

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第5984191号
(P5984191)

(45) 発行日 平成28年9月6日(2016.9.6)

(24) 登録日 平成28年8月12日(2016.8.12)

(51) Int. Cl.	F I
G06Q 30/06 (2012.01)	G06Q 30/06
G06Q 20/40 (2012.01)	G06Q 20/40
G08B 25/00 (2006.01)	G08B 25/00 510M
G08B 13/196 (2006.01)	G08B 13/196
A61B 5/1171 (2016.01)	A61B 5/10 360

請求項の数 20 外国語出願 (全 21 頁) 最終頁に続く

(21) 出願番号	特願2014-249517 (P2014-249517)	(73) 特許権者	516049559
(22) 出願日	平成26年12月10日(2014.12.10)		フェイスファースト インコーポレイテッド
(62) 分割の表示	特願2011-520118 (P2011-520118) の分割		FaceFirst, Inc.
原出願日	平成21年7月20日(2009.7.20)		アメリカ合衆国 カリフォルニア州 91361, ウェストレイクビレッジ, アゴウラロード 31416, スイート 250
(65) 公開番号	特開2015-122066 (P2015-122066A)	(74) 代理人	110001302
(43) 公開日	平成27年7月2日(2015.7.2)		特許業務法人北青山インターナショナル
審査請求日	平成26年12月18日(2014.12.18)	(72) 発明者	ローゼンクランツ, ジョセフ, イーサン
(31) 優先権主張番号	12/177, 103		アメリカ合衆国 カリフォルニア州 93012, カマリロ, アヴェニェーダアカソ 999
(32) 優先日	平成20年7月21日(2008.7.21)		
(33) 優先権主張国	米国 (US)	審査官	塩田 徳彦

最終頁に続く

(54) 【発明の名称】 管理生体認証通知システムおよび方法

(57) 【特許請求の範囲】

【請求項 1】

生体認証の利用により所定人物を識別して少なくとも1人のユーザに通知するための管理生体認証通知システム(MBNS)であって、
商業環境を含む複数の異なる種類の環境に設置された複数の画像取得システムであって、それぞれが第1コンテンツを取り込み、取り込んだ第1コンテンツが第1特徴セットを含む画像取得システムと、
比較モジュールおよびケースのデータベースであって、各ケースが第2コンテンツとケースグループとを含む比較モジュールおよびケースのデータベースと、を具備、
前記データベース内のケースのサブセットが、前記第1コンテンツを取り込んだ環境に基づいて選択され、前記サブセット内の少なくとも1つのケースの第2コンテンツが、前記所定人物の第2特徴セットを含み、
前記第1特徴セットが、前記データベースのケースのサブセット内の1またはそれ以上のケースの前記第2特徴セットと一致することを前記比較モジュールが見出した場合に、1またはそれ以上の一致したケースが特定され、
 当該管理生体認証通知システムはさらに、
 特定の一致したケースに対応する通知コンポーネントを受信するための1またはそれ以上の受信ノードを具備、
 (i) 前記一致したケースのケースグループに基づいて、前記通知コンポーネントの受信対象となる1またはそれ以上のユーザグループを特定できるように、ケースグループが

10

20

ユーザグループと結び付けられ、

(i i) 前記一致したケースのケースグループに基づいて、対象となる受信者に対応する 1 またはそれ以上の受信ノードを特定できるように、受信ノードがユーザまたはユーザグループと関連付けられており、

(i i i) 前記受信ノードは前記ユーザが選択可能であり、前記通知コンポーネントは前記ユーザが選択可能であることを特徴とする管理生体認証通知システム。

【請求項 2】

請求項 1 に記載の M B N S において、

対象となる受信者が、万引き犯のケースグループと関連付けられた警備員のユーザグループの警備員であることを特徴とする M B N S 。

10

【請求項 3】

請求項 1 に記載の M B N S において、

前記画像取得システムが、前記画像取得システムのビデオカメラにより取り込まれた複数のフレームから特定のフレームを選択し、前記フレームが顔画像を含み、

前記画像取得システムが、前記特定のフレームから顔画像を分離し、

前記第 1 特徴セットが、分離された顔画像から得られたものであることを特徴とする M B N S 。

【請求項 4】

請求項 1 に記載の M B N S において、

前記比較モジュールがコンピュータ装置に実装され、

当該 M B N S が、システム管理者によって使用されるためのアカウント管理モジュールをさらに具え、

前記アカウント管理モジュールが、システム管理者に対して、複数のユーザに M B N S へのアクセスを許可する手段と、複数のユーザの各々を受信ノードに関連付ける手段とを提供することを特徴とする M B N S 。

20

【請求項 5】

請求項 4 に記載の M B N S において、

前記アカウント管理モジュールが、管理者に対して、画像取得システムを追加してそのシステムを特定のユーザに関連付けるための手段を提供することを特徴とする M B N S 。

【請求項 6】

請求項 3 に記載の M B N S において、

第 1 コンテンツから得た情報が、前記ケースのデータベースにケースを登録するために使用されることを特徴とする M B N S 。

30

【請求項 7】

請求項 1 に記載の M B N S において、

複数の環境が複数のケースグループと関連付けられ、

第 1 コンテンツが、特定の環境において取り込まれ、

ケースとケースグループ間の特徴付けが、マッチングに使用される第 2 コンテンツの識別を容易にすることを特徴とする M B N S 。

40

【請求項 8】

請求項 1 に記載の M B N S において、

人の身元が前記通知コンポーネントに含まれ、

識別された人の傾向が前記通知コンポーネントに含まれ、

人の身元の決定が、第 1 コンテンツにより容易にされることを特徴とする M B N S 。

【請求項 9】

請求項 1 に記載の M B N S において、

前記比較モジュールは、前記通知コンポーネントに含まれる非画像情報を決定することを特徴とする M B N S 。

【請求項 10】

請求項 9 に記載の M B N S において、

50

複数のカテゴリの非画像情報が複数のケースグループに関連付けられ、
非画像情報のカテゴリとケースグループの関連付けが、前記通知コンポーネントに含まれる非画像情報の前記比較モジュールによる決定を容易にすることを特徴とするMBNS

【請求項 1 1】

請求項 1 0 に記載のMBNSにおいて、
前記通知コンポーネントは、第 1 コンテンツとともに取り込まれた同時音声を含むことを特徴とするMBNS。

【請求項 1 2】

請求項 2 に記載のMBNSにおいて、
特定の一致したケースが名前と対応するように、各ケースが、名前により少なくとも部分的に特徴付けられ、
通知コンポーネントの情報カテゴリが、一致したケースの名前と当局が関連付けた 1 またはそれ以上の人物を特定することを特徴とするMBNS。

10

【請求項 1 3】

請求項 2 に記載のMBNSにおいて、
前記通知コンポーネントを送信するためのハードウェア及びソフトウェアと、
前記通知コンポーネントを受信するための受信ノードのハードウェア及びソフトウェアと、
送信側のハードウェアと受信側のハードウェアとの間の通信路とをさらに具えることを特徴とするMBNS。

20

【請求項 1 4】

請求項 1 3 に記載のMBNSにおいて、
前記通信路は、ショートメッセージサービス(SMS)を介して受信ノードに前記通知コンポーネントを送るためのものであることを特徴とするMBNS。

【請求項 1 5】

請求項 1 3 に記載のMBNSにおいて、
画像を送信するための受信ノードのハードウェア及びソフトウェアをさらに具え、
前記通信路が、双方向通信路であり、画像を送るために受信ノードにより使用されることを特徴とするMBNS。

30

【請求項 1 6】

請求項 1 3 に記載のMBNSにおいて、
1 またはそれ以上の画像から得た情報が、前記ケースのデータベースにケースを登録するために使用されることを特徴とするMBNS。

【請求項 1 7】

請求項 1 6 に記載のMBNSにおいて、
申込みに基づくMBNSへのアクセスを有し、
前記受信ノードは、MBNSの申込者のところにあり、
前記データベースは、MBNSの申込者のところではなく、
前記通信路がワイドエリアネットワークを利用することを特徴とするMBNS。

40

【請求項 1 8】

請求項 1 3 に記載のMBNSにおいて、
受信した通知コンポーネントを転送するための受信ノードのハードウェア及びソフトウェアをさらに具えることを特徴とするMBNS。

【請求項 1 9】

請求項 1 8 に記載のMBNSにおいて、
前記受信ノードが、前記通知コンポーネントのコンテンツに基づいて、受信者のグループのうち特定の受信者に前記通知コンポーネントを転送することを特徴とするMBNS。

【請求項 2 0】

選択した内容を有する通知コンポーネントを、選択した受信ノードに自動的に配信する

50

生体認証ベースの方法であって、

ケースのデータベースを提供するステップであって、各ケースが、生体測定データセットおよびケースグループによって少なくとも部分的に特徴付けられる、ステップと、
商業環境を含む複数の異なるタイプの環境に画像取得システムを設けるステップと、
一つの前記画像取得システムから生体測定データセットを含む画像を取得するステップと、

前記データベースからケースのサブセットを選択するステップであって、前記ケースのサブセットが、前記画像を取得した特定の環境のタイプに関連したケースグループを有するデータベースのケースである、ステップと、

前記画像を前記ケースと比較して、一致するケースを特定するステップと、
各一致したケースについて、一致したケースに対応する通知コンポーネントを受信する1またはそれ以上の受信ノードを特定するステップとを具え、

前記受信ノードが、ケースとケースグループの関連付けと、受信ノードとケースグループの関連付けとに基づいて特定され、

各一致したケースについて、対応する通知コンポーネントの内容が、ケースとケースグループの関連付けに基づいており、

各一致したケースについて、対応する通知コンポーネントが、ケースにより特定された受信ノードに送信され、

前記受信ノードはユーザが選択可能であり、

前記通知コンポーネントはユーザが選択可能である、
ことを特徴とする方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、通知システムに関する。特に、本発明は管理生体認証通知システムおよび方法に関する。

【背景技術】

【0002】

小売店の犯罪、万引き、および不正行為はアメリカで増加している。この増加は、暴力の発生の増加をもたらす。2006年では、そのような場合に失われた財産の価値は、万引きを除いて、180億ドルであったと報告された。万引きは同じ年に400億ドルの損失をもたらし、2006年に合計580億ドルに達した。何人かはその問題の一部が小売店泥棒の「プロ集団」であったと提言しており、これは十分に組織された人々や大量の商品を盗む暴力団である。このレベルの犯罪と戦うために多くの監視システムが現在用いられているが、大抵の有効なシステムは生体認証製品を利用するものである。

【0003】

生体認証は、身体特性と行動特性に基づいて人を特徴づけて認識する方法に関する研究であり、または言い換えれば、測定可能な生物学的特性を用いて人を特定するシステムである。身体特性は、人間の体の特徴、例えば指紋、虹彩形状、および顔認識などに関するものである。行動特性は、署名、音声またはキーストロークに関連づけられたものである。生体認証は人が変えることができない特性を測定するため、それは認証目的と識別目的に最も有効である。

【0004】

生体認証は、広範囲の小売店、施設、エリア、情報および環境を安全にするためのツールの全セットの中でますます重要な部分になった。生体認証システムの利用が普及しているのは、このシステムが多くの従来のセキュリティシステム（例えばユーザ名、パスワードまたは個人の識別番号）より実質的にさらに安全性を提供することができるからである。顔認識技術は、例えば、人が家、事務所、または類似の環境に入場するのを許可するかどうかを判定するか、または人が指名手配されているかどうか判定するのに用いることができる。

10

20

30

40

50

【 0 0 0 5 】

一般に、「一対多のマッチング」として知られているものでは、生体認証の特徴抽出処理に先立って、生体認証の特徴のアナログ表現またはデジタル表現が生体認証キャプチャデバイスから取得される。多くの従来システムがデータを取り込むデジタル画像技術に依存しており、これは光学、カメラ、または他の電子機器を含む場合がある。画像のデジタル表現（すなわち、生または未処理の画像データ）は、次いで画像データを特定の表現（すなわち、生体認証マーカまたはテンプレート）に変換するアルゴリズムによって処理される。

【 0 0 0 6 】

生体認証の特徴は1または複数の生体認証サンプルから処理または抽出された情報であり、これは次に格納された生体認証の基準との比較に用いることができる。認証サンプルから、生体認証の特徴抽出がテンプレートを生成し、これはデータベースの1または複数の生体認証テンプレートと比較される。生体認証サンプルの統計学上の特徴により、通常完全に一致しない。その理由で、意志決定プロセスが生体認証テンプレートに従って生体認証データを決め、比較スコアが調整可能な閾値を超える場合に認証を確認するのであろう。顔認識はコンピュータを用いることによって機能し、人の顔の構造を分析する。生体認証ソフトウェアは、多くの点および測定値を取得し、目、鼻および口などの特徴間の距離を含む。これは、顎および前頭などの特定の特徴の角度と、顔の様々な部分の長さを含んでもよい。

【 0 0 0 7 】

今日の研究は、生体認証ソフトウェアの側面またはアルゴリズム開発に集中する。開発するアルゴリズムは、この分野で既知の問題、すなわち、偽陽性と陰性の高い数値を低減することを目的とし、これは他人受入率（FAR）と本人拒否率（FRR）と呼ばれ、統計モデルの第1種過誤および第2種過誤とみなされる。生体認証に関する技術は、セグメンテーション、分解法、すなわち固有顔、局所特徴分析（LFA）、および独立成分分析（ICA）を含み、さらにサポートベクトルマシン、Elastic Bunch Grapes、陰関数3次元モデルおよび方法を含む。

【 0 0 0 8 】

より正確でより精密なアルゴリズムが人の識別にとって不可欠であるが、現行システムの実装は大抵情報を適切に広めることができない結果となる。さらに、現行の技術ネットワーク製品を用いた実時間環境の実装では現行システムは不十分である。この不十分さは、環境上の管理欠如、ユーザの統合およびシステムネットワーク上の管理に由来する。

【 図面の簡単な説明 】

【 0 0 0 9 】

本発明は、以下の添付図面を参照した実施例によって記載される。

【 0 0 1 0 】

【図1】図1は、管理生体認証通知システムのブロック図である。

【図2】図2は、第1コンテンツを取り込むよう適合された管理生体認証通知システムの少なくとも1つの画像取得システムのブロック図である。

【図3】図3は、少なくとも1つの画像取得システム、比較モジュールおよび通知コンポーネントを含む管理生体認証通知システムのブロック図である。

【図4】図4は、比較モジュール、コンテンツ管理モジュール、および少なくとも1つの送信データポイントを含む少なくとも1つの通知コンポーネントを含む管理生体認証通知システムのブロック図である。

【図5】図5は、コンテンツ管理モジュールの詳細なブロック図である。

【図6】図6は、少なくとも1つの予め選択された受信ノードのブロック図である。

【図7】図7は、少なくとも1つの予め選択された受信ノードの実施形態のブロック図である。

【図8】図8は、管理生体認証通知システムの実施形態のブロック図である。

【図9】図9は、管理生体認証通知システムの実施形態のブロック図である。

【図 10】図 10 は、画像サーバを含む管理生体認証通知システムのブロック図である。

【図 11】図 11 は、ウェブサーバを含む管理生体認証通知システムのブロック図である。

【図 12】図 12 は、比較モジュールの処理のフローチャートである。

【図 13】図 13 は、管理生体認証通知システムの実施形態のブロック図である。

【図 14】図 14 は、少なくとも 1 つの画像取得システムおよび比較モジュールの処理のフローチャートである。

【図 15】図 15 は、サードパーティデータベースへのアクセスを提供する管理生体認証通知システムの実施形態のブロック図である。

【図 16】図 16 は、登録処理のブロック図である。

【図 17】図 17 は、登録処理に関連データを含むブロック図である。

【図 18】図 18 は、イベントを起動するコンテンツ管理モジュールのブロック図である。

【発明を実施するための形態】

【0011】

管理生体認証通知システム 100 が提供される。本書で開示されるものは、特に、インターネットなどの通信媒体上のユーザ対話型フィードバックシステムを含むことができる。後述する技術は、コンピュータソフトウェアアプリケーションを含み、これはユーザのコンピュータシステム上で実行されるとき、そのコンピュータシステムを構成し、その結果ユーザが情報を受信し、コンテンツ比較の結果に基づいて他の選択されたユーザまたはユーザのグループへ提供することができる。

【0012】

本書で用いられるように、インターネットとは、少なくとも通信するために伝送制御プロトコル/インターネットプロトコル(TCP/IP)を用いるネットワークおよびゲートウェイの世界的な収集のことをいう。ワールドワイドウェブ(WWW)とは、ハイパーテキスト転送プロトコル(HTTP)サーバに存在する相互連結したハイパーテキスト文書の全体集合のことをいい、ウェブサーバは任意の種類ウェブサーバ、例えばAPACHEとすることができる。本書で用いられるように、WWWとはさらに、安全なポートを介して暗号化と送信を提供するHTTPサーバ(HTTP(S))などのセキュアサーバにアクセスされる文書のことを少なくともいう。本書で用いられるように、用語「ウェブサイト」とは、1以上の関連のHTML文書並びに関連ファイル、スクリプトおよびデータベースのことを少なくともいい、これはWWW上のHTTPまたはHTTP(S)サーバによって提示することができる。用語「ウェブブラウザ」とは、HTML文書をユーザに閲覧させ、これらの文書に関するファイルおよびソフトウェアにアクセスさせるソフトウェアのことを少なくともいう。

【0013】

以下の実施形態に示されるシステムの任意の1以上の要素は、他の要素の何れかまたは全てから遠くに配置することができる。所定の実施形態の要素の何れかは、実際には、全く別のシステムの一部とすることができる。さらに、以下の実施形態について、それらは管理生体認証通知システム100に関して記載されるが、限定されないが指紋認識システム、虹彩認識システム、掌形判別システム、および署名認識システムを含む他の生体認証技術と共に本発明の多くの態様が利用可能である。本発明の少なくとも幾つかの実施形態は、画像から取り込まれた情報を利用する生体認証アプリケーションに特に有利である。

【0014】

図1は、管理生体認証通知システム100を示す。管理生体認証通知システム100は、第1コンテンツ110を取り込むよう適合された少なくとも1つの画像取得システム105と、システム100内のコンテンツを比較および配信するための比較モジュール140と、システム100を制御および管理するためのコンテンツ管理モジュール180と、少なくとも1つの予め選択された受信ノード220とを含む。

【0015】

10

20

30

40

50

図2は、少なくとも1つの画像取得システム105をより詳細に示している。少なくとも1つの画像取得システム105は、レンズ120と、演算処理装置125と、デジタルセンサチップ130と、メモリ135と、第1コンテンツ110とを取り込むよう適合されている。第1コンテンツ110は、少なくとも1つの画像取得システム105によって取り込まれ、管理生体認証通知システム100の比較モジュール140に送信される。

【0016】

図3は、比較モジュール140と通知コンポーネント170をより詳細に示す。比較モジュール140は、第1コンテンツ110を受信するよう構成され、少なくとも1つのプロセッサ145と、少なくとも1つのデータベース150と、少なくとも1つの検索エンジン160と、関連メモリ165とを含む。少なくとも1つの検索エンジン160は、少なくとも1つの画像取得システム105と少なくとも1つのデータベース150とに動作可能に接続される。少なくとも1つのプロセッサ145は、少なくとも1つの画像取得システム105と少なくとも1つの検索エンジン160とに動作可能に接続され、統計的閾値が比較されたコンテンツ間で満たされれば、通知コンポーネント170が生成される。

10

【0017】

図4は、比較モジュール140と、コンテンツ管理モジュール180と、通知コンポーネント170と、少なくとも1つの送信データポイント175とを示している。通知コンポーネント170は、第1コンテンツ110と、第2コンテンツ155が少なくとも1つのデータベース150に配置され、比較された後に比較モジュール140により送信される。コンテンツ管理モジュール180は、システム100の1人または複数人のユーザに、少なくとも1つの送信データポイント175を含む通知コンポーネント170の配信を管理および制御するよう構成される。

20

【0018】

図5は、コンテンツ管理モジュール180を詳細に示している。コンテンツ管理モジュール180は、比較モジュール140と相互作用することによって機能する管理生体認証通知システム100を管理および制御するための手段を提供する。システム100のユーザに必要な機能を提供する際に、コンテンツ管理モジュール180はケースモジュール(「CM」)185と、通知モジュール(「NM」)190と、データベース検索およびレポートモジュール(「DBRM」)195と、データベースと、サブスクリプションコンテンツモジュール(「SCM」)200と、支援モジュール(「SM」)205と、アカウント管理モジュール210(「AMM」)とを含む。

30

【0019】

コンテンツ管理モジュール180は、グラフィカルユーザインタフェース(GUI)として働き、ユーザとの対話処理と、フィードバック機能と、管理生体認証通知システム100を制御および管理する機能とを提供する。実施形態では、コンテンツ管理モジュール180はウェブポータルを介してネットワークを通してアクセスされる。コンテンツ管理モジュール180は、コンピュータ読み取り可能な媒体に格納されるコンピュータ実行可能命令を含むコンピュータ読み取り可能な実行可能プログラムに含まれ、汎用コンピュータシステムと共に利用可能である。別の実施形態では、コンテンツ管理モジュール180は、無線ネットワーク上でコンピュータとサーバの間で送信された1以上の搬送波信号などの送信媒体に含まれる。

40

【0020】

CM185は、管理生体認証通知システム100のコンテンツおよび情報をユーザに管理および生成させるよう構成されたモジュールである。CM185は、ケース情報と関連ケース識別番号(「CIN」)を生成する機能を提供し、さらにケース情報を修正する機能をユーザに提供する。ユーザは、少なくとも1つの画像取得システム105から取り込まれた第1コンテンツ110の「登録」によってケースを生成することができる。登録は、人から生体認証データを集め、続いて人の身元を表わす基準テンプレートにデータを格納するプロセスである。この手続きは重要であり、さもなければユーザがシステム100によって認識されない人に精通している必要がある。生成されたコンテンツは、次に比較

50

モジュール140の少なくとも1つのデータベース150に格納される。

【0021】

もし閾値または十分な類似度の条件を満たせば、CM185は第1コンテンツ110で第2コンテンツ155をさらに更新する機能を提供する。この特徴は不可欠であり、管理生体認証通知システム100は環境から利用可能な期限切れの情報と現行情報を有する。CM185はさらに、特定の基準に基づいてケース情報をユーザにグループ化させるよう構成されている。例えば、「ケースグループ」は「万引き犯」、「重要人物」、または「記録のある人」とラベルづけすることができる。通常、ケースグループは任意のグループとして規定することができ、ここでは識別が周囲環境にとって重要である。

【0022】

CM185はさらに格納されたコンテンツを管理する。CM185は通常データベース内の配置モジュールの機能を全て含む。この機能は、格納されたコンテンツ(DBRM195を参照)を検索することも可能なフィールドと、使用メニューと、情報を配置するためのタブ機能とを含む。含まれるフィールドは、名前と、生年月日と、性別と、違反リストと、経歴と、所見と、取引と、環境内の相互関係とを含むことができる。しかしながら、コンテンツをより十分に定義し、検索機能(DBRM195参照)を強化するために個人または環境に特有のフィールドをさらに追加することができる。

【0023】

NM190は、管理生体認証通知システム100の少なくとも1人のユーザに通知するための手段をユーザに提供するように構成されたモジュールである。NM190は、比較モジュール140と連動して、システム100のユーザと対話処理する様々な方法をユーザに選択させる。通知コンポーネント170は、情報を受信するユーザまたはユーザグループのNM190へのユーザ優先度または予め選択された入力に基づいて送信することができる。NM190で定義されるユーザまたはユーザグループは、1つまたは複数のケースグループ(CM185によって構成される)に結び付けることができる。実施形態では、NM190はユーザまたはユーザグループが少なくとも1つの通知コンポーネント170と、日、週、月および年などの時間間隔に基づく送信データポイント175とを受信するかどうかをユーザに判定させる。

【0024】

NM190はさらに様々な通知コンポーネント170を送信する機能をユーザに提供する。実施形態では、通知コンポーネント170は比較モジュール140から送信ことができ、これは実施形態では、様々な優先度または例えばSMS、MMS、電子メール、インスタントメッセージ、ボイスメールなどの様々な配信方法に基づく通知サーバを含む。さらに、NM190は少なくとも1つのデータベース150の幾つかの異なる種類のコンテンツをユーザに選択させることもでき、ここでは通知コンポーネント170と共に送信される。

【0025】

実施形態では、ユーザは閾値を制御することができ、ここでは第1コンテンツ110と第2コンテンツ155がそれぞれ比較される。しかしながら、この機能はAMM210に実装することもできる。実施形態では、ユーザがオペレータまたは例えば管理者権限の自動オペレータモジュールに閾値でない比較値を送信し、比較値を検証する際の第1測定値または第2測定値として実質的な類似度を判定することができる。この機能は、「確認のない」または閾値でない1または複数の比較値が生じる場合に利用することができる。

【0026】

多くのシナリオを詳述することができ、特定情報は予め選択された時間と方法で適切なユーザに送信され、彼らとその種類の情報を取り扱うよう選択するか、または彼ら個人に特有の様々な因子に基づいて送信すべき特定情報を要求しているため、上記実施例は決して限定するよう意図されていない。

【0027】

DBRM195は、レポートを開発し、管理生体認証通知システム100の少なくとも

10

20

30

40

50

1つのデータベース150を検索する機能をユーザに提供するように構成されたモジュールである。少なくとも1つのデータベース150は、CM185で生成されたフィールドを介してシステム100に提出された任意のケース情報により検索することができる。情報は、レコード、備考、所見、詳細、および環境内の個人の状態または性向に関してユーザに知らせることが可能な他の情報を含むことができる。ユーザはケースにアクセスおよび閲覧し、レポートを生成することができ、レポートは限定されないが、登録ログおよび通知ログ、さらに他の内部統計も含む。DBRM195は、任意の一般形式でこれらのログとレポートをエクスポートする機能も提供する。

【0028】

SCM200は、最新かつ利用可能なデータベースサブスクリプションを申し込み、管理し、および閲覧する機能をユーザに提供するように構成されたモジュールである。このモジュールは、管理生体認証通知システム100で参照されるコンテンツまたは第2コンテンツ155を増加させる。システム100はさらに利用可能なデータベースを集約化し、利用可能なデータベースの説明、各データベースの関連する値付け、および全コンテンツの参照などのサブスクリプション情報をユーザに提供する。SCM200は、システム100の他の申込者とデータベースを共有し、または「提携(Alliances)」を形成する機能をユーザに提供する。しかしながら、この機能は、実施形態では、CM185に含まれる場合がある。このモジュールの機能は、システム100を実装する権限を要求し、他のデータベースをデータマイニングする機能も提供する。データマイニングの処理は、他のサードパーティデータベースからデータを処理する機能を含み、それらのデータベースで見つかった顔画像と他の情報から処理または抽出された特徴セットに基づいて1または複数のデータベースを生成するであろう。

【0029】

SM205は、管理生体認証通知システム100を実装するシステム100の管理者または権限者と共にコンテンツ管理モジュール180のユーザに利用者対話処理とサポートを提供するように構成されたモジュールである。SM205は、システム100の問題を解決するユーザを支援するように構成された対話型プログラムを提供する。SM205に存在する問題も追跡し、管理することができる。SM205は、一般に提出された問題への回答を提供するよくある質問のアプリケーションを含み、さらにライブヘルプおよびチャットプログラムを含む他のサポート方法を含む。

【0030】

AMM210は、管理生体認証通知システム100と、ユーザアカウントと、アクセスを管理するインターフェースと、システム100のデータを実装する管理者または権限者を提供するように構成されたモジュールである。AMM210を介して、優先度を設定したり、他のユーザおよびCM185のサブユーザのアクセスの追加、削除、変更を含むシステム100への権限およびシステム100内での権限を設定したりする機能がある。AMM210は、少なくとも1つの画像取得システム105と、少なくとも1つの予め選択された受信ノード220と、さらにシステム100に関連した他のコンポーネントとを追加、編集、削除するように構成されている。従業員の増加および/または少なくとも1つの画像取得装置105を実装するエリアの増加によりコンポーネントが追加される場合、この特徴は特に重要である。

【0031】

実施形態では、AMM210は一つの権限により比較モジュール140と共に実装することができる、複数実装された管理生体認証通知システム100の制御を有する。この実施形態では、コンテンツ管理システム180の残りのモジュールを環境内に実装ことができ、またはウェブポータルによりユーザに提供することができる。この実施形態では、システム100のユーザは本書で記載されたモジュールにより比較モジュール140と対話処理することができる。この機能は、複数の環境に実装されたシステム100の制御と、それらの環境の1以上間の対話処理を可能にする。

【0032】

10

20

30

40

50

図6は、少なくとも1つの予め選択された受信ノード220を示している。実施形態では、ノードが端末であり、これは複数とすることができ、コンピュータネットワーク上のマザーボードがセントラルプロセッサ230と、プログラムおよびまたはデータを格納するための関連メモリ240（例えば、DRAM、ROM、EPROM、EEPROM、SRAM、SDRAM、およびフラッシュRAM）と、入出力制御部250と、任意の専用論理デバイス（例えばASIC）もしくは書換可能な論理デバイス（例えばGALと、リプログラマブルなFPGAと、ネットワークインターフェース260と、表示デバイス280と、1以上の入力デバイス290と、ハードディスクドライブ300と、フロッピーディスクドライブ310と、自身で通信を可能にし、これらのコンポーネントを接続するデータバス270（例えばSCSIバス、拡張IDEバス、またはウルトラDMAバス）とを含む。

10

【0033】

中央プロセッサ230は、任意の種類マイクロプロセッサとすることができる。表示デバイス280は、生成された出力を表示することが可能な液晶ディスプレイ（LCD）、陰極線管ディスプレイ（CRT）、または発光ダイオード（LED）などの任意の種類ディスプレイとすることができる。入力デバイス290は、キーボード、テンキー、タッチスクリーン、ポインティングデバイス、スイッチ、スタイラス、およびライトペンなどの本書に記載される入力部を提供することが可能な任意の種類デバイスとすることができる。

【0034】

ネットワークインターフェース260は、任意の種類デバイス、カード、アダプタ、またはコネクタとすることができ、これはコンピュータまたは他のネットワーク接続可能なデバイスへネットワークアクセスする少なくとも1つの予め選択された受信ノード220を提供する。一実施形態では、インターフェース260がインターネットなどのコンピュータネットワークに少なくとも1つの予め選択された受信ノード220を接続させることができる。コンテンツ管理モジュール180は、実施形態では、ハードディスクドライブ300、フロッピーディスクドライブ310、またはネットワークインターフェース260により予め選択された受信ノード220に読み込まれ、別の実施形態では、比較モジュール140内に含まれる。あるいは、プログラムがメインメモリ240の固定記憶部（例えば読み出し専用メモリ（ROM）チップ）に常駐することができる。

20

30

【0035】

少なくとも1つの予め選択された受信ノード220は、クライアントとサーバの少なくとも1つで実装することができる。「クライアント」とは、ファイルを要求または受信するものを意味するよう広く解釈することができ、「サーバ」とは、ファイルを送信または転送する実体と広く解釈することができる。実施形態では、少なくとも1つの予め選択された受信ノード220が通信コネクションを用いてネットワーク接続された環境で動作し、1以上のリモートコンピュータに接続する。リモートコンピュータは、パーソナルコンピュータ、サーバ、ルータ、ネットワークPC、ピアデバイスまたは他の共通ネットワークノードを含むことができる。通信コネクションは、ローカルエリアネットワーク（LAN）、ワイドエリアネットワーク（WAN）または他のネットワークを含むことができる。

40

【0036】

図7は、少なくとも1つの予め選択された受信ノード220の実施形態を示している。実施形態では、少なくとも1つの予め選択された受信ノード220が少なくとも1つの通知コンポーネント170を受信するためのトランシーバまたは他の類似する手段である。受信手段は、限定されないが、携帯電話、携帯情報端末（PDA）または他の類似する携帯型の携帯機器を含むことができる。さらに、この実施形態では、少なくとも1つの予め選択された受信ノード220が少なくとも1つの画像取得システム105として機能することができ、第1コンテンツ110を取り込み、通知コンポーネント170と少なくとも1つの送信データポイント175を受信する手段をユーザに提供する。トランシーバの使

50

用は、環境内のユーザに機動性と多用性を提供する。トランシーバは、クライアントサーバシステムまたはピアツーピアシステムなどの他のデバイスにネットワーク接続することができ、ユーザが環境内の別のトランシーバに情報を受信および送信させることができる。

【0037】

使用時には、環境内へ管理生体認証通知システム100を実装する際に、第1コンテンツ110が少なくとも1つの画像取得システム105により取り込まれる。実施形態では、第1コンテンツ110が人の画像であり、画像は実質的に顔面領域を含む。別の実施形態では、第1コンテンツ110が手書きまたは印字画像のマシンテキストへの電子翻訳または光学文字認識(OCR)であり、ここではマシンビジョンカメラまたはデジタルビデオカメラおよびコンピュータが英数字の読み出しおよび分析するのに用いられる。しかしながら、第1コンテンツ110は一般に環境に重要なあらゆる種類の情報とすることができる一方、ある種類の情報のみが比較モジュール140により認識され、残りの情報は分類、格納、およびコンテンツを比較するのと同じ方法でユーザ要求の際に読み出すことができる。

10

【0038】

図8は、一実施形態において、商業環境320に配置された少なくとも1つの画像取得システム105を示している。この実施形態では、商業施設が管理生体認証通知システム100を実装することができ、商業環境320で発生する「万引きによる在庫数減少(shrinkage)」または他の犯罪の量を低減する。図9で示されるように、別の実施形態では、同じ地域内の店舗または同じチェーン内の店舗は、システム100の申込者であり、少なくとも1つの中央データベース325を共有することができる。図示する構成は、ある店舗または複数の店舗に関して、コンテンツ管理モジュール180を構成することにより、情報の共有を可能にしており、特定の活動の通知または店舗チェーンもしくは地域に特有の人について別の「提携(Alliances)」を設けている。

20

【0039】

実施形態では、少なくとも1つの画像取得システム105がマシンビジョンカメラを含む。マシンカメラは、15fps(SXGA)または34fps(VGA)の何れかのフレームレートで取り込み、標準プロセッサ、オペレーティングシステム、SDRAMおよびイーサネット、USBシリアルポートおよびモニタ出力によるI/O接続などのカメラ特性を含む。マシンビジョンシステムのコンポーネントは、以下の幾つかを含むであろう：画像を取得するための光学部品を有する少なくとも1つのデジタルまたはアナログのカメラ。画像をデジタル化するためのインターフェース(CCTVカメラの場合に「フレームグラバ」)として広く知られている)。プロセッサ(しばしばPCまたはDSPなどの組み込みプロセッサ)(幾つかのケースでは、上記の全てはスマートカメラと呼ばれる単一デバイスに結合される)。結果を報告する入出力ハードウェア(例えばデジタル入出力)または通信リンク(例えばネットワーク接続)。画像センサへ所望の視界の焦点を合わせるレンズ。画像を処理し、かつ関連する特徴を検出するプログラム。実施形態では、マシンビジョンカメラが検出用の同期センサ(しばしば光学センサまたは磁気センサ)を含み、画像取得と画像処理を始動させる。画像を取得するための手段として管理生体認証通知システム100と連動して多くの利用可能なデジタルビデオとデジタルカメラを用いることができることを当業者は理解することができるため、この実施例は決して限定されるものではない。

30

40

【0040】

この実施形態では、図10に示されるように、少なくとも1つの画像取得システム105が多量の収集データのため、サイト上に少なくとも1つのサーバ385を含み、大量のデータ収集を取り扱う。この実施形態では、少なくとも1つの画像取得システム105が画像サーバ385に第1コンテンツ110を送信し、画像サーバ385は第1コンテンツ110を格納し、第1コンテンツ110と第2コンテンツ155との比較がそれぞれ閾値の類似度をもたらした後に(図14に示される処理)、比較モジュール140に送信する

50

。別の実施形態では、図 11 で示されるように、少なくとも 1 つの画像取得システム 105 が比較モジュール 140 のウェブサーバ 390 に第 1 コンテンツ 110 を送信する。この構成は、システム 100 の構成要素をネットワークに接続される様々な位置に存在させることができる。

【0041】

環境、または別の方法いわゆる「追跡環境」から第 1 コンテンツ 110 を取り込んだ後、第 1 コンテンツ 110 は次に比較モジュール 140 に送信される。このステップは一般に「画像取得」と呼ばれる。画像取得とは、コンピュータがコンピュータ内にカメラから画像データを取得する方法のことをいう。実施形態では、少なくとも 1 つの画像取得システム 105 が比較モジュール 140 に非圧縮ビデオを送信する。実施形態では、少なくとも 1 つの画像取得システム 105 がネットワーク上にある。

10

【0042】

図 12 は、比較モジュール 140 の処理を示す。比較モジュール 140 は、受信する第 1 コンテンツ 110 から 1 セットの記述子または特徴セット 110 a を生成するよう構成される。比較モジュール 140 は、少なくとも 1 つの検索エンジン 160 を含み、画像取得システム 105 と少なくとも 1 つのデータベース 150 とに動作可能に接続される。少なくとも 1 つの検索エンジン 160 は、メモリ 165 に格納された一連の命令を実行し、第 1 コンテンツ 110 の特徴セット 110 a と、第 2 コンテンツ 155 の実質的に類似する特徴セット 155 a とを処理するようプログラムされる。

20

【0043】

特徴セット 110 a および 155 a が所定の閾値を満たす場合、比較モジュール 140 は比較が一致していると判定する。次に通知コンポーネント 170 が送信され、これは実施形態では、比較モジュール 140 に動作可能に接続した通知サーバを含むことができる。別の実施形態では、比較が一致しない場合、通知コンポーネント 170 も送信することができる。前述したように、オペレータはこの連結点で使うことができ、実質的な類似度を判定する。しかしながら、マッチングが発生するかどうかには拘わらず、コンテンツは少なくとも 1 つのデータベース 150 に格納される。通知コンポーネント 170 は、NM 190 により利用可能に作成された任意の種類で構成され、同じモジュールによって示される任意の優先度で配信することができる。さらに、少なくとも 1 つの送信データポイント 175 も通知コンポーネント 170 と共に送信され、その形式とタイミングは同じように決定される。

30

【0044】

図 13 に示されるように、図 10 と図 11 に関して、管理生体認証通知システム 100 の実施形態である。この実施形態では、比較モジュール 140 が第 1 コンテンツ 110 の特徴セット 110 a を受信する。しかしながら、図 10 と図 11 で示されるように、第 1 コンテンツ 110 は画像サーバ 385 またはウェブサーバ 390 に格納され続ける。実施形態では、抽出処理が少なくとも 1 つの画像取得システム 105 で局所環境 320 内で実装される。この実施形態では、図 14 に示されるように、少なくとも 1 つの画像取得システムのプロセッサ 125 が、メモリ 135 に格納された一連の命令を実行し、第 1 コンテンツ 110 の特徴セット 110 a を処理するようプログラムされる。本書では、比較モジュール 140 で見つけられるアルゴリズムまたは抽出モジュールが少なくとも 1 つの画像取得システム 105 に実装される。比較モジュール 140 は次いで、図 10 に示されるように、特徴セット 110 a を第 2 コンテンツ 155 の処理された特徴セット 155 a と比較するよう構成される。統計的閾値または十分な類似度が満たされる場合、第 1 コンテンツ 110 は要求に基づいて比較モジュール 140 に送信される。

40

【0045】

実施形態では、比較モジュール 140 が第 1 コンテンツ 110 の特徴セット 110 a と第 2 コンテンツ 155 の特徴セット 155 a を処理するよう設計された顔認識アルゴリズムを含む。別の実施形態では、処理アルゴリズム、または自身にあるモジュールが少なくとも 1 つの画像取得システム 105 で商業環境内に実装され、特徴セット 110 a を処理

50

し、比較モジュール140を含む。比較モジュール140によって用いられる一連の命令は、Identix（登録商標）社（L-1 Identity Solutions Companyと合併した）の「FACE-IT」顔認識システム、またはCognitec Systemsの「Face VACS」（登録商標）を含むことができる。通常、広く利用可能な技術は、新しいヘアスタイル、眼鏡、または光の変化による変動と同様に、真似と老化を含む人の顔の変化と無関係に個人を特定することができる。

【0046】

コンテンツの比較に係るアルゴリズムは、関係するデータの統計上の近似を判定するよう実装されるため、個人の統計上の近似をさらに限定するように、例えばテキスト形式で、環境内の個人の他の特徴を特定するアルゴリズムと同様に、顔面識別の判定に複数のアルゴリズムを実装することができる。コンテンツを比較するための管理生体認証通知システム100と連動して、多くの利用可能なアルゴリズムを用いることができるため、その実施例は決して限定されないことを当業者は理解することができる。

10

【0047】

上記で示されるように、第1コンテンツ110と第2コンテンツ155をそれぞれ比較する際に、比較モジュール140が少なくとも1つのデータベース150から引き出す。しかしながら、コンテンツ管理モジュール180と連動する比較モジュール140は様々な異なるコンテンツ形式、データベースおよびサーバへのアクセスを提供する。図15が示すように、実施形態では、データベースのコンテンツは予め設定することができ、すなわち、それは一般のデータベースまたはサードパーティデータベース、例えば政府、法執行機関、国営データベース、またはユーザがデータマイニングするのに必要なデータベースなどの申し込みの結果である。別の実施形態では、上記に示されるように、第2コンテンツ155が局所環境320により予め設定され、これは内部の社内記録と文書以外に基づいてもよい。そのため、データベースのコンテンツは、ユーザ入力とフィードバックによりシステム100で生成されたコンテンツから構築することができる。第2コンテンツ155は、システム100の環境の外部から生成することもできる。

20

【0048】

図16に示されるものはCM185による登録処理である。この実施形態では、ユーザが管理生体認証通知システム100に個人を登録することができる。システム100は、特徴セット110aが処理され、少なくとも1つのデータベース155に格納されるときに生成処理または登録処理を含む。図17に示されるように、CM185は第1コンテンツ110と共に関連データ110bをアップロードする機能をユーザに提供し、例えば図6によって提供されるように、第1コンテンツ110に関する相互関係および/または所見を意味する。

30

【0049】

第1コンテンツ110と関連データ110bが少なくとも1つのデータベース150に入った後、それは第2コンテンツ155と関連データ155bになる。実施形態では、比較モジュール140が関連データ155b専用のデータベースを含み、別の実施形態では、本書に記載された各種類の関連データ155b専用のデータベースを含む。第2コンテンツ155は、次にユーザによってコンテンツ管理モジュール180により操作することができる。管理生体認証通知システム100は通常、システム100に既に保持されている個人の識別情報と、システム100にないが将来の日付で特定されることになっている個人の画像を保有する。

40

【0050】

第1コンテンツ110と第2コンテンツ155がそれぞれ一致しなければならない程度は「十分な類似度」と考えられる。類似度のこのレベルは、閾値または管理生体認証通知システム100のユーザにより示される所定セットのパラメータである。これらのパラメータはユーザによって変更されてもよく、実施形態では、AMM210によって定義されるように、システム100の権限を与えられたユーザによって変更される。比較モジュール140は特徴セット110aと155aの十分な類似度を判定し、その類似度の閾値を

50

満たすかどうかコンテンツ管理モジュール180によって判定されるとき、通知コンポーネント170と少なくとも1つの送信データポイント175が送信される。

【0051】

実施形態では、比較モジュール140が比較した特徴セット間で変化する類似度の程度に応じて複数の第2コンテンツ155を送信する場合または特徴セット110aおよび155aがシステム100の所定の閾値を満たさない場合、オペレータが実質的な類似度を判定する。上述されるように、オペレータは実質的な類似度を判定する際に第1測定値または第2測定値として実装することもできる。

【0052】

比較が所定の閾値を満たした後、ユーザによりNM190を介してコンテンツ管理モジュール180に入力した予め選択された基準に基づいて比較モジュール140が通知コンポーネント170を送信する。通知コンポーネント170は、NM190で説明されるように多くの異なる形態で構成することができる。通知コンポーネント170は無線通信することができ、限定されないがショートメッセージサービス(SMS)、マルチメディアメッセージサービス(MMS)、電子メール、インスタントメッセージまたは電子メールからのSMS、SMSからの電子メール、MMSからの電子メール、またはコンピュータからのSMSアプリケーションの利用を含む。

【0053】

少なくとも1つの送信データポイント175は、通知コンポーネント170と共に送信される情報であり、実施形態では、例えば比較モジュール140の比較画像などの画像または本書に記載された任意の形式の第2コンテンツ155を含む情報で構成される。別の実施形態では、少なくとも1つの送信データポイント175が関連データ155b、または最近比較された第2コンテンツ155に共に関連データ155bを含む。しかしながら、個人の記録またはその個人が関係があると知られている他人、既知の共犯者、本書で述べられた任意の他の形式で記載するコンテンツも送信することができる。

【0054】

さらに、犯罪状況では、第1コンテンツ110と第2コンテンツ155の比較がそれぞれ実質的に類似する閾値をもたらし、少なくとも1つの通知コンポーネント170が送出され、これはその犯罪者の識別を詳述し、例えば以前の犯罪履歴、逮捕状、州刑務所、刑務所、有罪判決、逮捕、容疑、関係機関、以前に盗んだ商品、スタッフの取り扱い、および暴力団所属などの関連データ155bを含むことができる。実施形態では、少なくとも1つの送信データポイント175が、例えば説明書、案内書、および/またはその環境の製品に特有のユーザーマニュアルなどの音声情報および/またはテキスト情報を含むことができ、これはCM185を介して記録することができる。しかしながら、少なくとも1つの送信データポイント175の詳細は、システム100で比較されるコンテンツに大きく依存する。そのため、商業環境への局所的な行動またはイベント、または他の個人についての一般的な情報も送信することができる。この特徴は、以前の買い物の傾向、量、およびよくある質問に基づくカスタマイズサービスを提供するのに役立つことができる。

【0055】

通知コンポーネント170は、管理生体認証通知システム100の1以上の機能として働く。別の実施形態では、通知コンポーネント170がイベントを起動または開始することができる。比較モジュール140は、アクチュエータ330へ命令信号として通知コンポーネント170を送信し、これはイベント、例えばモータを実行したり、またはアプリケーションで別のネットワーク接続されたデバイスを起動したりするよう機能する。電動イベントを起動する際には、サーボ機構を接続することができ、これは別のメカニズムまたはシステムの動作用の測定エネルギー量を供給および送信する。実施形態では、機能的なインタフェースがSMSゲートウェイと相互作用することができ、環境内の機能を実行する。しかしながら、通知コンポーネント170はイベントを起動する際に、様々な形態をとることができるため、その形態は提供される実施例によって限定されない。

【0056】

図18は実施形態を示しており、トランスデューサまたはアクチュエータモジュール330が含まれる場合、これは一般にクロック335、演算処理部345、および受信部340を含み、NM190を介してコンテンツ管理モジュール180から入力信号を受信することができる。アクチュエータモジュール330は出力として、モータと、例えばゲートコントローラ、ドア打撃によるロック、または他の類似デバイスなどのドア回路を乾接点を介して制御するコマンドを供給する。この実施形態では、環境の制御はコントローラにより発生し、これはネットワーク内の複数のデバイスへ出力コマンドを送信することができる。別の実施形態では、デバイスのオンまたはオフの何れかにスイッチを用いることができる。この実施形態では、ネットワークを越えてインタフェースへ2進数コマンドを送信し、または環境内の他のデバイスおよび/またはソフトウェアを制御する受信部にリモート接続することができる。

10

【0057】

通常、少なくとも1つの通知コンポーネント170の目的は、イベントを起動し、および/または個人のユーザに通知することである。しかしながら、個人の通知またはイベントの起動は、様々な形態をとることができ、状況により、様々な複数のユーザおよびデバイスを起動することができるため、その実施例は決して限定されないことを当業者は理解することができる。

【0058】

実施形態では、少なくとも1つの通知コンポーネント170が次に予め選択された受信ノード220に送信され、少なくとも1つの通知コンポーネント170の受信が固定端末および/またはトランシーバまたは他の携帯デバイスを起動することができる。実施形態では、予め選択された受信ノード220が複数のトランシーバである。複数のトランシーバは他のトランシーバに送信し、および/または環境内の他のトランシーバへ情報を再送信する。この実施形態では、商業環境320内の従業員が通信し、さらに画像データを送信し、コンテンツ管理モジュール180でコンテンツを登録することができる。別の実施形態では、トランシーバがさらにトランシーバに無線信号(例えば赤外線または無線周波数)を送信することによって動作する「ローカル」リモートコントロールとして働き、これは別の予め選択された受信ノード220と受信部を介してモータまたはアプリケーションに接続される。この実施形態は、環境内の別の制御レベルをシステム100のユーザに提供する。

20

30

【0059】

管理生体認証通知システム100は、実時間環境で集められた情報を制御および管理し、様々な外部の情報源から最新の情報のある環境と対話処理する機能を提供する。システム100はユーザに対話型システムコンポーネントを提供し、これは様々な技術を用いて利用可能な資源に情報を送信し、動的環境で実時間フィードバックを提供する機能を含む。

【0060】

管理生体認証通知システム100の利点は、システム100のコンテンツ管理モジュール180という構成要素である。コンテンツ管理モジュール180は、情報の識別が不可欠な環境へのコンテンツの配信を制御する。コンテンツ管理モジュール180は、実施形態では、ブラウザによるインタフェースを介してユーザにシステム100のリマインダーと対話処理させることができる。ユーザは、システム100で受信され、格納され、および比較されたコンテンツの制御も提供される。

40

【0061】

具体的には、管理生体認証通知システム100の利点は、少なくとも1つの通知コンポーネント170の送信を管理する機能である。コンテンツ管理モジュール180は、他のデバイスに関連づけられたアプリケーションまたはアクチュエータの起動などの環境内のイベントを管理する機能をユーザ、および情報を受信するユーザおよびユーザグループに提供する。この利点は、環境内の資源を実時間のシナリオで実装アルゴリズムの結果と交わるということである。

50

【 0 0 6 2 】

システム 1 0 0 は、ユーザに通知の種類、例えば送信モードの種類を管理する機能を提供する。送信時間は制御することもできる。本書では、通知コンポーネント 1 7 0 は、様々な所定の因子、例えば日時間隔に基づくよう導くことができる。万引き犯として知られている個人の少なくとも 1 つのデータポイント 1 7 5 を含む少なくとも 1 つの通知コンポーネント 1 7 0 が、利用可能な警備員へ送信することができる一方、個人の購入履歴を店員に送信したり、心臓病を持つと知られている人を心肺蘇生法を理解するスタッフの誰かに送信したりなど、システム 1 0 0 に向けられる用途はもっと沢山ある。

【 0 0 6 3 】

このアプリケーションは、環境内の様々なエリアへ特別な人または特定の入場を許可するのに用いてもよい。そのため、その状況に特有の情報を必要とする環境では多くの状況が想定できることを当業者は理解することができる、これは管理生体認証通知システム 1 0 0 と連動して用いることができるため、上記実施例は決して限定するよう意図されていない。

10

【 0 0 6 4 】

コンテンツ管理モジュール 1 8 0 によって提供される別の利点は、管理生体認証通知システム 1 0 0 の様々なデータベースとコンテンツを生成する選択肢をユーザに提供する機能である。コンテンツ管理モジュール 1 8 0 は、申し込みによってデータベースを生成し、局所環境 3 2 0 からコンテンツをデータマイニングし、または生成する機能を含む。この選択肢は、システム 1 0 0 のユーザにコンテンツの編集を制御させることができる。

20

【 0 0 6 5 】

管理生体認証通知システム 1 0 0 のコンテンツの生成は、生成されたコンテンツを参照する様々な追加データを含んでもよい。そのため、システム 1 0 0 の更なる利点は、システム 1 0 0 の例えば画像、備考を含む関連データを含む機能である。関連データは、少なくとも 1 つの通知コンポーネント 1 7 0 と同一または均等な様々な方法によりアップロードすることができる。さらに、システム 1 0 0 の別の利点は格納されたコンテンツを変更する機能である。この目的のため、コンテンツ管理モジュール 1 8 0 は、A M M 2 1 0 を介してシステム 1 0 0 のコンテンツを変更する人の安全対策を提供する。個人に関する更新通知は、個人がスタッフと特定の敵対関係を持っていたり、敵意を増していたり、もしくは武器を持っていると知っていたり、以前に店舗の特定のエリアを標的としたりする場合に重要である。したがって、もし権限を与えられれば、コンテンツの変更は最新のシステム 1 0 0 を維持するのに不可欠である。

30

【 0 0 6 6 】

管理生体認証通知システム 1 0 0 の別の利点は、少なくとも 1 つの予め選択された受信ノード 2 2 0 である。実施形態では、少なくとも 1 つの予め選択された受信ノードがトランシーバである。トランシーバは、環境内の次のユーザまたは職員に重要な情報を伝送するだけでなく、機動性を提供し、その情報に基づいたアプリケーションまたはイベントを起動する機能をユーザに提供する。これは、環境内の人々に追加の管理水準を設ける。さらに、トランシーバは環境内の別のトランシーバに通信することができる一方、トランシーバは比較モジュール 1 4 0 に画像を伝送し、コンテンツに基づいて少なくとも 1 つの通知コンポーネント 1 7 0 を受信することもできる。

40

【 0 0 6 7 】

管理生体認証通知システム 1 0 0 は、様々な環境で用いることができる。システム 1 0 0 は、周囲監視、自動入場、顧客認識または予め権限を与えられた訪問者識別として商業環境 3 2 0 に実装することができる。小売環境では、システム 1 0 0 が運用コストを低減し、スタッフの効率を上げるであろう。

【 0 0 6 8 】

戦略的な位置に設けた後、管理生体認証通知システム 1 0 0 がさらに万引きによる在庫数減少を低減するであろう。システム 1 0 0 は、データベースの広範囲の画像で個人をマッチングする確率を高めることによりこの結果を得る。システム 1 0 0 は常に、様々な情

50

報源、例えばサードパーティデータベース、ウォッチリスト、要求データマイニングサイトが設けられる環境から来るコンテンツを更新し、コンテンツに接続する。そのため、読み出された情報は様々な情報源の新しいデータと比較され、マッチングの確率を向上する。

【0069】

管理生体認証通知システム100は、複数の場所で用いられるよう設計され、中央監視所または本部を含む。そのため、システム100にネットワーク接続された複数の場所から取得した第1コンテンツ110は中央監視所に送信され、比較モジュール140が図10に示される処理を開始するが、システム100の利点は図13および図14に示されるような少なくとも1つの画像取得システム105の処理の実装である。

10

【0070】

少なくとも1つの画像取得システム105で特徴セット110aを処理するという利点は、特徴セット110aのみを比較のため送信させることができるということである。この比較結果がシステム100の所望の閾値に達する場合、比較モジュール140は少なくとも1つの画像取得システム105から第1コンテンツ100を要求する。システム100の多くのユーザがネットワーク接続する場合、これは特に重要である。この利点は、ネットワーク上で送信されるデータ量を低減するため、利用可能な帯域幅に対する負荷量を低減する。

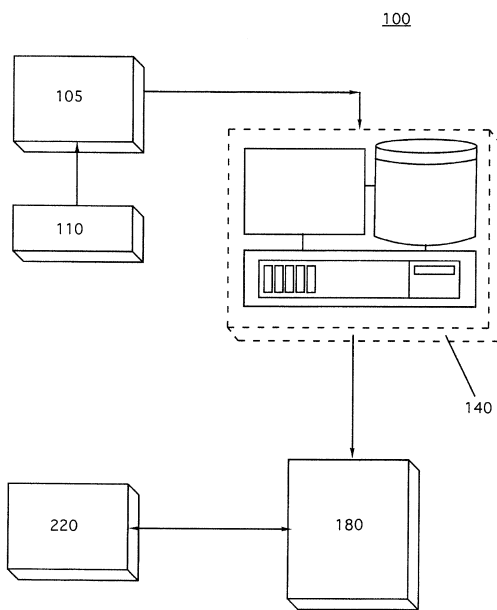
【0071】

特定の例示的な実施形態が記載され、添付図面に示されたが、この実施形態は単に例示的であり、本発明に限定的ではなく、当業者は変更を想定することができるので、本発明が図示され記載された特定の構成および配置に制限されないことを理解されたい。

20

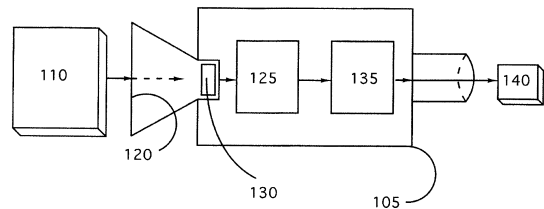
【図1】

FIG.1



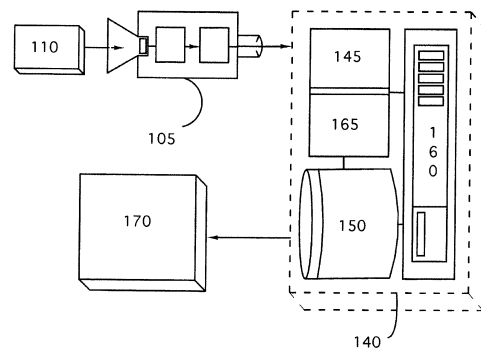
【図2】

FIG.2

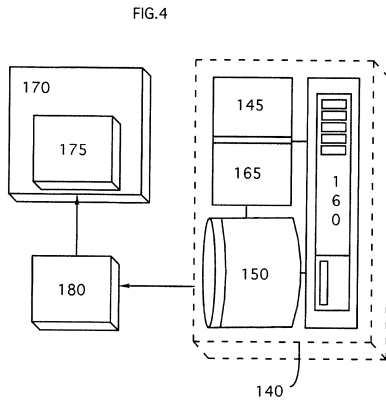


【図3】

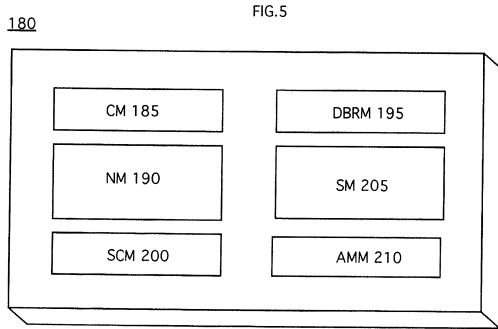
FIG.3



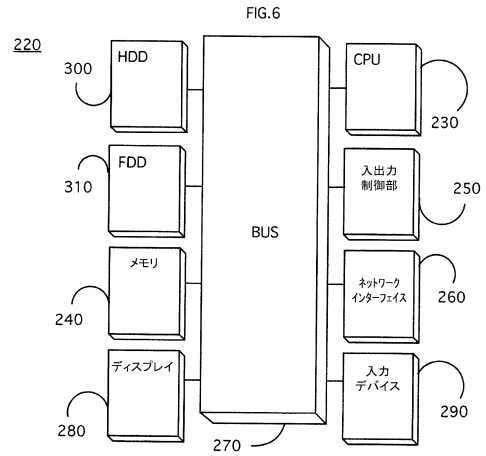
【 図 4 】



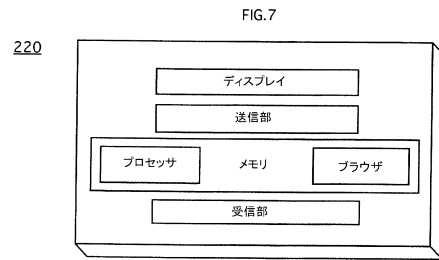
【 図 5 】



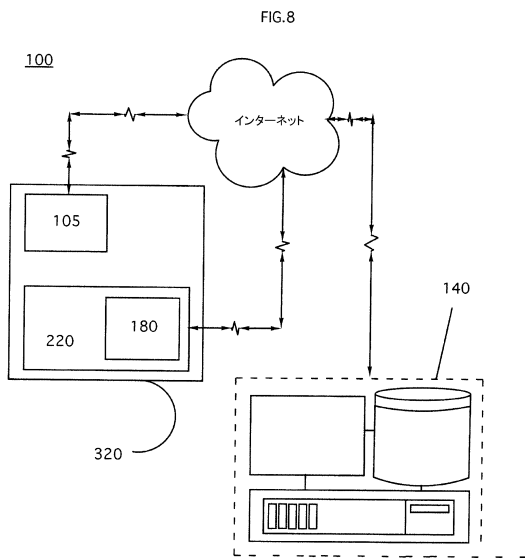
【 図 6 】



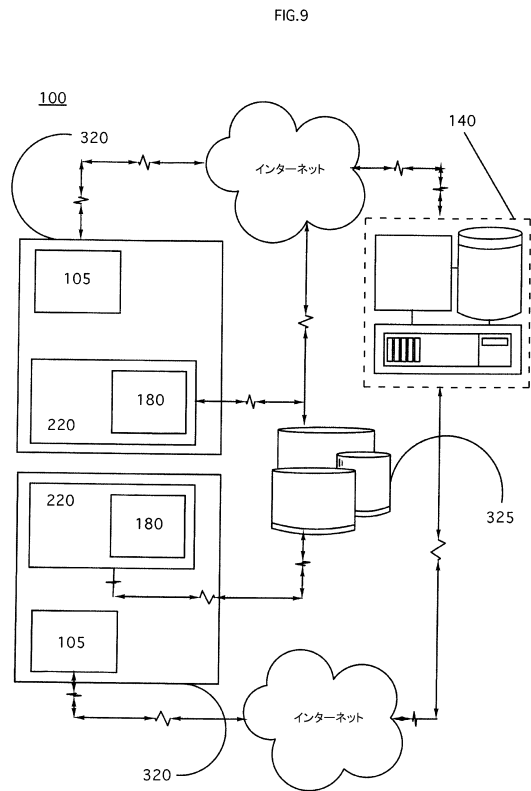
【 図 7 】



【 図 8 】

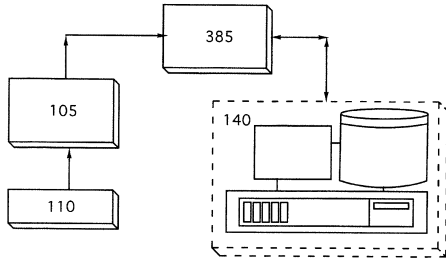


【 図 9 】



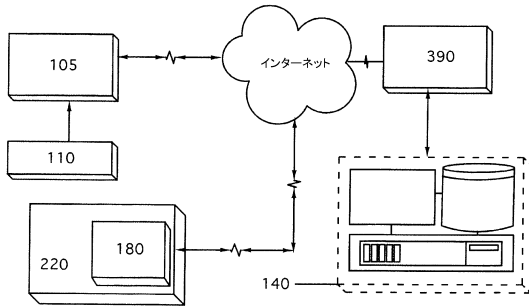
【図10】

FIG.10



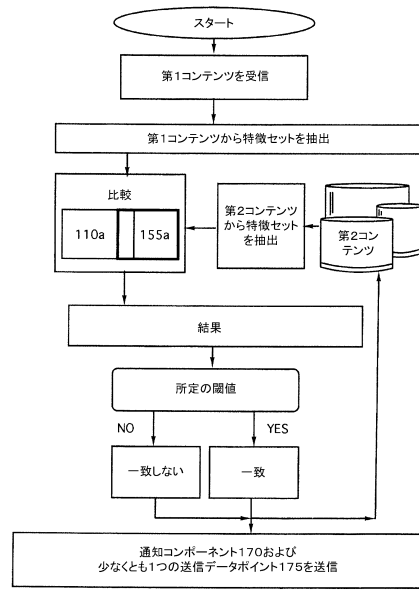
【図11】

FIG.11



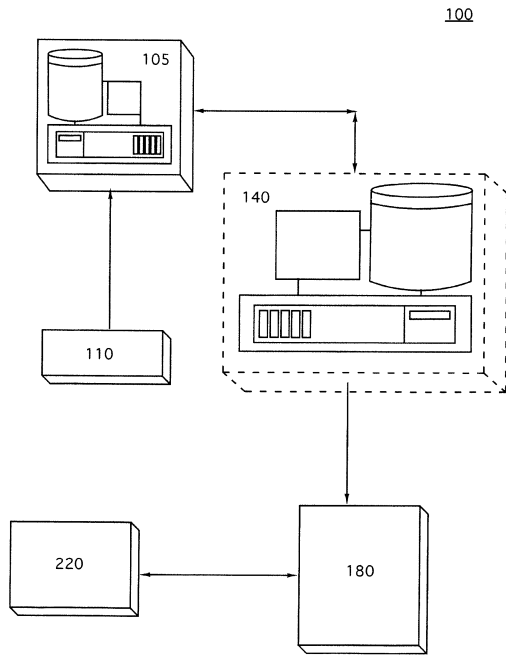
【図12】

FIG.12



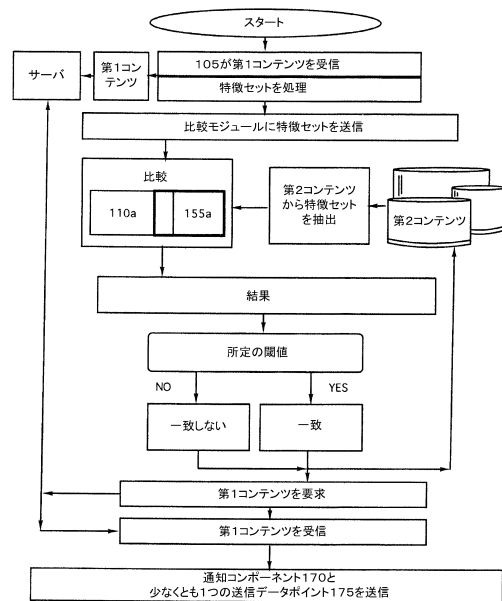
【図13】

FIG.13

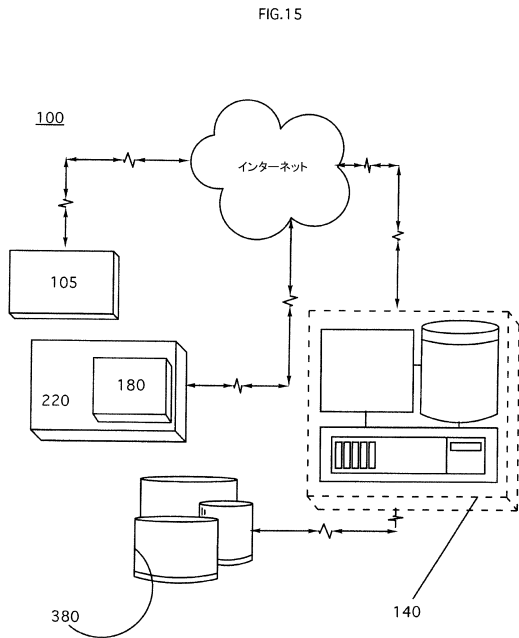


【図14】

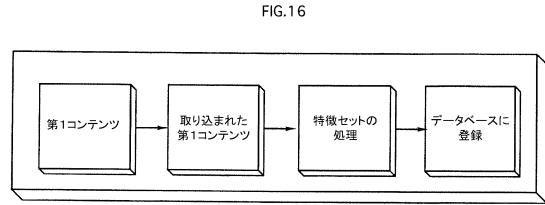
FIG.14



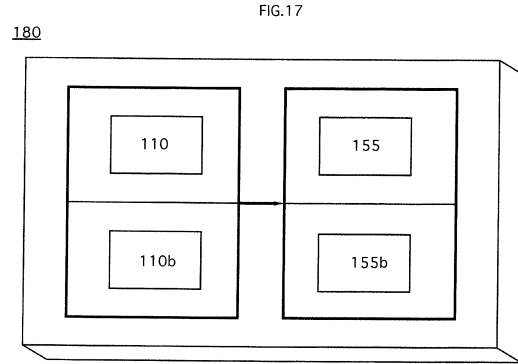
【図15】



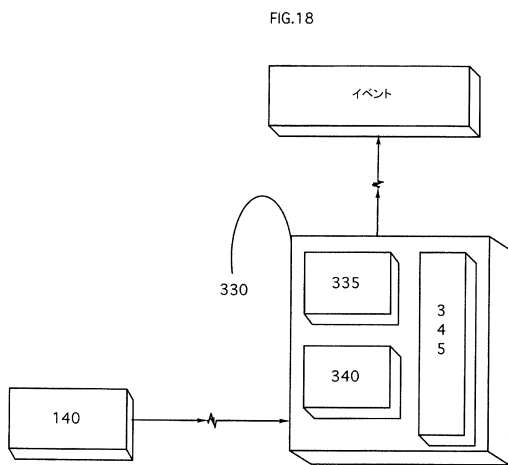
【図16】



【図17】



【図18】



フロントページの続き

(51)Int.Cl. F I
G 0 6 F 21/32 (2013.01) G 0 6 F 21/32

(56)参考文献 特開2004-013871(JP,A)
特開2008-003753(JP,A)
特開2006-109014(JP,A)
特開2007-249587(JP,A)
米国特許出願公開第2009/0092294(US,A1)
米国特許出願公開第2003/0126121(US,A1)

(58)調査した分野(Int.Cl., DB名)
G 0 6 Q 1 0 / 0 0 - 9 9 / 0 0
A 6 1 B 5 / 1 1 7 1
G 0 6 F 2 1 / 3 2
G 0 8 B 1 3 / 1 9 6
G 0 8 B 2 5 / 0 0