Signature Recognition Using Discrete Fourier Transform

Research · November 2015

DOI: 10.13140/RG.2.1.5182.6645

1 author:

Muzhir Al-Ani
University of Human Development, Sulaymaniyah
146 PUBLICATIONS **439** CITATIONS

SEE PROFILE

International Journal of Business and ICT
IJBICT is published in cooperation with The American Society for Competitiveness
March 2015, Vol.1, No.1-2
ISSN 2412-9917 www.IJBICT.com

Signature Recognition Using Discrete Fourier Transform

Ghazi Ibrahem Raho [1]

[1] *College of Business, CIS Department*
Amman Arab University, Amman, Jordan

Muzhir Shaban Al-Ani [2]

[2] *College of Computer, CS Department*
Anbar University, Anbar, Iraq

Abd Al-Karim Al-Alosi [3]

[3] *College of Computer, IS Department*
Anbar University, Anbar, Iraq

Lobna Anwar Mohammed [4]

[4] *College of Computer, CS Department*
Anbar University, Anbar, Iraq

Abstract

We use our signatures every day for wide range of applications. Signature pattern of a person can be implemented to recognize biometric characteristics. This form of recognition is commonly used authentication, verification and recognition. The recognition of signature pattern can be realized either online recognition or offline recognition. This work is implemented via offline recognition in which features are extracted from signature images using discrete Fourier transform (DFT). Data of signature patterns are collected from different persons in different forms to be implemented via the proposed system. Then the implemented system measures the differences between two signature images via preprocessing, feature extraction and matching of the results.

Keywords: ***Biometrics, Pattern Recognition, Signature Verification, Signature Recognition, Discrete Fourier Transform (DFT).***

I. Introduction

Digital image processing is a huge area of processing for their wide applications in different fields in addition this area need more experimental work to implement the viability of proposed solutions to a given problem [1]. Image processing techniques are used in various fields, such as automated inspection of industrial parts and security system, medical imaging, military applications, automated biometrics such as iris recognition, fingerprint authentication, face recognition, speaker recognition, satellite imaging for weather analysis and forecast, etc. [2].
The biometric term is an old term and comes from the Greek words bios (that means life) and metrikos (that means measure). Biometric is very important term that uses some characteristics of human body such as finger pattern, face pattern, retina vessel, fingerprint, hand geometry, iris pattern, gait cycle, and voice pattern to recognize and identify humans. Recently, a huge different of applications require very sensitive schemes to verify and identify of a person. In addition using biometric performances became very interesting issue in emerging applications and technologies. Traditional methods of identification such as, identification cards and passwords

have been used to block access to the secure systems but these methods are not secure and can be easily penetrated. The characteristics using human biometric cannot be forgotten, stolen and fraud. Identification of human using fingerprint biometrics from a given pattern or print depends on the ridges in the skin of a finger that commonly used for criminal realization [3,4].

Biometric characteristics (physical or behavioral) are very important to identify persons because these are unique characteristics and it difficult to find similar characteristics in two persons. These biometric characteristics have been used always by criminal justice agencies to identify suspects for a long time ago. Biometric recognition including many features such as face patterns (via face image in different position), iris patterns (via iris image), palm patterns (via palm image), voice patterns (via voice acquisition), hand veins (via veins acquisition), hand geometry (via hand geometry image), gait recognition (via gait cycle acquisition), DNA (Deoxyribonucleic acid) and other biometrics characteristics. Biometrics characteristics are divided into two main groups. These groups are physical characteristics and behavioral characteristics. Physical biometrics characteristics are implemented to get biological and physiological features such as finger print image, face print image, iris print image, and DNA pattern. Behavioral biometrics characteristics are not biological and not physiological characteristics such as distinctive and singular habits that include signature patterns, keystroke patterns and gait cycle to identify persons [5]. Figure (1) shows the biometric applications via their characteristics in which you can see that fingerprint occupy the most important applications.

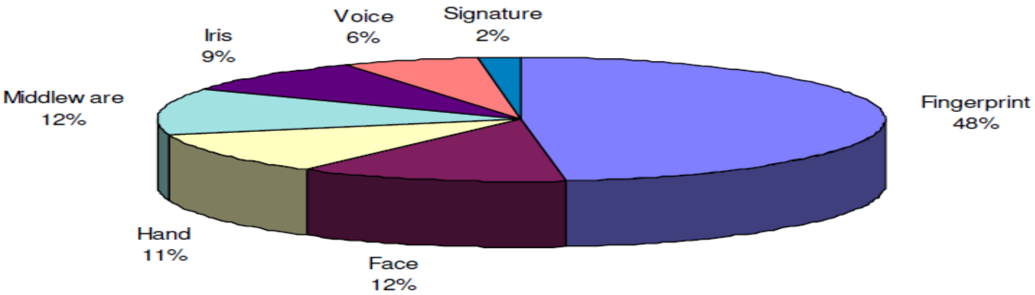


Figure (1) Biometrics Types

Wide range of security applications are implemented via biometric systems and these systems can be realized in two different methods. Verification mode can be implemented via asking the user to be already enrolled in the system (such as login name, identification card and passport). The first step of this case is acquiring the indicated biometric pattern to generate the characteristic data in which it is used to compare that data to the stored data [6].

Identification mode can be implemented via the identity of the user is a clearly unknown. In this mode of identification the biometric data is acquired then matched with all the stored data via the indicated database, so the user can be anytime and anywhere in the database [6].

As the need of biometric data (all types) becomes very important in our life, so the size of the database grows hugely. Technically, it is clear that identification process is more challenging and costly. It is clear that large databases are categorized according to a distinguished characteristic data in the biometric data. Then a mini searches are done for a certain record to reach a small set of data. This process maximize the accuracy via minimizes the number of related records per search [6].

As you try to enroll in the biometric system and before you can be verified successfully or identified perfectly by the system, you must be registered with the biometric system. Firstly the biometric data of the user is captured, secondly processed the captured data and thirdly stored the processed data in the system. There are several (usually three or five) biometric data samples are used to create a master template for the user, so the quality of the stored biometric data is important for the next authentication process. The registration operation of the indicated user with the biometric system is called enrollment in which you can adapt and introduce new user to the system [6].

II. Biometrics Collection and Storage

Collection of biometric data is a selective and dedicative process and there are many methods to do that. Each of these methods has different degrees for privacy and each falls into the following general groups [5]:

- Maximum set of data; these data are collected from wide range of persons, example; blood sample collected to get for example DNA.
- Minimum set of data, these data are collected from small samples, example retina print and fingerprint.
- Random data collected without direct knowledge, example images taken for different persons in different situations.

Biometric characteristics can be stored in different methods (traditional or digital), but in most applications, the stored images in biometrics systems are not real image (only features) to offer more capacity. Instead of that, biometric data are analyzed to form a digital pattern which is constructer from ones and zeros. Then formed pattern will be stored in a database or on any other device that prepared for this case in order to be used for the next step of processing. The company that responsible for this work has the decision to choose or cancel the obtained template [5].

III. Signature Recognition

Handwritten signature has huge number of application in different areas and these applications has been widely implemented and explained. These applications are widely used in security systems such as companies, universities and banking …etc. Signature verification of handwritten can be categorized into two main types: verification via online mode and verification via offline mode [7].

Online verification mode requires hardware devices such as stylus and an electronic tablet connected to a computer to grab dynamic signature information. Offline verification that no need of hardware devices, that deals with signature information which is in a static format stored on any device as personal computer [7].

The information of the signature via online mode approach includes the dynamic properties of signature. In this type of processing the information can be extracted about the static performance of signatures such as pressure points, strokes, writing speed and acceleration. This form of processing generated better performance because it is difficult to fraud the dynamic characteristics, but the system required more complex hardware to implement. Digitizer tablets (apply I/O digital interface) or pads that are sensitive for pressure to convert these data into digital forms. These devices are used to introduce real dynamic signature as shown in figure (2) [7].

Figure 2 Online Signature scanner (Digital Tablet)

Offline signature recognition in which, the signature pattern can be received from a stored device (with stored data), in which the signature pattern are stored in static form. So you can verify these patterns without present the person. This type of verification (offline) is convenient in different situations such as verification of documents, transactions via banks and companies … etc. Signature recognition systems via offline mode need to be designed precisely to reach an adequate accuracy needed for the customer [7].

IV. Level of Forgeries

Forgery deals with Creating, forging, or altering almost any document, with the intent to. Different types of forgeries are categorized into the following types as shown in figure (3):

- **Random Forgery**

Site victim's name is used in your style to create a type of fraud known as simple or random. This forgery represents the majority of cases of fraud although it is very easy to detect even with the human eye [9].

- **Unskilled Forgery**

The person who perform the signature with their style considering that he have not any knowledge of the spelling and experience. This can be done with observing the signature closely for an enough time [7].

- **Skilled Forgery**

There is no doubt the most difficult of all the fraud was created by professional fraudsters or persons who have experience in the signing copies. To achieve this type one either try to follow the tradition trace or to sign using the hard way. Figure 4 shows the various types of forgeries and it is clear the difference from original signature [7].

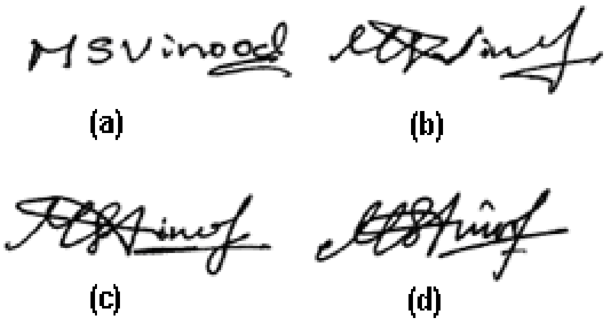


Figure (3) Types of signature tradition
a) Random type b) Unskilled type c) Skilled type d) Original Signature

V. Literature Review

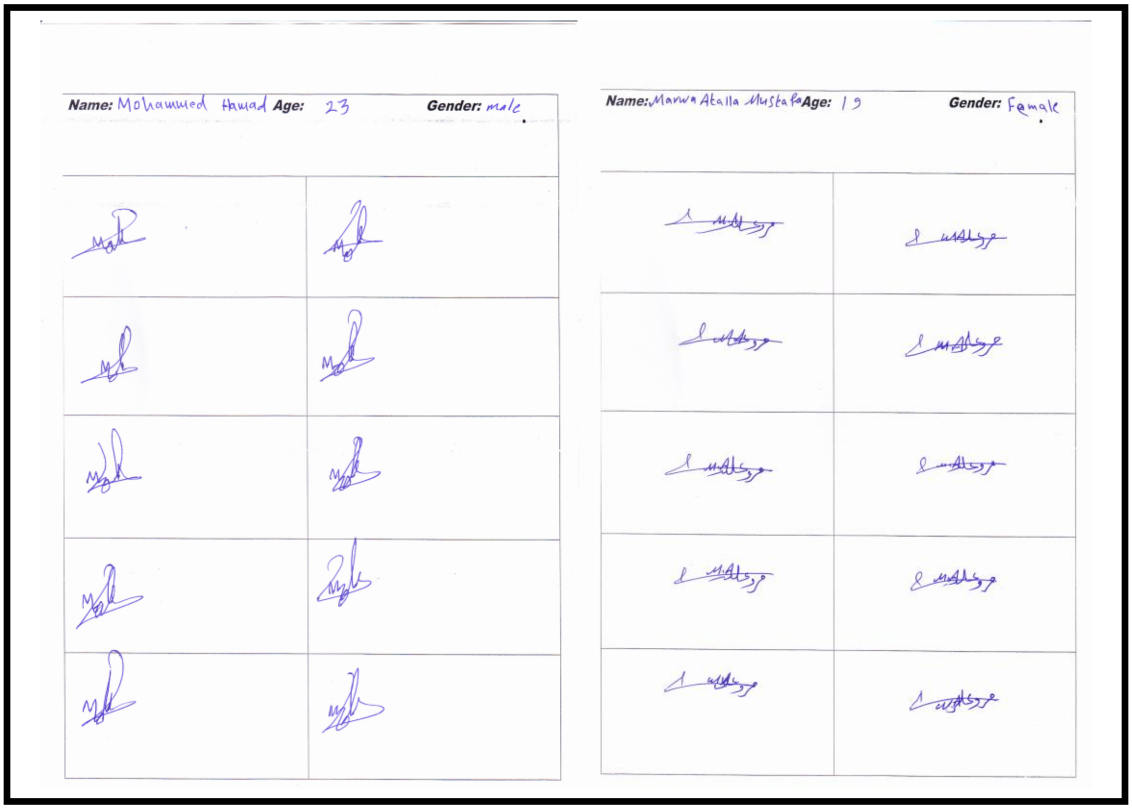
Luiz S. Oliveira, et al. (2008) presented a strategy for offline signature verification used Receiver Operating Characteristic (ROC) curves and this strategy analyze the choose of various fusion methods via the combination of the partial decisions using Support Vector Machine (SVM) technique. Then combined the ROC produced by various SVM classifiers using the analysis of maximum likelihood. This work is implemented via 100 persons as a stored database. The results obtained from the implemented system demonstrated that the person independent approach can reduce false rejection rate (FRR) but leaving the false acceptance rates (FAR) at levels that are acceptable [8].

Stephane Armand et al. (2006) introduced an efficient way to implement identification and verification via offline signature mode. To start the procedure, firstly determine the contour of signature by acquisition these contours from original image. The feature extraction process is implemented on the contour using efficient combination of the Modified Direction Feature (MDF) with combination of additional different features via different classifiers of Neural Network [9].

Sargur N. Srihari et al. (2004) applied writer independent of learning strategies that applied for a set of samples of signatures (real and not real signatures) prior to introduce and enroll of writer, and newly enrolled individual. There are many classification approaches and these are applied via two algorithms (method based on thresholding that is a standard method of biometric signature recognition and probability distribution method). Another method of classification applied based on pairs of feature and a support vector machine (SVM) method, this method called Nava Bayes [10].

VI. Data Gathering

The data gathering starts from collecting of images samples and introduce them to the step of reading as shown in figure (4). Twenty persons were taken to be consider in the system, each person have to introduce of twenty signatures and then entered through the prepared input device (scanner device), after that cropping each signature individually using the general function existing in Matlab package which is imcrop function and its equation is "A = imcrop(I)" where "I" is input image and each signature treated as separate image sample.



Name: Mohammed Hamad Age: 23 Gender: male.

Name: Marwa Atalla Mustafa Age: 19 Gender: Female.

Figure (4) Sample of data gathering

VII. Implemented Approach

The implemented system of the signature recognition passed through three main steps as shown in figure (5):

- preprocessing step (this step is important to improve the image enhancement and it use in the next step).
- feature extraction step (this step is important to improve the image features and characteristics of image and it is necessary to next step to obtain the best results in comparison).
- matching step (this step work on the two input images that passes through previous steps and returns the matching values).

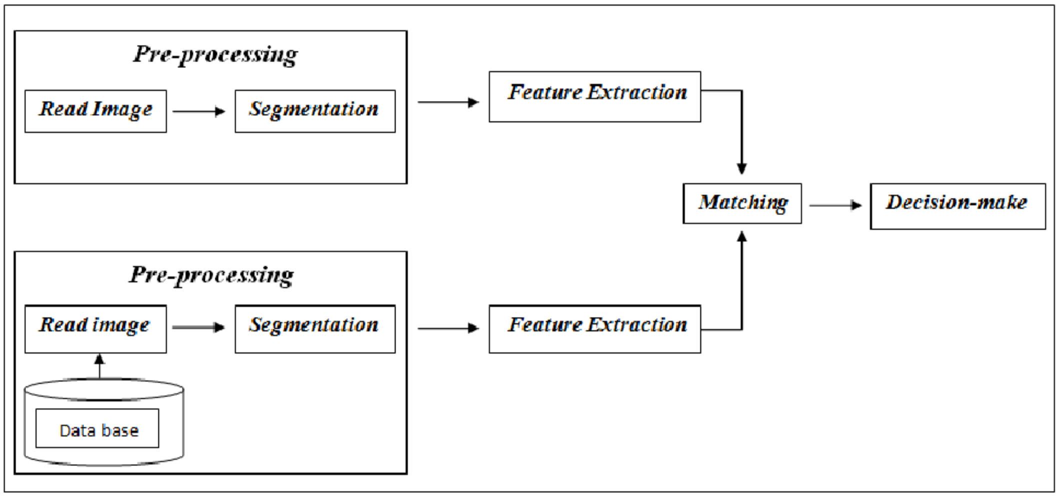


Figure (5) Steps of the implemented approach

Preprocessing Step

Images are collected from different persons and converted into digital images via digital scanner. Then these color images are converted into gray scale images in order to be ready for the preprocessing step as shown in figure (6). Preprocessing step starts after process of reading images. This step started by normalizing the signature images and then resizing these images to a proper size. In addition an operation of noise removal is applied via median filter. Then the edge detection process is used to enhance signature edges in which a suitable mask is selected to perform the convolution process as shown below:

Mask = [-1 -1 -1; -1 8 -1 ; -1 -1 -1] (1)

Feature extraction technique is implemented on the obtained pattern to generate features.

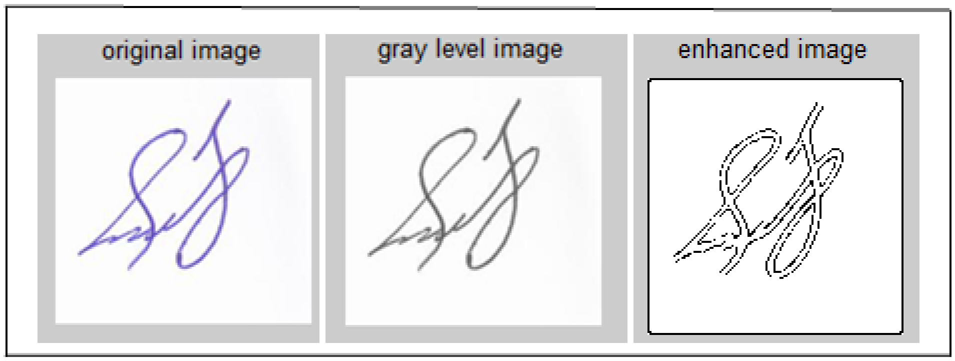


Figure (6) Steps of Signature Preprocessing

Feature Extraction Step

In this step, the method that used for feature extraction is the Discrete Fourier Transform (DFT). DFT is an efficient tool applied on images to separate an image into its sine waves and cosine waves. The output of the process converting images from time (spatial) domain into frequency domain. Normally image details are concentrated in low frequencies, noise and edges are concentrated in high frequencies. In frequency domain image, you can distinguish the frequencies that represented the image in addition you can know the frequencies that carry the noise. So you can apply a specific filter to illuminate that noise directly, which is an important area of applications including recognition, extraction, compression, analysis …etc. [11].

One point must be clear here that processing of images in time domain leads to more efficient resolution that that of frequency domain with respect of some frequency losses in frequency domain. [11].

It is clear that for any image processing procedure that the image size of the output must be equal in size for the input image, so numbers of pixels are the same for both images and this is true for time domain and frequency domain. [11].

DFT equation is given bellow:

$$G(u,v) = \frac{1}{MN}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1} g(m,n)e^{-j2\pi(\frac{mu}{M}+\frac{nv}{N})} \qquad (2)$$

Where g(m,n) is the input image in time domain.
G(u,v) is the output image in frequency domain.
m,n are the input index of time domain.
u,v are the input index of frequency domain.
M,N are represented the image dimensions.

A proposed method of DFT is implemented to extract the adequate features. But as we try to extract a real performance of the image contour so the time domain analysis is a perfect approach for a geometric structure [11].

VIII. Results and Analysis

The results generated after the matching step which gives the error ratio calculating the difference between the two compared images. The error ratio that generated after compared the image of signature with itself is zero. The error ratio of the signature image with the rest of images of the same person gives a value nearly more than zero. In addition if the error ratio is small we could know that the ratio of matching between the signature images is big and also could verify that this signature is the signature of origin person. But if the error ratio is big enough, this leads that this signature is the signature of foreign person because the ratio of matching is small. Table (1) illustrate error ratio between testing images and group of training images for a sample of the selected five persons.

Table (1): illustrate error ratio between testing images and training image

Signature images	Training image 1	Training image 2	Training image 3	Training image 4	Training image 5
Testing image (person1)	1.3576	1.5989	1.3564	1.6854	1.2099
Testing image (Person2)	2.3052	1.7516	1.0628	2.1714	2.2173
Testing image (Person3)	0.0017	1.7486	0.0020	1.5187	0.0039
Testing image (Person4)	1.4663	1.6383	2.1793	2.1845	3.1061
Testing image (Person5)	3.0011	2.4207	1.1899	1.9491	2.4043

IX. Conclusions

Signature recognition systems are used for many applications and have important roles in these applications. Also it has an important role in several areas of researches in different methods. Daily we use signatures and we need to verify these signatures to conform our secure life. This work presents a simple and effective signature recognition approach based on Discrete Fourier Transform (DFT) that used to extract features. Many individuals are enrolled via a constructed signature database. The obtained results indicated that a good and efficient recognition rate is recognized.

References

[1] Gonzalez Woods Eddins, “Digital Image Processing Using Matlab”, Errata Sheet, July 17, 2006 .
[2] Madhuri A.Joshi, “Image Processing An Algorithm Approach”, Asoke K.Ghosh,2006.
[3] Hazem M. El-Bakry, Nikos Mastorakis, "Personal Identification Through Biometric Technology", Proceedings of the 9th WSEAS International Conference on APPLIED INFORMATICS AND COMMUNICATIONS (AIC '09).
[4] Muzhir Shaban Al-Ani, "A Novel Thinning Algorithm for Fingerprint Recognition", International Journal of Engineering Sciences, 2013.
[5] Jennifer Lynch," from fingerprints to DNA :biometric data collection in U.S immigrant commutes and beyond" , AMERICAN IMMIGRATION COUNCIL May 2012.
[6] Zdeneˇk Ríha, Václav Matyáš , "Biometric Authentication Systems", Faculty of Informatics Masaryk University, November 2000.
[7] V A Bharadi, H B Kekre, "Off-Line Signature Recognition Systems", International Journal of Computer Applications, 2010.
[8] Luiz S. Oliveira, Edson Justino, Robert Sabourin, Fl´avio Bortolozzi, "Combining Classifiers in the ROC-space for Off-line Signature Verification", Journal of Universal Computer Science, 2008 .
[9] Stephane Armand, Michael Blumenstein , Vallipuram Muthukkumarasamy, "Off-line Signature Verification based on the Modified Direction Feature", International Conference on Pattern Recognition, 2006.
[10] Sargur N. Srihari, Aihua Xu and Meenakshi K. Kalera, "Learning Strategies and Classification Methods for Off-line Signature Verification", Int’l Workshop on Frontiers in Handwriting Recognition, 2004.
[11] K Manikantan, S Ramachandran," DFT domain Feature Extraction using
Edge-based Scale Normalization for Enhanced Face Recognition", Journal of Advanced Computer Science and Technology, 2012.

Authors

[1]Ghazi Ibrahem Raho, Associated professor at Computer Information System& Information Technology at Amman Arab University – Amman - Jordan. Doctoral Fellowship(1988)- Research & Computer –University of Marseilles-France.
Ph.D. (1981), in Computer Information System& Information Technology, College of Planning &Cybernetics - ASE – Romania. M.Sc. (1979), in Computer Information System& System Analysis College of Planning & Cybernetics – Romania. Postgraduate Diploma (1980), in Information &Applied mathematics UNESCO, Bucharest. B .Sc.(1976) Statistics Almustanseriy university Baghdad –Iraq.

[2] Muzhir Shaban Al-Ani has received Ph. D. in Computer & Communication Engineering Technology, ETSII, Valladolid University, Spain, 1994. Assistant of Dean at Al-Anbar Technical Institute (1985). Head of Electrical Department at Al-Anbar Technical Institute, Iraq (1985-1988), Head of Computer and Software Engineering Department at Al-Mustansyria University, Iraq (1997-2001), Dean of Computer Science (CS) & Information System (IS) faculty at University of Technology, Iraq (2001-2003). He joined in 15 September 2003 Electrical and Computer Engineering Department, College of Engineering, Applied Science University, Amman, Jordan, as Associated Professor. He joined in 15 September 2005 Management Information System Department, Amman Arab University, Amman, Jordan, as Associated Professor, then he joined computer science department in 15 September 2008 at the same university. He joined in August 2009 Computer Science Department, Anbar University, Anbar, Iraq, as Professor.

[3] Abdul Kareem A. Najem Al-Aloosy, has received Ph.D., Polytechnic of Wroctaw , Wroctaw , Poland , 1992. He received training course in UTBM & Polytech Engineering School at Marseille - France 2006. He worked 1992 – 1994 lecturer at the Computer Engineering Department, College of Engineering, Sabha University – Libya. He worked 1995 – 1998 in private sector in engineering field. He worked 1999 -2003 Lecturer at the Computer Eng. Dept. College of engineering / Al Nahrain University – Baghdad. He worked 2004 – 2006 assistant head of Computer Eng. Department, College of Eng. / Al Nahrain University–Baghdad. He worked 2006 – 2009 head of Computer Eng. Department in Computer Man College in Sudan. He worked 2009 – 2011 associate professor in informatics college in Arab International University in SYRIA. 2011—till now he joining as head of information system department in Computer College/ Anbar University.

[4] Lobna Anwar Mohammed has received B.Sc. in Computer Science from Computer Science Department, Al- Anbar University, Iraq, 2012. Now she is working on M.Sc. project (2013 - tell now) in Computer Science Department, Al - Anbar University. Her current study concentrated on image processing, biometrics recognition and identification.