International Journal of Applied Science and Mathematics
Volume 2, Issue 6, ISSN (Online): 2394-2894

Design of Face Recognised Access Control to Secret Facilities in Organisations

Folake Akinbohun
Computer Science Department,
Rufus Giwa Polytechnic, Owo,
Ondo State, Nigeria
Email: folakeakinbohun@yahoo.com

O. T. Jinadu
Computer Science Department,
Rufus Giwa Polytechnic, Owo,
Ondo State, Nigeria
Email: yimikajinad@gmail.com

E. O. Aliyu
Computer Science Department,
Adekunle Ajasin University,
Akungba-Akoko, Ondo State, Nigeria
Email: aliyuolubunmi@gmail.com

Abstract **– Security as one basic need of mankind requires the protection of our lives, assets and businesses. Organizations keep valuables such as in which money, goods and facilities including electronic applications in secret places and if unauthorized users have access to the secret place, such valuables may be taken with resultant great loss of reputation.**

The major breakthrough to counter company's insecurity is the emerging field of biometrics which allows verification of true individual identity based on a face recognition system, rule-based and signal processing that generates the door-opening signal of a secret room if an authorized employee is recognized.

This paper is a security solution that can be adapted for various market needs, such as offices, banks, insurance companies, hospitals, refineries and airports.

Keywords **– Access Control, Biometric System, Face Recognition, Rule-Based.**

I. INTRODUCTION

With the high rate of insecurity in the organizations today, the need for proper protection of company's property cannot be over-emphasised. Recently, waves of theft are beginning to spread with various organizations both private and public; hence a proper security approach needs to be adopted by these organizations.

Equipment, materials, money and goods etc are not exposed to every employee working in these organizations/companies. The organizations need to have a secret facility or strong room where all available items and materials etc can be kept for use and access to the secret facility be controlled. The use of such secret facility could be used to drive anti-insurgence devices if deployed.

Access controls are tools and controls used for identification, authentication, authorization and accountability in organisations. Access control in this context is often needed for access into organizations valuable buildings and banks etc that have a "physical access," which refers to interactions (such as a lock and key) in the physical environment, where equipment, money and goods are stored. It is good to allow authorized persons to have access to secret facilities of the organization with ease while keeping unauthorized persons out[11]

There is a wide range of biometric security devices and software available for different levels of security needs. There are very large complex biometric systems for organisations that require absolute airtight security. Biometric security using face recognition is a far better approach which uses human facial recognition software and digital video cameras to authenticate a person's identity[13]. A person wishing to gain access to the organisation would have his face scanned by the camera. The software in the computer then analyzes the placement of various features of the face, such as the eyes, nose, and mouth as well as the shape of such features. Face recognition software has also been employed by some governments who are looking for suspected thieves. Facial recognition allows some employees who have attained higher level to have access to organisation's facility in order to avoid loss of material and equipment.

Biometric is an automated method of identity verification or identification based on the principle of measurable physiological or behavioural characteristics such as finger-print, iris pattern, facial characteristics[10]

II. OBJECTIVE OF THE PAPER

The objective of the paper is to design a model for access control of a secret facility.

III. LITERATURE SURVEY

Face recognition is an active research area with a wide range of applications in the real world. In the recent years, a defined face recognition pipeline, consisting of four steps i.e. detection, alignment, representation, and classification has been presented. In the detection step, the place of the image including face is found. The alignment step ensures the detected face is lined up with a target face or a model. In the representation step the detected face is described in a way that several descriptions with certain aspects about the detected face are presented. Finally, the classification step determines whether a certain feature corresponds with a target face or a model.

In the face recognition, the feature representation of a face is a critical aspect. If representation step does not perform well, even the best classifiers cannot produce appropriate results. Good representations are those that on one hand minimize intra-person dissimilarities, on the other hand maximize differences between persons. Additionally, a significant representation should be fast and compact [5]. There are several views related to the classification of the feature extraction methods. One possible classification divides the feature extraction methods into Holistic Methods and Local Feature-based Methods.

Face recognition techniques are based on Geometric and Photometric approaches: Geometric approach considers individual features such as eyes, nose, mouth and shape of the head for developing a face model based on the size and the position of these characteristics while photometric approach uses statistical values that are extracted and subsequently, compared with the related templates[3].

A face recognition technique focuses on detecting important facial features such as the eye corners, nose tips, mouth corners and chin edge were implemented. Relative distances between facial features could be measured and a feature vector constructed to describe each face. These feature vectors could be used in comparing known faces in the database to unknown probe faces.

Rahimeh, Mehran and Behzad [7] pointed out that face recognition systems due to their significant application in the security scopes, have been of great importance in recent years. Trying to design the systems performing under different conditions (e.g. illumination, variation of pose, different expression and etc) is a challenging problem in the feature extraction of the face recognition. As feature extraction is an important step in the face recognition operation. Four techniques of feature extraction in the face recognition were reviewed and compared.

Adebayo, Onifade and Akinmosin [2] worked on combating terrorism with biometric authentication using face recognition. They implemented an authentication system based on face recognition for use at the airport and border points. Some images were trained using face recognition technique and combine it with a feature based technique. From this technique, they extracted some key features. The system then authenticates any immigrant by matching their faces with the faces of the known terrorist in the database.

IV. METHODOLOGY

The design of the new system for implementing the Access Tool Control (ACS) system is developed using a model that actually works with various parts: These parts are summarized as shown in figure 1.

The methodology involves round the eigen representation, Principal Component Analysis, Knowledge-base system and Digital Signal Processing. As described below:

A camera takes the images of the authorized employees' faces who have authentic access to the secret room or strong room of an organization or company. The face-images undergo series of procedures: Face-images, face detection, feature extraction, face recognition and verification or identification [9]. The geometric approach is adopted for feature extraction technique [3]

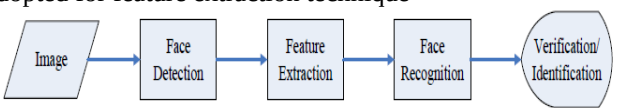

Fig.1. Conceptual Components for Access Control System

- The images are stored in the company database for access of the authorized employees.
- Training of the faces follows the training of the images in the database is performed based on the Principal Component Analysis technique and then eigenfaces are calculated:

Eigenface and Principal Component Analysis

The idea of eigenface is rather easy. Given a face data set (say *N* faces), first scale each face patch into a constant size (for example, 100x100) and transfer each patch into vector representation (100-by-100 matrix into 10000-by-1 vector). Based on these *N* *D*-dimensional vectors (*D*=10000 in this case), then apply the principal component analysis (PCA) [8] to obtain suitable basis (each is a *D*-dimensional vector) for dimension reduction. Assume *M is chosen for* projection basis (M<<D), each *D*-dimensional vector could be transformed into an *M*-dimensional vector representation [1] . Generally, these *M* projection basis are called eigenfaces. The algorithms for Principal Component Analysis (PCA)[4] technique for eigenfaces representation consisted of two steps of initial setting

A. EIGEN REPRESENTATION AND COMPONENT ANALYSIS OF THE FACE IMAGES

The Initial setting is defined as:

N D-dimensional vectors: $\{x\}_i^N = 1 \in R^D$

A set of M projection basis: $\{u_i\}_i^M = 1 \in R^D$

These basis are mutually orthogonal, and generally M<<D

1. The eigenface representation

For each $x_i (i = 1 \sim N)$, compute its projection onto $\{u_i\}_i^M = 1 \in R^D$, and get a new M-dimensional vector yi. This is to achieve dimension reduction.

B. PRINCIPAL COMPONENT ANALYSIS

The Component Analysis developed for the Access Control System (ACS) consists of the following steps implemented within the feature extraction technique:

i. The face images in the database:

$x_1, x_2, x_3, \ldots x_n$, then finding the mean image of the face images stored

Mean image $\varphi = \sum_{n=1}^{m} x_n$ .....(1)

ii. Subtract each face by the mean to obtain face differences

$\emptyset_i = \varphi - x_i$ .....(2)

iii. Determining the covariance matrix ∑of all the $\emptyset_i s$ (faces differences) are calculated

$\sum_{n=1}^{m} \emptyset_i \emptyset_n^T$ .....(3)

iv. Calculating the set of covariance ∑ (D-by (N-1) matrix, where each eigenvector is aligned as a column vector.

v. Preserving the M largest eigenvectors based on their eigenvalues (D-by-M matrix U)

$U^T \emptyset_i$ is the eigenface representation (M-dimensional vector) of the ith face

where,

φ = mean images

$\emptyset_i$ = subtraction of the mean image from each image

∑ = covariance matrix

V. KNOWLEDGE-BASED METHOD

The rule-based method encodes human knowledge of what constitutes a typical face. Usually, the rules capture

the relationships between facial features. The method is designed mainly for face localization, which aims to determine the image position of a single face. The knowledge-based method usually exploits information of the whole image.

Horizontal / vertical projection method adopted use the fairly simple image processing technique, the horizontal and vertical projection[6]. Based on the observations that human eyes and mouths have lower intensity than other parts of faces, these two projections performed on the test image and local minimums were detected as facial feature of employees training set which together constitute a face employee. Each face employee is validated by further detection rules as to test level by level, by scanning through if an employee face is in the database or not. A production rule is expressed as:

IF P_1 & P_2 & … & P_n …THEN Q_1 & Q_2 s… & Q_m

If the premise P_1 through P_n are true then perform actions Q_1 through Q_m where P_i (i= 1, 2, … n) are the condition and Q_j (j = 1, 2, …,m), the conclusions.

IF (employee($x(i)$) = $\emptyset_i$ THEN (employee's access "open").

If employee face is recognized by the system matches the data sets, the output is sent to the Digital Signal Processor.

VI. Digital Signal Processor

When the training of the face-images have been done level by level, generated digital signal is sent from the door of the secret facility/ room in the organization immediately the door handle is laid hold on using the discrete intelligence where the digital signals for the control switch that indicates "on" and "off" for "open" and "lock" respectively.

The discrete signal system transforms the input (faces of the employees) into another signal (the output- "on" indicate "to open for the employee"; "off" indicates "close against the employee") by means of a fixed set of rules or operations [12]

$$y(n) = x^2(n) \quad \text{..... (4)}$$

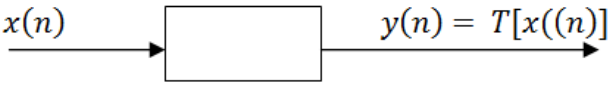

Fig.2. Discrete Signal System

VII. Outcome of Access Control System (ACS)

The line between access control and physical access can be blurred when physical access is controlled by software. Entry to a room is controlled by a chip and the electronic lock is controlled by the software. Only those authorized employee in the database are permitted entry to the room. If the employee meets the eigenweight requirements, entry is permitted.

The moment an authorized employee holds the handle of the door, the camera performs series of procedures of face recognition, checks the database, it then applies rule base of IF…THEN method to test the possibility of employee or non-employee. If the image matches the eigenfaces in the database, then digital signal processing takes place to send signal to the door. The then door opens for the authorized employee to the strong or secret room of the organization. If the image does not match, access is denied to any non-employee recognized as unauthorized user. The activity diagram of ACS is as shown in figure 3.

The employees' images who are recognized by the management of the organization are entered. Compare the faces' images and get the differences by feature extraction and face verification. The recognized faces are stored in the database. IF ….THEN is used to compare the faces. If a face is recognized, then a signal is sent to the control to open for the employee. If not access is denied.

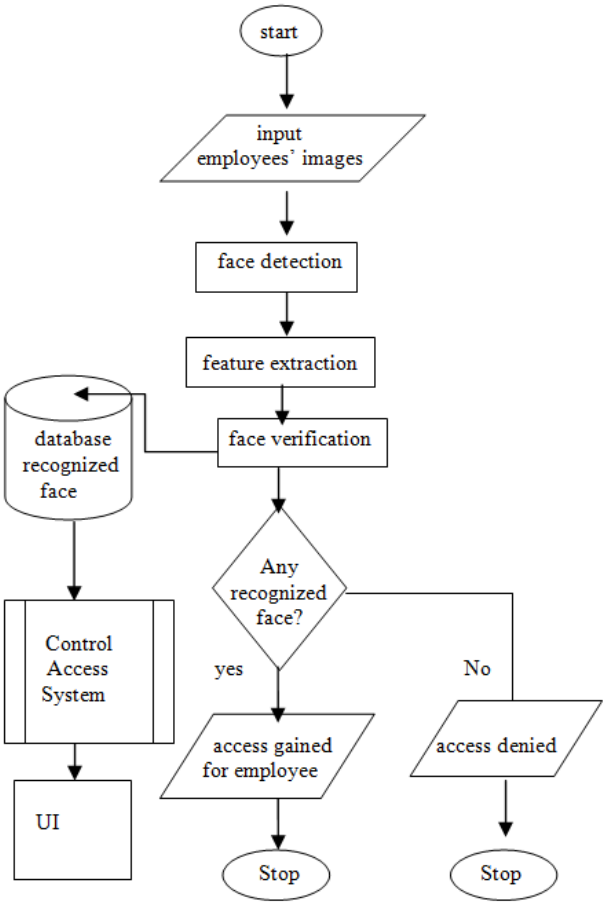

Fig.3. Flowchart for the Control Access System to a Secret Facility

VIII. Conclusion

Face recognition has been one of the most interesting and important biometric field to control access of employees in organizations. This major reason bears the need of automatic recognitions and surveillance systems. The developed system in this paper allows for comprehensive deployment after functional testing of modern external door knobs or handle allowing for keyless entry. It is able to make use of stored images in the database to allow only authorized employees into the sensitive area of such organization where they are installed and maintained.

REFERENCES

[1] A. F. Abate, M. Nappi, D. Riccio and G. Sabatino "2D and 3D Face Recognition: A Survey Pattern Recognition Letter", Vol. 28, no. 14,2007, pp. 1885-1906

[2] K. J. Adebayo, O. W. Onifade, A. S. Akinmosin, S. E. Yusuf and A. M. Dada "Combating Terrorism with Biometric Authentication Using Face Recognition", Nigeria Computer Society, *International Conference Proceedings* Vol. 22., 2011, pp 75-76

[3] R. O. Duda, P. E. Hart and D. G. Stoke. "Pattern Recognition" John Wiley & Sons, 2nd Edition, 2001

[4] T. Hastle, R. Tibshirani and J. Friedman "The Elements of Statistical Learning", Springer 2nd Edition, 2005.

[5] M. Grgic and K. Delac. "Face Recognition Homepage" [Online] Available http://www.facerec-org/general-info [Accessed 2014]

[6] C. Kotropoulos and I. Pitas. "Rule-Based Face Detection in Frontal Views" *Proc International Conference Acoustics, Speech and Signal Processing*, Volume 4, 1997, pp 2537-2540

[7] Rahimeh Rouhi, Mehran Amiri and Behzad Irannejad. "A Review On Feature Extraction Techniques In Face Recognition" Published by Signal & Image Processing : 2012, *An International Journal* (SIPIJ) Vol.3, No.6

[8] M. Turk and A. Pentland. "Eigenfaces for Recognition", *Journal of Cognitive Neurosceince*, 1991, vol. 3, no. 1, pp. 72-86

[9] Wei-Lun Chao (2010): 'Face Recognition" GICE, National Taiwan University

[10] W. Zhao, R. Chellappa, P. J. Phillips and A. Rosenfeld. "Face Recognition: A literature Survey", *Technical Report CAR-TR-948*, Center for Automation Research, University of Maryland, 2002

[11] B. S. Nataliy "Access control and Biometrics" *InfosecCd Conference '04*, USA, 2005, 124 – 127.

[12] H. Monson Hayes. "Digital Signal Processing" 2000

[13] P. P. Alexander & P. Peter Understanding User Perspectives on Biometric Technology. *Communication of the ACM*, 51(9), 2008, 15 – 118.

AUTHOR'S PROFILE

Folake Akinbohun (Mrs.)

bags M.Tech in Computer Science at Federal University of Technology, Akure, Ondo State, Nigeria and currently pursuing her Ph.D. Her field of study is artificial intelligence. She is a lecturer in Computer Science Department at Rufus Giwa Polytechnic, Owo, Ondo State, Nigeria.

Olayinka Jinadu (Mrs.)

has M. Tech in Computer Science and currently pursuing her Ph.D degree in Federal University of Technology, Akure. She specializes in Artificial Intelligence and Computer Architectural Modelling; and her current area of research is on Cognitive Radio Wireless Systems and Software Defined Networking. She is a senior lecturer in Computer Science Department at Rufus Giwa Polytechnic, Owo, Ondo State, Nigeria.

Ednah Olubunmi Aliyu (Mrs.)

possesses M.Tech in Computer Science at Federal University of Technology, Akure, Ondo State, Nigeria and pursuing her Ph.D. Her field of study is software engineering. She is a lecturer in Computer Science Department at Adekunle Ajasin University,Akungba-Akoko, Ondo State, Nigeria.