E-Passport Recognition System Based on ANNs

Lobna Anwar Mohammed
Science College, University of Al-Anbaar
Email:lobna90_ra@yahoo.com
Dr. Muzhir Shaban Al-Ani
Science College, University of Al-Anbaar
Email:muzhir@gmail.com
Dr. Ali Jbaeer Dawood
Science College, University of Al-Anbaar
Email:dralijd@yahoo.com

Received on:31/5/2016 & Accepted on:29/9/2016

ABSTRACT

Nowadays it is more necessary to perform the identity check of passengers quickly and reliably to prevent unauthorized border crossing, and limit the use of forger passport. This paper concentrated on the design E-passport using two main technologies which are biometric and RFID technologies. Biometric features are used to identify passport holder and the RFID is used to store andtransmit these features as required. This paper proposes a new approach to design and implement a robust biometric recognition system that could be used in e-passport system to identify and recognize person that own the identical e-passport. The ANN is used for recognition persons in this proposed system which was able to recognize persons registered in database in rate up to 81% and the percentage of fail in recognition was 19%.

Keywords: E-passport, Biometrics**,** RFID, Face Recognition, Principle Component Analysis (PCA), Distance Based Feature**.**

INTRODUCTION

The wide spread and integration of computers in almost every aspect of our daily life led to transit from physical documents to purely digital-based information in a wide range of scenarios. The processing of traditional passport documentation certainly requires physical handling: the content must be read and interpreted. As a result, traditional passport processing is slow and more exposed to error. Furthermore, most of these passports don't have enough security mechanisms and their authentication depend on handwritten signatures or stamps which can be easily forged. Moreover, the issuer of passport cannot be properly authenticated and it may be difficult to effectively prevent content alteration and counterfeiting. These security problems have been extensively addressed in electronic passport [1].

The design of electronic passport gives many benefits that it not only helps in checking that the person owning the document is the true holder, but also to make the travel more easier and increase the speed at which it takes an individual to clear customs and security checkpoints in airports. The e-passport combines a biometric identifier with RFID technology to strength the security and authenticity. Radio-frequency identification (RFID) is considered one of the most important technologies of twenty one century. This technology has the capability to achieve many objectives of corporations and government [2].

RFID is used in E-passport for two reasons, the automatic scanning of the passport and the possibility to add biometric features in the passport [3].

Aim of the work

The aim of this paper is to implement a robust biometric recognition system that use in e-passport. The main biometric types that are used in this proposed system are face and hand geometry. This work uses principle components analysis and distance based features to extract

https://doi.org/10.30684/etj.34.6B.15
2412-0758/University of Technology-Iraq, Baghdad, Iraq

important features from face and hand and also using Artificial Neural Networks (ANN) for recognition process.

Literature Review

There are several studies of electronic passport with biometric system and RFID during previous years and these are:

- Jonathan P. Chapman et al (2009) analyzed the electronic passport design of the International Civil Aviation Organization (ICAO). While many exist papers were focused on privacy and personal security of e-passports bearers, their focus was the actual security benefit countries obtained by the introduction of e-passports and related systems[4].
- Anshuman Sinha(2010) described the cryptographic protocols used in Basic Access Control (BAC) and Extended Access Control (EAC), suggested that The future of passports may shift from single-chip electronic RF to multichip modules with a combined data storage capacity from multiple chips. Future e-Passports may look like a secured solid disk with onboard sensors and limited or no printed information. [5].
- V.K. Narendira Kumar and B. Srinivasan (2011) presentedan attempt to acknowledge and account for the presence on e-passport scheme using face, fingerprint, and palm print and iris recognition, towards their improved identification [6].
- Eyad Abdullah Bogari et al (2012) presented a review of security features and vulnerabilities across two generations of the RFID enabled passports. The survey shows that some of the vulnerabilities of the first generation E-passports have been eliminated by the security features of the second generation [7].
- DominikMalˇc´ık and Martin Drahansk´y(2012) provided an insight into the electronic passports (also called e-passport) implementation chosen in the Czech Republic. Such a summary is needed for further studies of biometric passports implementation security and biometric passports analysis [8].
- V.K. Narendira Kumar and Dr. B. Srinivasan (2013) discussed embedded an RFID chip into the back cover of the passport. Border guards will be able to compare the face of the person standing in front of them with the image of the person stored onto the RFID chip [9].

Definition of E-passport

An electronic passport (e-Passport) is an identification document which possesses relevant biographic and biometric information of its bearer [6]. The main difference between classical passport and the electronic passport(e-passport)is the embedded electronic chip which employ wireless communication interface, this electronic chip is called RFID chip (radio frequency Identification) [10].

The main purpose of electronic passport (or sometimes called biometric passports) is to prevent the illegal entry of travelers into a specific country and to make the use of fraudulent passport documents more limited by using more secure and perfect identification of persons [11].

The e-passport presents a huge enhancement in both national and international security and improves the integrity of passports because it match the information that stored in RFID chip to one that printed in the document and physical characteristics of the bearer of passport, e-passport enable machines (instead of human)to check the biometric and biographic information written on passport [12].

In 2004, the International Civil Aviation Organization (ICAO) issued a set of recommendations and protocol specifications to countries that wished to use e-Passports. According to ICAO, an electronic passport must contains a contactless electronic reading device with internal storage space of at least 32 kilobits of size, coded accordingly to the Logical Data Structure (LDS) The passports that have these characteristics must have a special symbol on the cover that identifies them as e-Passports, the e-passport identifier symbol showed on Figure (1)[6, 13].

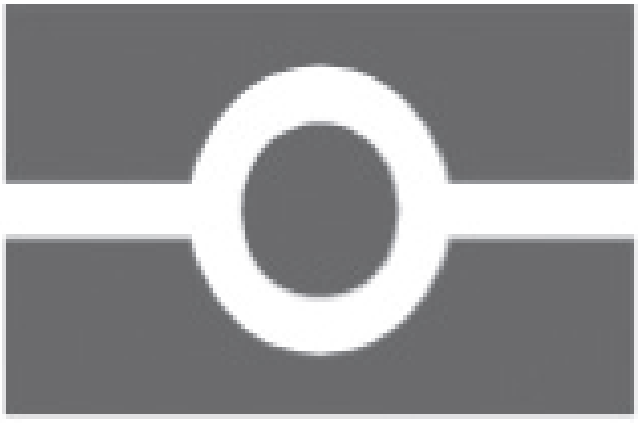

Figure (1) E-Passeport Identifier Symbol

RFID in E-passport

Radio Frequency Identification (RFID) technology has existed for decades. The term RFID is generally used to describe any technology that uses radio signals for identification purposes. Today, new applications for RFID embed RF technology in common objects, or "everyday" things used by individuals, such as library books, payment tokens, and government-issued identification, the e-Passport is an important example of these new RFID applications which has RF transponder embedded in the cover [14].

RFID devices consist of four elements: the RFID tags, the RFID readers, the antennas, and the computer network that is used to connect the readers [15].Figure (2) shows the main system components of RFID

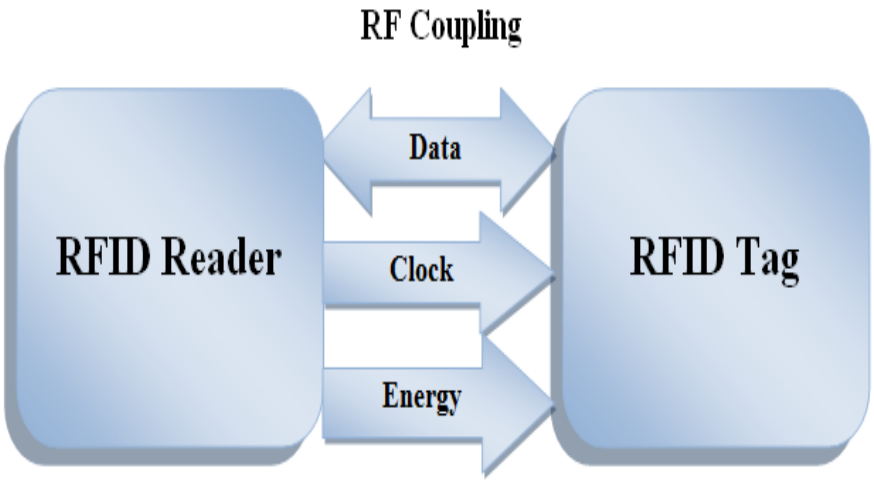

Figure (2) RFID Main System Components

Proposed system structure

The proposed system is using the biometric techniques to verify the identity of the passport's holder, so, this system implements two biometric techniques which are face recognition and hand geometry recognition using MATLAB2013 and also use artificial neural network (ANN) to recognize persons. The technique used to extract face features is principle

component analysis (PCA) which is statistical method used to extract information from face image.

The features of hand geometry are extracted using distance based features which is a method that use tip and valley points and also computed many distances (Euclidian distance) on hand .finally the features that computed from face and hand are entered into ANN that trained on these features and then tested to recognize persons that registered into database. Then the information of the recognized person are retrieved as shown in figure (3).

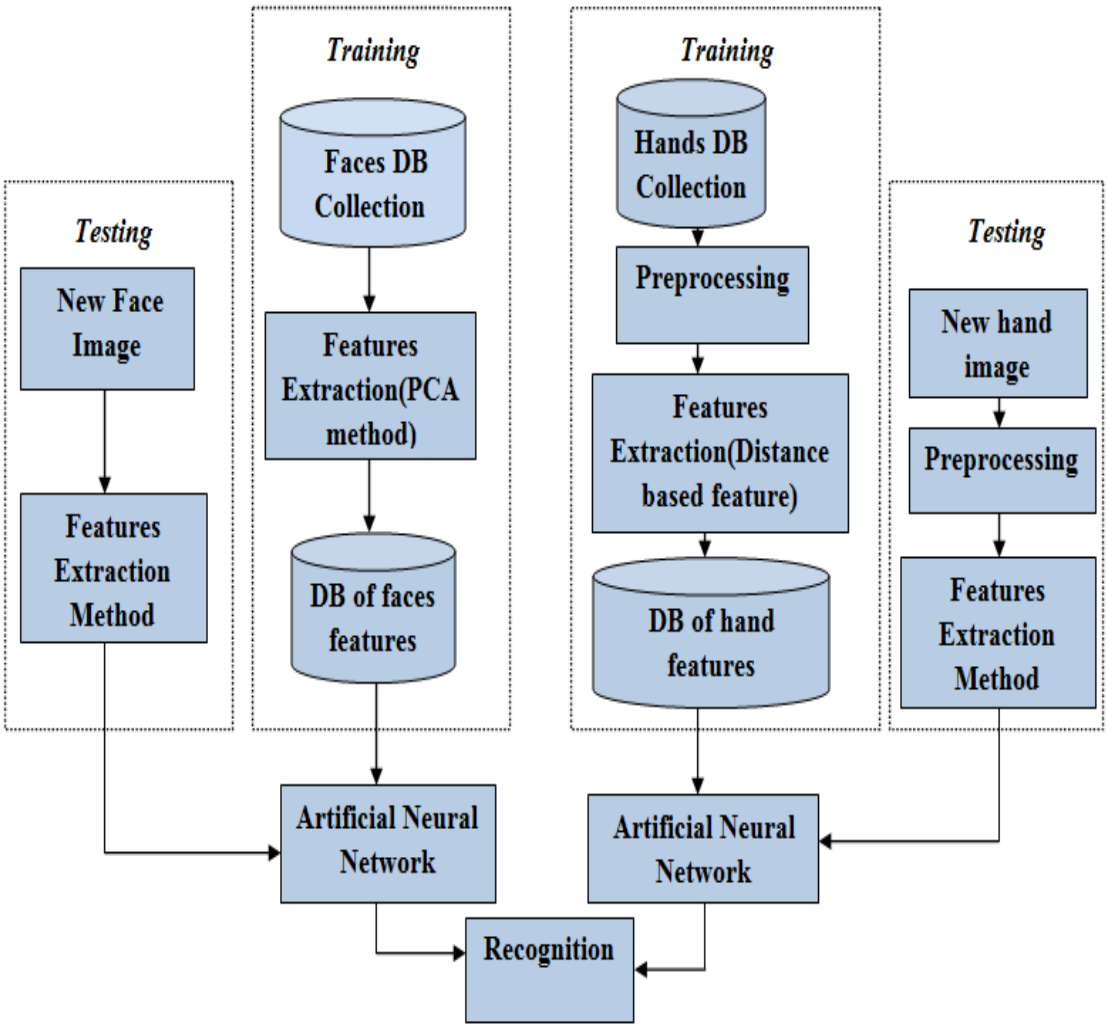

Figure (3) Block Diagram of Proposed Algorithm

Data Collection Phase

The database of faces contains 100 colored face image which built taking the face image of 10 persons and for each person 10 face image (7 for training and 3 for testing) and these faces image are taken from different views which men, the image could be taken while person's face is turned to left, right, up or down with different angles. This database is collected using a camera with 16.2 MEGA pixel resolutions.

Feature Extraction

After the collecting of faces images and building the database of faces, the next step is the reading process and that done by reading only 7 faces images for each person in the database (training) and the rest 3 images are used for testing later. The read colored images is then converted to gray images using the function (rgb2gray (image)).

The features extracted from faces images using principle component analysis (PCA) which extract weights (features) that stored in features database. The first stage of feature extraction is Eigen vector preparation that began with taking the 70 faces images which are converted to vectors by multiplying the rows with columns for each image, these 70 vectors are grouped into one matrix its row is equal to size of vector and its column is equal to number of images=70 and this matrix is called data matrix. The mean of each columns of data matrix is computed and subtract from each value in data matrix the value of its column's mean and that produce a new matrix (p).

After that the covariance matrix is calculated and then also calculates the Eigen value and eigenvectors to covariance matrix and finally takes Eigen vectors that correspond to maximum Eigen value which stored to be used later in features extraction phase.

After getting on Eigen vector matrix, we multiplying this matrix with P transpose (P') to get on features**.**The system takes from each face image 50 features which means for each person we take 350 features for only 7 images and that all features stored in features database (Excel).

Database collection phase

The database of hand geometry is built using scanner (canon 1024MF) with 300 resolutions to take images for hand. The database contains 100 hand images for 10 persons (10 images for left hand of each person), and using 7 images for training and 3 for testing.

Preprocessing Phase

The hand image is stored into database as a colored image, so, the first step of preprocessing is converting the colored image to grayscale image using (rgb2gray) function, after that convert the grayscale image to binary image that have black and white color only and that done using threshold value where the points in image are converted according to the function:

Input image (i,j) ≥ Threshold , Output Image (i,j) = 1

Input image (i,j) <Threshold , Output Image (i,j) =0

This process is called binarization and because the clear differences between the hand image (foreground) and the background of image (background) the binarization process will be easy and give results that conforms to reality. Thus, we get on binary image its white colour represents the user hand and its black colour represents the background of image**.**

The resulting image from the previous two steps also have some noises and we must remove these noises and enhance the image by applying some enhancement filters , the average filter were used and applied on image twice and then apply disk Filter also twice .

The process of detect the edge of hand is done by using one of edge detection algorithm which works on converting all points (white and black) to black points except boundary points. The edge detection algorithm must sure that the thickness of boundary as low as possible because the thickness of boundary has an effect on hand features measurements accuracy and also it is very important that edge detection algorithm don't neglected or loss the detection of any edge and also it mustn't detect false edge. These points detect the error rate which must be low. Finally the bottom part of hand is cutting to get on only an important part which has the features that desired. The steps of preprocessing are illustrated in Algorithm (1)

Algorithm(1) Preprocessing Steps

Input: Colored image of hand.
Output: Image after preprocessing.
Steps:

1. Read colored hand image
   Image=imread("Hand").
2. Convert colored image to gray
   Gray=rgb2gray(Image).
3. Convert gray image to black and white
   BW=im2bw(Gray).
4. Apply average filter to image
   Average filter=imfilter(BW , Average mask).
5. Apply Disk filter to filtered image
   Filtered image=imfilter(Average filter, Disk mask).
6. Read boundaries of all object inside filtered image and find the largest
   Largest- boundaries=boundaries of longest object in filtered result.
7. Define a new image of the same size of colored image with all pixels set to zero
   Result=zeros(size(image,1),size(image,2)).
8. Find the length of longest boundaries
   Boundary-Index=size(Longest-Boundary,1).
9. Set a counter to boundary pixel
   I=1.
10. Fill boundary pixel in the new image and clip each pixel that have row value larger than 900.
    - 10.1 Check reaching the end
      If I < Boundary-Index.
    - 10.2 Get the coordinates
      X=Longest-Boundary(I,1).
      Y=Longest-Boundary(I,2).
    - 10.3 Check Y and draw pixel if Y < 900
      If Y < 900
      Result(X,Y) =1.
    - 10.4 Increase the counter
      I=I+1.

Features Extraction

The algorithm that applied to extract features is distance based features which divided in two steps, the first step is to get on the tips and valley points which found in curvature places and called reference points and second step is computed the Euclidian distances between reference points. The Euclidean distance (ED) is calculated between two points (X1, Y1) and (X2, Y2) in hand and is given by equation (1) and finally save these distances in database as a features.

$$ED = \sqrt{(X_1 - X_2)^2 + (Y_1 - Y_2)^2} \quad \text{.....(1)}$$

The tip (fingertip) point is the point that its axis is higher than neighbor pointsaxis as shown in figure (4). In our implemented system we get on 5 tip points which is the tip points of the hand finger and the normal person usually have 5 tip points(tip1,tip2,….. ,tip5).

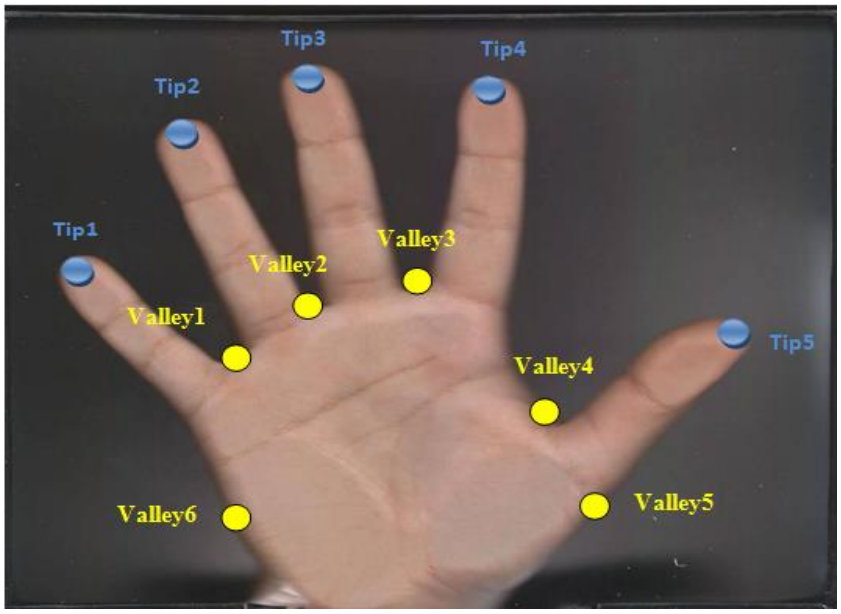

Figure (4) Tip and Valley Points

After finding the tip and valley points, the Euclidian distance has been calculated between these points and it is a fixed distance which is not changed when the status of hand is changed. These distances considered as a feature that extracted from hand image and stored into database, the number of the extracted features are 20 features (distances)(D1,D2, D3, D4,…….D20) for each hand image and since the number of hand images that taken for each person are 7 (for training) so, the number of hand features for every person are 140 features.

Training Using ANN

The artificial neural network (ANN) has been used in the implemented system to recognize system users (passport holders). The method that used is feed forward back propagation and with type Perceptron (multi layers).

This artificial network that is used in our system used the features that extracted from faces using PCA and stored into database and also use features extracted from hand using Distance based feature which stored into another database. There is a specific code number(IP) for each person that entered into database which has been supposed, the code number is a binary number that have 10 bits and it is unique for every person(the same number is supposed for face and hand for same person in databases) . The number of features (entries) to the ANN was the all 50 features extracted from face so, the number of nodes in input layer was 50 nodes and the number of hidden layer was 25 nodes and the output layer was 10 nodes as shown in figure (5)**.** While the number of entries to the ANN in hand geometry was the all 20 features extracted and there was no hidden layer and the output layer was 10 nodes as shown in figure (6).

Which means the ANN that is used in face recognition is multi layer Perceptron while the ANN using in hand geometry recognition is one layer because it doesn't have a hidden layer. In each iteration of Perceptron, the error should decrease and finally it is equal to zero. At the end the output of the neural network must equal to the code number (IP) of the person that the face image features entre to NN.

As mentioned before the faces images that used for training are 7 and the other 3 are used for testing the ANN and the same thing for hand (7 for training and 3for testing) and that means when the face or hand image (from 3 image) for a person entered into NN, the NN will be recognized these image and known this image is belong to true person that registered into

database and also could know person who don't have image in database by describing him as stranger. In that case the system will know that the NN is trained in correct way.

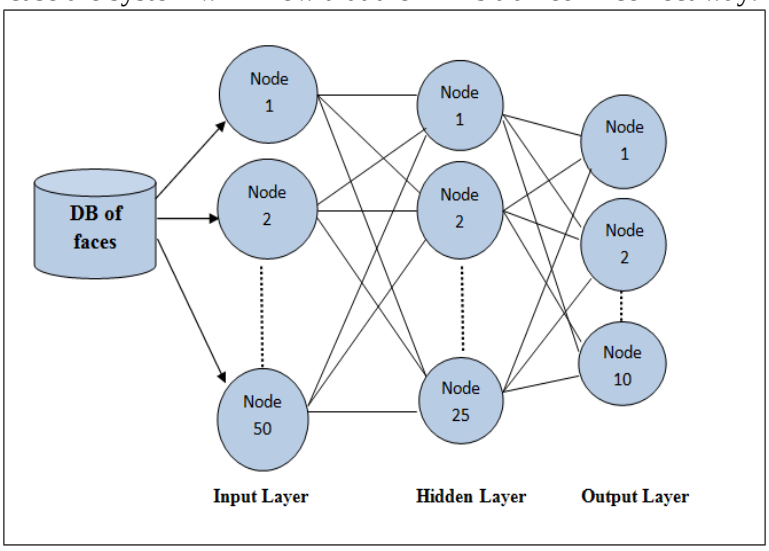

Figure (5) Training ANN on Face Images

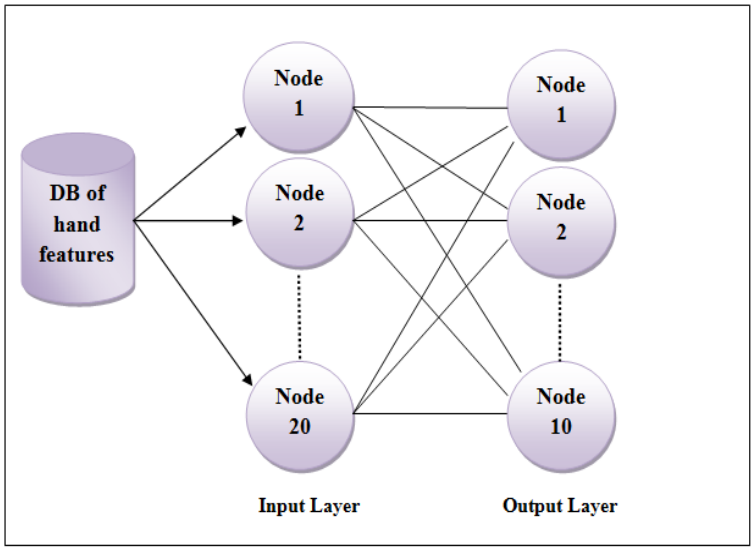

Figure (6) Training ANN on Hand Geometry

Recognition and Information Retrieving

After the ANN has been trained on recognition both face and hand, the system uses ANN to recognize persons. If a person exists into data base the system will recognize him and retrieve information which is specific for that person and stored into information database and this information are his name, address and age. On the other hand if the person is not registered into database which means that his face and hand are not exist into database and the ANN is not trained on the face and hand features, the system will tell that there is an error and ask to choose another person.

System Implementation

When the system runs, it waits for a person verify. First, the face image of the person is taken without any human intervention or attention of passenger and then hand geometry print is taken by enrollment on hand scanner. Then the system uses the current hand geometry image and face image to extract features and compares these features with features stored into database

and with hand and face features that stored on RFID chip embedded in E-passport. If this person exists in database, the system will give a match, else it gives no match and this process is repeated to each e-passport that entered into e-gate. The system implementation is illustrated in figure(7).

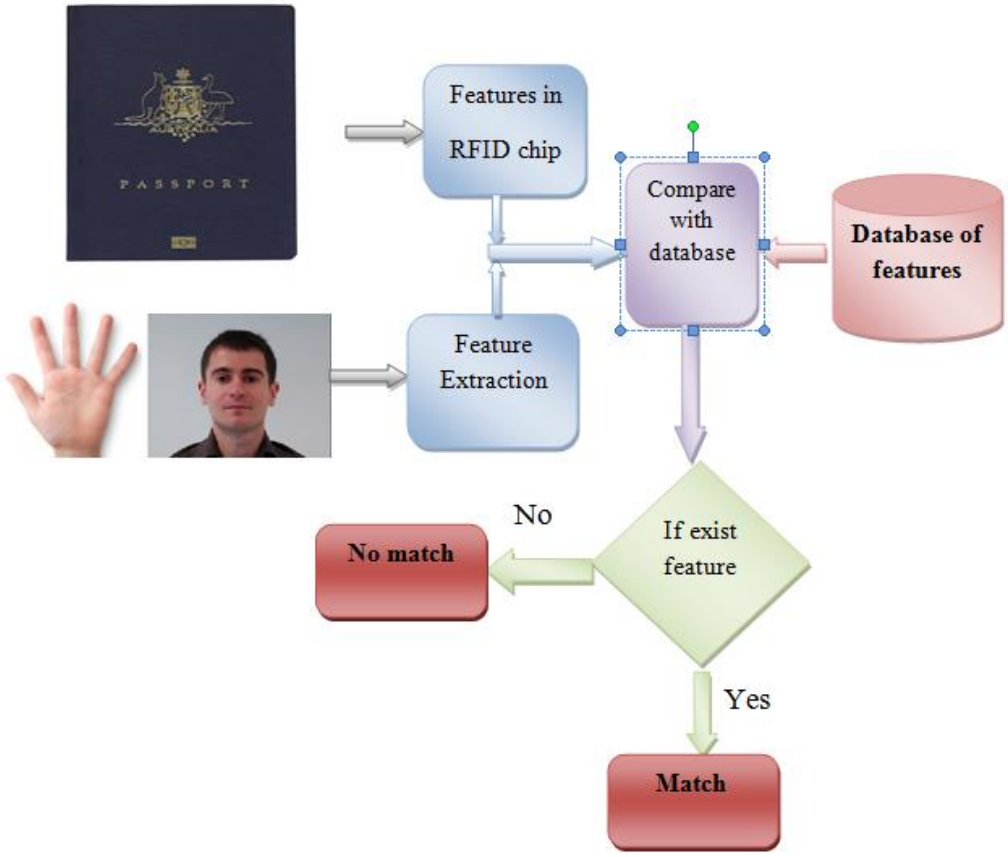

Figure (7) Block diagram of system implementation

Performance of ANN

The performance of the ANN that is used for face recognition is $8.9517e^{-07}$ at epoch 28 which is the epoch when the ANN has been trained and the time required for these 28 epochs for training the ANN on faces images is 29 minutes and 23 second.

In figure (8) where the x axis represents the epoch an y axis represents the main square error(mse) that begin with the value $10^{0}=0$ at beginning of training which is the biggest value and end with the value 10^{-6} which is the error at epoch 28 when the ANN is trained on recognition the face .

On the other hand, the best training performance of ANN that used for hand recognition is also $6.9557e^{-07}$ at epoch 580 when the ANN have been trained and the time required for these 580 epochs for training the ANN on hands images is 4 minutes and 13 second as show in figure(9)**.** Where the x axis represents the epoch and y axis represents the main square error(MSE) that begin with the value $10^{0}=0$ at beginning of training which is the biggest value and end with the value 10^{-6} which is the error at epoch 580 when the ANN is trained on recognition the hands**.**

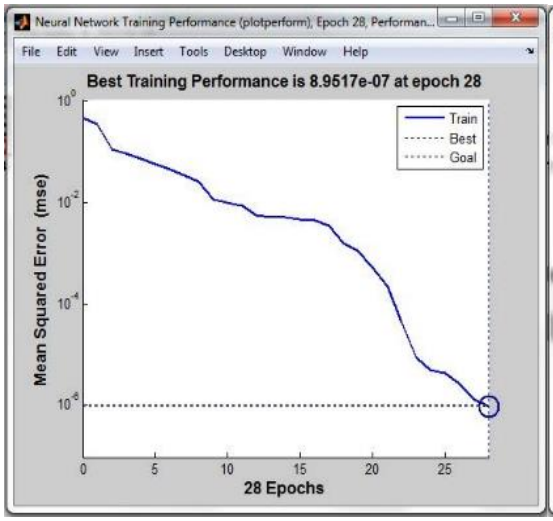

Figure (8) ANN Training for Face

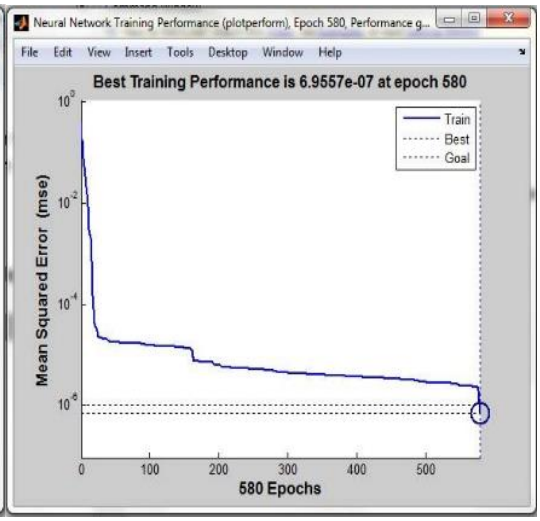

Figure (9) ANN training for Hand

CONCLUSION

The obtained results give high accuracy of recognition person using two biometric features for each person: the face and hand images to achieve the recognition, identification and security against passport forgery.

Applying PCA technique to extract features from face and distance based features method to extract features from hand give the system the power and robustness of identifying persons and retrieving their information.

Using artificial neural network (ANN) in this proposed system give a very good results of recognition both face and hand with Low percentages of error and high performance.

When collecting database for face and hand there was many thing must take into consideration like the position of person's face and the different views of face and the distance between face and camera which must be fixed and also the lighting and background. For hand image collection the status for hand on the scanner must be fixed.

REFERENCES

[1] Pablo Najera, Francisco Moyano, Javier Lopez, "Security Mechanisms and Access Control Infrastructure for e-Passports and General Purpose e-Documents", Journal of Universal Computer Science, vol. 15, no. 5, 2009.

[2] Brianne Christine Vollmer, "BIOMETRICS, RFID TECHNOLOGY, AND THE EPASSPORT:ARE AMERICANS RISKING PERSONAL SECURITY IN THE FACE OF TERRORISM?", Washington, DC, Washington, DC.

[3] Eili Bjelkåsen, Linda Walbeck Olse, "Security Issues in e-Passports- ICAO Standard and National Implementations as Part of the US Visa-Waiver Program", Agder University College Faculty of Engineering and Science, Grimstad, Norway, May 2006.

[4] Jonathan P. Chapman, Laila El Aimani, DenizSarier, "Determining the Security Enhancement of Biometrics in E-Passports", BONN-AACHEN INTERNATIONAL CENTER FOR INFORMATION TECHNOLOGY DEPARTMENT OF COMPUTER SECURITY, 2009.

[5] Anshuman Sinha, "A Survey of System Security in Contactless
Electronic Passports", arXiv, 2010.

[6] V.K. Narendira Kumar, B. Srinivasan," DESIGN AND IMPLEMENTATION OF E-PASSPORT SCHEME USING CRYPTOGRAPHIC ALGORITHM ALONG WITH MULTIMODAL BIOMETRICS TECHNOLOGY", International Journal of Advanced Information Technology (IJAIT) Vol. 1, No. 6, December 2011.

[7] Eyad Abdullah Bogari, Pavol Zavarsky, Dale Lindskog, Ron Ruhl," An Analysis of Security Weaknesses in the Evolution of RFID Enabled Passport", World Congress on Internet Security, 2012.
[8] DominikMalˇc´ık, Martin Drahansk´y, "Anatomy of BiometricPassports", Hindawi Publishing Corporation Journal of Biomedicine and Biotechnology, 2012.
[9] V.K. Narendira Kumar, Dr. B. Srinivasan ," Biometric Passport Validation Scheme using Radio Frequency Identification ", I. J. Computer Network and Information Security, 2013.
[10] Ivo Pooters, "Keep Out of My Passport: Access Control Mechanisms in E-passports", June 15, 2008.
[11] V.K. NARENDIRA KUMAR, B. SRINIVASAN, "Development of Electronic Passport Scheme for Cryptographic Security and Face, Fingerprint Biometrics using ASP.Net", I.J.Modern Education and Computer Science, 2012.
[12] V.K. NARENDIRA KUMAR, B. SRINIVASAN, "DESIGN AND DEVELOPMENT OF E-PASSPORTS USING BIOMETRIC ACCESS CONTROL SYSTEM", International Journal Of Advanced Smart Sensor Network Systems (IJASSN), Vol 2, No.3, July 2012.
[13] Ivo de Carvalho Peixinho, Auto Tavares da Camara Junior, "Evaluating the security of the Brazilian ePassportBrute force attack on the BAC protocol", ICOFCS, 2011.
[14] Marci Meingast, Jennifer King, Deirdre K. Mulligan, " Security and Privacy Risks of Embedded RFID in Everyday Things: the e-Passport and Beyond", JOURNAL OF COMMUNICATIONS, VOL. 2, NO. 7, 2007.
[15] Simson Garfinkel, Henry Holtzman, "UNDERSTANDING RFID TECHNOLOGY", Garfinkel .book, 2005.