Biometrics: Effectiveness and Applications within the Blended Learning Environment

Mohamed Sayed[1] and Farid Jradi[2]
1. Faculty of Computer Studies, AOU
(On Leave from Alexandria University, Faculty of Engineering)
P.O. Box 830 Ardiya 92400, Kuwait, msayed@aou.edu.kw
2. Faculty of Computer Studies, AOU
P.O. Box 830 Ardiya 92400, Kuwait, fjradi@aou.edu.kw

Abstract

Learning methods have been benefited by a large act of recent systems based on the merging of several models of teaching. Blended learning philosophy has undergone a deep change with the internalization of new engineering sciences such as biometric. While it is known that passwords or PIN should never be stored in the clear, biometric technologies are becoming the foundation of an all-inclusive array of highly secure identification and personal verification solutions. In this paper, we present an in depth discussion the effectiveness of applying different types of biometrics in blended learning environments. We outline an implementation and report the effectiveness of the fingerprint model as a secure biometric method on a database consisting of 13000 students.

Keywords: Blended learning, biometrics, e-learning, fingerprint matching, information technology.

1. Introduction

Technology provides speed and convenience for people and hence become a vital tool in the educational process. In a blended learning model where face to face learning is combined with technology, students and tutors as well as other stakeholders use computers and the internet to communicate and collaborate. The role of the internet provides opportunities to analyses the electronic activities performed for capturing patterns, trends and intelligence.

Blended learning is a means of teaching and learning which incorporates e-learning with traditional learning under one form. The philosophical system of blended learning based on maximizing the utilization of the information technology applications in the design of novel learning situations that combine classroom education and e-learning instructions. The e-learning tools such as software, computer facilities and the internet are merged with regular tutorials in which tutors meet with learners face to face most often. Face to face is a traditional synchronous method of learning while e-learning uses technology to provide synchronous and asynchronous pedagogy. In blended learning environment, the primary way of interaction between the students and the tutor is via electronic online systems, whereas the face-to-face interaction constitutes a secondary way of interaction. This could bring in a lot of troubles for the identification of students due to the insufficient contact meetings between the students and the tutor. Consequently, we explore the biometric methods used in identification mainly the fingerprints in solving the security problems emerged from the blended learning environment. Besides, it could be used effectively in the identification of females who are wearing the veil in the Middle Eastern countries in the exam attendance without any sensitivity.

Biometrics is automated methods of identifying a person based on a physiological or behavioral characteristic. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. Examples of physiological characteristics include hand or finger images, facial features, and iris recognition. Behavioral characteristics are traits that are determined or acquired dynamic signature verification, speaker verification, and keystroke dynamics are examples of behavioral features [5]. Biometrics has several advantages over traditional methods such as ID cards (tokens) or PIN numbers (passwords) for several grounds: (i) the person to be identified is required to be physically present at the point-of-identification; (ii) identification based on biometric techniques obviates the need to remember a password or carry a token. With the increased integration of data processors and internet into our daily lives, it is necessary to protect sensitive and personal information.

Biometric system is basically a pattern recognition scheme which recognizes a user by defining the genuineness of a specific anatomical or behavioral characteristic possessed by the user. Several significant events must be believed in planning a practical biometric system. First, a user must be enrolled in the system so that his biometric template or extension can be seized. This template is securely stored in a central database or a smart card issued to the user. The template is utilized for matching when an individual needs to be identified. Depending on the setting, a biometric system can work either in verification (authentication) or an identification mode [9].

The remainder of the paper is coordinated as follows: in section 2 we go through the definition and philosophical system of blended learning, section 3 focuses on biometrics and shows that biometrics, as a highly secure identification, is automated methods of telling apart a person based on a physiological or behavioral characteristic, section 4 outlines the use and strength of biometrics in a blended learning environment, section 5 shows the observational results, and conclusion is given in section 6.

2. Blended learning approach

Improving learning outcome has always been an important motivating factor in educational inquiry. In a blended learning environment where e-learning and traditional face to face class tutoring are combined, there are chances to explore the use of technology in improving the learning environment. Blended learning can be delineated as a learning platform where more than one type of learning is being utilized with the aim of optimizing the learning results and the cost of learning. There are many schools of thought on learning, and no one of them is applied exclusively to design blended learning materials. As there is no single learning theory to follow, we can employ a combination of theories to develop the material of blended learning. These existing learning theories, however, were developed before distributed and networked learning was used widely. In fact, we do not require a new stand-alone theory for blended learning, but a model that incorporates the different theories to steer the design of blended learning materials.

Blended learning provides opportunities for both self and cooperative learning, hence integrates all of these with the active-learning which is based on the new technologies. Blended learning also gives a beneficial opportunity to know different cultures, directs the learner toward research hand survey, provides feedback on time, and simulates the direct communication with the tutors. It is worth mentioning that the blended learning does not proceed with a fixed daily routine, but it sweeps over the phenomenon of boredom experienced by learners. It works to raise the motivation and the need to get a line that leads to create a state of satisfaction and acceptance to the learners. Moreover, blended learning increases the student’s engagement with the course because technology eases the communication between individuals or groups as easily as enabling access to the world wide network of knowledge. Blended learning courses can be visualized in a customized way that causes all kinds of students in their journey to knowledge. These courses are repeatable, containing quizzes, including both synchronous and asynchronous forums. They also contain instant feedbacks, chats, and emails which are monitored by specialists and accessible at convenient times. Active involvement of students in the learning process is important and improves the students’ grades and performance. Prior studies, see for instance [1], showed that learners who are active in their knowledge inquiries have better grades than learners who are receptive only.

Information technology can be utilized to increase the accumulation of information, concepts and accomplishments associated with the studied subjects and to assist learners and tutors to cope with the nature of the new digital community. In addition, information technology may be used to operate along the compatibility between various inflated and renewed information in different branches of cognitive life. It gives learners the fun and excitement, attains the learning more active, and its contributions effectively appear in teaching the disciplines that may symbolize the difficulty of the scholars. The reader who would wish to discover more about blended learning and the e-learning part of blended learning is referred to [4, 14, 15, 16].

3. Biometrics

There are many types of biometrics currently in use, and many more types to come in the very near future (DNA, holograms, etc.). Today, some of the most common ones in use are fingerprints, face recognition, iris recognition and hand and finger geometry.

Fingerprints: The patterns of friction ridges and valleys on an individual’s fingertips are unique to that individual. For decades, law enforcement has been classifying and determining identity by matching key points of ridge endings and bifurcations. Single of the most commercially available biometric technologies, fingerprint recognition devices for desktop and laptop access are now widely available from many different vendors at a low price. With these devices, users no longer ask to type passwords-instead, a touch provides instant access. Fingerprint systems can also be used in identification mode, see [7].

Face recognition: The identification of a person by their facial image can be managed in a numeral of different ways, such as by capturing an image of the face in the visible spectrum using an inexpensive camera or by utilizing the infrared patterns of facial heat emission. Facial recognition in visible light typically models key features from the central portion of a facial image. Using a wide assortment of cameras, the visible light systems extract features from the captured images that do not change over time, while avoiding superficial features such as facial expressions or hair. Some of the challenges of facial recognition in the visual spectrum include reducing the impact of variable lighting and detecting a mask or photograph. Some facial recognition systems may require a stationary or posed user in order to capture the image, though many systems use a real-time process to detect a person's head and locate the face automatically. Major benefits of facial recognition are that it is nonintrusive, hands-free, continuous, and accepted by most users.

Iris recognition: This type recognition method uses the iris of the eye, which is the colored area that surrounds the student. Iris patterns which are thought to be unique are obtained through a video-based image acquisition system. Iris scanning devices have been used in personal authentication applications for several years. Systems based on iris recognition have substantially decreased in price, and this trend is expected to continue. The technology works well in both verification and identification modes (in systems performing one-to-many searches in a database). Current systems can be used even in the presence of eyeglasses and contact lenses. The technology is not intrusive and does not require physical contact with a scanner. Iris recognition has been demonstrated to work with individuals from different ethnic groups and nationalities.

Hand and finger geometry: These methods of personal verification are well established and have been available for over 30 years. To achieve personal verification, a system may measure physical characteristics of either the fingers or the hands. These include length, breadth, thickness, and surface area of the hand. One interesting characteristic is that some systems require a small biometric sample (a few bytes). Hand geometry has gained acceptance in a range of applications. It can frequently be found in physical access control in commercial and residential applications, in time and attendance systems, and in general personal authentication applications.

Wireless biometrics will offer biometric authentication services to wireless and internet service providers. The technology will allow customers of wireless services and products to authenticate their identities when conducting electronic transactions. With the coming of wireless biometrics, biometrics systems are advent of age with the combination of engineering sciences that make new application options. The combination of fingerprint identification and wireless communication allows new fields of biometrics integration. As biometrics systems improve, become smaller and require less power for operation, the potential to integrate into new application grows. The power to operate the biometrics verification solution from battery supply is unprecedented. For instance, wireless biometrics consists of both the hardware and software for the fingerprint scanning devices that will be embedded in wireless handheld devices. The solution will come as a bundle of a range of validation, transaction management and content protection services based on the devices [18].

3.1 Structure and accuracy of biometric systems

A typical biometric system is composed of the following five integrated components [11]:

- A detector is applied to gather the information and convert the data to a digital format.
- Signal processing algorithms perform quality control actions and acquire the biometric template.
- A data storage component keeps information that new biometric template will be likened to.
- A matching algorithm compares the new biometric template to one or more templates kept in data warehousing.
- A decision procedure (either automated or human-assisted) uses the results of the matching component to create a system-level decision.

Technologies used in biometric system should be considered and evaluated giving full consideration to the following features [12]:

- Universality: Every person should have the characteristic. People who are mute or without a fingerprint will need to be adapted in some way.
- Uniqueness: Generally, no two people have identical features. Nevertheless, identical twins are hard to be distinguishable.
- Permanence: The characteristics should not change with time. A person's facial expression, for instance, may change with age.
- Collectability: The characteristics must be easily collected and measurable.
- Performance: The method must deliver precise results under varied environmental conditions.

- Acceptability: The general public must accept the sample collection routines. Nonintrusive methods are more satisfactory.
- Circumvention: The technology should be difficult to deceive.

3.2 Biometric systems: verification vs. identification

Verification (Am I who I claim I am?) involves confirming or denying a person's claimed identity by comparing a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample (for example, a fingerprint captured during a login). During the enrollment a sample of the biometric trait is captured, processed by a computer, and stored for later comparison [20].

On the other hand, in identification, the system has to recognize a person (Who am I?) from a list of *N* users in the template database whereby the biometric system identifies a person from the entire enrolled population by searching a database for a match based solely on the biometric. This is sometimes called one-to-many matching. Identification is a more challenging problem because it involves 1 to *N* matching compared to 1 to1 matching for verification, see [21].

3.3 Why biometrics

Utilizing biometrics for identifying human beings offers some unique advantages. Biometrics can be used to identify you as you. Tokens, such as smart cards, magnetic stripe cards, photo ID cards, physical keys and so forth, can be lost, stolen, replicated, or left at home. Also, passwords can be forgotten, shared, or observed. Moreover, today’s fast-paced electronic world means people are asked to remember a multitude of passwords and personal identification numbers for computer accounts, bank ATMs, e-mail accounts, wireless telephones, websites and so forth. Biometrics has the promise of fast, easy-to-use, accurate, honest, and less expensive authentication for a diversity of applications.

There is no one perfect biometric that fits all needs as well as each biometric system has its own advantages and disadvantages. There are, nevertheless, some common characteristics needed to make a biometric system usable. First, the biometric must be based upon a distinguishable trait. For example, for over a century, law enforcement has used fingerprints to identify people. There is a great deal of scientific data supporting the idea that no two fingerprints are alike. Technologies such as hand geometry have been employed for many years, and technologies such as, face or iris recognition has come into widespread usage [19, 22]. Some newer biometric methods may be just as accurate, but may need more research to show their uniqueness. The procedure should be ready and comfortable, such as throwing a photograph taken by a TV camera, speaking into a microphone, or matching a fingerprint scanner. Low price is significant, but most understand that it is not just the initial price of the sensor or the matching software that is required. Often, the life cycle support cost of providing system administration and an enrollment operator can overtake the initial cost of the biometric hardware.

In the end, the advantage that biometric verification provides is the ability to require more instances of verification in such a prompt and comfortable manner that users are not troubled by the additional demands. As biometric technologies mature and come into wide commercial use, dealing with multiple levels of verification or multiple instances of verification will become less of a burden for users.

3.4 Ethical issues around biometric identification technology

Many of the concerns people have about the role of biometric technologies for authentication and identification are related to ethical matters such as personal liberty, the confidentiality of personal data and the potential for abuse of such data. Will the biometric data be improperly collected, handled or stored? Will it be shared among different organizations without the individual’s knowledge or consent? Will it be used for purposes for which it was not originally collected for? Basic fears can be summed up as follows: privacy, social businesses, legal businesses and medical concerns.

4. Effectiveness of biometrics in blended learning

Some educational institutions begin to include blended learning as an alternative way of instruction. Using biometric in blended learning will facilitate the learning process as well as enhance the security through providing reliable trustworthy means for authentication. This will assist in bridging the gap between traditional and blended learning and lead to impose a good reputable image about blended learning. Likewise, using biometrics could be employed in introducing new feasible and effective online assessments in the learning process.

Presently, the student identities are authenticated through asking the student to sign beside his/her figure along the attendance sheet or checking through Learning Management system (LMS) attendance screen. These traditional ways for authentication could introduce a great deal of problems such as wasting time and losing control during taking attendance. Moreover, these ways are not dependable enough to preclude students from attempt cheating in exams through trying some students to perform exams in lieu of other scholars. Using biometrics such as fingerprint in blended learning will improve exam's security as well as enhance control over student attendance. For instance, fingerprints might be used in automating the verification of the student's attendance to tutorials. This is caused by putting in a fingerprint device at the ingress of the tutorial room. When the student puts down the tutorial room, his fingerprint will be read by the device which will enter the date and time of the attendance. At the conclusion of the semester, the student information system (SIS) will furnish a complete report about the student's attendance in a certain class. This information would be supplied to the department as well as to the student's parents.

Different biometric tools could be used for student's authentication like face recognition, iris recognition, voice identification, and so on. For instance, voice recognition could be utilized to authenticate a student doing some oral questions in an assignment. In this case, the computer system should be trained enough through a set of the student's voice print so that the entered voice could compare to perform the mating operation. It could as well aid in the certification procedure of some online verbal exams. For instance, some tests might require the students to do verbal answering for some queries. A spoken language recognition tool is implemented inside a learning management system (LMS). This instrument is applied to authenticate the student's answers through comparing student's voice print with the recording student's voice in the verbal activity. Through this technique, verbal activities in online assignments can be authenticated and verified. Nevertheless, the matching process for voice recognition may come across just about troubles which may contribute to inaccurate results. For example, a man catching a cold may alter his tone which will result in false recognition for his voice. Another drawback for voice recognition is that some humans have the talent to mimic sounds which can be utilized in doing plagiarism. The testing environment is an additional constraint on the voice recognition process whereby the voice signature needs to be recorded in a very calm platform. Any noise accompanied by the recording process may lead to improper recognition and subsequently false matching.

In a similar pattern, face recognition could be utilized for authentication process like authenticating a student making out an exam remotely. In this case, a webcam could be utilized to get the student's face that will be broadcast to a recognition system which will execute the comparison with a saved student's face print to perform the mating operation. An authentication system based on face recognition could suffer from high bandwidth demand; denial of some users due to privacy issues especially the girls wearing veils and setup environment.

For the above reasons and others, the fingerprint recognition system is advocated to be used in blended learning environment as it is cheaper to implement, does not involve training for users, simple to apply, give more accurate recognition results and easy to deploy when compared to other biometric systems. Moreover, using the fingerprint as an authentication tool for verifying student's attendance will assist in working out many social conflicts that could rise from the student's verification process in exams, especially for girls wearing the veil which is a real sensible and critical social issue for many people in the Islamic order. The application of fingerprint will bypass this problem and eliminate the need for girls to remove the veils in order to be placed. Another utilization of biometrics in blended learning is in conducting online exams whereby the fingerprints used to authenticate the student's identity which once correctly verified will activate the online exam screen and open a session for the student allowing him to take up the exam.

5. Fingerprints model

The design of a secure system for such biometric modalities requires an additional attention. This section models the fingerprints as a secure biometric storage problem. In this section we present some basic information about fingerprints and show how original biometric is stored on the device to allow decryption or authorized access. Our matching technique is described and some suggestions are put set forth. The system that is in use relies on matches against fingerprint templates previously stored.

5.1 Background

Fingerprint identification is the oldest method that has been successfully utilized in several applications. A fingerprint, as the name suggests, is the print or the impression made by our finger because of the patterns formed on the skin of our palms and fingers. It is fully formed at about seven months of fetus development and finger ridge configurations do not change throughout the life of an individual. Each of our ten fingerprints is different from one another and from those of every other person [8]. Even identical twins have different fingerprints. That makes them ideal for personal recognition. With age these marks get prominent, but the shape and the structures present in those fine lines do not undergo any alteration. For their permanence and unique nature, they have been used for not only in identification, but as well in the sphere of security as criminal and forensic investigation for a long time [13].

5.2 Outline and goals

Fingerprint device is utilized to authenticate student's attendance during the examinations. This could be made out as follows: Once the student accepted into the university, his/her fingerprint will be taken and saved in his record in the student information system (SIS). During the examination, the student will be required to introduce his/her ID number along with his/her fingerprint to the fingerprint device. A security module in SIS will compare his entered fingerprint with the preserved copy in SIS and confirm the authentication if matching occurs [17].

We use fingerprint device to authenticate student's attendance in doing online tests. This could be carried out as follows: Once a student registers in a course, his/her signature in SIS will be replicated into the student's course registration record. Before performing the online exam, the student will be prompted to enter his/her fingerprint on the fingerprint device which is plugged in to the computer placed in the examination room. The entered fingerprint will be matched to the preserved copy in the course registration record. If matching occurs, the exam screen on the computer will be activated and the student will be able to do the online exam [2].

Fingerprint device is likewise applied to authenticate student's attendance in classes. This could be enforced as follows: The lecture rooms will be fitted with fingerprint device connected to the learning management system. In one case a student goes to the lecture, he/she will be required to go in his fingerprint to the fingerprint device. The entered fingerprint will be compared to save a copy in the student's course registration record. If matching occurs, the student will be scored as present in the lecture at that particular engagement.

5.3 Capturing data

With the arrival of innovative electronic technologies, fingerprints for students can now be recorded digitally by scanning the fingertip. The scanning process is gentle, quick (it takes a few seconds) and clean (no ink is needed, unlike for traditional fingerprinting). Fingerprint sensors work in a similar manner, merely they are specifically planned to capture details of the fingertip. The sensors are usually arranged in a two-dimensional array and protected by a transparent layer of glass or plastic.

5.4 Matching phase

Fingerprint matching is a procedure of assessing the level of similarity (or difference) of two given fingerprints. The effect of the matching process could be a similar value, or it could be a decision of either match or no match. Either path, an algorithm is required to assess the overall conflict between the two fingerprints. When the result of the matching is involved to be a decision (match or no match), a threshold is required. The level of similarity between two fingerprints has to be more eminent than the threshold for the system to consider them as a match. The threshold is usually set according to the required security level: the higher the threshold, the more unmanageable it is for two fingerprints to be considered as a match; the lower the threshold the easier it is for them to be considered a match [10].

5.5 Errors in biometric recognition systems

The sensitivity of a fingerprint recognition system is determined by thresholds. The thresholds used in biometric recognition systems to set the balance point between security and convenience. For instance, when a threshold is set too low, different biometric data can appear to match when they are not the same. This is experienced as a false match. Conversely, when a threshold is set too high, biometric data from the same person can seem not to match because of slight variations. This is known as false non-match. False match refers to incorrectly think that two given sets of biometric data are matched [3]. The consequence of the former error is that imposters could gain access to resources they are not permitted to access. False non-match refers to incorrectly believe that two given sets of biometric data are not matched. The result of the latter error is that legitimate users could be declined access to resources they are entitled to access. False match is referred to as 'false acceptance' or 'false positive' and false non-match as 'false rejection' or 'false negative'. In practice, these two types of error are unavoidable with current technologies, but, ideally, both types should be kept to a minimum.

5.6 System implementation

The system includes two main components which are hardware and software tools.

Hardware component: Fingerprint sensor device along with an LCD screen is located at the entry of each classroom. The fingerprint sensor is employed to capture the fingerprints of students while the LCD screen notifies the student that his/her attendance has been marked [9].

Software tools: For the development of the system, the following software tools were used: Digital Persona's Software Development Kit [6], Microsoft Visual Studio 2008 and SQL Server 2005.

Database storage contains the fingerprint templates of students along with their information (names, registration numbers and subjects/lectures). When student enrolls his/her finger on the scanner his/her fingerprint is matched with database to mark the attendance.

6. Conclusion

Recent improvements in biometric technologies have resulted in increased accuracy at reduced price. Biometric technologies are posing themselves as the basis for many highly secure identification and personal verification solutions. Today's biometric solutions offer a means to accomplish fast, user-friendly verification with a high degree of accuracy and cost savings. Many biometric technology providers are already delivering biometric verification for a variety of web-based and client/server-based applications to fill these and other demands. Continued advances in technology will bring increased performance at a lower price.

Interest in biometrics is growing substantially. Evidence of the growing acceptance of biometrics is the availability in the marketplace of biometric-based verification solutions that are becoming more accurate, less expensive, faster, and easier to use. While biometric verification is not a magical answer that solves all authentication concerns, it will make it softer and cheaper for you to apply a variety of automated data systems. Future work will concentrate on using syndrome coding to provide a secure means of storing biometric data.

References

[1] Ahn, J., Weng, C. and Butler, B. (2013), "The Dynamics of Open, Peer-to-Peer Learning: What Factors Influences Participation in the P2P University", Proceeding of the 46th Annual Hawaii International Conference on System Sciences (Learning Analytics and Networked Learning track).

[2] Anumolu, M.B. and Bharadwaj, N. (2013), "An Online Examination System Using Wireless Security Application", International Journal of Engineering Trends and Technology (IJETT), **4** (9**)**, 3385-3387.

[3] Blackburn, D., Miles, C. and Wing, B. (2006), "National Science and Technology Council (NSTC), Subcommittee on Biometrics".

[4] Chen, C. and Jones, K. (2007), "Blended Learning vs. Traditional Classroom Settings: Assessing Effectiveness and Student Perceptions in an MBA Accounting Course", Journal of Educators Online, **4** (1**)**, 1-15.

[5] Higgins, P.T., Woodward, J.D. (jr) and Orlans, M.N. (2003), "Biometrics", McGraw Hill Osborne: New York.

[6] http://www.digitalpersona.com, Digital Persona, Inc. 720 Bay Road Redwood City, CA 94063 USA.

[7] Jain, A. and Aggarwal, S. (2012), "Multimodal Biometric System: A Survey", International Journal of Applied Science and Advance Technology, **1** (1), 58-63.

[8] Maltoni, D., Jain, A.K. and Prabhakar, S. (2005), "Handbook of Fingerprint Recognition", Springer: New York.

[9] Nawaz, T., Pervaiz, S., Arash K. and Azhar, U. (2009), "Development of Academic Attendance Monitoring System Using Fingerprint Identification", IJCSNS International Journal of Computer Science and Network Security, **9** (5), 164-168.

[10] Podio, F.L. and Dunn, J.S. (2005), "Biometric Authentication Technology: From the Movies to Your Desktop", NIST, 100 Bureau Drive, Stop 1070, Gaithersburg, MD20899-1070 [US Department of Commerce, 1401 Constitution Avenue, NW, Washington DC 20230].

[11] Raina, V.K. (2011), "Integration of Biometric Authentication Procedure in Customer Oriented Payment System in Trusted Mobile Devices", International Journal of Information Technology Convergence and Services, **1** (6), 15-25.

[12] Raina, V.K. and Pandey, U.S. (2011), "Biometric and ID Based User Authentication Mechanism Using Smart Cards for Multi-server Environment", INDIACom-2011, 5th National Conference on 'Computing for Nation Development' on 10-11 March, 2011 at BVICAM, New Delhi.

[13] Ratha, N. and Bolle, R. (2004), "Automatic Fingerprint Recognition Systems", Springer: New York.

[14] Sayed, M. (2013), "Blended Learning Environment: The Effectiveness in Developing Concepts and Thinking Skills", Journal of Education and Practice, **4** (25), 12-17.

[15] Sayed, M., Baker, F. (2014), “Blended Learning Barriers: An Investigation, Exposition and Solutions”, Journal of Education and Practice, **5** (4), 1-9.

[16] So, H.J, Bonk, C.J. (2010), “Examining the Roles of Blended Learning Approaches in Computer-Supported Collaborative Learning (CSCL) Environments: A Delphi Study”, Education Technology & Society, **13** (3), 189-200.

[17] Vacca, J.R. (2005), “Public *Key Infrastructure: Building Trusted Applications and Web Services*”, CRC Press.

[18] Vacca, J.R. (2006), “*Guide to Wireless Network Security*”, Springer.

[19] Vacca, J.R. (2006), “*NIST and Biometrics*”, NIST, 100 Bureau Drive, Stop 1070, Gaithersburg, MD 20899-1070 [US Department of Commerce, 1401 Constitution Avenue, NW, Washington DC 20230].

[20] Vacca, J.R. (2007), “*Biometric Technologies and Verification Systems*”, Elsevier Science & Technology.

[21] Wayman, J.L., Jain, A.K., Maltoni, D. and Maio, D. (2005), “*Biometric Systems Technology, Design and Performance Evaluation*”, London: Springer.

[22] Yang, J. (2010), “*Biometric Verification Techniques Combing with Digital Signature for Multimodal Biometrics Payment Systems*”, IEEE International Conference on Management of e-Commerce and e-Government, 405-410.