SECURE LAB ACCESS USING CARD SCANNER PLUS FACE RECOGNITION

Mr. P. Venu Gopal, Associate Professor, Dept. Of ECE, NRI Institute of Technology, JNTUK: venugopal@nriit.edu.in
D. Ravindra, E. Madhu Latha, B. Kishore Prakash, A. Anupama, Dept. Of ECE, NRI Institute of Technology, JNTUK: dwarapudiravindra123@gmail.com

Abstract

Facial recognition is a biometric recognition technology that verifies identity using information about human facial features so it is used for access control systems. Current access control systems are implemented using traditional Radio Frequency Identification (RFID) technology or keys. Users must carry an access card or key; the access card or key can be forgotten, lost, or copied by others to use an access control system. This study proposes a multi-function facial recognition access control system that uses Python and Intelligence RFID. The system's facial recognition scheme uses Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA) facial recognition algorithms. In addition, Password systems and Bluetooth access control systems were also introduced for high-security purposes. This project aims to design and implement a secure lab access system using a combination of card scanning and facial recognition technology. The system will utilize a card scanner to read identification cards, and a camera to capture facial images of users. The system uses PCA (Principal Component Analysis) and LDA (Linear Discriminant Analysis) for facial recognition to increase the accuracy and robustness of the facial recognition system. This addresses a problem with current facial recognition technology, which achieves good results for different facial models under different lighting conditions. To render the system more user-friendly and versatile, the system requires swiping and a password. The Intelligence RFID access control function uses a high frequency (13.56 MHz) and the ISO/IEC14443-3 protocol is used for data communication between the access card and the card reader. Using a dynamic binary search algorithm, the password is saved and read using an EEPROM. This study uses a combination of software and hardware to allow double confirmation, which increases the stability and accuracy of the system.

Keywords: Access control systems, principal component analysis (PCA), linear discriminant analysis (LDA), radio frequency identification (RFID), Dynamic binary tree search algorithm, face recognition, accuracy, and robustness.

I. Introduction

Facial recognition technology is widely used, especially in transportation hubs that require high levels of security, such as banks, airports, railway stations, public security departments, hotels, automotive systems, and laboratories. It is also used to ensure travel safety. An access control system is used to control the person who enters a facility. It allows a self-managed (no human intervention) system that allows safe areas to be separated from unsafe or public areas. Compared with other biometric systems that use fingerprints or palm prints or the iris, facial recognition requires no contact with the equipment and it can capture facial images at a distance. Radiofrequency identification (RFID) technology uses the electromagnetic field in space for bidirectional transmission of data to allow non-contact automatic identification.

Radio Frequency identification (RFID) technology uses the electromagnetic field in space for bidirectional transmission of data to allow non-contact automatic identification. They are easy to operate, free from external environment and human interference, and work automatically using radio frequency identification technology, which allows communication at a long distance without direct contact. In order to obtain an efficient facial recognition system, Two facial recognition techniques:

principal component analysis (PCA) and linear discriminant analysis (LDA) facial recognition algorithm. This system is also used for Raspberry Pi. Unlike a single feature extraction method, PCA combined with LDA produces good results and has a higher precision, the facial recognition part of this study uses PCA and LDA and the Intelligence RFID access control part uses the binary tree search algorithm.

The motivation of the project is to improve the security of a lab by implementing a more advanced and secure access control system that is less prone to errors and unauthorized access compared to traditional methods such as using keys or passcodes, to reduce the time and effort required for managing access to the lab by automating the process of granting or denying access based on a user's ID card and face information, to take advantage of the latest technology, such as card scanners and face recognition, to improve the security and efficiency of the lab access control system, to meet the security and compliance requirements of the lab or organization. To provide an additional layer of security and reduce the risk of unauthorized access, to promote the use of biometric authentication instead of traditional methods like passwords or key-based systems.

Ii. Literature review

Biometric technologies are used to identify individuals based on unique physical or behavioural characteristics. Among various biometric technologies, fingerprint recognition, face recognition, and iris recognition are most widely used for access control. Compared to other biometric technologies, face recognition is a convenient, non-intrusive, and cost-effective solution for access control. Recent research has shown that integrating face recognition with other biometric technologies can further enhance the security of access control systems. For example, combining face recognition with card scanner technology can provide two-factor authentication, requiring both a physical token (the access card) and biometric authentication (the user's face). A study by Zhou et al. (2020) proposed a system that uses face recognition and smart cards to control access to sensitive laboratory areas. The system requires users to present their smart card and verify their identity through facial recognition before gaining access. The results of the study showed that the proposed system was effective in preventing unauthorized access while providing a high level of convenience for authorized users. Another study by Kuo et al. (2021) proposed a face recognition-based access control system for a university laboratory. The system used a combination of facial recognition and RFID-based access control, requiring users to present their ID card and verify their identity through facial recognition.

III. METHODOLOGY

3.1 Problem Statement

To develop a secure laboratory access control system that combines face recognition and card scanner technologies to enhance the security of laboratory access control.

The proposed system should be accurate, reliable, and easy to use, while providing a high level of security against unauthorized access.

3.2 Facial Recognition System

3.2.1 Principle Component Analysis (PCA)

Principal Component Analysis (PCA) is a popular dimensionality reduction technique in machine learning and statistics. It is mainly used for visualizing and analysing high-dimensional datasets. PCA can also be used for data compression, noise reduction, and de-correlation of features.

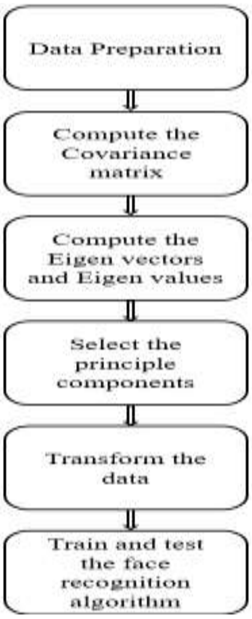

Data Preparation
Compute the Covariance matrix
Compute the Eigen vectors and Eigen values
Select the principle components
Transform the data
Train and test the face recognition algorithm

Fig.1. PCA working flow

Data preparation is collect a set of face images and pre-process them by resizing, normalizing, and aligning them to a standard size and orientation.

Compute the covariance matrix of the pre-processed face images, which represents the statistical relationship between the different pixels in the images.

COV (X, Y) = $\begin{bmatrix} cov(x,x) & cov(x,y) \\ cov(y,x) & cov(y,y) \end{bmatrix}$ --(1)

COV (X, X) = $\frac{1}{N-1}\sum_{for\ all\ X}(X-X')^{2}$ --(2)

Compute the eigenvectors and eigenvalues of the covariance matrix, which represent the principal components and their corresponding magnitudes.

det $\{c-\lambda I\}$=0 [Eigen values]--(3)

det $\{c-\lambda I\}$ U = 0 U=$\begin{bmatrix} u1 \\ u2 \end{bmatrix}$ [Eigen vector]--(4)

Select the principal components: Select a subset of the eigenvectors that capture the most variation in the data, based on their corresponding eigenvalues. This subset of eigenvectors is known as the principal components.

Transform the data: Transform the pre-processed face images into a lower-dimensional space using the selected principal components. This reduces the dimensionality of the face images and simplifies the face recognition algorithm.

Train and test the face recognition algorithm: Train the face recognition algorithm using the transformed face images and test its performance on a validation set of face images. By applying PCA to the face images in this system, you can reduce the dimensionality of the data and improve the accuracy and efficiency of the face recognition algorithm.

3.2.2 Linear Discriminant Analysis (LDA)

LDA is a classification algorithm that can be used to classify data into multiple classes based on a set of input features. In your project, LDA can be used to classify face images into authorized and unauthorized users based on their facial features.

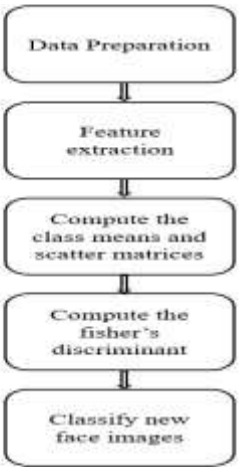

Data Preparation
Feature extraction
Compute the class means and scatter matrices
Compute the fisher's discriminant
Classify new face images

Fig.2. LDA working flow

Data preparation: Collect a set of face images and pre-process them by resizing, normalizing, and aligning them to a standard size and orientation. Also, create a labelled dataset indicating which face images belong to authorized and unauthorized users.

Feature extraction: Extract features from the pre-processed face images, such as the distance between the eyes, the angle of the nose, and the shape of the mouth. These features should capture the most important aspects of the face that distinguish between authorized and unauthorized users.

Compute the class means and scatter matrices: Compute the mean feature vectors and scatter matrices for each class, which represent the statistical properties of the feature vectors for each class.

Compute the Fisher's discriminant: Compute the Fisher's discriminant, which is a linear combination of the feature vectors that maximizes the between-class variance and minimizes the within-class variance. This discriminant separates the feature vectors into two classes: authorized and unauthorized.

Classify new face images: Given a new face image, extract its features and compute its feature vector. Then, apply the Fisher's discriminant to the feature vector to determine whether the image belongs to an authorized or unauthorized user. By applying LDA to the face images in this project, you can classify the images into authorized and unauthorized users based on their facial features. This provides an additional layer of security to the access control system and helps prevent unauthorized access to sensitive areas.

Machine learning is used to classify the traffic density level based on the output from Canny Edge Detection and Hough Line Transform.

3.3 RFID Access Control System

Radio Frequency Identification (RFID) access control systems are security systems that use RFID technology to control and manage access to a specific area or facility. The system typically consists of three main components: RFID tags or cards, RFID readers, and a control panel. Radio Frequency Identification (RFID) access control systems are electronic security systems that use radio waves to communicate between a reader and a tag or transponder attached to a person or an object. The primary purpose of RFID access control systems is to provide secure and efficient access to restricted areas.

3.4 Dynamic Binary Tree Algorithm

Dynamic binary tree algorithm is a data structure that allows efficient searching, insertion, and deletion of data elements. In your project, the dynamic binary tree algorithm can be used to select and implement the most appropriate access control system based on the user's preferences and the security requirements of the lab. the dynamic binary tree algorithm can be used to select and implement the RFID system, password system, and Bluetooth system in this project.

The steps for applying the dynamic binary tree algorithm to select and implement the access control systems in this project are as follows: Defining the security requirements of the lab, such as the level of security required, the types of threats that need to be protected against, and the criticality of the data and equipment in the lab. Defining the preferences of the lab users, such as the ease of use, the convenience, and the familiarity of the access control system. Build a dynamic binary tree that stores the various access control systems, such as the RFID system, password system, and Bluetooth system, as its nodes. The tree should be constructed based on the security requirements and user preferences defined in steps 1 and 2. Traverse the dynamic binary tree to determine the most appropriate access control system for the lab based on the security requirements and user preferences. Once the most appropriate access control system has been selected, implement it in the lab and integrate it with the other access control systems, such as the card scanner and face recognition algorithms. By using the dynamic binary tree algorithm to select and implement the access control systems in this project, you can ensure that the most appropriate system is chosen based on the security requirements and user preferences. This helps to provide a robust and effective access control system that prevents unauthorized access to the lab and protects sensitive data and equipment.

3.5 Flow Chart

The flow chart for the proposed system is as follows:

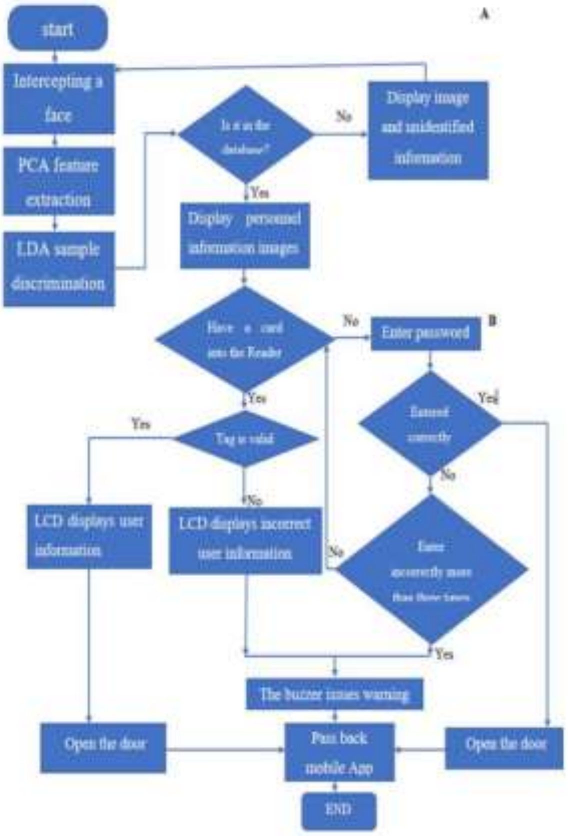

A
start
Intercepting a face
PCA feature extraction
LDA sample discrimination
Is it in the database?
No
Display image and unidentified information
Yes
Display personnel information images
Have a card into the Reader
No
Enter password
B
Yes
Tag is valid
Yes
Entered correctly
Yes
No
LCD displays user information
No
LCD displays incorrect user information
No
Enter incorrectly more than three times
Yes
The buzzer issues warning
Open the door
Pass back mobile App
Open the door
END

Fig.3. Flow chart of proposed system

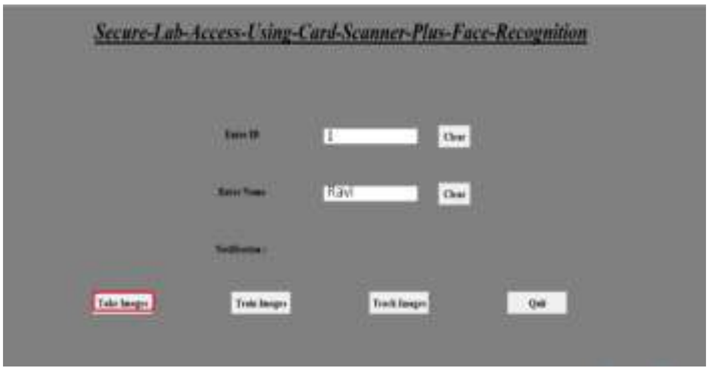
The flow chart outlines the system starts by connecting the hardware circuit to the PC and opening the Python IDLE window. The system is implemented using Python code, which includes face recognition algorithms to identify the user. Once the code is executed, a window appears for face recognition. The user enters their ID and name, and the system uses the webcam of the PC to take images of the user's face. These images are used as input for the face recognition algorithm. To train the face recognition algorithm, the user clicks on the 'Train Images' button. The algorithm uses techniques such as PCA (Principal Component Analysis) and LDA (Linear Discriminant Analysis) to train the images. The facial database is already stored in the PC, which helps the algorithm to learn and recognize the user's face accurately. Once the images are trained, the user can click on the 'Track Images' button to match the input image with the database. If the match is successful, the control moves to the Arduino board.

The Arduino board acts as a decision-making board and provides three options for access control: card scanning, password, and Bluetooth. The card scanner uses the MFRC 522 card reader to scan the access card. If the card scan is unsuccessful, the user can use the password system. The password system requires the user to enter a correct PIN on the matrix keyboard. If both of these systems fail, the Bluetooth access system is used. The Bluetooth access system requires the user to install the Bluetooth terminal app on their phone and connect it to the Bluetooth module in the circuit. The user gives the command '1' to unlock the door. If none of the systems provide access, the process restarts, and the user can try again.

In summary, the secure lab access system using card scanner and face recognition is implemented using Python code and Arduino board. The system uses face recognition algorithms to identify the user, and the Arduino board provides three options for access control: card scanning, password, and Bluetooth. The system provides multiple layers of security to ensure that only authorized users can access the lab.

IV. Result

After running the face recognition code on the PC the below-shown window will be opened, then enter the person ID and name and click on take images then it can take images as a database.



Secure-Lab-Access-Using-Card-Scanner-Plus-Face-Recognition

Enter ID 1

Enter Name Ravi

Notification :

Fig.4. Face recognition window

Then enter ID, and name of the person then click on Take images, it will take the images as input through the webcam of PC. That will be shown in below figure.

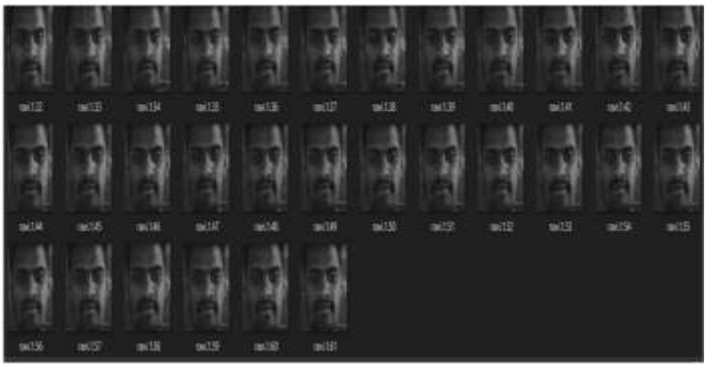
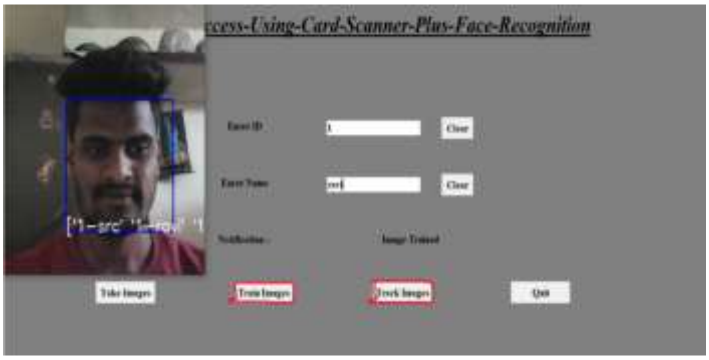


Fig.5. Face database

After taking the images, click on train images and then click on track images again the PC webcam will take the input and compare it with the database.



ccess-Using-Card-Scanner-Plus-Face-Recognition

Enter ID 1

Enter Name [illegible]

Notification : Image Trained

Fig.6. Tracking images

After the face recognition is granted, the command goes to the next authentication process is card scanning, password, and Bluetooth system. Now it shows the option like SCAN/PIN In display if we have a card then scan it will give access to the person.

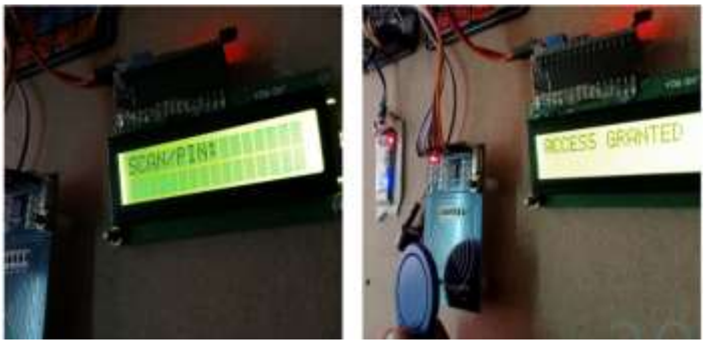


Fig.7. RFID system

Now the password system in this we press the # key in the matrix keyboard then the process will start.

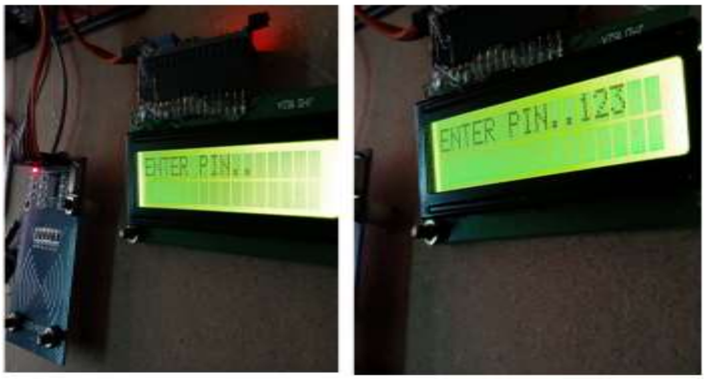


Fig.8. Password system

If both the systems will fail in giving access then the control goes to the Bluetooth system in the Bluetooth module is connected to our mobile app and we give the command as ’1’ then it will give access.

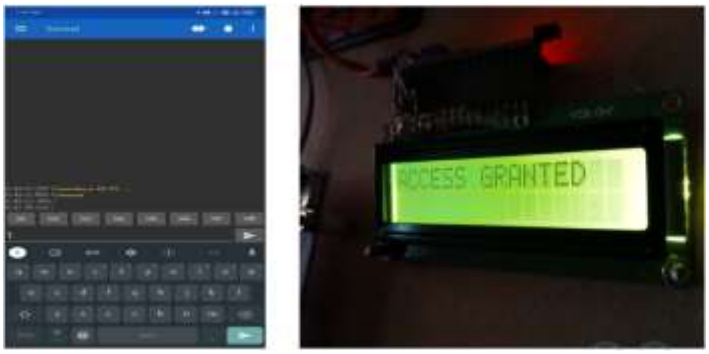
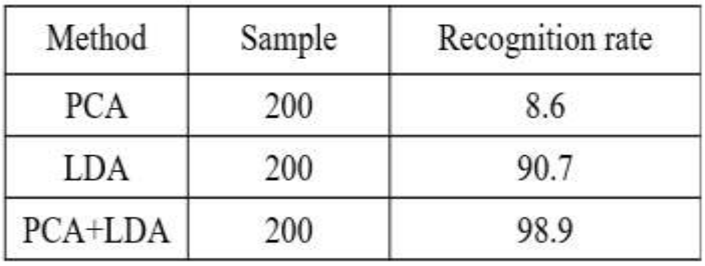


Fig.9. Bluetooth system

Finally, user get the access by all these systems are implemented by using different conditions and methods and then finally we get the access granted for the person to unlock the door for secured places.



Method	Sample	Recognition rate
PCA	200	8.6
LDA	200	90.7
PCA+LDA	200	98.9

The performance of the "Secure Lab Access Using Card Scanner Plus Face Recognition" system can be evaluated based on several key performance metrics. Recognition accuracy is a critical performance metric, as the system must be able to accurately recognize authorized users and deny access to unauthorized users. The system should have a recognition accuracy of at least 95% to ensure that only authorized users are granted access to the lab. Another important performance metric is the speed of the face recognition algorithm and access control system. The system should be able to quickly recognize the user's face and grant access. The system should be able to recognize the user's face and grant access within 3 seconds to minimize waiting times and ensure a smooth user experience. The system should be able to operate under varying lighting conditions and be able to recognize the user's face consistently in different environmental settings, with a minimum recognition rate of 90%.

IV. CONCLUSION

In conclusion, Secure Lab Access Using Card Scanner Plus Face Recognition System summarizes the main findings and results and highlights its advantages over existing systems. It provides a comprehensive summary of the project, including its strengths and limitations, and suggests its potential for future research and application. It will be more useful for unauthorized places and give more security than other systems. This study designs and implements a multi-functional facial recognition access control system that combines facial recognition technology and Intelligence RFID technology and uses a combination of PCA and LDA facial recognition and a dynamic binary tree anti-collision algorithm.

The system controls a user's access using an image of the user's face and the user's radio frequency identification card or input password and records the user's data. Compared with a traditional access control system, this system is multi-functional, simpler to operate, and highly secure. The experimental results show that the system is feasible and can be used in offices, laboratories, and other secure sites.

REFERENCES

[1] J. Liang, H. Zhao, X. Li, and H. Zhao, ''Face recognition system based on deep residual network,'' in Proc. 3rd Workshop Adv. Res. Technol. Ind. (WARTIA), Nov. 2017, p. 5.

[2] I. Taleb, M. E. Amine Ouis, and M. O. Mammar, ''Access control using automated face recognition: Based on the PCA & LDA algorithms,'' in Proc. 4th Int. Symp. ISKOMaghreb, Concepts Tools Knowl. Manage. (ISKO-Maghreb), Nov. 2014, pp. 1–5.

[3] X. Pan, ''Research and implementation of access control system based on RFID and FNN-face recognition,'' in Proc. 2nd Int. Conf. Intell. Syst. Design Eng. Appl., Jan. 2012, pp. 716–719, doi: 10.1109/ISdea.2012.400.

[4] A. A. Wazwaz, A. O. Herbawi, M. J. Teeti, and S. Y. Hmeed, ''Raspberry Pi and computers-based face detection and recognition system,'' in Proc. 4th Int. Conf. Comput. Technol. Appl. (ICCTA), May 2018, pp. 171–174.

[5] A. Hafid, S. Benouar, M. Kedir-Talha, F. Abtahi, M. Attari, and F. Seoane, ''Full impedance cardiography measurement device using raspberry PI3 and system-on-chip biomedical instrumentation solutions,'' IEEE J. Biomed. Health Informat., vol. 22, no. 6, pp. 1883–1894, Nov. 2018.

[6] A. Li, S. Shan, and W. Gao, ''Coupled bias–variance tradeoff for cross-pose face recognition,'' IEEE Trans. Image Process., vol. 21, no. 1, pp. 305–315, Jan. 2012. C. Ding, C. Xu, and D. Tao, ''Multi-task pose-invariant face recognition,'' IEEE Trans. Image Process., vol. 24, no. 3, pp. 980–993, Mar. 2015.

[7] J. Yang, Z. Lei, D. Yi, and S. Li, ''Person-specific face antispoofing with subject domain adaptation,'' IEEE Trans. Inf. Forensics Security, vol. 10, no. 4, pp. 797–809, Apr. 2015

[8] H. S. Bhatt, S. Bharadwaj, R. Singh, and M. Vatsa, ''Recognizing surgically altered face images using multiobjective evolutionary algorithm,'' IEEE Trans. Inf. Forensics Security, vol. 8, no. 1, pp. 89–100, Jan. 2013.

[9] T. Sharma and S. L. Aarthy, ''An automatic attendance monitoring system using RFID and IOT using cloud,'' in Proc. Online Int. Conf. Green Eng. Technol. (IC-GET), Nov. 2016, pp. 1–4.

[10] W. Shin and J. Kim, ''A capture-aware access control method for enhanced RFID anti-collision performance,'' IEEE Commun. Lett., vol. 13, no. 5, pp. 354–356, May 2009. 77

[11] W. Zhu, J. Cao, Y. Xu, L. Yang, and J. Kong, ''Fault-tolerant RFID reader localization based on passive RFID tags,'' IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 8, pp. 2065–2076, Aug. 2014.

[12] S. Qi, Y. Zheng, M. Li, Y. Liu, and J. Qiu, ‘‘Scalable industry data access control in RFID-enabled supply chain,’’ IEEE/ACM Trans. Netw., vol. 24, no. 6, pp. 3551– 3564, Dec. 2016.

[13] X. Wang and Y. Wang, ‘‘An office intelligent access control system based on RFID,’’ in Proc. Chin. Control Decis. Conf. (CCDC), Jun. 2018, pp. 623–626.

[14] O. A. Allah, S. Abdalla, M. Mekki, and A. Awadallah, ‘‘RFID based access control in registration system,’’ in Proc. Int. Conf. Comput., Control, Electr., Electron. Eng. (ICCCEEE), Aug. 2018, pp. 1–4.

[15] A. Mai, Z. Wei, and M. Gao, ‘‘An access control and positioning security management system based on RFID,’’ in Proc. 7th Int. Conf. Intell. Hum.- Mach. Syst. Cybern., Aug.