

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号
特許第6929751号
(P6929751)

(45) 発行日 令和3年9月1日 (2021. 9. 1)

(24) 登録日 令和3年8月13日 (2021. 8. 13)

(51) Int. Cl.

F I

G O 6 T 7/00 (2017. 01)

H O 4 N 7/18 (2006. 01)

G O 6 T 7/254 (2017. 01)

G O 8 B 25/00 (2006. 01)

G O 6 T 7/00 5 1 O B

H O 4 N 7/18 K

H O 4 N 7/18 G

G O 6 T 7/00 6 6 O A

G O 6 T 7/254

請求項の数 17 外国語出願 (全 22 頁) 最終頁に続く

(21) 出願番号	特願2017-193998 (P2017-193998)	(73) 特許権者	502208205
(22) 出願日	平成29年10月4日 (2017. 10. 4)		アクシス アーバー
(65) 公開番号	特開2018-116681 (P2018-116681A)		スウェーデン国 2 2 3 6 9 ルンド,
(43) 公開日	平成30年7月26日 (2018. 7. 26)		グレンデン 1
審査請求日	令和2年10月5日 (2020. 10. 5)	(74) 代理人	110002077
(31) 優先権主張番号	16194411.1		園田・小林特許業務法人
(32) 優先日	平成28年10月18日 (2016. 10. 18)	(72) 発明者	ダニエルソン, ニクラス
(33) 優先権主張国・地域又は機関	欧州特許庁 (EP)		スウェーデン国 2 2 3 6 9 ルンド,
			エンダラヴェーゲン 1 4, シー/オー
			アクシス コミュニケーションズ ア
			ーバー
早期審査対象出願			
			最終頁に続く

(54) 【発明の名称】 画定された領域内で物体を追跡するための方法及びシステム

(57) 【特許請求の範囲】

【請求項 1】

人間を追跡するための方法であって、

画定された領域へのアクセスを要求するときに人間によって提示される認証情報を読むこと、及び、事前に登録された人間たちの認証情報を含むデータベース内の認証情報に、前記人間によって提示された前記認証情報をマッチングさせることによって、前記画定された領域に入る前記人間を特定すること、

特定された前記人間の識別プロファイルであって、前記人間の外見を表す一組の識別特性を含む識別プロファイルを、前記画定された領域内で追跡される人間たちのリスト内に登録すること、

前記画定された領域内の情景から画像データを受信すること、

受信した前記画像データ内で検出された物体の一組の識別特性を生成すること、

検出された前記物体の生成された前記一組の識別特性と、前記画定された領域内で追跡される人間たちの前記リスト内に登録された識別プロファイルの複数組の識別特性との間の相関に基づいて、信頼性スコアを計算すること、

検出された前記物体の生成された前記一組の識別特性との最も高い相関を表す前記信頼性スコアに対応する一組の識別特性を含む、前記画定された領域内で追跡される人間たちの前記リスト内の識別プロファイルを特定すること、及び

検出された前記物体の生成された前記一組の識別特性との前記最も高い相関を有する前記一組の識別特性を含む特定された前記識別プロファイルに対応する計算された前記信頼

性スコアが、第1の所定の閾値よりも大きいならば、検出された前記物体を、特定された前記識別プロファイルに紐づけることを含む、方法。

【請求項2】

検出された前記物体の生成された前記一組の識別特性との前記最も高い相関を有する前記一組の識別特性を含む特定された前記識別プロファイルに対応する計算された前記信頼性スコアが、前記第1の所定の閾値よりも小さいならば、警報が発令される、請求項1に記載の方法。

【請求項3】

事前に登録された人間たちの認証情報を含むデータベース内の認証情報に、前記画定された領域を離れる人間によって提示された認証情報をマッチングさせることによって、前記画定された領域を離れる前記人間を特定すること、及び

前記画定された領域内で追跡される人間たちの前記リストから、前記画定された領域を離れる前記人間の識別プロファイルを除去することを更に含む、請求項1または2に記載の方法。

【請求項4】

検出された物体が、前記画定された領域内で追跡される人間たちの前記リストからのある人間の識別プロファイルに紐づけられた最後の時間ポイント以来、所定の活動期間が経過したならば、前記画定された領域内で追跡される人間たちの前記リストから、前記人間の前記識別プロファイルを除去することを更に含む、請求項1から3のいずれか一項に記載の方法。

【請求項5】

人間を事前に登録して、

前記人間が前記画定された領域にアクセスすることを許可する認証情報であって、事前に登録された人間たちの認証情報を含む前記データベースに保存される認証情報、および

前記人間の外見を表す識別特性を含む識別プロファイルであって、前記画定された領域内で取得される画像データから前記人間が特定されることを可能にする識別プロファイル

を生成することをさらに含む、請求項1から4のいずれか一項に記載の方法。

【請求項6】

受信した前記画像データ内の検出された前記物体の生成された前記一組の識別特性との前記最も高い相関を有する前記一組の識別特性を含む特定された前記識別プロファイルに対応する計算された信頼性スコアが、第2の所定の閾値よりも小さいならば、前記紐づける動作は実行されず、前記方法が、

検出された前記物体の生成された前記一組の識別特性を、前記画定された領域に入った人間たちのリスト内に登録された識別プロファイルの複数組の識別特性と比較すること、

検出された前記物体の生成された前記一組の識別特性に最も良くマッチングする一組の識別特性を含む、前記画定された領域に入った人間たちの前記リスト内の識別プロファイルを特定すること、及び

受信した前記画像データ内の検出された前記物体を、検出された前記物体の生成された前記一組の識別特性に最も良くマッチングする前記一組の識別特性を含む特定された前記識別プロファイルに紐づけることを更に含む、請求項1から5のいずれか一項に記載の方法。

【請求項7】

検出された前記物体の生成された前記一組の識別特性と、前記画定された領域に入った人間たちの前記リスト内に登録された前記識別プロファイルの前記複数組の識別特性との前記比較が、検出された前記物体の生成された前記一組の識別特性と、前記画定された領域に入った人間たちの前記リスト内の前記人間たちの登録された前記識別プロファイルの前記複数組の識別特性との間の相関に基づいて、信頼性スコアを計算することによって実行され、

検出された前記物体の生成された前記一組の識別特性に最も良くマッチングする前記一組の識別特性を含む、前記画定された領域内に入った人間たちの前記リスト内の前記識別プロファイルの前記特定が、検出された前記物体の生成された前記一組の識別特性との最も高い相関を有する一組の識別特性を含む識別プロファイルを選択することによって実行される、請求項 6 に記載の方法。

【請求項 8】

人間の外見を表す前記一組の識別特性の中の情報が、人間の身体又は顔の特性の幾何学的形状のパラメータ、人間の顔の特徴又は身体の特徴を表す数学的な表現、人間の衣服、肌、又は顔のテクスチャパラメータ、人間又は人間の部分の画像からの色のスペクトル、人間の歩き方、人間の動きのパターンから成る群から選択される、請求項 1 から 7 のいずれか一項に記載の方法。

10

【請求項 9】

検出された前記物体の生成された前記一組の識別特性に最も良くマッチングする前記一組の識別特性を含む前記識別プロファイル内の情報を、検出された前記物体の生成された前記一組の識別特性からの情報によって更新することを更に含む、請求項 8 に記載の方法。

【請求項 10】

検出された前記物体の生成された前記一組の識別特性に最も良くマッチングする前記一組の識別特性を含む前記識別プロファイル内の前記情報を更新する動作が、検出された前記物体の生成された前記一組の識別特性に最も良くマッチングする前記一組の識別特性を含む前記識別プロファイル内の現在の情報と、検出された前記物体の生成された前記一組の識別特性からの情報とに基づいて、統計的測定値を計算することによって実行される、請求項 9 に記載の方法。

20

【請求項 11】

検出された前記物体を、検出された前記物体の前記一組の識別特性に最も良くマッチングする特定された前記識別プロファイルに紐づけるステップが、前記画像データを取得した画像取得装置の識別子、前記画像データが前記画像取得装置によって取得された時間内のポイント、及び前記画像データを取得した前記画像取得装置の位置の群から選択された、受信した前記画像データに関連する情報を登録することを更に含む、請求項 1 から 10 のいずれか一項に記載の方法。

30

【請求項 12】

プロセッサによって実行されたときに、請求項 1 から 11 のいずれか一項に記載の方法を実行するように適合された指示命令を有するコンピュータ可読記憶媒体。

【請求項 13】

人間を追跡するためのシステムであって、
事前に登録された人間たちの認証情報を保存するデータベースと、
画定された領域内で追跡される人間たちのリストを保存するメモリと、
前記画定された領域内の情景から画像データを取得する少なくとも 1 つのカメラと、
前記データベース、前記メモリ、及び前記少なくとも 1 つのカメラに通信可能に連結されたプロセッサと、
を備え、前記プロセッサは、

40

前記画定された領域へのアクセスを要求するときに特定の人間によって提示される認証情報を読むこと、及び、前記特定の人間によって提示された前記認証情報を前記データベース内の認証情報にマッチングすることによって、前記画定された領域に入る前記特定の人間を特定し、

前記特定の人間の外見を表す識別特性を含む前記特定の人間の識別プロファイルを、追跡される人間たちのリスト内に登録し、

前記少なくとも 1 つのカメラによって取得された画像データ内で検出された物体の一組の識別特性を生成し、

検出された前記物体の生成された前記一組の識別特性と、前記画定された領域内で追跡

50

される人間たちの前記リスト内に登録された識別プロファイルの複数組の識別特性との間の相関に基づいて、信頼性スコアを計算し、

検出された前記物体の生成された前記一組の識別特性との最も高い相関を表す前記信頼性スコアに対応する一組の識別特性を含む、前記画定された領域内で追跡される人間たちの前記リスト内の識別プロファイルを特定し、及び

検出された前記物体の生成された前記一組の識別特性との前記最も高い相関を有する前記一組の識別特性を含む特定された前記識別プロファイルに対応する計算された前記信頼性スコアが、第1の所定の閾値よりも大きいならば、検出された前記物体を、特定された前記識別プロファイルに紐づける、ように構成されている、システム。

【請求項14】

前記プロセッサが更に、前記特定の人間の識別プロファイルを、前記画定された領域に入った人間たちのリスト内に登録するように構成されており、前記画定された領域に入った人間たちの前記リスト内の前記特定の人間の前記識別プロファイルは、画像データから前記特定の人間を特定するための情報を含むものである、請求項13に記載のシステム。

【請求項15】

前記プロセッサが更に、検出された物体が、前記画定された領域に入った人間たちの前記リスト内の前記特定の人間の前記識別プロファイルに紐づけられた最後の時間ポイント以来、所定の活動期間が経過したならば、前記画定された領域内で追跡される人間たちの前記リストから前記特定の人間の識別プロファイルを登録解除するように構成されている、請求項14に記載のシステム。

【請求項16】

前記データベースに前記人間の前記外見を表す前記識別特性を含む前記識別プロファイルを事前に登録するために、前記人間の画像を取得するように構成されたカメラを備える事前登録モジュールを更に備える、請求項13から15のいずれか一項に記載のシステム。

【請求項17】

前記認証情報を読むことが更に、認証情報入力装置を用いて前記認証情報を読むことを含み、前記認証情報入力装置は、前記認証情報を提示することによって前記画定された領域へのアクセスを要求するために前記画定された領域に入る前記人間によって用いられる、請求項13から16のいずれか一項に記載のシステム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、監視の分野に関する。特に、本発明は、カメラによって監視された画定された領域内で物体を追跡するための方法及びシステムに関する。

【背景技術】

【0002】

物体追跡のためのシステムは、カメラ監視の分野において興味深い用途を有する。多くの監視システムでは、犯罪科学映像検索のためのライブ映像資料及び記録映像資料の両方において、物体又は特に人間を追跡することが望ましい。

【0003】

物体追跡システムは、人間の活動が、例えば、犯罪活動に関して調査される必要がある様々な安全に関する状況において助けとなる。しかし、物体追跡システムは、調査のために統計データを収集するなどの、安全とは関係ない用途に対しても有用であり得る。多くの物体追跡システムは、人間たちがアクセス認証情報を得るために事前に登録する、オフィスビル、工場、ホテル、ゲートッドコミュニティ (gated community)、キャンパス、又は施設などの、画定された領域を監視するカメラシステムに適用されている。

【0004】

(重なる視野を有し得るか又は有し得ない) 監視カメラのシステム内で物体を追跡する

10

20

30

40

50

ために、異なる複数の監視カメラからの画像データ内で、物体、又はその物体の少なくとも特徴を認識できることが重要である。異なる複数の監視カメラは、異なるレンズ、開口部、画像センサなどを備えた異なる光学配置、及び異なる画像処理設定を有し得るので、これは、システム内の異なる複数のカメラからの画像データ内の物体の外見に影響を与え得る。更に、複数のカメラは、異なる物理的位置に取り付けられ、例えば、これもまた、カメラによって取得され処理される画像データ内の物体の外見に影響を与える、異なる照明スキームを有する。これらの問題は、US 7,529,411 B2で説明されている。

【0005】

US 7,529,411 B2は、映像監視システムによって取得された画像から引き出された識別情報が、1以上の記憶されたプロファイルと比較される、映像の複数のストリームの認識解析のためのシステムを教示している。US 7,529,411 B2で開示されたシステムの好適な実施形態では、各記憶されたプロファイルとの比較がなされるが、その比較は記憶されたプロファイルの選択されたサブセットに対してのみ行われることが可能である。

【0006】

しかし、US 7,529,411 B2で説明されるシステムの問題は、認識解析が多くの処理能力と処理時間を必要とするということである。

【発明の概要】

【0007】

上述の観点から、それ故、本発明の目的は、画定された領域内で物体を追跡するための改良された方法及びシステムを提供することである。特に、画定された領域内で物体を追跡するために必要な処理時間及び処理性能を低減させる方法及びシステムを提供することが目的である。

【0008】

本発明の第1の態様によれば、上述の目的は、人間を追跡するための方法によって達成される。人間を追跡するための方法は、事前に登録された人間たちの認証情報を含むデータベース内の認証情報に、人間によって提示された認証情報をマッチングさせることによって、画定された領域に入るその人間を特定するステップ、特定された人間の識別プロファイルであって、画像データから人間を特定するための情報を含む、識別プロファイルを領域内で追跡される人間たちのリスト内に登録するステップ、領域内の情景から画像データを受信するステップ、受信した画像データ内で検出された物体の一組の識別特性を生成するステップ、検出された物体の生成された一組の識別特性を、領域内で追跡される人間たちのリスト内に登録された識別プロファイルと比較するステップ、検出された物体の一組の識別特性に最も良くマッチングする、領域内で追跡される人間たちのリスト内の識別プロファイルを判定するステップ、及び検出された物体を、検出された物体の識別プロファイルに最も良くマッチングすると判定された識別プロファイルに紐づけるステップを含む。人間を追跡するための本方法の利点は、画像データ内で検出された物体の識別特性が、領域内で現在追跡されている人間たちの識別プロファイルと比較されるので、画定された領域内で物体を追跡するために必要とされる処理時間が低減され、画像データから人間を正確に特定する信頼性が高められるということである。処理時間が低減される1つの理由は、より少ない識別プロファイルが、検出された物体の識別特性と比較される必要があるということである。信頼性が高まるのは、識別特性が複数の識別プロファイルと類似してマッチングする可能性が低減される結果である。この効果は、更に、より少ない識別プロファイルが比較されるのに伴って、類似する特徴を有する候補を有する可能性が低減されるので、マッチングの信頼性が高まるということである。すなわち、プロセスが画像内の人間を正確に特定することは、より少ないエントリを含むリストの結果として、比較する人間の低減されたリスト内の識別プロファイルの間のより大きな差異のために、より容易になるであろうとすることができる。このやり方で、マッチングは、及び、それ故、追跡方法の最も処理が大変なステップのうちの1つは、最も可能性が高い候補に集中し、必ずしも全ての理論的に可能性がある候補に集中しないだろう。画定された領域に入ると特

10

20

30

40

50

定された人間たちの識別プロファイルが、領域内で追跡される人間たちのリストに登録されること、及び、識別プロファイルが、領域に入るときに特定のために使用される認証情報に紐づけられることは、更なる利点である。このやり方で、物理的アクセスシステムの信頼性は、領域内で追跡される人間たちのリストの識別プロファイルの登録における高い信頼性を実現する可能性を高めている。識別プロファイルの登録は、画定された領域に入る人間に紐づけられて実行され、それは、領域に入る人間に対応し得る物体が受信した画像内で検出される前に、追跡される人間たちのリストを作成するという利点を与える。これは、受信した画像内で各検出される物体に対して必要とされる処理時間及び処理性能を低減させる。

【0009】

10

本発明の更なる実施形態では、生成された一組の識別特性を登録された識別プロファイルと比較するステップが、生成された識別特性と登録された識別プロファイルとの間の相関に基づいて信頼性スコアを計算することによって実行され、生成された一組の識別特性に最も良くマッチングする識別プロファイルを判定するステップが、生成された一組の識別特性との最も高い相関を表す信頼性スコアに対応する識別プロファイルを選択することによって実行される。最も高い相関を判定するために信頼性スコアを使用することの利点は、それが、相関を処理効率に優れたやり方で定量化するという点である。

【0010】

本発明のまた更なる実施形態では、検出された物体の一組の識別特性に対して最も高い相関を有する識別プロファイルに対応する計算された信頼性スコアが、第1の所定の閾値よりも小さいならば、紐づけの動作は実行されない。これは、乏しい相関が最も良い相関である場合を取捨選択し、乏しい相関が追跡に影響を与えることを妨げることを可能にする。

20

【0011】

他の実施形態では、検出された物体の一組の識別特性に対して最も高い相関を有する識別プロファイルに対応する計算された信頼性スコアが、第1の所定の閾値よりも小さいならば、警報を発令するように更に開発される。乏しいマッチングは、検出された侵入者によるものであり得る。侵入者は、有効な認証情報を使用する適正な特定なしに画定された領域に入っており、したがって、領域内で追跡される人間たちのリストの部分ではなく、警報を発令することは、画定された領域の安全性を高める。

30

【0012】

更なる実施形態では、人間によって提示された認証情報を、事前に登録された人間たちの認証情報を含むデータベース内の認証情報とマッチングさせることによって、画定された領域を離れる人間を特定する更なるステップ、及び領域内で追跡される人間たちのリストから画定された領域を離れる特定された人間の識別プロファイルを除去する更なるステップが導入される。これらの実施形態は、領域内で追跡される人間たちのリストを更新し続けることを追加し、画定された領域を離れる人間を除去することは、候補のリストを低減させ、したがって、処理時間を低減させ、同時に、追跡の信頼性を高める。

【0013】

また更なる実施形態では、検出された物体が識別プロファイルに紐づけられた時間内の最後のポイント以来、所定の活動期間が経過したならば、領域内で追跡される人間たちのリストから、人間の識別プロファイルが除去される。これらの実施形態は、代替的に又は前述した事と組み合わせられて、領域内で追跡される人間たちのリストを更新し続けることを追加する。これらの実施形態は、候補のリストを低減させ、したがって、処理時間を低減させる。

40

【0014】

更なる実施形態では、領域に入った人間たちのリスト内に特定された人間の識別プロファイルを登録するステップが、該方法に追加される。領域に入った人間たちを含む別のリストの追加は、追跡方法が使用されたときに大多数の場合、処理時間及び処理リソースが低減され得るという点で有利である。それは、最も可能性が高い候補のみが領域内で追跡

50

される人間たちのリストに載っているからである。しかし、最も可能性が高い候補の1人が優れた十分な相関を有するマッチングを生成しない稀な場合、領域に入った人間たちのリストは、識別特性を、領域に入ったが最近の時間において検出された物体に紐づけられなかった人間たちの識別プロファイルと比較する可能性も提供する。

【0015】

以下の事が、本発明のまた更なる実施形態でも更に開発される。すなわち、受信した画像データ内の検出された物体の一組の識別特性に対して最も高い相関を有する識別プロファイルに対応する計算された信頼性スコアが第2の所定の閾値よりも小さいならば、紐づけの動作は実行されない。該方法は、更に、受信した画像データ内の検出された物体の生成された一組の識別特性を、領域に入った人間たちのリスト内に登録された識別プロファイルと比較すること、受信した画像データ内の検出された物体の一組の識別特性に最も良くマッチングする領域に入った人間たちのリスト内の識別プロファイルを判定すること、及び受信した画像データ内の検出された物体を、受信した画像データ内の検出された物体の一組の識別特性に最も良くマッチングすると判定された識別プロファイルに紐づけることを含んでいる。

【0016】

これは、領域内で追跡される人間たちのリストからの候補との最も高い相関を有するマッチングの信頼性スコアが、十分でなければ、領域に入った人間たちのリスト内の候補とマッチングする可能性を提供する。これは、更に、システムの信頼性を高める。

【0017】

更なる実施形態では、受信した画像データ内の検出された物体の生成された一組の識別特性と、領域に入った人間たちのリスト内に登録された識別プロファイルとの比較が、受信した画像データ内の検出された物体の生成された一組の識別特性と、領域に入った人間たちのリスト内の人間たちの識別プロファイルとの間の相関に基づいて、信頼性スコアを計算することによって実行され、及び、生成された一組の識別特性に最も良くマッチングする領域内に入った人間たちのリスト内の識別プロファイルの判定が、受信した画像データ内の検出された物体の生成された一組の識別特性との最も高い相関を表す信頼性スコアに対応する識別プロファイルを選択することによって実行される。最も高い相関を判定するために信頼性スコアを使用することの利点は、それが、処理効率に優れたやり方で相関を定量化するという点である。

【0018】

本発明の更に他の実施形態では、識別プロファイルが、人間の外見を表す1以上の組の識別特性を含む。それらの識別特性は、人間の身体又は顔の特性の幾何学的形状のパラメータ、人間の顔の特徴又は身体の特徴を表す数学的な表現、人間の衣服、肌、又は顔のテクスチャパラメータ、人間又は人間の部分の画像からの色のスペクトル、人間の歩き方、人間の動きのパターンから成る群から選択される。人間の外見を表すための識別特性は、追跡するための方法の処理の効率性と信頼性を更に高める。何故ならば、それは、外見の特徴を計算及び処理するやり方を提供するからである。

【0019】

別の一実施形態では、検出された物体の一組の識別特性に最も良くマッチングする識別プロファイル内の情報が、生成された一組の識別特性からの情報によって更新される。これは識別特性を連続的に更新するという利点を提供し、人間の視覚的外見は短期間で容易に修正され得るので、それは追跡の信頼性のために重要である。例えば、人間がコートを脱いだならば衣服は変更され、メガネを掛ける又は掛けない、髭を剃ったなどである。

【0020】

更に他の実施形態では、識別プロファイル内の情報を更新する動作は、識別プロファイル内の現在の情報と生成された一組の識別特性からの情報とに基づいて、統計的測定値を計算することによって実行される。これは、識別プロファイルを更新する処理効率が高いやり方を更に追加する。

【0021】

本発明のまた更なる実施形態では、検出された物体を、検出された物体の一組の識別特性に最も良くマッチングすると判定された識別プロファイルに紐づけるステップが、更に、画像データを取得した画像取得装置の識別子、画像データが画像取得装置によって取得された時間内のポイント、及び画像データを取得した画像取得装置の位置、の群から選択された画像データに関連する情報を登録することを含む。これは、物体検出の、位置、画像取得装置、及び/又は時間内のポイントに関する更なる情報を有するという利点を追加する。それは、正確な特定を行う信頼性、したがって、画定された領域内の物体追跡能力を高める。

【0022】

第2の態様によれば、本発明は、プロセッサによって実行されたときに、本発明の第1の態様との関連で説明された方法を実行するように適合された指示命令を有する、コンピュータ可読記憶媒体を備えたコンピュータプログラム製品に関する。本発明の第1の態様に対応する利点が、本発明の第2の態様に対しても適用可能である。

【0023】

第3の態様によれば、本発明は、以下のものを備えた、人間を追跡するためのシステムに関する。すなわち、事前に登録された人間たちの認証情報を含むデータベース内の認証情報に、その人間によって提示された認証情報をマッチングさせることによって、画定された領域に入る人間を特定するように構成された識別モジュールであって、人間の識別プロファイルであって、その人間を特定するための情報を含む、識別プロファイルを領域内で追跡される人間たちのリスト内に登録するように構成された登録モジュール、領域内の情景から画像データを取得するように構成された画像取得装置、画像取得装置によって取得された画像データ内で検出された物体の一組の識別特性を生成するように構成された識別特性生成モジュール、検出された物体の生成された一組の識別特性を、領域内で追跡される人間たちのリスト内に登録された識別プロファイルと比較し、検出された物体の一組の識別特性に最も良くマッチングする、領域内で追跡される人間たちのリスト内の識別プロファイルを判定するように構成されたマッチングモジュール、及び、検出された物体を、検出された物体の識別プロファイルに最も良くマッチングすると判定された識別プロファイルに紐づけるように構成された追跡モジュールである。本発明の第1の態様に対応する利点が、本発明の第3の態様に対しても適用可能である。

【0024】

第3の態様の更なる実施形態によれば、該システムは、更に、人間の識別プロファイルであって、画像データからその人間を特定するための情報を含む、識別プロファイルを領域に入った人間たちのリスト内に登録するように構成されたエントランス登録モジュールと、検出された物体が識別プロファイルに紐づけられた時間内の最後のポイント以来、所定の活動期間が経過したならば、領域内で追跡される人間たちのリストからその人間の識別プロファイルを登録解除するように構成された登録解除モジュールと、画像データ内の検出された物体の生成された一組の識別特性を、領域内の追跡される人間たちのリスト内に登録された識別プロファイルと比較し、画像データ内の検出された物体の一組の識別特性に最も良くマッチングする、領域内の追跡される人間たちのリスト内の識別プロファイルを判定するように構成されたマッチングモジュールとを備える。

【0025】

本発明の適用性の更なる範囲は、以下の詳細な説明から明らかになるだろう。しかし、当業者にとっては、本発明の範囲内の様々な変更及び修正がこの詳細な説明より明らかになるため、詳細な説明及び具体例は、本発明の好適な実施形態を示しながらも、例示的な形でのみ提示されることを理解されたい。したがって、記載のデバイス及び記載の方法は異なる場合があるため、この発明は、記載のデバイスの特定のコンポーネント部品又は記載の方法のステップに限定されないことを理解されたい。本明細書で使用される用語は、特定の実施形態を説明する目的のためにすぎず、限定的であることを意図しないことを更に理解されたい。明細書及び添付の特許請求の範囲で使用されるように、冠詞(「a」、「an」、「the」、及び「said」)は、文脈によって他のことが明らかに示され

10

20

30

40

50

ない限り、一又は複数の要素があることを意味していると意図されることに留意されたい。したがって、例えば、「センサ」(a s e n s o r)又は「前記センサ」(t h e s e n s o r)に言及した場合、これは幾つかのセンサなどを含んでもよい。更に、「含む(c o m p r i s i n g)」という用語は、他の要素又はステップを除外しない。

【 0 0 2 6 】

本発明の他の特徴及び利点は、添付の特許請求の範囲を参照して、現在の好適な実施形態の以下の詳細な説明から明らかになるであろう。

【図面の簡単な説明】

【 0 0 2 7 】

【図 1】画定された領域 1 0 1 の一例を示す。

10

【図 2】本発明による、物体を追跡するための方法のブロックスキームである。

【図 3】本発明による、物体を追跡するための代替的な方法のブロックスキームである。

【図 4】本発明による、物体を追跡するためのシステムのブロック図である。

【図 5】本発明による、物体を追跡するための代替的なシステムのブロック図である。

【発明を実施するための形態】

【 0 0 2 8 】

更に、図面では、同様の参照文字が、幾つかの図面を通して同様の部分又は対応する部分を指定する。

【 0 0 2 9 】

本発明の一実施形態による追跡方法及びシステムは、人間たちがアクセス認証情報を得るために事前に登録する、オフィスビル、工場、ホテル、ゲーテッドコミュニティ、キャンパス、又は施設などの、画定された領域を監視するカメラシステムに適用され得る。この詳細な説明では、画定された領域が、それに対してエントランスが物理的アクセス制御システムによって制御されるところの領域である。

20

【 0 0 3 0 】

当該技術分野で知られている物体を追跡するための種々のアプローチが存在し、それらのうちの 1 つは、対象物体を検出すること、及び、対象物体の特徴を記憶された候補物体の特徴とマッチングさせてベストマッチを見つけることに基づき、それらは、追跡方法の重要なステップである。画定された領域に対する候補物体の数は、多くてもよい。画定された領域が工場である実施例では、無論、人々が工場内で働いており、例えば、幾つかのチームがシフトで働いているかもしれない。人々は、工場へ物品を搬送し、工場から製品を搬送するための輸送員であり、一時的な訪問者であり、様々なサービス員であり、警備員などである。そのような上述の実施例では、画定された領域内の候補物体の数が多いという事実に加えて、特定の期間内において、特に、領域内で同時に存在する対象物体の数が多いかもしれない。何処で何時、工場内で同時に存在する物体の数がより多いかという一例は、1 つのチームの作業者たちがシフトを終了し、別の 1 つのチームの作業者たちが彼らのシフトを開始している工場内である。したがって、画定された領域を監視するカメラに接続された追跡システムは、多くの数の候補物体と多くの数の同時に存在する対象物体の両方を取り扱えることが必要である。多くの数の候補物体は、各検出された対象物体に対して沢山の処理が必要とされることを意味し、多くの数の検出された対象物体は、この処理が頻繁に実行されることを必要とすることを意味する。

30

40

【 0 0 3 1 】

本発明の一実施形態によるシステムの一実施例は、図 1 に描かれている。画定された領域 1 0 1 は、物理的アクセスコントローラ 1 0 3 a、1 0 3 b によって制御される、エントランス 1 0 2 a、1 0 2 b を通してアクセスされる。物理的アクセスコントローラ 1 0 3 a、1 0 3 b は、画定された領域 1 0 1 へのアクセスを要求する人間によって提示された認証情報を、事前に登録された人間たちの認証情報を含むデータベース内の認証情報にマッチングさせることによって、画定された領域への物理的アクセスを制御するように適合された、物理的アクセス制御システムの部分である。そのような物理的アクセス制御システムは、工場、オフィス、学校、研究所、ホテルなどで使用され得る。そこでは、特定

50

の領域へのアクセスが、事前に登録された人間たちの特定の群に制限されている。認証情報データベースの記憶と更に認証情報のマッチングとは、アクセスコントローラ 103 a、103 b で、又はアクセスコントローラ 103 a、103 b に接続されたサーバ 109 a において、局所的に取り扱われ得る。図 1 では、サーバ 109 a が、画定された領域 101 の外側であるが画定された領域 101 に連結された破線を有する筐体内に配置されている。サーバ 109 a のこの表現の目的は、サーバが、画定された領域 101 内に又は画定された領域の外側に物理的に配置され得ることを示すことである。サーバ 109 a が、画定された領域 101 の外側に配置されている場合には、それが、ネットワークを通じてアクセスコントローラ 103 a、103 b に接続され得る。アクセスコントローラ 103 a、103 b は、画定された領域へのアクセスを要求する人間が認証情報を提示するための、認証情報入力装置 104 a、104 b、例えば、キーパッド、生体測定スキャナ、又は光学的、磁氣的、若しくは無線周波数プロトコルのリーダ装置、又は類似の装置に接続されている。例えば、生体測定スキャナは、指紋、虹彩、網膜、又は顔をスキャンし得る。物理的アクセスコントローラ 103 a、103 b は、例えば、人々が彼らの認証情報を提示することなしに画定された領域 101 へ入ることを妨げるために通路内に配置され得る、ドア、エレベーター、門、回転ドア、スライドドア、又は別の移動可能なブロッキング装置を介する、画定された領域 101 への入場を支配するロック機構に接続されている。提示された認証情報が認証情報データベース内の認証情報とのマッチングに成功したことに応じて、及び様々なアクセスの規則に応じて、人間は画定された領域へのアクセスが与えられ得る。例えば、アクセス規則は、事前に登録された人間たちにアクセスが許される期間を規制し得る。

【0032】

エントランス 102 b は、登録領域 105 と繋がるように配置され得る。そこでは、画定された領域 101 へのアクセスを要求しようとしている人間が、画定された領域 101 へのアクセスのための認証情報を得るために事前に登録し得る。

【0033】

カメラ 106 は、事前登録のための人間の画像を取得するために使用され得る。取得された画像は、画像データから人間を特定するための情報を含む識別プロファイル編集するために使用され得る。識別プロファイルは、人間の外見を表現するための 1 以上の組の識別特性を含む。識別特性の例は、人間の身体又は顔の特性の幾何学的形状のパラメータ、人間の顔の特徴又は身体の特徴を表す数学的な表現、人間の衣服、肌、又は顔のテクスチャパラメータ、人間又は人間の部分の画像からの色のスペクトル、人間の歩き方、人間の動きのパターンである。人間の外見を表現するための識別特性に加えて、識別プロファイルは、人間の他の記述子、例えば、画定された領域内での人間の事前に決定された位置、又は人間によって運ばれる様々な携帯装置から送信される識別子も含み得る。識別プロファイルの編集は、事前登録プロセスの部分であっても又はなくてもよい。代替的に、識別プロファイルは、人間が画定された領域 101 に入った後で、画定された領域 101 を監視するカメラ 107 a ~ f からの画像データを使用して編集され得る。識別プロファイル内で使用される画像データは、部分的に事前登録の間に、部分的に画定された領域 101 内でも収集され得る。更に別の代替例は、別の監視システムなどの別のソースからの識別プロファイルを編集するために使用され得る、識別プロファイル又はデータをインポートする。

【0034】

識別プロファイルは、更に、画定された領域 101 を監視するカメラ 107 a ~ f からの画像データを用いて連続的に更新され得る。識別プロファイルを連続的に更新することは、有益であり得る。何故ならば、人間の外見に関するデータの少なくとも一部は、例えば、衣服、メガネ、髪型などのように、経時的に変化し得るからである。

【0035】

事前登録は、上述の登録領域 105 とは異なる他の場所で実行され得る。例えば、事前登録は、画定された領域 101 から遠隔に配置された他の登録領域で実行され得る。指定

10

20

30

40

50

された登録領域は、画定された領域へのアクセスを要求することが、画定された領域 101 へのアクセスを制御する物理的アクセス制御システムの認証情報データベースの中へ送信され、及び、挿入され得るときに、その認証情報が使用される限りにおいて、必要でさえないかもしれない。

【0036】

第2の画定された領域 108 も、画定された領域 101 の内側に配置され得る。それによって、人間は、まず、第2の画定された領域 108 に入る前に、画定された領域 101 へのアクセスを要求することが必要である。アクセス規則は、物理的アクセス制御システム内で規定され得る。それによって、画定された領域 101 の第1の部分へのアクセスを有する全ての人間たちは、第2の画定された領域 108 へもアクセスすることができる。アクセス規則は、代替的に、画定された領域 101 の第1の部分へ入ることができる人間のサブグループが、第2の画定された領域 108 に入ることができるようにも構成され得る。第2の画定された領域 108 は、物理的アクセスコントローラ 103c によって制御される、エントランス 102c を通してアクセスされる。物理的アクセスコントローラ 103c は、画定された領域へのアクセスを要求する人間によって提示された認証情報を、事前に登録された人間の認証情報を含むデータベース内の認証情報にマッチングさせることによって、画定された領域への物理的アクセスを制御するように適合された、物理的アクセス制御システムの部分である。認証情報データベースの記憶と更に認証情報のマッチングとは、アクセスコントローラ 103c で、又はアクセスコントローラ 103a、103b に関しては、アクセスコントローラに接続されたサーバにおいて、局所的に取り扱われ得る。アクセスコントローラ 103c は、以前に認証情報入力装置 104a ~ b に対して説明されたものと同様に、認証情報入力装置 104c にも接続されている。

【0037】

複数の監視カメラ 107a ~ f は、画定された領域 101 を監視している。監視カメラ 107a ~ f は、画定された領域 101 の第1の部分へのエントランス 102a ~ b と、更に、画定された領域 101 の内側に配置された第2の画定された領域 108 へのエントランス、更に、画定された領域内の他の領域へのエントランスも監視し得る。監視カメラ 107a ~ f は、画像データを記憶し、処理し、及び管理するためのサーバ 109b も含み得る、監視システムに接続されている。監視システムは、監視カメラ 107a ~ f の近くで働く局所的計算装置も含み得る。監視システムに接続された装置は、ネットワークを介して通信し、ネットワークは、有線又は無線データ通信ネットワーク、例えば、ローカルエリアネットワーク (LAN) 又は無線ローカルエリアネットワーク (WLAN) 又はワイドエリアネットワーク (WAN) などの、任意の種類の通信ネットワークであり得る。監視カメラ 107a ~ f は、画像シーケンスを生成することができる任意のデジタルビデオカメラ及び/又は画像シーケンスを生成することができる任意のアナログビデオカメラであり得る。監視カメラがアナログビデオカメラである場合、アナログビデオカメラは、アナログ画像情報をデジタル画像データに変換し、デジタル画像データをネットワーク 20 に提供する、コンバータに接続されている。そのようなコンバータは、ビデオエンコーダ又はビデオサーバであり得る。図1では、サーバ 109b が、画定された領域 101 の外側であるが画定された領域 101 に連結された破線を有する筐体内に配置されている。サーバ 109b のこの表現の目的は、上述したように、サーバが、画定された領域 101 内に又は画定された領域の外側に物理的に配置され得ることを示すことである。サーバ 109b が、画定された領域 101 の外側に配置されている場合には、それが、ネットワークを通じて監視カメラ 107a ~ f に接続され得る。代替的に、監視カメラ 107a ~ f は、局所的に又は監視カメラ 107a ~ f の近くで働く局所的な計算装置によって、画像データの記憶、処理、及び管理を取り扱うように装備され得る。監視システムは、記憶された識別プロファイルを取り扱い、監視カメラによって取得された画像データ内の物体の物体追跡を管理する。監視システムは、物理的アクセス制御システムに接続されている。サーバ 109a と 109b は、図1では、分離したユニットとして描かれているが、サーバ 109a と 109b の機能は、無論、1つの物理的サーバユニットで組み合わせられ

得る。

【 0 0 3 8 】

次に、図 2 を参照すると、図 1 で描かれたものなどの、画定された領域 1 0 1 内の人間を追跡するための方法が描かれている。方法は、画定された領域に入る人間を特定することによって開始する（ステップ 2 0 2）。特定は、人間によってシステムに提示された認証情報を、事前に登録された人間の認証情報を含むデータベース内の認証情報とマッチングさせることによって実行される。ステップ 2 0 2 は、図 1 との関連で説明された、例えば、人間によって提示された認証情報を読むための認証情報入力装置 1 0 4 と、提示された認証情報を事前に登録された人間の認証情報を含むデータベース内の認証情報にマッチングさせるアクセスコントローラ 1 0 3 とを備えた、物理的アクセス制御システムによって実行され得る。しかし、アクセスコントローラ 1 0 3 は、代替例として、提示された認証情報を中央サーバ 1 0 9 a に送信し、提示された認証情報の事前に登録された人間の認証情報とのマッチングを実行することができる。

10

【 0 0 3 9 】

画定された領域 1 0 1 に入る人間を特定するステップ 2 0 2 の後で、特定された人間の識別プロファイルが、領域 4 0 5 内で追跡される人間たちのリスト内に登録される（ステップ 2 0 4）。ステップ 2 0 4 を実行するための様々な代替例が存在する。特定された人間の識別プロファイルが、監視システムのために利用可能であるならば、その識別プロファイルは、「追跡される」又はそれと類似のものとしてラベルを付けられ得る。問題の識別プロファイルに対するポインターは、代替的に、領域 4 0 5 内で追跡される人間のリストから生成され得る。無論、識別プロファイルも、領域 4 0 5 内で追跡される人間たちのリストのための指定されたメモリに対して複製され得る。特定された人間の識別プロファイルが、監視システムのために利用可能でないならば、新しい識別プロファイルが、画定された領域 1 0 1 を監視する監視カメラ 1 0 7 によって取得された画像データから生成され得る。一実施例として、画定された領域 1 0 1 に対するエントランス 1 0 2 a を監視する監視カメラ 1 0 7 c は、そこから特定された人間の外見を表すための識別特性が引き出され、識別プロファイル内に登録され得るところの、画像データを取得するために使用され得る。画定された領域 1 0 1 へのエントランス 1 0 2 a を監視する監視カメラ 1 0 7 c によって取得された画像データは、特定された人間の現在の外見を表す識別特性を用いて利用可能な識別プロファイルを更新するためにも有用であり得る。識別プロファイルを更新するために画定された領域 1 0 1 へのエントランス 1 0 2 a を監視する監視カメラ 1 0 7 c によって取得された画像データを使用することの利点は、それが、認証情報を提示しマッチングさせることによって人間が特定されたときに、又はその直後に、実行されることであり、それは、十分な信頼性を伴ってその人間を画定された領域へ入れるために、その人間の確実な特定が行われたことを意味する。例えば、人間が、人間の外見を変える、新しい髪型、新しいメガネ、又は単に新しい衣服を有しているならば、識別プロファイルは、人間の特定が提示された認証情報から知られる、システム内のポイントにおいて、この外見に対して適合され得る。

20

30

【 0 0 4 0 】

その後、追跡方法は、領域内の情景から、画像データを受信する（ステップ 2 0 6）ことによって続けられる。受信された画像データは、画定された領域 1 0 1 を監視する監視カメラ 1 0 7 の何れかによって取得される。物体は、当該技術分野で知られている任意の物体検出アルゴリズムによって、受信された画像データ内で検出され得る。例えば、動いている物体は、運動検出アルゴリズムによって検出され得る。運動検出アルゴリズムのある実施例は、ビデオフレームを比較して、ビデオフレームの間の変化を検出する変化検出アルゴリズム、動いている最前面の物体を引き出す監視された情景の背景モデルを使用するアルゴリズム、A 1 m b 1 a d h による U S 8 , 1 2 1 , 4 2 4 内で説明されるものなどの時空間的アルゴリズム、又はそれらの任意の組み合わせである。それらの運動によって物体を検出するための代替例は、形状検出を使用して、それらの視覚的特徴によって物体を検出する。様々な種類のそのような物体検出方法が当該技術分野で知られている。例

40

50

えば、Viola, Paul, and Michael Jones, 「Rapid object detection using a boosted cascade of simple features.」Computer Vision and Pattern Recognition, 2001. CVPR 2001. Proceedings of 2001. IEEE Computer Society Conference on. Vol. 1. IEEE, 2001で説明されるように、物体を検出するために識別子のカスケードが使用される。これらのアルゴリズムにとって重要なのは、視覚的特徴なので、類似する視覚的特徴を共有する物体の群が検出され得る。そのような群の例は、顔、輸送体、人間などである。これらの方法の何れかが、分離して又は組み合わせられて使用され、画像データ内の物体を検出し得る。幾つかの物体は、同じ組の画像データ内でも検出され得る。物体検出は、画像データを取得した監視カメラ、又は画像データを取得した監視カメラからの画像データを受信した別の監視カメラの何れかによって、監視カメラ107において実行され得る。代替的に、物体検出は、監視システム内の監視カメラ107に接続されたサーバ109bにおいて、又は監視カメラ107の近くで働く局所的計算装置において実行され得る。

【0041】

物体が画像データ内で検出されたときに、検出された物体の視覚的外見を表す、一組の識別特性が生成される(ステップ208)。画定された領域101を監視する1以上の監視カメラ107によって取得された単一の画像フレーム又はビデオシーケンスからの画像データが使用されて、検出された物体の識別特性を生成し得る。様々な画像及び/又はビデオ解析アルゴリズムが使用されて、画像データから識別特性を引き出し生成し得る。そのような画像又はビデオ解析アルゴリズムの実施例は、例えば、Turk, Matthew A., and Alex P. Pentland, 「Face recognition using eigenfaces.」Computer Vision and Pattern Recognition, 1991. Proceedings CVPR '91., IEEE Computer Society Conference on. IEEE, 1991., gait features such in Lee, Lily, and W. Eric L. Grimson. 「Gait analysis for recognition and classification.」Automatic Face and Gesture Recognition, 2002. Proceedings. Fifth IEEE International Conference on. IEEE, 2002., or colors such in US 8,472,714 by Brogren et al.などの、顔の特徴を引き出すための様々なアルゴリズムである。

【0042】

識別特性は、画像データを取得した監視カメラ、監視システム内の別の監視カメラ、カメラの近くで働く局所的な計算ユニット、又は監視カメラに接続されたサーバ109bにおいて生成され得る。識別特性の生成は、受信した画像データ内で物体が検出されたことに応じて行われる。物体がシステムの一部内で検出され、識別特性の生成がシステムの別の部分で実行されるならば、画像データ内の検出された物体を表すデータは、物体を検出した部分から識別特性を生成する部分へ送信され得る。画像データ内の検出された構成要素を表すそのようなデータの例は、画像座標、タイムスタンプ、物体ラベル、色識別子、物体の画像などであり得る。これは、受信した部分が、検出された物体の識別特性を生成することによって物体を追跡する、方法を継続することを可能にする。

【0043】

その後、生成された識別特性が、検出された物体に対して記憶され、領域405内で追跡される人間たちのリスト内に登録された識別プロファイル内の識別特性と比較される(ステップ210)。領域405内で追跡される人間たちのリストを維持することによって、検出された物体の生成された識別特性を、画定された領域内にいる可能性を有する人間たちの完全なリストと比較する必要がない。それは、例えば、製造施設における全ての従

10

20

30

40

50

業員たち、オフィスで働いている全ての人間たち、ゲーテッドコミュニティで暮らしている全ての人間たちなどである。これは、特定の精度が高まること、大量の処理能力と処理時間が節約されること、及び実際の処理が限られた処理能力と処理時間を用いてシステムの構成要素において実行され得ることをもたらす。領域 405 内で追跡される人間たちのリストに載っている人間たちは、画定された領域に入ったことに応じてリストに登録されて、それによって、リストに載っているという事実のために、比較が行われるステップ 210 の一部分としてリストを作成するために、何らの時間又は処理能力も必要とされない。比較ステップ 210 は、特定と登録のステップ 202 と 204 よりも頻繁にシステムによって行われると推定されるようである。何故ならば、画定された領域 101 に入った人間たちは、画定された領域 101 を動き回る傾向があり、画定された領域内の多くの場所において監視カメラ 107 によって取得された画像データ内で検出され得るからである。したがって、リストを作成することに関連付けられる処理は、特定に応じて、画定された領域 101 に入る特定された人間たちを登録することによっても低減され得る（ステップ 202）。

【0044】

ステップ 212 では、検出された物体の一組の識別特性に最も良くマッチングする、領域 405 内で追跡される人間たちのリスト内の識別プロファイルが判定される。これは、如何に優れて識別プロファイル内の識別特性が、検出された物体の生成された識別特性にマッチングするかを表す、信頼性スコアを計算することによって実行され得る。例えば、信頼性スコアは、パーセンテージとして規定され得る。100%又は1は、識別特性の同一のマッチングを示し、0%又は0は、2つの完全に異なる識別特性を示す。識別特性のマッチングは、実行することが困難であり得る。何故ならば、マッチングのための原理として使用されている画像データは、照明状態、画像処理アーチファクト、監視カメラの性能などによって影響を受け易いからである。マッチングの信頼性を高めるために、幾つかの異なる識別特性が並行して使用され、組み合わせられた結果が使用され得る。ニューラルネットワークアプローチが使用され、検出された物体の生成された識別特性に最も良くマッチングする識別プロファイルを判定し得る。その後、ニューラルネットワークは、識別プロファイルと検出された物体の識別特性との間の最も高い相関を有する最も優れたマッチングを見つけるように訓練され、サーバ 109a ~ b に実装され、又は監視カメラ 107 若しくは監視カメラに接続された局所的計算ユニットにわたり分散され得る。訓練の経験に基づいて、その後、ニューラルネットワークは、最も優れたマッチングに到達することにおいて最も効率が良い、（1以上の）識別特性の組み合わせを使用し得る。したがって、ある識別特性は、それらが最も優れたマッチングを見つけることにおいて効率的でないならば、そのようなシナリオにおいて使用されないだろう。例えば、マッチングを見つけることにおける効率は、最も優れたマッチングを実際に見つけることの成功率、最も優れたマッチングを見つけるために必要とされるリソース、最も優れたマッチングを見つけるためにかかる時間、又は最も優れたマッチングを見つけるために必要とされる処理能力を指し得る。ニューラルネットワークは、マッチングを実行するための可能なアプローチのうちの1つ又は組み合わせを使用するように実装され得る。当該技術分野で知られている種々のマッチングアプローチが存在し、例えば、検出された物体の識別特性と識別プロファイルの識別特性との間のユークリッド距離が、Schroff et alの「Facenet: A unified embedding for face recognition and clustering.」Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2015によって、マッチングにおいて使用され得る。代替例は、Viola and Jones in 「Rapid object detection using a boosted cascade of simple features.」Computer Vision and Pattern Recognition, 2001. CVPR 2001. Proceedings of the 2001 IEEE computer Society Co

10

20

30

40

50

nference on . Vol . 1 . IEEE , 2001によって開示されたものなどの、特徴カスケードに基づくアルゴリズムを適用する。ユークリッド距離のアプローチを使用する場合、短いユークリッド距離が、識別特性の間の高い相関を表し、一方で、大きなユークリッド距離が、低い相関を表し得る。

【0045】

ステップ214では、検出された物体が、検出された物体の識別プロファイルに最も良くマッチングすると判定された識別プロファイルに紐づけられる。紐づけは、物体が検出された画像フレームに紐づけられるメタデータとして保存される、参照、タグ、又はポインターとして実施され得る。代替的に、又は組み合わせられて、ビデオフレーム若しくはビデオフレームのシーケンスに対する参照、タグ、若しくはポインター、又は代替的に時間

10

【0046】

識別特性の最も優れたマッチングを見つけるために信頼性スコアを使用することに加えて、それらは、最も優れたマッチングが実は乏しいマッチングであることの表示としても使用され得る。検出された物体の一組の識別特性に対して最も高い相関を有する識別プロファイルに対応する計算された信頼性スコアが、第1の閾値よりも小さいならば、検出された物体を最も優れたマッチングを生み出す識別プロファイルに紐づける動作は、実行されないだろう。これは、システムが、間違いをもたらし得る結果を記憶することを妨げ得る。警報も、生成され、そのような場合にシステムのオペレータに送信され得る。乏しい相関を有するマッチングのこれらの場合が、乏しいマッチングとして強調されることは重要であり得る。何故ならば、それは、画定された領域101へのアクセスを許容されていない人間が、何らかのやり方で画定された領域101へのアクセスを獲得したことの表示であり得るからである。

20

【0047】

領域405内で追跡される人間たちのリストを最新の且つ正確なものとして維持するために、画定された領域101を離れるとして特定された人間たちが、このリストから除去され得る。例えば、人間たちが画定された領域101から離れることを可能にするドアを開くために、彼らは、認証情報を提示することによって、画定された領域101を離れるものとして特定され得る。その後、提示された認証情報は、彼らのアイデンティティを見つけるために事前に登録された人間たちの認証情報を含むデータベース内の認証情報にマッチングされ得る。そして、領域405内で追跡される人間たちのリストから、彼らの識別プロファイルを除去することができる。

30

【0048】

所定の活動期間の間に検出された物体に紐づけられなかった識別プロファイルも、領域405内で追跡される人間たちのリストから除去され得る。したがって、画定された領域101に入った人間が、画定された領域101内の監視しない場所に滞在するならば、又は画定された領域101を離れるものとして特定されることなしに、画定された領域101を離れるならば、その人間は、その人間の識別プロファイルが最後に検出された物体に紐づけられて以来、所定の活動期間が経過した後で、領域405内で追跡される人間たちのリストから除去され得る。この特徴は、領域405内で追跡される人間たちのリストを正確に維持するように実装され得る。それは、追跡の処理時間を低減させ特定の精度を高めるために、必要とされるよりも多くの人間たちを含まないだろう。所定の活動期間の範囲は、システム毎に変動し得る。画定された領域101では、沢山の人間が頻繁に動き回り、領域を離れる人間たちを特定することが難しく、この期間を非常に短く設定することが賢明であろう。例えば、ホテルなどにおけるように、2、3名の人間たちだけが動き回り、画定された領域101内の監視されない場所により長く滞在するかもしれないシステムでは、この所定の活動期間は、通常、より長い期間に設定され得る。

40

【0049】

50

図3では、人間を追跡するための代替的な方法が表示されている。この方法は、図2を参照して説明された方法に基づき、その方法と共通な幾つかのステップを有し、その共通のステップは、簡略のために同じ参照番号が付されている。

【0050】

図3の追跡方法は、認証情報をマッチングさせることによって人間を特定すること（ステップ202）、及び領域405内で追跡される人間たちのリスト内で特定された人間の識別プロファイルを登録すること（ステップ204）によって開始する。ステップ202とステップ204の両方は、図2を参照して以前に説明されている。しかし、識別プロファイルは、領域505に入った人間たちのリスト内にも登録される（ステップ304）。領域505に入った人間たちのリストは、領域に入ったと特定された全ての人間たちの識別プロファイルを含む。リストを正確に維持するために、領域を離れるものと特定された人間たちは、リストから除去され得る。図2で表示された追跡方法と類似して、画像データがステップ206で受信され、受信した画像データ内で検出された物体の識別特性が、ステップ208で生成される。ステップ310では、その後、生成された識別特性と識別プロファイルの対応する識別特性との間の相関の信頼性スコアを計算することによって、生成された識別特性が、領域405内で追跡される人間たちのリスト内の識別プロファイルと比較される。信頼性スコアは、以前に説明されており、その説明は、ステップ310で計算される信頼性スコアにも適用される。検出された物体の生成された識別特性との最も高い相関を有し、それによって、最も高い信頼性スコアを生成する識別プロファイルは、ステップ213で選択される。生成された識別特性と最も高い相関を有する識別プロファイルとの間のマッチングの質を検査するために、最も高い相関に関連付けられた信頼性スコアが、ステップ316で、閾値と比較される。信頼性スコアが、この閾値よりも大きいならば、生成された識別特性と識別プロファイルとの間のマッチングは、検出された物体が識別プロファイルに紐づけられるステップ214へと続くのに十分優れた質を有している。

【0051】

しかし、信頼性スコアが閾値よりも大きくなければ、これは、生成された識別特性と識別プロファイルとの間のマッチングが、乏しい相関を有することを示す。これは、通常、領域405内で追跡される人間たちのリストから除去された人間が、再び領域の監視部分内で動き始めた場合であり得る。乏しい相関は、人間が、認証情報を提示することなしに領域に入ったことも示し得る。

【0052】

その後、生成された識別特性と識別プロファイルの対応する識別特性との間の相関の信頼性スコアを計算することによって、生成された識別特性が、領域505内に入った人間たちのリスト内の識別プロファイルと比較される（ステップ318参照）。ステップ312と類似して、その後、最も高い相関に対応する識別プロファイルは、ステップ320で選択され、ステップ214で検出された物体に紐づけられる。検出された物体の一組の識別特性に対して最も高い相関を有する識別プロファイルに対応する計算された信頼性スコアが、第2の閾値よりも小さいならば、検出された物体を最も優れたマッチングを生み出す識別プロファイルに紐づける動作は、実行されないだろう。これは、システムが、間違いをもたらし得る結果を記憶することを妨げ得る。警報も、生成され、そのような場合にシステムのオペレータに送信され得る。乏しい相関を有するマッチングのこれらの場合が、乏しいマッチングとして強調されることは重要であり得る。何故ならば、それは、画定された領域101へのアクセスを許容されていない人間が、何らかのやり方で画定された領域101へのアクセスを獲得したことの表示だからである。

【0053】

領域405内で追跡される人間たちのリストは、領域505に入った人間たちのリストのサブセットを含む。したがって、領域405内で追跡される人間たちのリストは、領域に入った人間たちのリストであり、現在追跡されている人間たちリストでもあり、又は少なくとも最近検出された物体に紐づけられた人間たちのリストである。これは、上述した

所定の活動期間を使用して実現され、特定の期間中に検出された物体に紐づけられなかった識別プロファイルを、領域内で追跡される人間のリストから除去し得る。したがって、領域 405 内で追跡される人間たちのリストは、画像データ内で物体が検出されたときに高い相関を有するマッチングの最も可能性が高い候補を含み得る。したがって、追跡する方法が使用されたときに大多数の場合、処理時間及び処理リソースが低減され得る。それは、最も可能性が高い候補のみが比較ステップ 310 内で使用されるからである。最も可能性が高い候補のうちの 1 つが優れた十分な相関を有するマッチングを生成しない稀な場合、第 2 の比較ステップ 318 が、識別特性を、領域に入ったが最近の時間において検出された物体に紐づけられていなかった人間たちの識別プロファイルと比較することの可能性も提供する。したがって、その後、人間が画定された領域 101 に入るならば、しかし、例えば、所定の活動期間よりも長い期間において監視カメラ 107 の何れかによって監視されていない室内に滞在するならば、その人間の識別プロファイルは、領域 405 内で追跡される人間たちのリストから除去され得る。しかし、人間は領域 505 に入った人間たちのリストに未だ載り得るので、その人間の識別プロファイルは、その人間が監視されていない部屋を離れ、監視カメラによって検出されたときに選択され得る。

10

【0054】

識別プロファイルが領域 405 内で追跡される人間たちのリストから除去されたときのような場合、識別プロファイルは、検出された物体を問題の識別プロファイルに紐づけるステップ 214 に応じて、再び領域 405 内で追跡される人間たちのリストにも登録され得る。

20

【0055】

領域 405 内で追跡される人間たちのリストが、領域 505 に入った人間たちのリストのサブセットを含むという事実によって、ステップ 318 で、信頼性スコアは、領域 405 内で追跡される人間たちのリスト内の識別プロファイルに対して再計算される必要はないかもしれない。ステップ 310 でこれらの識別プロファイルに対して計算される信頼性スコアは、ステップ 318 で再使用され得るか、又は、これらの識別プロファイルがステップ 318 で実行される比較に含まれないことが判定され得る。

【0056】

人間が領域に入ったと特定されたときの時間内のポイント以来、所定の存在期間が経過したならば、そのときも、領域に入った人間たちの識別プロファイルは、そのリストから除去され得る。

30

これは、領域 505 に入った人間たちのリストを最新の且つ正確なものに維持することにおいて有用である。何故ならば、人間たちが、その領域を離れるものと特定されることなしに、画定された領域を離れる可能性が存在し得るからである。所定の存在期間は、通常、画定された領域内の予期される存在期間よりも長い期間に設定され得る。例えば、画定された領域がオフィスビルならば、この期間は、幾らかの安全マージンを伴う予期される就業時間に設定され得る。

【0057】

検出された物体を選択された識別プロファイルに紐づけるステップ 214 に応じて、選択された識別プロファイルは、検出された物体の生成された識別特性からのデータを用いて更新され得る。代替例として、識別プロファイルの更新は、例えば、信頼性スコアを更新のために所定の閾値と比較することによって、マッチングの相関が十分に高いときにだけ行われ得る。更新を実行する 1 つのやり方は、識別プロファイル内の現在の情報と生成された一組の識別特性からの情報とに基づいて、統計的測定値を計算することであり得る。

40

【0058】

図 4 との関連で、人間を追跡するためのシステム 400 が説明される。人間を追跡するためのシステム 400 は、事前に登録された人間たちの認証情報を含むデータベース内の認証情報に、その人間によって提示された認証情報をマッチングさせることによって、画定された領域に入る人間を特定するように構成された識別モジュール 402、人間の識別

50

プロフィールであって、その人間を特定するための情報を含む、識別プロフィールを領域 405 内で追跡される人間たちのリスト内に登録するように構成された登録モジュール 404、領域内の情景から画像データを取得するように構成された画像取得装置 406、画像取得装置によって取得された画像データ内で検出された物体の一組の識別特性を生成するように構成された識別特性生成モジュール 408、検出された物体の生成された一組の識別特性を、領域 405 内で追跡される人間たちのリスト内に登録された識別プロフィールと比較し、検出された物体の一組の識別特性に最も良くマッチングする、領域 405 内で追跡される人間たちのリスト内の識別プロフィールを判定するように構成されたマッチングモジュール 410、及び検出された物体を、検出された物体の識別プロフィールに最も良くマッチングすると判定された識別プロフィールに紐づけるように構成された追跡モジュール 412 を備える。

10

【0059】

図 4 の識別モジュール 402 は、物理的アクセスコントローラ 103 a、103 b、又はサーバ 109 a などの、物理的アクセス制御システムに接続されたサーバに実装され得る。109 a 又は 109 b などの中央サーバは、通常、登録モジュール 404 の機能を含むが、登録モジュールの機能は、代替的には、当該技術分野で知られているピアツーピアプロトコルを使用して、監視カメラ 107 又は物理的アクセスコントローラ 103 に分散され得る。登録モジュール 404 は、更に、別の代替例として、1 以上の近くの監視カメラ 107 を担う（1 以上の）局所的計算ユニットに実装され得る。識別モジュール 402 は、登録モジュール 404 に接続され、特定された人間の識別子を登録モジュール 404

20

【0060】

監視カメラ 107 は、画定された領域 101 内の情景から画像データを取得する画像取得装置 406 の実施例である。監視カメラ 107 は、識別特性生成モジュールも含み、又は代替的に、このモジュールは、監視カメラ 107 に接続された中央サーバ 109 b に配置され得る。後者の場合、監視カメラは、監視された情景の画像データを中央サーバ 109 b に送信し、又は特に、物体の検出がカメラで実行されたならば、検出された物体の画像データを中央サーバ 109 b に送信する。

30

【0061】

マッチングモジュール 410 は、最も優れたマッチングを見つけるための比較を行うために、登録モジュール 404 から登録された識別プロフィールについての情報を受信し、識別特性生成モジュール 408 から生成された識別特性を受信する。以前に説明されたもののように、この比較は、信頼性スコアを計算し比較することによって行われ得る。その後、最も優れたマッチングをもたらす識別プロフィールを特定するデータが、検出された物体をこの識別プロフィールに紐づける追跡モジュール 412 に送信され得る。マッチングモジュール 410 と追跡モジュール 412 は、中央サーバ 109、近くのカメラを担う（1 以上の）局所的計算ユニット、分散された機能で、複数の監視カメラ 107、又は物理的アクセス制御サーバ 103 に実装され得る。

40

【0062】

図 5 は、人間を追跡するためのシステム 500 の別の一実施例を示している。システム 400 との関連で、以前に説明されたモジュールのうちの幾つかは、システム 500 内に存在する。これらのモジュールの説明は、システム 500 にも適用される。

【0063】

システム 500 の領域 505 に入った人間たちのリストの識別プロフィールを登録する

50

エントランス登録モジュール514は、物理的アクセス制御システムの部分として実装され、例えば、物理的アクセスコントローラ103に含まれ、又は物理的アクセスコントローラ103に接続された中央サーバに含まれ得る。エントランス登録モジュール514は、システム500の他のモジュールとの関連で、領域505に入った人間たちのリストのエントリに関して、情報を記憶し、通信を取り扱う。エントランス登録モジュール514は、サブモジュール、例えば、システム500の他のモジュールとの通信を取り扱う1つのサブモジュール、及び領域505に入った人間たちの実際のリストを記憶する1つのサブモジュールを備え得る。領域405内で追跡される人間たちのリストを用いて働くマッチングモジュール410に加えて、第2のマッチングモジュール512が、システム500内に含まれ、領域505に入った人間たちのリストの識別プロファイルとマッチングする。したがって、マッチングモジュール512は、最も優れたマッチングを見つけるための比較を行うために、エントランス登録モジュール514から登録された識別プロファイルについての情報を受信し、識別特性生成モジュール408から生成された識別特性を受信する。

10

【0064】

登録解除モジュール516は、システム500内で登録モジュール404に接続されている。検出された物体が識別プロファイルに紐づけられた、したがって、登録モジュール404に紐づけられた時間内の最後のポイント以来、所定の活動期間が経過したならば、登録解除モジュール516は、領域405内で追跡される人間たちのリストから人間の識別プロファイルを登録解除するように構成されている。登録モジュール404と同様に、登録解除モジュール516は、109a又は109bなどの中央サーバに実装され得る。しかし、登録解除モジュール516の機能は、代替的に、当該技術分野で知られているピアツーピアプロトコルを使用して、監視カメラ107又は物理的アクセスコントローラ103に分散され得る。別の代替例は、登録解除モジュール516を、1以上の近くの監視カメラ107を担う(1以上の)局所的計算ユニットに実装することである。

20

【0065】

更に、本発明は、その中で具現化されたコンピュータ可読プログラムコードを有する1以上コンピュータ可読媒体内で具現化された非一時的コンピュータプログラム製品の形態を採り得る。

【0066】

30

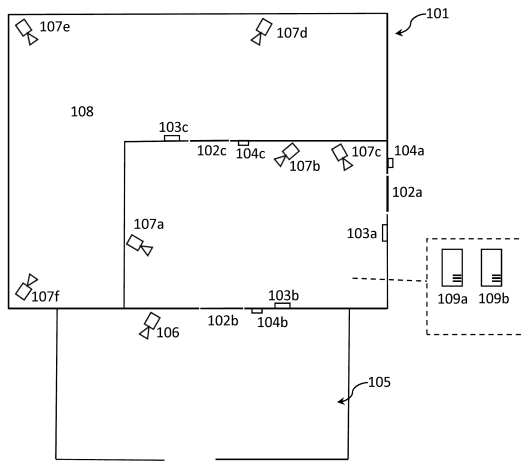
本発明による物理的アクセス制御システムと監視システムは、ビデオ管理システム、いわゆるVMSと更に接続され得る。一般的に、ビデオ管理システムは、監視カメラと監視カメラによって生成されたビデオとを管理するが、更に、物理的アクセス制御システムを管理するようにも拡張され得る。したがって、VMSと相互作用するオペレータは、本発明による物体を追跡するためのシステムも構成し得る。例えば、信頼性スコアのための上述された閾値は、VMSインターフェースを使用して、オペレータによって構成され得る。存在期間と活動期間とは、VMSを使用して同様に構成され得る。

【0067】

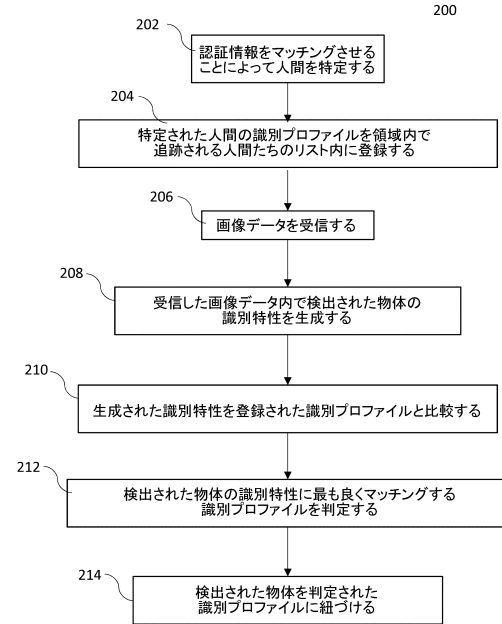
検出された物体と識別プロファイルとの間で行われる紐づけは、VMSによっても使用されて、例えば、オペレータによって特定された物体の画像データと物理的座標を集め得る。集められた画像データと物理的座標から、統計データのみならず視覚的図解が、オペレータの使用のために引き出され得る。この種類の物体追跡検索は、ライブデータを使用することと、いわゆる犯罪科学映像検索において記録された資料を使用することとの両方によって実行され得る。

40

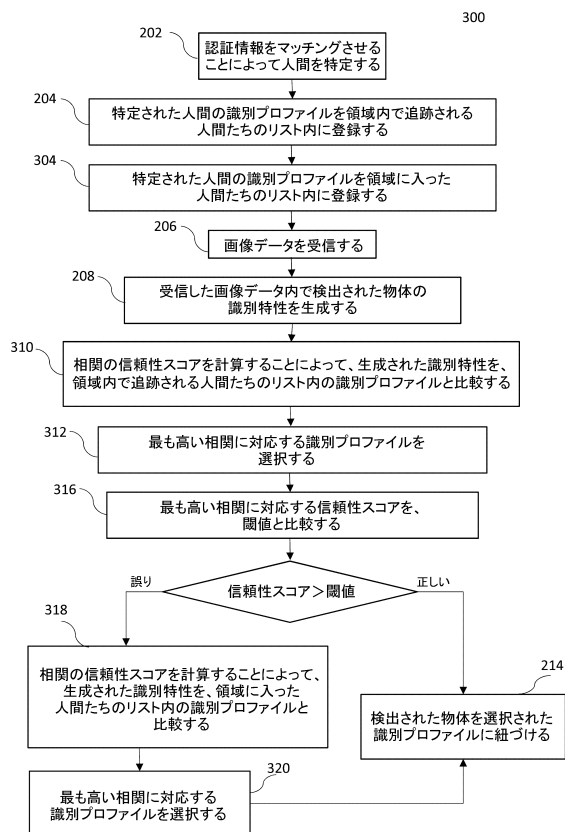
【図 1】



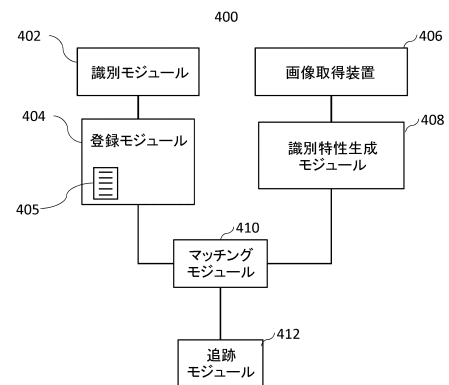
【図 2】



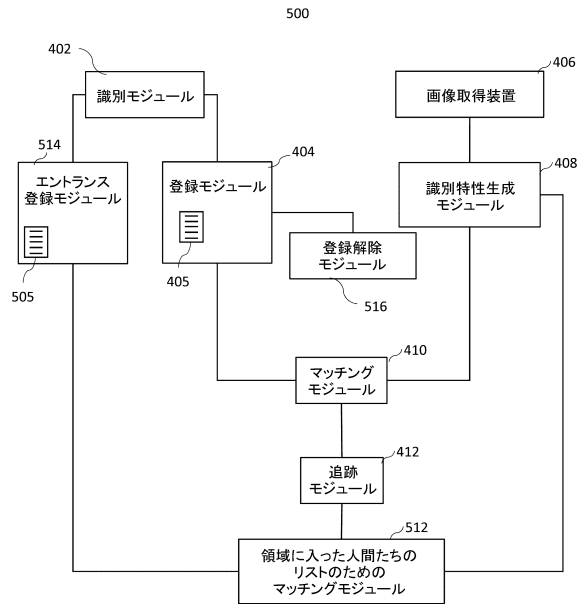
【図 3】



【図 4】



【図 5】



フロントページの続き

(51)Int.Cl. F I
G 0 6 T 7/00 3 5 0 C
G 0 8 B 25/00 5 1 0 M

(72)発明者 ハンソン, アンデルス
スウェーデン国 2 2 3 6 9 ルンド, エンダラヴェーゲン 1 4, シー/オー アクシス
コミュニケーションズ アーバー

審査官 新井 則和

(56)参考文献 特開2012-034253(JP,A)
特開2010-128938(JP,A)
特開2013-114348(JP,A)
特開2000-200357(JP,A)
特開2006-099615(JP,A)
MIN-GU KIM ET AL., A Survey and Proposed Framework on the Soft Biometrics Technique for Human Identification in Intelligent Video Surveillance System, JOURNAL OF BIOMEDICINE AND BIOTECHNOLOGY, vol. 2012, 2012年 1月 1日, pp. 1-7

(58)調査した分野(Int.Cl., DB名)
G 0 6 T 7 / 0 0 - 7 / 9 0
G 0 8 B 2 5 / 0 0
H 0 4 N 7 / 1 8