Data Hiding over Mobile Phones using Socket Network Communication

Dr. Ahmed S. Nori[1] , Shatha A. Baker[1]
[1]Computer Science Dept./ Mosul University
Mosul, Iraq

Abstract

The mobile phone is considered as wireless means of communication produced by sophisticated modern technology. After expanding use of mobile phones, establishing hidden communication is an important subject of security that has gained increasing importance. Therefore need to adopt the technology more sophisticated and more secret and preserve the information, Steganography was used. Steganography is a science hide confidential data in the carrier task inoffensive manner embeds the existence of hidden data without raising suspicion in order to keep the contact between the two callers confidential.

In this paper we proposed new methods to hide using Steganography to include confidential information (images, text, and voice) in images without getting any distortion brings attention. The operation of selecting sites to hide it has by generating random numbers using a private key, which is also used in the recovery operation. This paper is implemented on J2ME (Java 2 Micro Edition) platform.

Keywords: *Steganography, mobile phone, Socket, J2ME.*

1. Introduction

Mobile phones are the most technologically advanced devices that used in today, its affect on different aspect of life. With the expansion use of the mobile phone the issue of secure communication became more important.

Steganography is the art and science of writing hidden messages in such a way that no one, apart from sender and intended receiver, suspect the existence of the message. Images are the most popular cover object used for steganography [1].

In the last few years many wireless technologies have begun to appear. These technologies have become more available, flexible, and easy to use. WLAN, especially Wi-Fi, has appeared as a much more powerful and flexible alternative than wired LAN.

The most famous mobile phone programming languages is J2ME, which is a special version of java language for small devices such as mobile phone and PDAs (Personal Digital Assistant)[2].

In this paper we present proposed methods for image steganography on wireless networks based on the J2ME platform.

2. Related Work

Ritesh Pratap Singh & Neha Singh [3], they present an image steganography method for image steganography in Multimedia Message Service (MMS) using Code Division Multiple Access (CDMA) spread spectrum both in spatial domain and Transform domain.

Wuling REN & Dafeng YU [4], they introduces the J2ME platform for wireless networks based on communication technology, network programming interfaces Socket communication theory; and then analyzes and compares several common encryption algorithms; then proposed an encryption solutions based on J2ME Socket protocol, and gives the realization of the program.

Ravi Saini & Rajkumar Yadav[5], they proposed steganography algorithm uses the logical AND operation on the binary value of pixel intensity and binary value of the pixel portion. The message bit is inserted according to the result of logical AND operation.

Rahul Joshi, Lokesh Gagnani et. al [6], they have explain different applications have different requirements of the steganography technique used, with an emphasis on image steganography.

Mohammad Shirali-Shahreza [7], he purposed a new method for steganography in MMS messages. The method is based on both text and image steganography methods, and the data is broken into two parts and hidden in both text and image part of MMS message.

3. Steganography

Steganography is a strategy in which required information is to transmit a secret message through any other information such that the second information appears the same as original, where the existence of the secret message is concealed [8].

The word steganography is originally made up of two Greek words “stegos” meaning “cover” and “grafia” meaning “writing” defining it as “covered writing”[9].

Using steganography a secret message is embedded inside a piece of unsuspicious information and sent without anyone knowing the existence of the secret message. Steganography has been carried out on text, image, audio, video, etc. Most steganographic utilities hide information inside image, as it is relatively easy to implement images are mostly used in the process or of steganography because it is hard to break [10].

A possible formula of the process may be represented as[1]:

stego-medium= embedded message
+ cover medium + stego key

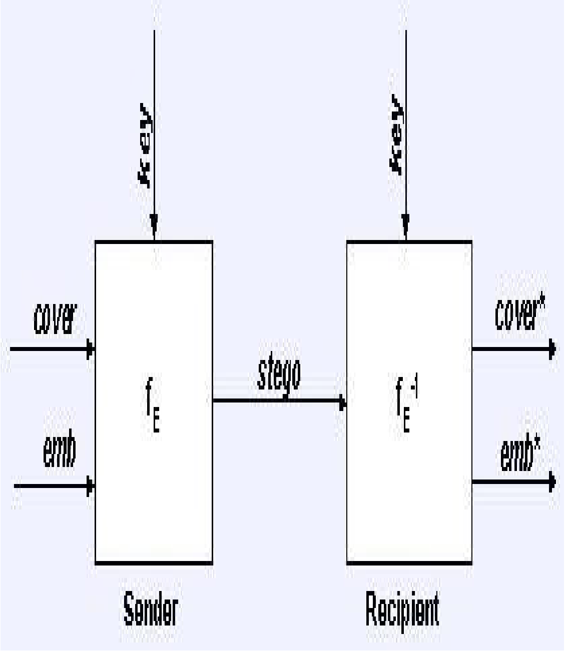

Figure 1: Basic model of steganography

fE : embedding process
fE^{-1} : extracting process
cover: cover data in which secret message will be hidden
emb: secret message
stego: cover data with the secret message

The most popular type of insertion method is known as Least Significant Bit (LSB) method. In this method, the least significant bit of each pixel of the cover image is replaced by bits of the secret message. The secret message is first converted entirely into bit stream. Then all those bits are substituted at the places of all least significant bits of all pixels. Each color pixel, or picture element of a digital picture is composed of three color components (Red, Green and Blue) and each component is represented by eight bits or one byte. The value of each byte is the bit pattern stored in the bytes. When the least significant bit of the byte of any component is replaced by another bit value, change in the value is least. By replacing LSB of most of the pixels of an image makes no significant visual changes that can be detected by human eyes. In this fashion, an entire secret message can be inserted inside a cover image[11].

4. Introduction of J2ME

J2ME (Java 2 Micro Edition) is an integral part of the Java 2, together with Java2 SE(Standard Edition), Java2EE (Enterprise Edition) they make up the main three versions of Java technology, and also work out by JCP (Java Community Process).

J2ME aims to serve large range of different device types, such as mobile phones, pagers, internet TVs, and personal digital assistants (PDAs).

J2ME include, See in Figure 2 [12] :

- Configurations
- Profiles
- Optional packages

Configuration has two categories:

- Connected Device Configuration (CDC) design for PDAs .
- Limited Connected Device Configuration (LCDC) design for mobile phone.

Mobile Information Device Profile (MIDP) is corresponding for profile to the mobile device in J2ME.

The MIDP application is packaged inside a Java ARchive (JAR) file, which contains the application class and resource files. In real device (mobile phone) the JAR file is loaded with the Java application descriptor file[13].

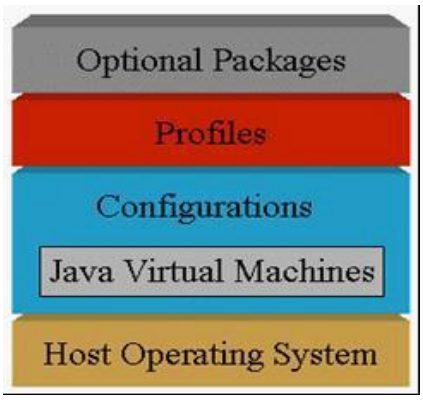

Fig. 2 Structure of J2ME systems

5. The Socket technology based on J2ME

Socket is a common data communication mode in communication network applications, often uses the client/server (C/S) system structure. At present, the Socket has been widely accepted, become a very popular network programming interface API. Through the Socket we can send TCP protocol data, data mainly transfer through IP protocol of the layer network protocol, thus socket is also considered as a network programming interface in TCP/IP protocol. The display of sending and receiving data by Socket is layered shown in Fig. 3[4].

Programming interface in MIDP2.0 provides two interfaces that are ServerSocketConnection and SocketConnection, respectively used to develop the server side of Socket and the client side. Through the two interfaces communicate between server and client[2].

The server side:

```
String url="socket://:6060";
ssc=(ServerSocketConnection)Connector. open(url);

try{
sc=(SocketConnection)ssc. acceptAndOpen()
dis=sc.openDataInputStream();
dos=sc.openDataOutputStream();
......}
```

The client side:

```
String url="socket://localhost:6060";
SocketConnection sc=null;
DataInputStream dis=null;
DataOutputStream dos=null;
StringBuffer buffer=new StringBuffer();

try{
sc=(SocketConnection)Connector.open(url);
dis=sc.openDataInputStream();
dos=sc.openDataOutputStream();
.......
}
```

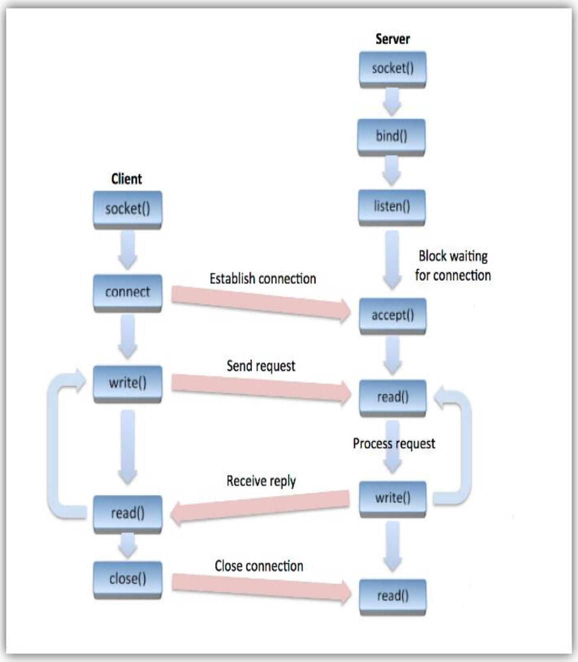

Fig.3 Socket communication between server and client

6. Proposed Methods

- **Image**

To embed one bit from secret image (S_bit) by using the Most Significant Bit (MSB) and Least Significant Bits (LSB1, LSB2) form the cover image.as shown in Fig. 4. To explain the method

```
If S_bit=MSB Then
  {     If (LSB1≠ LSB2) Then
            do nothing
        Else
            Change the value of LSB1
  }
Else
     If S_bit=1 then
      {
         LSB1=1
         LSB2=1
      }
   Else
     {
        LSB1=0
        LSB2=0
     }
```

When we want to extract the secret image by check the values of MSB, LSB1 and LSB2,

```
  If (LSB1≠ LSB2) Then
            S_bit=MSB
Else
  {
      If  ( LSB1=1 ) Then
             S_bit=1
      Else
            S_bit=0
   }
```

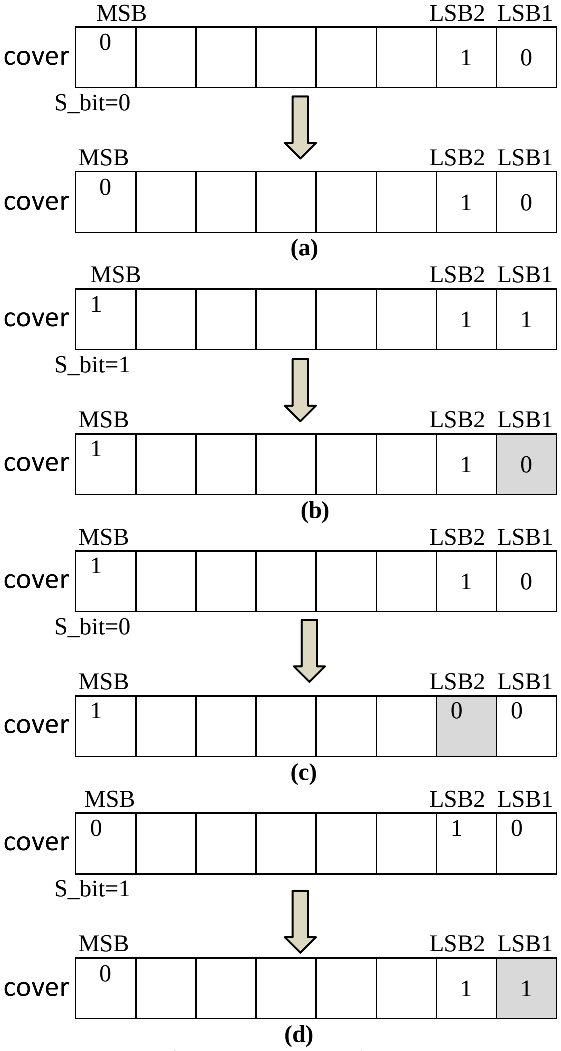

Fig. 4 Steps for Proposed Method for image

- **Text**

To embed one bit from secret text by using the stego bit and apply the XOR operation between them and the result put in the Least Significant Bit of the cover image.

$$LSB = Stego\ bit \oplus Secret\ bit$$

When we want to decode the secret text by inverting the operation according to the equation :

$$Secret\ bit = Stego\ bit \oplus LSB$$

The stego bit can be calculate as
for example: byte value of image was 101,

0	1	2	3	4	5	6	7
1	0	1	0	0	1	1	0

Rotate the byte

0	1	2	3	4	5	6	7
0	1	1	0	0	1	0	1

Implemented AND between bits of pixel and bits after rotate

0	1	2	3	4	5	6	7
0	0	1	0	0	1	0	0

Find the number of one's and number of zero's, if the one's greater than zero's stego bit equal one else zero.
the stego bit =0

- **Sound**

To embed one bit from secret sound by using the stego bit and apply the XOR operation between them and the result put in the Least Significant Bit of the cover image.

$$LSB = Stego\ bit \oplus Secret\ bit$$

When we want to decode the secret text by inverting the operation according to the equation:

$$Secret\ bit = Stego\ bit \oplus LSB$$

The stego bit can be calculate as for example: byte value of image was 250,

0	1	2	3	4	5	6	7
0	1	0	1	1	1	1	1

Divide the byte in the two parts

0	1	2	3
0	1	0	1

4	5	6	7
1	1	1	1

Add two parts and take the carry bit

1	0	0	1		1

Note: the two sides (sender and receiver) must be agreed together for using the same secret key. In our method, we use the sequence of day in a week (day no.).

1-Embedding Process

The embedding process carried on the sender side to get stego images, which sent to receiver using the steps below:

- **Input data:** secret message (image or text or sound), cover image, key.
- **Output data:** Stego image.

Step 1: Scan the cover image row by row and encode it in binary which contains the RGB value or intensity of each pixel.
Step 2: The secret message is converted into binary.
Step 3: Check the size of the stego image and the size of the secret message.
Step 4: Choose one pixel of the image randomly.
Step 5: Apply the proposed method according to the type of secret message.
Step 6: Set the image with the new values.
Step 7: Repeat Step5 and Step6 until all the secret bit chunks are mapped over the cover
Step 8: Send the stego image obtained to the receiver.

2- Extraction Process

The extraction process carried on the receiver side. Upon receiving the stego image, secret message must be extracted as given below:

- **Input data:** Stego image, key.
- **Output data:** Secret message.

Step 1: Scan the stego image row by row and encode it in binary which contains the RGB value or intensity of each pixel.
Step 2: Choose one pixel of the image randomly.
Step 3: Apply the proposed method according to the type of secret messge.

Step 4: Set the image with the new values.
Step 5: Repeat Step2 and Step3 until all the secret bit chunks are retrieved over the stego image.
Step 6: Finally, the image is constructed using all the pixels which is computed in Step 4 will reveal the secret message.

7. Results and Discussion

All experiments have been done on Nokia phones. For testing two color images, each of (256 x 256) and (512 x 512) pixels were used. These cover images are Rose, Boy, in figure (4).
To know the amount of difference between the original image and the target image (Stego image), three kinds for performance measurements between the two images are used [14], which are

(a) MSE: It is defined as cumulative squared error between cover & stego image. The equation of MSE given by:

$$MSE = \frac{1}{mn}\sum_{x=0}^{m-1}\sum_{y=0}^{n-1} steg\_im(x,y) - cover\_im(x,y) \cdots (1)$$

Where m, n = The size of stego image.

(b) PSNR: It is measure of quality of image. PSNR can represent by using equation given:

$$PSNR = 10.\log_{10}\left(\frac{(\text{Max value of Gray level})^2}{MSE}\right). \ldots(2)$$

(c) NC: It used to measure the similarity between cover image and stego image. Equation for NC is given below:

$$NC = \sum_{x=0}^{m-1}\sum_{y=0}^{n-1} steg\_im(x,y) * cover\_im(x,y) /$$

$$\sum_{x=0}^{m-1}\sum_{y=0}^{n-1}((cover\_im(x,y))^2 \qquad \ldots\ldots\ldots(3)$$

The table 1 indicates that (512 × 512) pixel image has more PSNR and less MSE as compared to (256×256) pixel images see figure 4. Also it indicates that the cover image has high similarity (NC) to the stego image with higher pixel cover images.

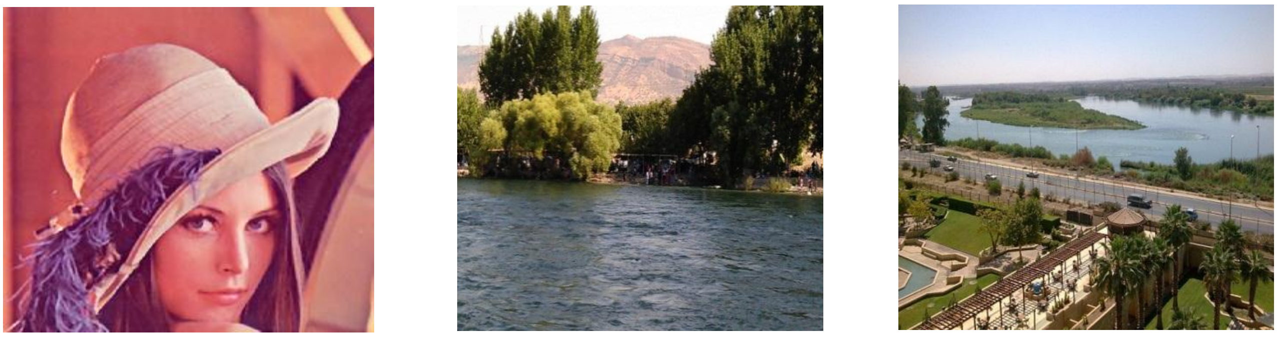
Image1
Image2
Image3

Fig. 5 Samples for image method

Table 1: Comparison MSE, PSNR and NC

Image	*Pixels*	*MSE*	*PSNR*	*NC*
Image1	256x256	0.2872	53.5489	1
Image2	512x512	0.0704	59.655	1
Image3	640 x 480	0.0397	62.1428	1

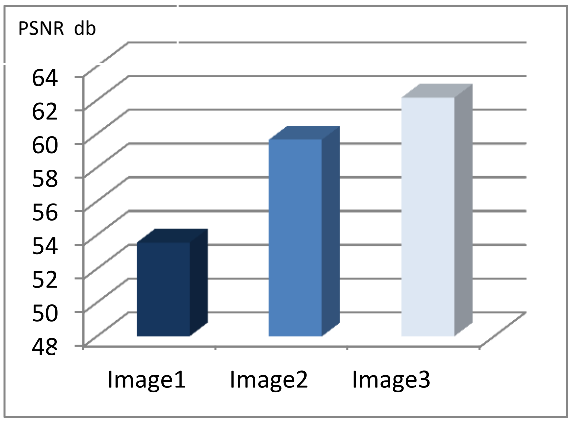

Fig. 6 PSNR Comparison of image method

Image4

Image5

Image6

Fig. 7 Samples for text method

Table 2: Comparison MSE, PSNR and NC

Image	*Pixels*	*MSE*	*PSNR*	*NC*
Image4	256x256	0.011	67.7168	1
Image5	512x512	0.0027	73.8171	1
Image6	640 x 480	0.0023	74.5135	1

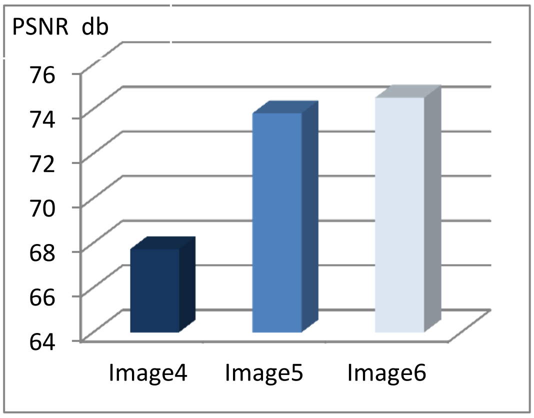

Fig. 8: PSNR Comparison of text method

Image7

Image8

Image9

Fig. 9 Samples for sound method

Table 3: Comparison MSE, PSNR and NC

Image	*Pixels*	*MSE*	*PSNR*	*NC*
Image7	256x256	0.122	57.2672	1
Image8	512x512	0.2816	63.6437	1
Image9	640 x 480	0.0222	64.6672	1

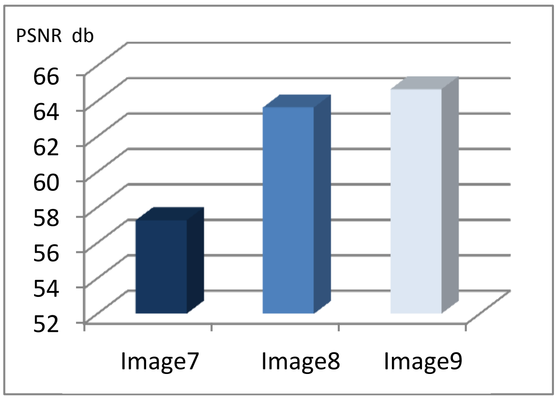

Fig.10 PSNR Comparison of sound method

The table 1, 2 and 3 indicate that 640x480 pixel image has more PSNR and less MSE as compared to 256×256 and 512 × 512 pixel images. Also it indicates that the cover image has high similarity (NC) to the stego image with higher pixel cover images.

8. Compare between Methods

Figure11: Sample for comparison methods

Table 4: Comparison MSE, PSNR and NC

Method	*Secret message*	*MSE*	*PSNR*	*NC*
Image	Image	0.213	54.847	1
	Text	0.3018	53.3336	1
	Sound	0.3328	52.9089	1
Text	Image	0.1587	56.1250	1
	Text	0.0481	61.3039	1
	Sound	0.0522	60.954	1
Sound	Image	0.0476	61.3547	1
	Text	0.0379	62.3444	1
	Sound	0.0376	62.3789	1

The table 4 indicates that the similarity of cover size (image, text, sound) gave an equal ratio for MSE, which considered as good performance. Also, the measure PSNR, approved the same result

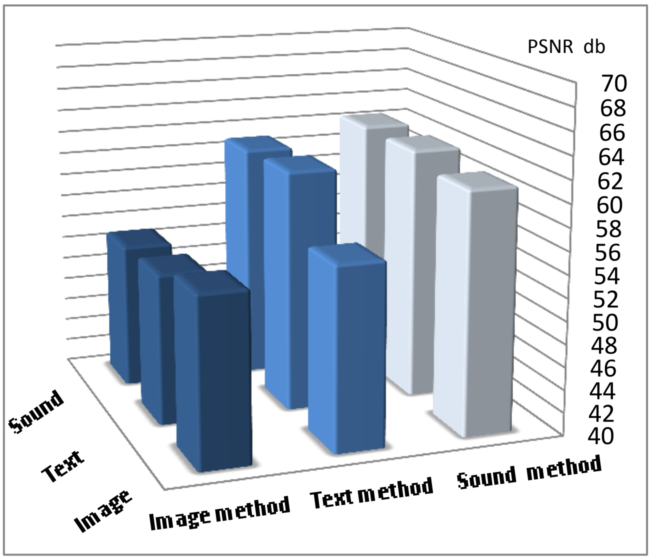

Fig. 12: PSNR Comparison of three methods

9. Conclusion

In this paper we presented and discussed the possibility for using steganography in the mobile phone. We examined images that could be applied as a cover in order to hide secret message (image, text, sound).

The proposed methods using comparison between data of cover image with secret message, which considered as a new methods. This centered on increasing the security by making use of pseudo-randomized key and also applicable to color level images.

References

[1] A. Kumar, and K. Pooja, , "Steganography- A Data Hiding Technique", International Journal of Computer Applications,Vol. 9, No.7, 2010.

[2] S. Li, and J. KNUDSEN, "Beginning J2ME: From Novice to Professional", Third Edition ed.: Apress, 2005.

[3] R. P. Singh, and , N. Singh, "Steganography in Multimedia Messaging Service of Mobile Phones Using CDMA Spread Spectrum", Akgec Journal of Technology, vol. 1, no.1, 2010.

[4] W. REN, and D.YU , "Research on encryption technology based on J2ME socket network communication," 2011 International Conference on Mechatronic Science, Electric Engineering and Computer (MEC), 2011, pp. 1969-1973.

[5] R.Saini, and R.Yadav, "A New Data Hiding Method Using Pixel Position and Logical AND Operation", International Journal of Computer and Electronics Research , Volume 1, Issue 1, June 2012.

[6] R. Joshi, L. Gagnani and S. Pandey, "Image Steganography", International Journal of

Advanced Research in Computer Engineering & Technology, Volume 2, Issue 1, January 2013.

[7] M. Sh. Shirali, “Steganography in MMS”, Proceedings of the 11th IEEE International Multitopic Conference (INMIC), Lahore, Pakistan,2007.

[8] R. Joshi, L. Gagnani, and S. Pandey, , “Image Steganography With LSB”, International Journal of Advanced Research in Computer Engineering & Technology ,Volume 2, Issue 1, January 2013.

[9] T. Morkel, , J.H.P. Eloff, and M.S. Olivier, "An Overview of Image Steganography", in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005.

[10] G. Huayong, H. Mingsheng, and W. Qian, “Steganography and Steganalysis Based on Digital Image”, International Conference & Signal Processing, IEEE, 2011.

[11] Sh. Baker and A. Nori, “Steganography in Mobile Phone over Bluetooth”, International Journal Of Information Technology And Business Management, Vol. 16, 2013.

[12] J. Keogh, “J2ME The complete Reference”, McGraw-Hill Publishing Company Limited, 2003.

[13] J. WHITE, and D. HEMPHILL, “Java 2 Micro Edition”, USA, 2002.

[14] N. Batra and P. Kaushik, “Data Hiding in Color Images Using Modified Quantization Table”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 1, Issue 8, 2012.

Dr.Ahmed S. Nori is currently an Assistant Professor at the Computer Science Department, College of Computer Science and Mathematics at Mosul University / IRAQ. He supervised over 15 M.Sc. thesis. Dr. Ahmed obtained his bachelor, master, and doctorate in Computer Science from Mosul University and Baghdad University in 1992, 1995, and 2006 respectively. Work with Mosul University / IRAQ since 1996 till now. His research area include Information Security, Computer Security, Multimedia, Image Processing, and Mobile programming.

Shatha A. Baker is currently a master student in computer science at Mosul University. Shatha obtained his bachelor in computer science from the Same college in 1997. Her interested research area include Mobile programming, Information Security and Multimedia communications .