(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7257765号
(P7257765)

(45)発行日　令和5年4月14日(2023.4.14)

(24)登録日　令和5年4月6日(2023.4.6)

(51)国際特許分類		FI		
G06T	*7/00 (2017.01)*	G06T	7/00	510F
H04N	*7/18 (2006.01)*	H04N	7/18	K
G06F	*16/00 (2019.01)*	G06T	7/00	660A
		G06F	16/00	

請求項の数　20　（全21頁）

(21)出願番号　特願2018-182700(P2018-182700)
(22)出願日　平成30年9月27日(2018.9.27)
(65)公開番号　特開2020-52822(P2020-52822A)
(43)公開日　令和2年4月2日(2020.4.2)
審査請求日　令和3年9月27日(2021.9.27)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　110003281
弁理士法人大塚国際特許事務所
(72)発明者　内田 悠美子
東京都大田区下丸子３丁目３０番２号
キヤノン株式会社内
(72)発明者　椎山 弘隆
東京都大田区下丸子３丁目３０番２号
キヤノン株式会社内
審査官　千葉 久博

最終頁に続く

(54)【発明の名称】　情報処理装置、認証システムおよびそれらの制御方法、プログラム

(57)【特許請求の範囲】

【請求項１】

複数の撮影装置に対応する複数の認証装置とネットワークを介して接続された情報処理装置であって、

前記複数の撮影装置に含まれる第１の撮影装置により撮影された撮影画像に含まれ該第１の撮影装置に対応する第１の認証装置により認証された第１のオブジェクトの認証に利用可能な認証データを生成する認証データ生成手段と、

前記認証データ生成手段により生成された認証データを、前記複数の認証装置に含まれる少なくとも１つの認証装置の認証ＤＢに反映させる反映手段と、

を備え、

前記認証データ生成手段は、前記第１のオブジェクトを認証した際に用いた前記第１の認証装置の認証ＤＢに含まれる第１の認証データに対応する第１の撮影条件とは異なる第２の撮影条件に対応する新規の認証データを生成し、前記第１の撮影条件に対応する新規の認証データの生成を抑止する

ことを特徴とする情報処理装置。

【請求項２】

前記認証データ生成手段は、前記第１のオブジェクトを含む撮影画像および前記第１のオブジェクトを含む撮影画像から生成されるオブジェクトモデルの少なくとも一方に基づいて新規の認証データを生成する

ことを特徴とする請求項１に記載の情報処理装置。

【請求項３】
前記認証データ生成手段は、前記第１のオブジェクトを含みかつ前記第２の撮影条件に対応する撮影画像に基づいて新規の認証データを生成する
ことを特徴とする請求項１に記載の情報処理装置。
【請求項４】
複数の撮影装置に対応する複数の認証装置とネットワークを介して接続された情報処理装置であって、
前記複数の撮影装置に含まれる第１の撮影装置により撮影された撮影画像に含まれ該第１の撮影装置に対応する第１の認証装置により認証された第１のオブジェクトの認証に利用可能な認証データを生成する認証データ生成手段と、
前記認証データ生成手段により生成された認証データを、前記複数の認証装置に含まれる少なくとも１つの認証装置の認証ＤＢに反映させる反映手段と、
を備え、
前記認証データ生成手段は、前記第１のオブジェクトを認証した際に用いた前記第１の認証装置の認証ＤＢに含まれる第１の認証データに対応する第１の撮影条件とは異なる第２の撮影条件に対応する第２の認証データを生成し、
前記認証データ生成手段は、前記第１の撮影装置により得られた複数の撮影画像に関して前記第１のオブジェクトを追尾して得られる画像群の中から前記第２の撮影条件に対応する画像を選択し前記第２の認証データを生成する
ことを特徴とする情報処理装置。
【請求項５】
前記第１の撮影装置により得られた複数の撮影画像におけるオブジェクトの撮影条件の出現確率を算出する算出手段を更に備え、
前記認証データ生成手段は、前記算出手段により算出された出現確率に基づいて前記第２の撮影条件を決定する
ことを特徴とする請求項４に記載の情報処理装置。
【請求項６】
前記認証データ生成手段は、更に、前記第１の撮影条件及び前記第２の撮影条件とは異なる第３の撮影条件に対応する第３の認証データを生成する
ことを特徴とする請求項１乃至５の何れか１項に記載の情報処理装置。
【請求項７】
前記撮影条件は、オブジェクトの撮影方向、オブジェクトの付帯物、照明条件の少なくとも１つを含む
ことを特徴とする請求項１乃至６の何れか１項に記載の情報処理装置。
【請求項８】
前記オブジェクトは、人の顔画像であり、
前記認証ＤＢに含まれる認証データは顔画像の特徴量である
ことを特徴とする請求項１乃至７の何れか１項に記載の情報処理装置。
【請求項９】
複数の撮影装置に対応する複数の認証装置とネットワークを介して接続された情報処理装置であって、
前記複数の撮影装置に含まれる第１の撮影装置により撮影された撮影画像に含まれ該第１の撮影装置に対応する第１の認証装置により認証された第１のオブジェクトの認証に利用可能な認証データを生成する認証データ生成手段と、
前記認証データ生成手段により生成された認証データを、前記複数の認証装置に含まれる少なくとも１つの認証装置の認証ＤＢに反映させる反映手段と、
を備え、
前記認証データ生成手段は、前記第１のオブジェクトを認証した際に用いた前記第１の認証装置の認証ＤＢに含まれる第１の認証データに対応する第１の撮影条件とは異なる第２の撮影条件に対応する第２の認証データを生成し、

前記反映手段は、前記認証ＤＢに含まれることになる複数の認証データにおける撮影条件の分散が大きくなるように、前記認証データ生成手段により生成された認証データを、前記複数の認証装置に含まれる少なくとも１つの認証装置の認証ＤＢに反映させる
ことを特徴とする情報処理装置。
【請求項１０】
複数の撮影装置に対応する複数の認証装置とネットワークを介して接続された情報処理装置であって、
前記複数の撮影装置に含まれる第１の撮影装置により撮影された撮影画像に含まれ該第１の撮影装置に対応する第１の認証装置により認証された第１のオブジェクトの認証に利用可能な認証データを生成する認証データ生成手段と、
前記認証データ生成手段により生成された認証データを、前記複数の認証装置に含まれる少なくとも１つの認証装置の認証ＤＢに反映させる反映手段と、
を備え、
前記認証データ生成手段は、前記第１のオブジェクトを認証した際に用いた前記第１の認証装置の認証ＤＢに含まれる第１の認証データに対応する第１の撮影条件とは異なる第２の撮影条件に対応する第２の認証データを生成し、
前記認証データ生成手段により生成された１以上の認証データに対して優先度を付与する付与手段を更に備え、
前記反映手段は、相対的に優先度が高い認証データを前記複数の認証装置に含まれる少なくとも１つの認証装置の認証ＤＢに反映させる
ことを特徴とする情報処理装置。
【請求項１１】
複数の撮影装置に対応する複数の認証装置とネットワークを介して接続された情報処理装置であって、
前記複数の撮影装置に含まれる第１の撮影装置により撮影された撮影画像に含まれ該第１の撮影装置に対応する第１の認証装置により認証された第１のオブジェクトの認証に利用可能な認証データを生成する認証データ生成手段と、
前記認証データ生成手段により生成された認証データを、前記複数の認証装置に含まれる少なくとも１つの認証装置の認証ＤＢに反映させる反映手段と、
を備え、
前記認証データ生成手段は、前記第１のオブジェクトを認証した際に用いた前記第１の認証装置の認証ＤＢに含まれる第１の認証データに対応する第１の撮影条件とは異なる第２の撮影条件に対応する第２の認証データを生成し、
前記反映手段は、更に、認証データの反映により認証ＤＢに含まれる認証データの個数が所定の上限を超える場合に該認証ＤＢに含まれる１以上の認証データを削除する
ことを特徴とする情報処理装置。
【請求項１２】
複数の撮影装置に対応する複数の認証装置とネットワークを介して接続された情報処理装置であって、
前記複数の撮影装置に含まれる第１の撮影装置により撮影された撮影画像に含まれ該第１の撮影装置に対応する第１の認証装置により認証された第１のオブジェクトの認証に利用可能な認証データを生成する認証データ生成手段と、
前記認証データ生成手段により生成された認証データを、前記複数の認証装置に含まれる少なくとも１つの認証装置の認証ＤＢに反映させる反映手段と、
を備え、
前記認証データ生成手段は、前記第１のオブジェクトを認証した際に用いた前記第１の認証装置の認証ＤＢに含まれる第１の認証データに対応する第１の撮影条件とは異なる第２の撮影条件に対応する第２の認証データを生成し、
前記反映手段は、前記第１のオブジェクトの移動軌跡を予測し、該移動軌跡に基づいて、認証データを反映させる認証ＤＢの順序を決定する

ことを特徴とする情報処理装置。
【請求項１３】
前記複数の撮影装置の各々と対応する認証装置とは一体の装置として構成される
ことを特徴とする請求項１乃至１２の何れか１項に記載の情報処理装置。
【請求項１４】
複数の撮影装置に対応する複数の認証装置とネットワークを介して接続された情報処理装置の制御方法であって、
前記複数の撮影装置に含まれる第１の撮影装置により撮影された撮影画像に含まれ該第１の撮影装置に対応する第１の認証装置により認証された第１のオブジェクトの認証に利用可能な認証データを生成する認証データ生成工程と、
前記認証データ生成工程により生成された認証データを、前記複数の認証装置に含まれる少なくとも１つの認証装置の認証ＤＢに反映させる反映工程と、
を含み、
前記認証データ生成工程では、前記第１のオブジェクトを認証した際に用いた前記第１の認証装置の認証ＤＢに含まれる第１の認証データに対応する第１の撮影条件とは異なる第２の撮影条件に対応する新規の認証データを生成し、前記第１の撮影条件に対応する新規の認証データの生成を抑止する
ことを特徴とする制御方法。
【請求項１５】
認証システムであって、
複数の撮影手段と、
前記複数の撮影手段に対応する複数の認証手段であって、該複数の認証手段の各々は対応する撮影手段により取得された撮影画像に含まれるオブジェクトをそれぞれの認証ＤＢに基づいて認証する、前記複数の認証手段と、
前記複数の撮影手段に含まれる第１の撮影手段により撮影された撮影画像に含まれ該第１の撮影手段に対応する第１の認証手段により認証された第１のオブジェクトの認証に利用可能な認証データを生成する認証データ生成手段と、
前記認証データ生成手段により生成された認証データを、前記複数の認証手段に含まれる少なくとも１つの認証手段の認証ＤＢに反映させる反映手段と、
を備え、
前記認証データ生成手段は、前記第１のオブジェクトを認証した際に用いた前記第１の認証手段の認証ＤＢに含まれる第１の認証データに対応する第１の撮影条件とは異なる第２の撮影条件に対応する新規の認証データを生成し、前記第１の撮影条件に対応する新規の認証データの生成を抑止する
ことを特徴とする認証システム。
【請求項１６】
認証システムの制御方法であって、
前記認証システムは、
複数の撮影手段と、
前記複数の撮影手段に対応する複数の認証手段であって、該複数の認証手段の各々は対応する撮影手段により取得された撮影画像に含まれるオブジェクトをそれぞれの認証ＤＢに基づいて認証する、前記複数の認証手段と、
を備え、
前記制御方法は、
前記複数の撮影手段に含まれる第１の撮影手段により撮影された撮影画像に含まれ該第１の撮影手段に対応する第１の認証手段により認証された第１のオブジェクトの認証に利用可能な認証データを生成する認証データ生成工程と、
前記認証データ生成工程により生成された認証データを、前記複数の認証手段に含まれる少なくとも１つの認証手段の認証ＤＢに反映させる反映工程と、
を含み、

前記認証データ生成工程では、前記第１のオブジェクトを認証した際に用いた前記第１の認証手段の認証ＤＢに含まれる第１の認証データに対応する第１の撮影条件とは異なる第２の撮影条件に対応する新規の認証データを生成し、前記第１の撮影条件に対応する新規の認証データの生成を抑止する
ことを特徴とする制御方法。
【請求項１７】
複数の撮影装置とネットワークを介して通信可能に接続された情報処理装置であって、
前記複数の撮影装置に含まれる第１の撮影装置により撮影された撮影画像に含まれ、該第１の撮影装置が有する第１の認証手段により認証されたオブジェクトの認証に利用可能な認証データを生成する認証データ生成手段と、
前記認証データ生成手段により生成された認証データを、前記複数の撮影装置に含まれ、前記第１の撮影装置とは異なる少なくとも１つの撮影装置が有する保持手段であって認証データを保持する認証データベースに反映させる反映手段と、
を備え、
前記認証データ生成手段は、前記オブジェクトを認証した際に用いた前記第１の撮影装置が有する認証データベースに登録されていた第１の認証データに対応する第１の条件とは異なる第２の条件に対応する第２の認証データを生成し、
前記認証データ生成手段は、前記第１の撮影装置により得られた複数の撮影画像に関して前記オブジェクトを追尾して得られる画像群の中から前記第２の条件に対応する画像を選択し前記第２の認証データを生成する
ことを特徴とする情報処理装置。
【請求項１８】
複数の撮影装置とネットワークを介して通信可能に接続された情報処理装置であって、
前記複数の撮影装置に含まれる第１の撮影装置により撮影された撮影画像に含まれ、該第１の撮影装置が有する第１の認証手段により認証されたオブジェクトの認証に利用可能な認証データを生成する認証データ生成手段と、
前記認証データ生成手段により生成された認証データを、前記複数の撮影装置に含まれ、前記第１の撮影装置とは異なる少なくとも１つの撮影装置が有する保持手段であって認証データを保持する認証データベースに反映させる反映手段と、
を備え、
前記認証データ生成手段は、前記オブジェクトを認証した際に用いた前記第１の撮影装置が有する認証データベースに登録されていた第１の認証データに対応する第１の条件とは異なる第２の条件に対応する第２の認証データを生成し、
前記オブジェクトは、人間の顔画像であり、
前記認証データ生成手段は、顔の領域を追尾して得られる画像群の中から、前記第１の認証手段による認証に利用した認証データでは認証されない顔向きに対応する前記第２の認証データを生成する
ことを特徴とする情報処理装置。
【請求項１９】
複数の撮影装置とネットワークを介して通信可能に接続された情報処理装置の制御方法であって、
前記複数の撮影装置に含まれる第１の撮影装置により撮影された撮影画像に含まれ、該第１の撮影装置が有する第１の認証手段により認証されたオブジェクトの認証に利用可能な認証データを生成する認証データ生成工程と、
前記認証データ生成工程により生成された認証データを、前記複数の撮影装置に含まれ、前記第１の撮影装置とは異なる少なくとも１つの撮影装置が有する保持手段であって認証データを保持する認証データベースに反映させる反映工程と、
を含み、
前記認証データ生成工程では、前記オブジェクトを認証した際に用いた前記第１の撮影装置が有する認証データベースに登録されていた第１の認証データに対応する第１の条件

とは異なる第２の条件に対応する第２の認証データを生成し、
前記認証データ生成工程では、前記第１の撮影装置により得られた複数の撮影画像に関して前記オブジェクトを追尾して得られる画像群の中から前記第２の条件に対応する画像を選択し前記第２の認証データを生成する
ことを特徴とする制御方法。
【請求項２０】
コンピュータを、請求項１乃至１３、１７、１８の何れか１項に記載の情報処理装置の各手段として機能させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、映像内のオブジェクトを認証する認証システムにおける認証データの管理技術に関するものである。
【背景技術】
【０００２】
近年、監視カメラの映像を用いて顔認証をおこなうシステムの実用化が進んでいる。指名手配犯や万引き犯の顔を認証することで、迅速な逮捕や犯罪の未然防止に活用することができる。また、イベント会場などでは要人の顔を認証して居場所を把握することで、イベントの運営や警備員の移動配置をスムーズに行うことが可能となる。
【０００３】
顔認証では、認証対象の人物について事前に登録された顔画像と、実際に撮影された映像内の人物の顔画像を照合して、同一人物であるか否かを判定する。そのため、事前に登録された認証データ（特徴量など）の顔向きと実際に撮影された顔向きとが異なると、認証精度が落ちるという課題がある。ただし、精度の高い顔認証を行うために、認証データの顔向きバリエーションを増やすと、照合処理の負荷が高くなるという課題がある。
【０００４】
そこで、複数のカメラで認証データを共有する技術が提案されている。特許文献１では、ある監視装置で認証された人物の特徴量および顔画像を他の監視装置に送信する技術が開示されている。特許文献２では、ある監視カメラで認証された人物の外見的特徴情報（服装の色、持ち物の形状等）を他の監視カメラに送信する技術が開示されている。また、特許文献３では、映像内の人物の特徴量があらかじめ登録された人物の特徴量と一致した場合に、設置条件ごとのＤＢに登録されていない特徴量（顔向き、表情）を特定し、ＤＢに追加する技術が開示されている。
【先行技術文献】
【特許文献】
【０００５】
【文献】特開２０１３－１５３３０４号公報
特開２０１６－１２７５６３号公報
特開２０１６－３８７７４号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
しかしながら、上述の従来技術においては、認証を成功した顔画像の特徴量のみ他の装置に送信されることになる。すなわち、その画像を撮影した方向に依存した顔の特徴量だけが認証データに追加され、元の認証データから大きく離れた顔向きの特徴量を追加することは出来ない。そのため、認証精度の向上は限定的なものとなる。
【０００７】
本発明は、このような問題に鑑みてなされたものであり、認証精度をより効率的に向上させることを可能とする技術を提供することを目的としている。
【課題を解決するための手段】

【０００８】
上述の問題点を解決するため、本発明に係る認証システムは以下の構成を備える。すなわち、複数の撮影装置に対応する複数の認証装置とネットワークを介して接続された情報処理装置は、
前記複数の撮影装置に含まれる第１の撮影装置により撮影された撮影画像に含まれ該第１の撮影装置に対応する第１の認証装置により認証された第１のオブジェクトの認証に利用可能な認証データを生成する認証データ生成手段と、
前記認証データ生成手段により生成された認証データを、前記複数の認証装置に含まれる少なくとも１つの認証装置の認証ＤＢに反映させる反映手段と、
を備え、
前記認証データ生成手段は、前記第１のオブジェクトを認証した際に用いた前記第１の認証装置の認証ＤＢに含まれる第１の認証データに対応する第１の撮影条件とは異なる第２の撮影条件に対応する新規の認証データを生成し、前記第１の撮影条件に対応する新規の認証データの生成を抑止する。
【発明の効果】
【０００９】
本発明によれば、認証精度をより効率的に向上させることを可能とする技術を提供することができる。
【図面の簡単な説明】
【００１０】
【図１】第１実施形態に係る認証システムに含まれる各装置の構成を示す図である。
【図２】第１実施形態における認証データ更新処理の概要を示す図である。
【図３】認証システムで利用される各種データを説明する図である。
【図４】オブジェクト認証処理のフローチャートである。
【図５】認証データ拡充処理のフローチャートである。
【図６】認証データ更新処理のフローチャートである。
【図７】第２実施形態に係る認証システムに含まれる各装置の構成を示す図である。
【図８】第２実施形態における認証データ更新処理の概要を示す図である。
【図９】認証システムで利用される各種データを説明する図である。
【図１０】顔向き頻度算出処理のフローチャートである。
【発明を実施するための形態】
【００１１】
以下に、図面を参照して、この発明の実施の形態の一例を詳しく説明する。なお、以下の実施の形態はあくまで例示であり、本発明の範囲を限定する趣旨のものではない。
【００１２】
（第１実施形態）
本発明に係る画像処理装置の第１実施形態として、顔画像により映像内の人物（オブジェクト）を認証する認証システムを例に挙げて以下に説明する。
【００１３】
＜システム構成＞
第１実施形態に係る認証システムは、複数の撮影デバイス１１８と、撮影デバイスから送信されたデータを処理し認証データの更新情報を生成する解析サーバ１１９と、を含む。
【００１４】
図１は、第１実施形態に係る認証システムに含まれる各装置の構成を示す図である。図１（ａ）は、撮影デバイス１１８のハードウェア構成を示しており、図１（ｂ）は、解析サーバ１１９のハードウェア構成を示している。また、図１（ｃ）は、撮影デバイス１１８及び解析サーバ１１９のソフトウェア構成を示している。
【００１５】
撮影デバイス１１８は、ＣＰＵ１０１、ＲＯＭ１０２、ＲＡＭ１０６、記憶部１０７、撮像部１０８、通信部１０９を含む。ＲＯＭ１０２には、後述する抽出部１０３、認証部

１０４、更新部１０５を実現するための制御プログラムが格納されている。
【００１６】
ＣＰＵ１０１は、ＲＯＭ１０２に格納されている制御プログラムを実行することにより、撮影デバイス１１８全体の制御をおこなう。ＲＡＭ１０６は、後述する各種データを一時記憶する。また、ＲＡＭ１０６は、ＣＰＵ１０１のワークエリアとしても利用される。
【００１７】
記憶部１０７は、認証処理に利用する１以上の認証データ（例えば、顔画像の特徴量）を格納した認証データベース（ＤＢ）１２０を記憶する。記憶部１０７の媒体としては、フラッシュメモリ、ＨＤＤ、ＤＶＤなどを用いることができる。撮像部１０８は、所与の撮影範囲を撮影し撮影画像である映像を生成するための機能部である。撮像部１０８で生成された映像は、制御プログラムを実行するＣＰＵ１０１により解析される。通信部１０９は、解析サーバ１１９などの外部装置と通信するための機能部である。通信部１０９は、有線接続であってもよいし無線接続であってもよい。また、インターネットなどのネットワークを介して外部装置と通信する構成でもよい。撮像部１０８により得られた映像および認証部１０４が算出した認証情報は、通信部１０９を介して解析サーバ１１９に送信される。
【００１８】
抽出部１０３は、撮像部１０８により得られた映像を解析し、映像内に映っているオブジェクトを抽出する。オブジェクトとしては、人物、人の顔領域、動物、物体などであり得る。ここでは、オブジェクトとして人の顔領域を想定して説明を行う。認証部１０４は、認証ＤＢ１２０を参照してオブジェクトを認証する。ここでは、認証ＤＢ１２０には、認証対象となる人物の顔画像の特徴量が格納されているものとする。更新部１０５は、解析サーバ１１９から更新情報を受信し、認証ＤＢ１２０に格納された認証データの更新を行う。
【００１９】
解析サーバ１１９は、ＣＰＵ１１０、ＲＯＭ１１１、ＲＡＭ１１３、記憶部１１４、入力部１１５、表示部１１６、通信部１１７を含む情報処理装置である。ＲＯＭ１１１には、後述する更新情報生成部１１２を実現するための制御プログラムが格納されている。
【００２０】
ＣＰＵ１１０は、ＲＯＭ１１１に格納されている制御プログラムを実行することにより、解析サーバ１１９全体の制御をおこなう。ＲＡＭ１１３は、後述する各種データを一時記憶する。また、ＲＡＭ１１３は、ＣＰＵ１１０のワークエリアとしても利用される。
【００２１】
記憶部１１４は、撮影デバイス１１８から受信した映像や撮影デバイス１１８を管理するためのデバイス管理情報１２１を記憶する。記憶部１１４の媒体としては、フラッシュメモリ、ＨＤＤ、ＤＶＤなどを用いることができる。入力部１１５は、操作ボタン、タッチパネル等で構成され、ユーザからの指示を受け付ける機能部である。表示部１１６は、液晶パネル等で構成され、処理対象となるデータや処理結果を表示する機能部である。通信部１１７は、撮影デバイス１１８などの外部装置と通信するための機能部である。更新情報生成部１１２により生成された更新情報は、通信部１１７を介して各撮影デバイス１１８に送信される。
【００２２】
更新情報生成部１１２は、撮影デバイス１１８から受信したデータを解析し、オブジェクトの認証に利用可能な認証データの更新情報を生成する。より具体的には、更新情報生成部１１２は、デバイス管理情報１２１を参照し、各撮影デバイス１１８の認証ＤＢ１２０に対して追加すべきオブジェクト特徴量を決定し更新情報として生成する。なお、デバイス管理情報１２１は、各撮影デバイス１１８の認証ＤＢ１２０に関する情報を管理する情報である。
【００２３】
なお、ここでは、図１（ｃ）に示す各機能部を、ＣＰＵが制御プログラムを実行するこ

とにより実現することを想定するが、１以上の機能部を電子回路などのハードウェアで実現するよう構成してもよい。

【００２４】

＜認証データ更新処理の概要＞

図２（ａ）は、第１実施形態における認証データ更新処理の概要を示す図である。ここでは、近隣に設置された３台の撮影デバイス２０１～２０３と１台の解析サーバ２０４とでシステムが構成されている状態を想定する。例えば、撮影デバイス２０１～２０３は通路に沿って設定されており、同一人物が時間差で撮影される可能性が高い。

【００２５】

図２（ｂ）および図２（ｃ）は、撮影デバイス２０１～２０３が利用する認証ＤＢ内の認証データを例示的に示した図である。第１実施形態では、３台の撮影デバイス２０１～２０３は、共通の認証ＤＢをそれぞれの装置内に有しているものとする。

【００２６】

図２（ｂ）は、認証ＤＢの初期状態であり、図２（ｃ）は、動作を開始してから時間が経過した後の認証ＤＢの状態を示している。認証ＤＢには、対象とする人物（指名手配犯や重要人物）の顔領域の特徴量が格納されている。特に、ここでは、人物ごと、顔の方向（顔向き）ごとに特徴量が管理されている。初期状態では限定された顔向きの特徴量が格納されており、この例では、人物Ａ、人物Ｂ、人物Ｃの正面顔の特徴量が、特徴量２０６～２０８として格納されている。上述したように顔認証は顔向きの影響を大きく受けるため、初期状態では正面以外の顔向きで撮影された人物については、認証は困難である。

【００２７】

図２（ａ）において、撮影デバイス２０１が人物Ｂを撮影し、人物Ｂの正面顔に対して認証した場合を考える。撮影デバイス２０１は、人物Ｂの認証情報を解析サーバ２０４へ送信する。解析サーバ２０４は、人物Ｂについて、認証時とは異なる顔向きの特徴量を取得する。ここでは、認証された人物Ｂを追尾して得られる一連のデータ（人物追尾トラック）から、正面以外の顔向きの特徴量を取得する。そして、解析サーバ２０４は、人物Ｂについての認証データを更新するための更新情報２０５を生成する。

【００２８】

解析サーバ２０４は、生成した更新情報を、撮影デバイス２０１および、当該撮影デバイス２０１の近隣に設置されている撮影デバイス２０２、２０３へ送信する。撮影デバイス２０１～２０３は、それぞれ、更新情報を受信し、各装置内の認証ＤＢに対して更新情報に従って特徴量を追加する。

【００２９】

図２（ｃ）は、更新情報を反映後の認証ＤＢの状態を示している。人物Ｂについて、初期状態（図２（ｂ））には存在しなかった特徴量２０９、特徴量２１０が追加されている。すなわち、撮影デバイス２０１～２０３において、初期状態で登録されていた顔向きとは異なる顔向きで撮影された場合でも、人物Ｂの認証をより好適に行うことが可能になる。特に、撮影デバイス２０１の近隣に設置された撮影デバイス２０２、２０３において、時間差で撮影される可能性の高い人物Ｂについて、認証データを効率的に拡充することができる。

【００３０】

ここでは、顔向きごとに特徴量を管理するものとして説明するが、顔向き以外の撮影条件の違いで特徴量を管理しても良い。一例としては、顔の表情、付帯物（メガネ、サングラス、マスク、帽子など）、照明条件（色、角度、明度など）の違いを用いてもよい。この場合には、初期状態で登録されていた表情、照明条件とは異なる表情、照明条件下で撮影された場合の認証精度を向上させることができる。また、認証対象のオブジェクトは人物に限定されるものではなく、動物、物体等に適用してもよい。この場合には、物体の撮影方向、物体の外観の違いで特徴量を管理すればよい。

【００３１】

図３は、認証システムで利用される各種データを説明する図である。図３（ａ）は、撮

影デバイスの認証ＤＢ１２０に格納される認証データであり、図２（ｂ）や図２（ｃ）に相当するデータである。認証データには、認証対象の人物の顔領域の特徴量が格納されており、オブジェクトＩＤ３０１で人物を一意に特定可能になっている。また、１人の認証対象人物に対して、複数の顔向きの特徴量を管理可能に構成されており、顔向きごとに特徴量３０２が記録されている。顔向きのバリエーションとしては、一例として、左右方向、上下方向それぞれについて一定角度（例えば３０度）で分割した範囲で管理することが出来る。

【００３２】

図３（ｂ）および図３（ｃ）は、解析サーバのデバイス管理情報１２１に格納されるデータである。図３（ｂ）は、複数の撮影デバイスをグループ化する管理データである。例えば、同一の施設、同一の都市などの単位で撮影デバイスをグループ化することができる。すなわち、ある撮影デバイスを、当該撮影デバイスで撮影された人物を今後撮影する可能性が高い他の撮影デバイスとグループ化している。ここでは、グループを特定するグループＩＤ３０３と、グループに属する撮影デバイスを特定するカメラＩＤ３０４とをセットにしたレコードを複数含むテーブルとして構成される。

【００３３】

図３（ｃ）は、撮影デバイス内の認証ＤＢ１２０を管理するための情報である。上述したように、第１実施形態では、認証ＤＢは同一グループ内で共通化されている。そのため、グループＩＤ３０３ごとに、各オブジェクトＩＤ３０１のどの方向の特徴量が認証ＤＢ１２０に記録されているかを管理する。図３（ｃ）の例では、複数の方向３０５（方向１、方向２）に対して、認証ＤＢ１２０への特徴量の記録有無をテーブルとして管理している。ここでは、特徴量が記録されていることを「〇」で示し、記録されていないことを「×」で示している。

【００３４】

図３（ｄ）は、更新情報２０５のデータを例示的に示している。上述したように、更新情報２０５は、解析サーバの更新情報生成部１１２が生成し、撮影デバイスに送信されるデータである。更新情報２０５は、オブジェクトＩＤ３０１と、更新種別３０６、方向３０７、特徴量３０８が格納されている。更新種別３０６は認証ＤＢ１２０に対する更新の種類を示すものであり、「追加」「削除」のいずれかが指定される。

【００３５】

解析サーバ１１９で拡充されたデータを認証ＤＢ１２０に認証データを追加する場合に「追加」を指定する。一方、認証ＤＢ１２０にすでに格納されている認証データを削除する場合に「削除」を指定する。例えば、認証ＤＢ１２０から優先度の低い認証データを削除する場合に用いる。

【００３６】

方向３０７は、顔向きの識別情報であり、認証データのどの顔向きのデータを追加または削除するのかを指定する。特徴量３０８は、顔領域の特徴量であり、更新種別３０６が「追加」の場合にのみ記録される。

【００３７】

＜各装置での詳細動作＞

以下では、撮影デバイスにおけるオブジェクト認証処理、解析サーバにおける認証データ拡充処理、撮影デバイスにおける認証データ更新処理についてより詳細に説明する。

【００３８】

図４は、オブジェクト認証処理のフローチャートである。当該処理は、撮影デバイス１１８の抽出部１０３および認証部１０４において実行される。例えば、フレーム画像の受信する間隔で繰り返し実行される。

【００３９】

ステップＳ４０１では、抽出部１０３は、撮影映像のフレーム画像を撮像部１０８から受信する。ステップＳ４０２では、抽出部１０３は、認証対象のオブジェクトを抽出する。上述したように、ここでは認証対象のオブジェクトは人の顔領域であるため、Ｓ４０２

では顔領域が抽出される。なお、画像から人物の顔領域を抽出する方法については、例えば、「P.Viola, M.Jones, "Rapid Object Detection Using a Boosted Cascade of Simple Features", Computer Vision and Pattern Recognition, 2001」（以降、非特許文献１と呼ぶ）に開示される技術を利用することが出来る。非特許文献１の手法では、事前に多数の顔画像を用いて顔領域特有の局所領域の輝度差を学習しておく。その上で、入力画像を探索窓で捜査し、各探索窓の輝度差を学習データと比較することにより、顔領域であるか否かを判定する。

【００４０】

以降のＳ４０３～Ｓ４０６では、認証部１０４は、Ｓ４０２で抽出された各オブジェクトに対して認証処理を実行する。ステップＳ４０４では、認証部１０４は、抽出されたオブジェクト特徴量の算出をおこなう。顔領域の特徴量の算出には、人物の顔画像内の目・口などの器官点を求め、各器官点のＳＩＦＴ（Scale Invariant Feature Transform）特徴量を用いることができる。なお、この特徴量は一例であり、他の特徴量を用いることもできる。

【００４１】

ステップＳ４０５では、認証部１０４は、Ｓ４０４で算出した特徴量を用いて、オブジェクトの認証をおこなう。ここでは、Ｓ４０４で算出した特徴量が、認証ＤＢ１２０に登録されている何れかの重要人物の特徴量（認証データ）と同一であるかを判定する。具体的には、Ｓ４０４で算出した特徴量と認証ＤＢ１２０に含まれる各認証データを比較する。そして、類似度が所定閾値よりも高い特徴量があれば、同一人物であると判定する。類似度の算出にあたっては、各器官点のＳＩＦＴ特徴量の距離の総和を求めて正規化したものを用いるとよい。もちろん、オクルージョンなどの対応に対してロバストにするために、距離が最も大きいものを除いて距離の総和を求めて正規化し、類似度を算出してもよい。

【００４２】

ステップＳ４０７では、認証部１０４は、認証情報とフレーム画像を解析サーバ１１９に送信する。認証情報は、画像内における認証されたオブジェクトの位置、認証されたオブジェクトのオブジェクトＩＤ、カメラＩＤである。なお、同一人物が複数のフレーム画像で連続して認証された場合に、解析サーバ１１９での処理が繰り返し実施されるのを防ぐため、同一人物の認証情報については所定時間内に１回だけ送信するよう構成してもよい。すなわち、同一人物の認証情報の繰り返し送信を行わないことにより、解析サーバ１１９における処理負荷を低減することが出来る。

【００４３】

図５は、認証データ拡充処理のフローチャートである。当該処理は、解析サーバ１１９の更新情報生成部１１２において実行され、撮影デバイス１１８から認証情報を受信した場合に実行される。具体的には、撮影デバイス１１８が認証したオブジェクトについて、撮影デバイス１１８における認証時に利用した認証データとは異なる顔向き（方向）の追加認証データ生成を行う。

【００４４】

ステップＳ５０１では、更新情報生成部１１２は、撮影デバイス１１８から認証情報を受信する。すなわち、上述のＳ４０７において撮影デバイス１１８が送信する認証情報を受信する。なお、上述のＳ４０７において撮影デバイス１１８が送信するフレーム画像は別途受信し、解析サーバ１１９内（例えば記憶部１１４）に蓄積するものとする。

【００４５】

ステップＳ５０２では、更新情報生成部１１２は、デバイス管理情報１２１を参照し、図３（ｂ）に示したグループ管理情報を用いて認証情報に付与されたカメラＩＤからグループを特定する。さらに、更新情報生成部１１２は、図３（ｃ）に示した認証ＤＢ管理情報を用いて、撮影デバイス１１８で認証されたオブジェクトについて、特定したグループの認証ＤＢ１２０に格納されている認証データの方向（顔向き）を取得する。

【００４６】

ステップＳ５０３では、更新情報生成部１１２は、解析サーバ１１９内に蓄積されてい

る複数時刻のフレーム画像群を用いて、同一オブジェクトの追尾および抽出を行う。ここでは、人物追尾技術を用いて認証された人物の別フレームでの人物領域を特定し、その人物領域に対して顔領域の抽出をおこなう。

【００４７】

人物追尾処理に関しては、例えば、特開２００２－３７３３３２号公報（以降、特許文献４と呼ぶ）に開示される技術を利用することが出来る。特許文献４では、あるフレームでの人物の検出位置を用いて、次フレームでの探索位置を推定しテンプレートマッチングにより追尾を行う。ここでは、認証情報に、画像内における認証されたオブジェクトの位置が含まれているので、その位置を基準として前後のフレームでの当該オブジェクトの追尾を行うことができる。

【００４８】

ステップＳ５０４では、更新情報生成部１１２は、追尾し抽出された複数の顔領域の画像に対して顔向きの判定を行い、顔向き毎にグループ化を行う。画像から人物の顔向きを検出する方法については、例えば、「Erik Muphy-Chutorian, "Head pose estimation for driver assistance systems: A robust algorithm and experimental evaluation", in Proc. IEEE Conf. Intelligent Transportation Systems, 2007, pp.709-714」（以降、非特許文献２と呼ぶ）に開示される技術を利用することが出来る。

【００４９】

さらに、追尾し抽出された人物の顔画像群から、代表となる顔領域画像を選択する。例えば、方向ごと（例えば３０°範囲ごと）に、大きいサイズの顔領域の画像をその方向の代表画像として選択することができる。この他、ブレ、眼つぶり、口あきや、付帯物（メガネ、サングラス、マスク、帽子など）、の観点で代表画像を選択してもよいし、これらの１以上の組み合わせによる総合判定により選択してもよい。

【００５０】

ステップＳ５０５では、更新情報生成部１１２は、顔向き（方向）ごとに選択された代表画像から特徴量を抽出する。より具体的には、追加拡充が必要な方向の代表画像の特徴量を抽出する。現在の認証ＤＢ１２０に格納されていない方向の代表画像の特徴量を抽出することで、現在の認証ＤＢ１２０で認証が難しい方向の認証データを拡充することができる。

【００５１】

ステップＳ５０６では、更新情報生成部１１２は、Ｓ５０５で抽出した１以上の特徴量を認証ＤＢ１２０に追加した際に、認証ＤＢ１２０内の特徴量の個数が所定の上限値以下に収まるかを判定する。上限値以下に収まる場合にはＳ５０７に進む。一方、上限値を超えると判定された場合にはＳ５０８へ進む。

【００５２】

上述したように、認証ＤＢ１２０は撮影デバイス１１８内で利用されるため、格納する特徴量の個数が多すぎると、認証処理の実行時間が長くなり実時間での処理が行えなくなる。このため、認証ＤＢ１２０に格納する特徴量の個数には上限値が予め設定されているのである。

【００５３】

ステップＳ５０７では、更新情報生成部１１２は、Ｓ５０５で抽出した全ての特徴量を追加対象として指定した更新情報を生成する。

【００５４】

ステップＳ５０８では、更新情報生成部１１２は、認証ＤＢ内に登録されている特徴量とＳ５０５で抽出した代表画像の特徴量に対して、優先度を付与する。ここでは、処理対象となっているオブジェクトについて、認証ＤＢ内の特徴量とＳ５０４で選択した代表画像の方向の分散が大きくなるように、優先度を付与することができる。例えば、方向の類似度で区分けを行い、区分けごとに１つの方向を選んで順に優先度を付与していくことで、優先度の高いものを選択した場合の方向の分散を大きくすることができる。最後に、優先度の高い順に認証ＤＢ内の上限に収まる個数の特徴量を選択する。

【００５５】
同時に複数の人物が認証された場合には、Ｓ５０６において上限を超えると判定される可能性が高くなる。そのため、複数のオブジェクト間で追加の認証データの個数を制御する必要がある。この問題を解決するために、Ｓ５０８において、現在処理対象となっているオブジェクトだけでなく、認証ＤＢ内の全てのオブジェクトについて、優先度を付与するよう構成しても良い。例えば、オブジェクトごとの追加の認証データの個数なるべく均一になるように優先度を付与していくことで、追加の認証データにおけるオブジェクトの多様性を確保することができる。また、認証対象の人物の重要度に差がある場合には、その重要度を用いて優先度を制御してもよい。重要度の高い人物の認証データの優先度を高くすることで、重要人物に対する認証精度を優先して上げることができる。

【００５６】
さらに、認証された時刻が最近であるオブジェクトの優先度をより高くするような補正をおこなっても良い。この場合は、より出現確率の高い人物の認証データを多くすることができる。

【００５７】
ステップＳ５０９では、更新情報生成部１１２は、Ｓ５０５で抽出した特徴量のうち、Ｓ５０８において優先度に従って選択された特徴量を追加対象として指定する。すなわち、相対的に優先度が高い特徴量から順に追加指定する。ステップＳ５１０では、更新情報生成部１１２は、認証ＤＢ内の特徴量のうち、Ｓ５０８で選択されなかった優先度の低い方向の特徴量を削除対象として指定する。そして、Ｓ５０９及びＳ５１０での指定に応じた更新情報を生成する。

【００５８】
ステップＳ５１１では、更新情報生成部１１２は、生成した更新情報を同一グループ内の複数の撮影デバイス１１８に送信する。ステップＳ５１２では、更新情報生成部１１２は、生成した更新情報に従って、図３（ｃ）に示す認証ＤＢ管理情報を更新する。

【００５９】
上述したように、認証データ拡充処理は、撮影デバイス１１８から認証情報を受信した場合に実行することを想定している。ただし、認証情報を受信した直後に行う代わりに、受信してから所定の時間が経過した後に実行するよう構成しても良い。これは、認証直後よりある程度時間が経過した後の方が、追尾により対象のフレーム数が増えており、顔向きのバリエーションをより多く増やすことができるからである。また、認証情報を受信した直後と、受信してから所定の時間が経過した後の両方で実行するよう構成してもよい。

【００６０】
また、上述の説明では、顔向きデータの拡充方法として人体追尾技術を用いるものとしたが、顔向きデータの拡充方法はこれに限定されるものではない。例えば、認証対象人物について様々な顔向き画像を格納した大規模なＤＢ（不図示）を用意しておき、解析サーバ１１９は、大規模ＤＢにアクセスし対象人物の認証時とは異なる顔向きの画像を取得しても良い。また、２次元画像から顔の３次元モデル展開をおこなう技術を用いて、認証時の顔画像データから異なる顔向きの画像を生成してもよい。

【００６１】
図６は、認証データ更新処理のフローチャートである。当該処理は、撮影デバイス１１８の更新部１０５において実行される。より具体的には、撮影デバイス１１８が、解析サーバ１１９から更新情報を受信した場合に実行される。

【００６２】
ステップＳ６０１では、更新部１０５は、更新情報を解析サーバ１１９から受信する。ステップＳ６０２では、更新部１０５は、更新情報において削除対象として記録された特徴量を認証ＤＢ１２０から削除する。ステップＳ６０３では、更新部１０５は、更新情報において追加対象として記録された特徴量を認証ＤＢ１２０に追加する。

【００６３】
なお、さらに、出現確率が低くなったオブジェクトの認証データを削除する構成にして

も良い。例えば、対象が指名手配犯である場合、逮捕された後は監視カメラに映ることはなくなる。また、対象がイベントの要人である場合、イベント期間終了後には映る確率は低くなる。このような場合に、解析サーバ１１９の入力部１１５を介して、出現確率が低くなったオブジェクトをユーザが手動で指定する。これにより、指定したオブジェクトの特徴量の削除を更新情報に設定し、同じグループに含まれる１以上の撮影デバイス１１８に送信することができる。

【００６４】

もちろん、出現確率が低くなったオブジェクトを手動で指定するのではなく、自動で判定するよう構成することもできる。例えば、イベントのタイムテーブルが判っている場合には、要人が参加するイベントの終了後には、出現確率を下げるようにすればよい。

【００６５】

また、出現確率を、人物や物体の時空間における移動予測に基づいて行うように構成することもできる。移動予測方法の一例としては、映像から人物の移動軌跡を計測し、主要な移動パターンを抽出することで予測をおこなうことができる。さらに、認証対象が指名手配犯の場合には、逮捕された場合に出現確率を下げるようにしてもよい。映像を解析して逮捕特有の動きを検知した場合に、逮捕されたと判定するように自動化することもできる。

【００６６】

特徴量を削除する際には、全ての方向の特徴量を削除するのではなく、基本となる方向（例えば正面方向）のみを残すようにしてもよい。また、元から格納されていた特徴量であるか、後から更新情報によって追加された特徴量であるかを判定する情報を併せて管理するよう構成しておき、追加された特徴量を特定して削除するようにしてもよい。

【００６７】

あるいは、認証データの各特徴量の更新日時を管理するよう構成しておき、更新日時の古い特徴量を削除するようにしてもよい。これによって、日時の経過によって同一人物の特徴が変化した場合に、新しい特徴量に優先して置き換えることができる。

【００６８】

なお、上述の説明では、図３（ｃ）に示す認証ＤＢ管理情報において、方向ごとに特徴量の格納有無を管理するものとした。ただし、格納有無の代わりに記憶数（登録数）を管理し、図５のＳ５０５において記憶数の少ない方向の代表画像を選択するよう構成してもよい。

【００６９】

また、上述の説明では、解析サーバ１１９は１台のみ設置する場合を想定したが、複数設置することも可能である。その場合、各撮影デバイス１１８は予め１つの解析サーバ１１９に対応付けられており、対応付けされた解析サーバ１１９に映像データおよび認証情報を送信する。なお、近隣同士の撮影デバイス１１８を分類するグループは、撮影デバイス１１８と解析サーバ１１９の対応付けとは非依存に設定することができる。例えば、１つの解析サーバ１１９が処理を担当する撮影デバイス１１８は１つのグループの一部分であってもよいし、複数のグループから構成されてもよい。解析サーバ１１９上の認証ＤＢ管理情報（図３（ｃ））およびグループ管理情報（図３（ｂ））には、すべての撮影デバイス１１８の情報が管理されており、解析サーバ１１９は任意の撮影デバイス１１８に更新情報を送信することが可能である。

【００７０】

さらに、撮影デバイス１１８と解析サーバ１１９の処理分担は、上述の形態に限定されるものではない。例えば、上述の説明では、オブジェクト認証処理を撮影デバイス１１８で行うものとしたが、撮影デバイス１１８は撮像部１０８のみを持つ構成としてもよい。その場合、抽出部１０３、認証部１０４、更新部１０５、認証ＤＢ１２０を不図示の別サーバ（認証サーバ）に配置してもよい。この場合には、撮影デバイス１１８から、認証サーバに撮影映像を送り、認証サーバで図４に示すオブジェクト認証処理を行ったうえで、解析サーバに情報を送信する。解析サーバで図５に示す認証データ拡充処理を実施し、最

後に認証サーバで図６に示す認証データ更新処理を行う。また、上記認証サーバと解析サーバを１つのサーバで兼ねるよう構成してもよい。その場合、解析サーバ１１９内に認証ＤＢ１２０を保有し、解析サーバ１１９でオブジェクト認証処理を行う。これらの構成によれば、解析サーバ１１９が生成した更新情報を撮影デバイス１１８へ送信する必要がないため、通信量を減らすことができる。

【００７１】

以上説明したとおり第１実施形態によれば、認証システムにおいて、解析サーバは、初期の認証ＤＢ内にはない顔向きの認証データを追加拡充する。この構成により、それぞれの撮影デバイスで今後映り込む可能性の高い人物の多様な顔向きでの認証精度を効率的に向上させることができる。特に、各撮影デバイスの撮影条件を考慮し、各撮影デバイスに適した認証用データを動的に拡充することにより、撮影デバイス等の低資源環境においても実時間で顔認証処理をおこなうことが可能となる。

【００７２】

（第２実施形態）

本発明に係る画像処理装置の第２実施形態として、第１実施形態と同様に、顔画像により映像内の人物を認証する認証システムを例に挙げて以下に説明する。上述の第１実施形態では、複数の撮影デバイス１１８をグループ化し、グループ内で同一の認証ＤＢ１２０を利用した。しかし、同一グループ内であっても、撮影デバイス１１８ごとに映りやすい顔向きが異なる場合がある。そこで、第２実施形態では、個々の撮影デバイスの認証ＤＢに対して個別に認証データを拡充する。

【００７３】

＜システム構成＞

図７は、第２実施形態に係る認証システムに含まれる各装置の構成を示す図である。図７（ａ）は、撮影デバイスのハードウェア構成を示しており、図７（ｂ）は、解析サーバのハードウェア構成を示している。また、図７（ｃ）は、撮影デバイス及び解析サーバのソフトウェア構成を示している。以下では、主に第１実施形態と異なる部分について説明を行い、同一の機能構成については説明を省略する。

【００７４】

解析サーバ１１９内のＲＯＭ１０２は、頻度算出部７０１を実現するための制御プログラムが更に格納されている。頻度算出部７０１は、撮影デバイス１１８ごとに、映りやすいオブジェクトの方向を算出し、その情報をデバイス管理情報１２１に記録する機能部である。

【００７５】

＜認証データ更新処理の概要＞

図８（ａ）は、第２実施形態における認証データ更新処理の概要を示す図である。ここでは、第１実施形態と同様に、近隣に設置された３台の撮影デバイス２０１～２０３と１台の解析サーバ２０４とでシステムが構成されている状態を想定する。ただし、上述したように、各認証ＤＢに対して個別に認証データの更新を行う点が第１実施形態と異なる。

【００７６】

図８（ｂ）は、認証ＤＢ１２０の初期状態であり、撮影デバイス２０１～２０３の認証ＤＢ１２０は、初期状態は共通であるものとする。初期状態では限定された顔向きの特徴量が格納されており、この例では、人物Ａ、人物Ｂ、人物Ｃの正面顔の特徴量が、特徴量２０６～２０８として格納されている。

【００７７】

図８（ａ）において、撮影デバイス２０１が人物Ｂを撮影し、人物Ｂの正面顔に対して認証した場合を考える。撮影デバイス２０１は、人物Ｂの認証情報を解析サーバ２０４へ送信する。解析サーバ２０４は、人物Ｂについて、認証時とは異なる顔向きの特徴量を取得する。ここでは、認証された人物Ｂを追尾して得られる一連のデータ（人物追尾トラック）から、正面以外の顔向きの特徴量を取得する。そして、解析サーバ２０４は、人物Ｂについての認証データを更新するための更新情報８０１～８０３を生成する。更新情報８

０１～８０３は、撮影デバイス２０１～２０３において、それぞれ映りやすい方向（顔向き）の認証データを選択したものである。例えば、撮影デバイス２０２において、やや右向き方向の顔が映りやすい場合には、やや右向き方向の顔を追加した更新情報８０２が撮影デバイス２０２向けに生成される。

【００７８】

解析サーバ２０４は、生成した更新情報８０１～を、それぞれ、撮影デバイス２０１～２０３へ送信する。撮影デバイス２０１～２０３は、それぞれの更新情報を受信し、各装置内の認証ＤＢに対して更新情報に従って特徴量を追加する。

【００７９】

図８（ｃ）～図８（ｅ）は、それぞれ、撮影デバイス２０１～２０３における更新情報反映後の認証ＤＢの状態を示している。人物Ｂについて、初期状態には存在しなかった特徴量８０４、特徴量８０５、特徴量８０６が追加されている。

【００８０】

これにより、撮影デバイス２０１で撮影され、時間差で撮影デバイス２０２と撮影デバイス２０３でも撮影される可能性の高い人物Ｂについて、各装置で撮影されやすい方向の認証データを拡充することができる。初期状態で登録されていた顔向きとは異なる顔向きで撮影された場合でも、重要人物の認証を高精度におこなうことが可能になる。

【００８１】

図９は、認証システムで利用される各種データを説明する図である。図９（ａ）は、撮影デバイス内の認証ＤＢ１２０を管理するためのテーブルである。ここでは、撮影デバイス１１８ごとに認証ＤＢが異なるため、カメラＩＤ３０４ごとに、各オブジェクトＩＤ３０１のどの方向の特徴量が認証ＤＢ１２０に記録されているかを管理する。

【００８２】

図９（ｂ）は、撮影デバイス１１８ごとに映りやすい方向（方向ごとの撮影頻度）の情報を管理するテーブルである。カメラＩＤ３０４ごとに、計算期間９０１、頻度９０２が記録されている。一例としては、所定の時間間隔ごとに顔向きの撮影回数を計測して、頻度９０２として記録することができる。

【００８３】

＜各装置での詳細動作＞

以下では、解析サーバにおける顔向き頻度算出処理、及び、解析サーバにおける認証データ拡充処理についてより詳細に説明する。なお、撮影デバイスにおけるオブジェクト認証処理、撮影デバイスにおける認証データ更新処理については第１実施形態と同様であるため説明は省略する。

【００８４】

図１０は、顔向き頻度算出処理のフローチャートである。当該処理は、解析サーバ１１９の頻度算出部７０１により実行される。

【００８５】

ステップＳ１００１では、解析サーバ１１９は、フレーム画像を撮影デバイス１１８から受信する。ステップＳ１００２では、解析サーバ１１９は、受信したフレーム画像からオブジェクトを抽出する。ここでは顔領域の抽出をおこなう。

【００８６】

ステップＳ１００３では、解析サーバ１１９は、抽出した顔領域の画像における顔の方向を判定する。画像から人物の顔領域を抽出する方法および顔向きの判定方法については、第１実施形態と同様に、非特許文献１や非特許文献２に示す技術を利用することが出来る。ステップＳ１００４では、解析サーバ１１９は、図９（ｂ）に示す頻度情報を更新する。具体的には、現在の期間９０１に対応する頻度９０２のカラムに、今回判定した顔向き情報を加算する。

【００８７】

ステップＳ１００５では、解析サーバ１１９は、頻度情報に所定の時間以上古い情報があるかを判定する。古い情報があると判定された場合には、Ｓ１００６に進む。古い情報

がないと判定された場合は、本処理を終了する。ステップＳ１００６では、解析サーバ１１９は、所定の時間以上古いと判定された頻度情報を削除した上で、本処理を終了する。このように所定の時間以上古い情報を削除することで、最新の状況に適した頻度情報のみを残すことができる。

【００８８】

次に、第２実施形態における更新情報生成部１１２の処理の変更点について述べる。第２実施形態では、Ｓ５０２において、図９（ａ）に示した認証ＤＢ管理情報を用いて、認証されたオブジェクトについて、グループ内の撮影デバイス１１８の認証ＤＢ１２０に格納されている認証データの方向を撮影デバイス１１８ごとに取得する。

【００８９】

また、ステップＳ５０５では、グループ内の撮影デバイス１１８ごとに、図９（ｂ）の頻度情報を参照し、映りやすい方向（顔向き）を判定する。一例として、映りやすい方向は、各方向の頻度の全方向の頻度に対する割合（出現確率）として求めることができる。各撮影デバイス１１８での映りやすい方向と、認証ＤＢ１２０内の認証データの方向を照合し、所定以上の映りやすさであるにもかかわらず、認証ＤＢ１２０内に特徴量が格納されていない方向を拡充が必要な方向として選択する。ステップＳ５０６以降の処理も同様に撮影デバイス１１８ごとに行うものとする。

【００９０】

以上説明したとおり第２実施形態によれば、認証システムにおいて、解析サーバは、初期の認証ＤＢ内にはない顔向きの認証データを追加拡充する。特に、各撮影デバイスにおける映りやすい方向を算出し、それぞれの撮影デバイスの認証ＤＢを個別に更新する。この構成により、それぞれの撮影デバイスで今後映り込む可能性の高い人物の多様な顔向きでの認証精度を効率的に向上させることができる。

【００９１】

なお、顔向き以外の撮影条件の違いに対して頻度情報を適用してもよい。また、顔向きを判定する方法は、顔向きの出現回数をカウントする他に、人物追尾技術を用いて取得した映像内の人物の移動軌跡の流れの量から算出するようにしてもよい。例えば、多くの移動軌跡が上から下方向に流れている場合には正面顔、左から右に流れている場合には左向きの横顔の出現確率が高いと判定できる。

【００９２】

（その他の実施例）

本発明は、上述の実施形態の１以上の機能を実現するプログラムを、ネットワーク又は記憶媒体を介してシステム又は装置に供給し、そのシステム又は装置のコンピュータにおける１つ以上のプロセッサーがプログラムを読出し実行する処理でも実現可能である。また、１以上の機能を実現する回路（例えば、ＡＳＩＣ）によっても実現可能である。

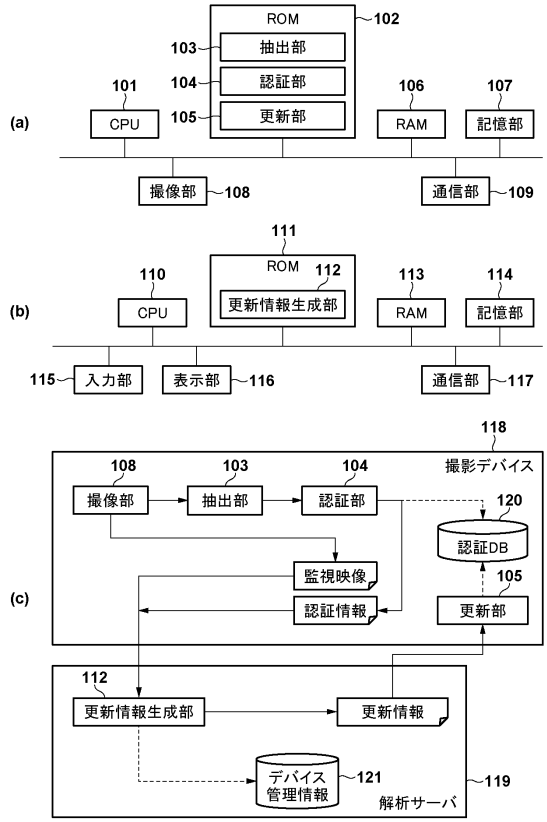
【符号の説明】

【００９３】

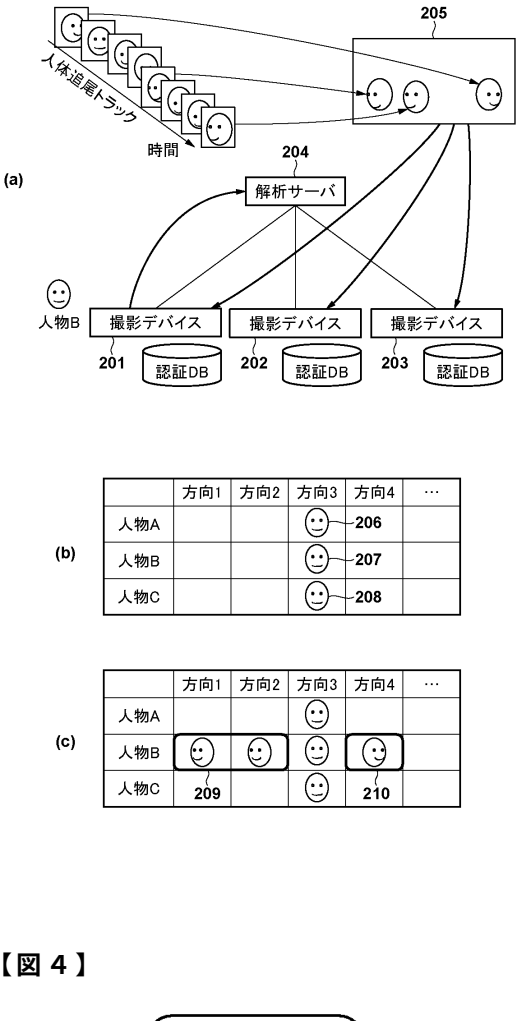
１０１　ＣＰＵ；　１０２　ＲＯＭ；　１０３　抽出部；　１０４　認証部；　１０５　更新部；　１０６　ＲＡＭ；　１０７　記憶部；　１０８　撮像部；　１０９　通信部；　１１０　ＣＰＵ；　１１１　ＲＯＭ；　１１２　更新情報生成部；　１１３　ＲＡＭ；　１１４　記憶部；　１１５　入力部；　１１６　表示部；　１１７　通信部

【図面】

【図１】



【図２】



(b)

	方向1	方向2	方向3	方向4	…
人物A					
人物B					
人物C					

206 207 208

(c)

	方向1	方向2	方向3	方向4	…
人物A					
人物B					
人物C	209			210	

【図３】

(a)

オブジェクトID	特徴量(方向1)	特徴量(方向2)	…
Object001	xxx		
Object002	xxx	xxx	
:	:	:	:

(b)

グループID	カメラID
Group001	Camera001
Group001	Camera002
:	:

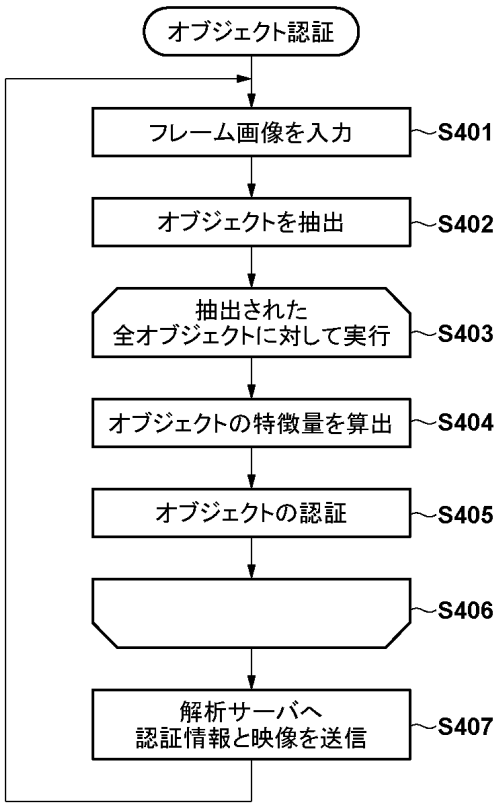
(c)

グループID	オブジェクトID	方向1	方向2	…
Group001	Object001	○	×	
Group002	Object002	○	○	
Group003	:	:	:	:

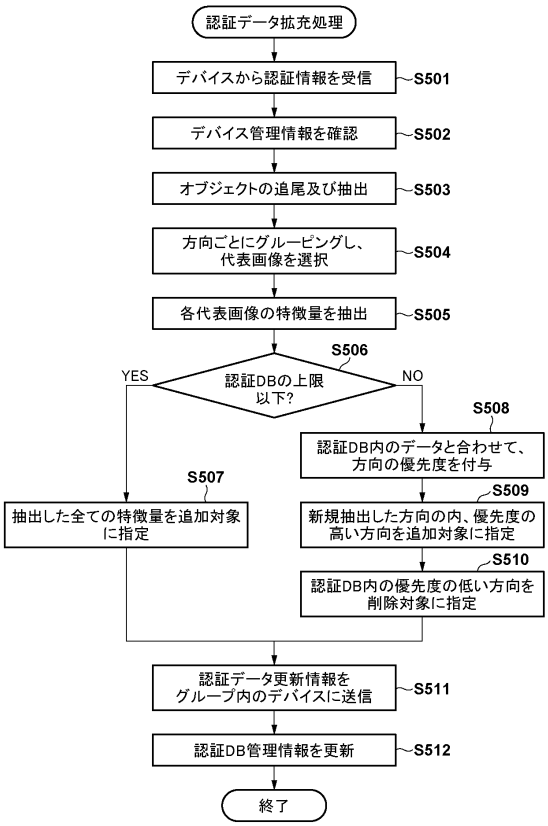
(d)

オブジェクトID	更新種別	方向	特徴量
Object001	削除	方向1	
Object001	追加	方向2	xxx
:			:

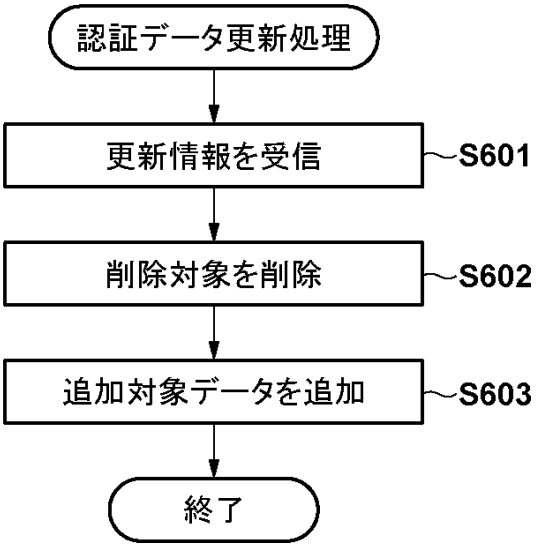
【図４】



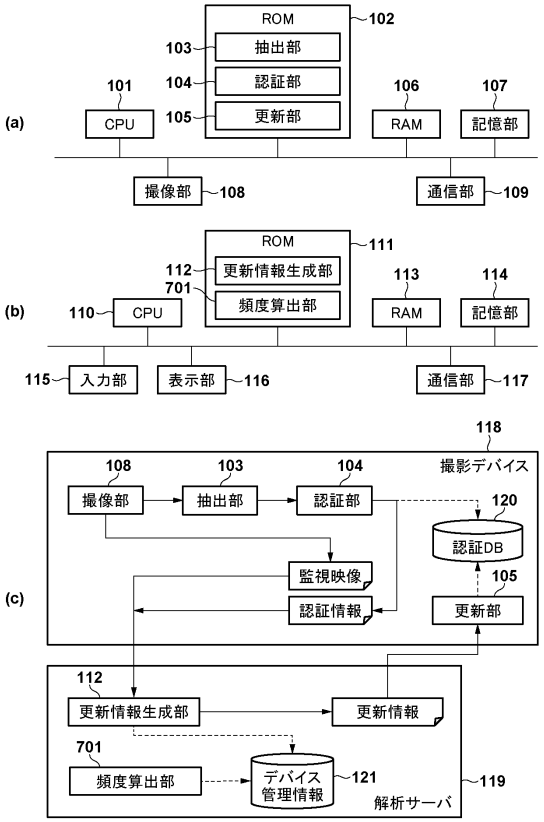
【図５】


認証データ拡充処理
デバイスから認証情報を受信
S501
デバイス管理情報を確認
S502
オブジェクトの追尾及び抽出
S503
方向ごとにグルーピングし、代表画像を選択
S504
各代表画像の特徴量を抽出
S505
S506
認証DBの上限以下?
YES
NO
S507
抽出した全ての特徴量を追加対象に指定
S508
認証DB内のデータと合わせて、方向の優先度を付与
S509
新規抽出した方向の内、優先度の高い方向を追加対象に指定
S510
認証DB内の優先度の低い方向を削除対象に指定
認証データ更新情報をグループ内のデバイスに送信
S511
認証DB管理情報を更新
S512
終了

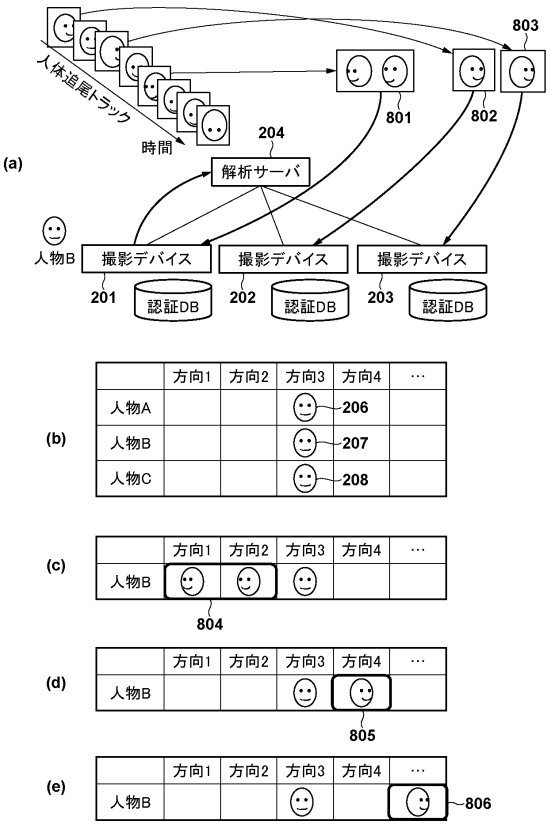
【図６】


認証データ更新処理
更新情報を受信
S601
削除対象を削除
S602
追加対象データを追加
S603
終了

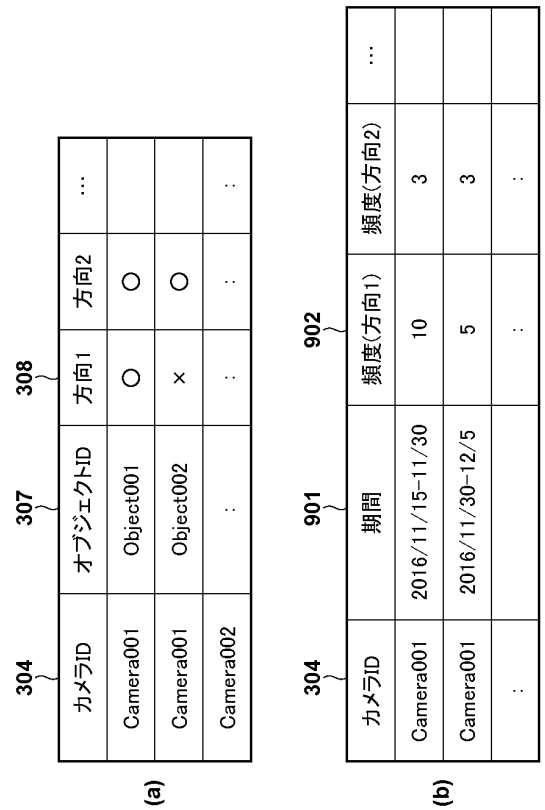
【図７】


(a)
ROM
102
103
抽出部
104
認証部
105
更新部
101
CPU
106
RAM
107
記憶部
撮像部
108
通信部
109
(b)
ROM
111
112
更新情報生成部
701
頻度算出部
110
CPU
113
RAM
114
記憶部
115
入力部
表示部
116
通信部
117
(c)
118
撮影デバイス
108
撮像部
103
抽出部
104
認証部
120
認証DB
監視映像
認証情報
105
更新部
112
更新情報生成部
更新情報
701
頻度算出部
デバイス管理情報
121
119
解析サーバ

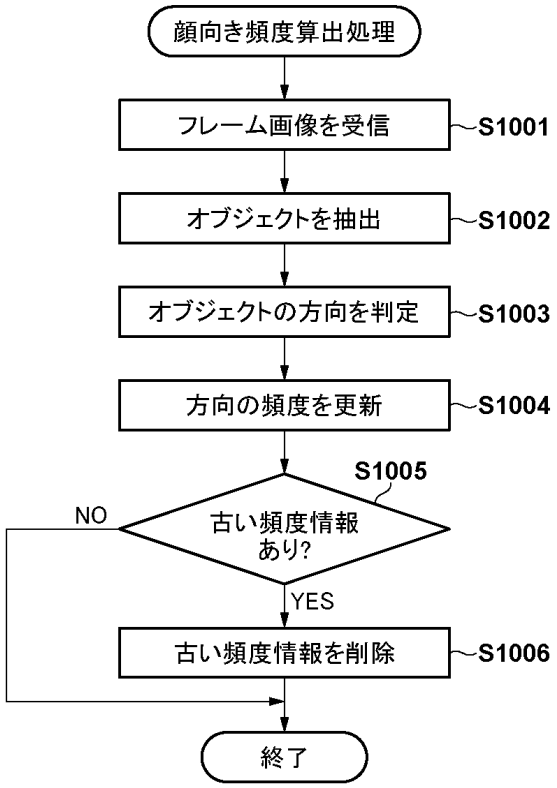
【図８】


(a)
人体追尾トラック
時間
803
801
802
204
解析サーバ
人物B
撮影デバイス
撮影デバイス
撮影デバイス
201
認証DB
202
認証DB
203
認証DB
(b)
方向1
方向2
方向3
方向4
人物A
206
人物B
207
人物C
208
(c)
人物B
804
(d)
805
(e)
806

【図９】


304
307
308
カメラID
オブジェクトID
方向1
方向2
…
Camera001
Object001
○
○
Camera001
Object002
×
○
Camera002
901
902
期間
頻度(方向1)
頻度(方向2)
2016/11/15−11/30
10
3
2016/11/30−12/5
5
3
(a)
(b)

【図１０】


顔向き頻度算出処理
フレーム画像を受信
S1001
オブジェクトを抽出
S1002
オブジェクトの方向を判定
S1003
方向の頻度を更新
S1004
S1005
古い頻度情報
あり?
NO
YES
古い頻度情報を削除
S1006
終了

フロントページの続き

(56)参考文献　特開２０１７－２２４１８６（ＪＰ，Ａ）
特開２０１７－３７３７５（ＪＰ，Ａ）
特開２０１７－３３５４７（ＪＰ，Ａ）
特開２０１４－１６４６９７（ＪＰ，Ａ）
特開２０１４－１０６７９４（ＪＰ，Ａ）
特開２０１０－２３８１８１（ＪＰ，Ａ）
特開２００９－２５８９９０（ＪＰ，Ａ）
特開２００８－１９９５４９（ＪＰ，Ａ）
特開２００７－１１５０７２（ＪＰ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｔ　７／００
Ｈ０４Ｎ　７／１８
Ｇ０６Ｆ　１６／００