IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 3, 2021, accepted April 29, 2021, date of publication June 9, 2021, date of current version June 21, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3087917

Design of Multi-Functional Access Control System

HAI-WU LEE, (Member, IEEE)
School of Science and Engineering, Xiangsihu College of Guangxi University for Nationalities, Nanning 530008, China
e-mail: 2439141397@qq.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 and the access card or a 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. This addresses a problem with current facial recognition technology, which achieve 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. The system designed in this paper not only improves security, but also has more flexible functions than other access control systems. This is a good example of other systems trying to implement more flexible validation.

INDEX TERMS Facial recognition, multi-functional, dimension reduction, dynamic binary search algorithm.

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 [1]. An access control system is used to control the personnel who enter 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 [2]. Xiang Pan used a FNN (Fuzzy Neural Network) for RFID and facial recognition to implement an access control system [3]. Xiang Pan Wazwaz *et al.* used a Raspberry Pi facial recognition system for security systems in public places, such as shopping malls, universities and airports, and for different situations and scenarios [4]. The Raspberry Pi is a supportive do-it-yourself platform for projects and applications that can be quickly prototyped using widely available and affordable components [5].

The widespread use of biometrics and the increasing popularity of plastic surgery means that several techniques have been created to evade recognition, so the security of facial recognition systems has deteriorated and facial images that are captured in an unconstrained environment often feature significant changes in posture. Annan Li *et al.* showed that changes in posture inhibit automatic facial recognition, so algorithms do not readily identify positive facial images. The effect of changes in posture on automatic facial recognition has been the subject of some studies [6], [7]. A practical facial recognition system must allow accurate recognition and recognize camouflage to distinguish the faces of real people (real faces) and attackers (pseudo-faces). Jianwei Yang proposed a face for a specific person scheme to prevent the use of camouflage. This uses a classifier that is specially trained to identify camouflage attacks, so there is no interference between subjects [8], [9].

Radio frequency identification (RFID) technology uses the electromagnetic field in a space for bidirectional transmission of data to allow non-contact automatic identification [10].

The associate editor coordinating the review of this manuscript and approving it for publication was bin Xu.

Unlike traditional IC cards, barcodes and magnetic cards, RF cards are typically non-contact and not easily damaged. 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 [11], [12].

In recent years, radio frequency identification technology has developed rapidly, become more mature, cheaper and easier to use. It is widely used for identity documents, access control systems, supply chain, inventory tracking, car-charging and production. In areas such as control and asset management, it has become an indispensable component of residential, banking, factories, libraries and other systems [13]–[16].

With the increasing demand for surveillance cameras [17], the demand for facial recognition systems has also increased, and many classic and modern facial recognition algorithms perform well in tests but recognition performance is poor in actual use. It is difficult to simultaneously reconcile illumination, image misalignment and occlusion changes in a test image. Wagner *et al.* proposed a conceptually simple facial recognition system that implements illumination changes, image misalignment and parts. This allows robustness and stability against occlusion [18]. The method that was proposed by Weiping Chen better identifies partially occluded faces and directly matches the sketch face and the photo face [19].

In order to obtain an efficient facial recognition system, Neel proposed two facial recognition techniques: principal component analysis (PCA) and linear discriminant analysis (LDA) facial recognition algorithm. This system is also used for the Raspberry Pi [20]. Unlike a single feature extraction method, PCA combined with LDA produces good results and has a higher precision ratio [21].

When Intelligence RFID system transmits data, there may be two or more tags within the recognition range of the reader, which causes communication conflicts [22]. To solve this collision problem, the anti-collision algorithms include ALOHA, Q-value and binary tree search [23]–[25]. The performance of ALOHA and Q-value algorithms deteriorates sharply as the number of tags increases. The maximum utilization rate for ALOHA is 36.8% and the Q value is 18.6% [26], [27]. Therefore, the facial recognition part of this study uses PCA and LDA and the Intelligence RFID access control part uses on binary tree search algorithm.

The overall design architecture of the system is presented and then the specific identity authentication methods. The process for the access control system is detailed and final experimental results and conclusions are given.

II. SYSTEM ARCHITECTURE DIAGRAM

The hardware system architecture diagram for this study is shown in Figure 1. It has two parts: a facial recognition system and an access control system.

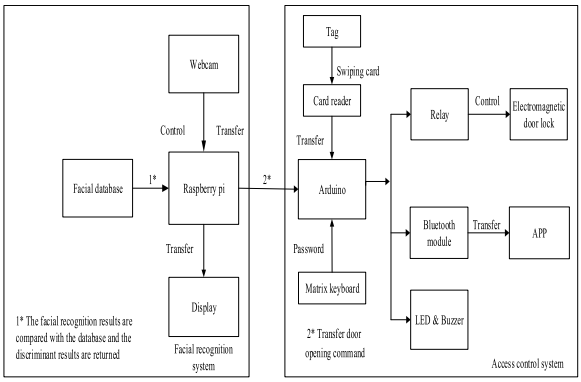


FIGURE 1. System hardware architecture.

A. FACIAL RECOGNITION SYSTEM

MCU: Raspberry Pi 3B+ is an ARM microcomputer motherboard that uses a Linux system.

Webcam: OV5647 Camera, for collecting facial images (testing 200 faces).

Display: Used to display the captured facial image.

Face database: Storage of the facial image in a raspberry pie. [28], [29]

B. ACCESS CONTROL SYSTEM

MCU: Arduino Uno is the access control panel and is responsible for receiving the Raspberry Pi access control commands and other access controls.

Matrix keyboard: 4*4 matrix keyboard for entering passwords.

Card reader: MFRC-522 sensor module reader for reading Tag card sequences.

Access Card: Tag (testing 500 tags).

Relay module: High and low level switching trigger.

Electromagnetic door lock: used as a switch.

LED buzzer: For door opening prompts and error alerts.

Bluetooth module: receives Arduino instructions to transfer attendance data to the mobile app.

Mobile APP: receives information that is transmitted by Bluetooth.

III. METHODOLOGY

The system has two components: a facial recognition system and Intelligence RFID.

A. FACIAL RECOGNITION SYSTEM

The facial recognition system uses Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA) algorithms.

(a) The PCA algorithm allows feature extraction and the reduction of mathematical dimensionality.

This study uses the PCA algorithm, which is a feature extraction method for statistical analysis. It has many applications. Feature extraction is a very important for a facial recognition system. Different recognition methods use

different strategies for extracting different features, as explained below:

1) FEATURE EXTRACTION

N facial images in the random face database are represented by $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \ldots \mathbf{x}_n$. The subscripts represent m and x vectors.

The average value for the facial image sample is calculated as shown in formula (1):

$$\mathbf{m_x} = \frac{1}{N}\sum_{i=1}^{N}\mathbf{x_i} \tag{1}$$

Equation (2) calculates the difference between each facial image and the average:

$$\varphi_\mathbf{i} = \mathbf{x_i} - \mathbf{m_x} \tag{2}$$

The covariance matrix is obtained using Formulae (1) and (2), as shown in Equation (3) [30]:

$$\mathrm{C} = \frac{1}{N}\sum_{i=1}^{N}\varphi_\mathbf{i}\varphi_\mathbf{i}^\mathbf{T} = \frac{1}{N}\mathbf{A}\mathbf{A}^\mathbf{T} \tag{3}$$

Matrix A is the centralized data. T: transpose matrix of $\boldsymbol{A}$.

2) REDUCTION OF MATHEMATICAL DIMENSIONS

The PCA algorithm reduces the dimensions of the facial image to ensure that the intra-class dispersion matrix for the sample is non-singular. From the matrix of the above equation (3), the front $p\,(p \ll N)$ feature maximum value λ_i and its corresponding eigenvector can be obtained. The orthogonal normalized feature space vector can be obtained from equation (4) [31]:

$$u_i = \frac{1}{\sqrt{\lambda_i}}A_{v_i} \quad (i = 1, 2, \ldots p) \tag{4}$$

Let the orthogonal normalized feature space be: $\omega = (u_1, u_2, \ldots u_p)$

Projecting the difference between each average and the face onto the orthogonal normalized feature space, the feature space is obtained using Equation (5):

$$W_{pca} = \omega^T\varphi_i \quad (i = 1, 2, 3 \ldots N) \tag{5}$$

The sample database for faces for this system shows that the PCA algorithm is sensitive to anomalous data. The anomalous data increases the estimation subspace deviation larger so the real situation is not represented and nonlinear data cannot be processed.

LDA Algorithm: The LDA algorithm extracts important features from the feature space. These features can be used to discriminate between similar and non-similar samples. The largest ratio between the inter-class dispersion S_b and the intra-class dispersion S_w in the database is selected, as shown in Formulae (6-7):

$$S_b = \sum_{i=1}^{C} P_i(\mu_i - \mu)(\mu_i - \mu)^T \tag{6}$$

$$S_w = \sum_{i=1}^{M}\sum_{x_i \in X_i}(x_k - \mu_i)(x_k - \mu_i)^T \tag{7}$$

where C and M are the total number of categories, P_i is the prior probability of the i^{th} sample, ?u_i is the average of the C_i samples and x_k is the i^{th} sample.

When the LDA algorithm is used for facial recognition, the intra-class dispersion matrix S_w of the image sample is singular because the sample is small. This occurs because the number of sample images in the database is much smaller than the number of pixels in all images. The system database for facial sample images is projected onto a feature subspace and the maximum value of W_{lda} is obtained for the feature subspace using Formula (8):

$$W_{lda} = argmax\frac{|W^T W_{pca}^T S_b W_{pca} W|}{|W^T W_{pca}^T S_w W_{pca} W|} \tag{8}$$

In equation (8), W_{pca} is the projection matrix for the PCA algorithm. Multiplying by equations (5) and (8) gives the eigenvector for W as the optimized eigenvalue, as shown in Equation (9):

$$W = W_{pca}W_{lda} \tag{9}$$

A combination of PCA and LDA can greatly reduce the number of dimensions and addresses the issue of a small sample while retaining the feature structure.

B. INTELLIGENCE RFID TECHNOLOGY

The Intelligence RFID card reader uses a dynamic binary tree search algorithm.

The binary tree search algorithm is controlled by the reader. A recursive method is used to continuously divide the conflicting tags. If there are two or more tags conflicts, all conflicting tags are divided into two left and right subsets and numbered 0 and 1. If there is no conflict in Subset 0, then the identification is successful. If there is a conflict, Subset 0 is divided into two subsets, 00 and 01, until all labels in subset 0 are identified, Subset 1 is then interrogated. The binary tree search algorithm is shown in Figure 2.

In Figure 2, Δ denotes all conflicting tags in the Reader identification range, O denotes Subset 0, $\square$ denotes Subset 1 and each node represents a time slot. The total number of time slots T(n) for the algorithm is calculated using Formula (10) [32].

$$T(n) = 2n + 1 \tag{10}$$

where n is all the parent elements in the tree. The greater the value of n, the greater is the total number of time slots for the algorithm.

For a binary tree with M elements, the number of comparisons $C(M)$ to be performed is calculated using Equation (11) and the average number of comparisons $C_{avg}(M)$ is calculated using Equation (12) [30].

$$\text{When M } > 1, \quad C(M) = C(\frac{M}{2}) + 1,\ C(1) = 1$$

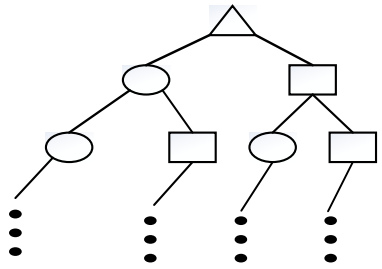


FIGURE 2. Schematic diagram of binary tree search algorithm.

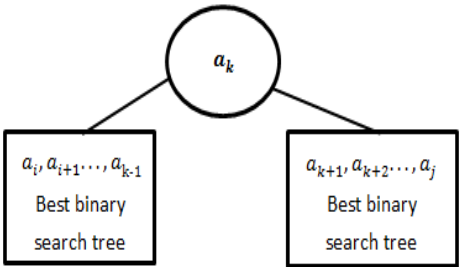


FIGURE 3. Binary tree rooted at a_k.

In the formula, $\frac{M}{2}$ is rounded down and because the algorithm uses a recursive method, it is assumed that $M = 2^K$:

$$C(2^K) = C(\frac{2^K}{2}) + 1 = \log_2 M + 1$$
$$C(M) = \log_2 M + 1 \tag{11}$$

Average comparisons

$$C_{avg}(M) \approx \log_2 M \tag{12}$$

Equations (10)∼(12) show that the greater the number of conflicting Mgs in the Reader recognition range, the greater is the total time slot for the algorithm, and the greater is the number of comparisons and the average comparison time, so the performance of the binary search algorithm is reduced. In order to address these problems, this study increases the efficiency of the binary tree search algorithm.

A binary tree with M elements can have a number of differently shaped binary trees of Catalan, as shown in Equation (13) [30]:

$$\text{When } M > 0, \quad c(M) = \binom{2M}{M} \frac{1}{M+1}, \; c(0) = 1 \tag{13}$$

If $a_1, a_2 \ldots, a_M$ are tags within the Reader identification range, $p_1, p_2 \ldots, p_M$ is their search probability, T_i^j is a binary tree that is composed of $a_i, a_{i+1} \ldots, a_j$ *and* $C[i, j]$ is the minimum average number of searches in this tree, where $1 \leq i \leq j \leq M$, then using the dynamic programming method, as shown in Figure 3, a root a_k is selected from $a_i, a_{i+1} \ldots, a_j$ and its element $a_i, a_{i+1} \ldots, a_{k-1}$ in the left sub tree T_i^{k-1} is the best permutation. The elements $a_{k+1}, a_{k+2} \ldots, a_j$ in the right sub tree T_{k+1}^j also give the best arrangement.

The number of layers in the tree are counted from 1, as shown in Equation (14) [30].

$$\begin{aligned} C[i,j] &= \min_{i\leq k\leq j}\{p_k.1 + \sum_{s=i}^{k-1} p_s.(a_s \text{ number of layers} \\ &\quad \text{in } T_i^{k-1} + 1) + \sum_{s=k+1}^{j} p_s.(a_s \text{ number of layers} \\ &\quad \text{in } T_{k+1}^{j} + 1)\} \\ &= \min_{i\leq k\leq j}\{p_k + \sum_{s=i}^{k-1} p_s.a_s \text{ number of layers in } T_i^{k-1} \\ &\quad + \sum_{s=i}^{k-1} p_s + \sum_{s=k+1}^{j} p_s.a_s \text{ number of layers in } T_{k+1}^{j} \\ &\quad + \sum_{s=k+1}^{j} p_s = \min_{i\leq k\leq j}\{\sum_{s=i}^{k-1} p_s.a_s \text{ number of} \\ &\quad \text{layers in } T_i^{k-1} \\ &\quad + \sum_{s=k+1}^{j} p_s.a_s \text{ number of layers in } T_{k+1}^{j} + \sum_{s=i}^{j} p_s\} \\ &= \min_{i\leq k\leq j}\{C[i,k-1] + C[k+1,j]\} + \sum_{s=i}^{j} p_s \\ &\quad \text{When } 1 \leq i \leq j \leq M, \\ C[i,j] &= \min_{i\leq k\leq j}\{C[i,k-1] + C[k+1,j]\} + \sum_{s=i}^{j} p_s \\ &\quad \text{When } 1 \leq i \leq M, \quad C[i,i] = p_i \end{aligned} \tag{14}$$

It is seen that the dynamic binary search tree algorithm selects the minimum value for $C[i, k-1]+C[k+1, j]$ when the number of conflicting Tag cards in the Reader recognition range is larger. Therefore, the dynamic binary tree search algorithm makes fewer average comparisons in the than that a traditional binary search tree algorithm and performance is increased.

IV. AUTHENTICATION PROCESS

In terms of facial recognition, Intelligence RFID and password authentication, two can be used as a set of authentication methods. When authentication is achieved, access is granted. There are three authentication combinations: face recognition and Intelligence RFID, facial recognition and a password and Intelligence RFID and a password. As shown in Figure 4, the system flow chart has two parts: image and Intelligence RFID. Facial recognition is used first and then one of the other two authentication methods is selected, Access is granted when the two-step authentication is achieved.

A. IMAGE IDENTIFICATION

The camera is initialized, features are extracted and the feature values are sent to the database for matching.

1. Intercept the face: Turn on the camera to capture the original picture.

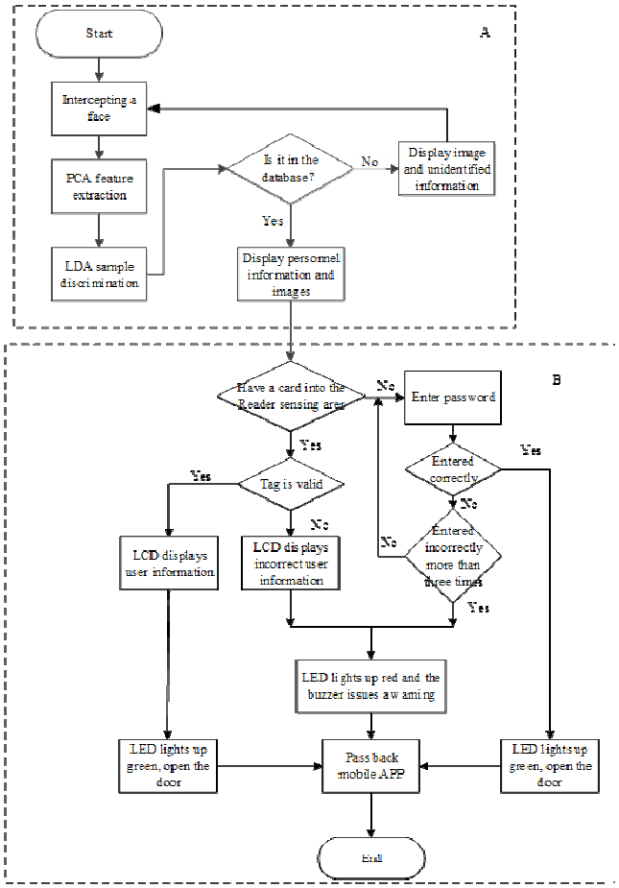


FIGURE 4. System flow chart.

2. PCA feature extraction:

(1) Convert a color image to a gray scale image.

(2) Gaussian filtering is used for denoising to increase the recognition rate.

(3) A mathematical method is used to obtain the average value for the facial image and the difference between the facial image and the average value and the covariance matrix is formed by the above values.

(4) The first p largest eigenvalues are obtained from the covariance matrix to reduce dimensionality and the feature space is obtained using orthogonally normalized space vectors.

(5) The difference between the facial image and the average value is projected onto the feature space to obtain a PCA feature space.

3. LDA sample discrimination:

(1) The vector in the PCA feature space is used for the in-class and inter-class formulae.

(2) Faces of the same type and different types of faces are separated.

(3) The eigenvectors for the intra-class and inter-class matrices are obtained and these eigenvectors are multiplied by the PCA feature space to obtain the LDA subspace.

(4) The averaged facial image is projected into the LDA subspace to calculate the Euclidean distance.

TABLE 1. Comparative analysis of PCA, LBP, LDA and CNN.

	sample	recognition rate
PCA	200	88.6
LBP	200	89.1
LDA	200	90.7
CNN	200	96.8
PCA+LDA	200	98.9

Database: This system's facial image sample library.

Display personnel information: personnel information and images are displayed on the display.

Unrecognized person: Displays unrecognized words and images.

Arduino: The door signal is transmitted to the Arduino by Raspberry Pi via the Bluetooth module.

B. INTELLIGENCE RFID

If the first step for authentication uses facial recognition, then the second step authentication can use a card or password.

a. When a tag enters the sensing area, the RF card reader reads the tag information and initiates authentication. If the user is authenticated, the LCD displays the user information and the LED is green, and the electromagnetic door lock is turned on. If the tag is invalid, the LCD displays the wrong user information, the LED is red and the buzzer sounds.

b. The user enters the password using the keyboard. If the entered password is correct, the LED is green and the electromagnetic door lock is turned on. If the password is entered incorrectly more than three times, the LED is red and the buzzer sounds.

User authentication Data is transmitted and the user information data is transmitted back to the mobile phone App through the Bluetooth module for processing.

V. COMPARATIVE ANALYSIS

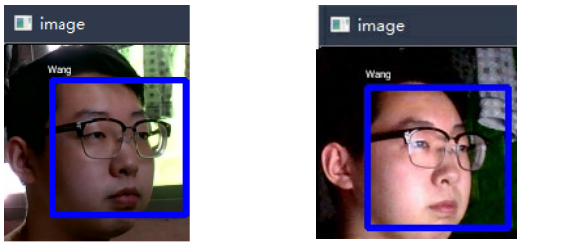
The comparative analysis is two parts: facial recognition and Intelligence RFID.

A. FACIAL RECOGNITION

PCA, LDA and other algorithms are shown in Table 1.

Figures 5 show the recognition result of CNN under different lighting conditions. Figure 5(a) shows the recognition result under dark light conditions and Figure 5(b) shows the recognition result under bright light. The experimental results in Table 1 show that the recognition rate for PCA combined with LDA is significantly higher than that for other algorithms. LBP is sensitive to direction information. CNN has many parameters, is not easy to optimize and incurs a large performance overhead during training.

This article take the improved convolution neural network, a total of 17 layer, the first convolutional layer filters



(a) Facial recognition in dark light (b) Facial recognition in bright light

FIGURE 5. Facial recognition in dark and bright light.

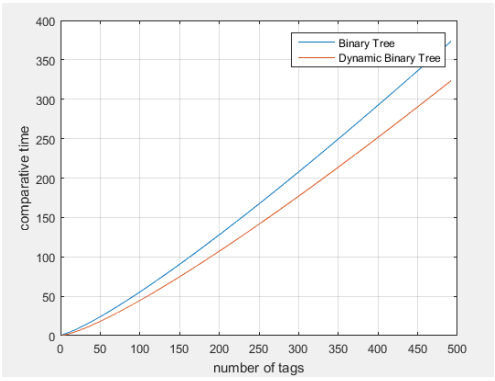


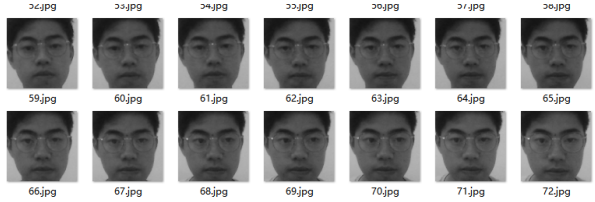
FIGURE 6. Algorithmic simulation of binary tree and dynamic binary tree.

64*64 input images, use the 32 convolution kernels, adopts full convolution method, each convolution kernel has a size of 3*3, big convolution is decomposed into multiple small convolution kernel, guaranteed under the same conditions, save network resources, to a certain extent, improve the network effect; Second use Relu activation functions to the output of the first layer as input of this layer, Relu function is one of the simple and efficient activation functions in convolutional neural networks, It's going to make the output of some neurons 0, to increase the sparse network, reduce the computing cost, at the same time reduce the dependencies between parameters, alleviate fitting problems, And the Relu function is easier to learn and optimize; The third layer is the pooling layer, which adopts the maximum pooling method. The maximum value of the covered area is selected as the eigenvalue of the area to reduce the size of the cross-layer image and achieve dimensionality reduction. The size of the pooling window is 2*2; The fourth layer is the Dropout layer. In the training stage, some randomness is added to the network through the Dropout layer to consciously reduce the model parameters, so as to make the model more robust and less prone to over-fitting. The ratio is 0.5. In addition, dynamic learning rate is used to speed up the convergence rate. Learning rate is used as a parameter to control the speed of model convergence to the local minimum value. If it is set improperly, it will affect the maturity of the model.

After that, the convolution layer, activation function, pooling layer, and Dropout layer continue to be used so that the data flowing through the network is multidimensional, while

TABLE 2. Comparative analysis of binary tree and dynamic binary tree.

	sample	search times
Binary Tree	500	375
Dynamic Binary Tree	500	325



(a) Facial images of Hao-Wen Mei in the database

(b) Facial images of Ji-Chao He in the facial image database

(c) Facial images of Fan-Fan Peng in the database

FIGURE 7. Facial images in the facial image database.

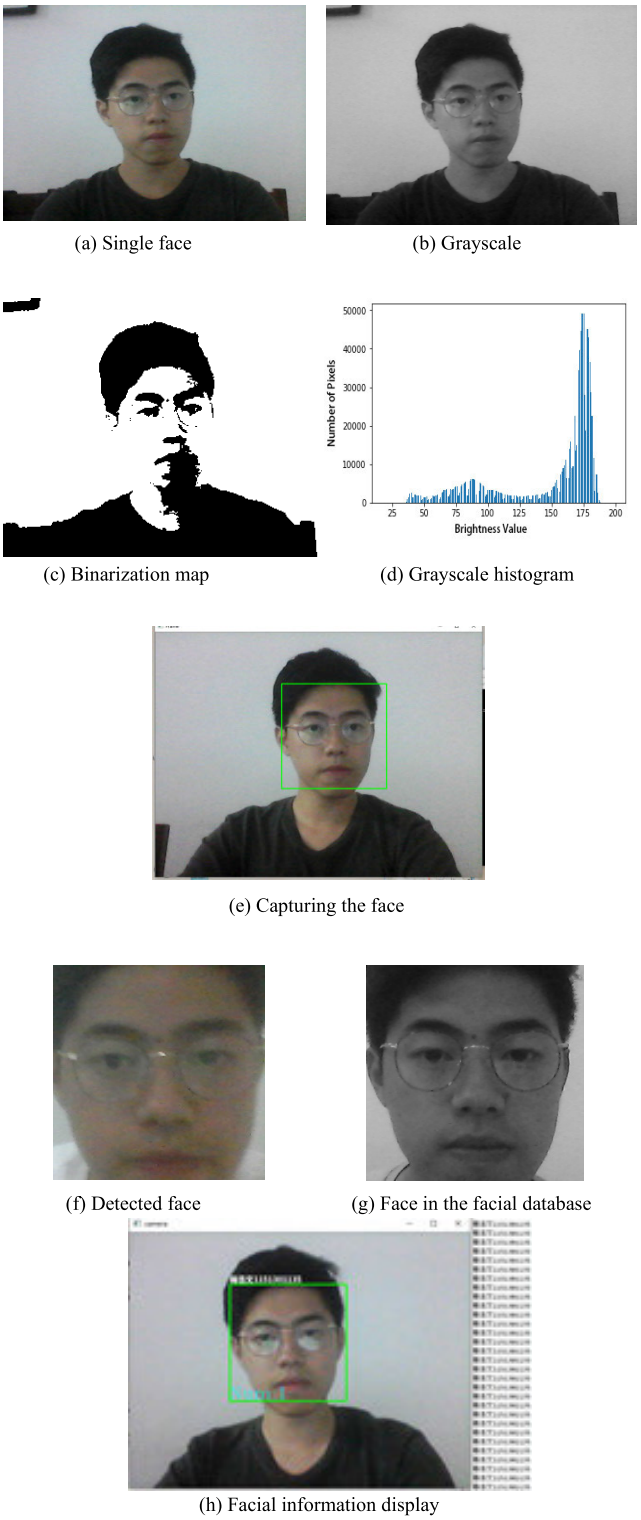
the full connection layer requires one-dimensional input, so a Flatten layer compacts the data into one dimension and then enters the full connection layer. The last layer uses the cross entropy loss function to complete the classification output.

PCA is significantly affected by illumination conditions and other factors that are not related to facial recognition. LDA extracts a set of feature vectors using class member information. The set of feature vectors depends on the difference between different faces: not the change in illumination conditions, facial expression or direction. Therefore, the combination of PCA and LDA reduces the sensitivity to illumination conditions and changes in facial pose, so recognition is more effective.

B. INTELLIGENCE RFID

The results for Binary Tree and Dynamic Binary Tree Search Algorithms are shown in Table 2.

Table 2 shows that for 500 tag samples, the number of basic binary tree searches is 375 and the number of improved dynamic binary tree searches is 325 so the number of searches is reduced by 13.3%. The results in Figure 6 show that the



(a) Single face (b) Grayscale

(c) Binarization map (d) Grayscale histogram

(e) Capturing the face

(f) Detected face (g) Face in the facial database

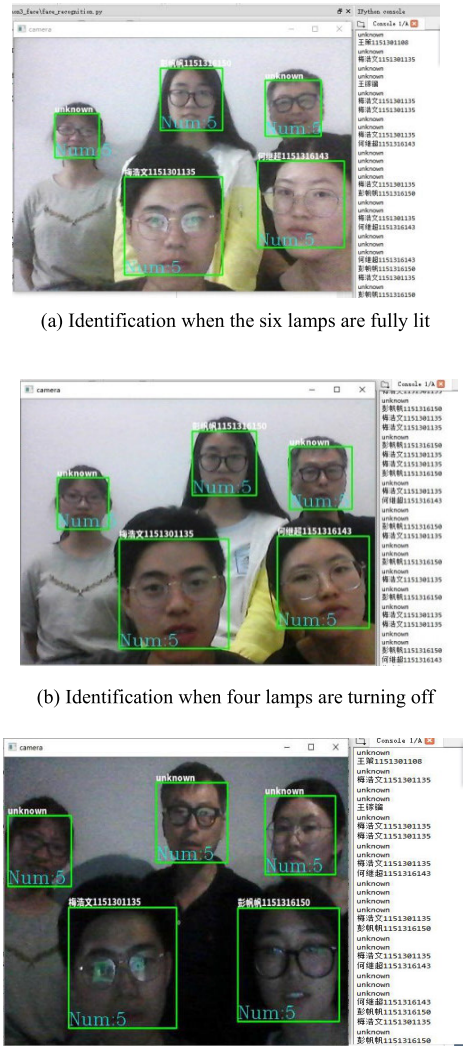
(h) Facial information display

FIGURE 8. Experimental results for images with only a single face.

dynamic binary tree search algorithm is superior to the basic binary tree search algorithm.

VI. EXPERIMENTAL RESULTS

The Results section has into two parts: facial recognition and Intelligence RFID.



(a) Identification when the six lamps are fully lit

(b) Identification when four lamps are turning off

(c) Identification in the dark

FIGURE 9. Images under three different lighting conditions.

A. FACIAL RECOGNITION

Features were extracted from 200 sample photos in the database. Single and multiple people were identified and tested under three different intensities of illumination. The experimental results are shown in Figures 7-10. [33]–[35]

The collection of facial information is the first step in facial recognition. Three separate folders were created to distinguish people's information, as shown in Figures 7(a)∼(c). The individuals are Mei Hao-wen, He Ji-chao and Peng Fan-Fan. These form part of the facial information database, each of which has 200 sample photos.

Figure 8 shows facial recognition for only one person. If the person's face is in the database, the person's information is displayed, as shown in Fig 8 (a)., which shows the original image. Fig (b) shows the grayscale image of the original image. Figure (c) shows the original image binarization, Figure (d) shows the drawing histogram, Figure (e) shows the captured face and Figure (f) shows the detection. The face of in Figure (g) shows the face in the facial database

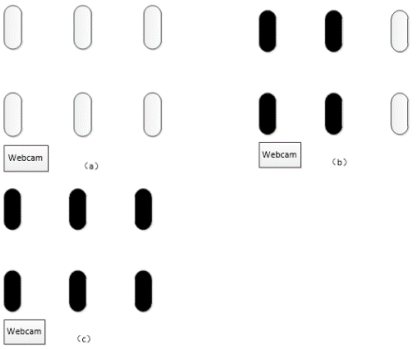
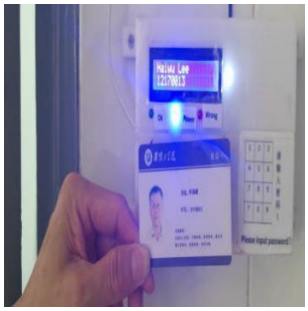


FIGURE 10. Three different lighting scenarios.

(a) LCD displays date and time before

(b) LCD displays "bingo"



(c) LCD displays name and student's ID

(d) LCD displays "wrong"

FIGURE 11. Single authentication card and no authentication card.

and a comparison of Figure (f) and Figure (g) is shown in Figure (h), which is the recognized facial information.

Figure 9 (a) shows facial recognition when the light is fully lit. Five faces are successfully recognized. Three of the faces are displayed with the character information and two unincorporated displays are seen. Figure (b) shows the facial recognition result with four lights turned off. Five faces are successfully recognized. Three are displayed in the library and the other two are not displayed, so are "unknown". Figure (c) shows the result for facial recognition in the dark, with a facial recognition error multiple times. The experimental results show that the effect on recognition is almost zero under normal lighting conditions, and a small number of faces are affected under extreme conditions.

(a) LCD displays "bingo"

(b) LCD displays name and student's number of first card

(c) LCD displays name and student's number of first card

(d) LCD displays name and student's number of second card

(e) LCD displays "wrong"

FIGURE 12. Multiple authentication cards and non-authentication cards.

Figure 10 (a) shows the result when six lamps are fully lit. Figure (b) shows the result when the four lamps are turned off and (c) shows the result for a dark environment.

B. INTELLIGENCE RFID

Single and multiple authentication cards, non-authentication cards and password input were tested. The experimental results are shown in Figures 11-14.

Figures 11 (a)∼(d) show that before swiping the card, the LCD displays the current date and time. When the authentication card enters the reading range of the card reader, the green LED lights and the LCD displays "bingo" and the user's name and number. It then waits for the second step of authentication and when this is achieved, the door is opened. When the unauthenticated card enters the reading range of the card reader, the red LED lights illuminate, the buzzer warns, the LCD displays wrong and the door is not opened.

(a) Correct password input: LCD displays "bingo"

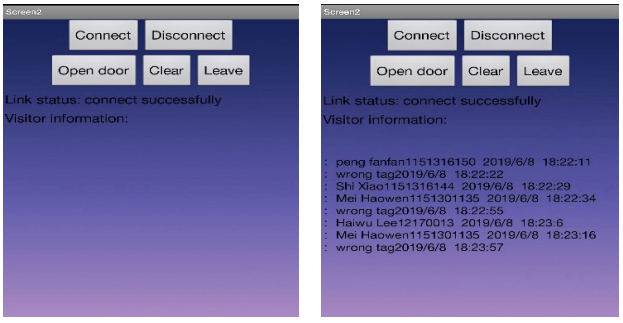
(b) Password input error: LCD displays "wrong"

(c) Mistakes more than three times: wait for 30 seconds

(d) Wait for 30 seconds

(e) After 30 seconds

FIGURE 13. Password input.



(a) APP operational page

(b) Attendance Record

FIGURE 14. APP.

Figures 12 (a)∼(e), show that when multiple authentication and non-authentication cards enter the reading range of the Reader, the Reader reads the card numbers of multiple cards. If the card is authenticated, the green LED lights, the LCD display bingo and lay the user's name and student number is displayed. The system then waits for the second step authentication and when this is achieved, the door is opened. If the card is a non-authentication card, the red LED lights, the buzzer sounds and the door does not open.

Figures 13 (a)∼(e) show that when the password input is correct, the green LED lights and the LCD shows "bingo". The system then waits for the second step authentication and when this is achieved, the door is opened. When the password input is wrong, the red LED lights illuminate, the buzzer sounds, the LCD shows "wrong" and when there are more than three password input errors times, the user must wait 30 seconds to input again.

Figures 14 (a) and (b) show that the mobile APP has five operation buttons:

(a) "Connect" button: the Bluetooth module is connected to the system and user attendance records are received.
(b) "Disconnect" button: disconnects the Bluetooth connection.
(c) "Open door" button: opens the door.
(d) "Clear" button: clears the screen.
(e) "Leave" button: allows the user to exit the APP.

VII. CONCLUSION

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. Facial recognition is 98.9% accurate on Raspberry PI 3B+. When multiple Tags collide, the search times for the dynamic binary tree anti-collision algorithm decrease by 13.3%. 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. ISKO-Maghreb, 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.

[7] 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.
[8] 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.
[9] 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.
[10] 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.
[11] 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.
[12] 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.
[13] 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.
[14] 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.
[15] 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.
[16] 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. 2015, pp. 537–540.
[17] W. W. W. Zou and P. C. Yuen, "Very low resolution face recognition problem," *IEEE Trans. Image Process.*, vol. 21, no. 1, pp. 327–340, Jan. 2012.
[18] A. Wagner, J. Wright, A. Ganesh, Z. Zhou, H. Mobahi, and Y. Ma, "Toward a practical face recognition system: Robust alignment and illumination by sparse representation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 34, no. 2, pp. 372–386, Feb. 2012.
[19] W. Chen and Y. Gao, "Face recognition using ensemble string matching," *IEEE Trans. Image Process.*, vol. 22, no. 12, pp. 4798–4808, Dec. 2013.
[20] N. R. Borkar and S. Kuwelkar, "Real-time implementation of face recognition system," in *Proc. Int. Conf. Comput. Methodologies Commun. (ICCMC)*, Jul. 2017, pp. 249–255.
[21] A. A. Aburomman and M. Bin Ibne Reaz, "Ensemble of binary SVM classifiers based on PCA and LDA feature extraction for intrusion detection," in *Proc. IEEE Adv. Inf. Manage., Communicates, Electron. Autom. Control Conf. (IMCEC)*, Oct. 2016, pp. 636–640.
[22] C. Shao, T. Kim, J. Yu, J. Choi, and W. Lee, "ProTaR: Probabilistic tag retardation for missing tag identification in large-scale RFID systems," *IEEE Trans. Ind. Informat.*, vol. 11, no. 2, pp. 513–522, Apr. 2015.
[23] D. Zhang, X. Wang, X. Song, and D. Zhao, "A novel approach to mapped correlation of ID for RFID anti-collision," *IEEE Trans. Services Comput.*, vol. 7, no. 4, pp. 741–748, Oct. 2014.
[24] M. A. Bonuccelli, F. Lonetti, and F. Martelli, "Exploiting id knowledge for tag identification in rfid networks," in *Proc. 4th ACM Workshop Perform. Eval. Wireless Ad Hoc, Sensor, Ubiquitous Netw. (PE-WASUN)*, 2007, pp. 70–77.
[25] S. Charoenpanyasak, Y. Sasiwat, W. Suntiamorntut, and S. Tontisirin, "Comparative analysis of RFID anti-collision algorithms in IoT applications," in *Proc. Int. Symp. Intell. Signal Process. Commun. Syst. (ISPACS)*, Oct. 2016, pp. 1–5.
[26] X. Chen, G. Liu, Y. Yao, Y. Chen, S. Miao, and Y. Su, "IRBST: An improved RFID anti-collision algorithm based on regressive-style binary search tree," in *Proc. Int. Forum Inf. Technol. Appl.*, Jul. 2010, pp. 403–406.
[27] B. Zhu, J. Wang, and G. Zeng, "A non-integral-Q algorithm for RFID system in anti-collision," in *Proc. 2nd Int. Conf. Control, Autom. Robot. (ICCAR)*, Apr. 2016, pp. 374–377.
[28] A. S. Georghiades, P. N. Belhumeur, and D. J. Kriegman, "From few to many: Illumination cone models for face recognition under variable lighting and pose," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 23, no. 6, pp. 643–660, Jun. 2001, doi: 10.1109/34.927464.
[29] K.-C. Lee, J. Ho, and D. J. Kriegman, "Acquiring linear subspaces for face recognition under variable lighting," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 27, no. 5, pp. 684–698, May 2005, doi: 10.1109/TPAMI.2005.92.
[30] C. R. Gonzalez and R. E. Woods, *Digital Image Procesing 3/E*. London, U.K.: Pearson, 2008.
[31] H. Farsi and R. Saleh, "Implementation and optimization of a speech recognition system based on hidden Markov model using genetic algorithm," in *Proc. Iranian Conf. Intell. Syst. (ICIS)*, Feb. 2014, pp. 1–5.
[32] A. Levitin, *Introduction to the Design and Analysis of Algorithms 2/E*. London, U.K.: Pearson, 2007.
[33] H. W. Lee and C. L. Hwang, "A study of skin color detection using a merging technique," *J. Chin. Inst. Eng.*, vol. 38, no. 3, pp. 406–414, Apr. 2015.
[34] H.-W. Lee, W.-T. Gu, and Y.-Y. Wang, "Design of face recognition attendance," in *Proc. IEEE 5th Int. Conf. Image, Vis. Comput. (ICIVC)*, Jul. 2020, pp. 222–226.
[35] H.-W. Lee and J.-X. Wang, "Internet of Things combined with identity design," in *Proc. IEEE Int. Conf. Consum. Electron. Taiwan (ICCE-Taiwan)*, Sep. 2020, pp. 1–2.

HAI-WU LEE (Member, IEEE) received the degree from the Department of Electronic Engineering, Kun Shan University, in 2000, the master's degree from the Institute of Computers, Communications, and Control, National Taipei University of Technology, in 2003, and the Ph.D. degree from the Department of Electrical Engineering, National Taiwan University of Science and Technology, Taipei, Taiwan, in 2014. He is currently a Professor with the Department of School of Science and Engineering, Xiangsihu College of Guangxi University for Nationalities. His research interests include the design and application of optimal control systems for biped walking robots, image processing, and intelligence RFID. He is a Reviewer of journals, such as IEEE TRANSACTIONS ON EDUCATION and IEEE ACCESS.