IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 10, December 2014.
www.ijiset.com
ISSN 2348 – 7968

# Secured Banking operations with face-based Automated Teller Machine

**Olutola Fagbolu[1], Olumide Adewale[2] Boniface Alese[2]and Osuolale Festus[2]**

[1] Department of Computer Science, The Polytechnic Ibadan, Ibadan, Oyo State, Nigeria

[2] Department of Computer Science, Federal University of Technology Akure, Akure, Ondo State, Nigeria

**Abstract**

With the introduction of the newest Automated Teller Machine (ATM) at Royal Bank of Scotland which operates without a card or authentication by entering Personal Identification Number (PIN) to withdraw cash up to £100, a more secured ATM can be designed and implemented with more secured feature of biometrics- facial recognition as PIN. Security is an indispensable issue in banking operations; with the advent of technology such as e-banking, mobile banking etc security has become an issue that needs utmost paramountcy. Principal Component Analysis (PCA) are employed in face recognition system, it seeks to capture the variations in a collection of face images and use them to encode and compare images of individual faces by using statistical dimensionality reduction method to produce the optimal linear squares decomposition of a training set and eigen faces. This research would afford the entire society more reliable ATM model and incidence of fraud which have decline the customer confidence on ATMs would be obliterated.

***Keywords***: *Personal Identification Number (PIN), biometrics, security, eigen faces, fraud.*

## 1. Introduction

Automated Teller Machines (ATMs) are increasingly used in banking operations to dispense cash with additional banking operations from deposits, withdrawals, checking current balance, point of sales of utilities and other services (Fagbolu, 2011). It is the electronic machine often found outside some banks that dispense money whenever personal coded card is inserted which provide more convenient alternatives to traditional dispensers such as bank tellers, automobile drive through facilities etc.

Automated Teller Machines are computerized telecommunication device that provides bank customers method of performing financial transactions in the public places without the need for human clerk or bank teller (an employee of a bank who deals with customers who are often referred to as cashier) (Wikipedia, 2012). ATM is an electronic cash machine that enables customers to withdraw paper money or carry out other banking transaction on insertion of an encoded plastic card (Encarta 2010). ATM often provide one of the best possible official exchange rates for foreign travelers that is if the currency being withdrawn from the ATM is different from that which the bank account is denominated in for example, withdrawing Ghanaian Cedis from a bank account containing Nigeria Naira, the money will be converted at an official wholesale exchange rate.

Crime at ATMs has become a nationwide issue that faces not only customers but bank also and hence need for security measures at banks must play critical contributory role in preventing attacks on customers which brought about the proposition of design of face based ATM. To illustrate the banking industry's understanding of the dangers posed to ATM customers a different approach to its operation and design are proposed in this research work although there are many more safety measures put in place for today's technology of ATM but proposed technology would offer cost effective technology and eradicate security breaches and prevent unnecessary expenditures. ATMs has brought about succour to Nigerian banking environment as long queues in banking halls has began to wane but all forms of security challenges encountered has made it to be an option between the devil and deep blue sea.

Facial recognition system are computer-based security system that are able to automatically detect and identify human faces which began in the late 80s and were introduced to football fans at 2004 Super Bowl (Thanh and Warren, 2006). ATM requires a user to pass an identity test before any transaction can be granted and the current technology uses the smartcard to access and control its operations but with associated problems ranging from duplication, loss, stolen cards and impersonation and these problems can be addressed by using facial recognition system. In the proposed system, access will be authorized by means of human face picture taken by camera. This system will however bring relief to

ISSN 2348 – 7968

prospective ATM users and decline the incidence of fraud; it will extract human face from the rest of the scene which will serve as identity test needed before any transaction would be granted, this system would measures nodal points on the face such as the distance between the eyes, the shape of cheekbones and other distinguishable features. The nodal points are then compared to the nodal points computed from a database of pictures in order to find a match. This paper proposes the use of biometric face-based access control system in ATM with the following advantages. It can be installed anywhere, a camera can be placed at convenient and unnoticeable point, moreover, it would never require the users to touch or interact with any other component before they pass an identity test for transactions to be granted.

It is an intelligent face based access control system that will enable automatic verification of identity by electronic assessment of physiological characteristics of a person. Biometric features have recently gained popularity in personal authentication by utilizing the following: - face, voice, hand shape, fingerprint, iris etc. The use of human face can be well accepted by users for its inherent merits and easy installation, hardware costs are reduced, human face can be captured by conventional cameras etc. The following circumstances would never happen if face based ATM were employed

1. Forgotten passwords that hinder many customers' access to their account and its information.
2. Misplacement of ATM card that often disallow users from withdrawing money cannot happen.
3. Fund withdrawal through card based ATM cannot be as secured as face based ATM which will guarantee only the account owners to their account and its information.

And the following were the drawbacks

1. Chip distortion or magnetic stripe – information stored on card can be distorted by man handling it and overuse which often damages the card and render it useless.
2. The card can be stolen or used by others at the permission of the card owner.

Although face recognition at ATM machines prevents fraud identification and eliminates the usage of personal identification number (PIN) but the design and implementation of face based ATMs have the following demerits.

1. This system can be fooled by put on hats, sunglasses, face masks and beards.
2. If a human face is stored in the database, a disguise or a minor change in appearance or even an unusual facial expression can confuse the system while changes of lighting and camera angle can have a significant effect on the accuracy of 2D systems.

## 2.0 Research Objectives

There are series of difficulties in the realization of face based ATM but because of its inherent advantages to society at large, its objectives are:-

1. Apart from secured banking operations, phishing, withholding of customers' cards, shoulder surfing, stealing and other man made challenges would be appropriately solved.
2. Facial recognition with biometric features provides second level of authentication without chip distortion or withholding of customers' cards.
3. Card fraud, stolen card and all other forms of anomalies can be eradicated.

## 3.0 Face-based Automatic Teller Machine (ATM) Model

### 3.1 Face Recognition Using Principal Component Analysis

An image space can be considered as a space having dimensions equal to the number of pixels making up the image and having values in the range of the pixels values and an image can be thought of as a point in the image space by converting the image to a long vector and by concatenating each column of the image one after the other (Bahtiyar, 1998). When all the face images are converted into vectors, they will be grouped at a certain location in the image space as they have similar structure, having eye, nose and mouth in common and their relative position correlated. This correlation is the main point to start the eigen–face analysis. The eigen–face method tries to find a lower dimensional space for the representation of the face images by eliminating the variance due to non-face images; that is, it tries to focus on the variation coming out of the variance between the face images. So eigen–face method aims to build a face space which describes the faces. The basis vectors of this face space are called the principal component and the eigen–face method is the implementation of PCA over images.

ISSN 2348 – 7968

### 3.2 Eigenfaces for Recognition

By considering information theory, relevant information in a face images are extracted and compare one face encoding with a database of models. Mathematically find the principal components of the distribution of faces, or the eigenvectors of the covariance matrix of the set of face images. A simple approach to extract the information contained in an image of a face is to somehow capture the variation in a collection of face images, independent of any judgment of features, and use this information to encode and compare individual face images. In mathematical terms, eigenface method finds the principal components of the distribution of faces, or the eigenvectors of the covariance matrix of the set of face images, treats an image as point (or vector) in a very high dimensional space. The eigenvectors are ordered, each one accounting for a different amount of the variation among the face images (Turk and Pentland, 1999).These eigenvectors can be thought of as a set of features that characterize the variation between face images. Each image location contributes more or less to each eigenvector. Each eigenface deviates from uniform gray where some facial feature differs among the set of training faces; they are a sort of map of the variations between faces. Each individual face can be represented exactly in terms of a linear combination of the eigenfaces. The number of possible eigenfaces is equal to the number of face images in the training set. However we can also represent the faces by approximating these by the best eigenfaces having largest eigen-values which in turn account for the most variance within the set of face images. This increases the computational efficiency.

The following steps are involved in the recognition process (Turk and Pentland, 1999): (i) initialisation: The training set of face images is acquired and eigenfaces are calculated which define the face space; (ii) when a new face is encountered, a set of weights based on input image and M eigenfaces is calculated by projecting the input image onto each of the eigenfaces; (iii) the image is determined to be face or not by checking if it is sufficiently close to face space; and (iv) if it is a face, the weight patterns are classified as either a known person or an unknown one. See figure 1 below.

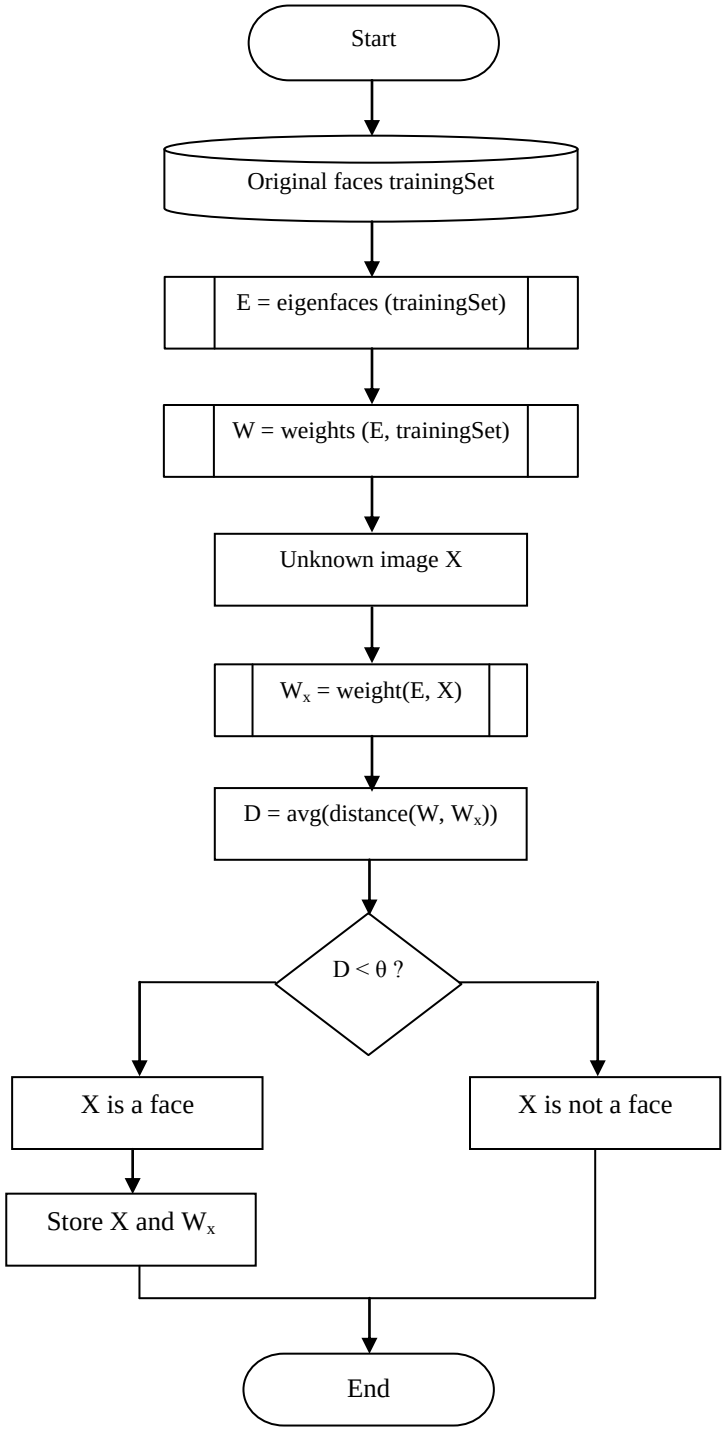


Figure 1: Simple functioning principle of the eigenface-based face recognition algorithm

ISSN 2348 – 7968

### 3.2.1 Calculating Eigenfaces with PCA

Since the images of faces are similar in overall configuration, they are not randomly distributed in the image space and they are described by a relatively low dimensional subspace. The main idea of the PCA is to find the vectors which best account for the distribution of face images within the entire image space.

Mathematically, let the image be denoted by *I*.

**Image** *I*: (*N* x *N*) pixels

(1.1)

Now the image matrix *I* of size (*N* x *N*) pixels is converted to the image vector $\Gamma$ of size (*P* x 1) where *P* = (*N* x *N*); that is the image matrix is reconstructed by adding each column one after the other.

Let the training set be denoted by $\Gamma$

**Training Set**: $\Gamma = [\Gamma_1 \Gamma_2 \ldots \Gamma_M]$

(1.2)

is the training set of image vectors and its size is (*P* x *M* ) where M is the number of the training images.

Now the Mean face is calculated by the equation:

**Mean Face**: $\Psi = \frac{1}{M}\sum_{i=1}^{M}\Gamma_i$

(1.3)

is the arithmetic average of the training image vectors at each pixel point and its size is *P* x *1*.

**Mean Subtracted Image**: $\Phi = \Gamma - \Psi$

(1.4)

is the difference of the training image from the mean image.

**Difference Matrix**: $A = [\Phi_1 \Phi_2 \ldots \Phi_M]$

(1.5)

is the matrix of all the mean subtracted training image vectors and its size is (*P* x *M*).

**Covariance Matrix**: $X = A.A^T = \frac{1}{M}\sum_{i=1}^{M}\varphi_i \varphi_i^T$

(1.6)

is the covariance matrix of the training image vectors of size (*P* x *P*).

An important property of the eigenface method is obtaining the eigenvectors of the covariance matrix. For a face image of size (*N* x *N*) pixels, the covariance matrix is of size (*P* x *P*), *P* being (*N* x *N*).

On the other hand, eigenface method calculates the eigen–vectors of the (*M* x *M*) matrix, *M* being the number of face images, and obtains (*P* x *P*) matrix using the eigenvectors of the (*M* x *M*) matrix.

Initially, a matrix *Y* is defined as,

$$Y = A^T.A = \frac{1}{M}\sum_{i=1}^{M}\Gamma_i\Gamma_i^T$$

(1.7)

which is of size (*M* x *M*) .

Then the eigenvectors $v_i$ and eigen–values $\mu_i$ are obtained thus,

$$Y.v_i = \mu_i .v_i$$

(1.8)

The value of Y is put in this equation,

$$A^T.A.v_i = \mu_i.v_i$$

(1.9)

Now both the sides are multiplied by A on the left side,

$$A.A^T.A.v_i = A.\mu_i.v_i$$

(1.10)

which can be represented as

$$A.A^T.A.v_i = \mu_i.A.v_i$$

(1.11)

$$X.A.v_i = \mu_i.A.v_i \quad \text{from (1.6)}$$

(1.12)

Now let us group $A.v_i$ and call it $\upsilon_i$. It is now easily seen that

$$\upsilon_i = A.v_i$$

(1.13)

ISSN 2348 – 7968

is one of the eigen–vectors of $X = A.A^T$.

Thus, it is possible to obtain the eigen–vectors of X by using the eigen–vectors of Y. A matrix of size (M x M) is utilised instead of a matrix of size (P x P) (that is, [{N x N} x {N x N}]). This formulation brings substantial computational efficiency. Instead of using M of the eigen–faces, M'≤M of the eigen–faces can be used for the eigen–face projection, in the next step, the training images are projected into the eigen–face space and thus the weight of each eigen–vector represent the image in the eigen–face space is calculated.

Projection: $w_k = v_k$

(1.14)

is the projection of a training image on each of the eigenvectors where $k = 1,2, ..., M'$.

Weight Matrix: $\Omega = [w_1\ w_2\ ...\ w_{M'}]$

(1.15)

is the representation of the training image in the eigenface space and its size is *M x 1*. So the images are just composed of weights in the eigen–face space, as they have pixel values in the image space. The important aspect of the eigen–face transform lies in this property. Each image is represented by an image of size (N x N) in the image space, whereas the same image is represented by a vector of size (M′ x 1) in the eigen–face space. Moreover, having the dimension structure related to the variance of the data makes the eigen–face representation a generalised representation of the data.

### 3.3 Classification of test image

For the classification of a new test image, it is mean subtracted first and projected onto the eigen-face space and then Nearest Mean algorithm (Yu et al, 1997), it is used for the classification of the test image vector in the standard eigenface method; that is, the test image is assumed to belong to the nearest class by calculating the Euclidean distance of the test image vector to the mean of each class of the training image vectors.

Test image vector: $\Gamma_T$

(1.16) is the test image vector of size $P \times 1$.

Mean subtracted image: $\Phi = \Gamma_T - \Psi$

(1.17)

is the difference of the test image from the mean image of size *P x 1*.

Projection = $v_k^T.\phi = v_k^T.(\Gamma - \Psi)^T$

(1.18)

is the projection of a training image on each of the eigenvectors where $k = 1,2,3,...\ M'$

Weight Matrix: $\Omega_T = [w_1\ w_2\ ...\ w_{M'}]^T$

(1.19)

is the representation of the test image in the eigenface space and its size is (M′ x 1).

A similarity measure is defined as the Euclidean distance between the test image vector and *i*th face class.

### 4.0 Architecture of a face-based ATM Security System

Face recognition refers to a very broad range of applications including secure access control, crowd surveillance, forensic facial reconstruction and police identification. The face identification problem can be formally posed as follows: given a probe $v_Q$ of an unknown person, determine the identity

identity $I_i$, $i \in \{1, 2,...,N, N+1\}$ where $I_1, I_2,...,I_N$ are the identities enrolled in the database and $I_{N+1}$ indicates the reject case where no suitable identity can be determined for the user. Thus:

$$\begin{cases} I_i \ if\ \max_i S(v_Q, v_i) \geq t, i = 1,2,...,N \\ I_{N+1}, otherwise \end{cases}$$

where $v_i$ is the biometric template corresponding to identity $I_i$, *S* is the function that measures the similarity between $v_Q$ and $v_i$, and *t* is a predefined threshold. Since biometric samples of the same individual taken at different times are almost never identical (due to different imaging conditions or different interactions between the user and the system), for example, it is difficult to determine the perfect match. Thus, instead of reporting a unique identity $I_i$, the system outputs a set of possible matches which can be determined in two ways: threshold-based or rank-based. Fig. 2 depicts the main modules in a face identification system.

ISSN 2348 – 7968

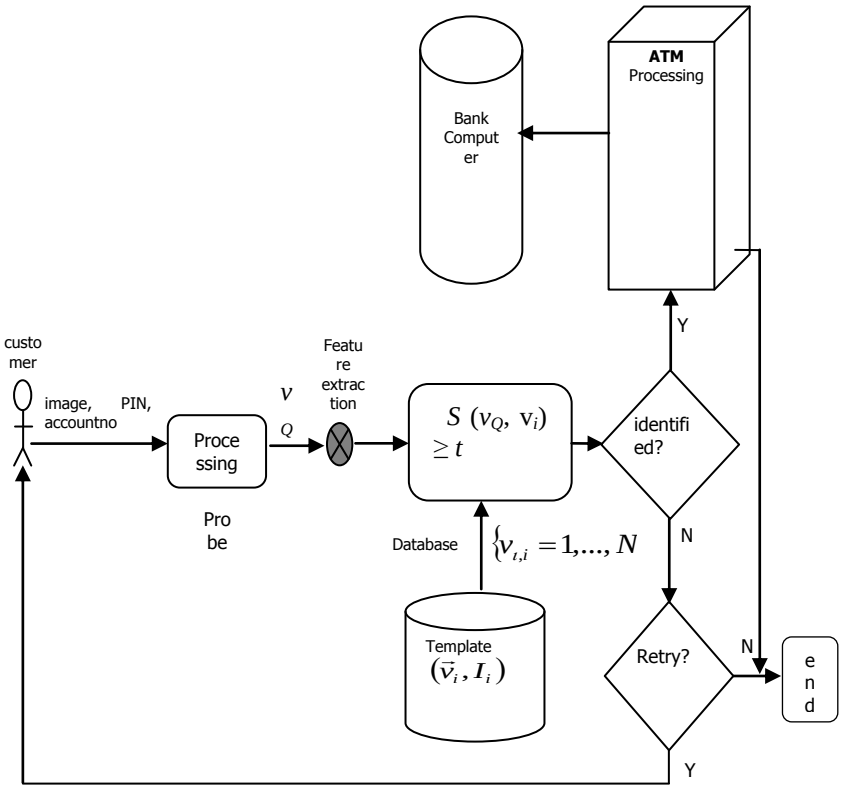


Fig. 2: Face identification: the probe $v_Q$ of an unknown user is matched against all biometric templates $v_i$ in the database to determine his/her identity. The system can operate in two modes. Watch list: are you in my database? and; basic identification: you are in my database, can I find you?

In a threshold-based mode, *t* is preset by the constructor according to the security level required. If t is too large, the system may fail to identify many users. If *t* is too small, the system will output a large number of possible matches, many of these are inaccurate. The more common approach to design an identification system is the rank based mode. The system typically determines a set of m best matches which present the highest matching scores. *m* is usually referred to as the rank. The system always returns a fixed number of outputs: the *m* known identities enrolled in the database that resembles the most to the unknown user, sorted in some order.

There are typically four basic components:

1. The data acquisition module

This module comprises the imaging and lighting apparatus necessary for capturing image data of the users. The present application requires an off-the-shelf 3D video camera that needs to be sufficiently fast to accurately capture real-time facial deformations. Since all 3D dynamic image capture systems today operate within a limited field of vision, they are not suitable for recognition from far distance, e.g. crowd surveillance. For this reason, the present study will focus solely on applications where the users are cooperative e.g. computer login and secure access control. The users are typically required to perform some short verbal or nonverbal facial actions; the recording conditions are designed to model as closely as possible real-life situations.

2. The feature extraction module

This module comprises the algorithms necessary for extracting and quantifying facial motion characteristics from videos. At enrolment, facial performances of known persons are collected and used to train a 3D spatiotemporal statistical model. This model can be subsequently used to estimate or extract facial dynamics from a given video footage. There are two feature extraction scenarios:

a. Ground-truth: very accurate technique for extracting facial motions but requires manual data annotation. This method is preferred whenever the feature extraction does not need to be performed automatically in real-time. For example, during the enrolment phase, biometric samples of known persons are extracted and stored in a database. This operation is performed behind the scene, manual landmark placement can be considered.

b. Model fitting: automatic feature extraction, typically by fitting a deformable model to unseen test scans and solving an optimization problem. Developing robust fitting algorithms is still a largely unsolved problem; therefore this method is much less reliable compared to the ground-truth method. It is however indispensable for the deployment of a fully automatic face recognition solution.

3. The database

This is a database that contains the biometric templates of known persons who are enrolled into the system. Typically, a biometric template is a pair ($I_k$, $v_k$) where $I_k$ is a known identity - e.g.

ISSN 2348 – 7968

name - and $v_k$ is the facial motion signature associated with $I_k$. The database can be either centralized or distributed e.g. a smart card carried by each user. The centralized scenario is more efficient to avoid counterfeit or lost cards, but it has to deal with scalability issues. In large-scale systems of thousands of identities, it can be computationally tasking to match the biometric sample of an unknown user – the probe – against all stored biometric templates in the database. In order to reduce the computational overhead of pattern matching, it is usually necessary to classify the templates in the centralized database. For example, if we know that the user is a man, there is no need to check his probe against women's templates.

4. The decision making module

This module comprises the pattern matching algorithms necessary for measuring the resemblance between two biometric samples, together with the implementation of the policy related to the matching process. Pattern matching involves comparing a probe of an unknown user to a biometric template in the database. The matching process generates a numerical estimation of the similarity. A threshold is usually defined by the system constructor which the biometric samples are considered as belonging to the same person. The choice of the threshold is a matter of policy. In a high-security application where the cost of a false acceptance could be high, system policy might prefer very few false acceptances and many more false rejections. In a commercial setting where the cost of a false acceptance could be small and treated as a cost of doing business, system policy might favour false acceptances in order not to falsely reject and thereby inconvenience large numbers of legitimate customers.

## 5.0 Recognition process: Unified Modelling Language Diagram

There exist two scenarios of face recognition: face verification and face identification, as shown in Fig. 1. They share similar feature extraction and pattern matching algorithms, but differ in the decision making process:

The identification problem is a one-to-many comparison in which the probe $v_Q$ of an unknown person is compared to all biometric templates $\{(I_k,v_k),k = (1,...,N)\}$ of known subjects enrolled in the database, e.g. in police identification. The system can operate in two modes. Watch list: are you in my database? and basic identification: you are in my database, can I find you?

Fig. 2: Face verification: given a probe $v_Q$ of an unknown person and a claimed identity $I_k$, determine if the person is a genuine user or an impostor. Typically, $v_Q$ is matched against $v_k$, the biometric template of $I_k$.

### 5.1 Face Identification

#### 5.1.1 System Architecture

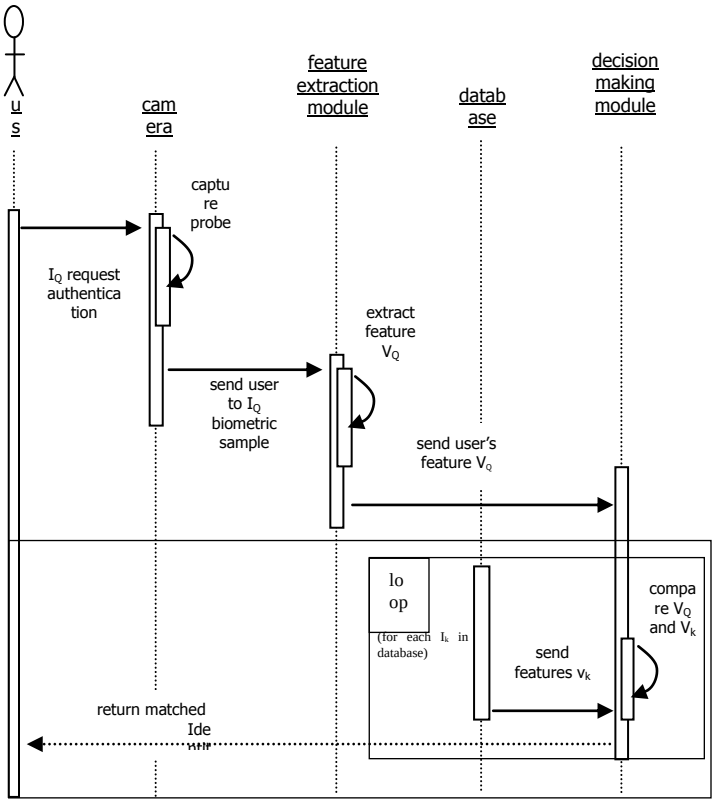


Fig. 3: Unified Modelling Language sequence diagram of the recognition process.

## 6.0 Conclusion and Recommendation

Face recognition has been an attractive area of research for both neuroscientists and computer vision scientists. Human beings are able to identify, with high rate of reliability, a large number of faces and face recognition researches illuminate computer vision. In this research, an ATM model that is more reliable in providing security by using facial recognition approach is presented with conceptual framework for use of face-

ISSN 2348 – 7968

based access control in ATMs. The research has shown that ATM users have encountered many problems in the past which the research work has offered solutions to. But for the scope of this research, further works could be considered in the area of integrating virtually all the biometric measures into a single system. This will invariably ensure maximum security in all ATM-related transactions and drastically reduce frauds and to overcome all the aforementioned problem it is advisable that government partner with banking sector to use biometric techniques "face-based access control" in ATMs as it will eradicate the problems associated with smartcard access control.

## References

[1] A4Vision Inc.," Source: http://www.a4vision.com. Last visited December 9, 2010.
[2] Bahtiyar A. Gül, (1998), Holistic Face Recognition by Dimension Reduction, Master of Science Thesis, Graduate School of Natural and Applied Sciences, the Middle East Technical University.
[3] Barkley, J. (1995), "Implementing Role-Based Access Control using Object Technology," First ACM Workshop on Role-Based Access Control, Gaithersburg, Maryland.
[4] Belhumeur, P. N; Hespanha, J. P and Kriegman, D. J. (1997), Eigenfaces versus Fisherfaces: Recognition Using Class Specific Linear Projection. IEEE Tran. on Pattern Analysis and Machine Intelligence, 19(7):711-720.
[5] Bishop, C. M. (1995), Neural Networks for Pattern Recognition. Oxford University Press Inc., New York.
[6] Brunelli, R and Poggio, P. (1993), Face Recognition: Features versus Templates. IEEE Tran. on Pattern Analysis and Machine Intelligence, 15(10):1042-1052.
[7] Chellappa, R; Wilson, C. L and Sirohey, S. (1995), Human and Machine Recognition of Faces: A Survey. Proc. of the IEEE, 83(5):705-740.
[8] Cognitec Systems GmbH Source: http://www.cognitec-systems.de. Last visited December 12, 2010.
[9] Cootes, T. J; Lanitis, A and Taylor, C. J, and (1997), Automatic Interpretation and Coding of Face Images using Flexible Models. IEEE Tran. on Pattern Analysis and Machine Intelligence, 19(7):743-756.
[10] Cottrell, G. W and Fleming, M. K. (1990), Face Recognition using Unsupervised Feature Extraction. In Int. J. Conf. on Neural Networks, pages 322-325, Paris.
[11] Dai, Y and Nakano, Y. (1998), Recognition of Facial Images with Low Resolution using a Hopfield Memory Model. Pattern Recognition, 31(2):159-167.
[12] Demers, D and Cottrell, G. W. (1993), Nonlinear Dimensionality Reduction. In Advances in Neural Information Processing Systems, pages 580-587.
[13] Diebold Inco. (2002), ATM Fraud Security white paper.
[14] Er, M. J; Wu, S and Lu, J. (1999), Face Recognition using Radial Basis Function (RBF) Neural Networks. In 38th Conference on Decision & Control, pages 2162-2167, Phoenix, Arizona USA.
[15] Essinger, J. (1987), ATM Networks, Their organisation security and finance, published by Elservier Int Bulletin Chp 6 Future developments.
[16] Fagbolu .O (2011), Security Issues in Information and Communication Technology Environment – A focus on Automated Teller Machine, International Journal of Physical Sciences, Nigeria ISSN 1597-8023, 7, No 2, 1-11.
[17] Fenton, M. (2008), by Admin. Banking systems and technology; The Blog. Taking ATM fraud prevention to the next level.
[18] Genex Technologies Inc.," Source: http://www.genextec.com. Last visited December 9, 2010.
[19] Geometrix Inc.," Source: http://www.geometrix.com. Last visited December 9, 2010.
[20] Gutta, S; Huang, J. R. J; Jonathan, P and Wechsler, H. (2000), Mixture of Experts for Classification of Gender, Ethnic Origin, and Pose of Human Faces. IEEE Trans. On Neural Networks, 11:948-959.
[21] Hamelink, C. (2000), "The Ethics of Cyberspace," Sage, London, Ind, N. "Living the Brand," Kogan Page, London.
[22] Haykin, S. (1999), Neural networks: A Comprehensive Foundation. Prentice-Hall International, New Jersey.
[23] Howell, A. J and Buxton, H. (1995), Invariance in Radial Basis Function Neural Networks in Human Face Classification. Neural Processing Letters, 2(3):26-30.
[24] Huang, J. (1998), Detection Strategies for Face Recognition Using Learning and Evolution. PhD thesis, George Mason University.
[25] ISACA// www.isaca.org/glossary (2007).
[26] Jolliffe, I. T. (1986), Principal component analysis. New York: Springer; University of Geneva; ISBN: 0-387-96269-7.
[27] Jøsang, A and Pope, S, (2005),User Centric Identity Management, AusCERT Conference 2005,
[28] Kalakota, R. and Whinston, A. B. (2001), "Electronic Commerce: A Manager's Guide" 2nd Edition, Addison Wesley, Harlow.
[29] Kohonen, T. (1988), Self-Organization and Associative Memory. Springer-Verlag, New York.
[30] Kumar, S. (2010), "Introduction to ISO 8583", www.codeproject.com/KB/scrapbook/ISO8583 accessed December 7, 2010.
[31] Lades, M; Vorbruggen, J. C; Buhmann, J; Lange, J; Von ser Malburg, C; Wurtz, R. P and Konen, W. (1997), Distortion Invariant Object Recognition in the Dynamic Link Architecture. IEEE Transactions on Computers, 42:300-310.
[32] Lawrence, S. C; Lee Giles; Ah Chung Tsoi, and Andrew D. Back, (1998), Face Recognition: A Convectional Neural Network Approach. IEEE Trans. on Neural Networks, 8(1):98-113.
[33] Lawrence, S. C; Lee Giles; Ah Chung Tsoi, and Andrew D. Back. (1997), Face Recognition: A Convolutional Neural Network Approach. IEEE Trans. on Neural Networks, 8(1):98-112.
[34] Lin, Shang-Hung; Sun-Yuan Kung; and Long ji Lin. (1997), Face Recognition/Detection by Probabilistic Decision-based Neural Network. IEEE Trans. on Neural Networks, 8(1):114-131.
[35] Liposcak, Z and Loncaric, S. (1999), Face Recognition from Profiles using Morphological Operations. In

ISSN 2348 – 7968

International Workshop on Recognition, Analysis, and Tracking of Faces and Gestures in Real-Time Systems, pages 47-52.

[36] Mammone, R. J. (1993), Artificial Neural Networks for Speech and Vision. Chapman and Hall, Cambridge.

[37] Marcia Crosland, NCR Corp. (2010), Consumer behaviour drives innovation in ATM technology. http://www.atmmarketplace.com .

[38] Neven Vision Inc.," Source: http://www.nevenvision.com. Last visited December 13, 2010.

[39] O'Gorman, Lawrence (2003), Comparing Passwords, Tokens, and Biometrics for User Authentication; Proceedings of the IEEE, Vol. 91, No. 12, December 2003, pages 2021 – 2040.

[40] Osuna, E; Freund, R and Girosi, F.(1997), Training Support Vector Machines: An Application to Face Detection. In IEEE Conference on Computer Vision and Pattern Recognition, pages 193-199.

[41] Penev, P and Atick, J. (1996), Local Feature Analysis: A General Statistical Theory for Object Representation. Network: Computation in Neural Systems, 7:477-500.

[42] Poggio, T and Sung, K. K, (1994) Example-based Learning for View-based Human Face Detection. ARPA Image Understanding Workshop.

[43] RCBC (2007), Rizal Commercial Banking Corporation. Electronic Banking (e-Banking) Consumer protection Policy.

[44] Robert J. B. (1981), Mechanisms of Human Facial Recognition. International Journal of Man-Machine Studies, 15(2):137-178.

[45] Schlichter, S. (2007), "Using ATM's abroad" www.msnbc.com/id/16994358 accessed December 8, 2010.

[46] Scholkopf, B; Smola, A. J and Bernhardt, A. (1998), Nonlinear Component Analysis as a Kernel Eigenvalue Problem. Neural Computation, 10(5):1299-1319.

[47] Shibboleth Project, (2004), *Shibboleth Architecture Protocols and Profiles.* Working Draft 05, 23. Internet2/MACE.

[48] Sirovich, L and Kirby, M. (1987), Low-dimensional Procedure for the Characterization of Human Faces. Journal of Optical Society of America, 4(3):519-524.

[49] Stonham, T. J. (1984), Practical Face Recognition and Verification with WISARD. In Aspects of Face Processing, pages 426-441.

[50] The Banker's Magazine, September, 1983.

[51] Thiagarajan, V. (2002), Information Security Management, BS 7799.2:2002, Audit Check List for SANS Institute, BS 7799 Audit Checklist.

[52] Thomaz, C. E; Feitosa, R. Q and Veiga, A. (1998), Design of Radial Basis Function Network as Classifier in face Recognition using Eigenfaces. In V*th* Brazilian Symposium on Neural Networks, pages 118-123.

[53] Turk, M and Pentland, A. P. (1991). Eigenfaces for Recognition. Journal of Cognitive Neuroscience, 3(1):71-86.

[54] Turk, M. A and Pentland, A. P, (1999), Face Recognition Using Enigenface, Vision and Modeling Group, the Media Laboratory Massachusetts Institute of Technology.

[55] Valentin, D; Abdi, H; O'Toole, A. J and Cottrell, A. W. (1994), Connectionist Models of Face Processing: A survey. Pattern Recognition, 27(9):1209-1230.

[56] Viisage, Littleton, MA," Source: http://www.viisage.com. Last visited December 9, 2010.

[57] Vladimir N. Vapnik. (1995), The Nature of Statistical Learning Theory. Springer Verlog, Heidelberg, DE.

[58] Weng, J; Ahuja, N and Huang. T. S. (1995), Learning Recognition Segmentation of 3-D Objects from 2-D Images. In Int. Workshop Face Gesture Recognition, Zurich, Switzerland.

[59] Wiskott, L; Fellous, J; Kruger, N and Christoph von der Malsburg. (1997), Face Recognition by Elastic Bunch Graph Matching. IEEE Tran. on Pattern Analysis and Machine Intelligence, 19(7):775-779.

[60] Wood, P. (2005), "Implementing identity management security - an ethical hacker's view", Network Security, Volume 2005, Issue 9, Pages 12-15.

[61] Yang, M. H, (2002), Kernel Eigenfaces vs. Kernel Fisherfaces: Face Recognition using Kernel Methods. In IEEE International Conference on Face and Gesture Recognition, pages 215-220, Washington.

[62] Yegnanarayana, B. (1999), Artificial Neural Networks. Prentice-Hall of India, New Delhi.

[63] Yu, M; Yan, G and Zhu, Q. (1997), New Face Recognition Method Based on DWT/DCT Combined Feature Selection, School of Computer Science, Hebei University of Technology, China.

[64] Yuille, Alan L. (1991), Deformable Templates for Face Recognition. Journal of Cognitive Neuroscience, 3(1):59-70.