当該メリットを享受しつつ、認証精度をさらに高める工夫が求められる。

[0006] 本開示の目的は、顔認証に対応するゲート装置のメリットを享受しつつ、

認証精度を高めることが可能な認証装置、認証方法、認証システムおよびプログラムを提供することである。

課題を解決するための手段

[0007] 本開示に係る認証装置は、

ゲート装置への進入者の携帯端末が前記ゲート装置の近傍に存在する場合に、前記携帯端末に登録される前記ゲート装置への進入者の登録情報と、複数の顔登録画像のうちの1つとを紐付ける処理を行う処理部と、

前記進入者の顔画像情報と前記複数の顔登録画像との照合結果に基づいて前記進入者を認証する認証処理において、前記登録情報に紐付けられた顔登録画像と前記進入者の顔画像情報との照合結果を、前記登録情報に紐付けられていない顔登録画像と前記進入者の顔画像情報との照合結果よりも優遇する認証部と、を備える。

[0008] 本開示に係る認証方法は、

ゲート装置への進入者の携帯端末が前記ゲート装置の近傍に存在する場合に、前記携帯端末に登録される前記ゲート装置への進入者の登録情報と、複数の顔登録画像のうちの1つとを紐付ける処理を行い、

前記進入者の顔画像情報と前記複数の顔登録画像との照合結果に基づいて、前記進入者を認証する認証処理において、前記登録情報に紐付けられた顔登録画像と前記進入者の顔画像情報との照合結果を、前記登録情報に紐付けられていない顔登録画像と前記進入者の顔画像情報との照合結果よりも優遇する。

[0009] 本開示に係る認証システムは、

進入者が進入可能なゲート装置と、

前記ゲート装置に対応して設けられ、前記進入者の顔画像情報を撮像する撮像装置と、

前記ゲート装置に対応して設けられ、前記進入者が所持する携帯端末にビーコン情報を送信するビーコン装置と、

前記携帯端末が前記ビーコン情報を受信したことに応じて、前記携帯端末

に登録される前記ゲート装置への進入者の登録情報と、複数の顔登録画像のうちの1つとを紐付け、

前記顔画像情報と前記複数の顔登録画像との照合結果に基づいて前記進入者を認証する認証処理において、前記登録情報に紐付けられた顔登録画像と前記進入者の顔画像情報との照合結果を、前記登録情報に紐付けられていない顔登録画像と前記進入者の顔画像情報との照合結果よりも優遇する認証装置と、

を備える。

[0010] 本開示に係るプログラムは、

認証装置と共に用いられる携帯端末を制御するプログラムであって、

前記認証装置は、

前記携帯端末から送信される前記携帯端末の利用者を示す登録情報と、複数の顔登録画像のうちの1つとを紐付ける処理を行い、

ゲート装置への進入者の顔画像情報と前記複数の顔登録画像との照合結果に基づいて、前記進入者を認証する認証処理において、前記登録情報に紐付けられた顔登録画像と前記進入者の顔画像情報との照合結果を、前記登録情報に紐付けられていない顔登録画像と前記進入者の顔画像情報との照合結果よりも優遇し、

前記プログラムは、携帯端末のコンピューターに、ビーコン情報を受信した場合に、前記ビーコン情報と前記登録情報とを送信するよう制御する処理を実行させる。

発明の効果

[0011] 本開示によれば、顔認証に対応するゲート装置のメリットを享受しつつ、認証精度を高めることができる。

図面の簡単な説明

[0012] [図1]本開示に係る認証システムの構成例を示す図である。

[図2]ユーザー管理サーバにおける顔登録画像とビーコンキャッチ情報との紐付けの一例を示す図である。

[図3]複数の認証候補のそれぞれの処理後スコアを示す図である。

[図4]認証装置における認証制御の動作例を示すフローチャートである。

[図5]認証装置におけるビーコンキャッチ情報の登録制御の動作例を示すフローチャートである。

[図6]携帯端末におけるビーコンキャッチ情報の送信制御の動作例を示すフローチャートである。

[図7]変形例に係る認証装置における複数の認証候補のそれぞれの処理後スコアを示す図である。

[図8]変形例に係る認証装置における認証制御の動作例を示すフローチャートである。

[図9]複数のビーコン装置を有する構成における、ビーコン装置の配置関係を示す図である。

[図10]複数のビーコン装置を有する構成における、ビーコン装置の配置関係を示す図である。

発明を実施するための形態

[0013] (実施の形態)

以下、本開示の実施の形態を図面に基づいて詳細に説明する。図1は、本開示に係る認証システムの構成例を示す図である。

[0014] 図1に示すように、本実施の形態に係る認証システム1は、例えば、空港、駅、イベント会場等の施設の出入り口に設置されるゲート装置（入場ゲート、改札ゲート等）を制御するシステムである。

[0015] 本実施の形態に係る認証システム1では、施設を利用する利用者の入退場の管理が、顔認証によって実行される。例えば、ゲート装置に進入する進入者が、ゲート装置を通過して施設内へ入場する場合、進入者が施設内への入場を許可された人物であるか否かが顔認証によって判定される。また、進入者がゲート装置を通過して施設外へ退場する場合、進入者が施設外への退場を許可された人物であるか否かが顔認証によって判定される。なお、「顔認証」とは、「顔画像を用いた照合」に含まれる概念と捉えてよい。

- [0016] 認証システム1は、ゲート装置10と、撮像装置20と、ビーコン装置30と、ユーザー管理サーバ40と、通過履歴管理サーバ50と、認証装置100と、を備える。
- [0017] ゲート装置10は、例えば駅等の施設に設置される自動改札機であり、進入者が進入可能に構成される。ゲート装置10は、図示しないCPU (Central Processing Unit)、ROM (Read Only Memory)、RAM (Random Access Memory) および入出力回路を備えている。
- [0018] ゲート装置10は、顔認証制御部、改札機制御部およびゲート開閉機能部等を有しており、施設への入退場を許可された人物の進入を容認し、施設への入退場を許可されていない人物の進入を阻止する制御を行う。
- [0019] 撮像装置20は、ゲート装置10への進入者の顔画像を撮像するカメラであり、ゲート装置10に対応して設けられる。ゲート装置10では、顔認証制御部が、撮像装置20により撮像された顔画像の情報を認証装置100に送信して、進入者の顔画像の照合を要求する。そして、顔認証制御部が、認証装置100から顔画像の照合結果を取得して、当該照合結果に基づいて、改札機制御部がゲート開閉機能部を制御することでゲートの開閉が制御される。
- [0020] ビーコン装置30は、ビーコン情報を送信する装置であり、ゲート装置10に対応して設けられる。ビーコン情報は、受信装置が当該ビーコン情報を受信（受波）することで、当該ビーコン情報を送信したビーコン装置30に付与される識別番号等を検出することが可能な信号である。ビーコン装置30が送信するビーコン情報は、ゲート装置10への進入者が所持する携帯端末2によって受信される。なお、本実施の形態では、ビーコン装置30は、Bluetooth（登録商標）を用いてビーコン情報を送信するものとする。ただし、ビーコン装置30は、他の無線通信方式によってビーコン情報を送信するものであっても構わない。また、受信装置が常に露出しているのであれば、ビーコン装置30は、電波ではなく赤外光などの光によってビーコン情報を送信するものであっても構わない。

- [0021] また、ビーコン装置30は、ゲート装置10の電源によって動作するようにしてもよい。こうすることで、電池駆動のビーコン装置のように、駆動時間の制限を考慮する必要がないので、ビーコン情報の発信周期等を自由に設定することができる。
- [0022] 携帯端末2は、例えば、進入者が所持するスマートフォン等の携帯用の端末であり、図示しないCPU、ROM、RAMおよび入出力回路を備えている。携帯端末2は、認証システム1に対応する、専用アプリケーションをインストールしたものであり、ビーコン装置30が送信するビーコン情報を受信可能に構成される。携帯端末2がビーコン情報を受信すると、ビーコンキャッチ情報が認証装置100に送信される。
- [0023] ビーコンキャッチ情報は、携帯端末2がビーコン情報を受信したことを示す情報であり、携帯端末2におけるビーコン情報の受信時刻と、進入者の登録情報と、ビーコン装置30のビーコン情報と等を含む。ビーコンキャッチ情報は、ビーコン装置30から認証装置100に送信されてもよいし、携帯端末2から認証装置100に送信されてもよい。本実施の形態では、携帯端末2から認証装置100に送信されるものとする。
- [0024] 進入者の登録情報は、例えば、認証システム1の専用アプリケーションにおいて登録された進入者の登録番号である。なお、登録情報は進入者を識別可能な情報であれば他の番号や文字列等であっても構わない。また、アプリケーションの識別番号や携帯端末2の識別番号など、進入者個人を間接的に識別可能な情報を登録情報として使用してもよい。
- [0025] ユーザー管理サーバ40は、認証システム1に登録した登録者の識別情報を管理するサーバである。ユーザー管理サーバ40には、登録者の顔画像が予め登録されている。登録された顔画像（以下、「顔登録画像」とする）は、当該顔登録画像の本人を識別する識別情報と紐付けて、ユーザー管理サーバ40に記憶されている（例えば、図2参照）。
- [0026] この識別情報は、進入者（登録者）が携帯端末2にインストールした専用アプリケーションにおいて登録した登録情報と同一であるもの、または同一

視可能なものであり、例えば複数の英数字をランダムに組み合わせて構成される番号である。

[0027] 通過履歴管理サーバ50は、進入者が認証装置100による認証を経由してゲート装置10を通過した履歴を示す情報を記録するサーバである。通過履歴管理サーバ50に記録される履歴の情報は、ゲート装置10への入場時刻の情報やゲート装置10からの退場時刻の情報等である。

[0028] 認証装置100は、例えばゲート装置10とは異なる位置に設けられたサーバであり、図示しないCPU、ROM、RAMおよび入出力回路を備えている。認証装置100は、予め設定されたプログラムに基づいて、進入者の認証の制御を行うように構成されている。認証装置100は、受信部110と、処理部120と、認証部130とを有する。

[0029] 受信部110は、携帯端末2から送信されるビーコンキャッチ情報を受信する。また、認証装置100では、受信部110が受信したビーコンキャッチ情報に基づくビーコン情報を、当該ビーコン情報に紐付くゲート装置10の位置情報に変換する。

[0030] 処理部120は、携帯端末2に登録される進入者の登録情報と、複数の顔登録画像のうちの1つと紐付ける処理を行う。具体的には、処理部120は、携帯端末2から登録情報を取得した場合、ユーザー管理サーバ40を参照し、ユーザー管理サーバ40における複数の顔登録画像に紐付けられた登録者の識別情報と登録情報とを照合する。

[0031] 処理部120は、進入者と一致する登録者が存在する場合、登録情報と識別情報に係る顔登録画像とを紐付ける処理を行う。具体的には、処理部120は、登録者の識別情報と、当該識別情報と一致する登録情報に係るビーコンキャッチ情報とを紐付けてユーザー管理サーバ40に登録する。

[0032] 例えば、図2に示す例では、ユーザー管理サーバ40に、識別情報と顔登録画像とを紐付けるテーブルにビーコンキャッチ情報の欄が設けられる。ビーコンキャッチ情報と紐付けられた識別情報におけるビーコンキャッチ情報の欄には、例えば、ビーコンキャッチ情報に含まれる情報が記載される。ビ

ーコンキャッチ情報と紐付けられていない識別情報ビーコンキャッチ情報の欄には、何の情報も記載されない。

- [0033] なお、ユーザー管理サーバ40における顔登録画像においてビーコンキャッチ情報が紐付けられていることが認識可能である限り、どのような形式でビーコンキャッチ情報が紐付けられていてもよい。また、顔登録画像に紐付けられるビーコンキャッチ情報は、ビーコンキャッチ情報の送信時刻および／または受信時刻や、ビーコン情報を送信したビーコン装置30に対応するゲート装置10の位置情報が認識可能にユーザー管理サーバ40に登録されるようにしてもよい。また、ビーコンキャッチ情報には、携帯端末2におけるビーコン情報の受信時刻が含まれてもよい。
- [0034] 認証部130は、ゲート装置10への進入者の顔画像情報に基づいて複数の顔登録画像の中から進入者を認証する。具体的には、認証部130は、ゲート装置10から顔画像の照合要求を取得した場合、撮像装置20から進入者の顔画像情報を取得する。
- [0035] 認証部130は、ユーザー管理サーバ40を参照し、ユーザー管理サーバ40における複数の顔登録画像と、顔画像情報とを照合して、複数の顔登録画像のそれぞれに係る複数のスコアを算出する。このスコアは、照合結果を示す値であり、本実施の形態では、照合結果が良好である（すなわち同一の人物である可能性が高い）ほど、スコアが高くなるものとして説明する。なお、顔登録画像のスコアの算出方法については公知の方法が用いられる。
- [0036] そして、認証部130は、算出した複数のスコアに応じて認証候補を抽出する。より詳細には、認証部130は、スコアが認証閾値未満となる顔登録画像を、認証候補から除外し、スコアが認証閾値以上となる顔登録画像を認証候補とする。本実施の形態では、後述する通り、携帯端末2に紐づけられたビーコンキャッチ情報に基づいてスコアの加算を行う場合があるため、あまりにスコアが低い認証候補であっても加算の結果、進入者が施設内への入場を許可された人物であると認証されることがある。しかし、スコアが極めて低い場合は、何らかの事情で携帯端末2を所持している別人である可能性

も高いため、このような別人までスコアの加算によって本人であると認証してしまうと誤認証が発生する。そこで、本実施の形態では、明らかにスコアが低い顔登録画像を予め認証候補から除外することで、このような誤認証の発生を抑制している。なお、スコアが低い顔登録画像を認証候補から除外せずに、スコアの加算処理の対象から除いても、同様の効果が得られる。

[0037] 認証閾値は、顔画像情報と、顔登録画像とが少なくとも類似していると判定できる程度のスコアの基準値であり、適宜設定可能である。

[0038] 認証部 130 は、スコアが認証閾値以上となる顔登録画像がない場合、認証システム 1 に登録されていない非登録者として進入者を認証する。認証部 130 は、スコアが認証閾値以上となる顔登録画像が 1 つであった場合、当該顔登録画像に紐付けられた登録者として進入者を認証する。

[0039] 認証部 130 は、スコアが認証閾値以上となる顔登録画像が複数あった場合、複数の顔登録画像のうち、ビーコンキャッチ情報に含まれる時刻情報が現在時刻から一定時間前までであるビーコンキャッチ情報と紐づけられている登録顔画像が存在するか確認する。

[0040] そして、認証部 130 は、このような顔登録画像が存在する場合、その顔登録画像のスコアに所定の加算処理を行う。つまり、認証部 130 は、進入者を認証する認証処理において、登録情報に紐付けられた顔登録画像と進入者の顔画像情報との照合結果を、登録情報に紐付けられていない顔登録画像と進入者の顔画像情報との照合結果よりも優遇する。この処理に用いる時刻情報としては、ビーコンキャッチ情報に含まれる任意の時刻情報を使用してよい。例えば、携帯端末 2 におけるビーコン情報の受信時刻、携帯端末 2 からビーコンキャッチ情報が送信された時刻、ユーザー管理サーバ 40 がビーコンキャッチ情報を受信した時刻が考えられる。本実施の形態では、一例として、携帯端末 2 におけるビーコン情報の受信時刻の情報をを用いるものとする。また、一定時間の例としては、例えば、ビーコン情報に対応するビーコン装置 30 から、認証装置 100 までの標準的な移動時間に基づいて設定される。現在認証を受けようとしている人物が、極端に古いビーコン情報に対

応する人物である可能性は低いためである。ただし、ビーコン装置30から認証装置100までの距離が遠かったり、他の施設などが存在する場合には、人物が道に迷ったり、他の施設に立ち寄る可能性があるため、一定時間を長く設定してもよい。

[0041] なお、顔登録画像に紐付けられたビーコンキャッチ情報に含まれるビーコン情報により変換されたゲート装置10の位置情報と、顔画像の照合を要求したゲート装置10の位置情報とが一致する場合、当該顔登録画像のスコアが加算処理の対象となる。

[0042] 認証部130は、加算処理が施されたスコアを含む複数のスコアの中から最も高いスコアに係る顔登録画像に紐付けられた登録者として進入者を認証する。

[0043] 例えば、図3に示すように、スコアが659の認証候補A1と、スコアが630の認証候補A2と、スコアが627の認証候補A3とが抽出されていたとする。この場合において、認証候補A2の顔登録画像の識別情報がビーコンキャッチ情報と紐付けられていたとすると、認証部130は、認証候補A2のスコアである630に、加算スコアとして、例えば100を加算する。

[0044] これにより、認証候補A2の処理後スコアが730となるので、複数の認証候補の中で認証候補A2が最も高いスコアとなる。その結果、認証部130は、認証候補A2に紐付けられた登録者として進入者を認証する。

[0045] 認証部130は、進入者を登録者または非登録者と認証した場合、ゲート装置10に認証結果を送信する。ゲート装置10は、認証部130より認証結果を取得した場合、その認証結果に応じてゲートの開閉を制御する。

[0046] 具体的には、ゲート装置10は、進入者が非登録者である認証結果である場合、ゲートを閉じる制御を行う。また、ゲート装置10は、進入者が登録者である認証結果である場合、ゲートを開く制御を行う。

[0047] このようにすることで、進入者の認証においてビーコンキャッチ情報の有無を考慮することができるので、認証システム1における認証精度を向上さ

せることができる。

[0048] ところで、複数の認証候補のうち、少なくとも2つにビーコンキャッチ情報が紐付けられていたとする。具体的には、例えば、顔の特徴が類似する2人の進入者（例えば、双子等）が進行方向に並んでゲート装置10へ進入しようとする、2人の進入者の携帯端末2がビーコン装置30のビーコン情報を受信したような状況が発生したとする。

[0049] この場合、認証部130は、ビーコン情報の受信時刻に応じて、認証候補を抽出するようにしてもよい。具体的には、認証部130は、複数の認証候補のうち、ビーコン情報の受信時刻が早い方を、認証候補として抽出する。これは、2人の進入者のうち、当該時刻が早い方が、先にゲート装置10に到達すると判断することによる。

[0050] このようにすることで、例えば、顔の類似した複数の進入者が同等のタイミングでゲート装置10へ進入する際の、認証候補の抽出を行いやすくすることができる。つまり、ビーコンキャッチ情報の受信時刻を考慮することで、複数の認証候補のうち、少なくとも2つにビーコンキャッチ情報が紐付けられていたとしても、ゲート装置10に先に到着した認証候補を推定しやすくなる。そのため、先にゲート装置10に到着した認証候補がゲート装置10を通過する可能性が高いと判断することで、当該認証候補を進入者と推定し、ひいては進入者の認証を行いやすくすることができる。

[0051] また、認証部130は、ビーコン情報の電界強度に応じて、認証候補を抽出するようにしてもよい。具体的には、認証部130は、複数の認証候補のうち、ビーコンキャッチ情報に係るビーコン情報の電界強度が強い方を、認証候補として抽出する。これは、2人の進入者のうち、ビーコン情報の電界強度が強い方が、ゲート装置10により近い位置に位置すると判断することによる。

[0052] ビーコン情報の電界強度の情報は、ビーコンキャッチ情報に含まれるようにしてもよい。また、電界強度の情報は、例えば携帯端末2で受信することで識別されるようにしてもよい。

- [0053] このようにすることで、例えば、顔の類似した複数の進入者が同等のタイミングでゲート装置10へ進入する際の、認証候補の抽出を行いやすくすることができる。つまり、ビーコン情報の電界強度を考慮することで、複数の認証候補のうち、少なくとも2つにビーコンキャッチ情報が紐付けられていたとしても、ゲート装置10に先に到着した認証候補を推定しやすくなる。そのため、先にゲート装置10に到着した認証候補がゲート装置10を通過する可能性が高いと判断することで、当該認証候補を進入者と推定し、ひいては進入者の認証を行いやすくすることができる。
- [0054] また、例えば、顔の類似した複数の進入者（通行人）がゲート装置10に近づいた後、一部の通行人がゲート装置10に進入しない場合でも、ビーコン情報の電界強度の変化を考慮することで、ゲート装置10に進入しない通行人を認証候補から除外することができる。つまり、ビーコン情報の電界強度を考慮することで、認証候補の抽出精度を向上させることができ、ひいては進入者の認証を行いやすくすることができる。
- [0055] また、認証部130は、携帯端末2の加速度センサ情報に基づいて、先にゲート装置10に到達する進入者を判断してもよい。
- [0056] 携帯端末2の加速度センサ情報は、例えば携帯端末2に内蔵される加速度センサによる移動ベクトルの情報であり、ビーコンキャッチ情報に含まれるようにするとよい。
- [0057] このようにすることで、2つのビーコンキャッチ情報が略同時刻に受信されていても、移動速度の速い方の認証候補がゲート装置10に先に到着すると推定し、ひいては進入者の認証を行いやすくすることができる。
- [0058] また、認証部130は、ゲート装置10の利用回数に応じて、認証候補を抽出して、認証処理において照合結果を優遇する顔登録画像を決定してもよい。具体的には、認証部130は、ゲート装置10毎にビーコンキャッチ情報の受信回数を、受信する度に記録して蓄積する処理を行う。なお、受信回数は、認証部で記録されても良いし、認証部以外の記録部に記録されてもよい。そして、複数の認証候補のうち、何れにもビーコンキャッチ情報が紐付

けられていない場合、認証部130は、進入者が進入しようとしているゲート装置と同一のゲート装置に対応するビーコンキャッチ情報の受信回数が最も多い認証候補の顔登録画像で、進入者を認証する。なお、認証部は、進入者が進入しようとしているゲート装置と同じ場所に設置されているゲート装置に対応するビーコンキャッチ情報の受信回数を用いて同様の処理を行ってもよい。複数のゲート装置が同じ場所に設置されている駅などの施設の場合、毎回同一のゲート装置を使用することは考えにくいためである。また、認証部130は、一定時間内の受信回数に基づいて上記の処理を実行することにより、ゲート装置10の利用頻度に応じた認証候補の抽出を行ってもよい。

[0059] このようにすることで、進入者が携帯端末2を所持し忘れた場合や携帯端末2の電源を切っている場合でも、認証を行いやすくすることができる。なお、上記ではビーコンキャッチ情報の受信回数が最も多い認証候補の顔登録画像を抽出するものとしたが、受信回数または受信頻度に基づいて複数の認証候補の顔登録画像を抽出するものとしてもよい。例えば、受信回数または頻度が所定の閾値以上である顔登録画像を抽出したり、受信回数または受信頻度の順位が上位から所定の順位以内である顔登録画像等を抽出したりすることが考えられる。

[0060] また、進入者が、正常に動作している携帯端末2を所持している場合にも、ビーコンキャッチ情報の受信回数または頻度を用いた処理を行うようにしてもよい。例えば、ビーコンキャッチ情報の過去の受信回数が多かったり受信頻度が高いほど加算スコアを増やしたり、受信回数が少なかったり受信頻度が低い場合には負の加算スコアを加算したりすることなどが考えられる。

[0061] また、処理部120は、進入者がゲート装置10を通過後、顔登録画像に紐付けられたビーコンキャッチ情報（登録情報）をユーザー管理サーバ40から消去する処理を行ってもよい。

[0062] このようにすることで、ビーコンキャッチ情報が、進入者の認証完了後において顔登録画像に紐付けられ続けることを抑制することができる。

- [0063] 以上のように構成された認証システム 1 における認証制御の動作例について説明する。まず、認証装置 100 における認証制御の動作例について説明する。図 4 は、認証装置 100 における認証制御の動作例を示すフローチャートである。図 4 における処理は、例えば、ゲート装置 10 の稼働中に適宜実行される。
- [0064] 図 4 に示すように、認証装置 100 は、顔画像照合要求があったか否かについて判定する（ステップ S 101）。判定の結果、顔画像照合要求がない場合（ステップ S 101、NO）、ステップ S 101 の処理が繰り返される。一方、顔画像照合要求がある場合（ステップ S 101、YES）、認証装置 100 は、顔画像情報を取得する（ステップ S 102）。
- [0065] 次に、認証装置 100 は、取得した顔画像情報と顔登録画像とを照合し、認証候補があるか否かについて判定する（ステップ S 103）。判定の結果、認証候補がない場合（ステップ S 103、NO）、認証装置 100 は、非登録者で進入者を認証する（ステップ S 104）。一方、認証候補がある場合（ステップ S 103、YES）、認証装置 100 は、認証候補が複数あるか否かについて判定する（ステップ S 105）。
- [0066] 判定の結果、認証候補が 1 つである場合（ステップ S 105、NO）、処理はステップ S 108 に遷移する。一方、認証候補が複数ある場合（ステップ S 105、YES）、認証装置 100 は、複数の認証候補の中にビーコンキャッチ情報の紐付けがある認証候補があるか否かについて判定する（ステップ S 106）。
- [0067] 判定の結果、ビーコンキャッチ情報の紐付けがある認証候補がない場合（ステップ S 106、NO）、処理はステップ S 108 に遷移する。一方、ビーコンキャッチ情報の紐付けがある認証候補がある場合（ステップ S 106、YES）、認証装置 100 は、当該認証候補のスコアに加算処理を実行する（ステップ S 107）。
- [0068] そして、認証装置 100 は、最も高いスコアの認証候補で進入者を認証する（ステップ S 108）。ステップ S 104 またはステップ S 108 の後、

本制御は終了する。

[0069] 次に、認証装置100におけるビーコンキャッチ情報の登録制御の動作例について説明する。図5は、認証装置100におけるビーコンキャッチ情報の登録制御の動作例を示すフローチャートである。図5における処理は、例えば、ゲート装置10の稼働中に適宜実行される。

[0070] 図5に示すように、認証装置100は、ビーコンキャッチ情報を受信したか否かについて判定する（ステップS201）。判定の結果、ビーコンキャッチ情報を受信していない場合（ステップS201、NO）、ステップS201の処理が繰り返される。一方、ビーコンキャッチ情報を受信した場合（ステップS201、YES）、認証装置100は、ビーコンキャッチ情報に基づく登録情報と一致する識別情報があるか否かについて判定する（ステップS202）。

[0071] 判定の結果、登録情報と一致する識別情報がない場合（ステップS202、NO）、本制御は終了する。一方、登録情報と一致する識別情報がある場合（ステップS202、YES）、認証装置100は、ビーコンキャッチ情報に基づくビーコン情報をゲート装置10の位置情報に変換し（ステップS203）、ビーコンキャッチ情報を顔登録画像に紐付けて登録する（ステップS204）。ステップS204の後、本制御は終了する。

[0072] 最後に、携帯端末2におけるビーコンキャッチ情報の送信制御について説明する。図6は、携帯端末2におけるビーコンキャッチ情報の送信制御の動作例を示すフローチャートである。図6における処理は、例えば、携帯端末2の電源がオンである間に適宜実行される。

[0073] 図6に示すように、携帯端末2は、ビーコン情報を受信したか否かについて判定する（ステップS301）。判定の結果、ビーコン情報を受信していない場合（ステップS301、NO）、処理はステップS305に遷移する。一方、ビーコン情報を受信した場合（ステップS301、YES）、携帯端末2は、ビーコン情報が、本実施の形態のシステム（本システム）のものであるか否かについて判定する（ステップS302）。

- [0074] 判定の結果、ビーコン情報が本実施の形態のシステムのものではない場合（ステップS302、NO）、処理はステップS305に遷移する。施設には本実施の形態のシステムとは異なるシステム向けのビーコンも存在する可能性があるため、そのようなビーコンを無視するためである。一方、ビーコン情報が本実施の形態のシステムのものである場合（ステップS302、YES）、携帯端末2は、ビーコンキャッチ情報を送信する（ステップS303）。
- [0075] 次に、携帯端末2は、所定時間が経過したか否かについて判定する（ステップS304）。判定の結果、所定時間が経過していない場合（ステップS304、NO）、ステップS304の処理が繰り返される。一方、所定時間が経過した場合（ステップS304、YES）、携帯端末2は、電源のオフ指令があるか否かについて判定する（ステップS305）。
- [0076] なお、所定時間は、ビーコンキャッチ情報の送信タイミングを考慮して適宜設定される時間である。この所定時間が設定されることにより、ビーコンキャッチ情報が頻繁に送信されることを抑制することができ、ひいては携帯端末2の電力消費量を低減することができる。
- [0077] 判定の結果、電源のオフ指令がない場合（ステップS305、NO）、処理はステップS301に戻る。一方、電源のオフ指令がある場合（ステップS305、YES）、本制御は終了する。
- [0078] 以上のように構成された本実施の形態によれば、進入者を認証する際、ビーコンキャッチ情報の取得の有無を考慮することができる。例えば、顔の特徴が酷似した複数の顔登録画像が存在する場合、そのうちの1つの顔登録画像に係る進入者が、ゲート装置10に進入する際、当該進入者の携帯端末2がビーコン装置30から送信されるビーコン情報を受信することで、認証装置100が、当該携帯端末2から送信されるビーコンキャッチ情報を取得する。
- [0079] これにより、ビーコンキャッチ情報における進入者の登録情報と、顔登録画像における識別情報とが照合されて、顔登録画像の識別情報と、登録情報

とが紐付けられる。その結果、ビーコンキャッチ情報が紐付けられた顔登録画像の登録者として進入者を認証しやすくすることができ、ひいては、認証システム1における認証精度を高めることができる。

[0080] また、進入者の携帯端末2としてスマートフォン等を利用することにより、進入者は、認証システム1に対応した特殊な装置を所持することなく、ゲート装置10を通過することができる。すなわち、本実施の形態では、顔認証に対応するゲート装置10のメリットを享受しつつ、認証精度を高めることができる。

[0081] ところで、ビーコンキャッチ情報を用いない構成の場合、顔の特徴が類似する2人の進入者のうちの第1進入者が、ゲート装置10で入場したとする。この場合、第1進入者に入場記録が通過履歴管理サーバ50に記録される。そして、第1進入者がゲート装置10から退場する前に、顔の特徴が類似する2人の進入者のうちの第2進入者がゲート装置10で入場しようとした際、第2進入者が第1進入者と誤認証された場合、第2進入者がゲート装置10に入場できない問題が生じるおそれがある。

[0082] それに対し、本実施の形態では、ビーコンキャッチ情報を考慮することで、第1進入者と第2進入者とを正確に認証することができるので、上記の問題が生じることを抑制することができる。例えば、携帯端末2を所持している第2進入者がゲート装置10へ入場しようとした際に、ビーコンキャッチ情報を考慮して正しい顔登録画像の認証スコアが加算されるので、第1進入者と同一人物だと誤認証される可能性を低減することができる。

[0083] また、第1進入者と第2進入者の顔の特徴が類似している場合、第1進入者が第2進入者だと誤認証される可能性があるが、第1進入者のビーコンキャッチ情報を用いることで、第1認証者が第2進入者であると誤認識される可能性を低減できる。これにより、第1進入者が第2進入者だと誤認証された結果、第2認証者がゲート装置10に入場できなくなる問題も発生しにくくすることができる。

[0084] なお、上記実施の形態では、ビーコンキャッチ情報が顔登録画像に紐付け

られているか否かでスコアの加算処理を行っていたが、本開示はこれに限定されない。例えば、ゲート装置 10 への通過履歴の情報に基づいて、進入者を認証してもよい。

[0085] 例えば、複数の認証候補が存在し、かつ、複数の認証候補における顔登録画像に一定時間内にビーコンキャッチ情報が紐付けられている状況であって、進入者がゲート装置 10 を入場しようとした状況が発生したとする。

[0086] この場合、認証部 130 は、例えば、通過履歴管理サーバ 50 を参照し、既にゲート装置 10 を通過している認証候補を除外し、ゲート装置 10 を通過していない認証候補に対して、認証に係る処理を行う。なお、複数の認証候補の全てがゲート装置 10 を通過している場合は、多重入場扱いとしてもよいし、通常通りの認証の処理を行うようにしてもよい。

[0087] また、複数の認証候補が存在し、かつ、複数の認証候補における顔登録画像に一定時間内にビーコンキャッチ情報が紐付けられている状況であって、進入者がゲート装置 10 を退場しようとした状況が発生したとする。

[0088] この場合、認証部 130 は、通過履歴管理サーバ 50 を参照し、ゲート装置 10 への入場履歴のない認証候補を除外し、ゲート装置 10 への入場履歴のある認証候補に対して、認証に係る処理を行う。なお、複数の認証候補の全てがゲート装置 10 への入場履歴がない場合は、退場拒否扱いとしてもよいし、通常通りの認証の処理を行うようにしてもよい。

[0089] このような構成によれば、進入者の通過履歴の情報をを用いることで、認証の処理を簡易にすることができる。また、進入者の通過履歴によって判断することにより、例えば、スコアが僅差であるような複数の進入者が、ゲート装置 10 への入場側、および退場側のそれぞれに存在した場合、入場と退場との違いによって識別しやすくすることができる。その結果、認証システム 1 における認証の精度を向上させることができる。

[0090] また、上記実施の形態では、複数の認証候補が存在した場合、処理部 120 の処理結果を常時利用したが、本開示はこれに限定されない。例えば、認証部 130 が複数の認証候補のスコア差に基づいて、処理部 120 の処理結果

を用いるか否かについて決定するようにしてもよい。

[0091] 具体的には、認証部130は、スコアが認証閾値以上となる顔登録画像が複数であった場合、複数のスコアのそれぞれのうち、スコアが高い順に所定の数の顔登録画像を認証候補として抽出する。

[0092] 所定の数は、例えば、3等、適宜設定可能な数である。本実施の形態では、所定の数が3に設定されている。

[0093] 認証部130は、抽出した複数の認証候補のスコア差に基づいて処理部120の処理結果を用いるか否かについて決定する。認証部130は、複数の認証候補のうち、最も高いスコアとなる認証候補とのスコア差が閾値以上である認証候補が存在する場合、処理部120の処理結果を用いないと決定する。つまり、認証部130は、スコア差が閾値以上である場合、登録情報に紐付けられた顔登録画像と進入者の顔画像情報との照合結果を優遇せずに、認証処理を行う。

[0094] この場合、認証部130は、例えば、複数の認証候補のうち、最も高いスコアの認証候補の顔登録画像に紐付けられた登録者として進入者を認証する。閾値は、スコア差として僅差となるような微小な値であり、適宜設定される。

[0095] 認証部130は、複数の認証候補のうち、最も高いスコアとなる認証候補とのスコア差が閾値未満である場合、処理部120の処理結果を用いると決定する。認証部130は、複数の認証候補のうち、処理部120により、進入者の登録情報と紐付けられた顔登録画像が存在する場合、当該顔登録画像に係る認証候補のスコアに所定の加算処理を行う。

[0096] 例えば、図7に示すように、スコアが568の認証候補B1と、スコアが569の認証候補B2とが抽出されていたとする。この場合において、認証候補B1の顔登録画像の識別情報がビーコンキャッチ情報と紐付けられていたとすると、認証部130は、認証候補B1のスコアである568に、例えば5を加算する。

[0097] これにより、認証候補B1のスコアが573となるので、複数の認証候補

の中で最も高いスコアとなる。その結果、認証部130は、認証候補B1に紐付けられた登録者として進入者を認証する。

[0098] また、スコア差が僅差である複数の認証候補の中で少なくとも2つの認証候補にビーコンキャッチ情報が紐付けられている場合、認証部130は、顔登録画像の登録日付に応じて、進入者の認証を行うようにしてもよい。

[0099] 顔登録画像の登録日付が古いほど、登録者の顔の特徴が変化している可能性があるため、顔登録画像の登録日付が新しい方を、認証候補として抽出することで、認証候補を抽出しやすくすることができる。

[0100] 以上のように構成された認証システム1における認証制御の動作例について説明する。まず、認証装置100における認証制御の動作例について説明する。図8は、認証装置100における認証制御の動作例を示すフローチャートである。図8における処理は、例えば、ゲート装置10の稼働中に適宜実行される。

[0101] 図8に示すように、認証装置100は、顔画像照合要求があったか否かについて判定する（ステップS401）。判定の結果、顔画像照合要求がない場合（ステップS401、NO）、ステップS401の処理が繰り返される。一方、顔画像照合要求がある場合（ステップS401、YES）、認証装置100は、顔画像情報を取得する（ステップS402）。

[0102] 次に、認証装置100は、3人の認証候補を抽出する（ステップS403）。なお、本フローチャートでは、認証式1以上となるスコアの認証候補がいることを前提としている。

[0103] 3人の認証候補を抽出したら、認証装置100は、スコアが最大である認証候補の第1スコアと、スコアが3番目である認証候補の第3スコアとの差分が閾値未満であるか否かについて判定する（ステップS404）。判定の結果、第1スコアと第3スコアとの差分が閾値未満である場合（ステップS404、YES）、処理はステップS406に遷移する。

[0104] 一方、第1スコアと第3スコアとの差分が閾値以上である場合（ステップS404、NO）、認証装置100は、第1スコアと、スコアが2番目であ

る認証候補の第2スコアとの差分が閾値未満であるか否かについて判定する（ステップS405）。判定の結果、第1スコアと第2スコアとの差分が閾値以上である場合（ステップS405、NO）、処理はステップS408に遷移する。

[0105] 一方、第1スコアと第2スコアとの差分が閾値未満である場合（ステップS405、YES）、認証装置100は、3人の認証候補の中にビーコンキャッチ情報の紐付けがある認証候補があるか否かについて判定する（ステップS406）。

[0106] 判定の結果、ビーコンキャッチ情報の紐付けがある認証候補がない場合（ステップS406、NO）、処理はステップS408に遷移する。一方、ビーコンキャッチ情報の紐付けがある認証候補がある場合（ステップS406、YES）、認証装置100は、当該認証候補のスコアに加算処理を実行する（ステップS407）。

[0107] そして、認証装置100は、最も高いスコアの認証候補で進入者を認証する（ステップS408）。その後、本制御は終了する。

[0108] このような構成によれば、スコア差が僅差となった場合に限り、ビーコンキャッチ情報の紐付けの有無を考慮するので、無駄な処理を省くことができる。また、携帯端末2の持ち主とは異なる進入者が当該携帯端末2を所持してゲート装置10を通過しようとする場合、ビーコンキャッチ情報が紐付けられる顔登録画像は、携帯端末2の持ち主であり、進入者のものに紐付けはなされない。そのため、進入者がゲート装置10に進入する際、進入者に係る顔登録画像のスコアに加算処理が施されることを抑制することができる。

[0109] また、スコア差が僅差である顔登録画像を、ビーコンキャッチ情報の紐付けによる加算処理により、正確な顔登録画像を選択して進入者を認証することができるので、認証の精度を向上させることができる。

[0110] また、閾値は、抽出された認証候補のスコアレベルに応じて変動させるようにしてもよい。例えば、スコアレベルが低い場合には、閾値の範囲を広げることが考えられる。スコアレベルが低い場合は、顔向きや照明、顔の隠蔽

状況等による影響により顔認証自体の精度が低下している可能性が高い。そのため、スコアレベルが低い場合には、精度の低下している顔認証単独に依存した判断を行うよりも、ビーコンキャッチ情報を併用した判断を行った方が正しい認証結果が得られる可能性が高い。ここで、本実施の形態では、スコアが僅差であると判定されるとビーコンキャッチ情報を併用した判断が行われるため、スコアレベルが低い場合に閾値の範囲を広げることによりビーコンキャッチ情報を併用した判断が発生し易くなるように制御することができる。なお、スコアレベルが高く、顔認証の精度が十分に信頼できる場合には、認証候補のスコア差が小さくとも正確な判断が行われている可能性が高い。そのため、ビーコンキャッチ情報を用いた加算処理を行うと、判断結果をかえって誤らせてしまうおそれがあるため、スコアレベルが高い場合には閾値の範囲を狭め、加算処理が発生しにくくなるようにしてもよい。

[0111] また、上記実施の形態では、ビーコン装置30が1つのゲート装置10に対応して1つ設けられていたが、本開示はこれに限定されない。例えば、複数のビーコン装置30が1つのゲート装置10に対応して設けられていてもよい。

[0112] 例えば、図9に示すゲート装置10には、4つのビーコン装置31, 32, 33, 34が設けられている。なお、図9におけるゲート装置10は、入口11と出口12とを有しており、図9では、入口11から出口12に向かう方向が、進入者のゲート装置10への入場方向であるとする。

[0113] 第1のビーコン装置31は、ゲート装置10の入口11よりも手前側（進入者の入場方向における上流側）に設けられている。第1のビーコン装置31は、ゲート装置10が配置される施設内の天井等に設けられている。

[0114] 第2のビーコン装置32は、ゲート装置10の入口11に対応する箇所に設けられている。第3のビーコン装置33は、ゲート装置10の出口12に対応する箇所に設けられている。つまり、第3のビーコン装置33は、ゲート装置10における、第2のビーコン装置32よりも、進入者の入場方向における下流側に設けられている。

- [0115] 第4のビーコン装置34は、ゲート装置10の出口12よりも奥側（進入者の入場方向における下流側）に設けられている。第4のビーコン装置34は、ゲート装置10は配置される施設内の天井等に設けられている。
- [0116] このような構成によれば、ゲート装置10付近を通行する通行人の進行方向を判断しやすくなるので、通行人が進入者に該当するか否かを見極めやすくすることができる。
- [0117] 例えば、各ビーコン装置31, 32, 33, 34から送信されるビーコン情報に基づくビーコンキャッチ情報の受信時刻に基づいて、認証部130が通行人の進行方向を判断しやすくなる。
- [0118] 具体的には、各ビーコン装置31, 32, 33, 34から送信されるビーコン情報が通行人の携帯端末2で受信して認証装置100がビーコンキャッチ情報を取得すると、認証装置100では、ビーコンキャッチ情報の第1受信時刻と、第2受信時刻と、第3受信時刻と、第4受信時刻とが記録される。
- [0119] 第1受信時刻は、第1のビーコン装置31に基づくビーコンキャッチ情報の受信時刻である。第2受信時刻は、第2のビーコン装置32に基づくビーコンキャッチ情報の受信時刻である。第3受信時刻は、第3のビーコン装置33に基づくビーコンキャッチ情報の受信時刻である。第4受信時刻は、第4のビーコン装置34に基づくビーコンキャッチ情報の受信時刻である。
- [0120] 通行人がゲート装置10へ入場する場合、例えば、第1受信時刻、第2受信時刻、第3受信時刻、第4受信時刻の順で認証装置100がビーコンキャッチ情報を取得するので、通行人が進入者であると推定することができる。
- [0121] また、通行人がゲート装置10に近づいたものの、ゲート装置10に入場せずに引き返したような場合、第1受信時刻、第2受信時刻のみ認証装置100がビーコンキャッチ情報を取得するのみとなるため、通行人が進入者ではないと推定することができる。
- [0122] すなわち、この構成では、複数の認証候補のうち、少なくとも2人の顔登録画像にビーコンキャッチ情報が紐付けられている場合、進入者と推定され

なかった顔登録画像に係る認証候補を除外しやすくなることができる。その結果、進入者の認証精度を向上させることができる。

[0123] また、この構成では、ビーコン装置のビーコン情報の送信範囲によっては、通行人がゲート装置10を通過しなくても、第1受信時刻から第4受信時刻のうちの複数の受信時刻が認証装置100に記録される可能性がある。

[0124] そのため、各ビーコン装置31、32、33、34から送信されるビーコン情報の電界強度を考慮して、認証装置100が進入者の推定を行ってもよい。

[0125] 例えば、通行人Cがゲート装置10における第1のビーコン装置31付近を通行したとする。この場合、認証装置100では、第1のビーコン装置31に係るビーコンキャッチ情報と、第2のビーコン装置32に係るビーコンキャッチ情報が記録される。

[0126] 第1のビーコン装置31は、第2のビーコン装置32よりも通行人Cに近い位置に位置するので、第1のビーコン装置31のビーコン情報の電界強度が、第2のビーコン装置32のビーコン情報の電界強度よりも大きくなる。そのため、通行人Cは、ゲート装置10に入場する前の位置に位置すると推定することができる。

[0127] また、通行人Cがゲート装置10の入口11に近づくと、第1のビーコン装置31から遠ざかる一方、第2のビーコン装置32に近づくこととなる。そのため、第2のビーコン装置32のビーコン情報の電界強度が、第1のビーコン装置31のビーコン情報の電界強度よりも大きくなる。そのため、通行人Cは、ゲート装置10により近い位置に位置し、ゲート装置10に近づいていると推定することができる。

[0128] また、通行人Cがゲート装置10内に入ると、認証装置100には、第2のビーコン装置32に係るビーコンキャッチ情報と、第3のビーコン装置33に係るビーコンキャッチ情報が少なくとも記録される。

[0129] ゲート装置10内に通行人Cが位置する場合、第2のビーコン装置32と第3のビーコン装置33との中間地点付近に通行人Cが位置することとなる

ので、各ビーコン情報の電界強度は近似した値となる。そのため、通行人Cは、ゲート装置10内に位置すると推定することができ、ひいては認証候補として抽出しやすくすることができる。

[0130] また、通行人Cがゲート装置10に近づいたものの引き返したような場合、第3のビーコン装置33に係るビーコンキャッチ情報は認証装置100に記録されない、または、ビーコン情報の電界強度が小さいものとなる。そのため、通行人Cは、ゲート装置10に進入する意思がないものと推定することができ、ひいては認証候補から除外しやすくすることができる。

[0131] また、通行人Cがゲート装置10を通過すると、第3のビーコン装置33から遠ざかる一方、第4のビーコン装置34に近づくこととなる。そのため、第4のビーコン装置34のビーコン情報の電界強度が、第3のビーコン装置33のビーコン情報の電界強度よりも大きくなる。そのため、通行人Cは、ゲート装置10を通過したと推定することができる。

[0132] これにより、通行人C（進入者）の位置を正確に推定することができるので、進入者の入退場記録を正確に管理することができる。

[0133] また、通行人Cの位置を正確に推定することにより、認証装置100による認証結果を例えば、通行人Cがゲート装置10を通過したことをもって確定するようにしてもよい。

[0134] 例えば、顔の類似した複数の通行人が同等のタイミングでゲート装置10に近づいて、1人の通行人（進入者）がゲート装置10を通過する一方、残りの通行人がゲート装置10を通過しない場合があったとする。

[0135] この場合、認証装置100では、複数の通行人の全てにおけるビーコンキャッチ情報が各顔登録画像に紐付けられるため、正確に認証候補を抽出できない可能性がある。

[0136] そのため、進入者がゲート装置10を通過していない時点では、認証装置100の認証結果を確定せずに、再度ビーコンキャッチ情報を認証装置100で取得するようにする。

[0137] このようにすることで、ゲート装置10を通過しない通行人の位置がゲ-

ト装置10の手前の位置に止まること、および、進入者がゲート装置10の奥側の位置に進行することが確認することが可能となる。その結果、認証装置100の認証結果を正確なものとしやすくすることができる。

- [0138] また、複数のビーコン装置が設けられる場合、携帯端末2におけるアプリケーションでは、所定の時間内に受信したビーコン情報をまとめてビーコンキャッチ情報として送信するようにしてもよい。所定の時間は、送信可能な情報の量や施設の運営時間等に基づいて任意に設定可能である。例えば、1日の営業時間が定められている一般的な施設の場合、日を跨いで顔認証を行うべき状況が発生する可能性は低いため、所定の時間は1日としてもよい。また、所定の時間は、各ビーコン装置の配置関係、通行人の移動速度等によって調整可能な時間であってもよい。
- [0139] また、携帯端末2は、ビーコンキャッチ情報を送信後、ビーコン情報の電界強度が規定値以上に变化した場合、再度、ビーコンキャッチ情報を送信するようにしてもよい。
- [0140] また、図9に示す構成では、複数のビーコン装置が進入者の進行方向に並んで設けられていた。しかし、複数のビーコン装置は、複数のゲート装置が並んで配置されている場合、その複数のゲート装置の並ぶ方向に並んで設けられていてもよい。
- [0141] 例えば、図10に示すように、複数のゲート装置10が進入者の進行方向に直交する方向に並んで設けられる場合、各ゲート装置10に対応して、ビーコン装置30がそれぞれ設けられている。ビーコン装置30は、例えばゲート装置10が配置される施設の天井部分に設けられている。
- [0142] この場合、各ビーコン装置30から送信されるビーコン情報の電界強度の違いにより、進入者がどのゲート装置10に進入しようとしているかを推定することが可能となる。
- [0143] 例えば、進入者D1が、図10における右から二番目のゲート装置10に進入する場合、ビーコン情報に係る電界強度は、図10における右から二番目のビーコン装置30のビーコン情報に係る電界強度が最も大きくなる。そ

のため、進入者D1が、図10における右から二番目のゲート装置10を通過すると推定することができる。

[0144] また、進入者D2が、図10における左から二番目のゲート装置10に進入する場合、ビーコン情報に係る電界強度は、図10における左から二番目のビーコン装置30のビーコン情報に係る電界強度が最も大きくなる。そのため、進入者D1が、図10における左から二番目のゲート装置10を通過すると推定することができる。

[0145] このように、進入者の通過するゲート装置を推定することにより、進入者の特定をしやすくすることができる。

[0146] また、上記実施の形態では、ビーコン情報に基づくビーコンキャッチ情報を認証装置100が取得していたが、本開示はこれに限定されず、進入者の登録情報が含まれる限り、ビーコンキャッチ情報以外の情報を認証装置が取得してもよい。

[0147] また、上記実施の形態では、複数の認証候補のうち、ビーコンキャッチ情報と紐付けられた顔登録画像が存在する場合、顔登録画像に係る認証候補のスコアに所定の加算処理を行っていたが、本開示はこれに限定されない。例えば、複数の認証候補のうち、ビーコンキャッチ情報と紐付けられた顔登録画像が存在する場合、当該顔登録画像に係る登録者で進入者を認証してもよい。

[0148] また、上記実施の形態では、認証部130は、スコアが認証閾値未満となる顔登録画像を、認証候補から除外し、スコアが認証閾値以上となる顔登録画像を認証候補とした上で、その認証候補に対してビーコンキャッチ情報を用いてスコアの加算処理を行うか否かを決定していた。しかし、スコアが認証閾値未満となる顔登録画像を認証候補から除外する処理は省略してもよい。すなわち、全ての顔登録画像を認証候補と見做し、スコアの加算処理を行う対象であるか否かを決定してもよい。

[0149] また、上記実施の形態では、開閉機能を持つゲート装置10を例として説明したが、これに限られるものではない。上記実施の形態の構成を、開閉機

能を持たないゲート装置に適用してもよい。開閉機能を持たないゲート装置の例としては、例えば、通行人の監視や記録を行うボール状のものなどが考えられる。

[0150] また、上記実施の形態では、受信部、処理部および認証部が認証装置に含まれる構成であったが、本開示はこれに限定されず、受信部、処理部および認証部が別々に設けられていてもよい。特に、顔認証の手法としては、単独の装置で一連の処理が完結する手法も多数の装置が協働して処理を行う手法も数多く知られているが、上記実施の形態の手法は、スコアに基づいて顔認証を行う方式であれば、そのスコアを算出する過程や構成を問わずに適用することができる。

[0151] また、上記実施の形態では、ビーコンキャッチ情報に対応する顔登録画像のスコアに加算処理を行っていたが、他の手法を用いてもよい。ゲート装置10に進入しようとするユーザーの顔画像情報とビーコンキャッチ情報に対応する顔登録画像との照合結果が、ユーザーの顔画像情報と他の顔登録画像との照合結果よりも優遇される（すなわち、ゲート装置10の通過が許可された人物として認証され易くなる）のであれば、その手法はスコアに加算には限定されない。例えば、ビーコンキャッチ情報に対応する顔登録画像との照合結果の評価においてのみ認証閾値を下げること等が考えられる。

[0152] また、上記実施の形態では、ユーザー管理サーバおよび通過履歴管理サーバが認証装置とは別に設けられていたが、本開示はこれに限定されず、ユーザー管理サーバおよび通過履歴管理サーバが認証装置に含まれていてもよい。

[0153] その他、上記実施の形態は、何れも本開示を実施するにあたっての具体化の一例を示したものに過ぎず、これらによって本開示の技術的範囲が限定的に解釈されてはならないものである。すなわち、本開示はその要旨、またはその主要な特徴から逸脱することなく、様々な形で実施することができる。

[0154] 2021年5月25日出願の特願2021-087546の日本出願に含まれる明細書、図面および要約書の開示内容は、すべて本願に援用される。

産業上の利用可能性

[0155] 本開示の認証装置は、顔認証に対応するゲート装置のメリットを享受しつつ、認証精度を高めることが可能な認証装置および認証システムとして有用である。

符号の説明

- [0156]
- 1 認証システム
 - 2 携帯端末
 - 10 ゲート装置
 - 20 撮像装置
 - 30 ビーコン装置
 - 40 ユーザー管理サーバ
 - 50 通過履歴管理サーバ
 - 100 認証装置
 - 110 受信部
 - 120 処理部
 - 130 認証部

請求の範囲

- [請求項1] ゲート装置への進入者の携帯端末が前記ゲート装置の近傍に存在する場合に、前記携帯端末に登録される前記ゲート装置への進入者の登録情報と、複数の顔登録画像のうちの1つとを紐付ける処理を行う処理部と、
- 前記進入者の顔画像情報と前記複数の顔登録画像との照合結果に基づいて前記進入者を認証する認証処理において、前記登録情報に紐付けられた顔登録画像と前記進入者の顔画像情報との照合結果を、前記登録情報に紐付けられていない顔登録画像と前記進入者の顔画像情報との照合結果よりも優遇する認証部と、を備える、
- 認証装置。
- [請求項2] 前記認証部は、前記進入者の顔画像情報と前記顔登録画像との照合結果を示す値であるスコアが所定の認証閾値よりも高い場合に、前記進入者が前記顔登録画像に対応する人物であると認証する、
- 請求項1に記載の認証装置。
- [請求項3] 前記認証部は、前記登録情報に紐付けられた顔登録画像と前記進入者の顔画像情報との照合結果を示すスコアに対して所定の加算処理を行うことで、前記登録情報に紐付けられた顔登録画像と前記進入者の顔画像情報との照合結果を優遇する、
- 請求項2に記載の認証装置。
- [請求項4] 前記認証部は、前記登録情報に紐付けられた顔登録画像と前記進入者の顔画像情報との照合結果を示すスコアに対する前記認証閾値を下げることで、前記登録情報と紐付けられた顔登録画像と前記進入者の顔画像情報との照合結果を優遇する、
- 請求項2に記載の認証装置。
- [請求項5] 前記認証部は、前記進入者の顔画像情報と前記複数の顔登録画像のそれぞれとの照合結果を示すスコアに応じて認証候補を抽出し、
- 前記登録情報に紐付けられた顔登録画像が前記認証候補に含まれて

いない場合、前記登録情報に紐付けられた顔登録画像と前記進入者の顔画像情報との照合結果を優遇せずに、前記認証処理を行う、

請求項 2 に記載の認証装置。

[請求項6]

前記認証部は、前記登録情報に紐付けられた顔登録画像と前記進入者の顔画像情報との照合結果を示すスコアと、前記登録情報に紐付けられていない顔登録画像と前記進入者の顔画像情報との照合結果を示すスコアとの差であるスコア差が所定の閾値以上である場合、前記登録情報に紐付けられた顔登録画像と前記進入者の顔画像情報との照合結果を優遇せずに、前記認証処理を行う、

請求項 2 に記載の認証装置。

[請求項7]

前記認証部は、前記スコアのレベルが低いほど前記所定の閾値を大きく設定する、請求項 6 に記載の認証装置。

[請求項8]

前記認証装置は、更に、前記複数の顔登録画像それぞれについて、前記登録情報に紐付けられた回数または頻度を記録する記録部を備え、

前記認証部は、前記回数または頻度に応じて、前記認証処理において照合結果を優遇する顔登録画像を決定する、

請求項 1 に記載の認証装置。

[請求項9]

前記記録部は、更に、前記登録情報を前記顔登録画像と紐付ける契機となったゲート装置の場所を記録し、

前記認証部は、前記進入者が進入しようとしているゲート装置の場所と同じ場所における前記回数または頻度に応じて、前記認証処理において照合結果を優遇する顔登録画像を決定する、

請求項 8 に記載の認証装置。

[請求項10]

前記処理部は、前記携帯端末が、前記ゲート装置に対応して設けられたビーコン装置からビーコン情報を受信したことに応じて、前記登録情報と前記複数の顔登録画像のうちの 1 つとを紐付ける処理を行う、請求項 1 に記載の認証装置。

- [請求項11] 前記登録情報は、前記携帯端末にインストールされる、認証システムのアプリケーションにおいて登録された前記進入者の登録番号であり、
- 前記複数の顔登録画像は、前記認証システムに登録された、前記ゲート装置が設置された施設への入退場が許可された人物の顔画像である、
- 請求項1に記載の認証装置。
- [請求項12] ゲート装置への進入者の携帯端末が前記ゲート装置の近傍に存在する場合に、前記携帯端末に登録される前記ゲート装置への進入者の登録情報と、複数の顔登録画像のうちの1つとを紐付ける処理を行い、
- 前記進入者の顔画像情報と前記複数の顔登録画像との照合結果に基づいて、前記進入者を認証する認証処理において、前記登録情報に紐付けられた顔登録画像と前記進入者の顔画像情報との照合結果を、前記登録情報に紐付けられていない顔登録画像と前記進入者の顔画像情報との照合結果よりも優遇する、
- 認証方法。
- [請求項13] 進入者が進入可能なゲート装置と、
- 前記ゲート装置に対応して設けられ、前記進入者の顔画像情報を撮像する撮像装置と、
- 前記ゲート装置に対応して設けられ、前記進入者が所持する携帯端末にビーコン情報を送信するビーコン装置と、
- 前記携帯端末が前記ビーコン情報を受信したことに応じて、前記携帯端末に登録される前記ゲート装置への進入者の登録情報と、複数の顔登録画像のうちの1つとを紐付け、
- 前記顔画像情報と前記複数の顔登録画像との照合結果に基づいて前記進入者を認証する認証処理において、前記登録情報に紐付けられた顔登録画像と前記進入者の顔画像情報との照合結果を、前記登録情報に紐付けられていない顔登録画像と前記進入者の顔画像情報との照合

結果よりも優遇する認証装置と、
を備える認証システム。

[請求項14] 前記認証装置は、前記登録情報に紐づけられた顔登録画像が複数ある場合、前記携帯端末における前記ビーコン情報の受信時刻に応じて、前記登録情報に紐づけられた顔登録画像が複数の顔登録画像から前記認証処理の対象となる認証候補を抽出する、

請求項13に記載の認証システム。

[請求項15] 前記認証装置は、前記登録情報に紐づけられた顔登録画像が複数ある場合、前記携帯端末における前記ビーコン情報の電界強度に応じて、前記登録情報に紐づけられた顔登録画像が複数の顔登録画像から前記認証処理の対象となる認証候補を抽出する、

請求項13に記載の認証システム。

[請求項16] 前記ビーコン装置は、複数設けられている、

請求項13に記載の認証システム。

[請求項17] 認証装置と共に用いられる携帯端末を制御するプログラムであって、

前記認証装置は、

前記携帯端末から送信される前記携帯端末の利用者を示す登録情報と、複数の顔登録画像のうちの1つとを紐付ける処理を行い、

ゲート装置への進入者の顔画像情報と前記複数の顔登録画像との照合結果に基づいて、前記進入者を認証する認証処理において、前記登録情報に紐付けられた顔登録画像と前記進入者の顔画像情報との照合結果を、前記登録情報に紐付けられていない顔登録画像と前記進入者の顔画像情報との照合結果よりも優遇し、

前記プログラムは、携帯端末のコンピューターに、ビーコン情報を受信した場合に、前記ビーコン情報と前記登録情報とを送信するよう制御する処理を実行させる、

プログラム。

[請求項18] 前記プログラムは、前記携帯端末のコンピューターに、
 所定の時間内に、複数のビーコン情報を受信した場合、前記複数の
 ビーコン情報を記憶する処理と、
 前記所定の時間が経過したときに、前記複数のビーコン情報をまと
 めて前記登録情報と共に送信するよう制御する処理と、を実行させる
 、
 請求項 17 に記載のプログラム。