Artificial Neural Networks Based Fingerprint Authentication

Dr. Abbas H. Issa
Electrical Engineering Department, University of Technology / Baghdad
Email:Abbas_hissa@yahoo.com

Received on:30/9/2014 & Accepted on:7/5/2015

ABSTRACT:

Fingerprint authentication and recognition is an important subject that has been widely used in various applications because of its reliability and accuracy in the process of authenticating and recognizing the person's identity. In this paper, an Intelligent Fingerprint Authentication Model (IFAM) based upon the neural network has been proposed. The proposed work consists of two main phases which are the features extraction and the authentication. The features extraction phase has been regarded via proposing a statistical and geometrical approach for determining and isolating the features of the fingerprint images. The proposed approach is called the Features Ring Approach which is abbreviated by FRA. The approach creates a circular ring centered at the core point of the fingerprint to bind the valuable features that are invariant under rotation and translation. The radius of the outer circle of the ring is suggested to be variable to give a variable area for the established circular ring.

The authentication phase of IFAM suggests the neural network to hold the job of verification of the extracted feature patterns resulted by FRA for a fingerprint image of certain person. This is done using a neural network trained with a collection of features patterns extracted from fingerprint images. Backpropagation (BP) is suggested as a training algorithm for the structured neural network.

Keywords: Authentication, Fingerprint, Gabor filter, Minutiae extraction, Artificial Neural Network, and Back-propagation.

التحقق الذكي لبصمة الاصبع اعتمادا على طريقة حلقة المميزات

الخلاصة:

تعتبر عملية التحقق والتمييز عن طريق بصمات الأصابع من المواضيع الهامة نظرا لأستخدامها على نطاق واسع في تطبيقات مختلفة بسبب وثوقيتها والدقة في عملية التحقق وتمييز هوية الاشخاص.تم في هذا العمل اقتراح نموذج تحقيق بصمة استنادا إلى الشبكة العصبية وتم الرمز له بـ IFAM. يتكون العمل من مرحلتين رئيسية هي: مرحلة استخراج الميزات ومرحلة التحقيق.تم التعامل مع مرحلة استخراج الخصائص عن طريق اقتراح مقاربة إحصائية وهندسية لتحديد وعزل ملامح الصور لبصمات الأصابع. ويسمى النهج المقترح بنهج حلقة الميزات الذي

يدعى بـ FRA. هذا النهج يخلق حلقة دائرية مركزها في النقطة الأساسية للبصمة وتحدد هذه الحلقة الميزات المهمة والمقاومة لعمليتي التدوير والانتقال لبصمة الاصبع. وقد تم اقتراح نصف قطر الدائرة الخارجية من الحلبة ليكون متغيراً للحصول على حلقة دائرية متغيرة المساحة.استخدمت الشبكات العصبية في مرحلة التحقيق للنموذج المقترح IFAMلغرض اتمام عملية التحقق من انماط المميزات المستحصلة بواسطة FRA والخاصة بصورة بصمات اصابع تابعة لشخص معين. ويتم ذلك باستخدام الشبكة العصبية المدربة اصلا على مجموعة من انماط المميزات المستخرجة من صور بصمات الاصابع الاخرى. وتم اقتراح خوارزمية الانتشار العكسي (BP) كخوارزمية التدريب الهجين للشبكة العصبية .

INTRODUCTION

Personal identity refers to a set of attributes (e.g., name, social security number, etc.) that are associated with a person. Identity management is the process of creating (linking the attributes to a physical person), maintaining and destroying identities of individuals in a population. One of the critical tasks in identity management is person authentication, where the goal is to either determine the previously established identity of an individual or verify an individual's identity claim [1].

Fingerprint is a fundamental method for the authentication of people. Fingerprint authentication is based on the immutability and individuality of fingerprints. Immutability refers to the permanent and unchanging character of the pattern on each finger from birth until death. Individuality refers to the uniqueness of ridge details across individuals. Finger ridge configurations do not change throughout the life of an individual except due to accidents such as bruises and cuts on the fingertips. This property makes fingerprints a very attractive biometric identifier [2].

In this paper, an Intelligent Fingerprint Authentication Model (IFAM) is proposed. Initially, fingerprint image is first enhanced by using Gabor filter, and then minutiae is extracted from the enhanced fingerprint image and produces feature set by geometrical and statistical approach based on core point and minutiae. The extracted features are fed to a neural network trained by Backpropagation (BP) algorithm.

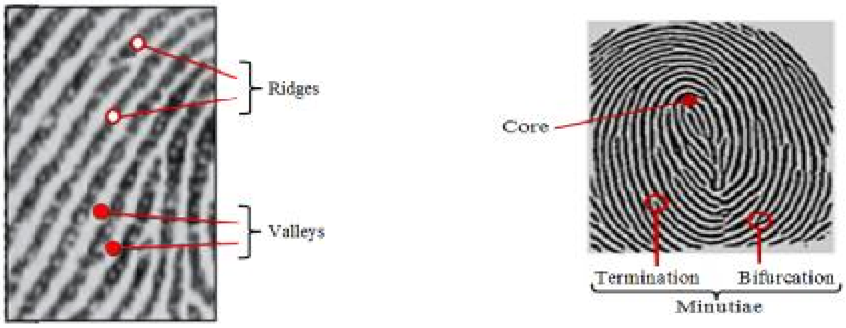
The approach is called the Features Ring Approach FRA and features is depends on core and minutiae point location, Suzan A. et al. [3] proposed a triangle shapes to extract features based on minutiae point, the features have been used as a set of descriptors for the fingerprint data and the set of descriptors was fed to the backpropagation neural network for the purpose of fingerprint recognition. Md. Mamunur et al. [4] presented filter feature of graphics editor and extracting the minutiae feature, then transforming the fingerprint image to 480x360 pixel images by minutiae location and the verification system based on ANN using backpropagation algorithm. Ju Cheng Yang et al. [5] proposed a system to detect a unique reference point to determine a Region-of-Interest (ROI) then a total of four sets of seven invariant moment features are extracted from four partitioned sub-images of an ROI and the matching use nonlinear Back Propagation Neural Network (BPNN).

The rest of this paper is organized as follows. In section II, the fingerprint representation and features are presented. Artificial neural network and Back-propagation algorithm are described in section III and IV. In section V, the proposed authentication model with the two phases which are the features extraction and the authentication are explained in details. Experimental results are shown in section VI. Finally, conclusions are given in section VII.

Fingerprint Representation and Features

A fingerprint is the reproduction of the exterior appearance of the fingertip epidermis. The most evident structural characteristic of a fingerprint is a pattern of interleaved ridges and valleys. In a fingerprint image, ridges (also called ridge lines) are dark whereas valleys are bright as shown in Figure (1-a) [2].

At the global level detail includes the general ridge flow and pattern configuration, which often run in parallel but exhibit one or more regions where they assume distinctive shapes (singular region**)** characterized by high curvature called core and delta . At the local level, other important features, called minutiae can be found in the fingerprint patterns. Minutia refers to the various ways in which the ridges can be discontinuous. For example, a ridge can abruptly come to an end (termination), or can divide into two ridges (bifurcation) [6] as shown in Figure (1-b).



(a) (b)

Figure (1) Fingerprint image (a) Ridges and valleys (b) Core and minutiae

Proposal Model

The Intelligent Fingerprint Authentication Model (IFAM) is proposed and designed to be consist of two main phases: features extraction phase and authentication phase. Figure (2) shows the block diagram of the proposed model.

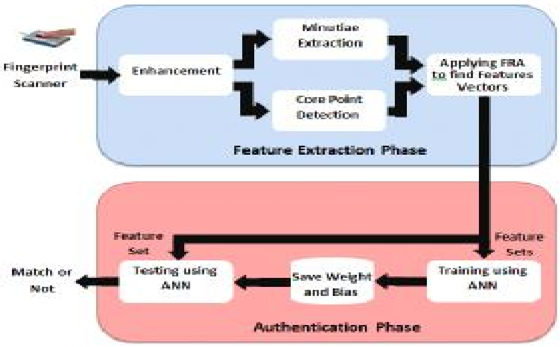


Figure (2) The block diagram of the proposed IFAM.

Features Extraction Phase

This phase treats and enhances the fingerprint image to extract its features. This paper proposes the Features Ring Algorithm (FRA) to determine and isolate the more interesting features to be fed to the next phase. To extract features vector of fingerprint, four stages must be performed which are:

- Enhancement
- Minutiae extraction
- Core point detection
- Applying FRA to determine the features vectors

1.1 Image enhancement

Enhancement technique is used to reduce the scanner noise and enhance the definition of ridges against valleys. Figure (3) shows the conceptual diagram of the fingerprint enhancement. The main steps include image segmentation, normalization and filtering.

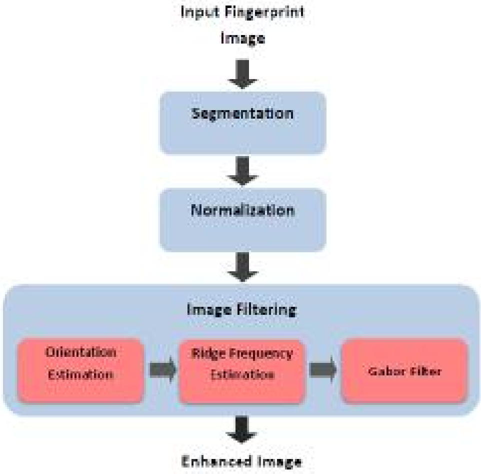


Figure (3) The conceptual diagram of the fingerprint enhancement

i) Segmentation

The term segmentation is generally used to denote the separation of fingerprint area (foreground) from the image background. Separating the background is useful to avoid extraction of features in noisy areas that is often the background**.**

Basically, the segmentation can be performed using a method based on variance threshold. Firstly, the image is divided into blocks and the grey-scale variance is calculated for each block in the image. If the variance is less than the global threshold, the block is assigned to be a background region; otherwise, it is assigned to be part of the foreground. The grey-level variance for a block of size *W*×*W* is defined as [7]:

$$V(k) = \frac{1}{W^2}\sum_{i=0}^{W-1}\sum_{j=0}^{W-1}(I(i,j) - M(I))^2 \qquad ...(1)$$

Where

V(k) is the variance for block *k*, *I(i, j)* is the grey-level value at pixel (*i*, *j*), *M(I)* is the mean grey-level value for the block *k* as shown in equation (2).

$$M(I) = \frac{1}{W^2}\sum_{i=0}^{W-1}\sum_{j=0}^{W-1} I(i,j) \qquad \ldots(2)$$

ii) Normalization

Normalization is a pixel-wise operation and does not change the ridge and valley structures. Normalization is used to standardize the intensity values in an image by adjusting the range of grey-level values so that it lies within a desired range of values**.**
Let *I* (*i*, *j*) represent the grey-level value at pixel (*i*, *j*), and *N* (*i*, *j*) represent the normalized grey-level value at pixel (*i*, *j*). The normalized image is defined as [8]:

$$N(i,j) = \begin{cases} M_0 + \sqrt{\dfrac{V_0(I(i,j)-M)^2}{V}} & if\ I(i,j) > M, \\ M_0 - \sqrt{\dfrac{V_0(I(i,j)-M)^2}{V}} & otherwise \end{cases} \qquad \ldots(3)$$

Where
M and *V* are the estimated mean and variance of *I*(*i*, *j*), respectively, and M_0 and V_0 are the desired mean and variance values, respectively.

iii) Image filtering

Filtering is used for preserving the true ridge and valley structures of the fingerprint. Image filtering is performed by using Gabor filter which is tuned to local ridge orientation and ridge frequency.
The orientation image represents an intrinsic property of the fingerprint images and defines invariant coordinates for ridges and furrows in a local neighborhood.
The orientation field of a fingerprint image defines the local orientation of the ridges contained in a fingerprint. Given a normalized image, the steps for calculating the orientation at pixel *(i, j)* are as follows [9]:

- Divide the normalized image into blocks of size *w*×*w*.
- For each pixel in the block, compute the gradients $G_x(i, j)$ and $G_y(i, j)$, which are the gradient magnitudes in the *x* and *y* directions, respectively. The horizontal Sobel operator is used to compute $G_x(i, j)$ and the vertical Sobel operator is used to compute $G_y(i, j)$.
- The local orientation at pixel *(i,j)* can then be estimated using the following equations:

$$\mathcal{V}_x(i,j) = \sum_{u=i-\frac{W}{2}}^{i+\frac{W}{2}}\sum_{v=j-\frac{W}{2}}^{j+\frac{W}{2}} 2G_x(u,v)G_y(u,v), \qquad \ldots(4)$$

$$\mathcal{V}_y(i,j) = \sum_{u=i-\frac{W}{2}}^{i+\frac{W}{2}} \sum_{v=j-\frac{W}{2}}^{j+\frac{W}{2}} \left(G_x^2(u,v) - G_y^2(u,v)\right), \qquad \dots(5)$$

$$\theta(i,j) = \frac{1}{2} tan^{-1}\left(\frac{\mathcal{V}_y(i,j)}{\mathcal{V}_x(i,j)}\right) \qquad \dots(6)$$

Where

$\theta(i,j)$ is the estimated orientation of the block centered at pixel *(i, j).*

In addition to the orientation image, another important parameter that is used in the construction of the Gabor filter is the local ridge frequency. The frequency image represents the local frequency of the ridges in a fingerprint.

The first step in the frequency estimation stage is to divide the image into blocks of size *w*×*w*. The next step is to project the grey-level values of all the pixels located inside each block along a direction orthogonal to the local ridge orientation. This projection forms an almost sinusoidal-shape wave with the local minimum points corresponding to the ridges in the fingerprint. The ridge spacing *S*(*i, j*) is then computed by counting the median number of pixels between consecutive minima points in the projected waveform. Hence, the ridge frequency *F*(*i,j*) for a block centered at pixel (*i, j*) is defined as [10]:

$$F(i,j) = \frac{1}{S(i,j)} \qquad \dots.(7)$$

Once the ridge orientation and ridge frequency information has been determined, these parameters are used to construct the even-symmetric Gabor filter. A two-dimensional Gabor filter consists of a sinusoidal plane wave of a particular orientation and frequency, modulated by a Gaussian envelope.

The even-symmetric Gabor filter which is given by a cosine wave modulated by a Gaussian. An even symmetric Gabor filter in the spatial domain is defined as [8, 10]:

$$g(x,y{:}\,\theta,f) = exp\left\{-\frac{1}{2}\left[\frac{x_\theta^2}{\sigma_x^2} + \frac{y_\theta^2}{\sigma_y^2}\right]\right\}.\cos(2\pi f.x_\theta) \qquad \dots(8)$$

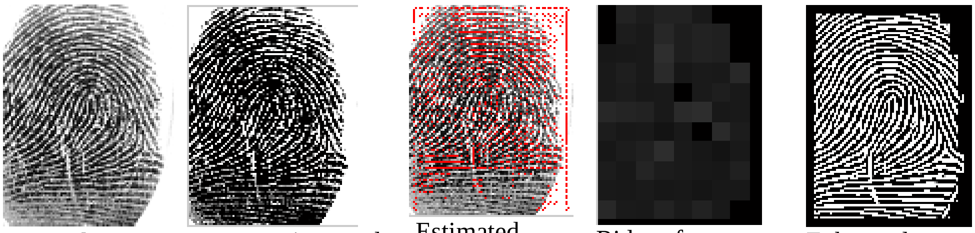
$$x_\theta = x\cos\theta + y\sin\theta \qquad \dots(9)$$

$$y_\theta = -x\sin\theta + y\cos\theta. \qquad \dots(10)$$

where

θ is the orientation of Gabor filter, *f* is the frequency of a sinusoidal plane wave, σ_x and σ_y are the standard deviations of the Gaussian envelope along the *x* and y axes and x_θ and y_θ

define the x and y axes of the filter. The result of image enhancement process can be shown in Figure (4).


Original Image

segmentation and normalization Image

Estimated orientation.

Ridge frequency estimation

Enhanced image

Figure (4)The result of image enhancement process using Gabor filter

Minutiae Extraction

Minutiae extraction process requires the fingerprint gray-scale image to be converted into a binary image. The binary images are usually submitted to a thinning stage which allows for the ridge line thickness to be reduced to one pixel. A simple image scan then allows the detection of pixels that correspond to minutiae. Figure (5) shows the block diagram of the minutiae extraction process.

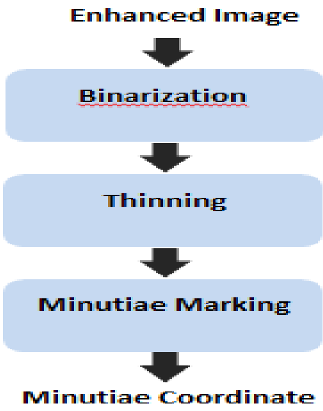


Figure (5) The conceptual diagram of the minutiae extraction

i) Binarization

The binarization process is used to convert gray-scale image into binary image. This process transforms the 8-bit Gray image to a 1-bit image with 0-value for ridges and 1-value for valley. This involves examining the grey-level value of each pixel in the enhanced image, and, if the value is greater than the global threshold, then the pixel value is set to a binary value one, otherwise, it is set to zero. The outcome is a binary image containing two levels of information, the foreground ridges and the background valleys [8,11].

ii) Thinning

Thinning is a morphological operation that successively erodes away the foreground pixels until they are one pixel wide. A standard thinning algorithm is used, which performs the thinning operation using two sub iterations. Each sub iteration begins by examining the neighborhood of each pixel in the binary image, and based on a particular set of pixel-deletion criteria, it checks whether the pixel can be deleted or not. These sub iterations continue until no more pixels can be deleted. The thinning algorithm will produce a skeletonized version of the binary image. This skeleton image is then used in the subsequent extraction of minutiae [8].

iii) Minutiae marking

In general, minutia points are detected by locating the end points and bifurcation points. The minutiae are marked by scanning the local neighborhood of each ridge pixel in the image using a 3x3 window.

Let p denote as a central pixel on a thinned ridge, and p_0, p_2, ..., p_7 are pixel belonging to an order sequence of pixels defining the eight neighborhood of p and $val(p_i)$={0,1} is the pixel value. It's simple to note that a pixel p with $val(p)$=1 as shown in Figure (6) [11] .

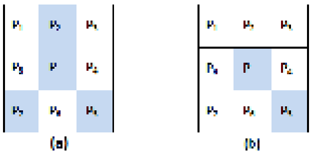


Figure (6) Examples of a ridge ending and bifurcation pixel.
(a) bifurcation pixel (b) ending pixel

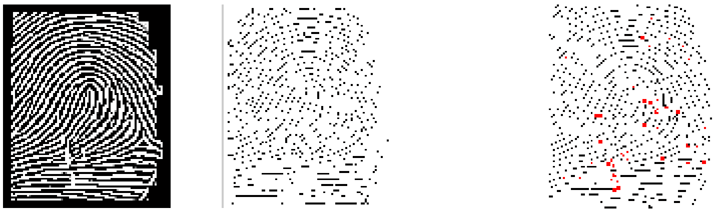
- If the sum of the pixels of the 8-nighborhhood of p equal 1, it is a ridge ending such as:

$$\sum_{i=1}^{8} val(p_i) = 1 \qquad \text{... (11)}$$

- If the sum of the pixels of the 8-nighborhhood of p equal 3, it is a ridge bifurcation such as:

$$\sum_{i=1}^{8} val(p_i) = 3 \qquad \text{.... (12)}$$

The results of minutia extraction process shown in Figure (7).



Enhanced image **Binarization and thinning** **Minutia marking**

Figure (7) The results of minutia extraction process

Core point determination

The core point is defined as "the point of the maximum curvature on the convex ridge," which is usually located in the central area of fingerprint. The majority of approaches for detecting the position of the reference point based on the orientation field of the image by searching the maximum curvature point from the orientation image.

Core point detection can be done using orientation coherence which describes the consistency of the local orientations in the neighborhood along the dominant orientation. The orientation coherence is poor in the high curvature ridge flows, while it is maximum for a smooth and parallel ridge flows. This algorithm is to detect a unique reference point consistently for all types of fingerprints [12].

Core point detection according to orientation coherence can be done by applying the following steps:

- Divide the normalized image into blocks of size $w \times w$.
- For each block centered at pixel *(i, j)*, compute the estimted orientation $\theta(i,j)$ using equation (13).
- Compute the orientation coherence

$$Coh = \frac{\left(\sum_i \sum_j \cos\left(2\theta(i,j)\right)\right)^2 + \left(\sum_i \sum_j \sin\left(2\theta(i,j)\right)\right)^2}{M} \qquad \dots(13)$$

Where

M is the number of orientations in the taken window.

If the current block was with local minimum coherence, then assign that block as a core point. The results of core point detection shown in Figure (8).

Figure (8) The results of core point detection

Features Ring Approach

The proposed Features Ring Approach (FRA) which is a statistical and geometrical approach is suggested to be applied for IFAM after marking the minutiae. FRA is used to;

Detect and discriminating the more interested features (minutiae) of the already enhanced fingerprint image, Produce the features vector to be fed to the authentication phase which is the second phase of IFAM model, and assure the fingerprint sample to be invariant against the translation, rotation problems. Figure (9) shows the operation steps of FRA.

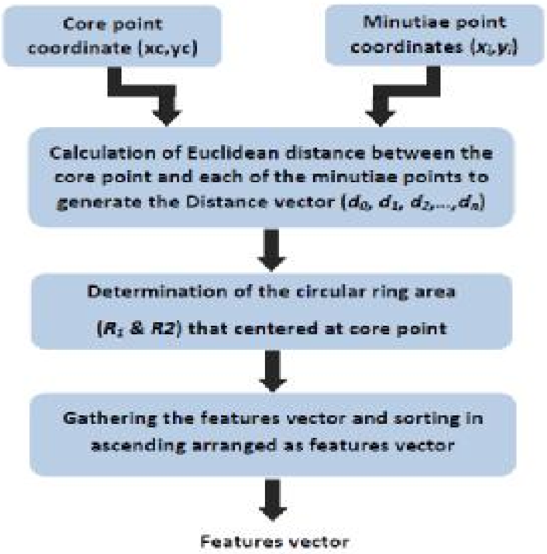

Core point coordinate (xc,yc)
Minutiae point coordinates (x_i,y_i)
Calculation of Euclidean distance between the core point and each of the minutiae points to generate the Distance vector (d_0, d_1, d_2,...,d_n)
Determination of the circular ring area (R_1 & $R2$) that centered at core point
Gathering the features vector and sorting in ascending arranged as features vector
Features vector

Figure (9) Operation steps of FRA.

The detailed steps for FRA are as follows:

1) Calculate the distance between the coordinates of each of the core point and minutiae points using Equation (14).

$$d_i = \sqrt{(x_c - x_i)^2 + (y_c - y_i)^2} \qquad \dots (14)$$

Where

(x_i,y_i) is the coordinates of the minutiae point For $i=0,1,\dots,n$, and (x_c,y_c) is the core point coordinate. The calculated distance,(d_i) will be sorted in ascending order and the produced distance vector, (d_0,d_1, d_2,…,d_n) , will be the intuitive vector of the fingerprint features.

2) Determine the circular ring area centered at the core point using the intuitive vector of features. The determined area will be with radii R1 and R2 and will bind the more interested features of the fingerprint as shown in Figure (10).

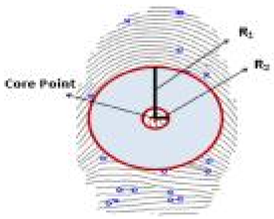


Figure (10) Circular ring area

The two radii R_1 and R_2 of the circular ring must be calculated by using the minimum distance d_{min} and the maximum distance d_{max} :

$$d_{min} = d_0$$
$$d_{max} = d_n$$

where d_0 and d_n are the minimum and maximum elements of the ascended intuitive features vector. The radius of the inner circle R_1 equal to d_{min}, while the outer radius, R_2 can be calculated as follows:

$$R_{2\,=}\ k \times (d_{max}\text{-}d_{min}) + d_{min} \qquad \ldots(15)$$

Where

k represents the floating factor and falls in the range $1 \leq k \leq 0$. Figure (11) shows the change in the area of the circular ring corresponding to the floating factor k.

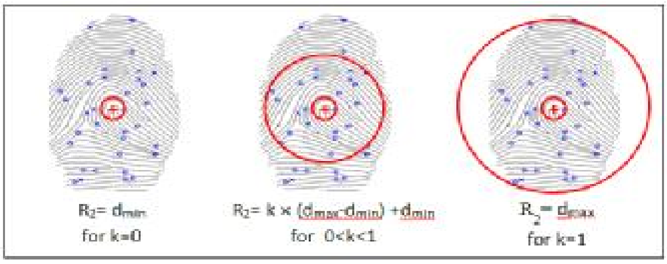


Figure (11) The change in the area of the circular ring corresponding to the floating factor *k*.

3) Gather the more interested features through establishing a boundary around the minutiae (in the form of distances) of the fingerprint as shown in Figure (12). These features can be sorted in ascending and arranged as features vector to be delivered to the next step of the proposed authentication model IFAM.

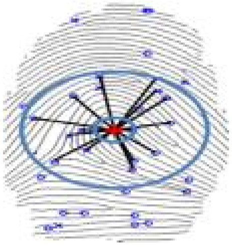


Figure (12) Feature ring

Authentication phase

This phase using the resulted features vector as an input to the Artificial Neural Network (ANN). After obtaining the features vector for fingerprint image in the first phase, IFAM will train the neural network with all the feature vectors of known fingerprint samples and store the adjusted weights values in a file. After that, IFAM will authenticate the individual by testing the unknown fingerprint sample after extract the feature vector.

1. Artificial Neural Network

Artificial Neural Network (ANN) has been applied to solve many problems. Learning, generalizations, less data requirement, fast computation, ease of implementation, and software and hardware availability features have made ANNs very attractive for the applications. These fascinating features have also made them popular in fingerprint authentication. It is a mathematical or computational model based on biological neural networks. An ANN consists of several simple units called “neurons” or artificial neurons, which are interconnected together and operate in parallel to process information, thus, known as parallel distributed processing systems or connectionist systems [13].

In most cases an ANNs are employed to solve Artificial Intelligence (AI) problems. Multilayered is one of the most popular ANN architectures used in biometrics authentication. Its structures consisting of three layers: input, output and hidden layers. One or more hidden layers might be used. The weights are adapted with the help of a learning algorithm according to the error occurring in the calculation. The error can be calculated by subtracting the ANN output from the desired output [14].

2. Back-propagation algorithm

The Back-Propagation (BP) algorithm was proposed in 1986 by Rumelhart, Hinton and Williams for setting weights and hence for the training of Multi-Layer Perceptron (MLP) [15].

Back-Propagation (BP) also referred to as “propagation of error” is a supervised learning method. It requires a teacher that knows, or can calculate, the desired output for any given input. In BP, the errors propagate backwards from the output nodes to the inner nodes. Back-propagation is widely used to calculate the error of the network with respect to the network's modifiable weights.

The network propagates the input from layer to layer until the output is generated by the output layer. If the pattern is different from the desired output, an error is calculated in each output neuron and then it is propagated backwards through the network from the output layer to the input layer. The weights of each neuron are adjusted as the error is propagated [13].

3. Design of Neural Network Structure

The suggested neural network structure is shown in Figure (13). This ANN is a feed forward multi-layer network with three layers (input, hidden, and output layers). The number of neurons in the input layer (*n*) is assigned due to the dimension of the feature vectors used. . The number of neurons in the output layer (*o*) which is represented as a binary output was decoded and assigned due to the number of persons. The number of neurons in the hidden layer (*h*) is based on the trial and error which is one of many approaches may be applied to assign the suite number for the hidden neurons.

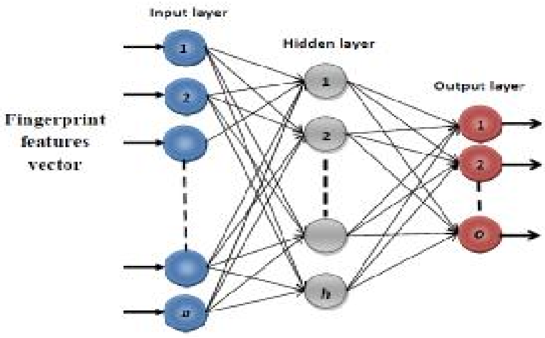


Figure (13) The structure of the NN.

4. Training the Designed Neural Networks

Training of a neural network is a process of determining the network parameters (weights and biases). When the training process is completed for the training data set, the updated weights and biases values were saved in a file to be ready for the testing procedure.

The weights of the neural network are adapted with the help of BP learning algorithm. In training using BP algorithm, ANN produces the output values after each iteration, and each iteration is referred to as an epoch. After each epoch, the learning error (Mean Squared Error (MSE) or Sum Squared Error (SSE)) of the network is evaluated to show if it has reached a minimum. The learning process continues on epoch by epoch until an arrangement of weights and biases produce the minimal error for a problem [16].

Experimental Results

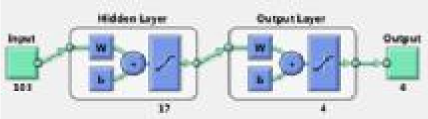
The fingerprint images for experiment were collect 80 samples from 10 persons using the ZK-4000 optical scanner. Eight fingerprints from each person were captured; five of them were used for training, while the rest three fingerprints were considered for testing. Therefore, total number of fingerprint training samples 50 and total number of fingerprint testing samples 30.

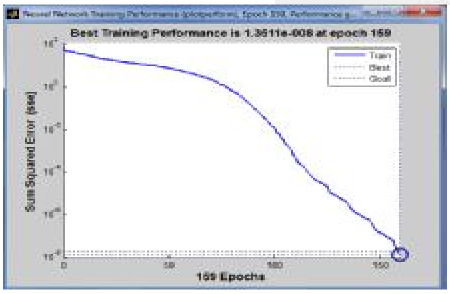
To evaluate the performance and achievement of IFAM, five cases have been suggested with respect to the floating factor *k* of equation (15). The five different values for factor *k* were taken to be (0.9, 0.8, 0.7, 0.6 and 0.5). An individual ANN model is designed for each of the five cases while, each network has *n* inputs, *h* hidden, and *o* output nodes (*n*-*h*-*o*).

Before training the weight and bias were initialized, while the used training algorithm was Bayesian Regulation, the performance is measured by SSE. Figure (14-a) shows the performance plot of the training error of ANN for each of the previously mentioned five cases. The figure shows how the algorithm tries to converge to a sum squared error to reached the goal error that represented by the dotted line in the plot.

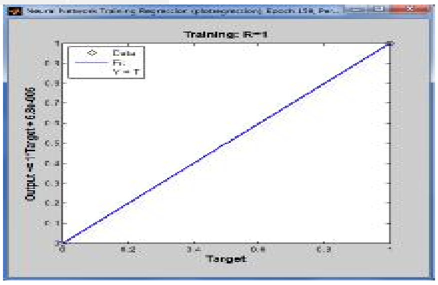
Figure (14-b) shows the regression plots for each of the five cases. The regression plots are used to validate the network performance. These plots display the network outputs with respect to targets for training set. For a perfect fit, the data should fall along a 45 degree line, where the network outputs are equal to the targets. For these three cases, the fit is reasonably good, with R values in each case equal 1 means that the training accuracy percentage is %100.

Case1(*k*=0.9)



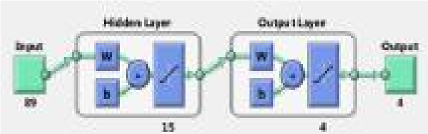


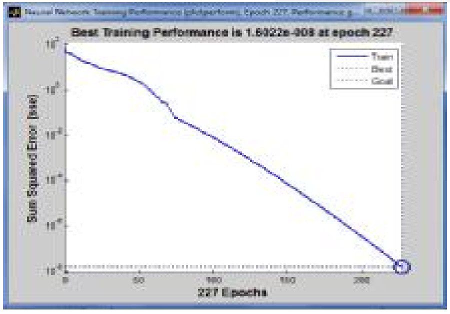
(a) Performance plot



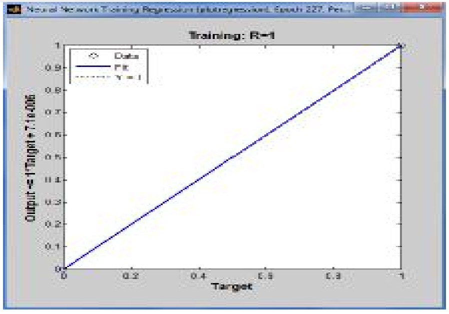
(b) Regression plot

Case2(*k*=0.8)



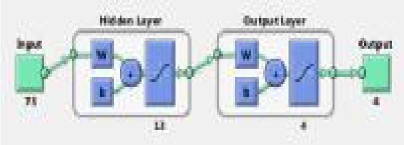


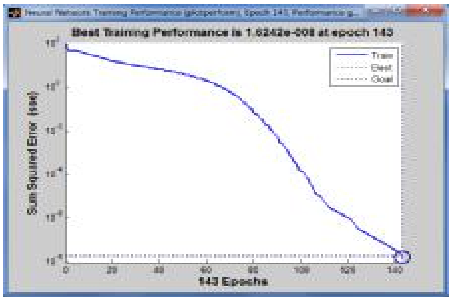
(a) Performance plot

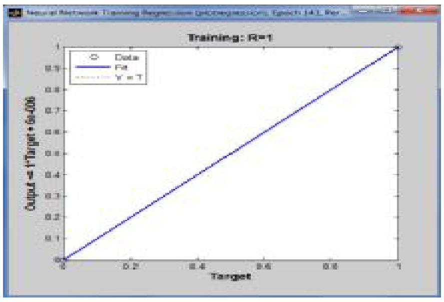


(b) Regression plot

Case3(*k*=0.7)

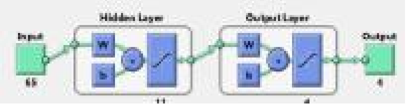


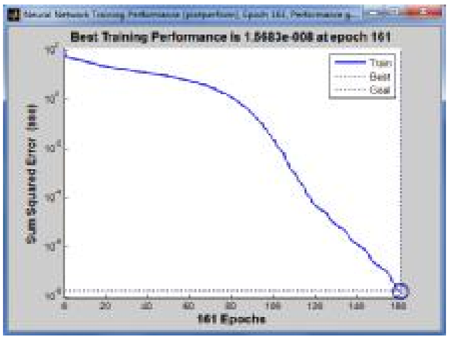


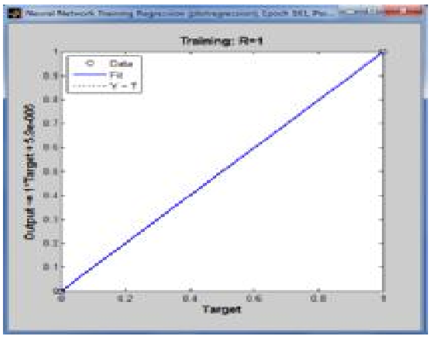


(a) Performance plot (b) Regression plot

Case4(*k*=0.6)

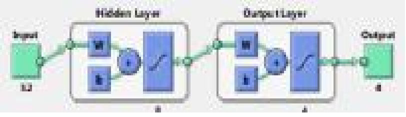


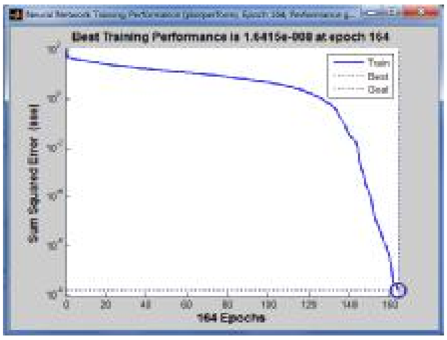


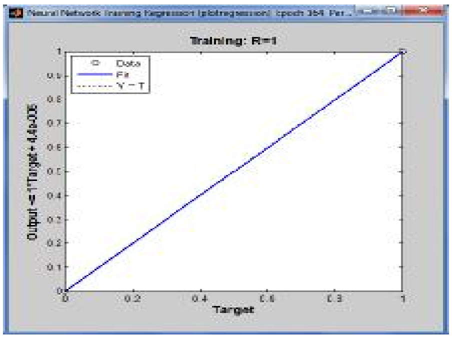


(a) Performance plot (b) Regression plot

Case5(*k*=0.5)







(a) Performance plot (b) Regression plot

Figure (14) Performance plot and Regression plot for training ANN

The same resultant training set of weights was used for testing the network with the aid of the testing sets or patterns. The testing accuracy of the five cases was calculated and illustrated in Table (1) through applying Equation (16):

$$Accuracy\ (\%) = \frac{N_c}{N_t} \times (100\%) \qquad \ldots.(16)$$

where N_c denotes to the number of correct fingerprints, while N_t is the total number of fingerprints.

Table (1): The effect of *k factor* on testing accuracy

	k factor	ANN Structure (n-h-o)	Testing accuracy 100%
Case1	0.9	103-17-4	85
Case2	0.8	89-15-4	91.25
Case3	0.7	73-13-4	90
Case4	0.6	65-11-4	81.25
Case5	0.5	52-8-4	76.25

The evaluation for the floating factor *k* which is used by the features extraction proposal, FRA, is shown in Figure (15). This figure shows the relation between the accuracy and factor *k* for five different values (0.9, 0.8, 0.7, 0.6, and 0.5), and the result of the test indicates that the best testing accuracy is 91.25 % and 90% when a factor *k* is 0.8 and 0.7 respectively.

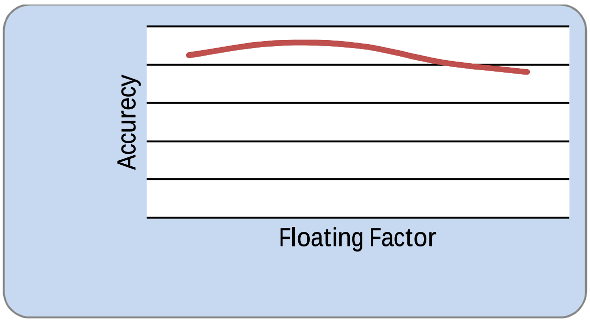


Figure (15): The relation between the accuracy and floating factor *k*

CONCLUSIONS

In this paper, a model for fingerprint authentication based on ANN with statistical and geometric approach is proposed. Using the fingerprint feature extraction, FRA (which is depending on the distance) gives us very attractive results. This is because the distance is a fixed value, and not changes with different situation of finger like rotation or translation. Furthermore, the determination of the circular ring region in fingerprint image makes the system depends on a fixed region every time the person logs into the proposed model and not on the overall image due to the change in fingerprint situations like transformation and rotation which makes the operation of extracting the same features every time an impossible matter. The experimental results have shown that the average of the best testing is 90.625% and this result improves the robust and the reliability of our proposed method.

REFRENCES

[1] Karthik N. “Multibiometric Systems: Fusion Strategies and Template Security” Ph.D. Thesis, Michigan State University, 2008.

[2] Daved M. et al, “Handbook of Fingerprint Recognition”, Springer, 2nd Edition, New York, 2009.

[3] Suzan A. Mahmood and Amera I. Melhum, “An Authentication System using Fingerprint Minutiae Extraction and Neural Network”, Journal of Al-Nahrain University, Vol. 13, No. 4, pp. 216-220, December, 2010.

[4] Md. M. R. and A. K. M. Aktar Hossain, “Fingerprint Verification System using Artificial Neural Network”, Information Technology Journal, Vol.5, No. 6, pp. 1063-1067, 2006.

[5] Ju C. Y. et al, “Fingerprint Verification Based on Absolute Invariant Moment Features and Nonlinear BPNN”, International Journal of Control, Vol.8, No. 6, pp. 800-808, 2008.

[6] Anil K. Jain et al, “Handbook of Biometrics”, Springer, 2008.

[7] Iwasokun G. Babatunde et al, “Fingerprint Image Enhancement: Segmentation to Thinning”, International Journal of Advanced Computer Science (IJCSE), Vol. 3, No. 1, 2012.

[8] A. El-Sisi, “Design and Implementation Biometric Access Control System using Fingerprint for Restricted Area Based on Gabor Filter”, The International Arab Journal of Information Technology, Vol. 8, No. 4, 2011.

[9] Jayant V. Kulkarni et al, “Orientation Feature for Fingerprint Matching” Elsevier, Pattern Recognition (PR) (39), No. 8, pp. 1551-1554, March, 2006.

[10] Raymond T., “Fingerprint Image Enhancement and Minutiae Extraction”, School of Computer Science and Software Engineering, University of Western Australia, 2003.

[11]Sachin H. et al., “Minutiae Fingerprint Recognition using Hausdorff Distance”, UNIASCIT, Vol. 1, No. 1, pp. 16-22, 2011.

[12] Xudong J. et al, “Reference Point Detection for Fingerprint Recognition,” IEEE, in 17th International Conference on Pattern Recognition, 2004.

[13] Jawad N., “An Intelligent System for Detection of Non-Technical Losses in Tenaga National Berhad (TNB) Malaysia Low Voltage Distribution Network”, M.Sc. Thesis, University of Tenaga National, 2009.

[14] Seref S.and Necla O,“An Intelligent Face Features Generation System from Fingerprints”,Turk. J. Electrical Engineering and Computer Science,Vol.17,No.2, 2009.

[15] Daniel G., “Principle of Artificial Neural Networks”, 2nd Edition, World Scientific, 2007.

[16] Natalie R. F., “Swarm Intelligence for Autonomous UAV Control", M.Sc. Thesis, Naval Postgraduate School, June, 2005.