(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6190041号
(P6190041)

(45)発行日　平成29年8月30日(2017.8.30)　(24)登録日　平成29年8月10日(2017.8.10)

(51)Int.Cl.		F I		
G06F 17/30	(2006.01)	G06F	17/30	120A
G06Q 50/26	(2012.01)	G06F	17/30	170B
G06F 21/62	(2013.01)	G06F	17/30	350C
G06F 21/32	(2013.01)	G06Q	50/26	
		G06F	21/62	354

請求項の数 11　(全 26 頁)　最終頁に続く

(21)出願番号　特願2016-511182(P2016-511182)
(86)(22)出願日　平成26年3月31日(2014.3.31)
(86)国際出願番号　PCT/JP2014/059443
(87)国際公開番号　WO2015/151155
(87)国際公開日　平成27年10月8日(2015.10.8)
審査請求日　平成28年9月12日(2016.9.12)

(73)特許権者　000001122
株式会社日立国際電気
東京都港区西新橋二丁目１５番１２号
(72)発明者　伊藤　渡
東京都小平市御幸町３２番地　株式会社日立国際電気内

審査官　齊藤　貴孝

最終頁に続く

(54)【発明の名称】安否確認システム及び秘匿化データの類似検索方法

(57)【特許請求の範囲】

【請求項１】

複数の標本データを保存する第１サーバと、前記第１サーバにアクセスする第２サーバとを備えた秘匿化データの類似検索方法であって、

前記第１サーバが、

前記複数の標本データを、標本データ空間において少なくとも局所的に距離保存されるような写像で秘匿化する第１ステップと、

前記秘匿化された標本データと任意データの対を、該秘匿化された標本データ自体に基づいてクラスタリングしてデータベースに記録する第２ステップと、を実行し、

前記第２サーバが、

クエリデータを、前記標本データにした方法と同じ方法で秘匿化する第３ステップと、

前記秘匿化されたクエリデータに基づいて、クエリデータに類似する標本データが記録されているクラスタを特定する第４ステップと、

前記特定されたクラスタから、前記秘匿化された標本データと前記秘匿化されたクエリデータの間の距離の計算によって、前記クエリデータに類似する１つの標本データを特定し、該標本データと対の任意データにアクセスする第５ステップと、を実行し、

前記第１ステップおよび前記第３ステップにおけるデータの秘匿化は、前記データをそのデータ空間上で量子化するサブステップと、前記データから、前記量子化されたデータを減算して残差を得るサブステップと、前記量子化されたデータを暗号学的ハッシュ関数に入力し、ハッシュ値を得るサブステップと、を有し、前記ハッシュ値と前記残差の組を

秘匿化されたデータとして出力するものであり、
前記第１サーバによる前記クラスタリングは、前記秘匿化された標本データの前記ハッシュ値の部分に基づいて、該ハッシュ値とクラスタとを１対１または多対１に対応付けるものであることを特徴とする秘匿化データの類似検索方法。
【請求項２】
複数の標本データを保存する第１サーバと、前記第１サーバにアクセスする第２サーバとを備えた秘匿化データの類似検索方法であって、
前記第１サーバが、
前記複数の標本データを、標本データ空間において少なくとも局所的に距離保存されるような写像で秘匿化する第１ステップと、
前記秘匿化された標本データと任意データの対を、該秘匿化された標本データ自体に基づいてクラスタリングしてデータベースに記録する第２ステップと、を実行し、
前記第２サーバが、
クエリデータを、前記標本データにした方法と同じ方法で秘匿化する第３ステップと、
前記秘匿化されたクエリデータに基づいて、クエリデータに類似する標本データが記録されているクラスタを特定する第４ステップと、
前記特定されたクラスタから、前記秘匿化された標本データと前記秘匿化されたクエリデータの間の距離の計算によって、前記クエリデータに類似する１つの標本データを特定し、該標本データと対の任意データにアクセスする第５ステップと、を実行し、
前記第１ステップおよび前記第３ステップにおけるデータの秘匿化は、与えられた特定の数に基づいて、前記データの要素数に対応する列数のランダムプロジェクション（ＲＰ）行列を生成するサブステップと、前記データを列ベクトルに見立て、ＲＰ行列を前から掛け算して、秘匿化されたデータを得るサブステップと、を有し、
前記第２サーバの前記データは、ベクトル空間の全域において実質的に距離保存されて前記秘匿化されたデータの空間へ写像されることを特徴とする秘匿化データの類似検索方法。
【請求項３】
前記ＲＰ行列は、ユニタリ行列であることを特徴とする請求項２記載の秘匿化データの類似検索方法。
【請求項４】
複数の標本データを保存する第１サーバと、前記第１サーバにアクセスする第２サーバとを備えた秘匿化データの類似検索方法であって、
前記第１サーバが、
前記複数の標本データを、標本データ空間において少なくとも局所的に距離保存されるような写像で秘匿化する第１ステップと、
前記秘匿化された標本データと任意データの対を、該秘匿化された標本データ自体に基づいてクラスタリングしてデータベースに記録する第２ステップと、を実行し、
前記第２サーバが、
クエリデータを、前記標本データにした方法と同じ方法で秘匿化する第３ステップと、
前記秘匿化されたクエリデータに基づいて、クエリデータに類似する標本データが記録されているクラスタを特定する第４ステップと、
前記特定されたクラスタから、前記秘匿化された標本データと前記秘匿化されたクエリデータの間の距離の計算によって、前記クエリデータに類似する１つの標本データを特定し、該標本データと対の任意データにアクセスする第５ステップと、を実行し、
前記第１ステップおよび前記第３ステップにおけるデータの秘匿化は、前記データを列ベクトルに見立て、そのベクトル空間において局所的に、距離が小さいほどハミング長が小さくなるように該データを符号化する第１サブステップと、該符号化されたデータに基づいて、所定の規則でランダムされたランダムプロジェクション（ＲＰ）行列を生成する第２サブステップと、列ベクトルに見立てた前記データに、ＲＰ行列を前から掛け算して、秘匿化されたデータを得る第３サブステップと、を有し、

前記第１サーバによる前記クラスタリングは、前記秘匿化された標本データを、該秘匿化された標本データの空間での互いの距離が小さいものが同じクラスタに集まるように行うことを特徴とする秘匿化データの類似検索方法。

【請求項５】

前記第１サブステップの符号化には、局所性鋭敏型ハッシュ、ベクトル量子化、誤り訂正符号、距離保存ランレングス制限符号、順列符号、距離保存マップ符号、ランクモジュレーション符号、グレイ符号の１つ或いは複数の組み合わせを用いることを特徴とする請求項４記載の秘匿化データの類似検索方法。

【請求項６】

複数の標本データを保存する第１サーバと、前記第１サーバにアクセスする第２サーバとを備えた秘匿化データの類似検索方法であって、

前記第１サーバが、

前記複数の標本データを、標本データ空間において少なくとも局所的に距離保存されるような写像で秘匿化する第１ステップと、

前記秘匿化された標本データと任意データの対を、該秘匿化された標本データ自体に基づいてクラスタリングしてデータベースに記録する第２ステップと、を実行し、

前記第２サーバが、

クエリデータを、前記標本データにした方法と同じ方法で秘匿化する第３ステップと、

前記秘匿化されたクエリデータに基づいて、クエリデータに類似する標本データが記録されているクラスタを特定する第４ステップと、

前記特定されたクラスタから、前記秘匿化された標本データと前記秘匿化されたクエリデータの間の距離の計算によって、前記クエリデータに類似する１つの標本データを特定し、該標本データと対の任意データにアクセスする第５ステップと、を実行し、

前記第１ステップにおける標本データの秘匿化は、前記標本データを、各要素の２進数表現における上位ビットと下位ビットとを分離する方法で２分割する第１サブステップと、前記２分割で得られた前記上位ビットのデータを、要素毎にグレイ符号化する第２サブステップと、１つの乱数を発生する第３サブステップと、前記乱数に基づいて、所定の規則で前記グレイ符号の一部を改変する第４サブステップと、前記乱数に基づいて、前記２分割で得られた前記下位ビットのデータを改変する第５サブステップと、前記改変された下位ビットのデータを列ベクトルに見立て、前記改変されたグレイ符号に基づいて生成したランダムプロジェクション（ＲＰ）行列を前から掛け算して、ランダム投影された下位ビットのデータを得る第６サブステップと、前記改変されたグレイ符号を誤り訂正符号化し、冗長シンボルを得る第７サブステップと、前記ランダム投影された下位ビットのデータと、前記冗長シンボルを連結して秘匿化されたデータを得る第８サブステップと、を有することを特徴とする秘匿化データの類似検索方法。

【請求項７】

複数の標本データを保存する第１サーバと、前記第１サーバにアクセスする第２サーバとを備えた秘匿化データの類似検索方法であって、

前記第１サーバが、

前記複数の標本データを、標本データ空間において少なくとも局所的に距離保存されるような写像で秘匿化する第１ステップと、

前記秘匿化された標本データと任意データの対を、該秘匿化された標本データ自体に基づいてクラスタリングしてデータベースに記録する第２ステップと、を実行し、

前記第２サーバが、

クエリデータを、前記標本データにした方法と同じ方法で秘匿化する第３ステップと、

前記秘匿化されたクエリデータに基づいて、クエリデータに類似する標本データが記録されているクラスタを特定する第４ステップと、

前記特定されたクラスタから、前記秘匿化された標本データと前記秘匿化されたクエリデータの間の距離の計算によって、前記クエリデータに類似する１つの標本データを特定し、該標本データと対の任意データにアクセスする第５ステップと、を実行し、

前記第３ステップにおけるクエリデータの秘匿化は、前記クエリデータを、各要素の２進数表現における上位ビットと下位ビットとを分離する方法で２分割する第１サブステップと、前記２分割で得られた前記上位ビットのデータを、要素毎にグレイ符号化する第２サブステップと、乱数として発生されうる全通りの数から試行する１つを決める第３サブステップと、前記試行する１つの数に基づいて、所定の規則で前記グレイ符号の一部を改変する第４サブステップと、前記改変されたグレイ符号を誤り訂正符号化し、冗長シンボルを得る第５サブステップと、前記冗長シンボルを用いて、改変される前の前記グレイ符号を誤り訂正復号化する第６サブステップと、前記誤り訂正復号化で訂正されたビットの位置に基づいて、前記２分割で得られた前記下位ビットのデータを改変する第７サブステップと、前記改変された下位ビットのデータを列ベクトルに見立て、前記改変されたグレイ符号に基づいて生成したランダムプロジェクション（ＲＰ）行列を前から掛け算して、ランダム投影された下位ビットのデータを得る第８サブステップと、を有し、

前記ランダム投影された下位ビットのデータと、前記冗長シンボルを連結して秘匿化されたデータを得る第９サブステップと、を有することを特徴とする秘匿化データの類似検索方法。

【請求項８】

前記第５サブステップの前記誤り訂正符号化は、前記グレイ符号が改変されうるビットの数の２倍に１を加えた数以上の誤り訂正能力を有し、前記第４ステップのクラスタの特定は、クエリデータに類似する標本データが記録されている可能性のあるクラスタを、前記第３サブステップの試行回数より少ない数に絞り込むものであることを特徴とする請求項７記載の秘匿化データの類似検索方法。

【請求項９】

複数の標本データを保存する第１サーバと、前記第１サーバにアクセスする第２サーバとを備えた秘匿化データの類似検索方法であって、

前記第１サーバが、

前記複数の標本データを、標本データ空間において少なくとも局所的に距離保存されるような写像で秘匿化する第１ステップと、

前記秘匿化された標本データと任意データの対を、該秘匿化された標本データ自体に基づいてクラスタリングしてデータベースに記録する第２ステップと、を実行し、

前記第２サーバが、

クエリデータを、前記標本データにした方法と同じ方法で秘匿化する第３ステップと、

前記秘匿化されたクエリデータに基づいて、クエリデータに類似する標本データが記録されているクラスタを特定する第４ステップと、

前記特定されたクラスタから、前記秘匿化された標本データと前記秘匿化されたクエリデータの間の距離の計算によって、前記クエリデータに類似する１つの標本データを特定し、該標本データと対の任意データにアクセスする第５ステップと、を実行し、

前記複数の標本データは、主成分分析、独立成分分析或いは線形判別分析により低次元化された画像特徴量ベクトル、または、バイオメトリクス情報であることを特徴とする秘匿化データの類似検索方法。

【請求項１０】

複数の標本データを保存する第１サーバと、前記第１サーバにアクセスする第２サーバとを備えた秘匿化データの検索システムにおいて、

前記第１サーバは、

前記複数の標本データを、標本データ空間において少なくとも局所的に距離保存されるような写像で秘匿化し、

前記秘匿化された標本データと任意データの対を、該秘匿化された標本データ自体に基づいてクラスタリングしてデータベースに記録するように構成され、

前記第２サーバは、

クエリデータを、前記標本データにした方法と同じ方法で秘匿化し、

前記秘匿化されたクエリデータに基づいて、クエリデータに類似する標本データが記録

されているクラスタを特定し、
前記特定されたクラスタから、前記秘匿化された標本データと前記秘匿化されたクエリデータの間の距離の計算によって、前記クエリデータに類似する１つの標本データを特定し、該標本データと対の任意データにアクセスするように構成され、
データの前記秘匿化は、前記データをそのデータ空間上で量子化し、前記データから、前記量子化されたデータを減算して残差を得て、前記量子化されたデータを暗号学的ハッシュ関数に入力し、ハッシュ値を得るものであり、前記ハッシュ値と前記残差の組を秘匿化されたデータとして出力するものであり、
前記第１サーバによる前記クラスタリングは、前記秘匿化された標本データの前記ハッシュ値の部分に基づいて、該ハッシュ値とクラスタとを１対１または多対１に対応付けるものであることを特徴とする秘匿化データの検索システム。
【請求項１１】
複数の標本データを保存する第１サーバと、前記第１サーバにアクセスする第２サーバとを備えた秘匿化データの検索システムにおいて、
前記第１サーバは、
前記複数の標本データを、標本データ空間において少なくとも局所的に距離保存されるような写像で秘匿化し、
前記秘匿化された標本データと任意データの対を、該秘匿化された標本データ自体に基づいてクラスタリングしてデータベースに記録するように構成され、
前記第２サーバは、
クエリデータを、前記標本データにした方法と同じ方法で秘匿化し、
前記秘匿化されたクエリデータに基づいて、クエリデータに類似する標本データが記録されているクラスタを特定し、
前記特定されたクラスタから、前記秘匿化された標本データと前記秘匿化されたクエリデータの間の距離の計算によって、前記クエリデータに類似する１つの標本データを特定し、該標本データと対の任意データにアクセスするように構成され、
前記複数の標本データは、主成分分析、独立成分分析或いは線形判別分析により低次元化された画像特徴量ベクトル、または、バイオメトリクス情報であることを特徴とする秘匿化データの検索システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、個人を容易に特定できない程度に秘匿化或いは保護された生体特徴情報などについて類似検索を行う秘匿化データ類似検索方法、及び、それを応用した安否確認システム等に関する。
【背景技術】
【０００２】
従来、監視カメラ等で撮影され或いは記録された映像（動画像）の中から、所望の人物を画像認識技術等を用いてコンピュータに検索させる人物検索システムが知られる（例えば、特許文献１乃至４、非特許文献１参照。）。このような、タグ付け等の外部情報に拠らずに画像そのものの特徴に基づき検索する技術は、一般にＣＢＩＲ（Content-Based Image Retrieval）と呼ばれ、人物の検索にも利用され始めている。
特許文献２は、画像から人物（の顔）が映った部分を切出し、人物を個々に特定するための特徴量として色ヒストグラム等を抽出し、この特徴量が所望の人物のものと類似する場合に同一人物であると推定する、映像検索システムおよび人物検索方法を開示している。
【０００３】
画像認識に用いる特徴量は、古くは主成分分析の固有顔のように画素の輝度値そのものであり、第一世代特徴量では、画素値（輝度）の分布やwavelet変換に基づくものが知られる。第二世代では、Haar-Like、HOG、EOH、Edgelet等の局所領域をもとにした特徴量が

知られ、ＳＩＦＴやＳＵＲＦのようにある注目する特徴点に関してスケール不変性を備えたものもある。第三世代では、これら局所領域の空間的関連性を考慮し学習に対象にするようになり、Joint Haar-like、Joint HOG、スパース特徴、Shapelet、共起確率特徴等が用いられるようになった。

近年では、第四世代とされるＰＳＡ（Pixel State Analysis）等の時空間特徴の研究がなされている（例えば、非特許文献２参照。）。

【０００４】

顔認識の性能は、学習に用いた顔画像データベースに依存する。コンテストでしばしば用いられるFERET顔データベースは、正面顔の他、右寄り、左寄りの顔を含む。このデータベースにおいて、２０１０年時点で、FAR（False Accept Rate：他人受入率）＝０．００１におけるFRR（False Reject Rate：本人拒否率）は０．０００３％程度の顔認識が実現されている。

【０００５】

顔認識において実用レベルの精度に至ったＣＢＩＲは、今後様々な分野での利用が期待されている。

その１つに、災害時等の安否確認システムが考えられる。

現在普及している災害時用の安否確認手段は、電気通信事業者が提供しているもので、例えば、安否を確認したい人（確認依頼者）、確認される側の人（非確認依頼者）が所定の電話番号に電話を掛け、相手或いは自己の電話番号とともに音声メッセージを残し、その後、相手側の人が所定の電話を掛け、自己の或いは相手の電話番号を入力するとその音声メッセージを再生できるというものである。

或いは、携帯電話やスマートフォン、パソコン等から、安否情報を文字で入力し、相手側の人は電話番号等で検索することでその安否情報を閲覧できるようなもの、同様の操作で音声も録音、再生できるものが、各種提供されている。また、被確認者のメールアドレスに安否情報の入力を促すメールを自動的に送信するものもある。

また、近年普及しているＳＮＳ（ソーシャルネットワーキングサービス）等も、安否確認の手段となりうる。

【０００６】

なお、本発明に関連して、ＣＢＩＲ技術を利用した、或いは何らかの個人情報と電話番号と対にして検索に利用した安否確認システム等が知られる（例えば、特許文献５乃至７参照。）。

また、画像を用いて人体の識別を行う技術が知られる（例えば、特許文献８乃至９参照。）。

【先行技術文献】

【特許文献】

【０００７】

【特許文献１】特開平５－１５４６５１号公報
【特許文献２】特開２００９－０２７４９３号公報
【特許文献３】特開２０１２－０６８７１７号公報
【特許文献４】特開２０１３－２１８５１１号公報
【特許文献５】特開２００３－３０４３００号公報
【特許文献６】特開２００６－２５４７９８号公報
【特許文献７】特開平９－１９８４０１号公報
【特許文献８】特開２０１２－８５１１４号公報
【特許文献９】特許５１２５４２４号公報

【非特許文献】

【０００８】

【非特許文献１】助川　寛、外４名、「顔画像認識による大規模人物検索システムの開発」、バイオメトリクス研究会資料、一般社団法人電子情報通信学、平成２４年８月２７日、ｐ．１０２－１０７、インターネット＜ＵＲＬ：http://www.ieice.org/~biox/2012/00

1-kenkyukai/pdf/BioX2012-18.pdf＞
【非特許文献２】山下隆義、“特定物体認識に有効な特徴量”、［online］、平成２０年１１月２８日、［平成２６年２月２１日検索］、インターネット＜ＵＲＬ：http://www.vision.cs.chubu.ac.jp/features/PPT/CVIM2008/ppt.pdf＞
【非特許文献３】Yair Weiss, et al、“Spectral Hashing”、［online］、［平成２６年２月２１日検索］、インターネット＜ＵＲＬ：http://people.csail.mit.edu/torralba/publications/spectralhashing.pdf＞
【非特許文献４】Anxiao Jiang, et al、“Rank Modulation for Flash Memories”、［online］、［平成２６年２月２１日検索］、インターネット＜ＵＲＬ：http://www.paradise.caltech.edu/papers/etr086.pdf＞
【非特許文献５】Alexander Barg and Arya Mazumdar、“Codes in Permutations and Error Correction for Rank Modulation”、［online］、［平成２６年２月２１日検索］、インターネット＜ＵＲＬ： http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.249.198&rep=rep1&type=pdf＞
【非特許文献６】古賀久志、「ハッシュを用いた類似検索技術とその応用」、Fundamentals Review、一般社団法人電子情報通信学会　基礎・境界ソサイエティ、平成２６年１月１日、第７巻、第３号、ｐ．２５６－２６７、インターネット＜ＵＲＬ：https://www.jstage.jst.go.jp/article/essfr/7/3/7_256/_pdf＞
【非特許文献７】Tuyls Pim, et al、“Capacity and examples of template-protecting biometric authentication systems”,ECCV Workshop BioAW, no.77, 2004、インターネット＜http://eprint.iacr.org/2004/106.pdf＞

【発明の概要】
【発明が解決しようとする課題】
【０００９】
上述した従来の安否確認システムは、被確認者が、自己が被確認者となっていることを自覚し、安否確認システムの知識があり、安否確認システムにアクセス可能な通信手段が利用可能であり、自発的アクセスしてメッセージ等を残すといった行動をすることが条件となり、これらを１つでも満たせないと安否確認を行うことができない。例えば、災害発生後、安全な場所への避難が完了し、肉親と連絡をとりたいと思った時、所などへの輻輳や回線寸断により固定電話がほとんど利用できない状況では、それ以外の通信手段を利用することが困難な年少者、高齢者は、安否確認ができない恐れがある。
【００１０】
また、災害時用或いは安否確認用のインターネット掲示板等が、多数存在するが、それらのほとんどは互いに連携しておらず、確認依頼者は、各掲示板でそれぞれ検索操作をしなければならないという問題がある。また、仮にそれら掲示板に被確認者や確認依頼者の顔の情報を登録することができたとしても、顔の画像がそのまま掲載されることへの心理的抵抗や、第３者に収集、利用等される恐れなどから、ほとんど登録されないことが予想される。
【００１１】
また、監視カメラ等で撮影した人物に対して、当人が気が付かないまま顔認証（既知の顔と照合すること）をおこなったり、顔情報を収集保存したりすることには、社会的同意が十分得られていないのが現状である。
従って、安否確認システムの構成としては、照合すべき顔（クエリ）をサーバ等に送る集中型よりも、撮影されたその場で照合する分散型のほうが、より受容されやすいと考えられる。その場合、各拠点において、顔データベースを安全に保持するセキュリティ技術が必要である。
【００１２】
同一人の生体情報同士の照合のみが行え、他の用途への転用、統計情報の収集等を困難にするものとして、テンプレート保護技術等があり、Fuzzy Vault、Cancelable Biometrics、Bioscript、Anonymous biometrics（非特許文献７参照）等が知られる。そのような

方法で保護されたデータは、暗号の様にランダム化されるので、元の生体情報を類推することは困難であり、また、等長写像ではないので、元の空間での類似度は１件ずつ試行して求めなければならない。このため、大規模高速検索への応用例は、発明者の知る限り、まだ無い。

【００１３】

そもそも類似検索は、検索されるべき情報と同一の情報を持ち合わせていなくても、その情報にたどり着けるということが本質であって、テンプレート保護を施したとしても、類似検索機能を提供する限り、システム構成如何にかかわらず、第三者は一般の暗号解読に比べて格段に少ない試行回数で所望の情報を入手しうる。また、生体情報は、そのようなオンラインの手法によらず、秘密裏に本人から直接入手されるリスクもあり、結局はそれらの入手コストと、テンプレート保護の攻撃コストのバランスの問題である。入手コストは、どの程度の類似度の範囲で検索結果を提示するかに強く依存するが、テンプレート保護は強力であればあるほど、類似の範囲を広げないと照合できない傾向がある。

【００１４】

本発明は、このような問題に鑑みてなされたものであり、被確認者に自己が被確認者となっている自覚がなくとも、安否確認システムの知識がなくとも、安否確認システムにアクセス可能な通信手段を直接利用することができなくとも、自発的な行動を必要とせず、被確認者の安否を確認できる安否確認システム等を提供することを目的とする。

【課題を解決するための手段】

【００１５】

本発明の一側面に係る安否確認システムは、尋ね人の顔の特徴量と、確認依頼者或いは前記尋ね人の個人情報と、確認依頼者の連絡先とのセットが、複数蓄積されたデータベースを提供するポータルサーバ（４）と、前記データベースのコピーを取得し、カメラで撮影した人物の顔画像から特徴量を抽出し、前記コピーの中から類似する特徴量を検索する現地サーバ（３）と、を備え、前記ポータルサーバは、前記顔の特徴量をテンプレート保護された状態で蓄積および提供し、前記現地サーバは、前記類似する特徴量の検索に成功すると、前記撮影した人物に向けて、前記類似する特徴量に対応する前記個人情報を提示して確認を求め、前記人物からの確認操作を受け付けると、前記確認依頼者の連絡先に通知することを特徴とする。

【００１６】

前記個人情報は、電話番号、であり、前記確認依頼者の連絡先は、メールアドレス或いは電話番号であり、前記顔の特徴量は、主成分分析、独立成分分析或いは線形判別分析により低次元化された、１００次元以下或いはデータサイズが１２８バイト以下のベクトルデータであり、ランダムプロジェクション、一方向性関数或いは公開鍵暗号の少なくとも１つを用いてテンプレート保護される。

前記ポータルサーバは、インターネットに接続され、前記テンプレート保護された状態の特徴量を含む前記セットを前記確認依頼者の端末（２）から受信するとともに、前記現地サーバが電子証明書を有するか或いは信頼できる場合、あるいは非常時にのみ、前記データベースを提供し、前記前記確認依頼者の連絡先への通知は、確認された前記人物を撮影した場所を示す情報を含む。

【００１７】

本発明の他の側面にかかる秘匿化データの類似検索方法は、複数の標本データを、標本データ空間において少なくとも局所的に距離保存されるような写像で秘匿化する第１ステップ（Ｓ２３、４４）と、前記秘匿化された標本データと任意データの対を、該秘匿化された標本データ自体に基づいてクラスタリングして記録する第２ステップ（６５）と、クエリデータを、前記標本データにした方法と同じ方法で秘匿化する第３ステップ（Ｓ８６）と、前記秘匿化されたクエリデータに基づいて、クエリデータに類似する標本データが記録されているクラスタを特定する第４ステップと、前記特定されたクラスタから、前記秘匿化された標本データと前記秘匿化されたクエリデータの間の距離の計算によって、前記クエリデータに類似する１つの標本データを特定し、該標本データと対の任意データに

アクセスする第５ステップと、を有する。
【発明の効果】
【００１８】
本発明によれば、被確認者が自発的にアクセスせずとも、被確認者を発見し、安否確認することができる。
【図面の簡単な説明】
【００１９】
【図１】安否確認システム１の構成図。
【図２】安否確認システム１のユースケース図。
【図３】確認端末３における顔を登録する機能のアクティビティ図。
【図４】図３のＳ２３における特徴量抽出処理を示す機能ブロック図。
【図５】図４のテンプレート保護部４４ａ～４４ｄの構成例。
【図６】ポータルサーバ４の機能ブロック図。
【図７】クラスタ化部６５の構成例。
【図８】現地サーバ２における、類似顔を探知する機能のアクティビティ図。
【図９】Ｓ８７のＤＢ検索の機能手段の構成例。
【図１０】テンプレート保護部４４ｅの構成例。
【図１１】Ｓ８７のＤＢ検索の機能手段の構成例。
【図１２】本人確認画面の例。
【発明を実施するための形態】
【００２０】
以下、本発明に係る実施形態について図面を参照して説明する。なお、各図の説明において、実質的に同一な機能を有する構成要素には同一の参照番号を付し、説明を省略する。
【実施例１】
【００２１】
図１～図４を参照して、実施例１にかかる安否確認システム１を説明する。図１には、安否確認システム１の構成を例示してある。
本例の安否確認システム１は、被確認者を撮影するカメラ等が接続された複数の現地サーバ２ａ～２ｃ（個々を区別しないときは現地サーバ２と呼ぶ。以下同じ。）と、それぞれの確認依頼者等が所有或いは操作する確認端末３ａ～３ｃと、確認端末３からの問合せを最初に受付け、現地サーバ２と確認端末３の間を仲介するポータルサーバ４と、で構成される。
【００２２】
本例の安否確認システム１は概略的には、確認端末３から、被確認者の顔画像の特徴量と電話番号等の情報とが入力され、それが各現地サーバ２ａ～２ｃに配信されて、現地サーバが自己のカメラで撮影された映像中の顔と照合されるというものである。被確認者の顔が検出された時には、現地サーバ２が合成音声を発してその被確認者を呼び止め、適宜本人確認或いは同意の操作を求め、確認がとれれば確認依頼者に通知される。
【００２３】
図２は、安否確認システム１のユースケース図である。なおこの図２は、現地サーバ２等の機能の全てを表現しているとは限らず、それらの機能を限定的に特定する意図はない。
現地サーバ２は、避難所の通用口やホール、その他往来の多い場所に、通行人の顔を撮影するビデオカメラとともに設置されたパソコンやタブレット等であり、所定のソフトウェアをインストールされると、その存在をポータルサーバ４に通知し、現地サーバ２として機能し始める。ビデオカメラは、好ましくはフルフレームでＨＤ撮影可能なものとし、その映像がＨＤＭＩ（商標）ケーブルにより現地サーバ２に入力される。現地サーバ２は、通行人に呼びかけるためのスピーカ、確認のための情報を表示する画面、通行人からの操作を受け付けるタッチパネル等のヒューマンＩ／Ｆを備える。またインターネットに接

続され、好ましくは、互いにＰ２Ｐネットワーク或いは自律分散データーベースを構成し、インターネットへの接続手段は、有線回線の他、ＬＴＥデータ通信や衛星インターネット等により複数確保される。

【００２４】

確認端末３は、携帯電話、スマートフォン、タブレット、パソコン等の、インターネットに接続してＷｅｂサイトを閲覧できる通信端末であり、確認依頼者が顔を登録するための機能、被確認者の確認通知を受信して表示する機能、更に好ましくは、人物の顔を対応付けて登録可能な電話帳機能を有する。顔を登録する機能は、確認依頼者が顔を選ぶ機能、電話番号等を指定する機能、送信ボタンを押す機能を含む。

【００２５】

ポータルサーバ４は、パブリックＩＰアドレスを有するＷｅｂサーバであり、被確認者の顔登録をするためのＷｅｂページを端末３に提供し、端末３から受取った登録情報を蓄積してデータベース（ＤＢ）を構築し、現地サーバ２に配信する。また、現地サーバ２から被確認者が確認された旨の通知を受取り、必要に応じデータベースに反映させる。また外部或いは内部のＳＭＴＰサーバを利用して被確認者に通知する。

【００２６】

図３は、確認端末３における顔を登録する機能のアクティビティ図である。本例では、確認端末３はAndroid（商標）端末とし、事前に顔登録アプリケーションがインストールされていることを想定する。このアプリケーションの本体は、java仮想マシンでの実行コードであり、難読化されていることが望ましい。

【００２７】

顔登録アプリケーションが起動されると、最初にステップＳ１１として、顔画像ソース選択画面を表示する。この画面では、顔画像ソースとして、確認端末３内に保存されている任意の画像ファイルから選択するか、連絡先（電話帳）から選択するかをユーザが指定する。

顔画像ソースとして任意ファイルが指定された場合、ステップＳ１２として、ギャラリ表示を行う。具体的には、Intentのインスタンスを生成し、setTypeメソッドにより対象が画像であることを指定し、setActionメソッドでアイテムの選択が目的であることを指定し、startActivityForResuitメソッドによりギャラリ表示を行い、戻り値としてユーザによるファイル指定の結果を取得させるためのIntentを発行する。このIntentはＯＳ側で適切に処理されギャラリ表示アプリケーション等が起動される。

【００２８】

ステップＳ１３として、onActivityResultメソッドにより、Ｓ１２のギャラリ表示の戻り値を受取る。確認端末３の画面はIntentに協調して遷移するため、Intentが戻ってくると画面は登録アプリケーションの表示に戻る。

一方Ｓ１１において顔画像ソースとして連絡先が指定された場合、ステップＳ１４として、連絡先の表示を行う。Ｓ１２と同様、startActivityForResuｌtでIntentを発行するが、リクエストコードとしてGALLERYではなくPICK_CONTACTを指定する。

【００２９】

ステップＳ１５として、onActivityResultメソッドにより、Ｓ１４の連絡先表示の戻り値を受取る。戻り値は、連絡先から選択された１人の人物を指すContactsContract.ContactsクラスのURIである。なお、Grant-uri-permission機能を用いて、１回のみのアクセスを可能なURIを取得することもできる。その後getContentResolver.queryメソッドでcursorインスタンスを生成しそのcursorを用いてＳ１３の戻り値と同様の、画像ファイルのURIを得る。また、この時点で当該人物の電話番号も取得しておいてもよい。

【００３０】

ステップＳ１６として、android.media.FaceDetectorクラスを用いて顔検出を行う。具体的には、画像ファイルのURI を指定したBitmapFactory.decodeFileメソッドでBitmapインスタンスを生成し、Bitmapインスタンスの幅や高さのプロパティ等を用いてFaceDetectorインスタンスを生成し、FaceDetectorインスタンスに対してfindFacesメソッドで認識

を行う。戻り値は認識した顔の数であり、詳細な結果（両目の間隔、顔中央の座標、顔の傾き、信頼度）はFaceDetector.Faceに格納される。

【００３１】

ステップＳ１７として、Ｓ１６の検出でエラーが発生しているか判断する。エラーは、顔の数が０、或いは信頼度が所定値以上の顔が存在しないことで判断される。エラーが発生したときはステップＳ１９に分岐する。

【００３２】

ステップＳ１８として、顔の切り出し（トリミング）を行う。具体的には、元のBitmapインスタンスと切り出し位置を指定したcreateBitmapメソッドにより、トリミングされた新たなBitmapインスタンスを得る。切り出し位置は、最も信頼度の高かった顔のFaceDetector.Faceのプロパティに基づき、一定の規則で計算するものとする。その後、所定のファイル名でFileOutputStreamインスタンスを生成し、そのファイル出力インスタンスを指定した、Bitmap.compressメソッドで、画像ファイルとして保存される。

なお、顔を所定の３次元モデル（例えば楕円体）に当てはめて、顔向きの補正をする場合は、画像を分割し、個々にMatrixクラスのpostRotateやpostSkewメソッドを適用後、１つの画像に合成する。

【００３３】

一方Ｓ１７でエラーと判断されていた場合、ステップＳ１９として、手動トリミング画面の表示を行う。Ｓ１４と同様、startActivityForResultでIntentを発行するが、intent.setData(uri)のuriにはＳ１６用いた画像ファイルのURIを指定し、putExtra(MediaStore.EXTRA_OUTPUT, uri)のuriにはＳ１８と同じ保存先ファイルのURIを指定しておく。

ステップＳ２０として、onActivityResultメソッドにより、Ｓ１９の手動トリミングの戻り値を受取り、Ｓ１６に遷移する。ここで受取る戻り値は適宜エラー処理に使用できるが、説明は省略する。

【００３４】

Ｓ１８の次に、ステップＳ２１とステップＳ２２とステップＳ２３が非同期で並列動作する。

ステップＳ２１では、ポータルサーバ４と通信を確立し、ポータルサーバ４からテンプレート保護用の乱数を受取る。

【００３５】

ステップＳ２２では、電話番号の入力を受け付ける画面を表示する。この画面には、数字を入力可能なテキストボックスと、入力した電話番号が確認依頼者（つまり検索端末３の操作者）のものか、被確認者（つまり登録される顔の人物）のものかの別（番号種別と呼ぶ）を指定するラジオボックスと、送信ボタンとを有する。より好ましくは、Ｓ１８で保存した被確認者の顔画像を表示し、「送信ボタンを押すとこの顔の特徴量情報が電話番号等とともにサーバに送信される」旨の確認メッセージも表示する。

なおＳ１５で、被確認者の電話番号のを取得できていた場合、予めテキストボックスに入力された状態で表示してもよい。なお確認端末３自体の電話番号は、操作者がその場で入力することが特段の手間ではないと考えられるため、自動取得はしていない。

また、確認依頼者と被確認者の両方の電話番号を入力できるようにしてもよく、更に任意で追加的な個人情報（被確認者の年齢、性別、その他の身体的特徴、メールアドレス、SNSアカウント、ハンドルネーム、住所、勤務先（学校名）等）を入力できるようにしてもよい。

最終的に送信ボタンの押下を検知すると、その時点で入力されていた電話番号や番号種別、追加的な個人情報を保持する。

【００３６】

ステップＳ２３では、被確認者の顔画像から特徴量を抽出し、テンプレート保護を施して、サーバへ送信するための「保護された特徴量」を生成する。このテンプレート保護には、Ｓ２１で受信する乱数が必要であり、乱数が得られるまでＳ２３は中断する。なお保護された特徴量のデータサイズは高々１００オクテット程度である。Ｓ２３の処理は、数

秒以内で終了できるよう、また難読化の意味でも、ＪＮＩ（Java Native Interface）等を介してネイティブコードに処理させることが望ましい。ネイティブなライブラリで入手可能なものにopenCV for Androidがあり、Javaから使うためのAPIの他、ネイティブ(C/C++)用のAPIも公開されている。

【００３７】

Ｓ２１～Ｓ２３が全て完了すると、次にステップＳ２４として、Ｓ２２の画面で入力されていた電話番号や番号種別等と、Ｓ２３で生成した保護された特徴量を、HTTP/TLSプロトコルや、ＳＭＳ（Short Message Service）を用いてポータルサーバ２へ送信する。ショートメッセージを用いる際は、保護された特徴量はBase64エンコードされる。

【００３８】

図４は、図３のＳ２３における特徴量抽出処理を示すブロック図である。サイズ・解像度正規化部４１は、受け取った顔画像を所定のサイズ（幅及び高さ）にリサイズするとともに、解像度やコントラストを正規化する。リサイズ直後の解像度は、原画像のサイズや解像度に依存し、ばらつきがあるため、抽出される特徴量（或いは特徴点）もばらついてしまう。ガウスフィルタ等のＬＰＦで常に一定以上の周波数の成分を除去するか、エッジや高周波成分の大きさを検出し、その値に応じた鮮鋭化／ぼかしフィルタ処理を施す。また必要に応じ、輝度ヒストグラムを求め、それに基づいてコントラストを正規化する。なおこれらの正規化処理は、特徴量抽出後に行うこともできる。

【００３９】

特徴量抽出部４２は、サイズ・解像度正規化部４１からの正規化画像から、特徴量を抽出する。特徴量としては、非特許文献２で述べられているような各種の公知のものが利用できる。本例では、正規化画像を小ブロックに分割し、小ブロック毎のエッジパターンの頻度についてのヒストグラムを求め、ヒストグラムの各ビンの値（度数）を所定の規則で１列に並べて得た列ベクトルを特徴量とし、その次元は１０００程度に達する。

【００４０】

次元圧縮部４３は、特徴量抽出部４２からの特徴量を入力し、より小さい次元の特徴量に変換して出力する。基本的には、主成分分析（ＰＣＡ）、線形判別分析（ＬＤＡ）、独立成分分析（ＩＣＡ）等の手法を用いる。つまり、予め多数の人の顔（標本）から抽出した特徴量から分散共分散行列或いはそれに類するものを求め、その固有ベクトルからなる変換行列（射影行列）Ａを用意しておく。変換行列Ａには、変換後の各主軸のスケールを一定にするための係数が乗算されており、次元削減部４３は、入力された特徴量にこの変換行列を単に掛け算するだけで、正規化された低次元化特徴量を得る。変換行列Ａの行数（低次元化特徴量の次元）は、標本数にもよるが、ＰＣＡやＬＤＡでは１００程度、ＩＣＡでは２０～３０程度で十分とされている。

変換行列Ａはシステム全体で共通でおり、基本的に運用中に変更することはしない。また、次元圧縮部４３における正規化は必須ではない。

ＩＣＡで得られる主軸は、人が他人の顔を覚えようとするときに意識する外見的特徴と似ており、例えば、ひげの有無、眼鏡の有無等をよく反映する軸がある。そのような不変性のない特徴の軸は、重みを下げたり、除去してもよい。

ＰＣＡ等で得た変換行列は正規直交基底となっており、次元圧縮後も距離関係がよく保存されている。このような性質のものとして後述のＲＰも使用でき、ＬＳＨ（Locality Sensitive Hashing）は補助的に使用できる。

【００４１】

テンプレート保護部４４は、次元圧縮部４３からの低次元化特徴量に、一方向性関数、ランダムプロジェクション（ＲＰ）または公開鍵暗号等を適用し、秘匿化された特徴量（或いはコード）を出力する。

図５及び図１０に、テンプレート保護部４４の構成の５つのバリエーションが示される。

図５の（ａ）の例のテンプレート保護部４４ａは、Anoymous biometrics（非特許文献７参照）を非常に簡略化した実装であり、低次元化特徴量を量子化する量子化器５１、量

子化された特徴量を暗号学的ハッシュ処理するハッシュ計算機５２、量子化前の低次元化特徴量から、量子化された特徴量を減算する減算器５３、とで構成される。

量子化器５１は、入力された低次元化特徴量をより荒く離散化するもので、例えばＬＳＨを利用する。本例では、低次元化特徴量が予めＰＣＡで処理され、スケールも正規化されているので、一種のＰＣＨ（Principal Component Hashing）として機能する。簡易的には、各軸の成分の値を複数の区間に等分割するだけでよく、成分の値の上位桁（上位ビット）を取り出すことでも達成できる。情報の損失を避けるため、離散化特徴量のビット長B_dは、ハッシュ計算機５２の出力するビット長B_hよりも少ないほうが良いと思われるが、実際にはほとんど問題ない。むしろテンプレート保護部４４ａが出力するビット長Ｂｔ（減算器５３の出力する残差のビット長Ｂｒと、B_hの和）が所望値となるよう、B_dを選べばよい。

ハッシュ計算機５２は、例えばＳＨＡ－１等のアルゴリズムに従い、離散化特徴量を一定のビット長B_hのハッシュ値を出力する。

もし、入力された低次元化特徴量が、量子化の境界付近にある（量子化残差の大きさが略等しい量子化値が複数存在する）場合、テンプレート保護部４４ａは、それら複数の量子化値に対応する複数のハッシュ値及び残差のセットを出力してもよい。

離散化特徴量は、Anoymous biometricsにおけるhelper dataに相当する。

なお、このテンプレート保護部４４ａでは、図３のＳ２１の乱数は使用しない。

【００４２】

図５の（ｂ）は、ＲＰを用いたキャンセラブルバイオメトリクスの例である。このテンプレート保護部４４ｂは、図３のＳ２１で受け取った乱数から、所定の規則でパラメータを生成する変換パラメータ生成部５４と、生成されたパラメータに基づき、低次元化特徴量を変換する変換部５５と、を備える。

変換パラメータ生成部５４は、例えば、予め用意した$B_d \times B_d$の行列を、乱数に従い所定の規則で行或いは列を入れ替えたり、符号を反転させたりしてランダムプロジェクション行列を得る。乱数として、このＲＰ行列を初めから受け取ってもよい。予め用意する行列は、ユニタリ行列が望ましく、単位行列でもよいし、各要素に正規乱数や一様乱数を用いたＲＰ行列でもよい。

変換部５５は、次元圧縮部４３からの低次元化特徴量（列ベクトル）に、ＲＰ行列を掛け算し、その結果をテンプレート保護部４４ｂの出力とする。

ここテンプレート保護部４４ｂは、次元圧縮は行わないものとして説明したが、行列の掛け算をしているだけという点で次元圧縮部４３と同じであり、これらの処理を一体化することは可能である。つまり、変換行列Ａの行を乱数に基づきに入れ替える等すればよい。

キャンセラブルバイオメトリクスでは、秘密の乱数あるいは保護された特徴量が流出した場合、乱数を更新し、記憶している特徴量は全て、新しい乱数でＲＰし直すことで、流出した情報によるなりすまし等を防ぐ。

ＲＰだけでは、ＲＰ後のサンプルにＰＣＡを適用するなどして成分を推定し元の特徴量或いは顔画像を復元する攻撃があり得るが、本例ではＲＰ前にＰＣＡ及び正規化されているので、各成分は独立に見え、このような解析はより困難となる。

本例のＲＰはユニタリ変換あるいはそれに似た変換としたので、変換後も距離関係が良く保存されている。

【００４３】

図５の（ｃ）は、秘密の乱数が与えられなくとも一定の秘匿性を有するＲＰの例である。このテンプレート保護部４４ｃは、テンプレート保護部４４ｂに加え、ハッシュ関数、誤り訂正復号、ベクトル量子化、距離保存ランレングス制限符号、順列符号（Permutation code）、距離保存マップ（ＤＰＭ）、Rank Modulation復号等のいずれか１つ以上を行うコード化部５７を備え、必要であれば別途、マッピング部５８を備える。テンプレート保護部４４ｃは、与えられた乱数ではなく、低次元化特徴量から一意に決まるタプル（符号やベクトル等）でランダム化したＲＰ行列を用いて、ランダムプロジェクションを行う

。
タプルは、例えば、テンプレート保護部４４ａと同様、疎に量子化した特徴量（ハッシュ値）を用いることができる。例えば、タプルを８ビット毎に切り出して、奇数ワードの値（０～１２７）で指定される行と、偶数ワードの値で指定される行とを交換することで、ＰＲ行列はランダム化される。同じバケットに量子化される低次元化特徴同士であれば、同じランダムプロジェクションを受けるので、距離関係が保存される。しかしバケットが異なると、距離は保存されない。秘匿性を重視するなら、この方法が有利である。
ＲＰ行列が、量子化特徴量と１対１対応するということは、保護された特徴量の各成分の大きさから、ＲＰ行列を推定される可能性を示唆する。しかしランダム化に符号反転操作が含まれいれば、推定をより困難にできる。ＲＰ行列のランダム化は、上記の行や列の交換や符号反転の他、ユニタリ性を（近似的に）維持するいかなる操作を含むことができ、これらの操作はできるだけ秘密にする。
【００４４】
ここで、ランダムプロジェクション手法を保持したまま、互いに近接するバケット同士を、近接したまま写像する方法を考える。１つの答えは、近接バケットのＲＰ行列が、ある２つの行（または列）が入れ替わっただけの関係になるよう、それらのタプルのハミング距離を最小（１）にすることである。ＬＳＨの派生であるSpectral Hashingがそれを実現している。Spectral Hashingでは、空間周波（モード）という概念を導入し、主軸上の最大値と最小値の間を、モード数の２倍の数に分割し、それらを交互に二元符号の０又は１のどちらかに符号化することで、ビット長が主軸数と同じバイナリ符号が得られる。より簡易には、ＰＣＨ（ＬＳＨ）の各主軸の成分を２値化するだけでよく、各成分を多値で表したい場合はグレイコードを用いる。
【００４５】
符号理論の分野では、ハミング長を保存する或いは強化する符号が古くから知られ、距離保存ランレングス制限符号、順列符号（Permutation code）、距離保存マップ（ＤＰＭ）等がある。また近年、Multi-Level Cellタイプのフラッシュメモリで誤り訂正を行うために開発されたRank Modulationも利用できる。これらは基本的に二元符号を扱うものなので、多値情報であるバイナリ表現された低次元化特徴量を、二元符号に変換する必要がある。
マッピング部５８はこの変換を行うものであり、一例としてグレイコードでマップ化する。
【００４６】
図５の（ｄ）は、公開鍵暗号を用いた例である。このテンプレート保護部４４ｄは、図３のＳ２１で受け取った乱数（公開鍵）に基づいて、低次元化特徴量を暗号化する公開鍵暗号化部６０を備える。
公開鍵暗号化部６０は、例えば、ゴッパ符号や低密度パリティ検査符号を利用したMcElice暗号或いはNiederriter暗号で低次元化特徴量を暗号化する。McElice暗号は、ｋ×ｎの生成行列Ｇ、ｋ×ｋの正則行列Ｓ、ｎ×ｎの転置行列Ｐを秘密鍵とし、Ｇ’＝ＳＧＰを公開鍵とする。この暗号は、符号となる多項式の一部に脆弱な部分があるものの、暗号化及び復号化の計算コストが低く、量子計算機に解読されにくいという利点がある。
【００４７】
図１０は、テンプレート保護部４４ｅの構成図である。このテンプレート保護部４４ｅは、テンプレート保護部４４ａ～４４ｃのアイディアに、ランダムなデータ改変と誤り訂正を組み合わせたものである。
ビット分割器１０１は、入力された低次元化特徴量のバイナリ表現における最上位１～２ビットと、残りのビットとに分割し、それぞれを量子化特徴量、残差特徴量として出力する。これらは、テンプレート保護部４４ａの量子化器５１と減算器５３の出力に相当する。
グレイ符号化器１０２は、量子化特徴量をグレイコード化する。なお、ビット分割器１０１が最上位の１ビットのみ取り出している場合は、不要である。

乱数発生器１０３は、都度、乱数を発生する。
データ改変器１０４は、乱数発生器１０３からの乱数に応じた所定の規則で、グレイコードの所定位置の１つのビットを反転するなどの改変を行う。
事前改変器１０５は、乱数発生器１０３からの乱数に応じた所定の規則で、残差特徴量の一部を改変する。例えば、乱数で決まる成分に対し、符号反転したり、ブロックスクランブルやモーフィング等のテンプレート保護手法等を適用する。なお、検索の初期段階において、事前改変器１０５で改変された特徴量で荒い類似検索をするため、ここでの改変の量は、個人の識別を困難にする程度に（単一人物の特徴量の分散より）大きく、かつ、荒い類似検索で発見できる程度に小さくする。
ＲＰ（Random Projection）処理器１０６は、データ改変器１０４からの改変されたグレイコードに応じた所定の規則で、ＲＰ行列を生成し、入力された低次元化特徴量に掛け算する。ＲＰ行列は、仮にＲＰ行列が判っても、その元となったグレイコードや低次元化特徴量が推定されにくいことが要求され、グレイコードの改変はこの要求に貢献する。
誤り訂正符号部１０７は、例えばＲＳ（リードソロモン）符号化器であり、冗長シンボルを出力する。
連結器１０８は、ＲＰ処理器１０６でＲＰされた特徴量と、冗長シンボルとを連結し、保護された特徴量として出力する。
【００４８】
図６は、本例の安否確認システム１のポータルサーバ４の機能ブロック図である。本例のポータルサーバ４はLAMP/LAPP環境で構築される。
httpサーバ６１は、例えばApatch HTTPサーバとOpensslであり、基本的には、コンテンツ記憶部６２が保持している、インターネット上で当該サイトを紹介するページ等の静的コンテンツを提供するとともに、検索端末３からの顔登録要求のhttpメッセージを受信する。
また、現地サーバ２からの要求に応じ、後述するＤＢのスナップショットや差分パッチを送信する。この際、少なくとも平時はＳＳＬ通信を用いることが望ましい。httpサーバ６１は、事前にパブリックＣＡから取得したサーバ証明書を有する。
【００４９】
コンテンツ記憶部６２は、トップページの他、検索端末３のウェブブラウザに実行及び表示させる顔登録用のページ、検索端末３にダウンロードすべき顔登録アプリケーションの提供先に誘導するページ、後述するＤＢ６６のスナップショットや差分パッチ等の、予め用意された静的コンテンツを保持する。
【００５０】
サーバサイド処理部６３は、例えばJava(商標)サーブレットであり、ポータルサーバ４としての動作をつかさどる。例えば顔登録要求のhttpメッセージの本体を、電話番号等の個人情報と、保護された特徴量とに分け、後述のクラスタ化部６５などを制御して、ＤＢ６６に登録させる処理をする。またＤＢ６６にスナップショット等を作成させ、それらを圧縮したファイルをコンテンツ記憶部６２に保存する。
サーバサイド処理部６３は、更にJava仮想マシン上で動作する高次機能を実行可能であり、例えばBitTorrent DNA（BitTorrentは商標）等のサーバ指向P2P技術を使った配信を行うこともできる。
【００５１】
プライベート認証局（CA）６４は、例えばOpensslの機能の一部であり、証明書を持たない現地サーバ２に対し、プライベートCA６４をルートとする独自の証明書を発行する。可能であれば、パブリックＣＡの方が望ましい。証明書が与えられる現地サーバ２は、官公庁や自治体等の公的機関、教育機関、その他公共性の高い団体（指定公共機関等）等により管理されている場合であり、ＩＰアドレスをwhoisサービスで調べるオンラインの方法や、書面等で申し込むオフラインの方法による。一旦発行された証明書は、災害時にＩＰアドレスが変わっても継続して使用できる。
【００５２】

クラスタ化部６５は、保護された特徴量を、保護されたまま或いは保護を解除して、複数あるクラスタのいずれかに分類し、そのクラスタＩＤを出力する。クラスタは、互いに近い複数の特徴量をグループ化したものである。類似検索（擬似最近傍検索）を顔登録数ｎに対してＯ（ｎ ｌｏｇｎ）で実現するために、各クラスタは登録数（クラスタサイズ）ができるだけ均等になるように制御される必要がある。周知のクラスタ化手法の多くは、クラスタ間或いはクラスタ内の距離を測り、それに基づきクラスタの統合・分割をしたり、クラスタの分類基準を更新したりする。本例のクラスタ化部６５は、必要に応じ、距離計算に必要なクラスタの統計情報や分類基準をＤＢ６６に保持させ、所定のタイミングで、分類の基準を更新する。

【００５３】

ＤＢ６６は、ハードディスク等の記憶媒体に、クラスタテーブル６７、クラスタ数と同数の特徴量テーブル６８、個人テーブル６９等を保持し、それらテーブルに対するデータの登録、更新、削除等を実行する。

クラスタテーブル６７は、実在するクラスタのＩＤを主キーとし、クラスタの場所（先頭アドレス）や属性（登録数、クラスタ内の統計情報、分類基準等）を保持する。

特徴量テーブル６８は、各クラスタの実体であり、顔ＩＤを主キーとし、当該クラスタに分類された特徴量を保持する。

【００５４】

個人テーブル６９は、顔ＩＤを主キーとし、その顔の本人（被確認者）や登録者（確認依頼者）の個人情報を保持する。個人情報は、登録者に連絡をとるための、登録者の電話番号或いはメールアドレスを含む。顔ＩＤは、登録された顔の個々にユニークに付されるＩＤである。

なおＤＢ６６自体の機能として、それらテーブルを暗号化して記録するようにしてもよい。

【００５５】

図７は、クラスタ化部６５の構成例である。クラスタ化部６５は、テンプレート保護部４４のバリエーションに対応して、複数のバリエーションがある。

図７の（ａ）は、テンプレート保護部４４ａに対応するクラスタ化部６５ａである。分離部７１は、入力される保護された特徴量を、暗号学的ハッシュ値と、量子化残差とに分離する。暗号学的ハッシュ値は、距離保存性が全くなく、ハッシュ値の異なる特徴量間の距離計量は不可能であるため、テンプレート保護部４４ａにおける量子化の境界と、クラスタの境界はそろえなければならない。本例では、１つのハッシュ値と１つのクラスタとを対応付ける（１対１）様態を基本とし、例外的に、１つのハッシュ値と複数のクラスタとを対応付ける（１対多）様態を用いる。

クラスタ分割部７２は、大きすぎるクラスタを分割するためのもので、クラスタテーブル６７ａからサイズを取得し、規定サイズのときに、周知のクラスタリング手法を用いて当該クラスタを、（現サイズ／規定サイズ）を整数化した数に分割する。クラスタリング手法としては、k-means法、分割統治法、Ward法等の階層的クラスタリング、１クラスＳＶＭ（２分割のみ）等が利用できる。そして分割後の各クラスタについて、分割インデックスを付与し、重心等のクラスタの属性をクラスタテーブル６７ａに記録する。

【００５６】

最短探索部７３は、ＤＢ６６に登録しようとする特徴量のハッシュ値で、クラスタテーブル６７ａからクラスタＩＤのハッシュ値部を検索し、そのクラスタＩＤ等を取得する。ハッシュ値が一致したクラスタが複数あるときは、読みだしたクラスタ属性（重心）に基づき、分類されるべきクラスタを決定し、そのクラスタＩＤを出力する。一致したクラスタが１つだけあるときは、そのクラスタの分割インデックスを出力する。当該ハッシュ値に対応するクラスタが１つもなければ、新規にクラスタを作成する。その際、分割インデックスは０とする。

ハッシュ値と分割インデックスとを連結したものをクラスタＩＤとし、そのビット長B_{ID}を128とすると、100万件の顔登録があってもクラスタテーブル６７ａの記録容量は最大

２４Ｍバイト程度で済み、オンメモリＤＢの支障にはならない。クラスタテーブル６７ａは、クラスタＩＤでソートしておけば、二分探索で容易に検索可能である。

【００５７】

図７の（ｂ）は、テンプレート保護部４４ｂに対応するクラスタ化部６５ｂである。入力される保護された特徴量は、固定のＲＰ行列によりランダムプロジェクションされ、それは実質的に等長写像とみなせる。従って任意のクラスタリング手法が利用可能であり、例えば非特許文献６に記載のＬＳＨ－Ｌｉｎｋを用いる。ＬＳＨ－Ｌｉｎｋは、階層的クラスタリングの一種であり、クラスタ間距離（最小距離）の近似計算にＬＳＨを用いたもので、単連結法の他、完全連結法にも応用可能である。ＬＳＨ－Ｌｉｎｋでは、別のクラスタに属する同じハッシュ値の要素（本例では特徴量）に絞って、距離計算を行う。

ＬＳＨ部７４は、ＤＢ６６のクラスタテーブル６７ｂに属性情報の１つとして保存されている、ＬＳＨの荒さを表すハッシュ関数情報を読出し、それに従って入力される保護された特徴量のハッシュ値を計算する。

【００５８】

クラスタテーブル６７ｂは、ハッシュ値（バケット）と、そのハッシュ値が属するクラスタのＩＤとを対応付ける辞書を有しており、ハッシュ値を引数にして単純にクラスタＩＤを読み出すことができる。この辞書は、ＬＳＨの荒さが異なる複数のバージョンがあり、クラスタリングの試行中の辞書は、ハッシュ値毎に、そのハッシュ値が得られた複数のクラスタＩＤ（直前のバージョン）およびその特徴量を保持し、距離計算に利用できるようになっている。

距離計算部７５は、その同じハッシュ値となった複数の特徴量の間の距離（マンハッタン距離）を計算する。

【００５９】

更新部７６は、距離計算部７５が得た距離と、ＬＳＨの荒さとを比較し、その距離を得た特徴量が属するクラスタを併合すべきかを判断し、新たなバージョンの辞書を作成してクラスタテーブル６７ｂを更新する。

なお、例示したテンプレート保護部４４ｂでは、同一人物の顔が複数登録されるような用途においては、単一人物が複数のクラスタに分類されるケースが十分少なくなるよう、実際にＤＢ６６に登録された各人の特徴量分布に対応したクラスタリングを行うことが望ましい。

【００６０】

テンプレート保護部４４ｃに対応するクラスタ化部６５ｃは、クラスタ化部６５ａまたはクラスタ化部６５ｂと同じであるので、図示を省略する。近隣の量子化された低次元化特徴量が、類似するＲＰ行列によって、互いに近隣のまま投影されることが期待できるのであれば、クラスタ化部６５ｂを、期待できなければクラスタ化部６５ａを用いればよい。

【００６１】

図７の（ｃ）は、テンプレート保護部４４ｄに対応するクラスタ化部６５ｄである。クラスタ化部６５ｄは、クラスタ化部６５ｂに、暗号復号化部７８を追加しただけであり、詳述を省略する。つまり、保護された特徴量は暗号復号化部７８によって一時的に低次元化特徴量に復号され、この低次元化特徴量に基づいて任意のクラスタリング手法を適用し、保護された特徴量が属するべきクラスタＩＤを決定する。なおＤＢ６６には、保護された特徴量がクラスタ化されて登録される。

【００６２】

テンプレート保護部４４ｅに対応するクラスタ化部６５ｅは、クラスタ化部６５ａまたはクラスタ化部６５ｂと同様に実現できる。クラスタ化部６５ｄは、クラスタ化部６５ａに基づく場合、入力される保護された特徴量が含んでいる冗長シンボルを、初期のクラスタＩＤに利用し、大きいクラスタは適宜分割すればよく、クラスタ化部６５ｂに基づく場合も、冗長シンボルを（ＲＰの影響を受けていない）ハッシュ値の一部として利用できる。

【００６３】
図８は、現地サーバ２における、類似顔を探知する機能のアクティビティ図である。この探知機能は、ビデオカメラと接続し、動画のフレームを取り出すためのドライバと、探知アプリケーションプログラムとで構成される。このアプリケーションは、クラッキング防止ツールにより、テンプレート保護処理や類似検索を行う部分のコードが暗号化されており、逆アセンブルやソフトデバッガによる動的解析が困難化されている。アプリケーションは、初めて起動されたときは、証明書を用いてポータルサーバ４からＤＢ６６のスナップショットをダウンロードし、その後も定期的に差分パッチをダウンロードしてローカルのＤＢ８０を更新するものとする。また現地サーバ２のカメラの設置場所を示す文字列（例えば、「ＡＢＣ町のＸＹＺ小学校避難所」）を設定する。
【００６４】
このアクティビティ図は、ステップＳ８１から開始する検索のコアの処理と、Ｓ８９から開始するユーザインタフェース等の外見的な処理とが、常に平行に動作することを表している。
まず、ステップＳ８１では、ビデオカメラで撮影された動画の最新の１フレームを取り込む。
次にＳ８２では、１フレームの画像から、AdaBoost等の公知アルゴリズムにより顔検出を試行し、１つ以上の顔が検出された時はその画像を切り出して、フレーム内での位置や信頼度等の属性情報とともに出力する。
次にＳ８３として、検出された顔のそれぞれについて、図４に示した特徴量抽出部４２及び次元圧縮部４３と同じ処理を行う。
【００６５】
次にＳ８４として、追跡中人物テーブルを用いて追跡処理を行う。この追跡処理は、新たに抽出された特徴量やその属性情報のそれぞれについて、以前（例えば数秒以内）に抽出された特徴量や属性情報と類似していないか、追跡中人物テーブルと照合し、類似したものが無ければ、その特徴量を登録時刻とともにテーブルに追加する。新たな特徴量の信頼度が所定値以上で、且つ、追跡中人物テーブル中の出力済みフラグが偽ならば、その特徴量を出力するとともに、出力済みフラグを真に更新する。テーブル中の、登録時刻が古い特徴量は削除する。
この追跡処理により、続いて行われる検索処理を、全数処理できる程度の頻度に絞ることができる。
【００６６】
次にＳ８５として、Ｓ８４の追跡処理で、検索すべき人物が出力されたか否かを判断し、出力が無ければ、今のフレームに対する処理を終了する。
次にＳ８６として、図４に示したテンプレート保護部４４における処理と同じ処理でテンプレート保護を行う。この保護された特徴量が、検索クエリとなる。なお、テンプレート保護部４４ｅの場合、続くＳ８７との間で後述する反復処理を伴う。
【００６７】
次にＳ８７として、Ｓ８６で与えられたクエリ特徴量に類似する（最近傍の）特徴量を、ＤＢ８０の中から検索する。ＤＢ８０は、ＤＢ６６と同じ内容のクラスタテーブル９１、特徴量テーブル９２、個人テーブル９３を有し、ポータルサーバ４で行われたクラスタ構造がそのまま維持されている。そこでは類似する特徴量がクラスターに凝集されており、検索対象のクラスターを１乃至数個検索し、更にそのクラスター内を検索するという多段階検索を行うことにより、数１０万件以上の登録があっても高速に検索できる。また、１つの特徴量のサイズが１２８バイトと小さいので、８００万件あっても１Ｇバイトであり、オンメモリでの超高速検索も現実的である。以下、テンプレート保護の種類毎に、ＤＢ検索の詳細を説明する。
【００６８】
図９及び図１１に、Ｓ８７におけるＤＢ検索の機能手段のバリエーションが示される。
図９の（ａ）の例のＤＢ検索手段８７ａは、テンプレート保護部４４ａで保護され、ク

ラスタ化部６５ａでクラスタリングされた特徴量を検索するものである。保護された特徴量は、ハッシュ値及び残差で構成され、分離器７１で取り出される。またクラスタリングは基本的にハッシュ値と１対１である。

クラスタテーブル９１ａは、ＤＢ６６内のクラスタテーブル６７ａと同じ内容であり、クラスタＩＤとしてハッシュ値を与えると、該当するクラスタの特徴量テーブル９２ａにアクセスできる。

【００６９】

特徴量テーブル９２ａは、ＤＢ６６内のそれと同じもので、保護された特徴量の内の残差が保持されている。

最小距離検索部９３は、当該クラスタの特徴量テーブル９２ａの中で、Ｓ８６で与えられた特徴量の残差と、距離（マンハッタン距離）が最も小さいものを探索し、その特徴量の顔ＩＤを出力する。クラスタのサイズが小さければ、線形探索で構わない。

【００７０】

図９の（ｂ）の例のＤＢ検索手段８７ｂは、テンプレート保護部４４ｂで保護され、クラスタ化部６５ｂでクラスタリングされた特徴量を検索するものである。この特徴量は、その特徴量空間の全体で距離保存されており、テンプレート保護に関係なく任意のクラスタリング手法が利用できる。

クラスタテーブル９１ｂは、クラスタテーブル６７ａと同じ内容であり、クラスタＩＤとしてハッシュ値を与えると、該当するクラスタの特徴量テーブル９２ａにアクセスできる。

【００７１】

クラスタテーブル９２ｂは、クラスタテーブル６７ｂと同じもので、ハッシュ値とクラスタＩＤを結びつける辞書と、クラスタリングに用いたハッシュ関数情報を保持している。

ＬＳＨ部９４は、クラスタテーブル９１ｂのハッシュ関数情報を読出し、クエリ特徴量のハッシュ値を出力する。このハッシュ値で辞書を参照し、通常１つのクラスタＩＤを得る。

その後、ＤＢ検索手段８７ａ同様、最小距離検索部９３が当該クラスタ内を検索する。

ＤＢ検索手段８７ｂは、テンプレート保護部４４ｃで保護された特徴量の検索にも使用できる。そのような特徴量は、（クラスタよりも十分大きい）巨視的には、距離保存されているとみなされる。

【００７２】

テンプレート保護部４４ｃで保護され、クラスタ化部６５ｃでクラスタリングされた特徴量を検索するＤＢ検索手段８７ｃは、ＤＢ検索手段８７ａまたは８７ｂと同様なので、説明を省略する。

【００７３】

テンプレート保護部４４ｄで保護され、クラスタ化部６５ｄでクラスタリングされた特徴量を検索するＤＢ検索手段８７ｄは、ＤＢ検索手段８７ｄに、暗号復号化部９４（暗号復号化部７８と同一構成である）を追加しただけなので、説明を省略する。

【００７４】

図１１の例のＤＢ検索手段８７ｅは、テンプレート保護部４４ｅで保護され、クラスタ化部６５ｄでクラスタリングされた特徴量を検索するものである。ここで扱う特徴量は、保護された特徴量の本体と、冗長シンボルとを含んでいる。クラスタ化部６５ｄは、冗長シンボルをＬＳＨのハッシュ値と組み合わせて、クラスタＩＤと対応付けるものとする。ＤＢ検索手段８７ｅは反復処理を伴うため、Ｓ８６のテンプレート保護の手段も一緒に図示してある。

【００７５】

ビット分割器１１１、グレイ符号化器１１２、及び、データ改変器１１４から誤り訂正符号部１１７までは、クエリを生成するテンプレート保護手段であり、図１０に示したビット分割器１０１、グレイ符号化器１０２、及び、データ改変器１０４から誤り訂正符号

部１０７と、それぞれ同じ構成である。
ただし、グレイ符号化器１１２は、データ改変を受ける前のグレイコードをＤＢ検索手段８７ｄに出力することができる。また、事前改変器１１５は、乱数ではなく、ＤＢ検索手段８７ｅから与えられる訂正ビット標識に応じて、改変を行う。また、ＲＰ処理器１１６は、ＤＢ検索手段８７ｅから与えられる訂正されたグレイコードに応じて、ＲＰを行う。
乱数試行制御器１１３は、全通りの乱数について試行する動作を制御するものであり、グレイコードの長さ（ビット数）に相当するｎ個の数を順次、データ改変器１１４に与える。従って、テンプレート保護手段からは、保護された特徴量（冗長シンボルを含む）が最大でｎ通り出力される。このｎ回の試行は、もしクエリと類似する登録がＤＢ８０にあった時に、その登録時に得られていたであろう冗長シンボルを探すためであり、それがハッシュ値がわずかに違ったためか、乱数によるかを区別せず、探すことができる。
【００７６】
誤り訂正復号化器１１９は、グレイ符号化器１１２からの無改変のグレイコードを、誤り訂正符号化器１１７からの冗長シンボルを用いて誤り訂正復号し、正常に訂正できた場合、訂正されたグレイコードと、訂正されたビットの位置を示す訂正ビット標識を出力する。訂正ビットが複数ある場合、１ビットずつ、訂正ビット標識を出力し、試行される。つまり複数の訂正ビットの内、１つは乱数による改変であり、残りは登録時と検索時との間に生じるハッシュ値のわずかな相違によるものと考える。
この結果、訂正ビット標識に基づいて事前改変され、訂正されたグレイコードに基づいてＲＰされた、保護された特徴量が得られる。
ＬＳＨ部１１９は、クラスタ分割部７２で用いられるものと同じハッシュ関数で、保護された特徴量のハッシュ値を計算する。
【００７７】
クラスタテーブル９１ｅは、クラスタテーブル９１ｂと同様のもので、クラスタ毎に、誤り訂正復号化器１１９へ入力された冗長シンボルと、ＬＳＨ部１１９からのハッシュ値とのセット（クラスタＩＤ）を引数としてアクセスすると、当該クラスタの特徴量テーブルにアクセスするためのアドレスやクラスタ属性を返す。ここでは、クラスタ属性として、そのクラスタに分類された任意の１つ以上の特徴量（代表特徴量）が利用可能だとする。もしクラスタ属性が利用不能でも、都度特徴量テーブル９２ｅにアクセスして特徴量を適当に１つ取り出せばよい。
なお、クラスタテーブル９１ｅは辞書型なので、辞書にない（クラスタが存在しない）場合は、次の試行に移動する。
【００７８】
距離計算機１２０は、距離計算部７５と同様のもので、クラスタテーブル９１ｅから返された当該クラスタの特徴量と、クエリの保護された特徴量との距離を計算し、ｎ回の試行の最中、所定の閾値以下の距離が得らる都度、試行中断信号を乱数試行制御器１１３に出力するとともに、最小距離検索部１２１に当該クラスタの特徴量テーブル９２ｅのアドレスを渡す。閾値は、ＬＳＨの荒さに基づき定める。距離が閾値以下になるには、偶然に冗長シンボルが一致するだけでは不十分で、その冗長シンボルを伴って登録された特徴量と類似するクエリが用意できなければならない。
なお、ＤＢ８０に同一人物の登録が複数ある場合、複数回、距離が閾値以下となりうる。
【００７９】
最小距離検索部９３ｅは、渡されたアドレスの特徴量テーブル９２ｅの中から、個人を識別できるレベルで、クエリの保護された特徴量との類似検索を行う。そして、最も類似する特徴量、或いは最初に距離が所定の閾値以下となった特徴量の顔ＩＤを出力する。
最終的にＤＢ検索手段８７ｅは、検索結果として、１つの顔ＩＤか、該当なしの情報を返す。
【００８０】

再び図８に戻り、Ｓ８８では、Ｓ８７の検索で類似人物が見つかっていれば、その結果（顔ＩＤ、特徴量の元となった画像等）を送信する。
なお、最初に動作を開始しているＳ８９は、この検索結果の受信を常に待ち受け、受信した１回分の検索結果を保持することができ、検索結果が保持されている或いは新たに受信したときは、Ｓ９０へ進む。
【００８１】
Ｓ９０では、カメラの前を通り過ぎようとしている人物を呼び止める合成音声を再生するとともに、その人物に本人確認を求める画面を表示する。その際、顔ＩＤを引数にしてＤＢ８０内の個人テーブルを参照して個人情報を取得し、個人情報が含む電話番号がその顔の本人（被確認者）のものか、登録者（確認依頼者）のものかに応じて、本人確認画面の内容を選ぶ。
【００８２】
図１２に、本人確認画面の例を示す。
図１２（ａ）は、本人の電話番号を提示する本人確認画面１２１である。この画面１２１は、画面の前の人物が、提示された電話番号が自分のものだと認識したときに押す同意ボタン（本人ボタン）１２２と、電話番号が自分のものではないと認識したときに押す否認ボタン（別人ボタン）１２３と、判断を保留したいときに押す保留ボタン１２４とを有する。
図１２（ｂ）は、登録者の電話番号を提示する本人確認画面１２６であり、同様に３つのボタンを有する。
【００８３】
本人確認画面が表示されると、Ｓ９１とＳ９２が平行して動作を開始する。
Ｓ９１では、人物によるヒューマンＩ／Ｆの操作を待ち受ける。
Ｓ９２では、タイマを始動する。このタイマはボタン押下のタイムアウト時間（例えば３０秒）になると発火し、ボタン押下が無くても次の処理へ進むことができる。
【００８４】
Ｓ９３では、いずれのボタンを押したか判断する。なお、保留ボタン１２４が押された場合は、特段何もしない。
同意ボタン１２２が押された場合、Ｓ９４として、Ｓ８８で取得した個人情報が示す確認依頼者のメールアドレスや電話番号に宛てて、本人（被確認者）が発見された旨のメールやショートメッセージを送信する。或いは、それらの送信を、ポータルサーバ２や電気通信事業者等に依頼してもよい。メール等には、確認された人物を撮影した場所を示す情報が記載される。メールやショートメッセージの受信が確認依頼者の端末で拒否設定されている可能性もあるので、送信に失敗したときは他の方法或いは他のサーバから再度送信することが望ましい。
【００８５】
Ｓ８９で同意ボタン１２２が押されたと判断された場合、Ｓ９５として、ＤＢ８０の特徴量テーブル或いは個人テーブルから、当該顔ＩＤのレコードを削除するなどして、カメラの前を再び通りかかっても、検索に該当しないようにする。
【００８６】
上述のように、現地サーバ２の探知アプリケーションプログラムは、使用できる管理者にしかＤＢ６６を利用できないようにされているので、本来の目的外の使用は困難になっている。また仮に、悪意の利用者に利用されることになっても、検索頻度が制限されているので、例えばフレーム毎に顔画像が切り替わるような映像を用意して検索結果を取り出そうとしても、パフォーマンスが得られない。また類似人物が見つかった場合、個人情報が暴露されうるが、それは電話番号に限られる。電話番号は、オンラインでのクラッキング行為には利用しにくく、また本人ではない登録者のものでは、個人情報としての価値も低いと考えられる。或いは、電話番号の代わりに、本人と登録者の間でしか理解できない秘密の合言葉等を用いてもよい。
【００８７】

以上説明した様に、本実施例１の安否確認システム１は、災害時などにおいて被確認者の能動的な作業なしに被確認者を検索できる。

本例の安否確認システム１は、様々に変形して実施することもできる。本例では通信環境の不安定さを考慮し、現地サーバ２へダウンロードされるＤＢは、ポータルサーバのＤＢ６６と同じとしたが、例えば、クラスタテーブルのみ、或いはクラスタテーブルと特徴量テーブルのみとし、類似検索の成否に応じて必要な情報はポータルサーバから逐次取得するようにしてもよい。

また、Ｓ９４の通知を受取った確認依頼者から、所定時間内に登録継続の依頼が無い場合や、登録から所定日数経過した場合に、ＤＢ６６から当該登録を抹消してもよい。

【００８８】

本例の安否確認システム１はまた、様々な用途に応用することもできる。本例では、本人が生存していることを前提としたが、例えば、警察や在外公館等が遺体の顔写真から身元を推定する目的にも使用できる。類似が認められた顔の登録者の連絡先（生データ）は、警察に提供され、親族等や歯科医に本人確認を依頼するために利用される。

なお、登録した内容が誰に開示されどのように使用されるか、登録者に認識できるように提示したうえで登録が行われることが望ましい。

或いは、登録する顔は遺体のものとし、安否確認依頼をクエリとしてもよい。

【００８９】

ここで、本発明に係るシステムや装置などの構成としては、必ずしも以上に示したものに限られず、種々な構成が用いられてもよい。また、本発明は、例えば、本発明に係る処理を実行する方法或いは装置や、そのような方法をコンピュータに実現させるためのプログラムや、当該プログラムを記録する一過性ではない有形の媒体などとして提供することもできる。

【産業上の利用可能性】

【００９０】

秘匿化されたデータを類似検索する装置等に広く利用でき、バイオメトリクス認証システム、ＣＣＴＶ（Closed-Circuit Television ）システム等に好適である。

【符号の説明】

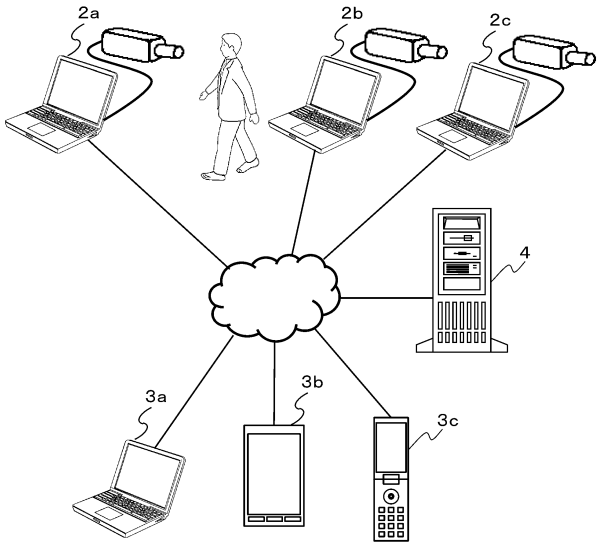
【００９１】

２：映像蓄積サーバ、　３：類似顔画像検索サーバ、　４：表示端末、　５：管理端末、　６：ＬＡＮ、　１１：施設、　１２、１２ａ、１２ｂ、１２ｃ、１２ｄ：監視カメラ、　１３：データベース（ＤＢ）、　１４：ホワイトリスト、１５：不審者登場リスト、１６：選別・間引き部、　１７：グループ化部、　１８：不審者候補検索部、　１９：不審者判断部、

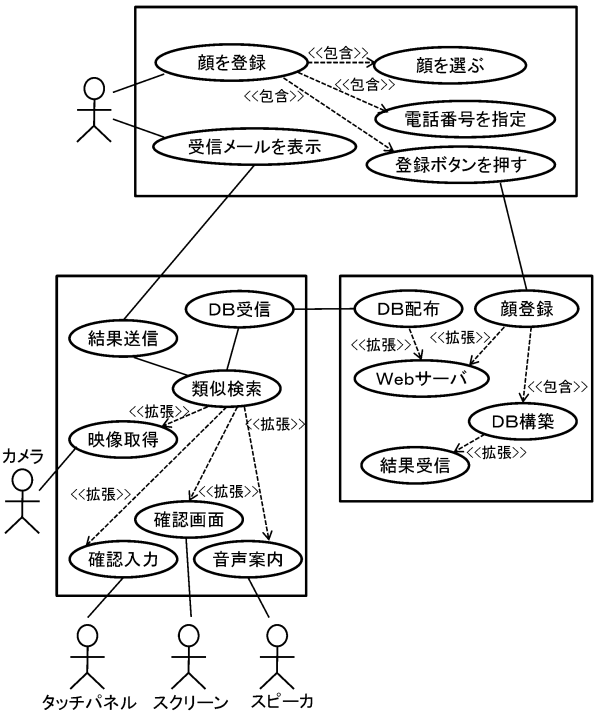
２１：カメラＩ／Ｆ、　２２：記録配信制御部、　２３：Ｗｅｂサーバ部、　２４：ストレージ、　２５：設定保持部２５、　４１：画像取得Ｉ／Ｆ、　４２：顔検出・特徴量算出部、　４３：顔登録・検索部、　４４：顔特徴量ＤＢ、　４５：Ｗｅｂサービス部、

４６：検索トリガー部、　４７：設定保持部、　４８：障害通知部、７１：人物ＩＤテーブル、　７２：最終検索日時リスト、　７３：ブラックリスト。

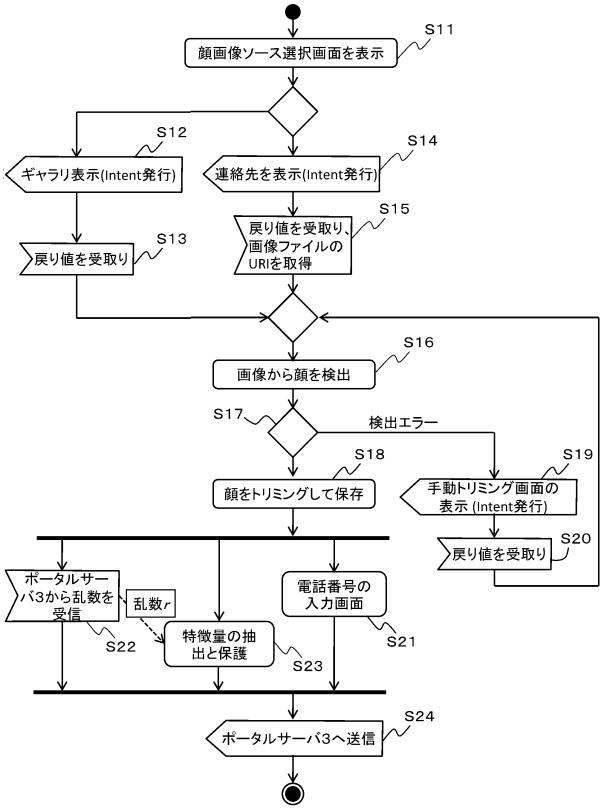
【図１】


2a
2b
2c
4
3a
3b
3c

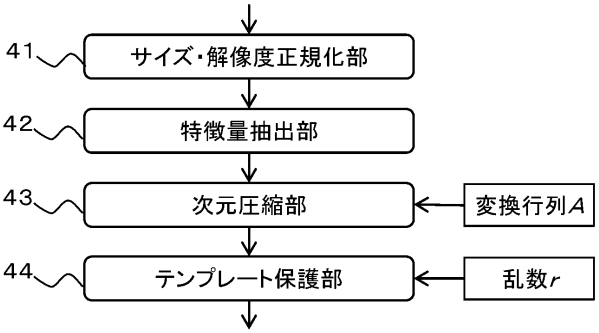
【図２】


顔を登録
顔を選ぶ
電話番号を指定
受信メールを表示
登録ボタンを押す
<<包含>>
DB受信
結果送信
類似検索
映像取得
確認画面
確認入力
音声案内
DB配布
顔登録
Webサーバ
DB構築
結果受信
<<拡張>>
カメラ
タッチパネル
スクリーン
スピーカ

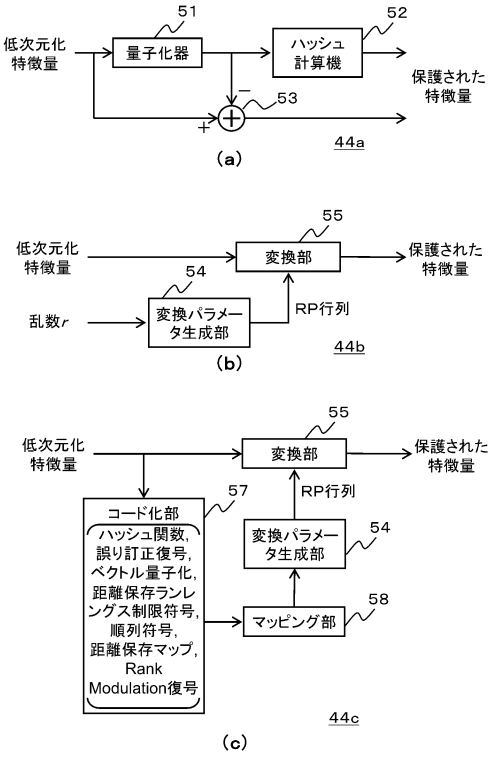
【図３】


顔画像ソース選択画面を表示
S11
ギャラリ表示(Intent発行)
S12
連絡先を表示(Intent発行)
S14
戻り値を受取り
S13
戻り値を受取り、画像ファイルのURIを取得
S15
画像から顔を検出
S16
S17
検出エラー
顔をトリミングして保存
S18
手動トリミング画面の表示 (Intent発行)
S19
戻り値を受取り
S20
ポータルサーバ3から乱数を受信
乱数r
S22
特徴量の抽出と保護
S23
電話番号の入力画面
S21
ポータルサーバ3へ送信
S24

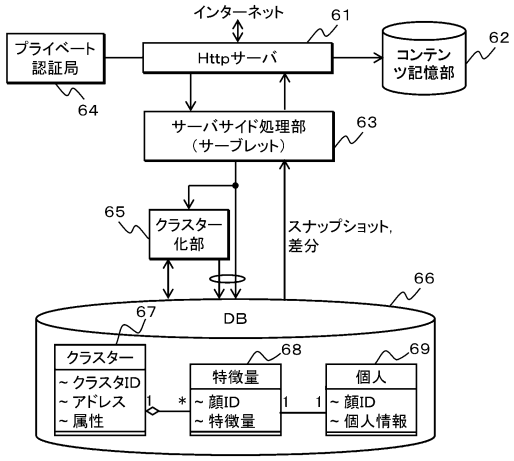
【図４】


41
サイズ・解像度正規化部
42
特徴量抽出部
43
次元圧縮部
変換行列A
44
テンプレート保護部
乱数r

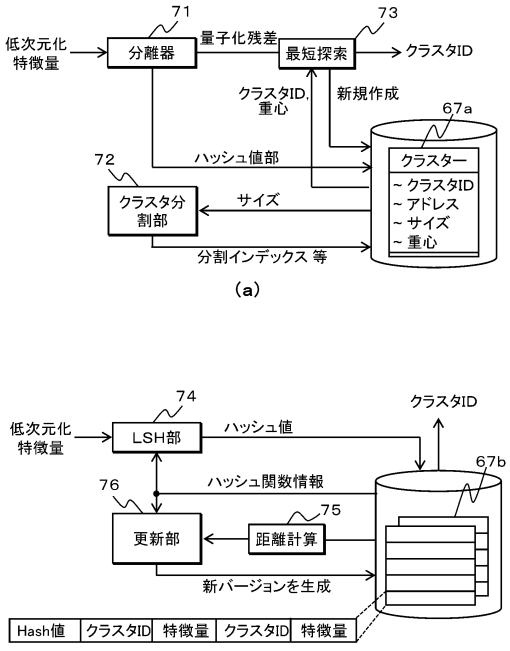
【図５】


低次元化特徴量
量子化器
51
ハッシュ計算機
52
保護された特徴量
53
44a
(a)
低次元化特徴量
変換部
55
保護された特徴量
54
乱数r
変換パラメータ生成部
RP行列
44b
(b)
低次元化特徴量
変換部
55
保護された特徴量
RP行列
57
コード化部
ハッシュ関数,
誤り訂正復号,
ベクトル量子化,
距離保存ランレングス制限符号,
順列符号,
距離保存マップ,
Rank Modulation復号
変換パラメータ生成部
54
マッピング部
58
44c
(c)
低次元化特徴量
公開鍵暗号化部
60
保護された特徴量
公開鍵
(乱数r)
44d
(d)

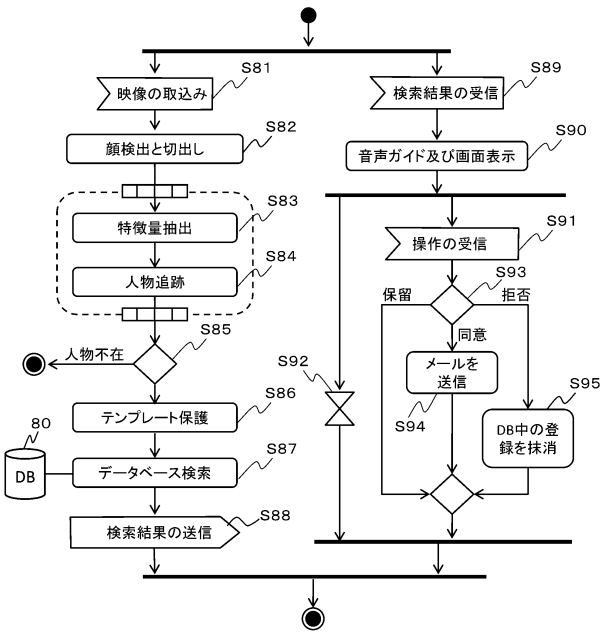
【図６】


インターネット
61
プライベート認証局
64
Httpサーバ
コンテンツ記憶部
62
サーバサイド処理部
(サーブレット)
63
65
クラスター化部
スナップショット,
差分
66
DB
67
クラスター
~ クラスタID
~ アドレス
~ 属性
68
特徴量
~ 顔ID
~ 特徴量
69
個人
~ 顔ID
~ 個人情報

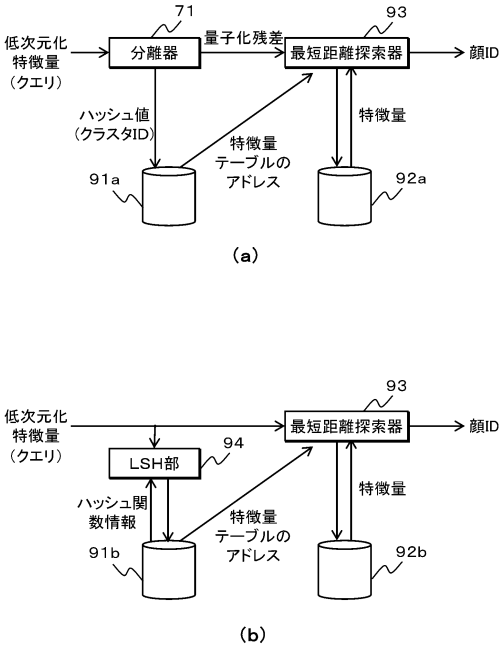
【図７】


低次元化特徴量
分離器
71
量子化残差
最短探索
73
クラスタID
クラスタID,
重心
新規作成
67a
クラスター
~ クラスタID
~ アドレス
~ サイズ
~ 重心
72
ハッシュ値部
クラスタ分割部
サイズ
分割インデックス 等
(a)
低次元化特徴量
LSH部
74
ハッシュ値
クラスタID
67b
76
ハッシュ関数情報
更新部
75
距離計算
新バージョンを生成
Hash値
クラスタID
特徴量
クラスタID
特徴量
(b)
低次元化特徴量
暗号復号化部
78
クラスター化部
65b
クラスタID
秘密鍵
DB66へ
65d
(c)

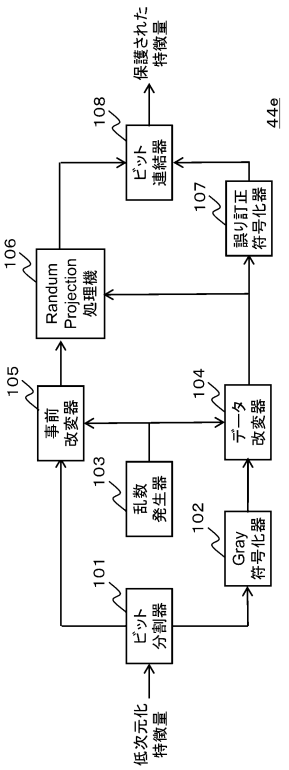
【図８】


S81
映像の取込み
S82
顔検出と切出し
S83
特徴量抽出
S84
人物追跡
S85
人物不在
S86
テンプレート保護
80
DB
S87
データベース検索
S88
検索結果の送信
S89
検索結果の受信
S90
音声ガイド及び画面表示
S91
操作の受信
S93
保留
拒否
同意
メールを送信
S94
S95
DB中の登録を抹消
S92

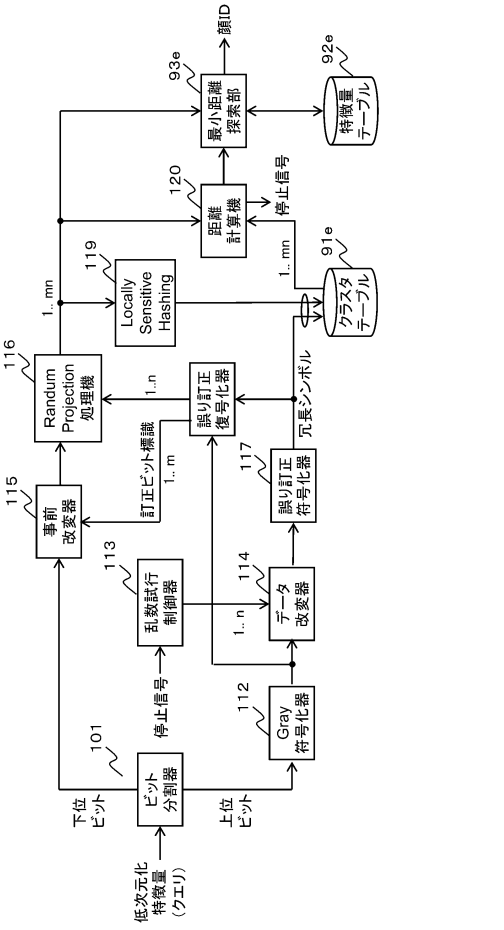
【図９】



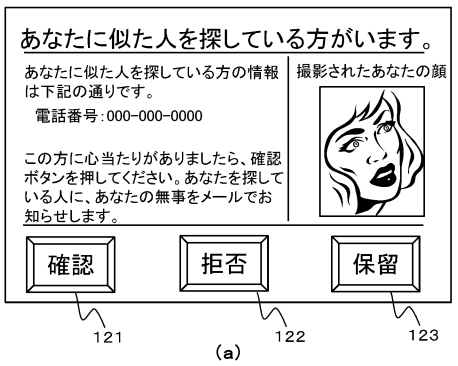
【図１０】

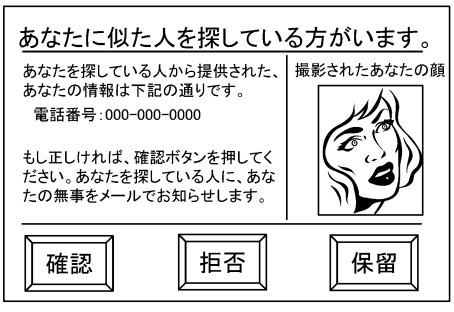


【図１１】



【図１２】





フロントページの続き

(51)Int.Cl. FI
G06F 21/32

(56)参考文献 特開２００７－０５２６９８（ＪＰ，Ａ）
特開２０１１－０２２６４１（ＪＰ，Ａ）
特開２００５－３０１６７７（ＪＰ，Ａ）
特開２００６－２４３７９８（ＪＰ，Ａ）
国際公開第２０１３／０８０３６５（WO，Ａ１）
特開２０１０－２１３２３０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ １７／３０
Ｇ０６Ｆ ２１／３２
Ｇ０６Ｆ ２１／６２
Ｇ０６Ｑ １０／００－９９／００