Journal of Engineering and Applied Sciences 14 (22): 8180-8186, 2019
ISSN: 1816-949X

Secure Mobile Learning System using Voice Authentication

Teaba Wala Aldeen Khairi
Department of Computer Science, University of Technology, Baghdad, Iraq

Abstract: In the last decade, the demand for learning through mobile devices has been increased, however, the security and authentication of these systems have less attention. This is because of researchers desirability to be more famous by unauthenticated publishing of their articles. Therefore, this study presents a proposed voice authentication for mobile learning (m-learning) system as a secure solution. In the proposed system, each of the server and clients (learners) in the designed learning system is provided with voice features extraction algorithm. HPSO algorithm is used for extraction the wavelet frequency domain features. These extracted features are then matched with stored database in order to give the permission of learning system accessibility. For (LL subband) FAR is 0.0, FRR is 0.01 and CVR is 99%. For (LL, LH, HL and HH) FAR is 0.0, FRR is 0.0 and CVR is 100%. The voice recognition time is about 1.04 sec.

Key words: Mobile learning, voice authentication, HPSO, wavelet transform, FAR, FRR, CVR

INTRODUCTION

The usage of mobile technology is growing and it affects other technologies by bringing in new innovation and methods. The reason for this growth is not only ease of use and mobility but also improvements in interaction and functionality in different contexts (Zare, 2010).

The m-learning is based on the use of mobile devices anywhere at any time. These devices must support wireless technology and have a possibility to present teaching materials (Georgieva *et al*., 2005).

m-learning generally represents the possibility for learners to participate in educational activities that are adaptable to the "learners mobility" where learning is not confined to a set physical location and time (Su and Cheng, 2013).

m-learning can be thought of as a subset of e-Learning (which is web-based delivery of content and learning management). m-learning is different from conventional e-Learningg. It was the adapting or customizing the content for delivery on mobile devices. Where the individual learners can use the wireless mobile technology for formal and informal learning where they can access additional and personalized learning materials from the internet or from the host organization. In authentication the entity or user is verified prior to access to the system resources. For example, a student who needs to access his university resources needs to be authenticated during the logging process. This is to protect the interests of the university and the student (Bogarin *et al*., 2018).

The traditional methods of authenticating per today depends on three factors that could be Bogarin *et al*. (2018). Something that user knows, this is the most common method for authentication for users often associated with text-based a password, picture-based passwords or a combination of a password and a username for most of web applications. Something that user has: user authentication in this case is based on something that user has a physical object. Something that user is inherent: these methods, referred to as biometrics, centers around authentication based on that person's unique traits. Traits can be physical such as fingerprints, voice or behavior such as walking patterns or typing patterns.

Biometric scanners on mobile devices might be more widespread than what it is today. Therefore, this research aims to design a secure m-learning system depending on voice authentication.

Literature review: Many researchers have proposed many related works about mobile learning and authentication in mobile learning. The following are some studies and researches which can so far, associated with this research. Harward *et al*. (2008), developed at the Massachusetts Institute of Technology a popular example of distributed architecture for remote labs which were iLabs. With iLabs the equipment was managed by Lab servers and authentication and access was moderated by a service broker. By Garcia-Zubia *et al*. (2010), presented the implementation of a new remote lab giving the students the chance to work with real experiments from a social 3D-based immersive environment.

By Nedungadi *et al.* (2011), presented the Virtual Labs Collaborative and Accessibility Platform (VLCAP) use by the large scientific community building multi disciplinary Virtual Labs (VL).

Shonola and Joy (2014), discussed the security concerns of mobile learning from the learner's perspective based on a study conducted in higher education institutions in Nigeria.

By Poljanowicz *et al.* (2014) showed the organization of distance learning, particularly the idea of b-learning, combining the accomplishment of classes carried on in the traditional way and via. computers.

Bahry *et al.* (2015), examined the existing researchers view on security measures on mobile learning. In general they discovered related measure on security which includes reliability, trust, privacy and security itself.

Karthiyayini (2016), explained m-learning concepts, techniques, components and its need have high level of interoperability between each other running on different operating systems.

By Shonola and Joy (2016), presented a mobile security enhancement application, designed and developed for android smart mobile devices in order to promote security awareness among students.

Swarm intelligence and HPSO: In 1989, the expression "Swarm Intelligence (SI)" was first introduced by Ahmed and Glasgow (2012). SI is defined as a relatively new branch of Artificial Intelligence (AI) that is used to model the collective behaviour of social swarms in nature such as ant colonies, honey bees and bird flocks. The computational modeling of swarms was proposed to produce low cost, fast and robust solutions to several complex problems (Ahmed and Glasgow (2012).

Particle Swarm Optimization (PSO) was introduced by Russell Eberhart an electrical engineer and James Kennedy, a social psychologist in 1995. PSO draws inspiration from the sociological behaviour associated with bird flocking. The underlying phenomenon of PSO is that knowledge the optimized solution by using a set of flying particles with velocities that are dynamically adjusted according to their historical performance. As well as their neighbors in the search space by social interaction in the population where thinking is not only personal but also social (Ahmed and Glasgow, 2012). After a series of minor alterations and elimination of the ancillary variables, the updating rules for calculating the next position of a particle were introduced in Eq. 1 and 2:

$$v_{i,j}^{k+1} = v_{i,j}^{k+1} + c_1 r_1 \left(xBest_{i,j}^{k} - x_{i,j}^{k}\right) + c_2 r_2 \left(xgBest_{j}^{k} - x_{i,j}^{k}\right) \quad (1)$$

$$x_{i,j}^{k+1} = x_{i,j}^{k} + v_{i,j}^{k+1} \quad (2)$$

Liu *et al.*(2014), proposed a modified version of PSO based on human behavior which is called Human Behavior Based Particle Swarm Optimization (HPSO). HPSO is proposed to improve the performance of SPSO. In standard PSO (SPSO), all particles only learn from the best particles Pbest and Gbest which it is an ideal social condition. However, considering the human behavior there exist some people who have bad habits will bring some effects on people around them. If we take warning from these bad habits or behaviors it is beneficial to us. Therefore, an objective view on these bad habits must be given. To simulate the human behavior, the global worst particle was introduced into the velocity equation of SPSO and the learning coefficient r3 which obeys the standard normal distribution that is r3 (0,1) can balance the exploration and exploitation abilities by changing the flying direction of particles. When the coefficient is positive it is called impelled leaning coefficient which is helpful to enhance the "flying" velocity of the particle, therefore, it can enhance the exploration ability. When the coefficient is negative, it is called penalized learning coefficient which can decrease the "flying" velocity of the particle, therefore is beneficial for improving the exploitationability. If r3 = 0 represents that these bad habits or behaviors have no effect on the particle. At the same time, the acceleration coefficients c1 and c2 have been replaced with 2 random numbers whose sum is equal to 1 in [0,1] this strategy decreases the dependence on parameters of the solved problem (Liu *et al.*, 2014). Therefore, the velocity Eq. 1 has been changed as shown in Eq. 3:

$$\begin{aligned} V_{i+1}^{d}(t) = {} & V_{i+1}^{d}(t) + r1(t).\left(Pbest_{i}^{d}(t) - X_{i}^{d}(t)\right) + r2(t) \\ & \left(Gbest^{d} - X_{i}^{d}(t) + r3\right)(t).\left(Gwrost^{d} - X_{i}^{d}(t)\right) \end{aligned} \quad (3)$$

In HPSO, the global worst particle is introduced who is of the worst fitness in the entire population at each iteration. It is denoted as Gworst and defined as shown in Eq. 4:

$$Gwrost(t) = \arg\max \begin{Bmatrix} \{f(Pbest_1), f(Pbest_2), \ldots, \\ f(Pbest_N)\} \end{Bmatrix} \quad (4)$$

where, f(.) represents the fitness value of the corresponding particle. Meanwhile, the pseudo code of implementing the HPSO is listed as shown in Fig. 1.

Randomly generate an initial population with positions and velocities
InitializePbest, Gbest and Gwrost

Evaluate fitness of all particles in $X = \{X_1, X_2,\ldots,X_n\}$; $Pbest \Leftarrow X$;
$Gbest \Leftarrow argmin \{f(Pbest_1), f(Pbest_2), \ldots, f(Pbest_N)\}$ Gwrost

$\Leftarrow argmin\{f(Pbest_1), f(Pbest_2),\ldots,f(Pbest_N)\}$

For t = 1 to T do

For each Particle i= 1, 2, …., N

Update velocity according to Eq. (3);

Update position according to Eq. (2) and Eq. (4) ;

End for,

Evaluate fitness of all particles in {X};

UpdatePbest, Gbest and Gwrost

End for.

Return the best solution

Fig. 1: Pseudo code of HPSO algorithm, pseudo code of QPSO algorithm

MATERIALS AND METHODS

The proposed system: The proposed system includes three sides. The first side is the administrator, the second side is the client and the third one is the web application server as shown in Fig. 2.

Administrator (Admin) side: Figure 3 shows the flowchart of the administrator side. The first step in this flowchart is to check the users name and password and then connect with web page of the web server to either giving support or giving lecture.

Client (User) side: On the client mobile side, there is an application in which it was designed by using android studio environment. Figure 4 shows the flowchart of the client mobile side. The first step is testing the client, if (he/she) was authenticated or not by using a new proposed method depending on voice HPSO algorithm.

Web application server: Figure 5 shows the flowchart of web application server. On web application server side there is a (webpage, database and web service).

The website of web application server is designed using Microsoft visual studio environment that provide a web pages using GUI for login screens and interacting. Database is designed in SQL server that serves as the underlying learning repositories.

A critical technique inside the web server is the web service which is shown in Fig. 6. The web service technique is designed by Microsoft Visual Studio environment with a new proposed method for authentication. The proposed method is compatible with

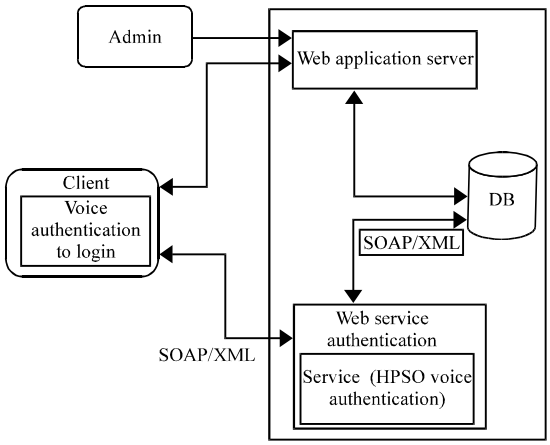

Fig. 2: Block diagram of the proposed system

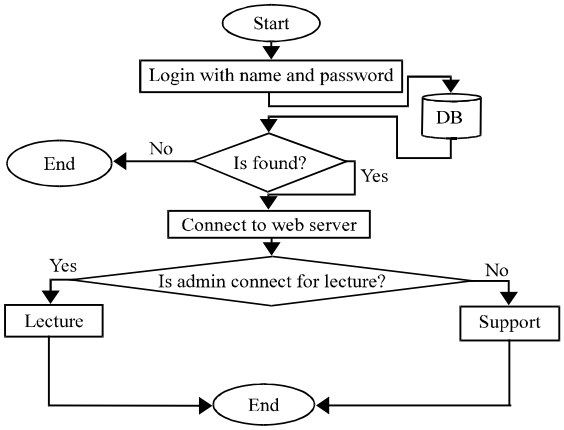

Fig. 3: Flowchart of admin

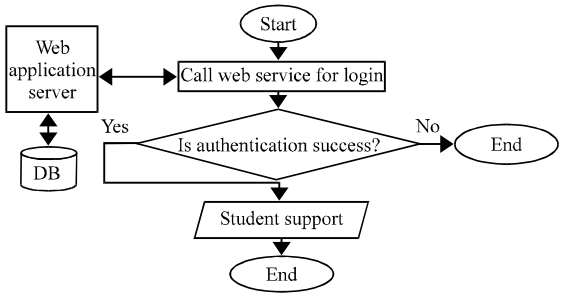

Fig. 4: Flowchart of the client side

client application and it is based on voice (HPSO). All communications that are passed via the web service are done by SOAP (Simple Object Access Protocol) with help of RPC (Remote Procedure Call).

Design of the proposed authentication technique: Client authentication is very important for the success of the

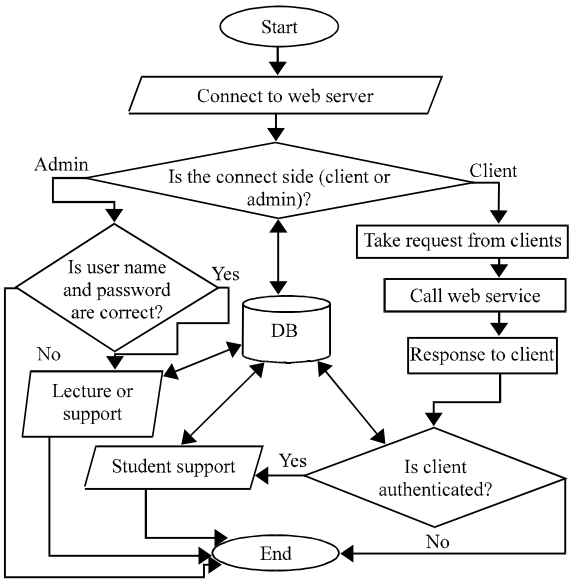

Fig. 5: Flowchart of web server

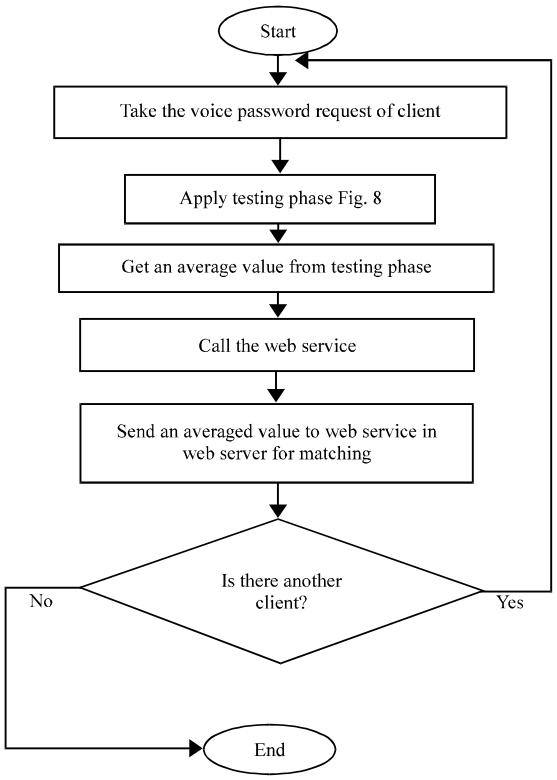

Fig. 6: Flowchart of the web service

proposed virtual learning system. This proposed authentication technique is used between two sides: (the web application server and the client) (Fig. 7 and 8). HPSO voice authentication is done in two phases

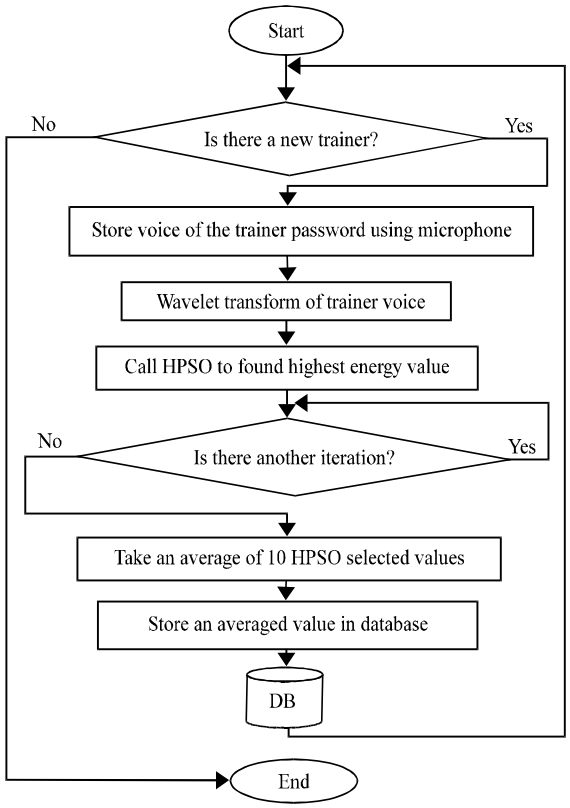

Fig. 7: Flowchart of the training phase in web server

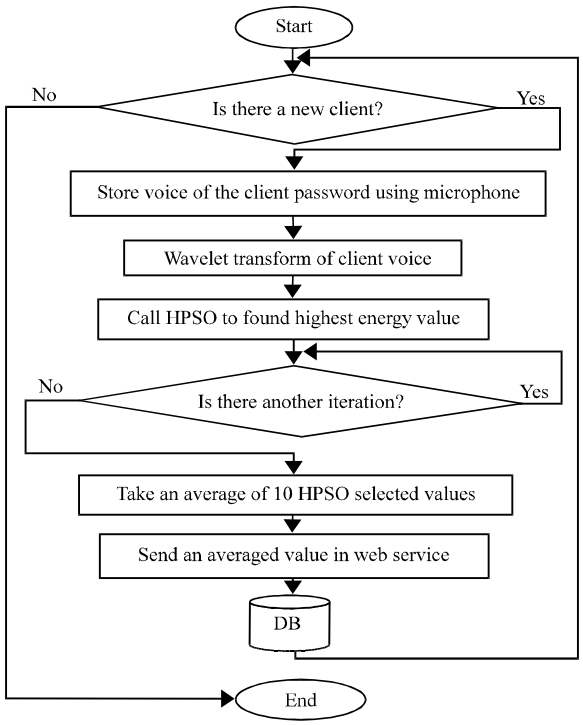

Fig. 8: Flowchart of the testing phase in client side

(training phase and testing phase). The used dataset is built using (30) student (20 males and 10 females) with (83.3% for training and 16.7% for testing). The training phase is done in web application server as shown in Fig. 7. The testing phase is done in client side as shown in Fig. 8.

The permission for client voice authentication is done in web server by matching client testing averaged value with database of tested averaged values. If matching is found then the client is authenticated, otherwise, authentication is failed. The implementation algorithm of normalized wavelet transform is done depending on (Antoine *et al*., 2010). However, HPSO is done depending on Fig. 1.

RESULTS AND DISCUSSION

Figure 9 shows the waveforms of (4) one-word client names which are recoded using the microphone of the computer. The sampling frequency voice is set at the 10000 Hz and the duration period set as 1 sec.

Table 1 shows the HPSO highest energy values for each wavelet subband: (LL, LH, HL and HH) for (4) clients.

Table 2 shows the averaged highest energy values for (4) clients for (10) iterations. Table 3 clarifies the matching (1 to -1) with database which are created in training phase.

Table 4 shows the time required for each iteration of HPSO in extracting highest energy values for the client (A). In order to measure performance of the proposed system Eq. 5-7:

$$FAR = \text{Number of false acceptation/Total number of test sample} \quad (5)$$

$$FRR = \text{Number of false rejection/Total number of test sample} \quad (6)$$

$$CVR = (1\text{-}FAR\text{-}FRR)*100\% \quad (7)$$

Table 5 shows the performance of the proposed system.

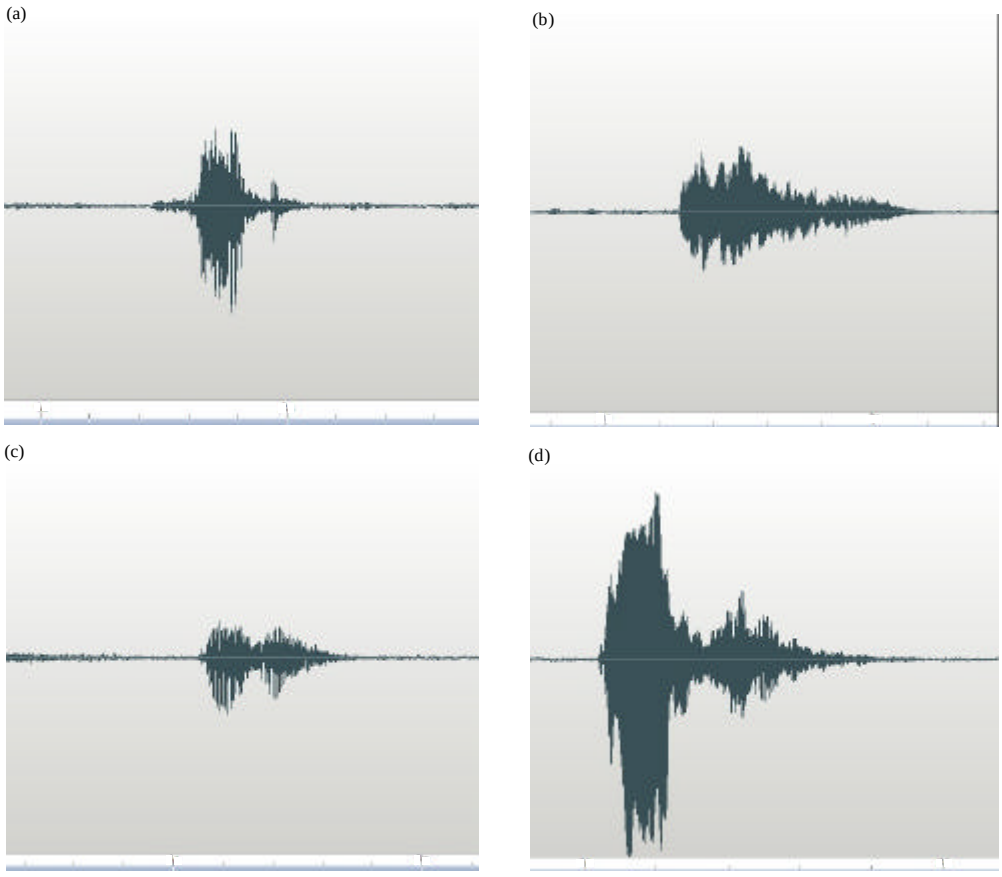

Fig. 9: Waveforms of (4) one-word client names: a) Jack; b) Sarah; c) Adam and d) Katia

Table 1: Highest energy values for 10 HPSO iterations for 4 clients

Clients/HPSO iteration	High energy values (LL)	High energy values (LH)	High energy values (HL)	High energy values (HH)
Jack				
1	162	40	30	18
2	160	42	33	17
3	163	41	31	19
4	159	39	29	18
5	162	43	32	19
6	164	40	34	20
7	161	44	30	19
8	159	45	29	20
9	164	41	33	21
10	160	39	28	22
Sarah				
1	170	33	32	17
2	171	32	30	18
3	172	30	31	19
4	169	30	33	18
5	173	31	32	17
6	172	30	30	16
7	171	29	31	17
8	170	34	33	19
9	174	31	34	20
10	175	32	31	19
Adam				
1	195	30	15	15
2	194	31	14	15
3	193	30	13	12
4	192	32	15	13
5	194	33	14	14
6	195	31	15	12
7	196	34	16	11
8	197	30	12	4
9	193	31	14	15
10	192	31	15	16
Katia				
1	151	19	69	38
2	150	20	71	40
3	151	19	68	39
4	153	21	70	39
5	149	18	69	37
6	154	22	72	41
7	151	21	70	40
8	151	20	71	39
9	153	21	72	38
10	153	23	73	40

Table 2: Averaged highest energy values

Clients	Averaged highest energy values (LL)	Averaged highest energy values (LH)	Averaged highest energy values (HL)	Averaged highest energy values (HH)	Averaged highest energy values (LL, LH, HL, HH)
A	161.4	41.4	30.9	19.3	63.25
B	171.7	31.2	31.7	18.0	63.15
C	194.1	31.3	14.3	12.7	63.10
D	151.6	20.4	70.5	39.1	70.40

Table 3: Matching process

Clients	Averaged highest values (LL,LH, HL, HH)	Averaged highest values (LL) (testing phase)	Averaged highest values (LL, HL, HH)	Averaged highest values (LL) (Training phase)	Matching depending (LL, LH, HL, HH) (%)	Matching depending on (LL) (%)
A	161.4	63.25	161.4	63.29	100	96
B	171.7	63.15	171.7	63.13	100	98
C	194.1	63.10	194.1	63.15	100	95
D	151.6	70.40	151.6	70.41	100	99

Table 4: Required time for iterations

Iteration of HPSO	Time required (sec)
1	0.16
2	0.24
3	0.32
4	0.40
5	0.48
6	0.64
7	0.70
8	0.78
9	0.93
10	1.04

Table 5: Performance of the proposed system

Error rate	Results
LL subband (FAR)	0.000
LL subband (FRR)	0.010
LL subband (CVR%)	0.990
All subbands (FAR)	0.000
All subbands (FRR)	0.000
All subbands (CVR%)	100.0

CONCLUSION

This study proposed a mobile learning system which is successfully implemented through the cooperation of the mobile phones and the server through web service technique. However, authentication stills an important topic in order to protect this system. The proposed system used HPSO algorithm as a feature extraction tool with following points to be discussed: in spite of the values located by PSO algorithm are not the most highest values but the averages of these values are good as features.

Iterations are chosen by compromising the selected values with the suitable time for HPSO algorithm. LL subband had the great effect on matching operation, however, if all subbands are considered the matching is reached to (100%). The proposed system has a good authentication performance.

REFERENCES

Ahmed, H. and J. Glasgow, 2012. Swarm intelligence: Concepts, models and applications. MSc Thesis, Queens University, Canada.

Antoine, J.P., D. Rosc and P. Vandergheynst, 2010. Wavelet transform on manifolds: Old and new approaches. Appl. Comput. Harmon. Anal., 28: 189-202.

Bahry, F.D.S., N. Anwar, N. Amran and R.P.M. Rias, 2015. Conceptualizing security measures on mobile learning for Malaysian higher education institutions. Procedia Soc. Behav. Sci., 176: 1083-1088.

Bogarin, A., R. Cerezo and C. Romero, 2018. A survey on educational process mining. Wiley Interdiscip. Rev. Data Min. Knowl. Discovery, 8: 1-17.

Garcia-Zubia, J., J. Irurzun, I. Angulo, U. Hernandez and M. Castro *et al*., 2010. SecondLab: A remote laboratory under second life. Proceedings of the IEEE International Conference on EDUCON 2010, April 14-16, 2010, IEEE, Madrid, Spain, ISBN:978-1-4244-6568-2, pp: 351-356.

Georgieva, E., A. Smrikarov and T. Georgiev, 2005. A general classification of mobile learning systems. Proceedings of the International Conference on Computer Systems and Technologies-CompSysTech Vol. 8, June 16-17, 2005, Technical University, Varna, Bulgaria, pp: 14-1-14-6.

Harward, V.J., J.A. Del Alamo, S.R. Lerman, P.H. Bailey and J. Carpenter *et al*., 2008. The ILAB shared architecture: A web services infrastructure to build communities of internet accessible laboratories. Proc. IEEE., 96: 931-950.

Karthiyayini, M., 2016. Developing M-learning application in intranet. Intl. J. Adv. Res. Comput. Sci. Software Eng., 6: 818-821.

Liu, H., G. Xu, G.Y. Ding and Y.B. Sun, 2014. Human behavior-based particle swarm optimization. Sci. World J., 2014: 1-14.

Nedungadi, P., R. Raman, K. Achuthan and S. Diwakar, 2011. Virtual labs collaborative and accessibility platform (VLCAP). Proceedings of the International Conference on IAJC/ISAM Vol. 276, April 29-30, 2011, University of Hartford, Boston and New York, ISBN:978-1-60643-379-9, pp: 1-14.

Poljanowicz, W., M. Roszak, W. Kowalewski and B. Kolodziejczak, 2014. Using a virtual learning environment as a key to the development of innovative medical education. Stud. Logic, Grammar Rhetoric, 39: 123-142.

Shonola, S.A. and M. Joy, 2016. Enhancing mobile learning security. Intl. J. Integrating Technol. Educ., 5: 1-15.

Shonola, S.A. and M.S. Joy, 2014. Mobile learning security concerns from university students perspectives. Proceedings of the 2014 International Conference on Interactive Mobile Communication Technologies and Learning (IMCL2014), November 13-14, 2014, IEEE, Thessaloniki, Greece, ISBN:978-1-4799-4742-3, pp: 165-172.

Su, C.H. and C.H. Cheng, 2013. 3D Game-based learning system for improving learning achievement in software engineering curriculum. Turk. Online J. Educ. Technol., 12: 1-12.

Zare, S., 2010. Intelligent Mobile Learning Interaction System (IMLIS): A personalized learning system for people with mental disabilities. Ph.D Thesis, University of Bremen, Bremen, Germany.