Journal of Engineering and Development, Vol. 12, No. 3, September (2008) **ISSN 1813-7822**

Implementation of an Efficient Access Control System for Secure Building

Asst. Prof. Dr. Khamis A. Zidan
Computer and Software Engineering Department, College of Engineering
Al-Mustansiriya University, Baghdad, Iraq

Abstract

This paper describes hybrid access control system based on a new approach of face recognition and PIN (Personal Identification Number) code identification, which is done by finding the closest match between features implemented on the same databases. This approach involves two identification and matching subsystems. The outputs from these subsystems are combined to decide the final output that authorizes the access to the secure building for certain persons while denying the access for the others.

In verification, a biometric identifier is compared to another template through a PIN number of database. Identification involves comparing an existing image against a large image database in order to identify the individual depicted. For this purpose, a camera is set in the door looking at the enter and the captured frames are analyzed. The implementation includes neural networks for PIN code identifications, and analysis starts by selecting the regions of interest in the face images using NN.

A neural network based upright frontal face recognition approach has been presented in this paper. The algorithm of face recognition is implemented using preprocessing of face image and two-stage neural network. The first net finds the eyes region of a person and improving image by histogram equalization. The second uses an image of the area around eyes region to identify the person. Using arbitration between multiple networks with rarely overlap in region images to clean up the results significantly improves the accuracy of the recognition. A feasibility investigation and evaluation for face recognition based solely on new concept is conducted which covers all conditions of human face recognition under varying lighting condition, varying facial expression, and varying pose.

The proposed system structure is implemented with newly proposed methods that allow fast processing and accurate recognition as a software package using C++ and Visual Basic.

الخلاصـــــة

لقد تم في هذا البحث اقتراح طريقه هجينه وكفوءة لنظام سيطرة دخول الأشخاص للأبنية الأمنية باعتماد طريقة جديدة لتمييز وجوه الأشخاص مع نظام مطابقة رقم التعريف الشخصيPIN. إن فكرة الطريقة الهجينة مكونة من نظامين فرعيين. الأول هو التعرف على وجه شخص وتمييزه من بين مجموعة كبيرة من وجوه الأشخاص والمخزونة في قاعدة البيانات داخل ذاكرة باستخدام الشبكات العصبية. والثاني البحث في قاعدة البيانات لإيجاد التطابق في PIN، بحيث إن مرحلة ربط تلك الخواص تتضمن مزج الخرج الناتج عن كل جزء من النظام للحصول على الخرج النهائي الذي يحدد الوجه المميز وPIN الخاصة به والمخزونة داخل قاعدة البيانات. والسماح للشخص المخول بالدخول ورفض الأشخاص غير المخولين و الغير موجودين في قاعدة البيانات.

نظام تمييز الوجوه يبدأ بالتقاط صورة أمامية لوجه الشخص بواسطة كاميرا عند مدخل البناية، وإدخال الصورة للنظام لأجراء عمليات معالجة أولية عليها تتضمن تقليص حجم الصورة باستخدام (Wavelet Transform) لزيادة سرعة النظام ولتقليل البيانات الداخلة إلى الشبكة العصبية. وبعدها أيجاد منطقة العيون لوجه الشخص، تليها تحسين خواص الصورة باستخدام (Histogram Equalization)، لكي توفر إمكانية عدم تأثر معلومات الصورة للتغييرات الطفيفة نتيجة الاختلاف بكفاءة الكاميرا وتحسين التباين داخل الصورة. وبعدها اخذ جزء من الصورة لمنطقة العينين وما يحيط بهما من منطقة تفاصيل الوجه لإجراء التماثل وبعدها التصنيف لغرض التمييز. إن تصميم نظام متكامل لتمييز صور الوجوه وتصنيفها يتضمن إدخال المعلومات إلى الشبكات العصبية المتعددة (Multiple Networks) التي توفر إمكانية عدم تأثر المعلومات لتغير الصورة جزئيا بحيث تغطي الظروف التي يتعرض لها وجه الشخص مثل ظروف إضاءة مختلفة، تعابير وجه الشخص مختلفة، والأوضاع المختلفة لصورة الوجه. إن شفرة التمييز تتضمن مزج الخرج الناتج عن كل جزء من الشبكات العصبية المتعددة للحصول على الخرج النهائي للشبكة الذي يحدد الوجه المميز وتصنيفه.

إن هيكلية النظام المقترح تم بنائها على شكل حقيبة برمجية باستخدام (C++ and Visual Basic). حيث تم اختبار النظام الجديد بالحالة ألعمليه وكان الأداء كفوء جدا في سرعة المعالجة ودقة التمييز العالية.

1. Introduction

Access control is concerned with determining the allowed activities of legitimate users, sensitivity level and the clearance level of the user accessing the system [1]. To assure the safety of an access control system, it is essential to make certain that the access control configuration will not result in the leakage of permissions to an unauthorized principal.

Access control system can be either online or offline meaning programmed and/or monitored in real time locally or remote; or manually (offline) by performing audits or programming at the actual door lock. Many buildings will have a combination of mechanical and electrical door hardware, making a perfect choice to manage a complete building door security. Electronic access control also includes the monitoring and surveillance of the opening through either a software audit trail and/or visual record captured by CCTV cameras and stored on video recorders for later analysis [1].

The level of control will depend on user need and the level of risk and exposure to loss or compromise for any physical and electronic access. Access will be assigned based upon the information needed to perform assigned duties. Electronic access is controlled through personal accounts, which allow an individual user to logon to specific applications or systems using personal or unique ID (Identification) and password. No one should use the ID or password of another, nor should anyone provide his or her ID or password to another. The password should only be given to personnel upon presentation of identification [1,2].

Access control policies can be as diverse as the applications that rely upon them, and are heavily dependent on the needs of a particular environment. For instance, the mandatory labeling policy for the military, the commercial integrity policy for banking, and the

confidentiality policy for healthcare institutions have each modeled their unique policies to meet their own internal control needs and external regulatory requirements. Furthermore, access control policies are dynamic in nature, in that they are likely to change over time in reflection of ever-evolving business factors, government regulations, and environmental conditions [1-5].

Recently, technology became available to allow verification of "true" individual identity. This technology is based in a field called "biometrics". Biometric access control are automated methods of verifying or recognizing the identity of a living person on the basis of some physiological characteristics, such as fingerprints, iris pattern, facial features, DNA, or some aspects of the person's behavior, and no two human are identical in these characteristics. Like his/her handwriting style, voice print or keystroke patterns. Since biometric systems identify a person by biological characteristics, they are difficult to forge [6].

Because of human inherent protectiveness of his/her eyes, some people are reluctant to use eye identification systems. Face recognition has emerged as an adequate technology for person identification in such systems which do not require any user's cooperation. Indeed, face technology has several advantages over other biometric systems. First of all, a face recognition-based system is passive, non-intrusive system to verify personal identity in a natural and friendly way. There is no need to use our fingers or to say some words in order to be recognized by the system [7]. Also, no expensive and specialized equipment are needed as a simple video camera connected to a personal computer is largely enough to build the system.

There are many works devoted to the face recognition problem. But most of them are oriented on obtaining higher recognition rate for some test face databases in the prejudice of identification robustness and stability for real applications. The rejections of misclassified or unauthorized persons are not studied well. For this reason, face recognition has drawn the attention of researchers in fields from security, psychology, and image processing, to computer vision. Numerous algorithms have been proposed for face recognition; for detailed survey please see [8,9]. Despite the commercial success of those face recognition products, a few research issues remain to be explored.

Holistic matching methods use the whole face region as the raw input to a recognition system. One of the most widely used representations of the face region is eigen pictures, which are based on Principal Component Analysis (PCA) [10-13]. Using PCA, many face recognition techniques have been developed: eigenfaces, which use a nearest neighbor classifier; feature-line-based methods, which replace the point-to-point distance with the distance between a point and the feature line linking two stored sample points. Being able to offer potentially greater generalization through learning, neural networks/learning methods have also been applied to face recognition [14,15]. One example is the probabilistic decision based neural network method. One of the most successful systems in this category is the graph matching system, which is based on the dynamic link architecture. Using an unsupervised learning method based on a self-organizing map, a system based on a conventional neural network has been developed. Hybrid methods are based on using both

local features and the whole face region to recognize a face, as the human perception system uses.

Two major benefits of Artificial Neural Systems (ANS) are storage capacity and classification speed. ANS can store large number of complex patterns; faces, visual scenes. It can classify new patterns and store patterns quickly. The classification speed is independent of the number of patterns stored [16,17].

The present work for face recognition used two neural networks: the first neural network starts with a face image as input. The task of this net is to localize the eyes. A second neural network will use the information from the area around eyes region to recognize the person. This approach is typical for admission control.

A feasibility investigation and evaluation for this work face recognition based solely on new concept is conducted which covers all conditions of human face recognition, under varying lighting condition, varying facial expression, and varying pose. It is a very encouraging finding that the proposed face recognition technique has performed consistently superior to other methods in all the comparison experiments. It considers different thresholding approaches for rejecting unauthorized persons and unreliable cases. The neural network discriminative power in conjunction with thresholding based rejection is presented. Also it presents different architectures of neural networks ensembles and their stability for classification and robustness for rejection unauthorized persons. Most of the applications of face recognition to access control suffer from either low recognition speed due to the complex analysis of facial images, or to the low recognition accuracy [18]. The newly proposed method allows fast processing and accurate recognition. The system is tested and achieved a recognition rate of 98% and a recognition time of 0.0021 sec using 1520 MHz PC.

2. Performance Evaluation Metrics

The system achieves different recognition results on different training runs due to the probabilistic character of NN training for PIN identification and face recognition subsystems, to get the final output (decision). In person access control task experiment, it should take in mind thresholding algorithms for rejection of unauthorized persons. The recognition system must reject such cases as much as possible, but perform well for authorized persons.

In order to measure performance of algorithms, the three standard biometric measures to indicate the identifying power are False Rejection Rate (FRR) (the number of authorized persons, considered as unauthorized, divided by total number of authorized attempts), False Acceptance Rate (FAR) (the number of unauthorized persons, considered as authorized, divided by total number of unauthorized attempts), and Recognition Rate (RR) (the number of persons (correctly classifies) divided by total number of access attempts).

Thresholding algorithm gives better recognition rate for all threshold ranges and better FRR/FAR. It is much stricter to unauthorized persons and slightly stricter for authorized persons. This access control system tunes its threshold value to reject all imposters (minimizing FAR). It may also improperly reject some authorized users

(maximizing FRR) [6]. Therefore, the system is implemented to provide a variable threshold setting for the customers to strike a balance.

3. Structure of Proposed Access Control System

Face recognition technology is considered ideal for access control, fast, accurate and simple to enhance security without introducing complex access control procedures that make it difficult for employees to gain entry. In organizations with a large number of persons, speedy access control is a must and with face recognition, it can make matches in under a second with precision.

Figure (1) describes a structure implementation of a hybrid access control system based on face recognition and PIN code identification, which is done by finding the closest match between features implemented on the same databases, which authorizes the access to the secure building for only certain persons while denying the access for the others. Identification involves comparing an existing image against a large image database in order to identify the individual depicted. In verification, a biometric identifier is compared to another template through a PIN number of a database, which includes neural networks for PIN code identifications. For this purpose, a camera is set in the door looking at the enter and the captured frames are analyzed. A face recognizer determines who this person, that is searches the database to find the best match to the incoming face image using a neural network based upright frontal face recognition approach.

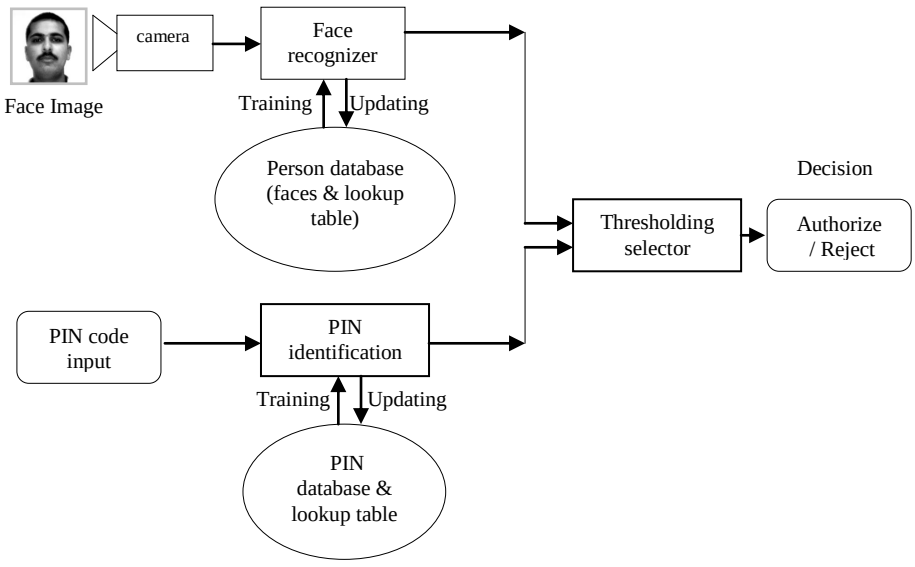


Figure (1) A structure of access control system based on face recognition and PIN identification

The level of control will depend on user need and the level of risk and exposure to loss or compromise for any physical and electronic access. The approach involves hybrid system of two subsystems identification and matching, and the output from these subsystems are combined to decide final out for authorized or rejected to entry to secure building. Using face

recognition in conjunction with another authentication factor for dual factor authentication, which include PIN code, therefore, significantly increases security for building access.

4. Characteristics of the Proposed Access Control System

Network access control via a new approach of face recognition not only makes intruder virtually impossible to steal one's "PIN code" that is not enough for authorization, but also increases the user friendliness in human computer interaction and provides more efficient coding scheme. This paper shows the generic framework reader of PIN code and face recognition based on the appearances of particular persons. Several famous face recognition algorithms, eigenfaces and Fourier transform, also are implemented for comparisons. Therefore, the characteristics of the proposed access control system are:

1. The system is on-line with human interaction, user interface, PIN keypads, and image capture.
2. PIN code of 11 digit from keypad, which is set near to the camera at the enter in the door looking of the system.
3. Face images are gray-scale, 2-D frontal, upright views of almost uniform illumination.
4. It used static matching.
5. Final output of the system means authorized or unauthorized (rejected) present person to enter the building.

5. PIN Identification

A neural network is used for this stage to locate the PIN code for identification. It is assigned based upon the personal accounts, which allow an individual user to logon to database through unique PIN code. The PIN should only be given to personnel upon presentation of identification. No one should use the PIN of another, nor should anyone provide his or her PIN to another. Therefore, the first component of the system that receives as input a PIN code of the person, and then passed through a neural network, which decides whether the PIN, which generates an output signifying the presence or absence of person, respectively in the database. Then, the output from PIN code identifier with a face recognizer are combined through a threshold level to decide the final output for acceptable or rejected the person to enter to the building. The network turned out to work very well. In the test of network, the PIN taken at a factor of 11 digits. The network is trained to find the PIN in a PIN database and lookup table.

6. Face Recognition Using Neural Networks

Proactive computing aims to design and develop smart environments that adapt and adjust to the user's movements and actions without requiring any conscious control. In other words, the system should be able to identify the users, interpret their actions, and react appropriately. Thus, one of the first and most important building blocks of such environments is a person identification system.

The work describes the robustness of new NN classifiers with respect to the False Acceptance and False Rejection errors by using a new thresholding approach for rejection of unauthorized persons, with ensembles of NN different architectures. The newly proposed approach of face recognition allows fast processing and accurate recognition. In this system, a camera is set in the door looking at the enter and the captured frames are analyzed. **Figure (2)** shows an example of the considered environment.

Figure (2) An example of the environment: A camera is set in the door looking at the enter and captured images

6-1 Theoretical Background

Neural network related methods achieved better recognition results compared with classical methods. Multilayer Perceptron (MLP) neural network is a good tool for classification purposes [19-21]. It can approximate almost any regularity between its input and output. The NN weights are adjusted by supervised training procedure called backpropagation. Backpropagation is a kind of the gradient descent method, which search an acceptable local minimum in the NN weight space in order to achieve minimal error. The usual motivation for applying a backpropagation net is to achieve a balance between correct responses to training patterns and good responses to new input patterns (i.e., a balance between memorization and generalization).

In experiments it uses many hidden layer and units in NNs. The number of units in the input layer is equal to the number of image pixels. In order to speed up the classification and to reduce the amount of data needed (in particular with respect to neural networks) the resolution is reduced by using Discrete Wavelet Transform (DWT).

6-2 Implementation of Face Recognition Subsystem

6-2-1 Face Database

Most of the researches experiments used the Olivetti Research Ltd (ORL) face database [22], but for the proposed practical application approach, this database is insufficient. Therefore, a 256 grayscale bitmap face image of 320x320 pixel is obtained using a digital camera coupled to personal computer, who are allowed to enter the building. Thereby, it doing a relational database, which contains 400 images compiled from 40 subjects (authorized) with 10 images each. The images are taken against a white homogeneous background with varying lighting conditions. The faces are in a frontal upright position and show a range of expressions. Side movement and head tilt were tolerated to a limited extent only as shown in **Fig.(3)**. This database just like the ORL face database, but have further information, which consists of a set of face images and a table of information that are connected together by the primary key with PIN code by relational database, as well as a rejection (unauthorized) faces. There are 200 face images to train the neural network on rejection of unknown faces in database. In this work 10 images per person were taken; half of the images for training and the other half for testing selected at random.

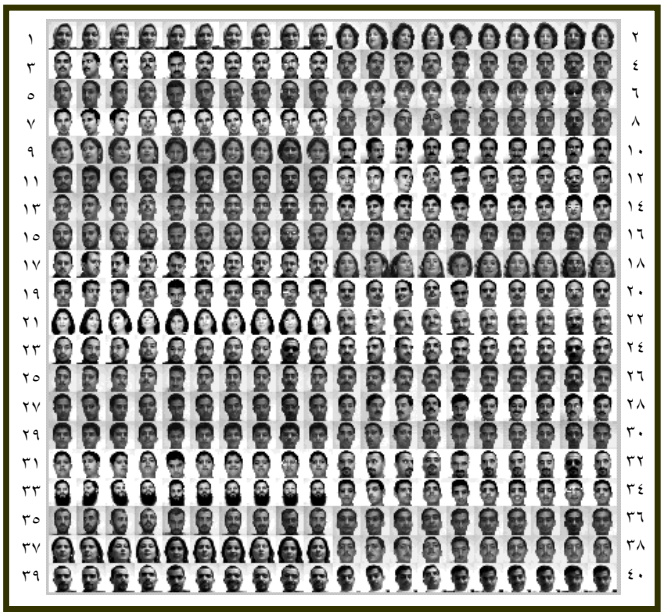


Figure (3) Example of database face images

6-2-2 Generic Framework of Proposed Face Recognition Subsystem

To deal with facial expression changes only the "significant facial region" is used instead of using the whole facial area to perform recognition task. The significant facial region is a square area close to the center of the human face. It contains eyes, nose and the mouth. Study shows that facial expressions and hairstyle changes have less influence on the significant facial region, and yet the face is still recognizable by viewing only the significant

facial region [6,23]. **Figure (4)** shows a high-level block diagram with the significant facial region face recognition subsystem.

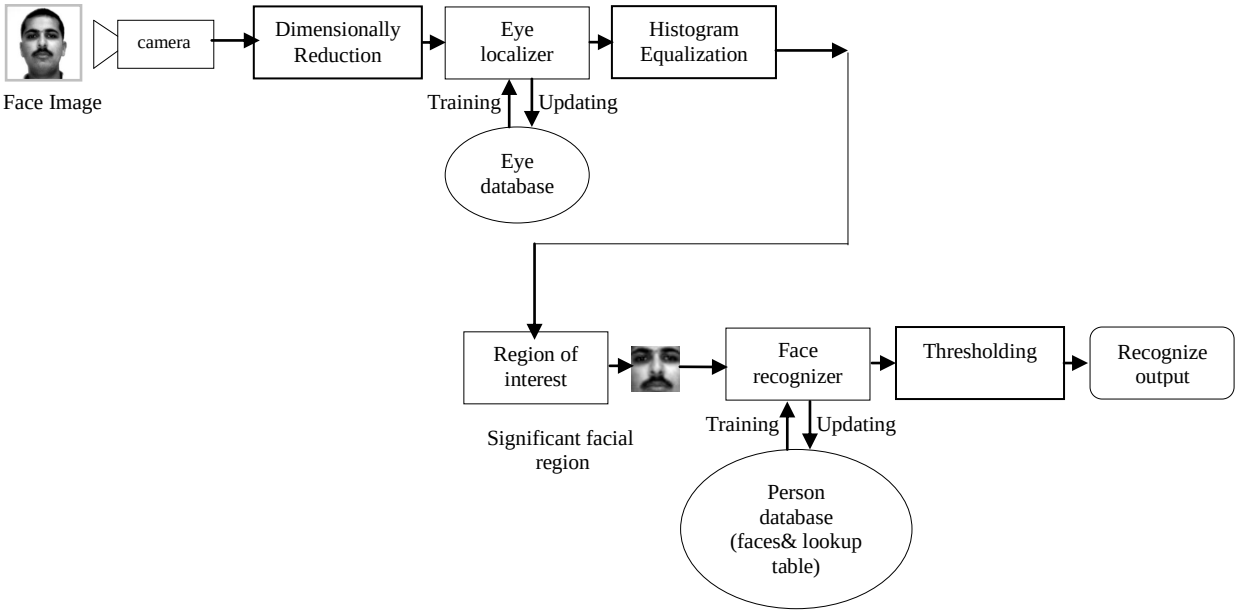


Figure (4) A framework face recognition subsystem

A face recognition algorithm can be divided into two neural networks functional modules: one to localize the eyes in the image obtained from the digital camera "eye localizer" that produces only an "approximate" location of the eyes face. In addition to find the "exact" location of the face for recognition, a second net use this information from the windows on the eyes to recognize the person. The face recognition subsystem is implemented to use the locations of eyes, nose and mouth for assistance. A face recognizer determines who is this person, by searching the database to find the best match to the incoming face image. In the first approach, the images are obtained by using a digital camera coupled to a personal computer.

The database is assembled under different constraints (lighting, head tilt, facial expression). In this architecture, a lot of effort is needed to reduce the input space to guaranteeing a good performance under usual conditions, which should not affect recognition. Backpropagation based networks are used for the process of recognition.

6-2-2-1 Preprocessing For Image Size Reduction

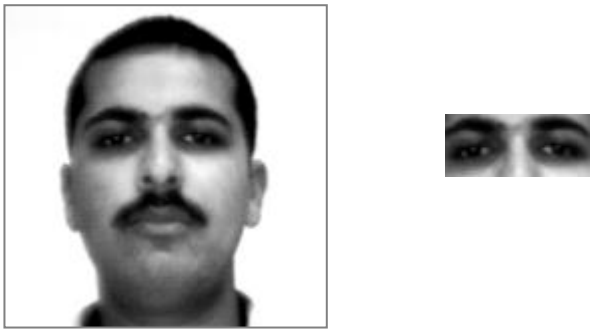
The main drawback of such network, regardless of its architecture and learning algorithm, is the size of its inputs. A 320x320 pixels image represents 102400 inputs. Furthermore, the network should be provided with a large number of images so that decent generalization can be achieved. Therefore, if it is combined with a large number of training epochs, training would require a huge amount of time and resources. One of the most modern transform, used today in a number of applications is the DWT. This is a very versatile

orthogonal transform and a multi-resolution approach that is very fastly computed. It is used with very good results for data compression and enhancement of the signal to noise ratio [24]. In fact, approximately 50% of the largest wavelet coefficients are needed to be retained in order to yield a fair reconstruction of the input. A method to reduce the number of inputs, while, at the same time, increase the flexibility and the redundancy of the total system is presented. In addition, the computational requirements are considerably less than other compression methods, and are more suited to VLSI implementation [24,25].

6-2-2-2 Finding the Eyes

A relatively small window (20x40 pixel) is used for this first stage that needs only to locate the eyes. The network turned out to work very well. In a test of the redundancy of network, the image taken at a factor of two shorter distances to the camera. Although the network is trained to find the eyes in an image recorded at a given distance, there is no difficulty in finding them in this extreme close-up, it uses image recorded by scanners to train and test the neural network.

The first component of this stage receives as input a 20x40 pixel region of the face image, and then passed through a neural network, which decides whether the window contains eyes, by generating an output signifying the presence or absence of eyes, respectively. Typically vectors from windows outside the face are significantly smoother than vectors from the eye region. Provided that the window is not too big, these vectors turn out to have gross properties that are very similar. A relatively small window is used to scan for the eyes region are shown in **Fig.(5)**. The reason is that the eyes of different persons are most similar in the center of the eyes. **Figure (6)** shows the histogram of eyes region and another part of the same face image outside of eyes region. While the first stage neural network is to find the common properties of eyes, the second one should find the differences. Thus, for recognition larger than the window size, is repeatedly in size of 40x40 pixel for second net.



(a) **(b)**

Figure (5) Example of facial image in (a), with scanning rectangles of 20x40 pixels over the eyes in (b)

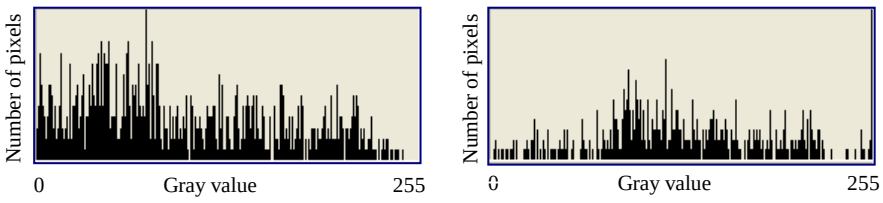


Figure (6) (a) Histogram of image eyes region. (b) Histogram of image from another part of same face outside of eyes region. The window is 20x40 pixels

6-2-2-3 Preprocessing for Lighting Variation and Contrast

The variation is caused by lighting and camera characteristics. There is a major source of variation (apart from intrinsic differences between faces), which are result in brightly or poorly lighted images, or images with poor contrast. These problems are first addressed by using a simple image processing approach. The images are preprocessed to make them suitable for recognition purposes and improve the recognition performance. To alleviate the influence of the illumination effect, it takes conventional image enhancement technique (histogram equalization). The histogram equalization is performed to enhance the contrast of images by transforming the values in an intensity image.

6-2-2-4 Individual Face Recognition Networks

In this work, a multi-networks solution for face recognition is suggested. The main emphasis is on reducing the number of the necessary calculations before training through backpropagation. This work is geared towards the use of multi-networks that implement layers of different types of networks. Each of which specialize in a specific task, in this architectures, a lot of effort are spend toward reducing the input space and guaranteeing a good performance under usual conditions, where lighting, rotation and tilting effects should not affect recognition.

The algorithm operates into stages: it applies a set of neural network based recognizers to an image of significant facial region, and then uses an arbitrator to combine the outputs. The network has retinal connections to its input layer; the receptive fields of hidden units are shown in **Fig.(7)**. The input image is broken down into smaller pieces. There are four types: 16 pieces each 10x10 pixel subregions, 64 pieces each 5x5 pixel subregions, 16 pieces overlapping 5x40 pixel horizontal stripes of pixels, and 16 pieces overlapping 40x5 pixel vertical stripes of pixels. The shapes of these subregions are chosen to allow the hidden units to recognize local features that might be important for face recognition. It is important that the input is broken into smaller pieces instead of using complete connections to the entire input. In particular, the horizontal stripes allow the hidden units to recognize such features as mouths or pairs of eyes and translating the image up or down. The vertical stripes allow the hidden units to recognize such features as nose and translating the image left or right. While

the hidden units with square receptive fields might recognize features such as individual eyes, the nose, or corners of the mouth.

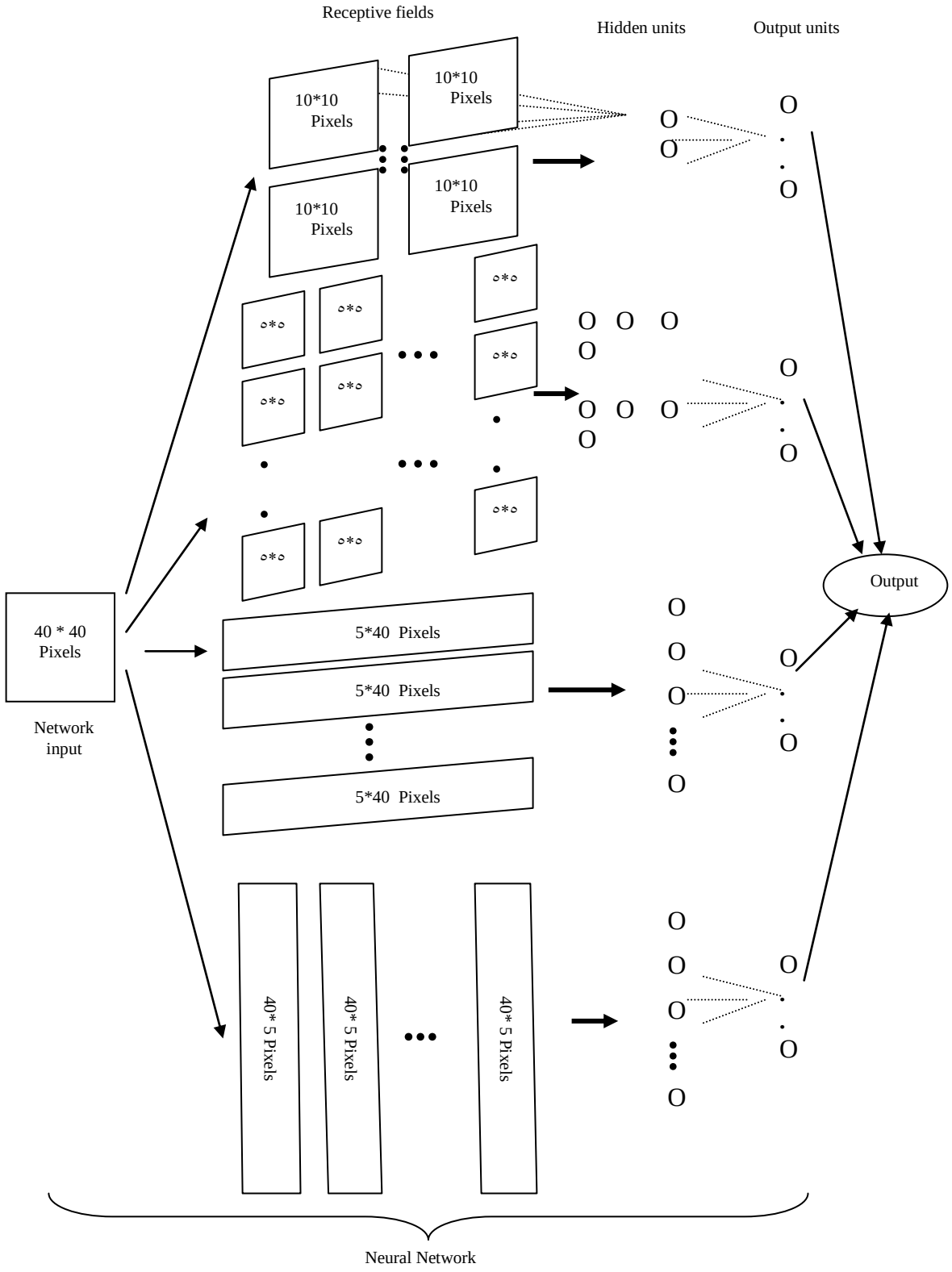


Figure (7) The basic algorithm used for face recognition

6-2-2-5 Arbitration among Multiple Networks

It is applied multiple networks, and arbitrate between their outputs to produce the final decision. Each network is trained in a similar manner, but with random initial weights.

Classification is performed by means of the threshold. This allows the use of a threshold in order to gain some confidence in the decision. If the output result of the closest match is smaller than the selected threshold, the subsystem rejects the test image. Use of a threshold makes it possible to reject faces that do not belong to the trained subject. This is a very important property for a face recognition approach. Therefore, a non-linear classifier is also constructed. The use of arbitration multiple networks significantly improves the accuracy of the recognizer. The technique, "thresholding", involves combining multiple, near by recognition into one.

The networks rely most heavily on the eyes, then on the mouth and corners, and then on the nose. It uses a bootstrap algorithm, which adds false recognitions into the training set as training progresses. Simple heuristics, using rarely overlap in region images, is further improve the accuracy. The use of arbitration between multiple networks and heuristics to clean up the results significantly improves the accuracy of the recognition.

6-2-2-6 Training Face Images

The images are divided into two exclusive sets: the training set and the test set. The training set is used to initialize and prepare the system to recognize arbitrary images and to fine tune the algorithm parameters. The test set is the set of images which is used to evaluate the performance of the system after training is completed.

Each network sub-net consists of input layer, one or two hidden layers and an output layer. Output nodes as individuals to be recognized, which is encoded on (n) binary outputs to allow for maximum faces to be recognized. The number of outputs units can be increased to fit a larger number of faces.

A large number of nonface or wrong (rejected) face images are needed to train the face recognizer, because the variety of nonface images is much greater than the variety of face images (authorized). The number of output nodes depends on the number of classes that are recognized. When it uses the coded output nodes of neural network, the rejected images gives a specified code not similar to the coded one of any class of 40 classes that is known. **Figure (8)** shows examples of an authorized person recognized by the system and an unauthorized one rejected by the system.

(a) **(b)**

Figure (8) Examples where: (a): An authorized person is recognized. (b): An intruder to the system is rejected. With sample faces of database

6-2-2-7 Identifying the Person

While the first stage neural network is to find the common properties of the eyes, the second net will determine the differences. These neural networks are of different architecture and have different input nodes, different hidden nodes and have as many output nodes as the individuals to be recognized. The larger number of inputs is due to the larger window used.

To give the recognizer some robustness to slight variations in the faces for experiments, the weights and biases of the network are initialized to random values between [-0.05, 0.05]. The maximum number of training epochs is 3000. To allow comparisons, the same training and test set size of images are used. Hence there are 200 training images and 200 test images in total and no overlap exists between the training and test images, as well as 200 face images to train the neural network on rejection of unknown (unauthorized) faces in database.

On the first iteration of this loop, the network's weights are initialized randomly. After the first iteration, the weights computed by training in the previous iteration are used as the starting point. The process is repeated many times for each pattern in the training set until the total output error converges to the minimum or until some limit is reached in the number of training iterations completed.

Each sub-net is trained on half set images per person. The neurons use the bipolar activation function, the training algorithm used in error backpropagation algorithm with a momentum term. When using momentum, the net is proceeding not in the direction of the gradient, but in the direction of a combination of the current gradient and the previous direction of weight correction [16].

6-3 Experimental Results

A thorough approach performance investigation, which covers all conditions of human face recognition, has been conducted. They are face recognized under varying lighting condition, varying facial expression, and varying pose.

To examine the system performances under head pose variations, the database contains frontal views of 40 people. Each person has images with different head pose variations (two frontal parallel pose, one looking to the right, one looking to the left, one looking downwards, one looking upwards). The recognition results are acceptable and equal to 94% for varying pose.

The face database is used to evaluate the performances under varying lighting condition, and facial expression.

6-3-1 Face Recognition under Varying Lighting Conditions

Ideally, an object representation employed for recognition should be invariant to lighting variations. It has been shown theoretically that, for the general case, a function invariant to illumination does not exist.

The experiment is implemented using face images taken under different lighting conditions. The experiments reveal a number of interesting points: The variations of lighting condition did affect the performance. Nevertheless, the recognition rates approach is still high and acceptable. The recognition rates, when only one light is on, stayed as high as 95.8%.

6-3-2 Face Recognition under Facial Expression Changes

Similar experiments are conducted to evaluate the effects of different facial expressions on the performances. The recognition rate is dropped very little, that is because of selected a square area close to the center of the human face, which contain significant facial region instead of whole face image. The recognition rate is about 92% which is acceptable.

6-4 Recognition Results

6-4-1 Variation of Number of Hidden Neurons and Hidden Layers

Hidden layers and hidden neurons play a critical role in the operation of backpropagation learning because they act as feature detectors. As the learning process progresses, the hidden neurons in these layers begin to gradually discover the salient features that characterize the training data.

For most applications, a single hidden layer is sufficient. Some times, difficult learning tasks are simplified by increasing the number of internal layers. So, for complex mapping, two hidden layers may give better generalization and may make training easier than a single hidden layer.

Table (1) shows the accuracy of the face recognition approach as the number of hidden layers and hidden neurons in the network are varied. A good performance for the network is 75 nodes for the first hidden layer and 50 nodes for the second hidden layer.

Table (1) Accuracy of face recognition approach with varying number of hidden layers and hidden neurons in the network subnets

No. of hidden layers	**One hidden layer**		**Two hidden layer**	
No. of hidden neurons	65	75	75 , 40	75, 50
Recognition rate	89.8%	92%	94.2%	98%

6-4-2 Recognition Results with Arbitrating Among Networks

It is interesting to note that the face recognition approach generally have a higher recognition rate for faces with arbitrating among four networks than for the other types of arbitration as shown in **Table (2)**. Most of the persons whose faces have variability of images by rotating, translating, expression, and lighting condition. Thus the recognition rate for some faces is lower, when it used some of this arbitration.

Table (2) Recognition rate with varying of arbitration output

Type	**Recognition rate**
Output of one network (10*10)	64%
Arbitrating among two networks (10*10) and (5*5)	78.3%
Arbitrating among three networks (10*10) and (5*5) and (5*40)	94%
Arbitrating among four networks (10*10) and (5*5) and (5*40) and (40*5)	98%

7. Other Methods

7-1 Fourier Transform

The Fourier transform method is implemented for comparison purposes, as it is one of the successful algorithms available. This technique is based on the Fourier spectra of facial images, thus it relies on a global transformation. The classification is done by means of the Euclidean distance. The distances between the feature vector of a presented test face and all the feature vectors in the training set are calculated. The smallest distance then gives the closest match. If that match belongs to the same person the classification is successful. This allows the use of a threshold in order to gain some confidence in the decision, if the distance of the closest match is greater than the selected threshold the system rejects the test image. Use of a threshold makes it possible to reject faces that do not belong to the trained subjects, a very important property for a face recognition system. The resolutions used in the available database of images are 320x320 pixels. Thus, the images had to be compressed and resizes until the desired dimensions are reached 128x128 pixels. The classification is correct in 92.2% of the cases of the same database.

7-2 Eigenfaces

It is called Principal Component Analysis, and a few parameters used for representation are extracted from a face [26]. Those parameters are obtained by a projection of the face onto a coordinate system given by the eigenvectors of the covariance matrix of the training set. These eigenvectors, themselves images, are termed eigenfaces and span a vector space called face space. Each face is then encoded by means of its coordinates in this face space. Matching of two faces corresponds to a calculation of the Euclidean distance between their face space representations. It is found that gives the best results (with as few variables used as possible) on the images used here. The classification is correct in 93.6% of the cases of the same database.

7-3 Comparison between Methods

It is of paramount importance that the number of errors made is minimized. The work presented in this paper comprises a new approach that achieves 98% correct recognition. In particular it is found to be superior to the other methods that have been used on the same database of facial images. **Table (3)** shows a comparison of performances of the three methods.

It is remarkable that all the methods are capable of distinguishing between known and unknown faces. The neural networks with 75, 50 units in its hidden layers do achieve comparable results. However, the other networks, the eigenface, and Fourier transform methods perform less well.

Table (3) Comparison of performances of the three methods

Method	Recognition rate
Fourier transform method	92.2%
Eigenface method	93.6%
Neural network method with (75,40) units of hidden layers	94.2%
Neural network method with (75,50) units of hidden layers	98%

8. Access Control System Performance

This application is used by which access to a secure building is controlled by a face recognition approach and PIN identification, and then reduced to a simple, known or unknown (authorized/rejected) approach. For these applications it is desirable for the system to be adjusted to make 0% misclassifications. The system is implemented for dynamic information environment by system administrators and responsible for maintenance operation.

The test set consists of images that are not part of the training set. It seems reasonable to assume that the choice of training and test images could influence the performance; the system is tested using two chosen divisions of training and test sets. In both experiments the correct identification remained at 98%. The system is implemented to provide a variable

threshold setting for the customers to strike a balance, and appropriate for their security requirements. At high security thresholds, it keeps intruders out, but some employees may have to be more exact in how they present themselves for verification. At low thresholds, authorized employees can easily gain entrance, but someone without authorization might also be permitted through.

The security level of control system depends on customer need and the level of risk and for this application requires near 100% rejection of intruders. Combined access is based upon the face recognition and personal accounts, which allow an individual user to logon to database through unique PIN code. The PIN should only be given to personnel upon presentation of identification. No one should use the PIN of another, nor should anyone provide PIN to another. Thus, authorized users will have to suffer, 2% rejection rate. The system is tested in practical application by random choice of 10 persons and it gives 100% correct classification.

The recognition time is the time required to have an output of the system when an image and PIN code is applied to the input. This work is implemented by using a special programming. Since, the recognition time depends on the efficiency of the recognition program, the programming language and on the speed of computer used, as well as the network structure, therefore, the proposed system structure is implemented as a software package using C++ and Visual Basic, and the time for system recognition is 0.0021 sec by using 1520 MHz PC.

9. Conclusions

This paper presents a proposed system that is applicable for access control, which consists of PIN keypad to enter the 11 digit individual as well as a camera at the front door of a building, to extract face image of people and quickly identifies them using a database of known individuals. The system is able to recognize individuals in frontal face image. A combination of face recognition approach with a PIN code might lead to further increase in reliability. It applied a new threshold method for rejection of all unauthorized persons.

The newly proposed method allows fast processing and accurate recognition, the time for system recognition reached 0.0021 sec by using PC with 1520 MHz CPU, and the correct recognition rate is 98%.

Improvements presented in this paper are by creating a real access control system. First, an image must be equalized in brightness and contrast, to bring it to uniform conditions. The second improvement lies in the domain of the better, ensembles of NN different architectures and NN training. NN needs a set of rejected examples to narrow areas with unauthorized persons.

The work demonstrated that a two stage neural network can be used to find the eyes region of a person and to identify the person. Significant reduction of the processing time is obtained by implementing the neural network(s) with many inputs. But, in order to reduce this number a preprocessing using wavelet transform is considered.

The proposed method is less sensitive to illumination changes. It is a very encouraging knowing that the proposed face recognition approach can achieve higher recognition accuracy with much less storage requirement and computational time .

The proposed approach to face recognition achieves excellent recognition results both as a classifier and when confronted with faces not belonging to any of the persons used for training.

10. References

1. V. C., Hu, D. F., Ferraiolo, and D. R., Kuhn, ***"Assessment of Access Control Systems"***, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, September 2006.

2. D., Bryliuk, ***"Access Control by Face Recognition using Neural Networks and Negative Examples"***, The 2nd International Conference on Artificial Intelligence, September 16-20, Crimea, Ukraine, 2002, pp. 428-436.

3. Gasser, M., ***"Building a Secure Computer System"***, Van Nostrand Reinhold Publication, 1988.

4. V., Hu, D., Frincke, and D., Ferraiolo, ***"The Policy Machine for Security Policy Management"***, Proceedings ICCS Conference, San Francisco, May 2001.

5. V., Hu, D. R., Kuhn, and D., Ferraiolo, ***"The Computational Complexity of Enforceability Validation for Generic Access Control Rules"***, Proceedings IEEE SUTC2006 Conference, Taichung, Taiwan 2006.

6. S. H., Lin, ***"An Introduction to Face Recognition Technology"***, Informing Science Special Issue on Multimedia Informing Technologies-Part 2, Vol. 3, No. 1, 2000, shanghung.lin@ic-media.com

7. A., Hadid, M., Heikkila, T., Ahonen, and M., Pietikainen, ***"A Novel Approach to Access Control Based on Face Recognition"***, Department of Electrical and Information Engineering, University of Oulu, Finland.

8. R., Chellappa, C. L., Wilson, and S., Sirohey, ***"Human and Machine Recognition of Faces: A Survey"***, Proc. IEEE, Vol. 83, May 1995, pp. 705-741.

9. J., Zhang, Y., Yan, and M., Lades, ***"Face Recognition: Eigenfaces, Elastic Matching, and Neural Nets"***, Proc. IEEE, Vol. 85, No. 9, 1997, pp. 1423-1435.

10. Y., Gao, and M. K., Leung, ***"Face Recognition Using Line Edge Map"***, IEEE Transaction on Pattern Analysis and Machine Intelligence, Vol. 24, No. 6, June 2002.

11. Javier Ruiz-del-Solar, and Pablo Navarrete, ***"Eigenspace-Based Face Recognition: A Comparative Study of Different Approaches"***, IEEE Transactions on Systems, Man, and Cybernetics-Part C: Applications and Reviews, Vol. 35, No. 3, August 2005.

12. M., Kirby, and L., Sirovich, ***"Application of the Karhunen-Loeve Procedure for the Characterization of Human Faces"***, IEEE Transactions on Pattern Recognition and Machine Intelligence, Vol. 12, No. 1, January 1990, pp. 103-108.

13. S. T., Gandhe, K. T., Talele, and A. G., Keskar, ***"Face Recognition Using Contour Matching"***, IAENG International Journal of Computer Science, Vol. 35, No. 2, 2006.

14. S. T., Gandhe, K. T., Talele, and A. G., Keskar, ***"Face Recognition Using Isodensity Maps-A Neural Network Approach"***, In 1st International Conference on Emerging Applications of Information Technology (EAIT) Organized by Computer Society of India, Kolkata Chapter, Kolkata, February 2006, pp. 129-132.

15. Z., Pan, and H., Bolouri, ***"High Speed Face Recognition Based on Discrete Cosine Transforms and Neural Networks"***, Science and Technology Research Center, University of Hertfordshire, Hatfield, Herts, AL10 9AB, UK, 1999, z.pan,h.bolouri@herts.ac.uk.

16. S. W., Smith, ***"Digital Signal Processing"***, California Technical Publishing USA, 1999.

17. A., Eide, C., Jahren, and S., Jorgensen, ***"Eye Identification for Face Recognition with Neural Network"***, Ostfold College, Halden, 1996.

18. W., Zhao, R., Chellappa, P. J., Phillips, and A., Rosenfeld, ***"Face Recognition: A Literature Survey"***, ACM Computing Surveys, Vol. 34, No.4, Dec. 2003, pp. 399-458.

19. A. I., Wasserman, ***"Neural Computing: Theory and Practice"***, New York, Van Nostrand Reinhold, 1989.

20. V., Golovko, and V., Gladyschuk, ***"Recirculation Neural Network Training for Image Processing"***, Advanced Computer Systems, 1999, pp. 73-78.

21. H. A., Rowley, S., Baluja, and T., Kanade, ***"Neural Network-Based Face Detection"***, PAMI, January 1998.

22. Stave Lawrence, C., Lee Giles, Ah., Chung Teoi, and Andrew, D. Back, ***"Face Recognition: A Convolutional Neural Network Approach"***, IEEE Transaction on Neural Network, Special Issue on Neural Networks and Pattern Recognition, Vol. 8, No. 1, 1997, pp. 98-113.

23. S. H., Lin, S. Y., Kung, and L. J., Lin, ***"Face Recognition/Detection by Probabilistic Decision-Based Neural Network"***, IEEE Trans. Neural Networks, Vol. 8, No. 1, Jan. 1997, pp. 114-132.

24. S., Pittner, and S., Kamarthi, ***"Feature Extraction from Wavelet Coefficients for Pattern Recognition Tasks"***, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 21, No. 1, January 1999, pp. 83-88.

25. H., Schildt, ***"Complete Reference of Borland C ++"***, Prentice Hall, 1997.

26. M., Turk, and A., Pentland, ***"Eigenfaces for Recognition"***, Journal of Cognitive Neuroscience, Vol. 3, No. 1, 1991, pp. 71-86.

Acknowledgements

The author would like to appreciate the collaboration of the staff and students of Computer and Software Engineering Department in Al-Mustansiriya University for participating in the performance of work as a volunteered in face database.