iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 Issue: XI Month of publication: November 2022

DOI: https://doi.org/10.22214/ijraset.2022.47404

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue XI Nov 2022- Available at www.ijraset.com

A Model for Unauthorized Person access in a Particular Area

Rajesh Prakash Suryawanshi[1], Akshay Dashrath Phadatare[2]
[1, 2]Yashoda Technical Campus, Satara ,Maharashtra - 415003

Abstract: A method of unauthorized person identification in a particular area of an entity includes maintaining a database of identification data specific to the person and condition of entries and time period, providing a unique description for each person enabling access to the person identification data in the database.

The automated face recognition system uses a new face-finding and an automated eye- finding approach combined with an intelligent metric. This allows templates to be placed on any size chip or into two-dimensional (2-D) barcodes for self-authenticating documents, as well as for quick easy transmission over the internet, wireless devices, or Ethernet (i.e., LAN, WAN, etc.).

A biometric and identity enrollment camera for collecting personal data includes a slidable main module and at least one modifiable section removable coupled to the main module. The main module includes a processor and one or more biometric sensing devices coupled to the processor.

Methods of detecting authorized person identity, differentiating between users of a computerized service, and detecting an unauthorized person. The data management facility may be geographically distributed at a plurality of data management sites and the data storage nodes may exist inside and outside of a particular area of the first person.

Keywords: Automated face recognition system, Biometric system, (2-D) barcodes, data management sites, and data storage nodes.

I. INTRODUCTION

This invention relates to a method of unauthorized person identification. This invention has particular exclusive application to a method of unauthorized identifying persons which a lifelong distinctive identity such as computers, computer records, computer software, network hardware including RF local and wide area network access equipment, databases, database records, categorized watch lists for individual’s person, portable computer storage devices, art. Such individual persons, equipment, records, and articles are here in after collectively referred to as “an individual or individuals or entities”.

Positive identification of individuals is important for preventing unauthorized access to or passage from selected locations and areas such as buildings, college classrooms, and all associated areas, whether on or off-site of the respective college classroom or the like.

Positive identification of individuals is particularly important for making decisions concerning unauthorized access to a particular area.

According to the present invention, biometric data specific to an individual can be stored on a card. The card can be proffered at a reading camera wherein the biometric data is read by a card reader or the like and compared with the biometric properties of the individual proffering the card.

A high correlation between the card data and the contemporaneously acquired data of the individual proffering the card results in access and a low correlation causes a refusal.

This system however does not prevent unauthorized cards from being produced which may be used for gaining unauthorized access to a facility.

The present invention aims to alleviate at least one of the above disadvantages and to provide a method of and apparatus for providing identification that will be reliable and efficient in use. With the foregoing in view, this invention, in one aspect, resides broadly in a method of providing identification of unauthorized person entries.

Including the steps :

1) Maintaining a database of identification data specific to the appearance and/or condition of the authorized and unauthorized person entry;
2) Providing a unique description for each person enabling access to the person identification data in the database

II. MATERIAL & METHODS

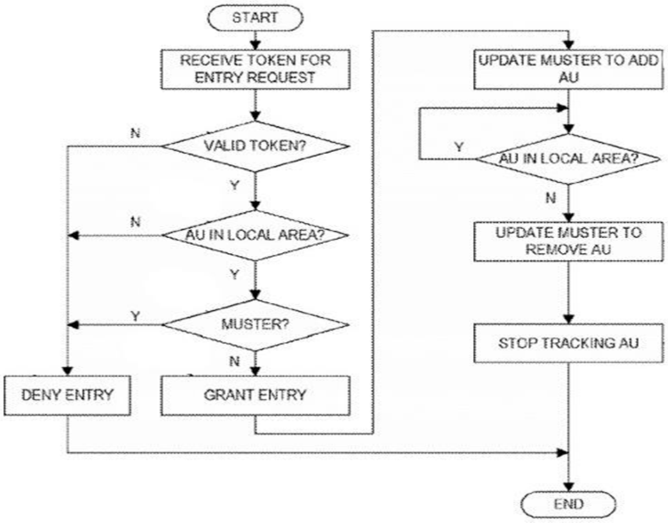

Fig 1. A flowchart diagram illustrating operation of the access control system

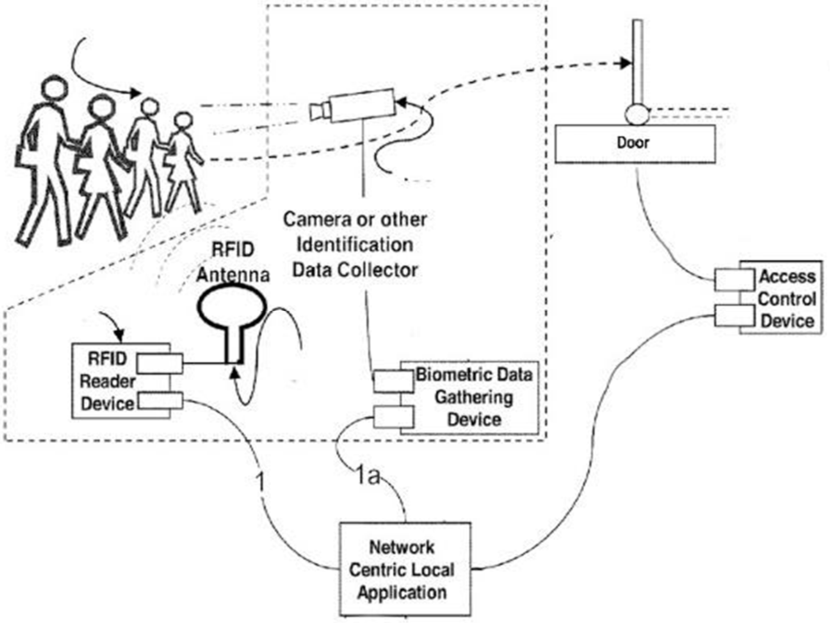
Door
Camera or other Identification Data Collector
RFID Antenna
RFID Reader Device
Biometric Data Gathering Device
Access Control Device
1
1a
Network Centric Local Application

Fig 2. The response is categorized as before entiry

III. METHODOLOGY

Fig .1, A flowchart diagram illustrating operation of the access control system for controlling any of the control libel barriers or according to an exemplary embodiment. Operation is primarily performed by the access system for making access decision and the user location information system for tracking location and updating the muster. At a first block , the access system receives a token for requesting entry into one of the restricted areas . at next block , the access system determines whether the received token is a valid token. A "valid' token indicates that the corresponding authorized user (AU) is granted entry at the given time and under any other conditions, if applicable. If the token is valid, operation proceeds to block in which the access system consults the user location information system to determine whether the corresponding authorized user is located within the local area .

If the authorized user is determined to be in the local area at block , operation proceeds to block to query whether the authorized user is already on the muster . If the user is not on the muster at block , operation proceeds to block to grant entry to the authorized user. Fig. 2, the response is categorized as before, server application unit requests the linked Biometric data from enrolment or “authorized person ’ and “ unauthorized person " databases. The authorized person database passes back recorded biometric Data and authorizes the unauthorized person database to pass back unauthorized person recorded biometric data to the server application unit . Unauthorized person, and authorized person biometric data are compared to validate the integrity of the authorized person and unauthorized person databases.

Failure to reach required threshold causes an alert signal to be Sent to internal security personnel.

IV. CONCLUSIONS

1) The unauthorized person cannot enter into the particular premises without permission of the authority.
2) One can also take the attendance using this system.
3) The system is also used for security of students, employees.
4) The system can be proved a good time saver.

V. ACKNOWLEDGMENT

I'd like to thank Professor Mrs. Vanmala Kadam and Professor Mrs. Pranjal Gade, my research supervisors, for their patient instruction, passionate support, and constructive criticisms of this study effort.

I'd also want to thank Dr. Sunita Jadhav for her guidance and help in keeping my development on track. My heartfelt gratitude also goes to Mrs. Shweta Thorat for his assistance with the meteorological data analysis, Ms. Snehal Jadhav who assisted me in technicians

I'd also want to thank the technicians at department's laboratory for their assistance in providing me with the resources I needed to run the application.

REFERENCES

[1] https://creativecommons.org/licenses/by/4.0/legalcode
[2] *https://patents.google.com/patent/US8359278B2*
[3] *https://testpubchem.ncbi.nlm.nih.gov*