Advanced Engineering Technology and Application

ISSN: 2090-9543 VOLUME 8, ISSUES 2, 2019 www.egyptfuture.org/ojs/

Development of Biometric Fingerprint Authentication System in AOU -Bahrain

*Abdulrahman Al-Awadhi** *and Sarmad Mohammad*

ITC, Arab Open University (AOU), Kingdom of Bahrain

Received:2 Feb. 2019, Revised: 22 Mar. 2019, Accepted: 27 Apr. 2019.
Published online: 1 May 2019.

Abstract: Main objective of this research is to develop the existing fingerprint authentication system implemented in AOU Bahrain which automatically uses only fingerprints matching between measured & reference template minutia stored in database for validating identity of employee. Modified Employee authentication System suggest adding more security measures which are facial and smart card (RFID tag) to be scanned by car park barrier sensor when employee entering and leaving car park also same smart card to be swiped in case employee entering & leaving university by walking in order to increase system security. Modified system is designed to ensure that the organization is equipped with the high level of human resource tracking for each separate department of the organization. The main feature of Employee authentication System is time tracking for employees. The system is integrated and implemented with biometric facial & fingerprint features that identifies certain or specific employee as well as possess of smart card. The system can be accessible from remote network. The developed system also includes the employee fingerprint and facial verification, employee attendance, employee tracking, employee leave, and salary payment modules. The operational activities of the system are accessed or controlled by IT service department, also the research work is concerned with the study of security & errors of actual existing biometric fingerprint authentication system implemented in AOU Bahrain compared to suggested modified combined method which implements fingerprint, facial and smart card (RFID tag).

Keywords: Bio-metric, Security, Finger print matching and RFID authentication application.

1 Introduction

Biometric fingerprint authentication system shown in Figure.1 consists of sensor that capture the raw biometric data of users, which requires contact with the employee biometric fingerprint, sensor influence the system's convenience of use, acceptability and reliability [1], also influence how secure the system is. Second component feature extractor takes the raw data from the sensors as an input, extracts from it the key features and converts them into a digital representation called a template, can be seen as a form of non-reversible compression. It significantly reduces the complexity of the original biometric sample, decreases the resources required to store and process the biometric and prevents the original biometric data from being reconstructed from the template [2].

Some systems further process the templates by incorporating encryption so that the data is better protected. used to hold templates, It may be a local storage medium, such as a smart card, or it may be the storage facilities of the same computer as the rest of the security system or, it may be a remote server, templates need to be protected and backed up, If a remote server is used, a secure communication link between the security system and the server is needed [3].

The benefit of storing a database of templates on a server is that multiple security systems can share the data. However, this practice can also make the database more vulnerable to malicious attacks, and that increases the risk of a breach of data security. Compares the template created from an input biometric sample with a stored template. For each comparison, it measures the similarity (or differences) between the two templates and produces a quantitative reference such as a similarity value which decides whether the input template and the stored template match, based on the similarity value from the matcher [4].

2 Methodology

The Actual existing Fingerprint Biometric implemented in

AOU System is shown in Figure 2, while modified suggested authentication system including the RFID card (something employee possess) and of the two subsystems face and fingerprint (something about employee) as shown in Figure 3 and the steps listed below:

Step1: employee scan smart card (RFID tag) by car park barrier sensor when employee entering and leaving car park also same smart card to be swiped in case employee entering & leaving university by walking in order to increase system security.

Step2: Fingerprint features that identifies certain or specific employee scanned then minutia pair extracted as shown in Figure 4 for matching process.

Step3: The shapes and geometries of employee faces are all different, by establishing sufficient reference points on the face and measuring the lengths between the reference points as shown in Figure 4, it is possible to create a template that uniquely represents employee, the process of creating a template from the original image (feature extraction) is described as a non-reversible compression. In the figure 4 face image, the human face is represented by only 13 numbers, for which the file size is considerably smaller than the file size of the original facial image.

When the decisions of the three subsystems do not agree (one system thinks it is a match another thinks it is non-match), then the outcome of the combined system is non-match. This means the outcome of the combined system will be a match only when the outcomes of three (RFID card, fingerprint & face) of the subsystems are matches, when the outcome of either subsystem is a non-match, the outcome of the combined system will be a non-match.

The sensitivity of a fingerprint recognition system is determined by thresholds. The same is true of all biometric recognition systems the discussion here applies not just to fingerprint recognition systems, but to biometric recognition systems generally. The thresholds used in biometric recognition systems set the balance point between security and convenience. For example, when a threshold is set too low different biometric data can appear to match when they are not the same which is known as a False Match (FM). False match refers to incorrectly believing that two given sets of biometric data are matched then consequence of the former error is that intruders could gain access to resources they are not allowed to access.

Conversely, when a threshold is set too high biometric data from the same person can appear not to match because of slight variations which are known as false non-match (FNM). False non-match refers to incorrectly believing that two given sets of biometric data are not matched. The consequence of the latter error is that legitimate users could be refused access to resources they are entitled to access.

- False match (FM) is referred to as 'false acceptance' or 'false positive' by some authors, and false non-match (FNM) as 'false rejection' or 'false negative'.
- In practice, these two types of error are unavoidable with current existing AOU finger print recognition system but implementing combined system will reduce FM to a minimum.
- With respect to these two errors, biometric recognition systems are typically assessed by the false match rate (FMR), which is the probability of a false match type of error, and the false non-match rate (FNMR), which is the probability of a false non-match type of error. Table.1: illustrates a comparison of the FNM and FM related to Security, Convenience and Consequences (SCC). This means that systems are usually assessed based on statistical information.

Table1: illustrates a comparison of the FNM and FM related to Security, Convenience Consequences (SCC).

	False Non-Match FNM	**False Match FM**
Threshold (t)	Set High	Set Low
Security	Increased security	Less security
Convenience	Less Convenience	Increased Convenience
Consequences	FR – False Rejection False Negative (F-) FNMR – False-Non-Match Rate Legitimate User (authorized) rejected	FA – False Acceptation False Positive (F+) FMR – False-Match Rate Illegitimate User (intruder) accepted

Figure 5 shows error rate versus threshold (t) related to FMR and FNMR, where the FMR decreases as the threshold increases, and the FNMR increases. This makes sense: a higher threshold means that the matching score between two biometric samples is required to be higher, and so the two samples must be more similar to be considered a match. The magnitude of the error rate at the point where the two curves intersect is the equal error rate (EER). The EER is an important piece of information in aiding system administrators to set the threshold. Recognition errors can be reduced by applying multiple metrics to identify a person. This can be achieved by using more than one biometric such as face and fingerprint, or by using a biometric along with a conventional security. measure smart card possess by employee. It is more unlikely that two individuals would have similar multiple metrics, so the probability of a false match is lower using suggested new recognition system that makes use of combined face and fingerprint biometric subsystems.

3 System Testing

The following testing values have been obtained for the fingerprints & face separately for 50 employee samples as shown in Figure 6 accepted verified fingerprint and denied one samples.

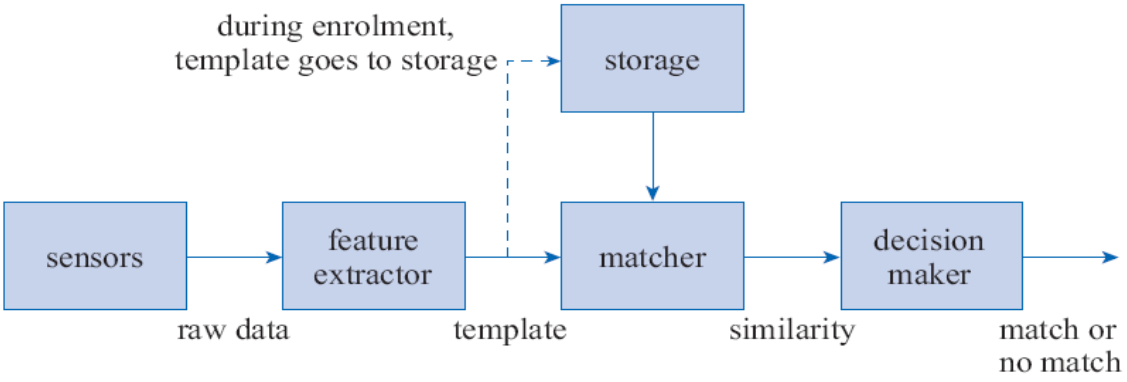

Fig.1: Five components of Fingerprint (FP) biometric authentication System.

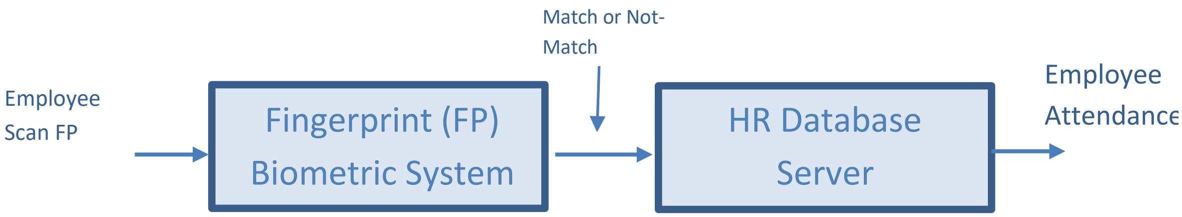

Fig.2: Existing Fingerprint Biometric System Block Diagram.

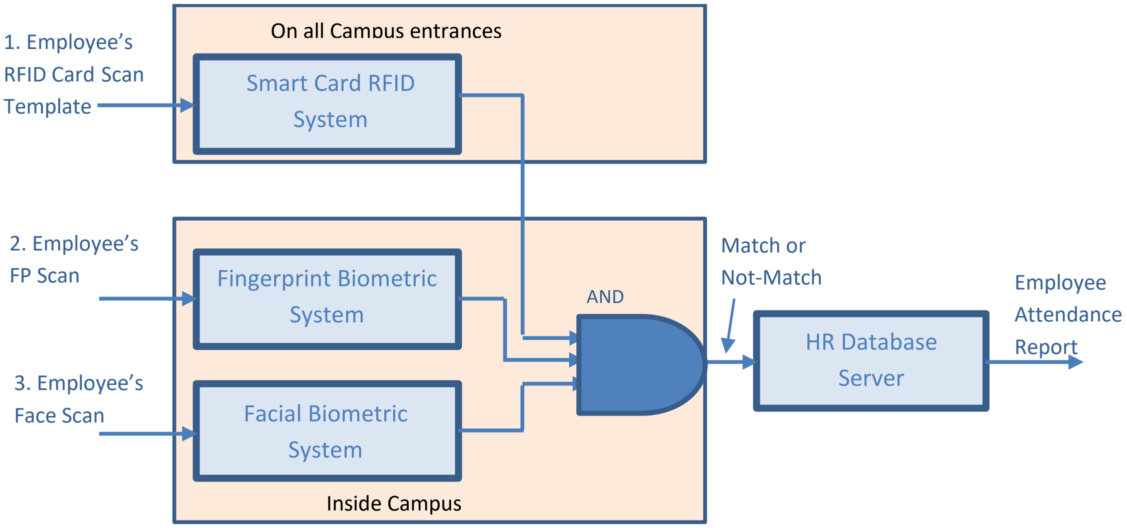

Fig. 3: Suggested Modified Automated Authentication Attendance System Block Diagram.

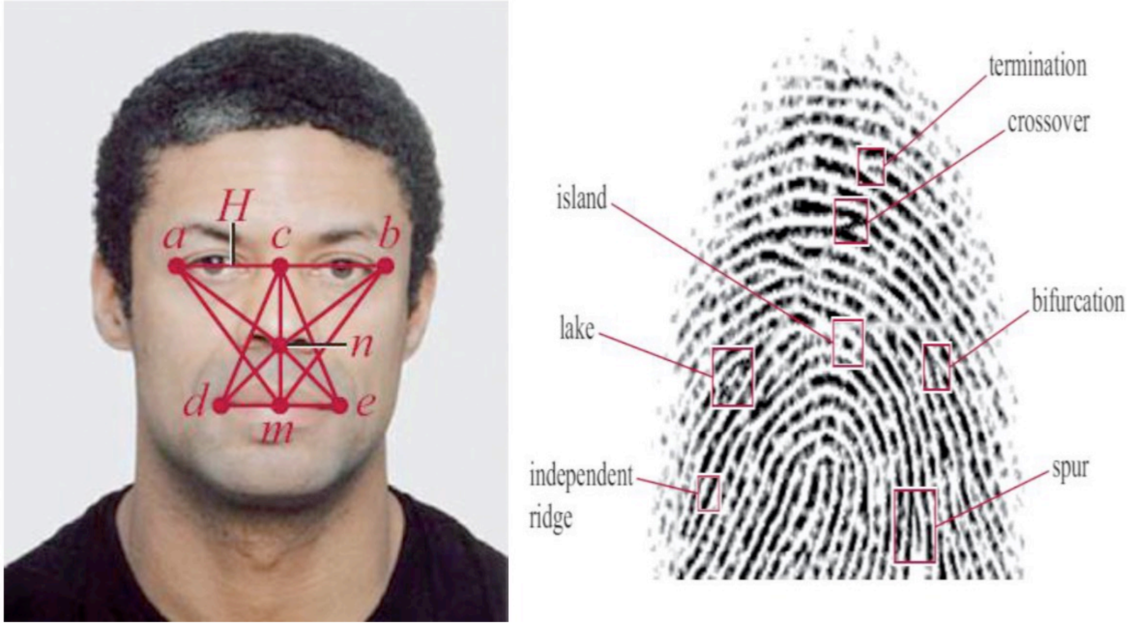

Fig. 4: Facial & fingerprint template to be extracted from employee face & fingerprint.

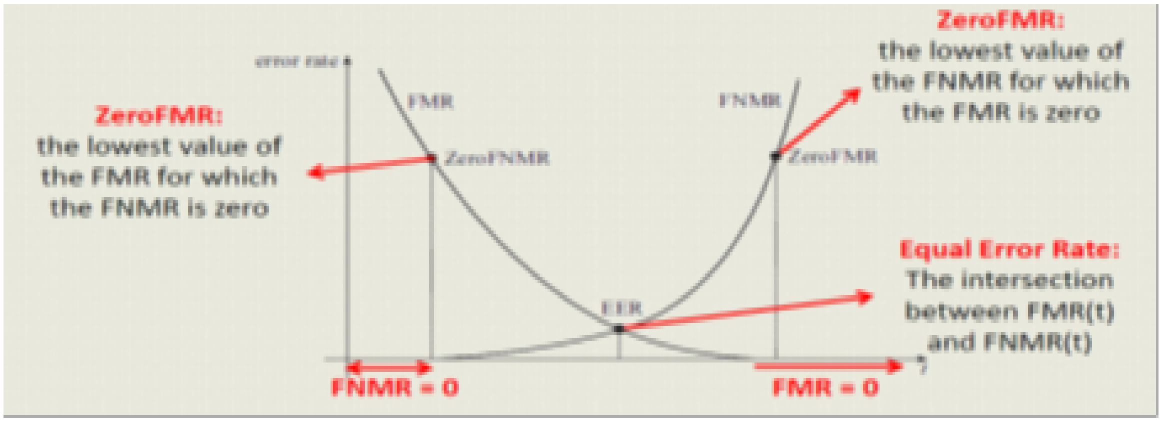

Fig.5: Error rate versus threshold (t) related to FMR and FNMR.

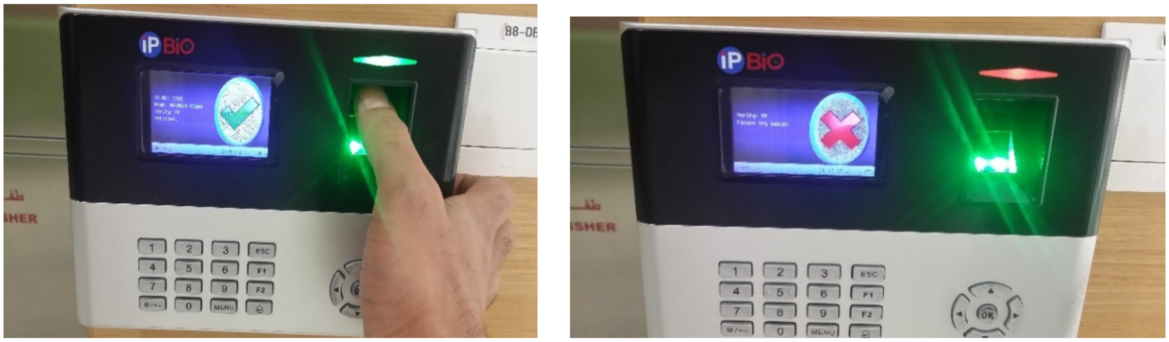

Fig. 6: Actual existing fingerprint system in AOU.

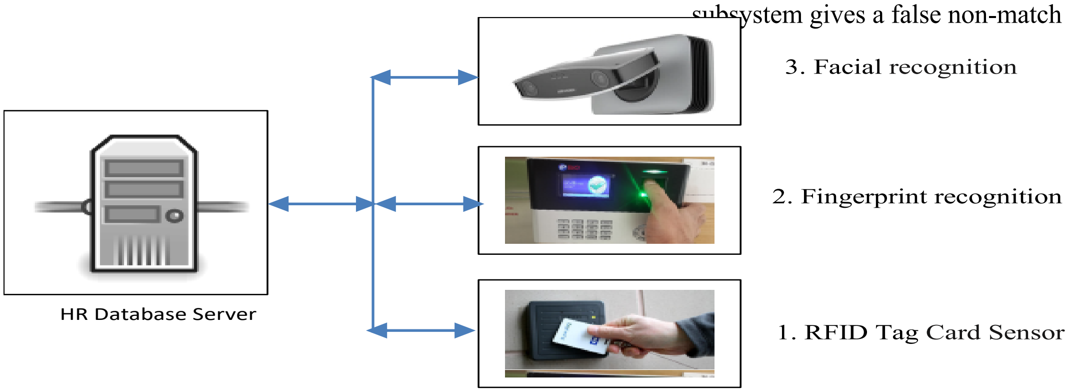

Fig.7: Suggested Modified Automated Authentication Attendance System layout.

First step of authentication procedure is that employee scan smart card (RFID tag) by car park or main gate barrier sensor while entering or leaving campus. Secondly employee scan fingerprint then his/her minutia pair extracted and send to HR server for verification, at same location and time the faces captured at with finger print of taken 50 AOU employee samples by given recognition system camera, mounted at same location of finger print system as shown in figure 7, which capture employee face which is represented by only 13 numbers send to the HR server for verification, for which the file size is considerably smaller than the file size of the original facial image then to be compared to a reference value of employee face stored in HR database system. The employee has to scan his finger print and camera will capture employee facial pattern automatically at the same time.

After testing result of 50 employee's samples for both finger print and facial, FMR and FNMR rates (denied samples out of total 50 samples) have been calculated respectively for both fingerprint & facial result as follow:

- The FMR of the fingerprint subsystem is 1%
- The FNMR of the fingerprint subsystem is 6%.
- The FMR for the face subsystem is 4%
- The FNMR for the face subsystem is 8%
- A false match can only occur if both subsystems wrongly match.
- FMR of the combined system can be calculated as given in equation 1:

$$FMR_c = FMR_1 \text{ x } FMR_2 \qquad (1)$$

- $FMR_c = \frac{4}{100} \times \frac{1}{100} = \frac{4}{10000} = 0.0004 = 0.04\%$
- This means the FMR_c of the combined system is much smaller (at 0.04%) than is the FMR of either of the two constituent systems (which are 4% and 1%) which means higher security.

- $FNMR_c$ of the combined system, a false non-match can occur if either the face subsystem or the fingerprint subsystem gives a false non-match
- $FNMR_c$ of the combined system can be calculated as given in equation 2:
- $FNMR_c = FNMR_1 + FNMR_2 – (FNMR_1 \text{ x } FNMR_2)$ (2)
- From probability theory: $FNMR_c$ of the combined system is
- $FNMR_c$ = 6% + 8% – (6% × 8%) = 14% – 0.48% = 14.48%.
- The $FNMR_c$ of the combined system has not gone down but it has gone up (less convenience)

Whether this $FNMR_c$ value is acceptable would depend on the situation. In conclusion, FMR_c minimized to 0.04%, so no more illegitimate users will be allowed to access system, but more legitimate users will be denied access but $FNMR_c$ should be kept with acceptable level to be more convenience decided by security administrator.

4 Conclusions

The evolution of computerized time and attendance systems provide AOU a means to produce accurate and efficient payrolls. Biometric "time clocks" raise the benefits of these systems to a new level. By verifying the identity of each person as they punch, biometric systems ensure payroll accuracy. The cost savings gained by the elimination of badge administration further bolsters the system's return on investment. Badge based terminals will continue to be a part of the time and attendance landscape. Ease of use, speed and system integration are important factors in choosing a time and attendance system. Different applications require different solutions whether they are biometric, badge, or another technology, biometrics make the dream of payroll accuracy a reality, as final conclusion security increased where using suggested combined biometric FMRC reduced to 0.04% (higher security), better than using one biometric type FMR (which are 4% and 1%), where fewer illegitimate users will be allowed access, but FNMRC increased to 14.48% which indicates that more legitimate users will be denied access (less convenience). Suggested system implement using RFID card, fingerprint and facial recognition attendance system. Due to the benefits of the automated system for monitoring staff attendance that was developed in this study, the system is hereby recommended to all private and government organizations in other AOU branches in order to take proper records and manage the staff activities in their organization.

The future scope of this study is to manage risks in suggested biometric security system; it is desirable to identify the possible risks and their causes and consequences which are known as Risk Assessment, where risk assessment consists of two stages: risk analysis and risk evaluation.

- Risk analysis consists of identifying and describing the possible sources of risk and then estimating how likely each risk is to occur and how severe its impact would be on suggested system.

Risk evaluation consists of deciding what steps need to be taken to avoid or prevent each risk – or whether the impact of a particular risk is sufficiently low that no action needs to be taken.

References

[1] Judith Williams, Roger Jones and Patrick Wong Communication and Information technology. Open university-UK., 2012.

[2] Aberdeen, F, Time Management System in Organization. Wesley Pub. London,2008.

[3] Crowell, K, Importance of biometric Technology. Carnegie Mellon University., 2002.

[4] Feng Zhao and Xiaoou Tang, "Preprocessing and post-processing for skeleton-based fingerprint minutiae extraction", Pattern Recognition Society, Published by Elsevier Ltd., 2006.

[5] Sheetal, V. and Chander, K. Biometric Recognition system: An introduction. Department of computer science and applications k.U; Kurukshetra, Haryana, India., 2012.

[6] Swanirbhar, M. and Saurabh, P. Biometrics: Concepts, Methodologies, Tools and Application. Management Association, Information Resources. IGi Global Publisher., 1852, 2016.

[7] Trucco E. Introductory Techniques for 3D Computer Vision. Prentice-Hall, Vision and Pattern Recognition.,1998.

[8] Clodfelter, R .Journal of Retailing and Consumer Services Biometric technology in retailing : Will consumers accept fingerprint authentication ? Journal of Retailing and Consumer Services., **17(3)**, 181–188, 2010.

[9] Abhyankar, A., & Schuckers, S. Integrating a wavelet-based perspiration liveness check with fingerprint recognition., **42**, 452–464, 2009.

Abdulrahman Al-Awadhi was born in Kingdom of Bahrain in 1963. He studied in Bahrain for all school grades and continued Diploma in Bahrain University. He received Bachelor degree in Electrical and Electronic Engineering from Roger Williams University, RI, USA in 1987, and Ph.D. degree in Electrical and Electronic Engineering from Bradford University, Bradford, UK in 1994.

He started his professional work in 1995 by establishing his own American franchised IT training center in the name of "New Horizons computer Learning Center" in Kingdom of Bahrain. In March 2007, he started his academic carrier by joining Arab Open University AOU as lecturer then promoted to assistant professor within the first year. In 2010, he promoted as head of IT department in AOU Bahrain Branch. He appointed as Acting Director in AOU Bahrain from January 2011 to September 2013. His main interest of research is IT and E-learning technology.

Dr. Al-Awadhi, Assistant Professor, is currently head of research committee in AOU Bahrain. He is also member of few consulting committees in some of the private universities in Bahrain.

Dr. Sarmad Mohammad (PhD Computer Science). B.Sc. degree in Control & System Engineering-University of Technology (UOT)-Baghdad-Iraq, graduated in 1978 with grade good (78%) ranked the third out of fifty-four graduates M.Sc. degree in Electronic Engineering (UOT) Baghdad-Iraq graduated in 1984 with grade good (77%). Dissertation (Microprocessor based remote KWH meter reading).

Ph.D. degree in computer science oriented to image processing. Hungarian Academy of Science (MTA)- (KFKI)- Budapest - Hungary 1993. Dissertation (Performance Improvement of Image Processing Workstation oriented to orthogonal transforms).

More than 20 years teaching experience in various IT courses, currently assistant professor in ITC –Arab Open University (AOU) teaching various computer topics in Computer Science department Sept. - 2010 Kingdom of Bahrain. http://www.aou.org.bh

Research area: e-learning, image processing & computer security.