P- ISSN 1991-8941 E-ISSN 2706-6703 *Journal of University of Anbar for Pure Science (JUAPS)* Open Access
2017,11 (1) :68-75

Personal Identification based on Multi Biometric Traits

Wigdan J. Al-Kubaisy **Muzhir S. Al-Ani**
University of Anbar – College of Computer Science and Information Technology

ARTICLE INFO

Received: 07 / 03 /2017
Accepted: 11 / 5 /2017
Available online: 00/04/2017
DOI: 10.37652/juaps.2017.141533

Keywords:
component;
formatting;
style;
styling;
insert (key words.

ABSTRACT

The biometric system that based on single biometric measure (Unimodal) are usually contained variety of problems and limitation like noisy data, does not provide high security and non-university, so we used the multibiometric system to improve the recognition rate, get better security than the unimodal systems and higher efficiency. This study aims to identify a person by using multibiometric traits (Signature, Face and Fingerprint) by using different technique (Singular Value Decomposition (SVD,PCA and wavelet energy). The quality and accuracy of the identification and recognition of the person are measured in this system by computing the Peak Signal to Noise Ratio (PSNR) and the Mean Square Error (MSE) for face, fingerprint, and signature.

Introduction

identification of people among each other has always been a tough and challenging task for the researchers. there are many techniques which are used for identifying a person but biometric technique is the standard one which allows us for online identification of individuals on the basis of their physiological and behavioral features [1]. biometric system is essentially a pattern recognition system. this system works by capturing the biological actions of people such as taking fingerprints or signature, then extracts a range of benefits from these measures, and competition with the other set of features in order to identify the person[2].

———** Corresponding author at: University of Anbar – College of Computer Science and Information Technology
.E-mail address:

As today's society becomes more complex, the security of information becomes more and more important. various methods for biometric personal identification have been proposed nowadays [3]. the chances of an individual losing his/her biometric information are far less the forgetting a password or losing a card. through these types of verification, comes an increased role of responsibility, and security [4]. a biometric system based on physiological characteristics is normally more reliable than one which adopts behavioral characteristics, even if the last may be easier to integrate within certain specific application [5].

I. EASE OF USE

1- Types of Biometrics:

A lot of techniques have been applied for different applications, description and verification becomes more and more important task for these applications especially in security systems [6]. Biometric systems use a variety of physical or behavioral characteristics like fingerprint, face, hand/finger geometry, iris, retina, signature, gait, palm print, voice pattern, ear, hand vein, odor or the DNA information of an individual to establish identity**.** It is expected to effectively meet all the requirements (for example, accuracy, applicability, and cost) imposed by each biometric applications and one which (such as digital rights management (DRM), and access control, distribution of welfare). In other words, do not biometric ideal but a number of them are acceptable. And established specific biometric importance to the application depending on the nature and requirements of the application, and the distinctive characteristics of biometric [7].

A brief introduction to some of the **commonly** used biometric characteristics is given below:

1.1: Face Biometric:

Most of the facial characteristics stable for many years in his entire life, and usually cannot be taken away or copied from one person to others.

Compared to other vital characteristics, facial recognition to find more applications in biotechnology. Recently, many methods of facial recognition proposal, and achieved encouraging results .Figure (1) shows face biometric. The face recognition technique has become very important because of its efficiency for enhanced security without informing the person[8].

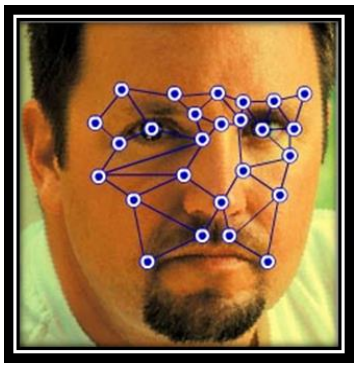


Figure 1: Face Biometric

1.2: Iris Biometric:

One of the most important biometric recognition system that identify people based on their eyes is called Iris Recognition. Iris is the main important part of the human eye; it consists of circular muscle and the other longitudinal control in the amount of light passed the retina through the human eye, Verification of identity on a large scale in many applications because the systems have been used to increase needed for the highest level of security needs. Iris recognition that is a biometric authentication method, based on the characteristics of the iris extract the eyes of the individual, Figure (2) shows example of iris biometric. Everyone has a unique Iris. Even the presence differences between identical twins and between the left and right eye of the same person [9].

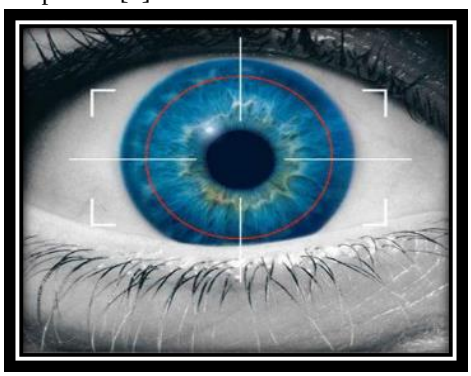


Figure 2: Iris Biometric

1.3: Signature Biometric

Signature is a special case of handwriting, which include special characters and emotions. Figure (3)shows an example of a biometric signature. It can be for many of the signatures to be unreadable. They are a kind of handwriting art objects. However, the sign can be handled as an image, and therefore, it can be identified using computer vision techniques and artificial neural network. Signature recognition and verification involves two separate missions, but strongly linked: one of them is to identify the owner of the signature, and the other is the decision about whether the signature is real or fake. Also, depending on the need, it is placed to recognize the signature and verification problem into two main categories: (i) the recognition of the signing of the online verification systems (SRVS) and (b) non-SRVS. Online SRVS some peripheral requires special units to measure the hand speed and pressure of the human hand when it creates the signature. On the other hand, almost all off-line SRVS systems rely on image processing and feature extraction techniques. In the last two decades, in parallel with advances in sensor technology, some successful SRVS put online [10].

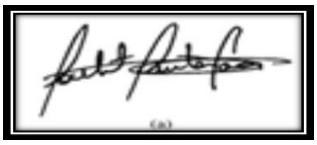


Figure 3: Signature Biometric

2- Neural Network:

The neural network is a model for a computer simulation of parts of the human brain using behavior patterns replicated in small carried out to achieve the results of the perceived events.

Artificial Neural Network (ANN), often called simply a "neural network" (NN), is athlete model or computational model based on biological neural networks.

It consists of a coherent set of artificial neurons and processes information using a relational approach to the account. In most cases ANN is an adaptation which changes its structure based on external or internal information that flows through the network during the learning system [11].

3- This Research Vs. Other Work In The Field Of Identification The Person:

This work is differs from other work in the approach that we used in the collection of the database because we don't use database that available in the internet but we collect it and also the type of the database (the fingerprint through the stump pads, face by camera and offline signature), the other different is mostly research use two biometrics but in this research use three biometrics and three different technique and we obtain a good results in the definition of the persons.

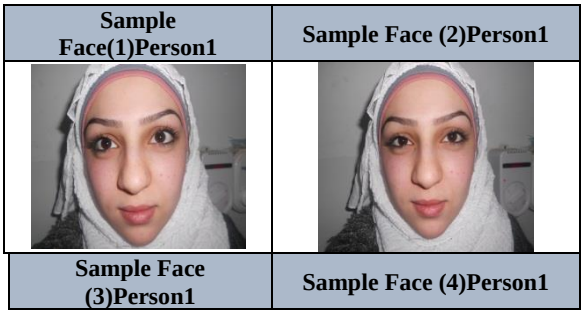
4- Biometric Database

The biometric system is normally involving database for the purpose of recognition and identification, the database can captured by many manners for example Cameras are used to capture face, iris, ear and lips images. Fingerprints can be collected using scanners and stump pads, while other devices such as an electronic pad can be used to capture the handwrite signature. In this system the Databases were obtained from students in department of computer science and department of information technology from college of computer science and information technology in University of Anbar. The total number of the database that is collected 150 samples (five samples of face, fingerprint and signature, taken from thirty students). For the training phase we have been taken the first three images and the other two images we used it for testing. In other word we have 90 samples used to train the neural network and 60 samples used in the test phase**.** Figures (4thrugh 6) show examples taken from the database that used in this research**.**

5- The Proposed System:

The proposed system is used to design a hybrid biometric system for the purpose of identification a person by using three biometric measures (face, fingerprint and signature) and the neural network for training, The implementation passed through two phases the first one is the Testing phase and this involve many steps, the first step is captured the data base by using the camera for capturing the face images , the stump pads for fingerprint and the pen for signature.

The second step is the preprocessing phase and this phase involve many steps, these steps are: binarization this step is done by converting the image of fingerprint and signature from color image to gray by using the luminance technique and then convert the gray image to binary image (white and black) by using Otsu Threshold, the next step is the resizing to the image (256*256). For signature must do thinning by using Skeleton method, while the preprocessing for face involve two steps the first one implemented the skin color detection and the second is the principal component analysis (PCA).The second phase of the system is the phase of Training in this phase use the Artificial Neural Network (ANN) is used for training the features. Figure(7) show the block diagram of the proposed system.



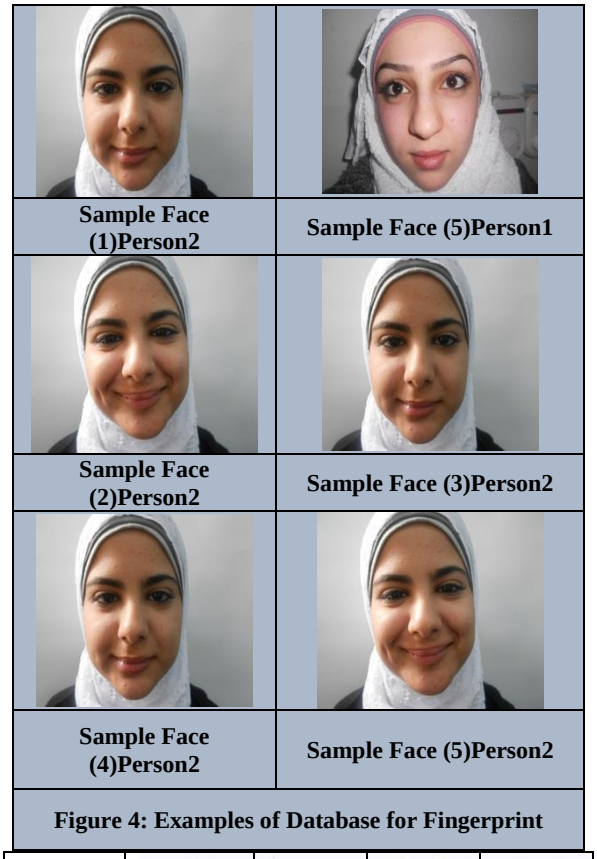


Figure 4: Examples of Database for Fingerprint

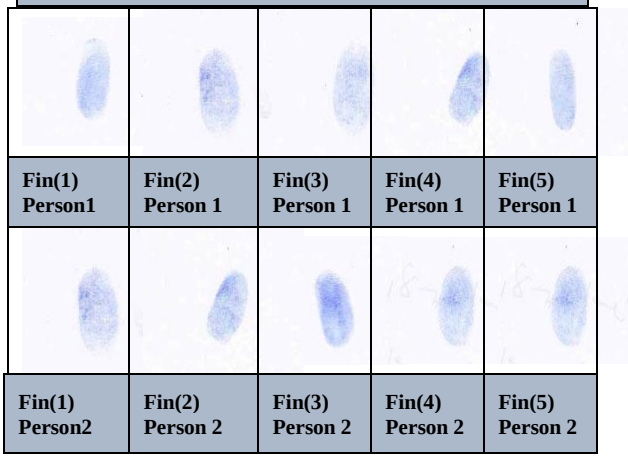


Figure 5: Examples of database for face

Figure 6: Examples of Database for Signature

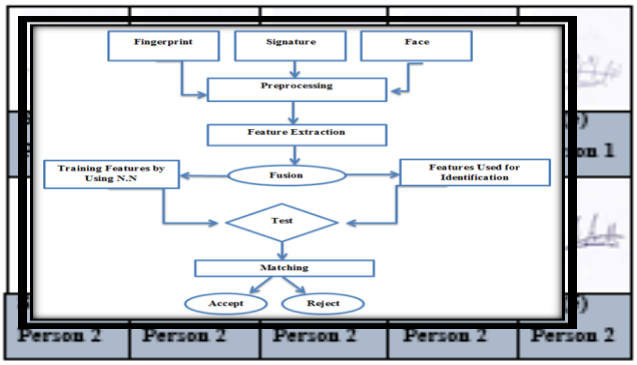


Figure 7: The Block Diagram for the Proposed System

6- The Preprocessing Steps:

The processing steps are implemented on the input image, the goal of this step is to reduce the computational time, eliminating many of the effects of changing illumination and reduce the effect of the noise, this stage is passed through many steps these steps is:

6.1- Resizing:

The samples of the images that used in this system are different in size and therefore this difference leads to different in the length of the feature vectors. For this reason it is necessary to do resizing for all the samples that have been used in training and testing in order to be all the images in same size, the equation that we used for this purpose is [12]:

$$i_{reseized(n,m)} = \sum_{y=1}^{n} \sum_{x=1}^{m} i_{gryscale(x,y)} \quad \ldots\ldots(1)$$

6.2 - Image Binarization:

The phase of binarization involves two steps; the first step in the image binarization process is the conversion of color image to gray image (where its gray scale is 256 levels), the following equation represent the essential equation for binarization [13]:

Where R=read, G=green, B =blue

Then the second step is converting the gray image to a binary image which consists of two colors (black and white).Binary image is the simplest type of The image that has only two possible values of pixel density. Usually they are displayed as black and white. In number, the two values are 1or 255 for white, and 0 for black. And often they produce binary images by the threshold gray or color image. This type of images is frequently used in computer vision applications where the only information required for the task is the general shape, or information. This step is doing only for fingerprint and signature samples.

6.3- Thinning and Skeletonization:

The thinning process is used for signature. The goal of thinning is to eliminate the thickness differences of pen by making the image one pixel thick. The aim of this is to reduce the character features to help in feature extraction and classification, while Skeletonization is used for fingerprint ,Skeletonization is used to remove selected foreground pixels from the binary image. So the outcome is a representation of a signature pattern by a collection of thin arcs and curves.

6.4- Skin Detection and PCA:

These two techniques are used for preprocessing to the face biometric, The operation of finding the skin colored pixels and regions of an image are called the skin color detection. This operation is commonly used as a preprocessing step in order to find the area that may be having human faces. A skin detector especially is used for converting a given pixel into an appropriate color space and then uses a skin classifier to designate the pixel whether it is a skin or a non-skin pixel. The function of the skin classifier is determining the decision boundary of the skin color class in the color space according to training database of skin-colored pixels. The principal components analysis (PCA), well-known for the ability of pressure and intensity against lighting contrast and noise within acceptable limits, is a technique used widely to identify the faces. The PCA allows high-dimensional data to be represented compactly with fewer numbers of coefficients.

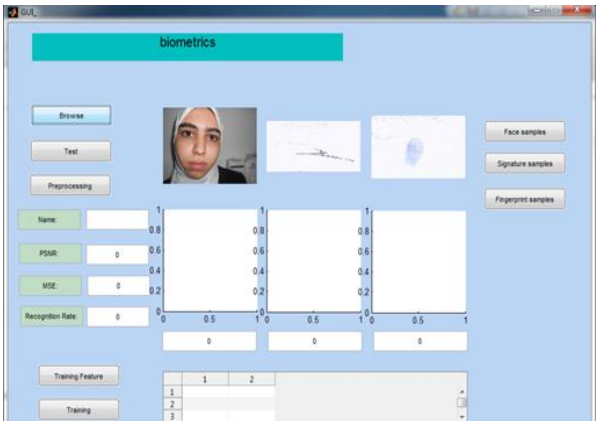


Figure 8: Fetch the Image of the three Biometric object

7- The Result of Preprocessing:

At the end of the preprocessing phase obtained a ninety skeletonized images for fingerprint and signature and ninety of binarized face image (three images for thirty persons), these images saved in order to use them in the feature extraction phase.

8- The Feature Extraction:

The goal of feature extraction is to be able to describe the objects to an extent such that the classification becomes possible. A good feature will yields the same (or nearly same) value for all instances of one class and something different for instances belong to other classes. The purpose of a feature is to create an abstract symbolic representation, and to make it possible to discriminate between classes. Feature extraction is always an important, and still it is difficult step in image verification.

8.1- Wavelet Decomposition :

The discrete wavelet transform can be defined as a series of waterfalls filters. X represent the input image that can supply separately the low pass filter (L) and high pass filter (H). The

Subsampled represent the output of the two filters. Rebuilt the original image by synthesis filters (L) and (H)

$$Grayscale(i,j) = R*0.21 + G*0.71 + B*0.08 \quad \ldots\ldots\ldots\ldots(2)$$

which take the up sampled y_L and y_H as inputs. The resulting lowpass subband y_L and high pass subband y_H are shown in Figure (10).

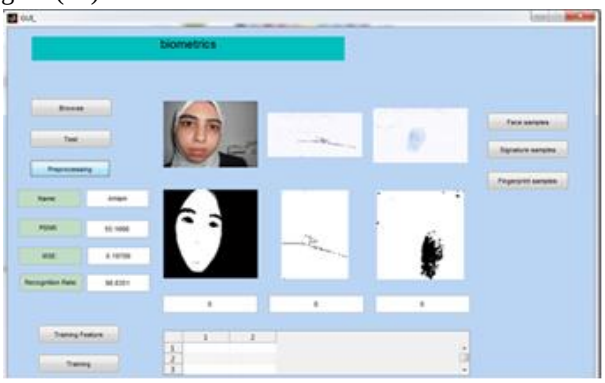


Figure 9:The Preprocessing Phase and Results of Test

We can defined the mathematical representations of Y_L and Y_H as [14]:

$$y_L(n) = \sum_{i=0}^{t_L} L(i)X(2n-1) \quad \ldots\ldots(3)$$

$$y_H(n) = \sum_{i=0}^{t_H} H(i)X(2n-1) \quad \ldots(4)$$

8.2- Wavelet Energy:

The Wavelet energy can be defined as the method that can used to find the wavelet energy for 1-D wavelet decomposition. The wave energy offers a proportion of energy compatible with parataxis and vectors that include the energy discussion detail ratio. The equation (5) shows how to compute the wavelet energy [15]:

$$WE(s_i) = \sum_{j=1}^{L_i} w^2(s_i,j)/L_i \quad \ldots\ldots \quad (5)$$

Where the scale is s_i, the total number of coefficient in scale is L_i, the current wavelet coefficient in scale is w (s_i,j) .

8.3 -Singular Value Decomposition SVD:

The Singular Value Decomposition (SVD) can be an important topic in linear reparation by many famous mathematicians. SVD have many implementation and theoretical values; we can apply the SVD on any real matrix(m, n) and this consider as a feature that specialized the SVD. Consider that we have a matrix A, this matrix have m rows and n columns and R as a rank, where $R \leq n \leq m$. So we can factorized the matrix A in to three matrices as follows [16]:

$$A = USV^T \quad \ldots\ldots\ldots(6)$$

The matrix U is an orthogonal matrix m*m

$$U = [U_1, U_2, \ldots, U_r, U_{r+1}, \ldots U_m] \quad \ldots(7)$$

Ui represent the vector of columns for i=1, 2,... m, and this forming an orthonormal array:

$$U_i^T U_j = \delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases} \quad \ldots\ldots(8)$$

V represent a matrix that an m*n orthogonal matrix

$$V = [V_1, V_2, \ldots, V_r, V_{r+1}, \ldots V_m] \quad \ldots\ldots(9)$$

Vi represent the vector for i=1, 2,..., n, form an orthogonal set:

$$V_i^T V_j = \delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases} \quad \ldots\ldots(10)$$

The S is represent an m*n diagonal matrix with singular values (SV) on the diagonal. The matrix S can be

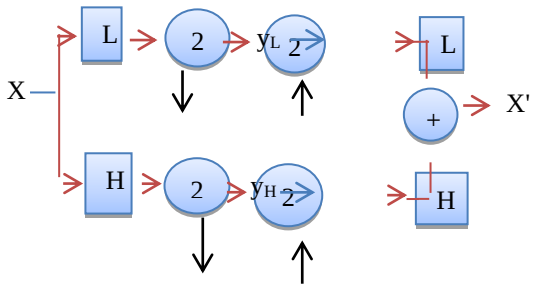


Figure 10: The Process of wavelet Decomposition and Reconstructions

showed in following:

$$S = \begin{bmatrix} \sigma_1 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ 0 & \sigma_2 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \sigma_r & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 & \sigma_{r+1} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0*q & \ldots & 0 & 0 & \ldots & \sigma_n \\ 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \end{bmatrix} \quad \ldots(11)$$

For i=1, 2,..., n, σ represent the singular values of matrix A

9- The Result of Feature Extraction:

Singular value decomposing (SVD) was performed on the three feature vectors. This method has been used to extract the characteristics of each vector. Using SVD helps exposing the geometrical characters of the vectors. It was used as a tool for optimizing the feature vector that will be used for the next stage. Using SVD results three matrices (U), (S) and (V).Contains the Eigen values of the vector in the main diagonal of the matrix and zeroes elsewhere. In this phase we was obtained a three vector one for face ,the second for fingerprint and the last one for signature , each vector contains four features. Finally we will save the features that have been extracted in this phase for the purpose of recognition.

10- The Fusion :

The technique that used to integrate the classification results from each biometric channel is called the Biometric fusion. Multimodal biometric fusion mix between the aspect from different biometric features to. Improve power and reduce restrictions on single aspects. The competence of the fusion scheme dramatically affects the precision of a multimodal biometric system. There are many levels of fusion (sensor level fusion, feature level fusion, match score level, rank level fusion and the decision level fusion), in this system the feature level fusion is used.

11- The Result of Fusion:

The results that obtained from the feature extraction phase is three feature vectors (for face, signature and fingerprint), these vectors were fused in the feature fusion phase. In this phase the three vectors will be combining in one vector to be used in the recognition phase as shown in the Figure (11), the CD1...CD4 is the (Coefficient of wavelet Decomposition) energy of wavelet decomposition for each level.

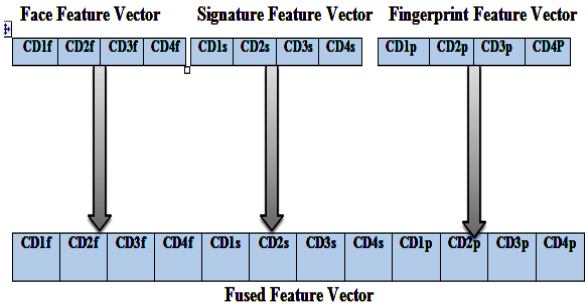


Figure 11: Feature Vector Fusion

12- The Matching:

Identification system and recognition system using matching phase between new data and old data saved in large database to recognize the image. If this data is matched with any data from database then identification is verified, and if not matching data then this data is new and not exist in database.

13- The Training:

In this phase the Neural networks is used because it have a major ability to extract the meaning from a complex or inaccurate data; They can be used to extract observation patterns and trends that are very complex to be observed by humans or other computer techniques. The trained neural network can be used as an "expert" in the category of information given for analysis. One of the most powerful methods of learning is the Backpropagations method . It's more useful method in training of multilayered neural nets. The network is provide an enforcement for how it is doing on a task, it can filter the errors for the information and is used to modify the connections between the layers, which improve the work.

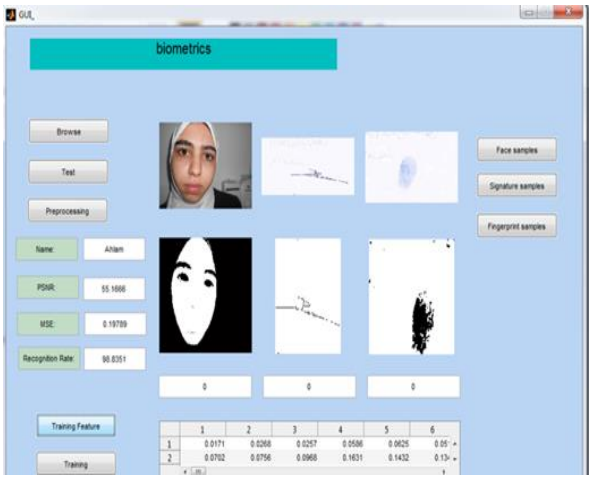


Figure 12: The Result of Training

14- The Final Results:

According to the above mentioned operation the proposed system is going through two stages, training and testing. In this section the result obtained from both phases well is evaluated according to biometric performance measurement metrics. Table (1) shows the obtained recognition rate, mean square error (MSE) and the peak signal to noise ratio (PSNR) for signature, fingerprint and the face. The recognition rate of the system is 98.983.

Table (1) MSE, PSNR and Recognition Rate of the System

	PSNR	MSE	Recognition Rate
Fingerprint	55.1666	0.19789	98.8351
Signature	56.7882	0.13623	98.6398
Face	60.9485	0.052268	99.4731

The MSE and PSNR are calculated when the samples are tested. The quality and accuracy of the identification and recognition of the person is measured in this system by computing the Peak Signal to Noise Ratio (PSNR) and the Mean Square Error (MSE) for face, fingerprint and signature images. In Figures (12and 13) two types of error (mean square error (MSE) and Peak Signal to Noise Ratio (PSNR) have been computed to the face fingerprint and signature images of 10 persons, each has three images and the value of both PSNR and MSE is shown in Table(2). The time of 10 tests is shown in Table(3).

In Figures (13) and (14), the least PSNR was acquired from image no.1 and the max PSNR was acquired from image no. 9 for the same person. The reason behind this is that the brightness and contrast differ between these two images.

This difference is caused by the light where the image was taken and the distance between camera and person. The light of the second image was higher than the

fourth one which gave effecting on the result. The better matching is happened when the MSE is decreased and the PSNR increase, The FAR of the system is 0.1 and the FRR=0.

Table (2) The Value of PSNR and MSE

The Value of PSNR	The Value of MSE
59.4879	**0.0625206**
56.8865	**0.13318**
54.7271	**0.21896**
53.4901	**0.29112**
55.2652	**0.19345**
52.511	**0.36474**
58.106	**0.10057**
55.6549	**0.17684**
50.7809	**0.54324**
54.2908	**0.2421**

Table (3) The Elapsed Time

The number of test	Elapsed time in Millesecond
Test 1	**1.29057**
Test 2	**1.47496**
Test 3	**1.26932**
Test 4	**1.19936**
Test 5	**1.32155**
Test 6	**1.31011**
Test 7	**1.35391**
Test 8	**1.35288**
Test 9	**1.25309**
Test 10	**1.16333**
Average	**1.298908**

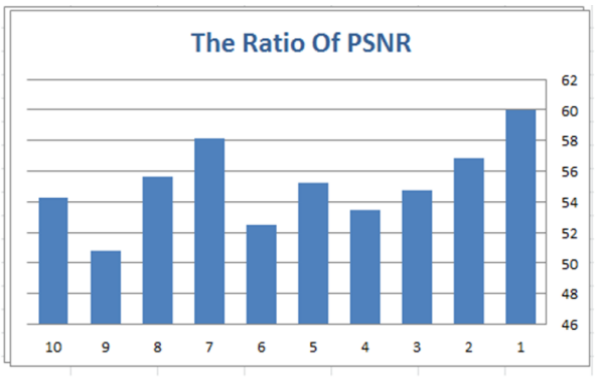


Figure 13 :The PSNR Result

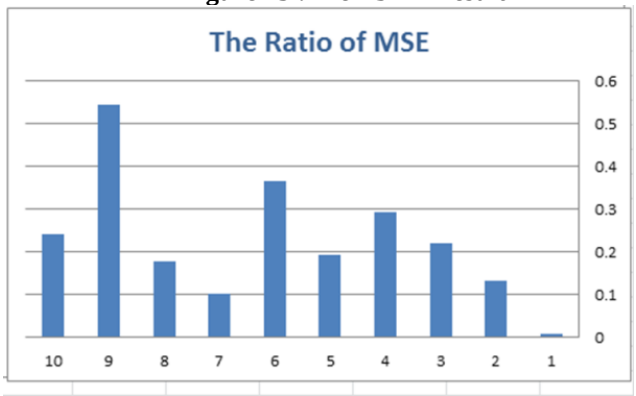


Figure 14 :The MSE Results

References:

1- K.Nath,K.Naryan,A.Agrawl,"Vein Based Personal Identification Systems :A Review",I.J.Intelligient Systems and Applications,2016.

2- M. Serrano, Ayala and P. Melin,"Intelligent Hybrid system for person identification using biometric measures and modular neural networks with fuzzy integration of responses", 2009.

3- A. K.Jaine ,A. Ross and S.Pahakar,"An introduction biometric recognition ",Appeared in IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, 2004.

4- J. Whan Kim, H. Gyucho and E. Youngcha ,"A study on enhanced dynamic signature verification for the embedded system" ,2005.

5- K.Ali Al-heety ,"Biometric Iris Recognition based on hybrid technique",International Journal on Soft Computing (IJSC), 2011.

6- Saranya.K.R , Vanitha.S , Selva priya.G , Minojini.N , Nivi.A.N ," A Comprehensive Approach for Multi Biometric Recognition Using Sclera Vein and Finger Vein" , International Journal of Advanced Research in Computer and Communication Engineering , 2015.

7- G. Osman ,M. suzur, H.and Mohd Nasir Ismail ,"Enhanced Skin Color Classifier Using RGB Ratio Model", International Journal on Soft Computing (IJSC),2012.

8- Yi-Chun Lee, Chin-Hsing chen ,"Face Recognition Based on Digital Curvelet Transform",IEEE,2008.

9- R.Saini,N.Rana ,"Comparison of Various Biometric Methods", International Journal of Advances in Science and Technology (IJAST), 2014.

10- E. j.Rjustino,F. Bortolozzi,et al, "Offline Signature Verification Using HMM for Random ,Simple and Skilled Forgeries", 2010.

11- Faros, A.: Biologically Inspired Modular Neural Networks. Blacksburg, Virginia,(May 2000); Kennedy, J., Eberhart, R.C.: Particle swarm optimization. In: Proceedings
of IEEE International Conference on Neural Networks, Piscataway, NJ, pp1942–1948 (1995).

12- Information Resouces Management Association; "Image Processing: Concepts, Methodologies, Tools, and Applications: Concepts"; Informance Science Reference, IGI global press, 2013.

13- W.Ritscher; "HLSL and Pixel Shaders for XAML Developers", O'Reilly press, 2012.

14- H. Malepati; "Digital Media Processing DSP Algorithms Using C", Elsevier Inc., 2010.

15- E. Mao, Linli Xu, and W. Tian; "Emerging Computation and Information technologies for Education", Advances in Intelligent and Soft Computing, Springer press, 2012.

16- Biometric Facial Recognition: Using facial traits to identify people.

التعرف على الشخصية بالاعتماد على الصفات البايومترية المتعددة

وجدان جابر الكبيسي **مزهر شعبان العاني**

الخلاصة

التعرف على الهوية هي تقنية واعدة التي يمكن أن تحل المشاكل الأمنية في مجتمعنا خصوصا انه في السنوات الاخيرة كان هناك تركيز كبير على الامن في العالم.واحدة من القضايا المهمة في مجال الامن هو الحاجة الى التوثيق الصحيح للاشخاص. هناك الطرق التقليدية التي تستخدم لإثبات هوية الشخص مثل كلمات السر أو مفاتيح أو بطاقات التعريف، ولكن يمكن بسهولة لهذه التمثيلات البديلة للهوية أن تفقد أو تكون مشتركة أو تلاعب بها أو سرقتها مما يؤدي الى الاضرار بالامن . القياسات البيولوجية توفر أمن أفضل من الطرق التقليدية، وزيادة في الكفاءة، وزيادة راحة المستخدم. يمكن تقسيم القياسات البيولوجية الى قسمين الجزء الاول يتضمن الصفات البدنية او الجسمية وهي التي تعتمد على شكل الجسم مثل البصمة والوجه وقرنية العين اما الجزء الثاني فهو الصفات السلوكية وهي التي تعتمد على سلوك الانسان مثل التوقيع والصوت. في هذه البحث تم تقديم النظام البيومتري الهجين للتعرف على الشخص بأستخدام ثلاث من القياسات البايولوجية وهي الوجه والبصمة والتوقيع. النظام المنفذ يتكون من ستة خطوات رئيسية الخطوة الاولى,هي تجميع البيانات من طلبة كلية علوم وتكنلوجيا المعلومات الحاسوب / جامعة الانبار ومن ثم بناء قاعدة البيانات.الخطوة الثانية ,تتضمن مجموعة من المعالجات على البيانات مثل تحويل الصور من الملونة الى ابيض واسود بأستخدام حد العتبة وتحديد حجم الصورة.الخطوة الثالثة هي مرحلة استخراج الميزات المهمة من كل صورة بأستخدام طرق متعددة وتسمى هذه المرحلة بمرحلة استخلاص الميزات حيث نقوم بوضع الميزات المستخرجة من الوجه والتوقيع والبصمة في ثلاث ناقلات.المرحلة الرابعة هي الاندماج في هذه المرحلة يتم دمج الخصائص التي حصلنا عليها في الخطوة السابقة ووضعها في متجه او ناقل واحد.المرحلة الخامسة هي الاختبار و يتم فيها مقارنة الخصائص التي حصلنا عليها مع البيانات الموجودة في قاعدة البيانات و المرحلة السادسة هي المطابقة حيث نقوم بمقارنة النتائج التي حصلنه عليها في مرحلة الاختبار مع الخصائص التي قمنا بتدريبها بأستخدام الشبكة العصبية البيانات الموجودة في قاعدة البيانات للتعرف على الشخص فيما اذا كان موجود او لا.