(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2013-27011
(P2013-27011A)
(43)公開日　平成25年2月4日(2013.2.4)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/08	(2006.01)	H04L	9/00	601A	5C052
H04N	5/225	(2006.01)	H04N	5/225	C	5C122
H04L	9/32	(2006.01)	H04N	5/225	F	5J104
H04N	5/76	(2006.01)	H04L	9/00	673D	
			H04N	5/76	B	

審査請求 未請求　請求項の数 6　ＯＬ　（全 13 頁）

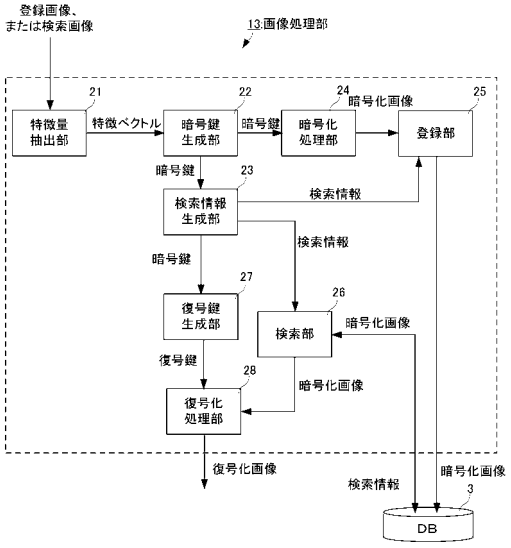
(21)出願番号　特願2011-163049 (P2011-163049)
(22)出願日　平成23年7月26日 (2011.7.26)

特許法第３０条第１項適用申請有り　研究集会名：京都大学工学部情報学科特別研究試問会　主催者名　：国立大学法人京都大学　開催日　：平成２３年２月７日

(71)出願人　504132272
国立大学法人京都大学
京都府京都市左京区吉田本町３６番地１
(71)出願人　000002945
オムロン株式会社
京都市下京区塩小路通堀川東入南不動堂町８０１番地
(74)代理人　110000970
特許業務法人　楓国際特許事務所
(72)発明者　藤田　智彦
京都府京都市左京区吉田本町　国立大学法人京都大学　工学部情報学科内
(72)発明者　舩冨　卓哉
京都府京都市左京区吉田本町　国立大学法人京都大学　学術情報メディアセンター内
最終頁に続く

(54)【発明の名称】画像管理装置、画像管理プログラム、および画像管理方法

(57)【要約】
【課題】暗号化して記録保存している画像を確認することが許容されている管理者等の一部の人に対しても、画像を確認したい対象者と無関係の人については、そのプライバシを保護することができる画像管理装置を提供する。
【解決手段】特徴量抽出部２１が、入力された画像に撮像されている人物の顔の特徴量を抽出する。暗号鍵生成部２２が抽出した人物の顔の特徴量から暗号鍵を生成し、検索情報生成部２３が抽出した人物の顔の特徴量から検索情報を生成する。暗号化処理部２４が生成した暗号鍵で画像を暗号化し、登録部２５が検索情報と、暗号化した画像と、を対応づけてデータベース３に登録する。また、検索部２６が生成した検索情報により、データベース３に登録されている暗号化した画像を検索する。そして、復号化処理部２８が検索された画像を復号化する。
【選択図】図２



【特許請求の範囲】
【請求項１】
画像入力部に入力された画像に撮像されている人物の顔の特徴量を抽出する特徴量抽出部と、
前記特徴量抽出部が抽出した人物の顔の特徴量から暗号鍵を生成する暗号鍵生成部と、
前記特徴量抽出部が抽出した人物の顔の特徴量から検索情報を生成する検索情報生成部と、
前記暗号鍵生成部が生成した暗号鍵で、この暗号鍵を生成した画像を暗号化する暗号化処理部と、
前記検索情報生成部が生成した検索情報と、前記暗号化処理部が暗号化した画像と、を対応づけて記録媒体に登録する登録部と、
前記検索情報生成部が生成した検索情報により、前記記録媒体に登録されている暗号化した画像を検索する検索部と、
前記検索部により検索された画像を復号化する復号化処理部と、を備えた画像管理装置。
【請求項２】
前記暗号鍵生成部が生成した暗号鍵から、復号鍵を生成する復号鍵生成部と、
前記復号化処理部は、前記検索部により検索された画像を、前記復号鍵生成部が生成した復号鍵で復号化する、請求項１に記載の画像管理装置。
【請求項３】
前記検索情報生成部は、前記暗号鍵生成部が生成した暗号鍵を、予め定めた一方向性のハッシュ関数に与えたときに得られたハッシュ値を検索情報として生成する、請求項１、または２に記載の画像管理装置。
【請求項４】
前記特徴量抽出部は、Ｎ次元ベクトルで、前記画像入力部に入力された画像に撮像されている人物の顔の特徴量を抽出し、
前記暗号鍵生成部は、特徴量の次元毎に、その次元の値を予め定めた閾値で２値化したＮビット列を暗号鍵として生成する、請求項１～３のいずれか１項に記載の画像管理装置。
【請求項５】
画像入力部に入力された画像に撮像されている人物の顔の特徴量を抽出する特徴量抽出ステップと、
前記特徴量抽出ステップで抽出した人物の顔の特徴量から暗号鍵を生成する暗号鍵生成ステップと、
前記特徴量抽出ステップで抽出した人物の顔の特徴量から検索情報を生成する検索情報生成ステップと、
前記暗号鍵生成ステップで生成した暗号鍵で、この暗号鍵を生成した画像を暗号化する暗号化処理ステップと、
前記検索情報生成ステップで生成した検索情報と、前記暗号化処理ステップで暗号化した画像と、を対応づけて記録媒体に登録する登録ステップと、
前記検索情報生成ステップで生成した検索情報により、前記記録媒体に登録されている暗号化した画像を検索する検索ステップと、
前記検索ステップにより検索された画像を復号化する復号化処理ステップと、をコンピュータに実行させる画像管理プログラム。
【請求項６】
画像入力部に入力された画像に撮像されている人物の顔の特徴量を抽出する特徴量抽出ステップと、
前記特徴量抽出ステップで抽出した人物の顔の特徴量から暗号鍵を生成する暗号鍵生成ステップと、
前記特徴量抽出ステップで抽出した人物の顔の特徴量から検索情報を生成する検索情報

生成ステップと、
前記暗号鍵生成ステップで生成した暗号鍵で、この暗号鍵を生成した画像を暗号化する暗号化処理ステップと、
前記検索情報生成ステップで生成した検索情報と、前記暗号化処理ステップで暗号化した画像と、を対応づけて記録媒体に登録する登録ステップと、
前記検索情報生成ステップで生成した検索情報により、前記記録媒体に登録されている暗号化した画像を検索する検索ステップと、
前記検索ステップにより検索された画像を復号化する復号化処理ステップと、をコンピュータが実行する画像管理方法。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、駅、繁華街、ショッピングセンタ、コンビニエンスストア等に設置した防犯カメラの撮像画像をデータベース等の記録媒体に記録保存するとともに、必要に応じて記録媒体に記録保存している撮像画像の確認が行える画像管理装置、画像管理プログラム、および画像管理方法に関する。
【背景技術】
【０００２】
従来、駅、繁華街、ショッピングセンタ、コンビニエンスストア等では、防犯カメラを設置している。管理者や警備担当者は、防犯カメラの撮像画像を確認し、特異な行動をとった不審者等の人物（以下、単に不審者と言う。）がいれば、その不審者に対して対応する。また、防犯カメラの撮像画像は、しばらくの間、データベース等の記録媒体に記録保存しており、必要に応じて確認することができる。
【０００３】
データベース等の記録媒体に記録保存される撮像画像には、不審者だけでなく、多数の人（不審者でない人）が撮像されている。したがって、記録保存している撮像画像の管理者は、この撮像画像が漏洩した場合であっても、撮像されている人のプライバシの保護を考慮しなければならない。このプライバシの保護を実現するために、画像を暗号化してデータベース等の記録媒体に記録保存するものがある（特許文献１～３等参照）。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２００９－　４４３１１号公報
【特許文献２】特開２００８－１７８０５４号公報
【特許文献３】国際公開ＷＯ２００６／１１５１５６号
【発明の概要】
【発明が解決しようとする課題】
【０００５】
しかしながら、特許文献１～３等に記載されているものは、データベース等の記録媒体に記録保存されている撮像画像が漏洩した場合に、漏洩した撮像画像が誰にでも確認されるのを防止しているだけであった。
【０００６】
一方で、防犯カメラの撮像画像は、上述したように、必要に応じて確認できるように、しばらくの間、データベース等の記録媒体に記録保存している。すなわち、特許文献１～３等に記載されているものは、管理者等の一部の人については、データベース等の記録媒体に暗号化して記録保存されている撮像画像を、復号化して確認できるように構成している。したがって、管理者等の一部の人は、不審者等の特定の人物（対象者）について記録保存されている撮像画像を確認するとき、記録保存されている撮像画像に撮像されている対象者とは無関係である不特定多数の人の撮像画像についても確認できる。このため、管理者等の一部については、記録保存されている撮像画像に撮像されている不特定多数の人

のプライバシが保護されていなかった。例えば、管理者等の一部の人が、対象者について記録保存されている撮像画像を確認したときに、確認した撮像画像に撮像されていた対象者と無関係の人の個人情報を偶然知り、それを周囲の人にもらす可能性がある。また、管理者等の一部の人が、悪意を持って、記録保存されている撮像画像を確認することもある。

【０００７】

この発明の目的は、暗号化して記録保存している画像を確認することが許容されている管理者等の一部の人についても、画像を確認したい対象者と無関係の人については、そのプライバシを保護することができる画像管理装置、画像管理プログラム、および画像管理方法を提供することにある。

【課題を解決するための手段】

【０００８】

この発明の画像管理装置は、上記課題を解決し、その目的を達するため、以下のように構成している。

【０００９】

特徴量抽出部が、画像入力部に入力された画像に撮像されている人物の顔の特徴量を抽出する。画像入力部に入力される画像は、静止画像であってもよいし、動画像であってもよい。動画像の場合は、その動画像を構成するフレーム画像に対して処理を行う。特徴量抽出部は、例えば撮像されている人物の顔の輪郭、目、鼻、口等の顔部品の大きさや形状等を特徴量として抽出する。

【００１０】

暗号鍵生成部が、特徴量抽出部が抽出した人物の顔の特徴量から暗号鍵を生成する。検索情報生成部が、特徴量抽出部が抽出した人物の顔の特徴量から検索情報を生成する。暗号化処理部が、暗号鍵生成部が生成した暗号鍵で、この暗号鍵を生成した画像を暗号化する。登録部が、検索情報生成部が生成した検索情報と、暗号化処理部が暗号化した画像と、を対応づけて記録媒体に登録する。

【００１１】

したがって、記録媒体に登録されている画像（記録保存されている画像）は、その画像に撮像されている人物の顔（顔の特徴量）に基づいて生成された暗号鍵で暗号化されている。すなわち、記録媒体に登録されている画像は、その画像に撮像されている人物によって復号化するのに用いる鍵（復号鍵）が異なる。復号鍵は、その画像の暗号化に用いた暗号鍵と同じ鍵（暗号鍵）であってもよいし、異なる鍵（暗号鍵と対になる鍵）であってもよい。

【００１２】

また、画像入力部には、暗号化して記録媒体に記録保存する画像だけでなく、記録媒体に記録保存されている画像を確認するときに、画像を確認する人物（検索対象者）の顔画像も入力される。

【００１３】

特徴量抽出部は、検索対象者の顔画像が画像入力部に入力された場合も、上述したように、対象者の顔の特徴量を抽出し、検索情報生成部は、ここで抽出された検索対象者の顔の特徴量に基づき、検索情報を生成する。

【００１４】

検索部が、検索情報生成部が生成した検索情報により、記録媒体に登録されている暗号化した画像、すなわち検索対象者の画像を検索する。そして、復号化処理部が、検索部により検索された画像を復号化する。

【００１５】

したがって、記録保存している画像を確認することが許容されている管理者等の一部の人は、暗号化して記録媒体に記録保存されている画像に対して、検索対象者が撮像されている画像を簡単に確認できる。一方で、検索対象者が撮像されていない画像については、復号化しないので、検索対象者とは無関係の人にかかるプライバシは、管理者等の一部の

人に対しても保護できる。
【００１６】
　また、暗号鍵生成部が生成した暗号鍵から、復号鍵を生成する復号鍵生成部を設けてもよい。この場合、復号鍵は、その画像の暗号化に用いた暗号鍵と対になる鍵を生成する。
【００１７】
　また、検索情報生成部は、暗号鍵生成部が生成した暗号鍵を、予め定めた一方向性のハッシュ関数に与えたときに得られたハッシュ値を検索情報として生成する構成にしてもよい。このように構成すれば、記録媒体に記録保存している暗号化した画像に対応づけている検索情報から、対応する画像の暗号鍵や復号鍵が生成されるのを防止できる。したがって、記録媒体に記録保存されている画像が漏洩した場合においても、記録されている検索情報から、対応する画像が復号化されるのを防止できる。これにより、記録保存している撮像画像が漏洩した場合であっても、撮像されている個人のプライバシを十分に保護できる。
【００１８】
　さらに、暗号鍵生成部は、特徴量抽出部が抽出した人物の顔の特徴量を用いて暗号鍵を生成する。例えば、特徴量抽出部が、Ｎ次元ベクトルで、画像入力部に入力された画像に撮像されている人物の顔の特徴量を抽出し、暗号鍵生成部が、特徴量の次元毎に、その次元の値を予め定めた閾値で２値化したＮビット列を暗号鍵として生成する。これにより、暗号化して記録保存されている画像に撮像されている人物の顔と、検索時に入力された対象者の顔の画像との間における、アングルの違いや、背景の明るさの違い等により生じる、抽出される顔の特徴量の違いを吸収することができる。
【発明の効果】
【００１９】
　この発明によれば、暗号化して記録保存している画像を確認することが許容されている管理者等の一部の人に対しても、画像を確認したい対象者と無関係の人については、そのプライバシを保護することができる。
【図面の簡単な説明】
【００２０】
【図１】画像管理装置の主要部の構成を示すブロック図である。
【図２】画像処理部の機能構成を示す概略のブロック図である。
【図３】登録処理を示すフローチャートである。
【図４】登録処理の過程を説明する図である。
【図５】検索処理を示すフローチャートである。
【発明を実施するための形態】
【００２１】
　以下、この発明の実施形態である画像管理装置について説明する。
【００２２】
　図１は、この発明の実施形態である画像管理装置１の主要部の構成を示すブロック図である。この画像管理装置１には、撮像装置２、データベース３（ＤＢ３）、および表示装置４が接続されている。
【００２３】
　撮像装置２は、例えば駅、繁華街、ショッピングセンタ、コンビニエンスストア等に設置されている防犯カメラである。データベース３は、撮像装置２で撮像した撮像画像を記録保存する記録媒体である。表示装置４は、撮像装置２が撮像している撮像画像をリアルタイムで表示したり、データベース３に記録保存されている画像を表示したりするためのモニタである。
【００２４】
　この画像管理装置１は、撮像装置２の撮像画像を暗号化し、暗号化した撮像画像をデータベース３に登録（記録保存）する。また、画像管理装置１は、データベース３に記録されている画像を検索し、この検索で得た画像を復号化し、表示装置４に出力する。この画

像管理装置１に接続される撮像装置２は、１台であってもよいし、複数台であってもよい。また、撮像装置２の撮像画像を記録保存するデータベース３は、画像管理装置１毎に備える構成であってもよいし、複数の画像管理装置１で共有する構成であってもよい。

【００２５】

画像管理装置１は、図１に示すように、制御部１１と、画像入力部１２と、画像処理部１３と、操作部１４と、出力部１５と、を備えている。

【００２６】

制御部１１は、画像管理装置１本体各部の動作を制御する。

【００２７】

画像入力部１２は、撮像装置２を接続している。画像入力部１２は、撮像装置２から撮像画像が入力される。また、画像入力部１２は、後述する検索画像の入力も受け付ける。

【００２８】

画像処理部１３は、画像入力部１２に入力された登録画像（撮像装置２の撮像画像）を処理し、この画像を暗号化してデータベース３に記録保存する。また、画像処理部１３は、画像入力部１２に入力された検索画像を処理し、データベース３に記録保存されている画像の中から該当する画像を検索し、検索した画像を復号化する。

【００２９】

操作部１４は、キーボードやマウス等の入力デバイスを有し、オペレータによる入力操作を受け付ける。オペレータは、データベース３に記録保存されている画像の確認が許容される管理者等である。

【００３０】

出力部１５は、表示装置４を接続している。出力部１５は、画像入力部１２に入力された画像や、データベース３から検索して復号化した画像を、接続されている表示装置４に出力する。出力部１５は、上述した表示装置４以外に、プリンタ等の印字装置の接続も行える。

【００３１】

次に、上述した画像処理部１３の機能構成について説明する。図２は、画像処理部１３の機能構成を示す概略のブロック図である。画像処理部１３は、特徴量抽出部２１と、暗号鍵生成部２２と、検索情報生成部２３と、暗号化処理部２４と、登録部２５と、検索部２６と、復号鍵生成部２７と、復号化処理部２８と、を有している。

【００３２】

特徴量抽出部２１は、画像入力部１２に入力された登録画像、または検索画像に撮像されている人物の顔の特徴量を抽出する。輪郭、目、鼻、口等の顔部品の大きさや形状等、特徴量を抽出する項目（抽出項目）については予め定めている。抽出する特徴量は値である。特徴量抽出部２１は、抽出した特徴量に基づくＮ次元のベクトル（以下、特徴ベクトルと言う。）を生成する。特徴ベクトルは、数十～数百程度（５０～２００程度）の次元ベクトルである。撮像されている人物が同一人物であれば、２つの画像から抽出した特徴ベクトル間の距離は比較的小さいが、２つの画像間における、アングルの違いや、背景の明るさの違い等により、完全に一致することは稀である。撮像されている人物が同一人物でなければ、２つの画像から抽出した特徴ベクトル間の距離は、同位置人物である場合に比べれば極めて大きくなる。

【００３３】

暗号鍵生成部２２は、特徴ベクトルの次元毎に、その値を予め定めた閾値と比較し、閾値未満であれば「０」、閾値以上であれば「１」としたＮビット列の暗号鍵を生成する。これにより、同一人物が撮像されている画像であれば、ある程度の確率で同じ暗号鍵を生成することができる。

【００３４】

検索情報生成部２３は、暗号鍵生成部２２が生成した暗号鍵から検索情報を生成する。具体的には、暗号鍵生成部２２が生成した暗号鍵を、予め定めている一方向性のハッシュ関数に与え、このときに得られたハッシュ値を検索情報として取得する。上述したように

、同一人物が撮像されている画像であれば、ある程度の確率で同じ暗号鍵を生成することができるので、同一人物が撮像されている画像であれば、ある程度の確率で同じ検索情報が得られる。また、暗号鍵は、特徴量抽出部２１が抽出した画像（登録画像、または検索画像）に撮像されている人物の顔の特徴量に基づいて生成していることから、検索情報も特徴量抽出部２１が抽出した画像に撮像されている人物の顔の特徴量に基づいて生成されている。

【００３５】

暗号化処理部２４は、暗号鍵生成部２２が生成したＮビット列の暗号鍵を用いて、登録画像を暗号化する。暗号化処理部２４は、静止画像を暗号化するときは、その静止画像にかかる画像データを暗号鍵で暗号化する。また、暗号化処理部２４は、動画像を暗号化するときは、その動画像にかかる動画像データ（ＭＰＥＧ等により圧縮された動画像データ）を暗号鍵で暗号化する。

【００３６】

登録部２５は、暗号化処理部２４が暗号化した画像（暗号化画像）と、検索情報生成部２３が生成した検索情報と、を対応づけてデータベース３に登録する。登録部２５は、暗号鍵生成部２２が生成した暗号鍵については、データベース３に登録した暗号化画像に対応づけない。すなわち、データベース３に記録保存している暗号化画像には、検索情報が対応づけられているが、暗号鍵については対応づけられていない。

【００３７】

検索部２６は、検索情報生成部２３が生成した検索情報を用いて、データベース３に記録保存されている画像を検索する。

【００３８】

復号鍵生成部２７は、暗号鍵生成部２２が生成したＮビット列の暗号鍵から、この暗号鍵と対になる復号鍵を生成する。暗号鍵と、復号鍵とは同じ鍵であってもよい。この場合、復号鍵生成部２７は、不要にできる。

【００３９】

復号化処理部２８は、復号鍵生成部２７が生成した復号鍵で、検索部２６が検索した画像の復号化を行う。

【００４０】

画像管理装置１は、復号化処理部２８が復号化した画像を出力部１５から出力する。

【００４１】

この画像管理装置１の動作について詳細に説明する。この画像管理装置１は、登録処理、および検索処理を実行する。登録処理は、撮像装置２の撮像画像を暗号化してデータベース３に登録（記録保存）する処理である。また、検索処理は、データベース３に記録保存されている暗号化画像の中から、指定する人物が撮像されている画像を検索し、得られた画像を復号化して出力する処理である。

【００４２】

まず、登録処理について説明する。図３は、登録処理を示すフローチャートである。画像管理装置１は、撮像装置２の撮像画像が登録画像として画像入力部１２に入力されている。

【００４３】

特徴量抽出部２１は、画像入力部１２に入力されたフレーム画像毎に、そのフレーム画像に人物の顔が撮像されているかどうかを判定する（ｓ１）。画像処理部１３は、人物の顔が撮像されていない画像については、以下に示すｓ２以降の処理を実行しない。すなわち、人物の顔が撮像されていない画像については、データベース３に登録しない。

【００４４】

特徴量抽出部２１は、ｓ１で人物の顔が撮像されている画像であると判定すると、撮像されている人物の顔の特徴量を抽出し、ここで抽出した特徴量に基づく、Ｎ次元の特徴ベクトルを生成する（ｓ２）。例えば、図４（Ａ）に示す人物Ａの顔が撮像されている場合、

特徴ベクトルＡ＝（ｘ１，ｘ２，ｘ３，・・・ｘｎ）を生成し、
図４（Ｂ）に示す人物Ｂの顔が撮像されている場合、
特徴ベクトルＢ＝（ｙ１，ｙ２，ｙ３，・・・ｙｎ）を生成し、
図４（Ｃ）に示す人物Ｃの顔が撮像されている場合、
特徴ベクトルＣ＝（ｚ１，ｚ２，ｚ３，・・・ｚｎ）を生成する。このｓ２で生成する特徴ベクトルの各次元の値は特徴量である。

【００４５】

暗号鍵生成部２２は、特徴量抽出部２１が生成した特徴ベクトルから、暗号鍵を生成する（ｓ３）。ｓ３では、予め定めた閾値Ｔｈを用い、特徴ベクトルの次元毎に、その値が、予め定めている閾値Ｔｈ以上であれば「１」、閾値Ｔｈ未満であれば「０」としたＮビット列の暗号鍵を生成する。

【００４６】

また、検索情報生成部２３は、暗号鍵生成部２２が生成した暗号鍵から検索情報を生成する（ｓ４）。検索情報生成部２３は、暗号鍵生成部２２が生成した暗号鍵を、予め定めている一方向性のハッシュ関数に与え、このときに得られたハッシュ値を検索情報として取得する。暗号鍵生成部２２が生成した暗号鍵を検索情報から得ることは理論的にいえば不可能ではないが、実質的には非常に困難である。

【００４７】

暗号化処理部２４は、暗号鍵生成部２２が生成した暗号鍵で、この暗号鍵を生成した人物の顔が撮像されている登録画像を暗号化する（ｓ５）。すなわち、登録画像に撮像されている人物の顔の特徴量に基づいて生成した暗号鍵により、この人物の顔が撮像されている登録画像を暗号化する。

【００４８】

ｓ４と、ｓ５にかかる処理の順番は、どちらが先であってもよい。

【００４９】

登録部２５は、暗号化処理部２４が暗号化した暗号化画像と、検索情報生成部２３が生成した検索情報と、を対応づけてデータベース３に記録保存する（ｓ６）。このとき、暗号鍵生成部２２が生成した暗号鍵については、データベース３に記録する暗号化画像に対応づけない。

【００５０】

なお、データベース３に記録保存する画像は、静止画像であってもよいし、動画像であってもよい。動画像の場合は、暗号鍵を生成した人物が撮像されている動画像にかかる動画像データを生成し、この動画像データを暗号鍵で暗号化すればよい。

【００５１】

このように、データベース３には、暗号化画像と、検索情報とが対応づけて登録され、これが記録保存される。

【００５２】

次に、検索処理について説明する。図５は、この検索処理を示すフローチャートである。オペレータが、データベース３に記録保存されている暗号化画像に対して、検索する人物（検索対象者）の顔が撮像されている画像（検索画像）を画像入力部１２に入力する。この検索画像の入力は、例えば、検索対象者の顔画像が撮像されている写真等をスキャナで読み取らせて入力する構成であってもよいし、検索対象者が撮像されている写真等の画像データを入力する構成であってもよいし、さらには、撮像装置２で撮像した検索対象者が撮像されているフレーム画像を入力する構成であってもよい。

【００５３】

この検索処理では、画像入力部１２に検索画像が入力されると（ｓ１１）、上述した登録処理と同様に、特徴量抽出部２１が、画像入力部１２に入力された検索画像に撮像されている人物の顔の特徴量を抽出し、Ｎ次元の特徴ベクトルを生成する（ｓ１２）。

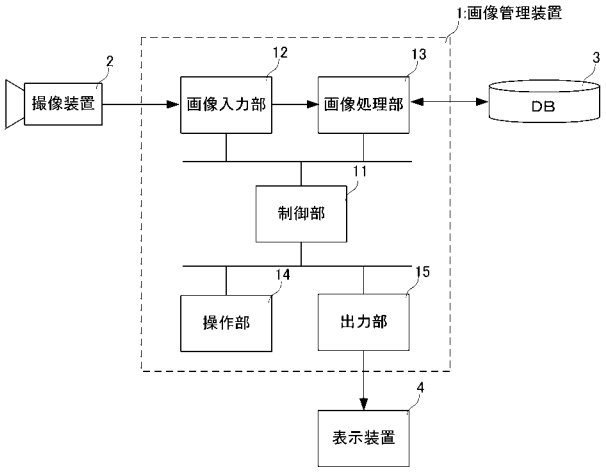
【００５４】

暗号鍵生成部２２は、特徴量抽出部２１が生成した特徴ベクトルから、暗号鍵を生成す

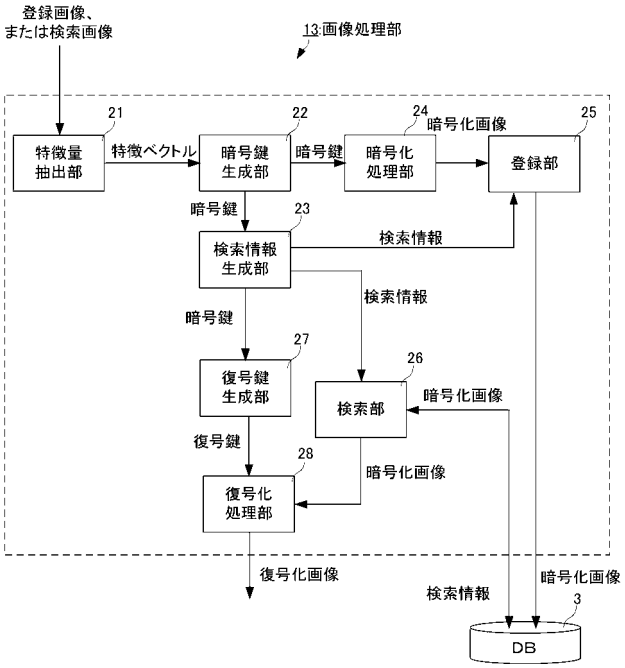
る（ｓ１３）。ｓ１３は、上述したｓ３と同じ処理である。
【００５５】
一般に、同一人物であっても、撮像画像における周辺の明るさや、顔の向き等のアングルの相違により、完全に一致する可能性は極めて低いが、顔の特徴量が同じであることから特徴ベクトルが大きく異なることはなく、ある程度近似したもの（極めて近いもの）になる。そして、上述したように、暗号鍵は、特徴ベクトルを、次元毎に、予め定めた閾値Ｔｈで２値化したＮビット列であるので、同一人物である場合、暗号鍵生成部２２で生成される暗号鍵は、ある程度の確率で一致する。
【００５６】
検索情報生成部２３は、暗号鍵生成部２２が生成した暗号鍵から検索情報を生成する（ｓ１４）。ｓ１４は、上述したｓ４と同じ処理である。また、上述したように、同一人物である場合、暗号鍵生成部２２で生成される暗号鍵が、ある程度の確率で一致することから、検索情報も同じ確率で一致する。
【００５７】
検索部２６は、ｓ１４で生成した検索情報をキーにして、データベース３を検索する（ｓ１５）。ｓ１５では、データベース３に記録保存されている画像中から、検索情報が一致する画像（暗号化された画像）を検索する。上述したように、同一人物である場合、検索情報がある程度の確率で一致することから、データベース３に記録保存されている画像の中で、今回入力された検索画像に撮像されている人物が撮像されている画像については、ある程度の割合で検索できる。また、データベース３に記録保存されている画像の中で、今回入力された検索画像に撮像されている人物が撮像されていない画像が、誤って検索されることもない。
【００５８】
復号鍵生成部２７は、ｓ１５で検索された画像があれば（ｓ１６）、ｓ１３で生成した暗号鍵で暗号化された画像を復号するのに用いる復号鍵を生成する（ｓ１７）。復号鍵は、ｓ１３で生成した暗号鍵に対になる鍵である。例えば、暗号鍵を公開鍵とした場合における、秘密鍵が復号鍵である。
【００５９】
なお、ｓ１３で生成した暗号鍵を、復号鍵とする構成であってもよい。この場合、ｓ１５にかかる処理を不要にできる。
【００６０】
また、画像処理部１３は、ｓ１５で検索された画像がなければ、該当画像なしを制御部１１に通知する（ｓ１８）。
【００６１】
復号化処理部２８は、検索部２６によるデータベース３の検索により得られた暗号化画像を、ｓ１７で生成した復号鍵で復号する（ｓ１９）。
【００６２】
画像管理装置１は、復号化処理部２８が復号化した画像を出力部１５から出力する。
【００６３】
このように、画像管理装置１は、オペレータが用いた検索画像に撮像されている人物については、データベース３を検索し、記録保存されている当該人物が撮像されている画像を復号化して出力する。一方、オペレータが用いた検索画像に撮像されていない人物については、データベース３から検索されることがないので、オペレータ等に対しても検索対象者以外の人のプライバシを十分に保護することができる。
【００６４】
また、データベース３には、暗号化した画像と、検索情報と、を対応づけて登録しているだけであるので、このデータベース３に記録保存している画像が漏洩しても、データベース３に記録保存している暗号化画像が復号化されて確認されるのを防止できる。したがって、データベース３に記録保存している画像の漏洩に対するプライバシの保護も十分に確保できる。

【００６５】
なお、登録画像に撮像されている人物が複数人である場合は、撮像されている人物毎に暗号鍵を生成し、生成した暗号鍵毎に、画像を暗号化してデータベース３に記録保存すればよい。
【００６６】
また、上記の例では、同一人物が撮像されている場合、生成する暗号鍵、および検索情報を、ある程度の確率で一致させるために、特徴ベクトルに対して、予め定めた閾値Ｔｈを用いてＮビット列の暗号鍵を生成し、この暗号鍵を予め定めた一方向性のハッシュ関数に与え、このときに得られたハッシュ値を検索情報とする構成としたが、以下のように最近傍法を利用してもよい。
【００６７】
まず、予め特徴ベクトル空間に対し、ランダムに代表点をＫ個生成しておく。撮像されている人物の顔画像から取得された特徴ベクトルの値を求める際、この特徴ベクトル空間中で、最も近傍にある代表点を探索する。そして、このベクトル（あるいは、探索した代表点のＩＤ）から、暗号鍵を生成する。この方法であれば、代表点の近傍にある特徴ベクトルからはすべて同じ鍵を生成することができる。また、任意の特徴ベクトルに対して、Ｋ種類の鍵を生成することから、代表点の個数であるＫを十分に大きくしておけば、上記の例と同様の効果を奏する。
【００６８】
なお、この場合、Ｋを大きくすると、最近傍点を探索する際に必要な計算量が大きくなるが、公知のＶＰ木(Vantage-point tree)のようなデータ構造を導入することで、その計算量が十分に抑えられる。
【００６９】
また、画像管理装置１は、上述した登録機能のみを有する第１の装置と、上述した検索機能のみを有する第２の装置と、の２つの装置に分けて構成してもよい。
【符号の説明】
【００７０】
１…画像管理装置
２…撮像装置
３…データベース（ＤＢ）
４…表示装置
１１…制御部
１２…画像入力部
１３…画像処理部
１４…操作部
１５…出力部
２１…特徴量抽出部
２２…暗号鍵生成部
２３…検索情報生成部
２４…暗号化処理部
２５…登録部
２６…検索部
２７…復号鍵生成部
２８…復号化処理部

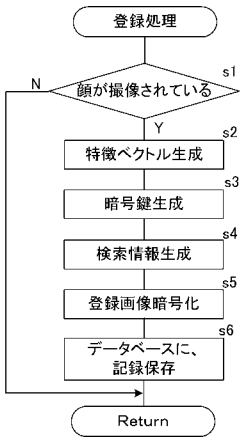
【図１】


1:画像管理装置
2
撮像装置
12
画像入力部
13
画像処理部
3
DB
11
制御部
14
操作部
15
出力部
4
表示装置

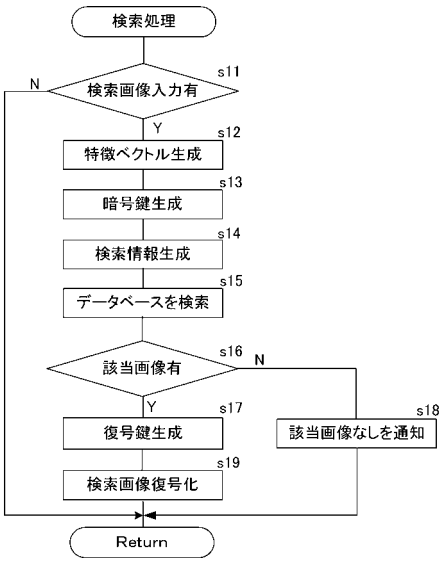
【図２】


登録画像、
または検索画像
13:画像処理部
21
特徴量
抽出部
特徴ベクトル
22
暗号鍵
生成部
暗号鍵
24
暗号化
処理部
暗号化画像
25
登録部
暗号鍵
23
検索情報
生成部
検索情報
暗号鍵
27
復号鍵
生成部
26
検索部
暗号化画像
復号鍵
28
復号化
処理部
暗号化画像
復号化画像
検索情報
暗号化画像
3
DB

【図３】


登録処理
s1
顔が撮像されている
N
Y
s2
特徴ベクトル生成
s3
暗号鍵生成
s4
検索情報生成
s5
登録画像暗号化
s6
データベースに、
記録保存
Return

【図５】


検索処理
s11
検索画像入力有
N
Y
s12
特徴ベクトル生成
s13
暗号鍵生成
s14
検索情報生成
s15
データベースを検索
s16
該当画像有
N
Y
s17
復号鍵生成
s18
該当画像なしを通知
s19
検索画像復号化
Return

【図４】

(A)

特徴ベクトル：(x1, x2, x3, ・・・, xn)

⇩

暗号鍵：(1, 0, 0, ・・・, 1)

⇩

検索情報：(XXXXX)

(B)

特徴ベクトル：(y1, y2, y3, ・・・, yn)

⇩

暗号鍵：(1, 1, 0, ・・・, 0)

⇩

検索情報：(YYYYY)

(C)

特徴ベクトル：(z1, z2, z3, ・・・, zn)

⇩

暗号鍵：(0, 1, 1, ・・・, 1)

⇩

検索情報：(ZZZZZ)

フロントページの続き

(72)発明者　森村　吉貴
京都府京都市左京区牛の宮町　国立大学法人京都大学　物質－細胞統合システム拠点内
(72)発明者　美濃　導彦
京都府京都市左京区吉田本町　国立大学法人京都大学　学術情報メディアセンター内
(72)発明者　労　世紅
東京都港区港南二丁目３番１３号　オムロンソーシアルソリューションズ株式会社内
(72)発明者　倉田　剛
東京都港区港南二丁目３番１３号　オムロンソーシアルソリューションズ株式会社内

Ｆターム(参考) 5C052 AB03 AB04 AC08
5C122 DA11 EA07 FH11 FK23 GA18 GA34 HA02 HA24 HA29 HA32
HB01 HB05
5J104 AA16 EA04 EA15 EA23 JA03 JA21 NA02 NA37 PA14