BIOMETRIC ACCESS SYSTEM USING FACIAL RECOGNITION

*** Ifeoma B. Asianuba** **Ayegba Sunday**

*ifeomaasianuba@gmail.com

Department of Electrical/Electronic Engineering University of Port Harcourt Choba Rivers State Nigeria.

Abstract

In most developing countries, security of lives and properties is increasingly threatened on daily basis. Traditional security system requires the use of a key, a security password, an RFID card, or ID card which probably can be forgotten and lead to access denial. However, these security items can also be stolen by unauthorized persons. As a result, there is a need to look into aspects that can guarantee a higher security level for access in area of restrictions. The human face is an indisputable identifier which cannot be borrowed, lost stolen or left out. Every individual is characterized with his own unique features which when implemented will validate the identity of an individual. This is achieved by deploying biological data and matching algorithm for identification and authentication. In this paper, the human face is used to implement a security platform to grant access by quantifying the features and match them against stored templates in a database. This choice is necessitated by the unique presentations of the basic features of the human face. This system is a cost effective and a reliable approach for securing items and facilities. In other words, the human face can be said to be a secured password.

Keywords; Microcontroller, raspberry pi camera, Pattern matching.

I INTRODUCTION

Face is the most important part of our body, in that it can reflect different emotions of an individual. The use of non-living things

like (smart cards, plastic cards, Pins, tokens, keys) for authentication and access in restricted areas are still in use today. There are two types of biometric system each with its unique characteristics; physiological characteristics (face, fingerprint, finger geometry, hand geometry, palm, iris, ear contours and voice). The second is behavioral characteristics which include (gait, signature and keystroke dynamics etc). Sometimes behavioral traits may changes due to illness, fear, hunger etc. this changes serves as a limitation to this approach. Face detection and recognition system is cheap, simple, accurate and non-intrusive process as compared to other biometric system for authentication. This system has two categories as face detection and face recognition.

Face recognition is an important application of Image processing owing to its use in many fields. A facial recognition system is a computer application capable of identifying or verifying a person from a digital image or a video frame from a video source. One of the ways of achieving this is by comparing selected facial features from the image and facial features on a database system. It is typically used in security systems and can be compared to other biometrics such as fingerprint recognition systems. Some facial recognition algorithms identify facial features by extracting landmarks, or features, from an image of the subject's face. For example, an algorithm may analyze the relative position, size, and/or shape of the eyes, nose, cheekbones, and jaw. These features are then used to search for other images with matching features (Rutva Safi 2019).

II REVIEW OF RELATED WORKS

Most algorithms deployed for facial recognition systems collates a number of images of the required human face, extracts the necessary information from the facial data and saves it in the provided memory space. A probe image is then compared with the face data. One of the earliest successful systems is based on template matching techniques applied to a set of salient facial features, providing a sort of compressed face representation. Recognition algorithms can be divided into two main approaches; geometric approach, which looks at distinguishing features, or photometric approach, which is a statistical approach that

distills an image into values and compares the values with templates to eliminate variances.

Zanuy et al, 2004, proposed a PC-based system as a more suitable approach for testing the device, and can be easily transferred to a low-cost ARM core PC. This Low-cost finger print scanners are designed to lock the computer screen and avoid passwords.

Choi et al, 2005, proposed a new algorithm for an acoustic intruder detection system for home security. This algorithm estimates the variation of features in the room acoustic transfer function to detect intruders. The system ranges from the personalized security systems of a home to large-scale systems for the protection of crucial national installations.

Zuo et al, 2005, proposed real-time embedded face recognition system for consumer applications which enables a personalized service by automatic identification of users. This system is embedded into a smart home environment for user identification.

Zhao et al, 2006 proposed a new method which is based on singular value decomposition (SVD) updating algorithm, this is an SVD updating-based IPCA (SVDU-IPCA) algorithm. Using this algorithm, the approximation error is mathematically proved to be bounded.

The wireless sensor network can be achieved using the ZigBee module and ZigBee tags. These are used to identify the access objects. By using the digital consumer device, digital door lock module can be implemented to control both the access and lock system.

Zhao et al, 2008, proposed a low cost GSM/GPRS based wireless home security system which includes two modules namely sensor nodes for wireless security and a GSM/GPRS gateway. Using a wireless transceiver module the data transfer between gateway and sensor nodes can be established.

Liting et al, 2009, described an effective, efficient face live detection method which uses physiological motion detected by estimating the eye blinks from a captured video sequence and an eye contour extraction algorithm. This technique uses the

conventional active shape model with a random forest classifier trained to recognize the local appearance around each landmark.

In Ibrahim et al, 2009, the work focused on the study and development of an automated face recognition system with the potential application for office door access control. This technique of Eigen face is based on the principle component analysis (PCA) and artificial neural networks. Three main factors of face recognition are considered namely illumination, distance and subject's head orientation on the developed system that is purposely built for office door access control.

Kim et al, 2010 proposed an enhanced multimodal personal authentication system for mobile device security which integrates the modalities like voice, face and teeth using the various fusion techniques such as the weighted summation rule, K-NN, Fisher and Gaussian classifiers, and by which the authentication performance of the system is evaluated.

Kramberger et al, 2011 proposed the architecture of a door phone embedded system with interactive voice response. The main advantage of this system is even in noisy environment the effectiveness of speech recognition is increased using embedded microphone array. The system uses two different platforms namely user identification and verification platform based on a VoIP door phone embedded system and server-based speaker authentication system.

Wencheng et al, 2019 reviewed a system that allows the use of accurate and secured finger print based biometric access system. A Face Recognition System based on Eigen face method in which Eigen method for face recognition and Euclidean distance method to compare the image of the person concerned with the images in the database can also be implemented. It proved to be efficient, fast and also with high accuracy.

Anjali et al 2017, described an automatic system with secure locking utilizing IOT application for home security.

Raghu et al 2013, designed a locker opening and closing system using RFID, fingerprint, password and GSM authentication, the system scans for the unique identification number of the user, fingerprint and password.

Anubala et al 2014, designed an intelligent door lock system. The device used a fingerprint sensor as the security system, the fingerprint of the user is stored in the system. When a person wants to access the system, the fingerprint sensor checks for the user fingerprints, if it is stored in the system, the door will be open automatically.

Umar F *et al*, 2014, designed a RFID security access door control system. The system combines RFID technology and biometrics to accomplish the required task. When the RFID installed at the entrance of the hostel detects a number, the system captures the user image and scans the database for a match. If both the card and capture belong to a registered user, access is granted; otherwise the system turns on the alarm and makes an emergency call to the security van through the GSM modem.

Senthilkumar et.al, 2014, proposed a work on Embedded Image Capturing System Using Raspberry Pi. In the work, an image was captured and compared with that on the database for authentication. The limitation was includes the fact that the system couldn't work properly in an ambient light condition. Automated Door Access System with Face Design and Recognition can be implemented for face detection using PCA (Principal Component Analysis) for the comparison of images. The limitation of this approach lies on the fact that it is not a robust and efficient approach.

Januzaj. et al, 2015, proposed real time access control for face recognition using Raspberry pi instead of GSM services and relay. The limitation of the work was that it couldn't control the background light situation and ambient light conditions for an efficient authentication process.

Lwin.et al, 2015, proposed a door lock access system which consists of three subsystems which include face recognition, face detection, and automated door access control. Face recognition is actualized by using the PCA (Principal Component Analysis). Access is granted to the authorized person based on command from the microcontroller. Demerit of this system requires images to be taken through a web camera continuously until the 'stop camera' button is activated. Personal computer (PC) is usually

associated with the microcontroller, in order words; the entire system will be ineffective if the PC crashes or is non-functional.

Kartik et al, 2015, proposed two systems, one is based on GSM technology and other uses a web camera to detect the intruder.

The organization of this paper is as follows. In section II, the integrated architecture of the proposed system is elaborated

III METHODOLOGY

The block diagram for the signal flow of the biometric access system using raspberry pi facial recognition system is shown in fig. 1 below. The circuit is divided into four sections; each section performs a specific task.

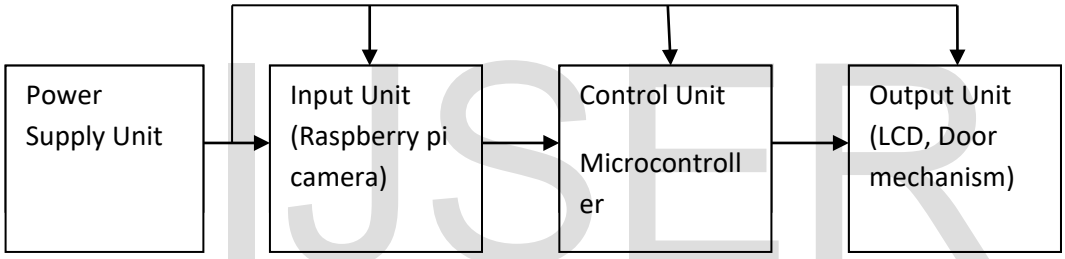


Figure 1: Block Diagram of the Raspberry Pi Facial

The input unit is made of the raspberry pi camera. The module requires 5 dc volt for its operation. The control unit is made of the Raspberry pi controller with operating voltage of 5 volt dc. The output unit is made up of the relays, the motor, gear system and the sliding door. The relay uses 5 volt dc to operate. The motor and gear system requires 12 volt dc to operate.

The input unit is made up of the raspberry pi camera that captures the human face and sends the data to the microcontroller. The raspberry pi camera board plugs directly into the raspberry pi. It is able to deliver a crystal clear 5mp resolution image to the raspberry pi.

The control unit is the raspberry pi 3 module controller that is use to receive the image of the user and scans if the image is stored in the system, if it is already stored it allow access to the

building, if not it alerts the user to stare at the camera again for facial input to be taken. The system uses an open CV library for the processing of the image of the individual. The open CV library makes use of the principal component analysis (PCA) algorithm.

The controller sends a signal to the output unit, when a face is recognize. The output unit is made up of transistor relay driver, which controls the closing and opening of the door by forward/ reverse biasing of the relays as the need be.

The user is able to communicate with the device via the use of a liquid crystal display which the microcontroller sends data to, for the user to visualize and communicate with the system. The liquid crystal display is connected to the analogue pins (pin 22 to pin 28) of the microcontroller. The liquid crystal displays information to the user to place face on the camera. it also displays the indication “door open” or “door closed” for the user.

The door system is controlled by the microcontroller via the two relays used in the system. The relays are connected to the uln2004 (transistor array chip) IC (U3), which is used to switch on and off the relay. The IC is used in the circuit, due to the current gain of the array of transistor used in the internal architecture of the IC. The IC (U3) turn the relay when a 5 volt is sent to it by the microcontroller and turns off when a 0 volt is sent to it by the microcontroller.

The microcontroller is programmed using python language. The system worked based on the algorithm and program used to drive the control unit using python language program and the PCA algorithm. Principle Component Analysis (PCA) is an Eigen face recognition algorithm which uses feature vectors extracted from a frontal view of the face. The user face is inputted into the system via a camera, the PCA algorithm extracts the Eigen faces, Eigen vectors and mean from the image by performing a mathematical process on a set of trained images depicting different human faces.
The image training process is defined as a set of flattened vectors and these vectors are assembled together into a single matrix. The extracted Eigen vectors of the matrix are stored in a database. Eigen vectors are defined by the face spaces which are the training face images that are projected.

This results in the variation between the set of faces without emphasis on any one facial region like the eyes or nose.

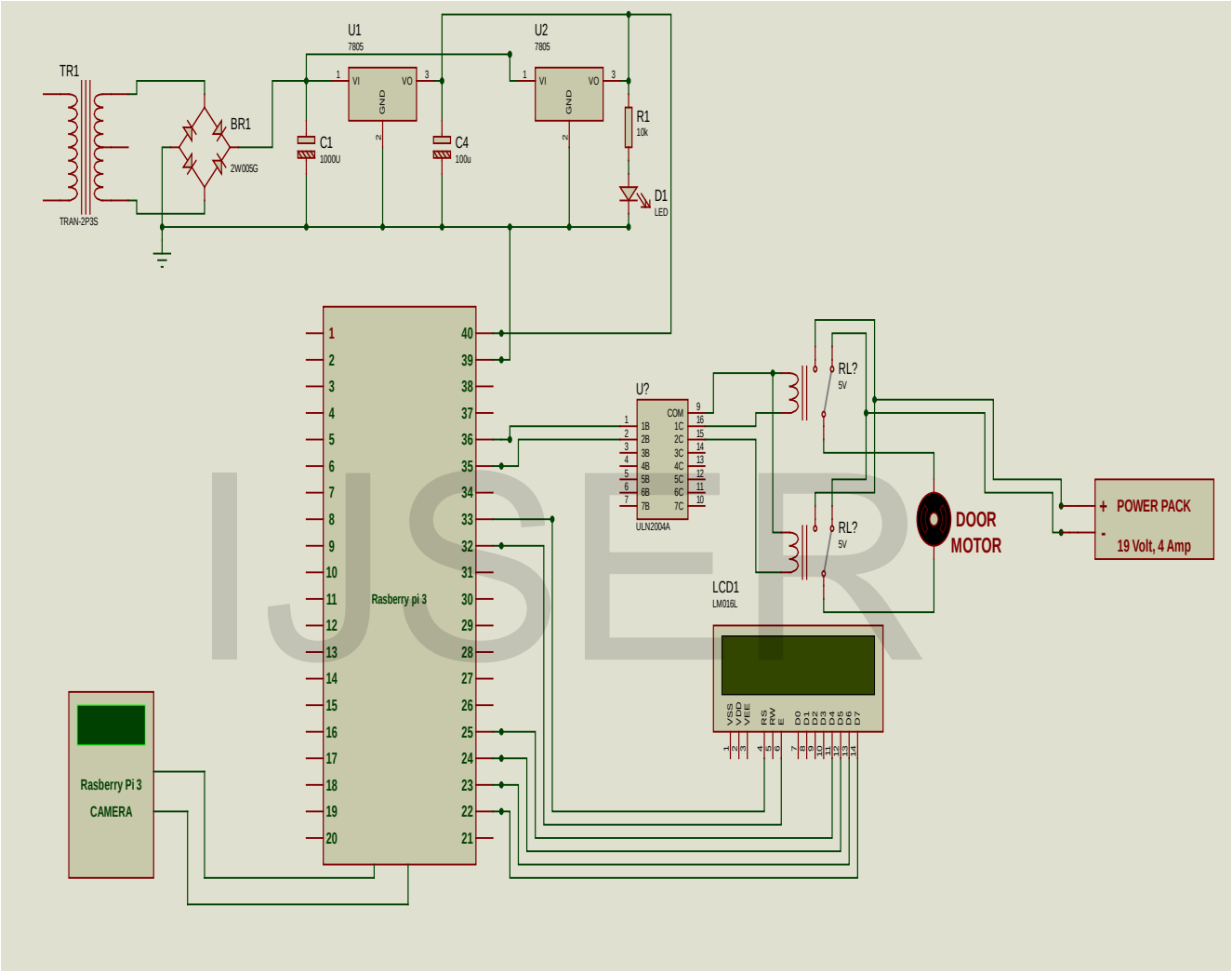
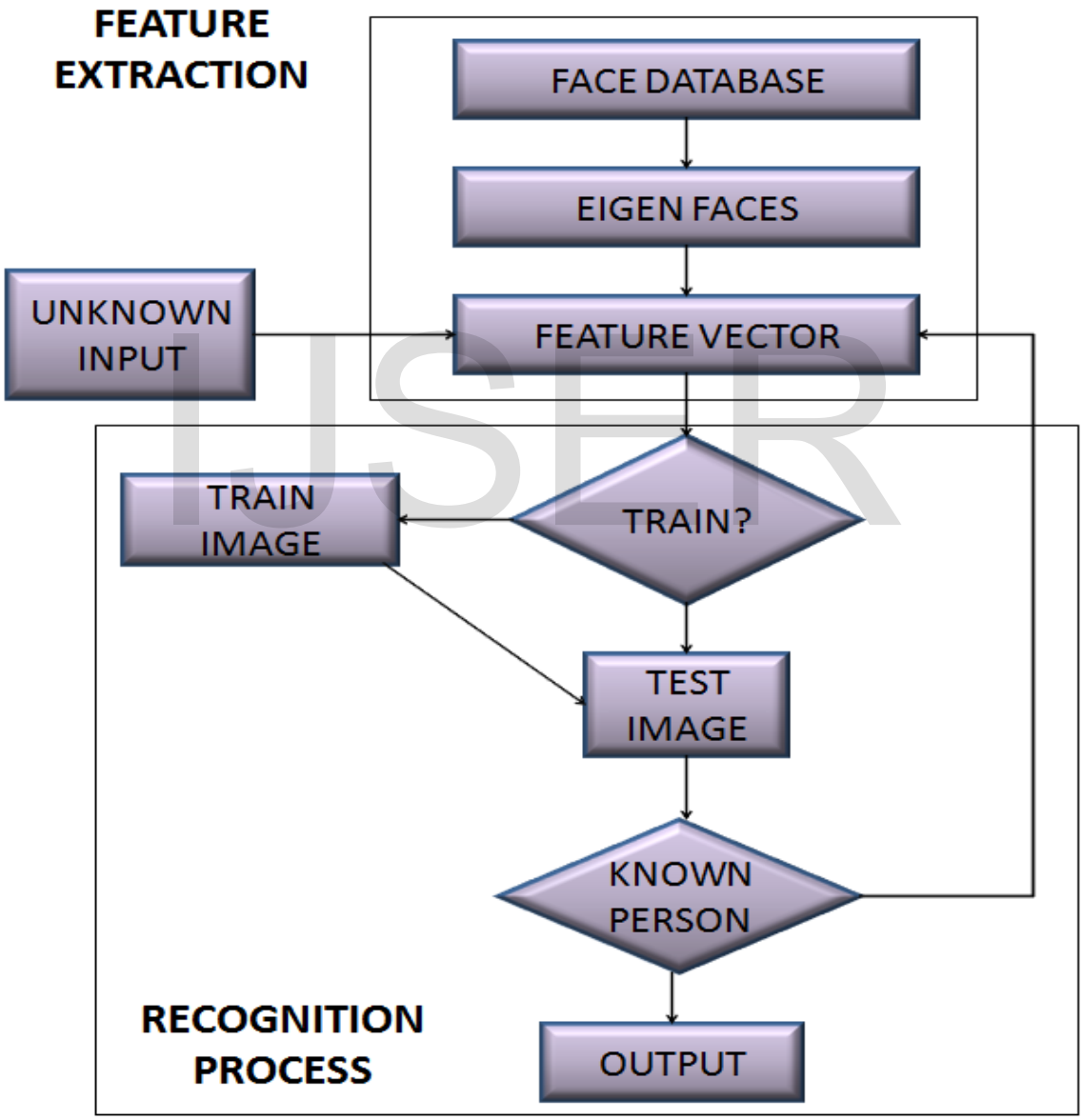


Figure 3.2: Circuit Diagram Biometric Access System Using Facial Recognition

The algorithm involves the training of the system to understand the pattern of the user face by taking pictures of the user and creating vectors for each image taken, the several vectors gotten from the images used in training the system are assembled together to form a single matrix that will be stored in the system memory (database).

Flowchart of the System



IV ANALYSIS OF RESULT

The following detail is obtained from the individuals whose information will be stored in the data base of the microcontroller;

1 The distance between the two eyes

2 The lateral distance from the eyes to the ears.

3 The slant distances from the two eyes to the tip of the nose.

4 The vertical distance between the nose and the mouth.

5 The slant distance between the ears and the chin.

The information listed above is saved in the memory of the microcontroller. More data from the face can be determined and included in the data base of the system. The more the parameters to be matched for authenticity the better and accurate is the device. The face is placed before the camera to take a snap shot in the presence of large intensity of light. The information is converted into binary data which is implored for comparison to grant access through the door. The information is saved for as many individual whose data needs to be imputed into the microcontroller.

The motor turns in a clockwise direction to open the door once the information from the face through the camera matches the pattern in the data base. This is achieved by allowing current to passive through to drive the relay which activates the motor to turn the door open and grant access. The LCD is an output unit which describes the state of the system. It displays “user face been scanned” once the system is undergoing pattern matching. It also will display “door open” once access is granted.

Table 1; TABLE OF RESULT

Facial ID store location/Process	**CONTROL FUNCTION**
REGISTER	The user registers his or her face in the database of the system.
DELETE	This process is used to delete the user face, when necessary
ENTER	This is used to cross-check the system if the information on the user's face is stored in the system
Facial Match Found	Door opens
Facial Match not found	Door not open

V CONCLUSION

Facial recognition system is an efficient approach which should be deployed in areas where authentication cannot be manipulated. Implementing this device require the use of an algorithm which trains the system to understand the pattern of the key features of the human face to guarantee access to designated areas. This feature is peculiar to every individual. This makes the use of this technique a guarantee for security check.

REFERENCES

Anjali Patel and Ashok Verma. IOT based facial recognition security system. *International journal of computer Applications volume 172 Issue* 4 August 2017.

Anubala B., Rahini M., and Bavithra T. Intelligent Door Locking System, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 *International Conference on Humming Bird. 2*014.

Choi, K.-M.Kim, J.-W.Jung, S.-Y.Chun, and K.-S.Park, "*Acoustic intruder detection system for home security," IEEE Transaction on Consumer Electron.,* volume 51, no. 1, pp: 130-138, Feb. 2005.

Hwang Jim Ha, Yvette E. Gelogo and Haeng- Kon kim. Internet of things (IOT) frame work for U-health care system. *International Journal of Smart home, Volume 9,* issue 11, 2015 pg 323-330.

Januzaj Yiber, Artan Luma, Yimer Januzaj and Vehbi Ramaj, Real time access control based on face recognition. 2015 *international conference on Network Security & Computer Science (ICNSCS) June 10-11 2015 Antalya (Turkey).*

Karthik Nandakumar, Aril K Jain and Arun Ross. 50 years of Biometric Research: *Accomplishment, Challenges and Opportunities,* Pattern recognition Letters 2016.

Kim Dong-Ju, Kwang-Woo Chung, and Kwang-Seok (2010).Hong, "*Person Authentication using Face, Teeth and Voice Modalities for Mobile Device Security*", IEEE Trans. Consumer Electron., vol. 56, no. 4, pp. 2678-2685.

Lwin Hteik Htar, Aung Soe Khang and Hiia Myo Tun. Automatic Door Access system using Face Recognition. *International Journal of Scientific & technology Research, Volume 4 issue 8 June 2015*. ISSN 2277-8616 pp 294-299.

Raghu Ram Gangi1, Subhramanya and Sarma Gollapudi. Locker opening and closing system using RFID, fingerprint, password and GSM. *International Journal of Emerging Trends & Technology in Computer Science(IJETTCS) Web Site:* www.ijettcs.org, Volume 2, Issue 2, 2013.

Rutva Safi (2009). Facial Recognition Systems- *The new future of Biometrics Identification*. Retrieved from https//apiumhub.com/tech-blog Barcelona/facial recognition-biometrics-identification/

Senthil Kumar M. and Gayathri R. Robert Palm Vein Recognition System using LMKNCN classification. *International journal of Engineering Research and Applications,* Volume 4 issue 1 January 2014 pp221-226 ISSN 2248-9622.

Umar Farooq, MahmoodulHasan, Muhammad Amar, AtharHanif, and Muhammad Usman Asad. RFID Based Security and Access Control System. IACSIT *International Journal of Engineering and Technology, Volume 6, No. 4, 2014,*

Wencheng Yang, Song Wang, Jiakan Hu, Guag Lou Zheng and Craig Valli. Security and Accuracy of finger print-Based Biometrics: A Review. *Symmetry 2019,* volume 11, doi:103390/Sym 11020141 pp 1-19.

Zhao Haitao, Pong Chi Yuen, and James T. Kwok, (2006) *"A Novel Incremental Principal Component Analysis and Its Application for Face Recognition"*, IEEE Transactions On Systems, Man, And Cybernetics—Part B: Cybernetics, Vol. 36, No. 4, pp. 873-886.

Zuo, and P. H. N. de With, (2005). *"Real-time embedded face recognition for smart home"*, IEEE Transaction on Consumer Electron, volume 51, no. 1, pp 183-190.