(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 619 638 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
25.01.2006 Bulletin 2006/04

(51) Int Cl.:
G08B 13/196 *(2006.01)* ***G07C 9/00*** *(2006.01)*

(21) Application number: **04425554.5**

(22) Date of filing: **23.07.2004**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL HR LT LV MK

(71) Applicant: **Urmet Domus S.p.A.**
10154 Torino (IT)

(72) Inventor: **Minarelli, Giorgio**
10129 Torino (IT)

(74) Representative: **Spandonari, Carlo et al**
Spandonari & Modiano S.r.l.
Corso Duca degli Abruzzi 16
10129 Torino (IT)

(54) Airport surveillance system

(57) A plurality of videocameras (10, 12, 14) are deployed to watch passengers waiting to board planes and having respective boarding cards (26). The passengers' boarding cards include RFID tags (28) containing respective passenger ID codes. Radio transceivers (30, 32, 34) attached to respective videocameras are deployed for interrogating said RFID tags at their passage and for obtainign their respective ID codes. A control computer (18) is connected for receiving data from the videocameras and the transceivers. The computer extracts, whenever an RFID tag is sensed by one of the transceivers, biometric parameters corresponding to said biometric records of the passengers, on the basis of the signal from the attached videocamera, compares them with the parameters in the associated biometric record, and signals an abnormal condition in case they fail to agree. Moreover, the computer measures the passenger's position, compares it with the position of the boarding gate associated with it in the data-base, and signals an abnormal condition whenever the passenger has deviated farther than a predetermined amount from the path going from an entrance gate to the associated boarding gate.

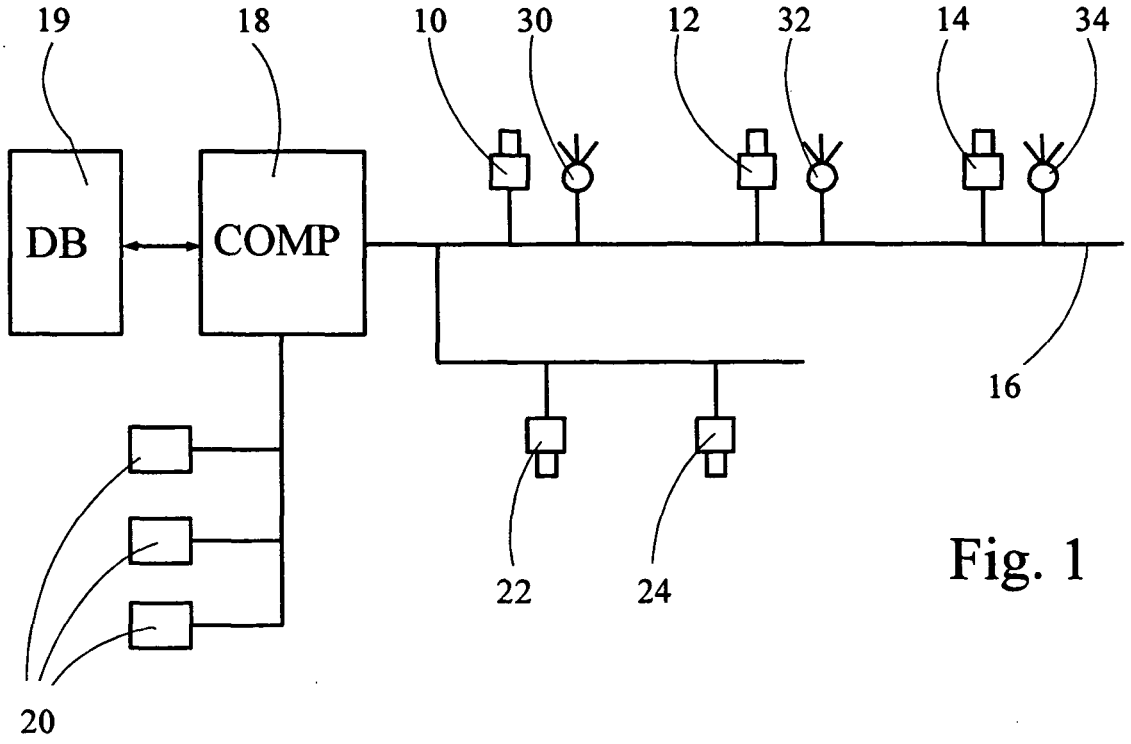

Fig. 1

EP 1 619 638 A1

Description

[0001] This invention is concerned with a surveillance system for the security of airports.

[0002] It is known to keep under surveillance, by means of video cameras, extensive premises such as museums, libraries, companies and industrial plamts, etc., in an attempt to discover any intruders.

[0003] Such surveillance systems are also used for surveying public places such as railway stations or airports, in an attempt to discover persons who, through suspicious behavior, appear to betray criminal intents, say also of a terroristic type. However, this kind of surveillance by video cameras is only capable of locating persons with suspiciou looks or dress, or persons in flagrantly performing illicit actions, but is ineffective in locating malicious persons who deceptively exhibit anodyne and *proper* looks and behavior. Moreover, the effectiveness of surveillance critically depends on the operator's attention level, which is bound to decrease in time.

[0004] It is therefore the main object of the invention to improve known surveillance systems for the security of airports, in order to make them more effective in discovering a greater range of abnormalities in the behavior of waiting persons, which would be unlikely to be discovered with known surveillance systems.

[0005] Another object is to at least partly automate the recognition of aberrant conditions in a surveillance system for airport security, whereby the effectiveness of the surveillance is less dependent on lack of attention of the operators.

[0006] The above and other objects and advantages of the invention, such as will paeear from the following disclosure, are achieved by the invention by a surveillance system for airport security having the features recited in claim 1.

[0007] The dependent claims recite other advantageous features of the invention.

[0008] A preferred, non-limiting example of the invention is described below, with reference to the attached, schematic drawings, wherein:

- Fig. 1 is as block diagram of a surveillance system according to the invention;

- Fig. 2 is a boarding pass, modified for operating with a surveillance system according to Fig. 1.

[0009] The surveillance system of the invention is intended for monitoring a boarding area in a commercial airport comprising, in a way known per se, passages and halls leading to boarding gates, as well as annexes such as shops, coffeehouses, restrooms (not shown). With reference to Fig. 1, a number of video cameras such as 10, 12, 14 are disposed at different points of the boarding area, including its annexes, and are connected, through a bus 16, to a control computer 18, by which the attendant staff can switch the video streams to view the images shot by cameras 10, 12, 14 on one or more monitors such as 20.

[0010] Cameras 10, 12, 14 are deployed at appropriate points to allow the surveillance staff to watch the passengers that have already been checked-in for boarding and are therefore waiting in the waiting area, and are provided with respective boarding cards. Typically, videocameras should be placed near the entrance gate to the boarding area where the boarding pass is checked, as well as near the boarding gates leading to the airplanes, where the boarding pass is withdrawn, but further video cameras are typically disposed at other appropriate points.

[0011] Moreover, further videocameras such as 22, 24 are connected to the control computer 18, which further videocameras are associated with check-in desks in the airport, so that they will portray the face of persons while they are checking in and obtaining a boarding pass.

[0012] According to the invention, each boarding pass 26, on which are printed travel data (passenger name, boarding gate, timetable, etc.) also incorporates a so-called RFID tag 28, comprising, as known per se, a transmitter microchip coupled to an aerial *built* as a printed winding (not shown), and capable of transmitting, upon interrogation, a data string comprising an ID code unique for each tag. The ID code is, for instance, a number assigned in progressive order during manufacture of the tag. The tag can be attached to the boarding pass as a sticker, or it may be sandwiched in the paper.

[0013] A radio transceiver 30, 32, 34 is respectively associated to each video camera 10, 12, 14. Each transceiver is capable of interrogating an RFID tag passing within its action range, and of receiving said ID code, for forwarding to control computer 18.

[0014] Transceivers 30, 32, 34 are advantageously located at the entrance gate (metal detector), at the entrances to the restrooms, near the shop cash registers, in the corridors leading to the boarding halls, at the entrances to the boarding halls, etc.

[0015] When the boarding pass 26 is issued at the check-in desk, the associated ID code is stored by the control computer 18 in a data-base 19, together with the passenger's travel information, i.e. destination, number of the boarding gate and estimated boarding time.

[0016] Moreover, videocamera 22 or 24 at the desk portrays the face of the person checking in, and control computer 18 processes the image to build a biometric record. The latter typically comprises a few tens of biometric parameters that are characteristic of each person surveyed. The parameters forming said biometric record are then associated to the ID code of the boarding pass being issued, together with the above mentioned boarding information.

[0017] Biometric recognition by extracting characteristic features of the face is a known technology, and several commercial systems are available on the market, for instance from Identix, Inc., at Minnekonta, Minnesota, U.S.A.

[0018] By the above procedure, data-base 19 is progressively updated with fresh registrationa, and, on the other hand, whenever a passenger boards a plane and his boarding pass is read and annulled at the boarding gate, computer 18 delets the corresponding ID code from data-base 19, together with the associated biometric record and any other associated data.

[0019] At the same time, control computer 18 cyclically scans transceivers 30, 32, 34, and, whenever a person together with the RFID tag of his boarding pass walks within the action range of one of the transceivers, the computer, on the one hand, receives from it the boarding data, and, on the other hand, it will process the video signal simultaneously received from the associated videocamera 10, 12, 14, in order to extract from the person's portrait his biometric data. The computer inputs both such pieces of information into the passengers' data-base, keeping tack of all measures. The computer can therefore check whether the movements of a person in the airport are normal or abnormal with respect to the foreseeable path to the boarding gate or to legitimate destinations such as shops, restrooms, etc.

[0020] The computer performs the following checks on the collected data:

1) Comparing the place where the surveyed person is located and the his point of embarkation; whenever a surveyed person is found to have considerably deviated from the path to his destination gate, the circumstances is signaled to the staff for further analysis.

2) Comparing an identikit of the surveyed person with an identikit stored at check-in time; a failure of agreement shows that either the person has disguised himself in the meantime, or that there has been an exchange or transfer of his boarding pass; this circumstance is also signaled to the staff for further analysis.

[0021] Preferably, computer 18 also periodically scans the data-base to check whether there are any passengers whose ID codes have not been sensed by at least one transceiver for a time longer than a predetermined threshold. Such prolonged lack of contact is also signaled as an abnormal condition requiring attention.

[0022] Due to the above signaling, the staff is free to concentrate their attention on specific cases, and to follow the movement of suspicious persons which would hardly have been located by conventional video-surveillance procedures. Signaling by the computer may be made by automatic selection of the videocamera that is pointing on the suspicious passenger and switching to a predetermined monitor 20.

[0023] The RFID tags used in the inventive system are preferably of the so-called passive type. As it is known, such passive tags are not provided with a battery, and obtain their supply voltage from the power radiated by the interrogating transceiver. The radiated radio frequency is collected by an aerial printed on the tag, is rectified and is supplied to the microcircuit. Such passive RFID tags have the advantage of a very low cost, so that they can be used with disposable boarding passes. However, where the low cost is not a requirement (say, with recycled boarding passes), it falls within the principles of the invention also the use of RFID tags of the active type, i.e. provided with a battery.

[0024] Moreover, although the above described embodiment can be made with RFID tags without an on-board writable memory, it falls within the scope of the invention also to use tags having a writable memory. In this case, the travel data could be written in the tag memory at the time of check-in and subsequently read there by the computer (as well as, possibly, updated in case of variations), without the necessity of transferring the data to a centralized data-base. The biometric data might also be written in the memory of the RFID tag and then read by the computer when required, via the transceivers 30, 32, 34. The term "data-base" in this specification and in the claims should therefore be understood in its wider logical meaning of a coordinated complex of data, irrespectively of the physical location of the component memories.

[0025] The expression "boarding pass" should be understood not only in the sense of the conventional paper boarding pass, but also in the wider sense of a token authorizing embarkation, however it is made.

[0026] It should be understood that many changes may be made to the preferred examples disclosed above, within the spirit of the invention. For instance, the computer might carry out other actions, beside the ones listed above, and in particular it might update the data-base in case of changes to the time and gate of boarding for a certain flight. Also, other data could be collected, beside those listed above, such as data concerning purchases made in the airport shops, and other check for abnormal conditions may be made beside those disclosed above.

[0027] The physical constitution of the surveillance system masy also be inplemented in a number of different ways. For instance, the connection buses may be coaxial cables, optical fibers or wireless communication, according to an arbitrary local area network protocol. The videocameras may also be of different kinds, for instance they might also be analog, the conversion of the signal to a digital form, when necessary, being carried out in the surveillance center.

[0028] All the above and other changes should be regarded as falling within the inventive concept as defined in the attached claims.

Claims

1. A surveillance system for the security of airports, comprising a plurality of più videocameras (10, 12, 14) connected to a control computer (18) and de-

ployed to watch passengers waiting to board planes and provided with respective boarding cards (26), **characterized in that** the system further comprises RFID tags (28) containing respective ID codes and incorporated in the respective boarding cards of the passengers, and radio transceivers (30, 32, 34) attached to respective videocameras and connected to the control computer and deployed for interrogating said RFID tags at their passage and for transmitting the respective ID codes to the computer,
and **in that** the control computer (18) is programmed for:

- maintaining a database (19) of biometric records comprising characteristic parameters of the passengers' faces, their ID codes and their respective associated boarding cards;
- extracting, whenever an RFID tag is sensed by one of the transceivers, biometric parameters corresponding to said biometric records of the passengers, on the basis of the signal from the attached videocamera, comparing said biometric parameters with the parameters in the associated biometric record, and signaling an abnormal condition in case they fail to agree;
- measuring, whenever an RFID tag is sensed by one of the transceivers, the passenger's position, comparing it with the position of the boarding gate associated with it in the data-base, and signaling an abnormal condition whenever the passenger has deviated farther than a predetermined amount from the path going from an entrance gate to the associated boarding gate.

2. The surveillance system of claim 1, **characterized in that** the computer is also programmed for periodically checking whether any ID codes have not been sensed by at least one transceiver (30, 32, 34) for a time longer than a predetermined threshold and for signaling this condition.

3. The surveillance system of one of claims 1 or 2, **characterized in that** it further comprises a videocamera associated to each of the passenger check-in desks and connected to the control computer, and **in that** the control computer (18) is programmed for extracting, from the video data generated by the videocameras of the check-in desks, a record of biometric parameters that are characteristic for each passenger.

4. The surveillance system of any of claims 1 to 3, **characterized in that** said RFID tags (30, 32, 34) are of the passive type.

5. The surveillance system of any of claims 1 to 4, **characterized in that** whenever the control computer (18) signals an abnormal condition it will automatically switch to a predetermined monitor (20) the video signal coming from the videocamera that is shooting the suspect passenger.

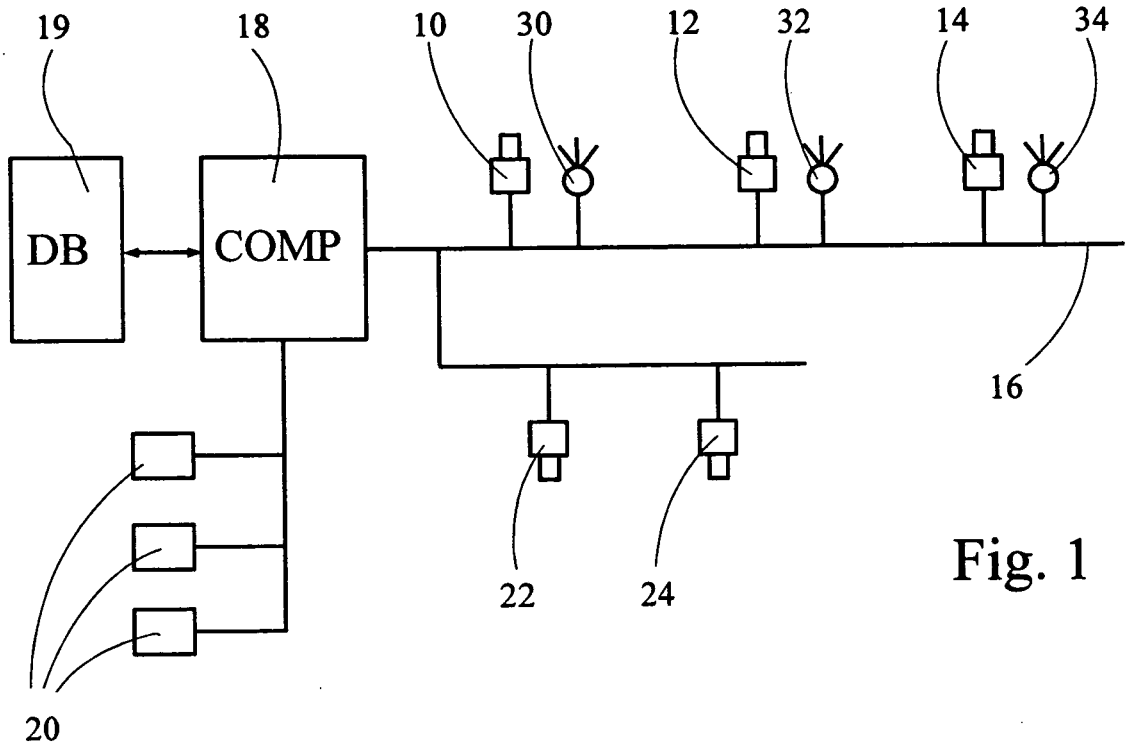

Fig. 1

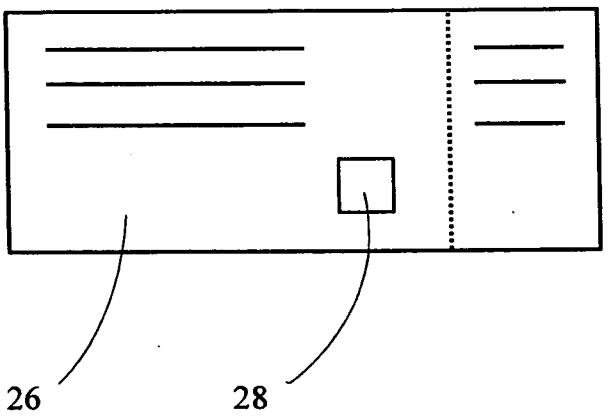

Fig. 2

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 04 42 5554

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X Y	US 2003/128099 A1 (COCKERHAM JOHN M) 10 July 2003 (2003-07-10) * paragraphs [0016], [0023], [0034], [0036], [0040] - [0043], [0045], [0052], [0055], [0057], [0059], [0060], [0064]; figures 1-5 * -----	1,3,4 5	G08B13/196 G07C9/00
Y	US 2003/197612 A1 (IMASAKI NAOKI ET AL) 23 October 2003 (2003-10-23) * paragraphs [0003], [0069] - [0072]; figures 1,3,4,13 * -----	5	
			TECHNICAL FIELDS SEARCHED (Int.Cl.7) G08B G07C

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	14 December 2004	Wright, J

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 04 42 5554

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

14-12-2004

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003128099 A1	10-07-2003	NONE	
US 2003197612 A1	23-10-2003	JP 2004005511 A	08-01-2004

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82