

# Taking Multiple-Choice Quiz by SMS on Mobile Phones Including Analyzing Property

Mohammad Shirali-Shahreza  
 Computer Science Department  
 Sharif University of Technology  
 Tehran, IRAN  
 Email: [shirali@cs.sharif.edu](mailto:shirali@cs.sharif.edu)  
 Website: <http://mohammad.shirali.ir>

**Abstract**— Recently Mobile Learning (M-Learning) has attracted much attention. Due to advantages of SMS (Short Messaging Service) on mobile phones we present a safe and protected method for taking multiple-choice quizzes by using the SMS on mobile phones in this paper.

In this method questions of quiz are sent to students along with their answers through some SMS messages. The students will receive their grades immediately after answering the questions and this grade is also sent to the instructor or professor along with the student's answers through an SMS Picture Message. Answers of questions and the student's grade are hidden in SMS picture message through steganography and then they are sent. The concerned data will be destroyed within the image after they are extracted from image in order to improve security and to eliminate the possibility of cheating. The instructor of lessons can improve his next quizzes through studying and investigating students' grades and their given answers. This method has been implemented using J2ME programming language on a Nokia 6230i mobile phone.

**Index Terms**— E-learning, M-learning, Mobile Phone, Steganography, SMS (Short Message Service).

## I. INTRODUCTION

The method of learning in the last several decades has undergone many changes and developments. Transition from the old systems of learning to the modern methods of learning has been the concerns of many instructors and students. Meanwhile, virtual learning has received attention because of the large extent of the Internet. The main cause of this is it is possible for the individuals to have communication from afar and to reduce some expenses (although some other expenses and special grounds are needed).

Along with the Internet, wireless networks such as the mobile phone are growing rapidly. Today, one out of each six persons in the world has a mobile phone. As a result, these systems can be used for learning [1]. However, the important problem in the meanwhile is to find appropriate structures for implementing learning systems on such devices while considering their limitations.

One of the popular services on the mobile phone is the SMS (Short Message Service). The SMS is the transfer

and exchange of short text messages between mobile phones. In this service, also one can send binary images with a 72×28-pixel size in binary messages. The structure of SMS picture message is described in section 4. These messages are carried out indirectly and by a component known as the SMSC [2].

The SMS has such advantages as low costs, offline SMS sending, exchanging SMS simultaneously with establishing telephone contacts, etc.

According to the above statements, a method has been provided in this paper for taking multiple-choice quizzes through the mobile phone and by using the SMS so that the questions are sent as SMS messages by the instructor to the student, the student answers the questions and then the grade and answers are sent back by an SMS to the instructor [3]. For sending the answers of the student (along with the questions), in order to obtain the grades on the client-side, a method of steganography of grades within an SMS picture message is used so as to prevent cheating by the student.

Steganography is a method of covert exchange of data, highlighted in recent years, chiefly aimed to hide data within a cover media so that other individuals fail to realize their existence [4]. I will explain this method in section 4.

Moreover, after extracting the answers of the questions, information within the message is destroyed. Also the student's grade is sent to the instructor by using the method of steganography so as to maintain the security of the grade. I will talk about my proposed method in section 3.

As most people have mobile phones and the SMS is a popular service, this method covers a wide spectrum of users. In addition, the cost of SMS is very low and any student has to send only one SMS message that contains his grade. Section 5 contains discussion on the advantages of this plan.

My proposed method was implemented with the J2ME language on a Nokia 6230i mobile phone. The project consists of two programs: instructor's program and student program. Both programs are run on the mobile phone. The instructor's program prepares the students' quizzes and sends them. The student's program takes the

quiz, calculates the grade and shows it. Finally the student grade and his answers are sent to the instructor by the student's program. The details are provided in section 5.

Taking quizzes by Internet is make further attention in recent years, but taking exams on mobile phones are less done because of their limitation such as no keyboard, small screen, etc. The following section contains a study of the work performed in this respect.

This method is not limited to taking multiple-choice quizzes and also can be used for other activities like making elections, taking tests with descriptive or short answers, etc. The final section is the future works and final conclusion.

## II. RELATED WORKS

### A. Mobile Learning

Most work performed by M-learning and especially taking quizzes has been done by using technologies such as WAP (Wireless Application Protocol). As to the use of the SMS for learning, see references [5] and [6]. However, the only work reported on M-quiz by SMS is reference [7]. A summary of the work performed by it is as follows:

In this method, questions are shown to the students in PowerPoint slides. Then the students answer the questions by SMS in certain forms. The questions are in one of these four forms: single-choice, multiple-choice, fill-in-the-blank test forms and matching two lists.

Finally the students should connect to internet by a computer and get their test result.

I will provide a full description of my proposed method in section 3. However, here I briefly mention the differences of my method with this method:

1. In my proposed method, also the questions are sent by SMS.
2. In this method, the students refer to the Internet for viewing their grades while, in my proposed method, the answers of the questions are sent in steganography form and the student, after answering to the questions, sees his results on the client-side without communicating with his instructor.  
Then, in the end, the test grade is sent to the instructor in an stegano image, which the data is hidden in it by using steganography method.
3. In this method, the answers of the questions are sent without any security consideration while, in my method, the answers of the questions and also the student's grade are sent in an stegano image which contributes to the security of the testing.

### B. Steganography in Color Images

The most cover media used for steganography is image. As a result, numerous methods have been used to this end. The reason is the large redundant in the images and the possibility of hiding information in the images without attracting attention to human visual system.

Work performed on steganography in image can be classified into three major groups: temporal method, spatial domain method and fractal method:

#### 1) Temporal Method

In this method, the data in question is added to quantities of luminosity of pixels in the image. One of the commonest methods of temporal method is the least significant bit (LSB) method, in which information is hidden in one to four least significant bits [8]. Figure 1 shows a sample of LSB steganography.

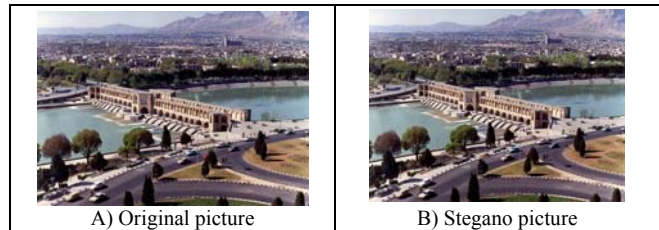


Figure 1. An example of LSB Steganography

#### 2) Spatial Domain Method

Another method is the calculation of conversion of frequency of the image and adding information in the frequency domain. A well-known method is to use the Discrete Fourier Transform (DFT) or the Discrete Cosine Transform (DCT) [9]. Considering the use of exchange of cosine transform in JPEG image format, this method is good for said format.

#### 3) Fractal Method

The other method of steganography is based on fractal compressing. In this method, blocks of the image that contain repeated patterns are selected and information is saved in them [10].

### C. Steganography in Black & White Images

Most steganography work so far carried out on pictures has been on color or grayscale pictures and little work has been done on B&W pictures, because B&W pictures are sensitive to changes and, for example, change in one pixel of the picture in a white area would be quite visible while, in color pictures, if the color of a pixel is changed slightly, this would not be tangible.

Here the data are hidden in SMS picture messages, which are Black and White (B&W) images. So we study some work carried out on B&W images.

#### 1) Using Dithered Images

In this method, data are saved in dithered images. In old newspapers, the dithered method in the form of B&W dots were used for printing color or grayscale pictures and the pictures looked grayscale from a distance. The problem with this method is that it cannot be used for normal two-color pictures and, on the other hand, a small number of data can be saved in the picture [11].

#### 2) Method to Displace Words and Lines

In this method, by displacing the text or changing the distance between words, data are hidden in the printed picture of a text. The problem with this method is that it can only be used for pictures of text and cannot be used for regular pictures [12].

### 3) *Changing two bits in each block*

In this method, the input picture is divided into  $m \times n$  blocks. Then each block is changed by apply XOR with a key on that block, so that the block is encoded. Considering the weight matrix, at most 2 bits of each block are changed. In this method, if the block dimensions are  $m \times n$ , each block can hide  $\log_2(mn+1)$  bits of data. The main advantage of this method is the high stegano capacity of this method. However, its major drawback is the tangible changes in the output picture [13], [14], [15].

### 4) *Changing one bit in each block*

In this method, the B&W pictures are first divided into  $m \times n$  blocks and then, in each block, at most one bit of information is hidden. For each block, the possibility of saving is calculated and, if the possibility exceeds a certain limit, the middle pixel in that block is changed according to the data in question. The major advantage of this method is the intangible changes in the resulting pictures. The drawback of this method is the low steganography capacity of the pictures. The more the edges of the picture, the higher the steganography capacity will be [16], [17].

## III. MY PROPOSED ALGORITHM

In this project, the aim is multiple-choice quizzing by SMS so that the student receives the questions by SMS and, after answering to the questions, receives the result of the test on the client-side. The result along with test answers is then sent back to the instructor. So instructor can analyze the student answers and grade. The full details of this project are as follows:

In the beginning, the instructor has to prepare the test questions and their answers on his computer. As the questions have to be sent to the students by SMS, he should install an SMS gateway on his computer so as to be able to send and receive the SMS messages. The instructor, in turn, saves the student numbers of all the students and their mobile phone numbers in a file. Then, by providing the questions and their answers and also a file containing the mobile phone numbers of the students to the program, which we will explain later, he will send the questions to the students.

After receiving the questions and their answers, if the total number of the questions is more than what should be sent for the students, e.g. the total number of questions is 20 and for each student 5 questions have to be sent, then the program randomly selects 5 questions for each student and displaces the choices of each question so that the students' questions will be different from each other. The numbers of questions for each student are saved on the instructor computer to analyze students' answers later. Now, if the number of questions is  $n$ , the program will prepare  $n+1$  SMS messages, and the questions are in the second SMS message to  $n+1^{\text{th}}$  SMS message. There is a picture in the first SMS message (for example the university logo), in which the answers of the tests are hidden by using steganography method.

Steganography means hiding information in a cover media so that the others will not notice that such

information exists. Here, by using the method of steganography in the SMS, the test answers are hidden in the SMS picture message.

The method of SMS steganography is fully described in section 4. Briefly speaking, in this method, in order to hide information in an SMS picture message, the picture is divided into smaller blocks. If the change of the pixels of the block is not noticeable, a pixel of the block is changed and, thus, information is hidden in the picture. There is also a password based on which data are encoded.

In this project, the test answers and also the exam time are hidden in the picture so that the students cannot extract the answers directly.

The amount of information capable of hiding in SMS is limited. An SMS picture message contains 234 blocks of  $3 \times 3$  and maximum one bit of information can be hidden in each block. If one quarter of the picture contained the above phrase (58 blocks), 176 blocks remain for hiding the information. As some blocks are incapable of hiding information, if only  $1/3^{\text{rd}}$  of blocks were capable of hiding information, about 50 blocks remain for hiding information. In order to hide the time of examination, assuming that the exam lasts maximum 256 minutes (usually the time of quizzes is short), we need 8 bits or equivalent of 8 blocks. In order to hide the answer of each 4-choice question, we need 2 bits or equivalent to 2 blocks. Therefore, up to 20 answers can be hidden in each picture message, because 40 blocks are needed for 20 questions. Considering the 8 blocks needed for hiding the time of exam, a total of 48 blocks is needed. Therefore, 50 blocks are capable of hiding information up to 20 questions. So, an SMS picture message is proper for sending time of examination and answers of questions up to maximum 20 questions.

Also, since the test answers are sent to the student, the student does not need sending the answers to the instructor and then receiving a grade from the instructor. But after answering to the questions, he sees his grade at the same moment and has to send, later, his test grade with the test answers so instructor can analyze students' answers later. The details will be provided later.

When  $n+1$  SMS messages are prepared, all the SMS messages are sent to the appropriate student. This is applied separately for all the students.

The student receives the SMS messages by the special program that is installed on his mobile phone. The program gives time to the student to answer the received questions within a certain period of time extracted from inside the first SMS picture message. Section 4 provides how information is extracted from the picture containing steganography information.

Now, the program shows the SMS messages respectively and receives answers from the student. After the student answers all the questions, the program provides the grade and the grade along with the answers are hidden in an SMS picture message and sent back to the instructor. The picture used for hiding the grade is the same as the first SMS picture message. The instructor's

telephone number is specified according to the received SMS messages.

Thus, even if the student is not able to send the SMS message at that moment, he can send the result to the instructor later without the quiz to be interrupted by this. Moreover, after extracting the appropriate answers from the first SMS picture message, the answers within the SMS message are destroyed (stealth data). This makes it impossible for the student to further take the quiz (Figure 2).

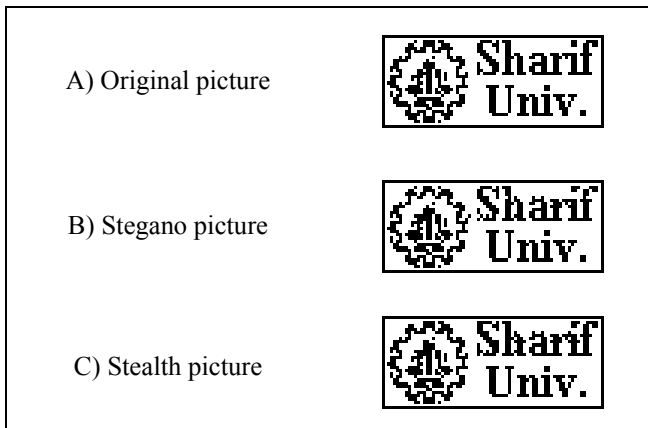


Figure 2. Hiding data in an SMS picture message

Now the instructor receives the SMS picture message containing the student's grade and answers, and, after extracting them from the picture, records the grade and answers with the appropriate program.

The student's specifications are extracted according to his mobile phone number from the file in which the personal information of each student and his mobile phone number are already saved.

#### IV. STEGANOGRAPHY METHOD

Steganography is a method of covert exchange of data, highlighted in recent years, chiefly aimed to hide data within a cover media so that other individuals fail to realize their existence. This function is the main privilege of the method over its counterparts in terms of covert exchange of data. For example, in cryptography, encrypted data hint at their existence of data while content remains secret to others. However, in steganography even the existence of data remains unknown [18].

Most steganography works are done on images [1], video-clips [19], music and sounds [20]. But few works are carried out on the text steganography [21].

Recently, data security has increased through a combination of the steganography and other previously mentioned methods. Steganography has other applications besides covert exchange of data, including in copyright protection, preventing e-document forging and so on [4].

This is the algorithm used for steganography in the pictures of SMS messages in mobile phones [22], [23]:

First the received picture is converted to B&W. As the size of the SMS picture message must be 72×28 pixels, a

72×28-pixel conversion of the picture is created. The saving format of the SMS picture is OTA. The structure of this format is as follows [24].

The header of this format containing 4 fixed bytes as follows:

- Byte 1) 0000 0000 (→ 0)
- Byte 2) 0100 1000 (→ 72)
- Byte 3) 0001 1100 (→ 28)
- Byte 4) 0000 0001 (→ 1)

As you can see in the above header, the second and third bytes indicate the height and width of the picture.

The structure of the body of the picture contains the pixels in 0 and 1. The amount of each pixel is saved in one bit. In each bit, 0 indicates the black and 1 the white color. Thus, every 8 pixels are saved in one byte. The order of saving of the pixels is from the left to the right and from the top to the bottom of the picture. Considering the size of the picture, the entire size of an SMS picture message is 256 bytes (Figure 3).

$$\text{Image Size: } ((72 \times 28 \text{ bit}) \div 8) \text{ byte} + 4 \text{ byte} = 256 \text{ byte}$$

Figure 3. Size of an SMS picture message

Now, one should have B&W picture steganography. The main idea in B&W picture steganography is changing pixels of the image that are less noticeable because, in color and grayscale pictures, information can be hidden by making a slight change in the color, which does not apply to B&W pictures. For example, a black point put in an area of the picture that is fully white will be noticeable. As a result, the first action to be done is to identify areas of the picture that would not be noticeable by anyone in case of hiding information and changing pixels. In the proposed algorithm, first the picture is divided into 3×3 blocks, and then the percentage of proportion of each block is calculated for steganography in it which is called flip-ability [17]. To calculate the flip-ability, a table containing all the possible models is prepared for B&W coloring of a 3×3 block and the flip-ability of each of the modes is calculated for steganography. Now, by searching the table and finding the corresponding mode of the selected block, the flip-ability of the block is determined for steganography.

The possible modes for B&W coloring of a 3×3 block is  $2^9 = 512$  modes. However, it is not necessary to calculate the flip-ability of all the modes. Simply by calculating a limited number of modes, one can find the flip-ability of all the modes because one can find the coloring modes of a 3×3 block by such conversions as rotating the picture, mirroring the picture or complementing the picture. Figure 4 shows the flip-ability value for a number of different coloring modes of a 3×3 block. In this figure a larger value indicates that the change of center pixel is less noticeable hence the change is more likely to be made for hiding information. The remaining modes, as already mentioned, are calculated according to this figure and by making the conversions. This lookup table has been developed by improving and correcting the table proposed by reference [17].

0.000	0.010	0.010	0.125
0.000	0.375	0.125	0.375
0.000	0.000	0.250	0.625
0.000	0.000	0.125	0.125
0.000	0.000	0.000	0.125
0.250	0.000	0.125	0.375
0.000	0.000	0.000	

Figure 4. The flip-ability lookup table for 3x3 patterns.

After calculating the flip-ability of each block, if the value exceeds a certain limit and the block can undergo steganography, one bit of information is hidden in the block.

For steganography of one bit of information in a block, first the white cells in the block are calculated. For steganography of one bit with value of 1, the number of white cells must be an even number. Therefore, if the number of white cells of the block is an odd number, by reversing the middle cell of the block, the number of white cells in the block will be an even number and, therefore, bit 1 will be hidden in this block of the picture (Figure 5).

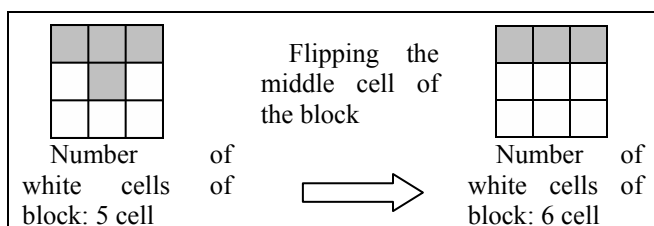


Figure 5. Hiding a bit with value of 1 in a 3x3 block

To hide one bit with a 0 value, the number of white cells in the block must be an odd number. Therefore, if the number of white cells in the block is an even number, by flipping the middle cell of the block, the number of white cells changed into an odd number and, thus, bit 0 will be hidden in this block of the picture.

As it is not possible to carry out steganography definitely in all the blocks, the maximum size of data that can undergo steganography in an SMS picture is 27 bytes (Figure 6).

$(72 \times 28 \text{ bit}) \div 9 = 216 \text{ bit}$	$216 \div 8 = 27 \text{ byte}$
---	--------------------------------

Figure 6. Maximum capacity of an SMS picture for hiding data

Indeed, before steganography, information is encoded by a password received from the user and then it is hidden in the picture.

During extraction of information from the picture, first the SMS picture is divided into 3x3 blocks. Then the flip-ability of each block is calculated with the method described in the steganography section. If the block can undergo steganography, one bit of information from that block is extracted. To do so, if the number of white cells in the block is even, the value of the hidden bit in the block is 1. If the number of white cells in the block is odd, the hidden bit in the block is 0. After full extraction of the entire hidden bits in the picture, information is decoded with a password received from the user.

The decoder program, after extracting hidden information from the SMS picture, removes the information from the picture and saves the picture without any data on the recipient's mobile phone. Morphological methods are used for removing hidden data from the picture. The method used in this project is smoothing the borders of the picture [25].

The size of the hidden information is hidden at the beginning of the picture in one byte so that a proper quantity of the information can be extracted from the picture.

## V. EXPERIMENTAL RESULT

This project provides a method for taking multiple-choice quizzes by SMS, in which the steganography is used for increasing the security of the exchange of questions and grade.

To implement the method, the J2ME (Java 2 Micro Edition) programming language has been used. This language is a special version of the Java language for small devices such as the mobile phone and PDA. The project consists of two separate programs, one for the instructor and one for the student.

In the instructor's program, first the program receives the questions (which are up to 20) from the instructor. A small picture (for steganography of the answers) is also received from the instructor, which is the university logo in this case (Figure 7). Then the program reads the mobile phone number and the student number of each student from the file containing information of each student.

The program first selects 5 questions for each student while following the algorithm provided in section 3 and displaces the answers. Then saves the question numbers. The steganography program, which is run separately, hides the answers and the time of the quiz in the received picture. This picture is now sent, along with five prepared questions, to all students.

**M-Quiz Professor Edition**

**Enter number of tests:**  
20

**Enter default file names:**  
problem

**Enter image file name:**  
sharif.png

Exit

Figure 7. An screenshot of instructor's program

In the student's program, which is run on his mobile phone, six SMS messages are received. First, from inside the first SMS picture message, the duration of the quiz and the answers of the questions are extracted by the SMS data extraction program—which is run separately—and the data within the picture is destroyed. Then the quiz questions are shown to the student respectively (Figure 8). The student has to enter the answers within the determined period of time.

In the end, the student's answers are compared with the correct answers and the student is given a grade. The grade and answers are hidden by the steganography program separately in the first SMS picture message. The SMS picture message is sent to the instructor. The instructor runs the SMS data extraction program to extract and record the student's grade.

**M-Quiz Student Edition**

**1- CISC machines**

**1) have fewer instructions than RISC machines**

**2) have medium clock speeds**

**3) use more RAM than RISC machines**

**4) use variable size instructions**

2

Back Next

Figure 8. An screenshot of student's program

Both the instructor's and the student's programs were written by J2ME programming language and run on a Nokia 6230i mobile phone.

For compiling the programs, I use Sun Java Wireless Toolkit for CLDC 2.5. I am also using Java 2 Platform Standard Edition Development Kit 5.0. For developing my programs on Nokia mobile phones, I am using Carbide.j 1.5 software.

Instructor's software consists of four classes. One of these classes is responsible for implementation of program GUI (Graphical User Interface). This class, which has been extended from "Form" class, receives necessary information such as number of quiz questions, name of files containing questions, etc from the instructor. The other class of this program is doing main operations such as finding and opening files of questions, creating SMS messages containing questions and sending them, etc. The other two classes of the program are hiding answers of questions inside an SMS picture message according to algorithm described in section 4. These two classes are executed by main class of the program.

For working with files (such as opening files containing questions) we have used JSR75 Optional Package. This optional package enables users to have access to files and directories existing on such devices as mobile phones through presentation of FileConnection API. By using it we can create, read, and write files and directories on mobile phones and on memory cards installed on mobile phones [26].

We have used JSR120 optional packages, named WMA (Wireless Messaging API), for sending and receiving of SMS messages. This package enables users to work with SMS messages and also binary SMS messages such as SMS picture messages [27].

The instructor's program can indeed be run on a computer with an SMS gateway.

Student's software consists of six classes. One of these classes is responsible for implementation of program GUI. This class has been extended from "Form" class. This class is displaying the questions and receiving answers from student and finally displaying the grade to the student.

The other class of the program which is the main class of program, calculates student's grade and then sends it to the instructor. At first this class extracts answers of questions using the two other classes, which are created for extracting hidden data from SMS picture messages. Then it displays the grade to the student using the GUI class. At last it hides student's grade and answers given by the student in an SMS picture message and sends it to the instructor by the two other classes of the program which are created for hiding data in SMS messages.

## VI. ADVANTAGES

In this section some advantages of my method are mentioned:

1. The mobile phone is a public facility and most individuals have mobile phones. On the other hand, the SMS is a popular service. Therefore, the proposed method covers a wide spectrum of students.
2. The SMS is an inexpensive service.
3. To take the quiz, each student only needs to send one SMS message in order to send the grade. Also all the quiz processes are carried out on the student's mobile phone, i.e., in general, this method is a client-side method. Therefore, this method has low costs for the student and, because of lack of too exchange of questions and answers between the student and instructor, the security of the quiz is high.
4. By using steganography in SMS picture messages, the security of this project for sending the correct answers and the final grade has been improved.
5. By destroying the hidden correct answers in SMS picture messages after extracting the answers from the picture, any misuse will be made impossible.
6. Because of not using sophisticated technologies, this method can be implemented on simple mobile phones as well and there is no need to use advanced mobile phones.
7. Instructor can evaluate each student by reviewing his grade and his answers to questions. Also he can improve his next quizzes by analyzing the students' answers to each question.

## VII. CONCLUSION

This paper provides a method for taking multiple-choice quizzes by SMS. By using SMS steganography, the test security has been improved as well. Also the answers of student test are sent back to the instructor and he can analyze the exam in future.

In addition to mobile phones, this method can be used on other devices such as PDAs.

The proposed method not only can be used for taking multiple-choice tests, but it can also be used for tests with descriptive or short answers.

Because of the low costs of this method for the student, it can be used in poor regions as well. Also, as only two contacts between the student and instructor are required (one for receiving the questions and the other for sending the grade), even if a telephone contact cannot be established by the student's mobile phone, the quiz will not be disrupted. Therefore, this method can be applied even at times such as travels and flights.

## REFERENCES

- [1] M. Shirali-Shahreza, "An Improved Method for Steganography on Mobile Phone," *WSEAS Transactions on Systems*, Vol. 4, Issue 7, July 2005, pp. 955-957.
- [2] GSM 03.40 v7.4.0, Digital cellular telecommunications system (Phase 2+), Technical realization of the Short Message Service (SMS), *ETSI 2000*, <http://www.etsi.org>.
- [3] M. Shirali-Shahreza, "M-Quiz by SMS," *Proceedings of the 6<sup>th</sup> IEEE International Conference on Advanced Learning Technologies (ICALT 2006)*, Kerkrade, The Netherlands, July 5-7, 2006, pp. 726-729.
- [4] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding-a survey," *Proceedings of the IEEE*, Vol. 87, Issue 7, July 1999, pp. 1062-1078.
- [5] L. Bollen, S. Eimler, and H. U. Hoppe, "The use of mobile computing to support SMS dialogues and classroom discussions in a literature course," *Proceedings of 2004 IEEE International Conference on Advanced Learning Technologies*, Joensuu, Finland, 30 August-1 September 2004, pp. 550-554.
- [6] A. Stone, J. Briggs and C. Smith, "SMS and interactivity-some results from the field, and its implications on effective uses of mobile technologies in education," *Proceedings of 2002 IEEE International Workshop on Wireless and Mobile Technologies in Education (WMTE 2002)*, Växjö, Sweden, 29-30 Aug. 2002, pp. 147-151.
- [7] A. Tretiakov and K. Kinshuk, "Creating a Pervasive Testing Environment by Using SMS Messaging," *2005 IEEE International Workshop on Wireless and Mobile Technologies in Education (WMTE 2005)*, Tokushima, Japan, 28-30 November 2005, pp. 62-66.
- [8] K. Curran, K. Bailey, "An Evaluation of Image Based Steganography Methods," *International Journal of Digital Evidence*, vol. 2, issue 2, Fall 2003, pp. 1-40.
- [9] N. Provos and P. Honeyman, "Hide and Seek: An Introduction to Steganography," *Security & Privacy Magazine*, May/June 2003, pp. 32-44.
- [10] L. M. Marvel, C. G. Boncelet, Jr., and C. T. Retter, "Spread spectrum image steganography," *Proceedings of the IEEE Transactions on Image Processing*, August 1999, pp. 1075-1083.
- [11] K. Tanaka, Y. Nakamura, and K. Matsui, "Embedding secret information into a dithered multi-level image," *Proceedings of IEEE Military Communications Conference*, 1990, pp. 212-220.
- [12] S. H. Low, N. F. Maxemchuk, J. T. Brassil, and L. O'Gorman, "Document marking and identification using both line and word shifting," *Proceedings of the 14<sup>th</sup> Annual Joint Conference of the IEEE Computer and Communications Societies*, vol.2, 1995, pp. 853-860.
- [13] Y. C. Tseng, Y. Y. Chen, and H. K. Pan, "A Secure Data Hiding Scheme for Binary Images," *IEEE Transaction on Communications*, Vol. 50, No. 8, Aug. 2002, pp. 1227-31.

- [14] Y. Y. Chen, H. K. Pan, and Y. C. Tseng, "A Secure Data Hiding Scheme for Two-Color Images," *Proceedings of the IEEE Symposium on Computers and Communications*, 2000, pp. 750-755.
- [15] Y. C. Tseng and H. K. Pan, "Secure and Invisible Data Hiding in 2-Color Images," *Proceedings of the IEEE INFOCOM*, 2001, pp. 887-896.
- [16] M. Wu, E. Tang, and B. Liu, "Data hiding in digital binary image," *Proceedings of the IEEE International Conference on Multimedia & Expo*, New York, 2000.
- [17] M. Wu and B. Liu, "Data Hiding in Binary Image for Authentication and Annotation," *IEEE Transaction on Multimedia*, vol. 6, no. 4, August 2004, pp.528-538.
- [18] J.C. Judge, "Steganography: Past, Present, Future", *SANS white paper*, November 30, 2001, <http://www.sans.org/rr/papers/index.php?id=552>, last visited: 19 February 2007.
- [19] G. Doërr and J. Dugelay, "A guide tour of video watermarking", *Signal Processing: Image Communication*, vol. 18, no. 4, 2003, pp. 263-282.
- [20] K. Gopalan, "Audio steganography using bit modification", *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP'03)*, Hong Kong, vol. 2, April 6-10, 2003, pp. 421-424.
- [21] N. F. Maxemchuk and S. Low, "Marking Text Documents", *Proceedings of the IEEE International Conference on Image Processing*, Santa Barbara, CA, Oct. 26-29, 1997, pp. 13-16.
- [22] M. Shirali-Shahreza, "Steganography in SMS," *Proceedings of the 11<sup>th</sup> International CSI Computer Conference (CSICC'2006)*, School of Computer Science, IPM, Tehran, Iran, 24-26 January 2006, pp. 905-910, (in Persian).
- [23] M. Shirali-Shahreza, "Stealth Steganography in SMS," *Proceedings of the third IEEE and IFIP International Conference on Wireless and Optical Communications Networks (WOCN 2006)*, Bangalore, India, 11-13 April 2006.
- [24] Nokia, "Sending Content over SMS to Nokia Phones", Version 1.0, *Forum Nokia*, May 2001, <http://www.forum.nokia.com>, last visited: 19 February 2007.
- [25] R. Haralick and L. Shapiro, *Computer and Robot Vision*, Vol. I, Addison-Wesley, 1992.
- [26] Java Community Process (JCP), "URLConnection Optional Package 1.0 Specification," 07 June, 2004, <http://www.jcp.org/en/jsr/detail?id=75>, last visited: 19 February 2007.
- [27] Java Community Process (JCP), "Wireless Messaging API (WMA) specification," 25 April, 2003, <http://www.jcp.org/en/jsr/detail?id=120>, last visited: 19 February 2007.



**Mohammad Shirali-Shahreza** is nineteen years old. He is an undergraduate student in computer science at Sharif University of Technology in IRAN. He got his diploma from Allameh Helli high school, Tehran, IRAN, that is a school for exceptional talents students.

His project on Steganography won the best prize of 5<sup>th</sup> Iranian Khwarizmi young festival.

He has 23 accepted papers in international conferences and eight published papers in journals.

He also has more than ten papers submitted for conferences and journals.

He won the "young researcher award" of the 2<sup>nd</sup> IEEE International Conference on Information & Communication Technologies: from Theory to Applications (ICTTA'06).

He also won the "young researcher award" of the 11<sup>th</sup> International CSI Computer Conference (CSICC'2006).

He won the undergraduate youngest research award from Iranian Society of Cryptology (2006).

He is a student member of IEEE and Iranian Computer Society

His research background includes Steganography, CAPTCHA, Java and Mobile programming.