Journal of information and communication convergence engineering
http://jicce.org

J. Inf. Commun. Converg. Eng. 10(1): 5-10, Mar. 2012

Regular Paper

Current State of and Cutoff Schemes for Academic Misconducts in the Cyber Classes

Jongjung Woo*[*], ***Member, KIICE***

School of Information Technology, Sungshin Women's University, Seoul 136-742, Korea

Abstract

The cyber class has many advantages because it removes the limitations of sharing the same time and space of a class in a classroom. However, most instructors still hesitate to use it because it is more vulnerable to academic misconduct than a face-to-face class. To overcome this problem, we identified suspected cheaters out of a group of test-takers through several objective data, and verified whether or not the suspects were actually cheaters. By investigating the status of academic cheating, we also implement our assessment system with Skinner's reinforcement theory in order to eliminate or reduce cyber misconducts.

Index Terms: Academic misconduct, Cyber class, IP address, Reinforcement theory

I. INTRODUCTION

It is difficult for students to learn from their classes based on existing education methods in knowledge-based societies in which the creation and dissipation of knowledge happen relatively quickly. The advance of information technology and the appearance of constructivist theory have gradually shifted teaching and learning from an instructor-centered paradigm to a student-centered paradigm instead [1, 2]. In particular, we have recently observed an increased interest in the cyber class, a typical example of student-centered teaching and learning in which certain temporal and spatial limitations are removed. Thus, most universities and industries are conducting and introducing cyber classes in the Republic of Korea [3].

However, the cyber class requires instructors to not only develop the curricula for classes, but also to operate the learning management systems (LMSs). Moreover, cyber classes do not currently employ effective protocols for verifying the students' identity or against student academic misconduct because e-learning is performed online (in contrast to face-to-face learning). There are more substitute exam takers and group cheaters in cyber classes than in face-to-face classes. Therefore, it is more difficult for instructors to fairly assess students' scholastic achievement in cyber classes. To overcome such problems, researchers have proposed blended learning [4, 5], exams consisting of randomly-ordered questions [6], and preventing substitute exam takers by employing verification techniques such as analysis of behavioral characteristics, facial recognition, and so on [7-9]. There is little research on cyber misconduct. Some studies are based on questionnaires which might not be exact or true, thereby making the results of such studies difficult to interpret.

Our study assesses the current status of misconduct taking place in the cyber classes of a real university by exploiting the IP address, the examinees' personal information, etc., instead of relying on data from a questionnaire given to the examinee. In addition, we propose and implement an intermittent assessment system

Received 05 September 2011, **Revised** 26 September 2011, **Accepted** 04 October 2011
***Corresponding Author** E-mail: jwoo@sungshin.ac.kr

Open Access **http://dx.doi.org/10.6109/jicce.2012.10.1.005**

print ISSN:2234-8255 online ISSN:2234-8883

of pop-up quiz questions interspersed throughout the online study material by using Skinner's reinforcement theory in order to prevent such cyber cheating.

II. RELATED WORKS

A. General Perception of Cyber Misconduct

Education is often used as a means to attain employment; therefore, employers prefer result-oriented to process-oriented education or quantity-oriented to quality-oriented. In order to obtain good grades, most undergraduates who are trying to cheat justify substitute exam taking, cheating, and plagiarizing homework [10, 11]. Moreover, many students try to improve their academic record by repeatedly taking the same class. The cheating techniques of face-to-face learning include writing exam answers on desktops or walls, using crib sheets, and trading papers, all of which are easily caught and disciplined by proctors. Therefore, academic misconduct can be prevented by intense vigilance. The environment of cyber classes is different from that of their face-to-face counterparts. Cyber classes allow for various cheating techniques that are distinct from those used in face-to-face classes. Few strategies for reducing or preventing cheating in cyber classes have been reported in the literature.

B. Cyber Cheating Prevention Techniques

E-learning has many academic advantages, but it also has many disadvantages, such as requiring time, technology, and manpower to develop learning content. Moreover, e-learning does not have any proper schemes for preventing academic dishonesty and cheating because examinees are free temporary or spatially from proctors [6-8]. Several examinees can easily trade their answers; they can even congregate in the same area and solve their exam together. It is impossible to detect cyber cheaters without the examinee's confession. The frequency of academic dishonesty and cheating in cyber classes is independent of the level of invigilation, while in the face-to-face class a higher degree of invigilation achieves less frequent academic misconduct. Thus, many researchers are still studying the prevention of cyber academic misconduct.

Except for blended learning, cutoff schemes against cyber cheating can generally be classified as shown in Fig. 1. The cutoff scheme of blended learning is beyond the scope of this paper because the scholastic assessment of blended learning is almost the same as that of face-to-face learning. Personal identification of examinees, random-ordered questions, and essay questions can reduce cyber misconduct, but it is difficult to detect cyber cheaters after exams.

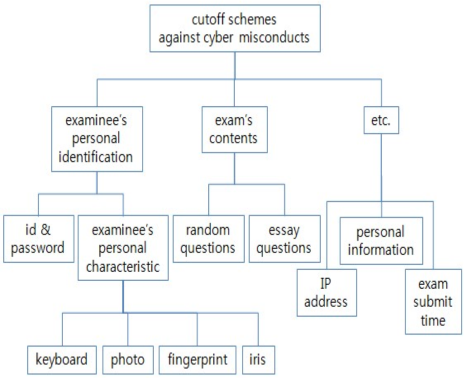


Fig. 1. Cutoff schemes against cyber cheating.

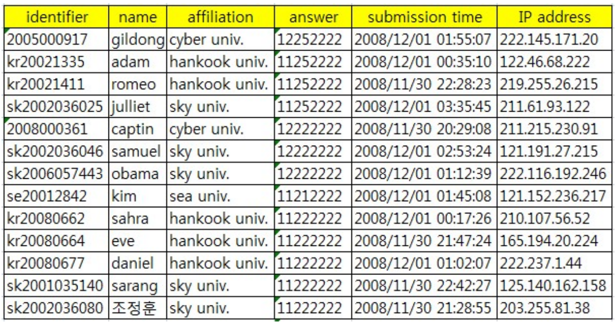
The other approaches can detect cyber cheaters (even after exams) as well as prevent cyber cheating. The first approach, examinee personal identification, verifies whether or not the attendee is the actual examinee by using his password or his biometric/behavioral characteristics. The password cannot prevent substitute exam taking. The biometric or behavioral characteristics can prevent substitute exam taking, but they require the examinees to install additional hardware such as a webcam. The second approach based on the exam contents is that each examinee has different questions or essay questions. Different questions can be randomly chosen from an exam question bank or be set in different orders. This method can remove or reduce an examinee's cyber cheating. However, this scheme has disadvantages, in that instructors should prepare many questions to create the question bank in advance or spend a great deal of time in scoring essay questions. The final approaches are to find traces of IP addresses, the examinee's personal information, or submission time during or after the exam. This scheme can keep examinees from meeting together and sharing their answers, but it is difficult to discipline these cyber cheaters unless they do confess their dishonesty.

III. STATE OF ACADEMIC MISCONDUCT OF THE CYBER CLASS

The state of academic misconduct performed in cyber classes will be investigated in section III-A. Section III-B describes how the cyber cheaters in section III-A can be verified to be real cheaters and describes the distribution of possible groups of cyber cheaters.

A. Case Study of Cyber Cheaters

Online exams in cyber classes are similar to open book exams in face-to-face classes. An online exam is generally taken in a personal area at a given time for a given duration, thereby making fair invigilation difficult. In cyber classes, there are many forms of academic misconduct such as substitute exam taking, group cyber cheating, sharing answers by using communication media, and so on. Hence, it is almost impossible to prevent substitute exam taking because the examinee finds it inconvenient to attach additional hardware to his computer for personal identification as described in section II-B. Therefore, we focus on cyber cheating in groups or through communication media. We have chosen three cyber classes that were opened in a cyberuniversity in 2008-2009. This cyber university is a consortium of about 20 non-cyber universities. Learners are students from a non-cyber university. We collect some data such as examinees' IP addresses, personal information, submission time, and similarity of incorrect answers, as is shown in Fig. 2. Hence, the first three columns (identifier, name, and affiliation) are not real because of privacy concerns. Moreover, the fourth column consists of a series of concatenated answers for multiple choice or true/false questions.



identifier	name	affiliation	answer	submission time	IP address
2005000917	gildong	cyber univ.	12252222	2008/12/01 01:55:07	222.145.171.20
kr20021335	adam	hankook univ.	11252222	2008/12/01 00:35:10	122.46.68.222
kr20021411	romeo	hankook univ.	11252222	2008/11/30 22:28:23	219.255.26.215
sk2002036025	julliet	sky univ.	11252222	2008/12/01 03:35:45	211.61.93.122
2008000361	captin	cyber univ.	12222222	2008/11/30 20:29:08	211.215.230.91
sk2002036046	samuel	sky univ.	12222222	2008/12/01 02:53:24	121.191.27.215
sk2006057443	obama	sky univ.	12222222	2008/12/01 01:12:39	222.116.192.246
se20012842	kim	sea univ.	11212222	2008/12/01 01:45:08	121.152.236.217
kr20080662	sahra	hankook univ.	11222222	2008/12/01 00:17:26	210.107.56.52
kr20080664	eve	hankook univ.	11222222	2008/11/30 21:47:24	165.194.20.224
kr20080677	daniel	hankook univ.	11222222	2008/12/01 01:02:07	222.237.1.44
sk2001035140	sarang	sky univ.	11222222	2008/11/30 22:42:27	125.140.162.158
sk2002036080	조정훈	sky univ.	11222222	2008/11/30 21:28:55	203.255.81.38

Fig. 2. Part of data collected for case study.

It is more difficult or almost impossible to investigate statistics for academic misconduct in cyber classes compared to offline classes. A cyber class has more kinds of academic cheating methods than offline classes. In a cyber-class, it is possible for an examinee to try to cheat more actively or positively because the examinee and proctor are not at the same place. However, we can easily identify a suspected group cheaters because they use similar IP addresses, attend the same university, and submit their papers at similar times. Cheaters who share their answers through communication cannot easily be detected because only their affiliations and incorrect answers are similar. Thus, it is difficult to catch this kind of cheater without their confessions. For now, we investigate the states of the former (group cheaters). Table 1 shows the status of cyber cheating. It is composed of 3 courses that have 9 exams. We use the following criteria for group cyber cheating: 1) the same C-class IP addresses, 2) the same university and the same entrance year of examinees' identifiers, and 3) ranges between submission times are within 10 minutes.

Table 1. Status of cyber cheating

Course	year/ semester	Mid/ Final	No. of registers	No. of non- takers	Suspects
X	2008/2	Mid	856	34	262
		Final	848	60	290
Y	2008/2	Final	65	4	9
Z	2008/2	Mid	135	35	16
		Final	127	21	0
	2009/1	Mid	93	33	8
		Final	93	21	13
	2009/2	Mid	149	31	23
		Final	145	26	25

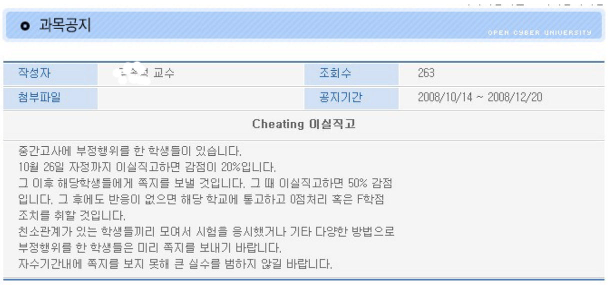
If the above conditions are all met, then we consider an examinee as a suspected cheater. Table 1 indicates no suspects in the final exam of course Z in the second semester of 2008. This is because we detected cheaters and put several warning notices on the class bulletin after the mid-exam. Thus, to obtain meaningful statistics, we remove the result of the final exam of course Z in the second semester of 2008. Table 1 shows that among 2,384 registered students, 244 students did not take exams and 646 students are suspected cheaters. Thus, the number of total examinees is 2,140. About 30.2% of examinees per course are assumed to try dishonesty on taking the exam. This ratio is too high to be acceptable. About 34.3% (for X), 14.8% (for Y), and 9.3% (for Z) of the examinees are assumed to be group cheaters, respectively. Examinees who take course X have the highest ratio of cyber cheating. One reason is that the exam of course X consists of multiple choice or true/false questions that are adapted for large-scale classes owing to easy scoring. Another reason is that courses Y and Z use a question bank and random questions with a tight exam time, while course Z does not.

B. Verification of Cyber Cheating in the Case Study

To investigate whether or not the suspected cheaters shown in Table 1 are actual cheaters, we have chosen course Z from three courses, a mid-scaled class. First, to verify group cheating, we check the three criteria in section III-A - IP addresses, personal information, and submission time - for assumed cheaters. Table 2 shows that there are four kinds of groups that use the same C-class IP addresses. Even though eleven examinees are in the same IP-addressed group, we exclude them from the suspected cheaters because they do not have common personal information and submit their papers at different times.

Table 2. Distribution of possible group cyber cheaters

No. of examinees per a group	No. of groups	No. of assumed cheaters
2	5	4
3	1	2
4	1	4
10	1	6



과목공지

OPEN CYBER UNIVERSITY

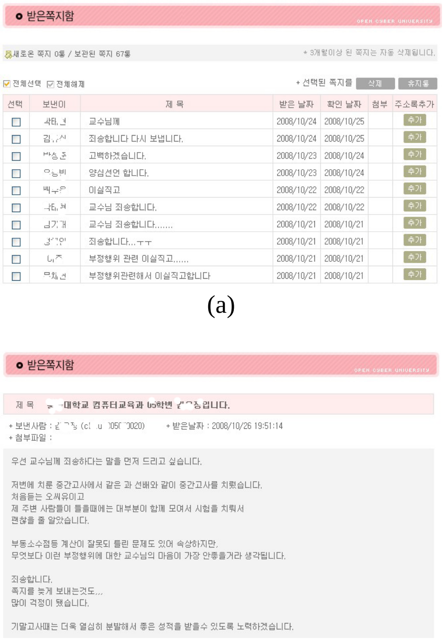
작성자	[redacted] 교수	조회수	263
첨부파일		공지기간	2008/10/14 ~ 2008/12/20

Cheating 이실직고

중간고사에 부정행위를 한 학생들이 있습니다.
10월 26일 자정까지 이실직고하면 감점이 20%입니다.
그 이후 해당학생들에게 쪽지를 보낼 것입니다. 그 때 이실직고하면 50% 감점
입니다. 그 후에도 반응이 없으면 해당 학교에 통고하고 0점처리 혹은 F학점
조치를 취할 것입니다.
친소관계가 있는 학생들끼리 모여서 시험을 응시했거나 기타 다양한 방법으로
부정행위를 한 학생들은 미리 쪽지를 보내기 바랍니다.
자수기간내에 쪽지를 보지 못해 큰 실수를 범하지 않길 바랍니다.

Fig. 3. Course announcement for screening actual cheaters from suspects.

To distinguish actual cheaters from suspects, we made two announcements about dishonesty after the midterm exam. We sent suspects a warning message shown in Fig. 3 and even phoned them, too. The warning message tells them that they are group cheaters, some points will be deducted for their grades if they confess their misconduct, and they will fail the course otherwise.



받은쪽지함

OPEN CYBER UNIVERSITY

새로온 쪽지 0통 / 보관된 쪽지 67통 * 3개월이상 된 쪽지는 자동 삭제됩니다.

☑ 전체선택 ☑ 전체해제 + 선택된 쪽지를 삭제 휴지통

선택	보낸이	제 목	받은 날짜	확인 날짜	첨부	주소록추가
□	[redacted]	교수님께	2008/10/24	2008/10/25		추가
□	[redacted]	죄송합니다 다시 보냅니다.	2008/10/24	2008/10/25		추가
□	[redacted]	고백하겠습니다.	2008/10/23	2008/10/24		추가
□	[redacted]	양심선언 합니다.	2008/10/23	2008/10/24		추가
□	[redacted]	이실직고	2008/10/22	2008/10/22		추가
□	[redacted]	교수님 죄송합니다.	2008/10/22	2008/10/22		추가
□	[redacted]	교수님 죄송합니다.......	2008/10/21	2008/10/21		추가
□	[redacted]	죄송합니다...ㅜㅜ	2008/10/21	2008/10/21		추가
□	[redacted]	부정행위 관련 이실직고......	2008/10/21	2008/10/21		추가
□	[redacted]	부정행위관련해서 이실직고합니다	2008/10/21	2008/10/21		추가

(a)

받은쪽지함

OPEN CYBER UNIVERSITY

제 목 [redacted]대학교 컴퓨터교육과 05학번 [redacted]입니다.

+ 보낸사람 : [redacted] + 받은날짜 : 2008/10/26 19:51:14
+ 첨부파일 :

우선 교수님께 죄송하다는 말을 먼저 드리고 싶습니다.

저번에 치룬 중간고사에서 같은 과 선배와 같이 중간고사를 치뤘습니다.
처음듣는 오씨유이고
제 주변 사람들이 들을때에는 대부분이 함께 모여서 시험을 치뤄서
괜찮을 줄 알았습니다.

부동소수점등 계산이 잘못되 틀린 문제도 있어 속상하지만,
무엇보다 이런 부정행위에 대한 교수님의 마음이 가장 안좋을거라 생각됩니다.

죄송합니다.
쪽지를 늦게 보내는것도,,,
많이 걱정이 됐습니다.

기말고사때는 더욱 열심히 분발해서 좋은 성적을 받을수 있도록 노력하겠습니다.

(b)

Fig. 4. Message inbox and message contents.

As a result, all of the assumed group cheaters (16 examinees) sent response notes back that they admitted their dishonesty and asked to be excused. Luckily, there were no suspects who claim to be innocent. Fig. 4a shows a received message box that the cheaters sent, and Fig. 4b shows one of the cheaters' messages. According to our expectation, there were no cheaters on the final exam of the same course as shown in Table 1. Therefore, it is not too much to say that all assumed cheaters in Table 1 must have been actual cheaters who met in the same computer laboratory at the same time, solved their questions together, and shared their answers.

Table 3 shows the transition rates of cyber cheating between the midterm exam and final. We excluded course Y because it does not have a midterm exam. We also excluded a course Z from the second semester in 2008 because there were no cheaters on the final exam. In general, the cheating ratio of the final exam is higher than that of the midterm exam. As the final exam approaches, it is natural that learners become more concerned about their grades than when the midterm does.

Table 3. Ratio of group cyber cheaters

Course	year/semester	Transition of cheating ratios between mid/final exams (%)
X	2008/2	31.9/ 36.8
Y	2008/2	NA / 14.8
Z	2008/2	16.0 / 0
	2009/1	13.3 / 18.1
	2009/2	19.5 / 21.0

NA: not applicable.

To investigate the status of sharing or trading examinees' answers through communication media such as e-mail and cell phones, we analyzed some of the same data that was used in section III-A. We excluded 16 cheaters and 35 non-takers from 135 registered students. We asked 10 examinees among 84 exam-takers by a phone call whether or not they were involved in cheating, but we could not force them to respond. Moreover, there were no confessions, and they even complained about being suspected for no reason. Therefore, it is almost impossible to investigate this kind of cheating without the examinees' confessions.

IV. INTERMITTENT ASSEMENT SYSTEM THAT MINIMIZES ACADEMIC MISCONDUCT

Cyber classes have a high possibility of group cyber cheating due to their characteristics. The proctor cannot see how examinees take the exam because they are in different locations. Thus, the results of scholastic achievement in a cyber-class are not accurate. If the instructor gives learners their credits or grades in cyber classes by using mainly midterm and final exams, he will confronted with various types of cyber cheating and cannot assess the learners' acquired knowledge. Therefore, we propose and implement an assessment system that is applied by Skinner's reinforcement theory, and thus eliminate or reduce group cyber cheating. Reinforcement is the overall condition that delivers a stimulus after a response that results in an increase in future rates [12]. In particular, intermittent reinforcement makes learners study better [13]. There are several LMSs that apply this reinforcement theory [14, 15]. However, they are trivial systems with simple quizzes. Therefore, this study applies intermittent reinforcement into scholastic assessment without mid/final exams on the basis of the results of the cyber cheating analysis in section III-B. That is, we randomly select some questions from a question bank. Learners can experience questions on random pages of their learning content. No learners can predict on what page questions will pop up. Thus, learners have no choice but to take the exam within a given time while studying. They cannot earn their grades without studying because they do not have any exams other than the popup exams.

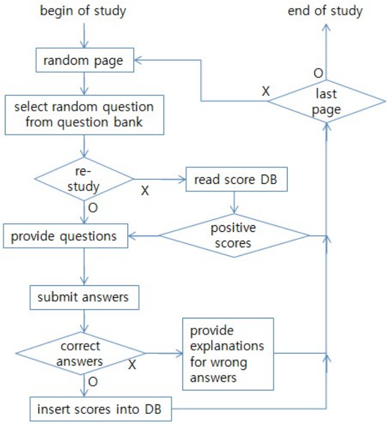
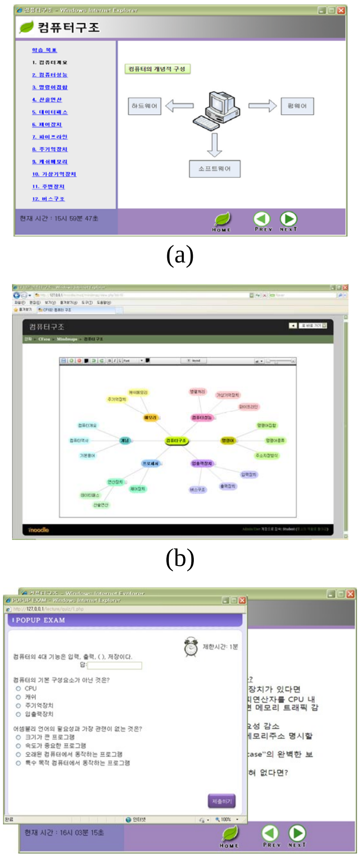


Fig. 5. Flow of proposed assessment system.

The assessment system proposed in this research causes the learner to experience intermittently random questions that unexpectedly pop up on random pages. Fig. 5 shows the flow of our assessment system. The assessment system stores the learner's answers in the score database, and it provides the learner some explanation if his answer is wrong. Our system does not pop up questions that he has already solved if he studies the same material repeatedly.

We implement our assessment system in Windows XP and an Apache web server by using MySQL, personal hypertext preprocessor (PHP), and JavaScript. In addition, we exploit Moodle [16], open source and free software, as our LMS. Fig. 6a shows an example course page in our LMS, Fig. 6b provides a mind map of an overall structural abstract of a given course's contents, and finally Fig. 6c shows a random question window that popped up on a random page during studying.



(a)

(b)

(c)

컴퓨터의 4대 기능은 입력, 출력, ( ), 저장이다.

답:

컴퓨터의 기본 구성요소가 아닌 것은?

○ CPU
○ 캐쉬
○ 주기억장치
○ 입출력장치

어셈블리 언어의 필요성과 가장 관련이 없는 것은?

○ 크기가 큰 프로그램
○ 속도가 중요한 프로그램
○ 오래된 컴퓨터에서 동작하는 프로그램
○ 특수 목적 컴퓨터에서 동작하는 프로그램

Fig. 6. Example screens of proposed assessment system.

V. CONCLUSIONS

Instructors still hesitate to use e-learning in spite of its advantages. One of the main reasons is that online exams are easily exposed to academic misconduct. Thus, this study investigates the nature of academic cheating in online classes in a non-cyber university by identifying the IP addresses and personal information of examinees and the submission time of exam-answers. Moreover, we confirmed through IP addresses and other indicators that suspected cheaters were actual cheaters based on their confessions. Finally, we implemented our assessment system for e-Learning in order to root out or reduce cyber cheating by applying Skinner's reinforcement theory.

Future work must include the trends in scholastic achievement according to whether or not our assessment system is used in cyber classes and the status of cyber cheating through communication media and its prevention.

ACKNOWLEDGMENTS

This work was supported by the Sungshin Women's University Research Grant of 2011.

REFERENCES

[1] T. D. Duffy and D. H. Jonassen, "Constructivism: new implications for instructional technology," *Educational Technology,* vol. 31, no. 5, pp. 7-12, 1991.

[2] J. Woo, B. Kim, and O. Lee, "A study on the blended learning as an alternative of face-to-face learning in university," *Journal of Korean Institute of Information Technology,* vol. 7, no. 2, pp. 219-225, 2009.

[3] Korea Education and Research Information Service (KERIS), Status of e-learning and revitalization plan in higher education, Seoul: KERIS, Research Report no.: KR2004-25, 2004.

[4] I. Oh, "Analysis of actual status of blended learning: comparison between domestic and foreign," *Industry Education Research,* vol. 6, no. 1, pp. 41-62 , 2004

[5] C. R. Graham, "Blended learning systems: definition, current trends, and future directions," in *The Handbook of Blended Learning: Global Perspectives, Local Designs*, San Francisco: Pfeiffer, pp. 3-21, 2006.

[6] J. Jang and H. Kim, "Prevention of cheating on-line test with random question," *Proceedings of the Korean Institute of Information Scientists and Engineers,* vol. 29, no. 2, pp. 397-399, 2002.

[7] H. Kim and J. Ko, "Design and implementation of cheat prevention system for online test based on interactive," *Journal of Korean Institute of Information Technology,* vol. 7, no. 3, pp. 253-261, 2009.

[8] J. KO. J. Shim, and H. Kim, "A study of cheat prevention method for online test using image frame analysis," *Journal of Korean Institute of Information Technology,* vol. 7, no. 5, pp. 313-320, 2009.

[9] G. Cho and D. Kwak, "A study of the authentication of on-line test participants under e-learning," *Proceedings of the Korean Institute of Information Scientists and Engineers,* vol. 31, no. 1, pp. 499-501, 2004.

[10] D. Yang, "The difference of male undergraduates` levels of scholastic achievement and experience of cheating behavior in examination according to the sense of values of success," *Korean Educational Review,* vol. 10, no. 2, pp. 249-269, 2004.

[11] W. H. Shim, "Academic dishonesty: prevalence, determinants, techniques, and prevention strategies," *The Journal of Elementary Education*, vol. 14, no. 1, pp. 85-106, 2000.

[12] B. F. Skinner, *Beyond Freedom and Dignity*, New York: Alfred A. Knopf; 1971.

[13] G. D. Borich, *Effective Teaching Method: Research Based Practice*, 6th ed. Boston, MA: Prentice Hall; 2006.

[14] H. Kim and S. Yu, "An online learning system for evaluating learner's activities and study level," *Journal of the Korea Society of Computer and Information,* vol. 13, no. 6, pp. 69-76, 2008.

[15] J. Lee, "A study design for improvement of interactivity at e-learning," *Journal of the Korea Contents Association,* vol. 10, no. 2, pp. 197-203, 2002.

[16] Moodle [Internet]. Available: http://www.moodle.org.

Jongjung Woo
received the B.S. degree from the Department of Electronics of Kyungpook National University in 1982, and the M.S. and Ph.D. degrees from the Department of Electrical & Computer Engineering of University of Texas at Austin, in 1990 and 1993, respectively. He has worked as a professor in the School of Information & Technology at Sungshin W. University since 1993. His current research interests include embedded software, mobile computing, computer architecture, parallel processing, and e-learning.

http://dx.doi.org/10.6109/jicce.2012.10.1.005