Information Security in E-Learning through Identification of Humans

Hassan Haleh, Zohreh Nasiri and Parisa Farahpour

Abstract—During recent years, the traditional learning approaches have undergone fundamental changes due to the emergence of new technologies such as multimedia, hypermedia and telecommunication. E-learning is a modern world phenomenon that has come into existence in the information age and in a knowledge-based society. E-learning has developed significantly within a short period of time. Thus it is is of a great significant to secure information, allow a confident access and prevent unauthorized accesses. Making use of individuals' physiologic or behavioral (biometric) properties is a confident method to make the information secure. Among the biometrics, fingerprint is more acceptable and most countries use it as an efficient methods of identification. This article provides a new method to compare the fingerprint comparison by pattern recognition and image processing techniques. To verify fingerprint, the shortest distance method is used together with perceptronic multilayer neural network functioning based on minutiae. This method is highly accurate in the extraction of minutiae and it accelerates comparisons due to elimination of false minutiae and is more reliable compared with methods that merely use directional images.

Keywords—Fingerprint, minutiae, extraction of properties, multilayer neural network

I. INTRODUCTION

IT and all its related fields are the most heated discussions of public and scientific meetings of the previous years so that everyone seeks to use the hidden knowledge of this industry. Some of IT related fields are e-learning, electronic commerce, electronic management, and electronic health. Electronic education is a fruit resulted from applying IT for educational purposes. E-learning is performed through network communication and using electronic tools. Information security and preventing unauthorized accesses are of great importance in network communications. The traditional security and identification methods such as passwords cannot be reliable anymore and are not able to satisfy the present security demands. Biometric technology is one of the newly emerged technologies that can meet the demand. Among biometric technologies, fingerprint is the most important physiologic indicator used for identification purposes. Each fingerprint image includes raised and hollow grooves. To compare two fingerprints, some characteristics of the two images should be compared with each other. So far various characteristics are suggested to compare fingerprints,

Faculty Of Mechanical & Industrial Engineering, Islamic Azad University ,Qazvin Branch, Qazvin ,Iran (Tel : +98-281-367-0051; E-mail: hhaleh@qiau.ac.ir

including sweat pores exist inside the grooves. This method requires images of high accuracy that are costly and time consuming. Most fingerprint comparison systems are based on comparison of minutiae [3, 4, and 5]. Minutiae are known as Glaton characteristics. Minutiae are formed by joining of two raised grooves. The beginning and end of a raised groove also are from minutiae. [6] Sometimes, it is hard to identify a fingerprint due to the breakage of the grooves, difficulty of making distinction between two close grooves, the unevenness of the grooves, fingerprint defects caused as a consequence of a wound or burning, and imperfect recording of the image. Thus, it is usually compulsory to improve the image before finding the minutiae [7, 8, and 9]. In part 2 of this article, histogram equalization, Laplace & Fourier transform, and median filter are discussed as methods applicable to enhance the image quality , part 3-1 discusses how to make a binary image, part 3-2 is about normalization of an image and in part 3-3 the image is segregated from the background. Part 3-4 provides us with the directional pattern of the image. Gabor filter is applied on the image in part 3-5. In part 3-6, the image skeleton is extracted and in part 3-7 the minutiae are made clear using perceptronic multilayer neural network. Part 3-8 deals with elimination of the false minutiae and part 3-9 deals with fingerprints comparison. Section 4 and 5 provide you with the experimental findings and conclusion.

II. FINGERPRINT QUALITY ENHANCEMENT

To process the fingerprint image and prepare it for comparison operation, it should be of a desirable quality and thus the quality should be enhanced. In practice, due to the factors effective on fingerprint images, some of these images are weak in quality and the grooves are not definable. The identification of the fingerprint may be problematic due to the following reasons: poor camera adjustment, nonlinear sensors, or movement of camera

Thus, first the fingerprint images should be enhanced to allow clear defining of minutiae. Due to the static nature of fingerprint, application of single filter may not be enough and to enhance the quality various methods should be used.

A. Histogram equalization

Histogram of an image shows the way pixels are distributed in an image by illustrating the frequency chart based on the color intensity level. Through equalization of the histogram, the image is enhanced and changes in a way that to open the

histogram (equation 2).

$$q = \tau(p) \qquad (1)$$

$$\sum_{i=0}^{k} G(q_i) = \sum_{i=0}^{k} H(p_i) \qquad (2)$$

B. Fourier transform

After equalization of the image, the two dimensional Fourier method is applied. To do this we follow formula (3). For this, 32×32 blocks are used and the value of f equals 0.000001.

F=FFT2 (imgw(k,l)),(k,l)=LocalBlock(k,l) of image

$$\text{Factor}= |F|^f , f \in [0,1] \qquad (3)$$

imgEnhancedBlock =Histeq(IFFT2(F×factor))

Fig. 1 image after application of Fourier transforms

C. Laplace filter

The major advantage of this filter is that it enhances the edges. Equation 4 represents Laplace filter.

$$L(x,y) = \frac{\partial^2 I}{\partial x^2} + \frac{\partial^2 I}{\partial y^2} \qquad (4)$$

Where I is the image matrix, ∂x represents gradient in the direction of X axis and ∂y represents gradient in the direction of Y axis. The matrix used in Laplace filter is illustrated in figure 2.

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & -8 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

Fig. 2 matrixes applied in Laplace filter.

D..median filter

The median filter is a low pass filter that uses M×N neighborhood. It first arranges all neighborhoods in an ascending way and chooses the median and substitutes it for the central pixel. This filter is nonlinear and does not reflect the noise effect.

III. FINGERPRINT MATCHING STEPS

A. Binarization

To make a binary image a threshold value is considered for the light intensity. Next "1" is attributed to some pixels and "0" to others.

B. Normalization

To include all images in an acceptable range of intensity, they should be normalized. There are various methods of normalization the most important of famous of which is formula 5. As we know, statistically, data are considered normal if their mean is 0 and their variance is 1. Such data have a normal distribution. In formula 6, N represents the normalized image and 1 is the image we want to make normal. M0 and V0 are the mean and variance that should be applied to the image. M and V are the image variance and mean.

$$N_i(x,y) = \begin{cases} M_0 + \sqrt{\dfrac{V_0 * (I(x,y) - M_i^2)}{V_i}}, if \quad I(x,y) > M_i \\ M_0 - \sqrt{\dfrac{V_0 * (I(x,y) - M_i^2)}{V_i}}, otherwise \end{cases} \qquad (5)$$

C. Segmentation

A fingerprint may be surrounded by some undesirable points and background that cause inaccuracy and noise. Thus the image should be separated from the background. A fingerprint image usually includes black and white grooves and a background that is white exists also in the heart of the image. In such conditions, we use variance. For this purpose, we divide the image into equal blocks and calculate the variance of each block. When the variance of each block is less than the threshold value, we consider it zero. In this case, due to the overlap of the grooves, the block containing them has a high variance and the block containing background points has a low variance.

D. Directional image

The directional pattern is a discrete matrix the elements of which illustrate the local direction of the grooves. This pattern is able to collect the fingerprint data properly and help us retrieve defected fingerprints. In a directional pattern, only the angels of up to 180 degrees are taken into account because the angels between 180º to 360º may be substituted with their equivalent angels ranging between 0º to 180º. After separating image from the background, the direction of each block should be specified. Various methods are applied for this purpose, among which we select gradient method due to it high accuracy [2]. To obtain a gradient image, Sobel filter is applied. The filter includes two parts each defining one matrix. One for the image gradient in the direction of X axis($\partial x(I,j)$) and the other for the image gradient in the direction of Y axis ($\partial y(I,j)$). To achieve better results the following stages are required:

1- The image is divided into W×W blocks [2]

2- ∂x and ∂y for each block are calculated by the above said filters.

$$\begin{bmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix}$$

Fig. 3 Sobel gradient matrixes in vertical directions

$$V_x(i,j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=i-\frac{w}{2}}^{i+\frac{w}{2}} 2\partial_x(u,v)\partial_y(u,v) \tag{6}$$

$$V_y(i,j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=i-\frac{w}{2}}^{i+\frac{w}{2}} \partial^2_x(u,v)\partial^2_y(u,v)$$

$$\theta(i,j) = \frac{1}{2}\tan^{-1}\left(\frac{V_y(i,j)}{V_x(i,j)}\right)$$

Θ represents the local direction of each point inside the block. However, to obtain a directional image, the angel is doubled to nullify the effect of rotation for 2π.

$$\Phi_x(i,j) = \cos(2\theta(i,j)) \tag{7}$$

$$\Phi_y(i,j) = \sin(2\theta(i,j))$$

Next each of the above vectors is passed through a low path filter such as Gaussian filter .

O represents the directional image and Φ is a vector passing through a low-pass filter.

$$O(i,j) = \frac{1}{2}\tan^{-1}\left(\frac{\Phi'_y(i,j)}{\Phi'_x(i,j)}\right) \tag{8}$$

Fig. 4 directional image of fingerprint

E. Gabor filter

To clean noise and enhance the grooves structure, the fingerprint image is filtered by Gabor filter bank in different directions. Gabor filters are middle path filters selecting both the direction and the frequency and have an ideal resolution both in space and spatial frequency. The fingerprint grooves have various local directions and frequencies. Through adjustment of Gabor filters, the structure of the grooves may be saved and the noise can be reduced. The symmetric filter of Gabor pair is illustrated by formula 10[12, 13].

$$G(x,y,f,\theta) = \exp\left\{\frac{-1}{2}\left[\frac{x'^2}{\delta^2_x} + \frac{y'^2}{\delta_y^2}\right]\right\}\cos(2\pi f x') \tag{9}$$

$$x' = x\sin\theta + y\cos\theta$$

f represents the sinus frequency of filter along Θ direction, from the axis. δv and δx are respectively the constants of Gusi window space in the direction of x and y.

Various values (135, 90, 45, and 0) are used for Θ angel in the direction of x axis. Here the mean frequency of the grooves is considered as the filter frequency (i.e. 1/k). K is the average distance between the grooves. For each Θ angel, there exists one filter to be applied to each fingerprint image. Thus we will have four filtered images. Zero degree filter boosts parallel grooves of x axis while weakens others. Filters act similarly in other directions.
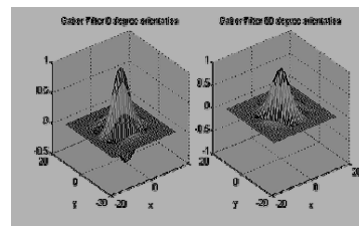
$$y' = x\cos\theta - y\sin\theta \tag{10}$$

Fig. 5 Gabor filter

F. Thinning

To obtain the minutiae, first the grooves should be thinned. This is done by morphology.

Fig. 6 the image thinned by morphology

G. Extraction of minutiae using neural network

To extract minutiae, a multilayer perceptronic neural network including 9 entries, 8 hidden layers and an output is used. (Due to using 3×3 blocks, we will have 9 entries). When the output is 1, the entry will be one of the defined patterns and if it is -1 the entry will be none of the defined patterns.
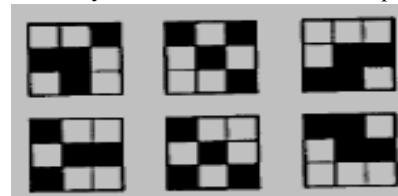

Fig. 7 some of the patterns used in identification of the minutiae

As it is illustrated in the figure, all of the patterns of 3×3 blocks are binary and the minutiae of the image can be finding using their patterns. [1]

H. Remove False Minutiae

When making enhancement in an image, some close points may be separated or linked to each other. Thus to eliminate the undesirable factors, the micro points that are too much close each other should be ignored in the image skeleton.

I. Matching

After extraction of the characteristics, the shortest distance method is used to compare two fingerprints. In this method, the two fingerprints are laid on each other and the points of one image matching exactly the corresponding points of the other image are counted. Ultimately, the total number of the conforming points is divided by the total number of the extracted points (formula 11). If the number of the matching points and the number of the extracted points are the same, the fingerprints are considered one.

Ratio=number of matching minutia / total minutiae (11)

If the ratio of contract is smaller or equal with the threshold value, the fingerprints are considered one and otherwise they are considered different [1].

To find the shortest distance between the points, the following formula is used

$$DD = \sqrt{(x_2 - x_1)^2 - (y_2 - y_1)^2} \qquad (12)$$

If   DD<= threshold & AD<= threshold then
Matching two points is accepted
Else
Matching points is rejected
End

DD refers to the distance difference and AD refers to angel difference. When the two points match, the distance difference between the horizontal and vertical axes of the first and the second point will be zero, smaller or equal with the threshold value. [1]

1- To match one certain micro point from the first fingerprint with the whole minutiae of the second fingerprint:

1-1: formula 12 for all points is calculated

1-2: the minimum DD and AD values are calculated to find the minutiae of the first fingerprint and the second one.

1-3: if the minimum threshold value is less than or equal with the threshold value, then AM=AM+1

AM represents the number of acceptable minutiae.

1-4: if there are still some minutiae in the first fingerprint, we will go to stage 1.

2- Formula 11 is calculated for the acceptable minutiae achieved at the stage 1-3 and for all minutiae.

3- If the ratio is less than or equal with the threshold value, both fingerprints are considered identical.
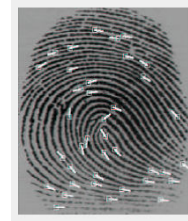

Fig. 8 finding fingerprint minutiae

IV. EXPERIMENTAL RESULTS

Using database FVC2004, 74 images were selected and calculations were performed through MATLAB software. Repeating the experiment for 1014 times, the error was zero in the neural network. Having 9 entries and 10 hidden layers, we had 90weights and we used hyperbolic tangent function.

In order to match the fingerprints once the thinned images and next ordinary images were used. Thinning images increased the accuracy and speed

TABLE I
THE THRESHOLD VALUES USED IN DIFFERENT PARTS

Stage	Threshold
segmentation	0.08
Minutiae extraction	-.9993<X<1.0007
Distance of two minutiae from two images	10
Angel difference of the two points	13
Ratio of matching	72

V. CONCLUSION

The identification systems functioning based on fingerprint biometrics generally use the existing minutiae of the fingerprint image to differentiate among various individuals. In low quality images the extracted minutiae are affected by undesirable factors and noise. This reduces the identification accuracy. This article, presents some methods to improve the image quality. These methods are able to enhance the image quality. Next using a perceptronic multilayer neural network including 10 hidden layers, 9 entries and one exit (as explained above), the speed and accuracy of finding the minutiae is increased. Since the minutiae are the characteristics of a fingerprint image, this improves the accuracy of contrasting two fingerprints. Another advantage of this method is that it shortens the calculation operation for a large number of fingerprints.

REFERENCES

[1] a.zahedpoor," a new method for fingerprint matching with neural network", 4th security conferences, industry Iran University, 2007.
[2] p.jafari,"fingerprint classifying with artificial intelligence methods", m.sc thesis, Tabriz university, 2006.
[3] R.Ross,A.Jain, "From Template to Image: Reconstructing fingerprints From Minutiae Points", IEEE Transactions On Pattern Analysis and Machine Intelligence, Vol. 29, No. 4, April 2007.
[4] D. Miao, Q. Tang, "Fingerprint Minutiae Extraction Based On Principal Curves ", Department Of Computer Science and Engineering, Tongji University, 2004.

[5] T. Ohtsuka, A. Kondo, "A New Approach to Detect Core and Delta of the Fingerprint Using Extended Relationalgraph, "Ieee Proc. Of 2005 Icip, Vol. 3, Pp. 249–252, 2005.

[6] Xiping, T.Jie, W.Yan, "A Minutia Matching Algorithm In Fingerprint Verification," Pattern Recognition, International Conference Pattern On Recognition Vol. 4, Pp. 4833, 2000.

[7] S.Greenberg, D.Kogan,"Fingerprint Image Enhancement Using Filtering Techniques", Electrical And Computer Engineering Department, Ben-Gurion University Of The Negev, Beer-Sheva 2001.

[8] R. Ramli,A. Rosaliza,"A Segmentation Algorithm Based-On Histogram Equalizer For Fingerprint Classification System", Second International Conference On Electrical And Computer Engineering Icece, PP.26-28, December 2002

[9] L.Hong, Y.wan, Anil Jain, "Fingerprint Image Enhancement: Algorithm and Performance Evaluation", Ieee Transactions On Pattern Analysis And Machine Intelligence, Vol. 20, No8, PP.777-789, August 1998.

[10] Philips D. ,Wang Y. ,"A Fingerprint Orientation Model Based On 2D Fourier Expansion And Its Application", Ieee, Tran, Pattern Analysis And Machine Intelligence,Vol29 , No4,PP.573-585 ,April 2007

[11] D.Maio,R.Cappelli," Fingerprint Classification by Directional Image Partitioning", IEEE Transactions On Pattern Analysis And Machine Intelligence, Vol. 21, No. 5, May 1999

[12] J.W. Yang, L.F. Liu, and T.Z. Jiang, Y. Fan, "A modified Gabor Filter Design Method for Fingerprint Image Enhancement, "Pattern Recognition, PP.1805-1817, 2003.

[13] C.Hong, L.Miao,"A Gabor Filter Based Fingerprint Enhancement Algorithm in Wavelet Domain", Communications and Information Technology, Vol. 2, PP.1468-1471, October 2005.