



# **A Steganography-Based SMS and MMS Services for Secure Messages Exchange on Mobile Networks**

خدمات الرسائل القصيرة و رسائل الوسائط المتعددة المعتمدة علي اخفاء المعلومات  
في تبادل الرسائل الآمينة في شبكات الموبايل

**By**

**Salwa alsharif**

**Supervisor**

**Prof. Dr. Alaa Hussein Al-Hamami**

**This thesis is submitted in partial fulfillment of the  
requirements for the degree of master in computer  
science.**

**Department of Computer Science**

**College of Computer Sciences and Informatics**

**Amman Arab University**

**January 2013**

**Amman Jordan**

*Amman Arab University*

*Authorization Form*

I, salwa alsharif, authorize the Amman Arab University to supply copies of my thesis to libraries or establishments or individuals on request, according to the Amman Arab University regulations.



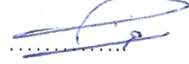
Signature: 

Data: 20/3/2013

## APPROVAL

This thesis titled "A Steganography-Based SMS and MMS Services for Secure Messages Exchange on Mobile Networks", has been successfully defended and approved by examining committee on 26/2/2013.

### Examination Committee

		signature
Dr. Nedhal A. Al-saiyd	Chairman	
Prof. Dr. Alaa Hussein Al-Hamami	Member & supervisor	
Dr. Feras Fares Mousa Al-mashagba	Member	

## DEDICATION

*With Love and Faithfulness, I dedicate this work,*

*To my husband saleh elgade who always stood beside me giving me his support and the power to proceed*

*To my daughter hawa and my son almahdi*

*To my father Muftah, and my mother najmia and my brothers and sister*

*To my supervisors,*

*Prof. Dr. Alaa Hussein Al-Hamami*

## Acknowledgments

*Praise and thanks be to Allah who guided us and pleased hurry it is my pleasure to express my deepest gratitude and sincere thanks to my Supervisors Prof. Dr. Alaa Hussein Al-Hamami for their continuous guidance throughout my work my deepest and sincere thanks are presented to all members of the examination committee.*

## Table of contents

DEDICATION.....	IV
Acknowledgments.....	V
Table of contents .....	VI
Table of Figures .....	VIII
List of Abbreviations.....	XI
Abstract.....	XIV
Abstract in Arabic.....	XV
Chapter One Introduction.....	1
1.1: Mobile Phone.....	1
1.2: Mobile Phone and Wireless Communication .....	2
1.3: Mobile Phone Services .....	3
1.4: Mobile Phone and Steganography.....	4
1.5: Mobile Phone Security .....	5
1.6: Steganography .....	6
1.7: Types of Steganography.....	7
1.8: Categories of Steganography .....	8
1.10: Steganography Classification of Techniques .....	11
1.11: The Statement of Problem.....	12
1.12 Contribution .....	12
1.13: Research Hypothesis.....	13
1.14: Research Tools.....	13
1.15: Thesis Organization.....	19
Chapter Two Literature Review.....	20
2.1. Introduction .....	20
2.2. Literature Reviews .....	21
2.3 The Proposed Work.....	29
Chapter Three The Developed System Design .....	30
3.1. Introduction .....	30

3.2 The Developed Steganography Software Design on Mobile Application	31
The System Activity Diagram is shown in Figure (3. 2)	34
3.3 Project Environment (Net beans 7.0.2 “J2ME”)	35
3.5.2 Process extracting secret information within SOAP consists of the following	41
3.6 MMS Menu	44
3.6.1.1 Process embedding secret information into digital image used LSB algorithm and DCT algorithm	45
3.6.1.2 Process extracting secret information from digital image used LSB algorithm and DCT algorithm	49
3.6.2 MMS _Double Cover	51
3.6.2.1 Process embedding secret information into two digital images used LSB algorithm and DCT algorithm	53
3.6.2.2 Process embedding secret information into two digital images used LSB algorithm and DCT algorithm	56
Chapter four Results and Discussions	61
4.1 Introduction	61
4.2 SMS_MGS Menu	62
4.3 MMS_MSG Menu: are divided into (Single cover, Double cover)	69
4.3.1 MMS _Single cover	69
4.3.2 MMS _Double cover: MMS _double cover sender form as the following:	75
4.4 Conclusion:	81
Chapter Five Conclusions and Recommendations for Future work	82
5.1. Introduction	82
5.2. Conclusions	82
5.3 Future Works	84
Reference:	85

## Table of Figures

Figure (1.1): The mobile phone.....	3
Figure (1.2): The wireless space .....	4
Figure (1.3): Pure Steganography process.....	9
Figure (1.4): Secret key Steganography.....	10
Figure (1.5): Public key Steganography.....	10
Figure (1.6): Categories of Steganography.....	11
Figure (1.7): Steps of Steganography.....	13
Figure (1.8): Discrete cosine transform of an image.....	21
Figure (3.1): Show HelloMIDLet.java to the proposed design.....	39
Figure (3.2): Shows project chart.....	40
Figure (3.3): Show send SMS message .....	44



Figure (3.4): Show send MMS message .....53
Figure (4.1): Shows Steganography in mobile application software and two main menus (SMS, MMS).....61
Figure (4.2): Shows the sender select text covers SMS.....62
Figure (4.3): Shows cover text and the senders write the secret message.....63
Figure (4.4): Show process embedding and menu contains send and save options by the result.....64
Figure (4.5): Shows the option saves to save result in the mobile.....65
Figure (4.6): Show process sends to the result.....66
Figure (4.7): Show process extracts the secret message.....67
Figure (4.8): Shows when the sender selects single cover and next select cover (image).....68
Figure (4.9): Show the image cover and the sender to write secret message, so show result to process embedding.....69

Figure (4.10): Show option save the result when the sender is unwilling to be sent to the receiver.....	70
Figure (4.11): Show process sends to the result.....	71
Figure (4.12): Show process extract secret message from the image .....	72
Figure (4.13): Show mine screen MMS _double and select cover1.....	73
Figure(4.14): Show the embedding cover1and writes MGS, and embedding result into cover2.....	74
Figure (4.15): Show save the result when the sender is unwilling to be sent to the receiver.....	75
Figure (4.16): Show process sends to the result.....	76
figure (4.17): Show process extract secret message from the cover .....	77

## List of Abbreviations

AES	Advanced Encryption Standard
AIM	Application Instant Messaging
API	Application Programming Interface
ATM	Automatic Transfer Money
CDC	Connected Device Configuration
CLDC	Connected Limited Device Configuration
DCT	Discrete Cosine Transform
DES	Data Encryption Standard
ECC	Elliptic Curve Cryptography
GIF	Graphics Interchange Format
GSM	Global System for Mobile Communications
ICQ	Internal Control Questionnaire
ICT	Information and Communications Technology
IPV6	Internet Protocol version 6
JCP	Java Community Process
JPEG	Joint Photographic Experts Group
J2ME	Java 2 Micro Edition

J2SE	Java 2 Standard Edition
JVM	Java Virtual Machine
LSB	Least Significant Bit
MIDI	Musical Instrument Digital Interface
MIDP	Mobile Information Device Profile
MMS	Multimedia Messaging Service
MP3	Moving Picture Third
MPEG4	Moving Picture Experts Group
NTRU	Northern Territory Rugby Union
OSI	Open Systems Interconnection
PDA	personal digital assistants
PINS	Personal Identification Numbers
PNG	Portable Network Graphic
P2P	Peer-to-Peer
PSTN	Public Switched Telephone Network
RSA	Rivest Shamir Adelman
SMS	Short Message Service

SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TEA	Tiny Encryption Algorithm
WAP	Wireless Application Protocol
WEP	West European Politics
XML	Extensible Markup Language

## Abstract

In recent years, Internet and mobile is widely used for communication. Short Messaging Service (SMS) and Multimedia Messaging Service (MMS) are the most popular services provided by the telecommunication companies. These services make the communication so fast and easy; attention toward information security must be increased, protection becomes a necessity because of the threats to the privacy and security. Hiding technique or as called Steganographic is used to hide the transferred secret information existence with other information. When data is hidden within text or image apparently may look the same for the naked eye of a person.

The Steganography software for mobile application is designed upon using the mobile phone messaging architecture system and use Steganography technique to hide secret messages into SMS and MMS covers , by using SOAP algorithm to embedded secret message into cover message and generate Stego text (SMS) and using LSB algorithm to embed secret message into cover image and generate Stego image (MMS) and using the same menu for the messages of the mobile phone system to send messages to one or more users at the same time, and it is possible to extract directly the hidden secret message by the receiver. This software is implemented by using J2ME (Java 2 Micro Edition) programming language and our dependence flexibility of the software load on all types mobiles that have the property of the send messages without any modification or conditions for flexible software and ease of capacity and conclusion that steganography software can demonstrate both reliability and portability at the same time.

The result of the proposed solution shows that using the Steganography technique in SMS and MMS, we used the same facility of the messages in the mobile phone system will increase the protection of the privacy and secrecy of sent messages.

## Abstract in Arabic

في السنوات الماضية ، إستخدام الإنترنت والهاتف النقال على نطاق واسع للاتصال و خدمة الرسائل القصيرة (SMS) وخدمة رسائل الوسائط المتعددة ( MMS ) هي من أكثر الخدمات التي تقدمها شركات الاتصالات ، هذه الخدمات تجعل الإتصالات سريعة وسهلة لذلك علينا أهتمام بزيادة أمن المعلومات بسبب التهديدات التي تتعرض لها الخصوصية والأمنية اصبح الحماية ضرورة. تقنية إخفاء المعلومات أو ما يسمى الستيكانوكرافي يستخدم لإخفاء المعلومات السرية ونقلها مع غيرها من المعلومات، وذلك بأخفاء المعلومات السرية داخل النص أو الصورة التي قد يبدو الشيء نفسه بالنسبة للعين المجردة لأي شخص.

صممت برمجيات الستيكانوكرافي لتطبيقات الهاتف النقال باستخدام نفس نظام الهندسة المعمارية للتراسل للهاتف النقال ، واستخدامنا لتقنية الستيكانوكرافي لإخفاء الرسائل السرية داخل اغطيات SMS و MMS و استخدام خوارزمية SOAP لتضمين الرسالة سرية داخل الرسالة الغطاء وتوليد النص مغطي (SMS) و استخدم خوارزمية LSB لتضمين الرسالة سرية داخل صورة الغطاء و توليد صورة مغطي (MMS) و كذلك اعتمدنا استخدام نفس نظام قائمة الرسائل للهاتف النقال لإرسال الرسائل إلى واحد أو أكثر من المستخدمين في نفس الوقت ومن الممكن استخراج الرسالة السرية المخفية مباشرة من قبل المتلقي.

وتم تنفيذ برمجيات الستيكانوكرافي باستخدام لغة البرمجة (J2M)، واعتمدنا المرونة لتحمل البرمجيات علي جميع انواع اجهزة النقال التي لديها خاصية ارسال الرسائل بدون اي قيود او شروط لمرونة البرمجيات وسهولة القدرات واستنتاج ان برمجيات الستيكانوكرافي يمكنها تثبت كل من الموثوقية والقابلية في نفس الوقت.

نتيجة الحل المقترح تبين أن استخدام تقنية الستيكانوكرافي في SMS و MMS، واستخدامنا لنفس نظام ارسال الرسائل للهاتف النقال يزيد من حماية خصوصية وسرية الرسائل المرسله

## Chapter One Introduction

The mobile phone (cellular) has become one of the most omnipresent communication devices within the past decade. Mobile phones used to be an esoteric device, but today is certainly the most pervasive communicative device that people carry. The mobile phone can connect people "anytime", "anywhere".

With the wide spread and high penetration of mobile phones, the use of the mobile phone at anytime, anywhere and anyway, and the rapid development of the mobile phone can be attributed to many factors, including increased portability, capacity, as large size memory, large process power and Internet browsing, declining costs and added value-added services. Furthermore, mobile phone technology is becoming more advanced every year; for example, new mobile telephone models are offered every three months from numerous manufacturers.

Also, mobile phone help people use them in several fields, such as, electronic trade, business and the market. Users can now watch movies, play video games, listen to music, and pay for goods and bills [1].

In recent years, mobile phones play a major role in facilitating communications. Phones calling have become audio and video instead of only audio, in addition, Short Message Service (SMS) and Multimedia Message Service (MMS).

### 1.1: Mobile Phone

A mobile phone is a device that can send and receive telephone calls via a radio link while moving around wide geographical area; it does so by connecting to the mobile network operated by mobile phone operator. It also has access to wireless Public Switched Telephone Network (PSTN), a type of the waves short analog or digital



telecommunications in which subscribers have a wireless connection from the mobile phone to relatively nearby the transmitter[2]. Figure (1.1) shows some type of mobile phones.



Figure (1.1): Some type of mobile phones.

The mobile devices have less memory and less processing power , but last developments in the field of telecommunications lead to an increase in processing power, memory size ,capability and computation of personal computer and provide the wireless network everywhere from around the world.

## 1.2: Mobile Phone and Wireless Communication

Mobile phones can be connected to wireless communications network by radio waves or satellite broadcast. Telecommunication networks are a collection of transmitters and receivers, and communications channels that send messages one to another. Some digital communications networks contain one or more routers working together to transfer the right information to the user. Analog communications network consists of one or more switches which establish a connection between two or more users, for both types of network; it may be necessary to amplify or recreate the signal when they are transported over long distances [3]. Figure (1.2) shows the wireless space.

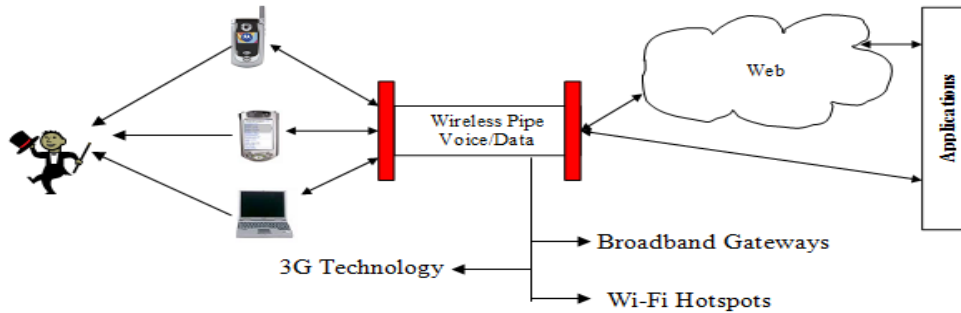


Figure (1. 2): The wireless space [3].

### 1.3: Mobile Phone Services

Most mobile phones provide services such as SMS, and MMS. New phones may also provide Internet services such as web browsing and e-mail [4]. In recent years, mobile networks have seen an increase in the use of astronomical SMS and MMS.

The SMS is a communications protocol allowing the interchange of short text messages between mobile telephone devices. The SMS can be said that more popularity data services on mobile networks at the present time, though originally bred as a mechanism to relay voice mail messages as a part of the Global System for Mobile Communications (GSM). Specification in 1992 evolved SMS to one of the wireless data services the most successful in recent years [5].

SMS allows users to exchange short messages with alphanumeric other users worldwide. The arisen SMS on mobile use modern telegraphy radio pagers memorandum radio using standardized protocols and specific phone later as parts of the GSM series communications criteria in 1985 as ways to send messages up to 160 characters to and from mobile phones GSM. The SMS way is connected to a number of characteristics that contributed to an increase in popularity. First support the device to send and receive SMS messages in almost everywhere, ranging from low-end mobile phones to the web interface phrases which are accessible via regular

Computers over the Internet. Second support plug and routing of SMS messages by most cellular networks throughout the world, and the consequent the contact form store and forward like e-mail messages, which do not ignore the message if you cannot receive immediately it by hand and alternatively are stored in the server interim and re-sent at a later date [6].

The MMS was evolved from the popularity of the SMS messaging system and uses the Wireless Application Protocol (WAP). WAP is a protocol that permits mobile devices to communicate with Internet servers via the mobile radio communications network.

The MMS is a standard for sending and receiving multimedia messages. The MMS can include any combination of formatted text, images, and photographs, audio and video clips. The images can be in any standard format such as GIF and JPEG. Video formats such as MPEG4 and audio formats such as MP3 and MIDI are also supported by MMS.

The MMS can be described as a new messaging framework seeking to fill the gap between mobile radio communication networks and the Internet. Users of mobile devices are sending messages to one another via mobile radio communications networks, and users connected to the Internet are communicating with one another via servers connected to the Internet using Simple Mail Transfer Protocol (SMTP) and email addresses [7].

#### **1.4: Mobile Phone and Steganography**

SMS and MMS is a way to send messages from one mobile to another. Steganography secures SMS or MMS, and it secures the exchange information. Without having privacy of information, there is no meaning of communicating using extremely high end technologies like SMS or MMS. This can be achieved by using Steganography, which is the process of hiding secret information inside some carrier. SMS and

MMS can be used as carriers for hiding information on mobile devices.

Steganography is a technology of hiding messages inside some carriers to shelter the communication so that the outsiders may not discover the existence of information in the carrier. This is the major distinction between Steganography and other methods of hidden exchange of information. For example, in cryptography method, people become aware of the existence of information by observing coded information, although they will be unable to comprehend the information. However, in Steganography, nobody will understand the existence of information in the resources. MMS Stenography is a combination of image and text Steganography. SMS is a combination of text and text Steganography; we can hide part of data in image and part of data in text [8].

### **1.5: Mobile Phone Security**

The development of digital devices and fast growth in wireless communications systems make mobile phone not merely a phone, but it is considered as a small computer. Can user from connect to the Internet, or display digital images, and play movies and music. It can be used as Automatic Transfer Money (ATM) or playing games, etc., make mobile susceptible to many security threats [9].

The extensive use of these systems increases the possibility of infiltration. Therefore, the security of information transmitted in these devices becomes a major issue for users and developers. Security threats in the mobile network are tapping a negative impact on data, cell phones are the following target for criminals and data to possess the most sensitive information are more vulnerable to attack [10]. Thus, we need to work in order to minimize both the loss of privacy and loss of information.

Security threats in the mobile network are ranging from tapping a negative impact on data theft; mobile phones are the following target for criminals and to possess the most sensitive information are more vulnerable to attack [10].

Thus, we need to work in order to minimize both the loss of privacy and loss of information. Steganography has been used to exchange information without intercepted by unwanted viewers.

In this research, we are trying to improve privacy and security to send subtle messages through the merge process texts or text in image which is common on mobile phones; it is not a magnet for hackers to attack the message.

### **1.6: Steganography**

Steganography is the art and science of communication invisible, through information hiding in other information, and thus hides the existence of the information communicated. Derived from the word hide information "stegos" Greek words meaning "cover" and "grafia" meaning "writing" identify as "writing covered" [11].

Steganography is the art and science of writing hidden messages in such away that no one regardless of sender and the intended receiver doubted in the presence the message, a form of security through obscurity.

The advantage of Steganography, over cryptography alone, is that messages do not attract attention to themselves, plainly visible encrypted messages—no matter how unbreakable—will arouse suspicion, and may in them be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, Steganography can be said to protect both messages and communicating parties.

Steganography includes too the hiding of information within computer files. In digital Steganography, electronic communications may include Steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for Steganographic transmission because of their large size [12].

## 1.7: Types of Steganography

The different types of Steganography techniques that are available are [13]:

Pure Steganography.

Public key Steganography.

Secret key Steganography.

**Pure Steganography:** is the process of embedding the data into the object without using any private keys. This type of Steganography entirely depends upon the secrecy. This type of Steganography uses a cover image in which data is to be embedded (to embed the message into image) as shown in Figure (1.3).

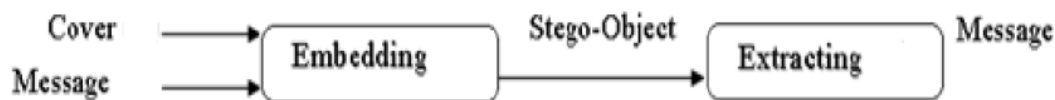


Figure (1. 3): Pure Steganography process [13].

These types of Steganography can't provide strong security because it is easy for extracting the message if the unauthorized person knows the embedding method. It has one advantage that it reduces the difficulty in key sharing.

**Secret key Steganography:** is another process of Steganography which uses the same procedure other than using secure keys. It uses the individual key for embedding the data into the object which is similar to symmetric key. For decryption, it uses the same key which is used for encryption as shown in Figure (1.4).

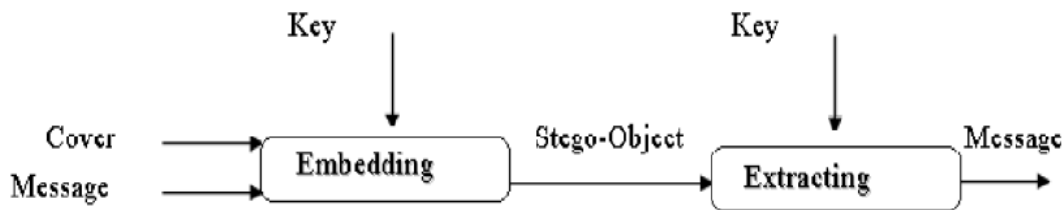


Figure (1.4): Secret key Steganography [13].

This type of Steganography provides better security compared to pure Steganography. The main problem of using this type of Steganographic system is sharing the secret key. If the intruder knows the key it will be easier to decrypt and access original information.

**Public key Steganography:** uses two types of keys: one for encryption and another for decryption. The key used for encryption is a private key and for decryption is a public key and is stored in a public database [13] as shown in Figure (1.5).



Figure (1.5): Public key Steganography [13].

### 1.8: Categories of Steganography

Almost all digital file formats can be used for Steganography, but the formats that are more suitable are those with a high degree of redundancy.

Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display [14]. The redundant bits of an object are those bits that can be altered without the alteration being detected easily [15]. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding. Figure (1. 6) shows the four main categories of file formats that can be used for Steganography.

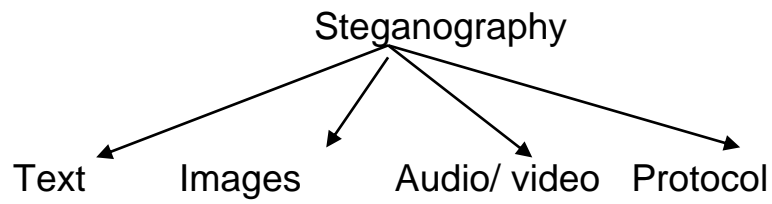


Figure (1. 6): Categories of Steganography.

### Text Steganography

Text Steganography, which is what this study specifically deals with, uses text as the medium in which to hide information. The definition of text Steganography remains broad in order to differentiate it from the more specific “linguistic Steganography”. Text Steganography can involve anything from changing the formatting of an existing text, to changing words within a text, to generating random character sequences or using context-free grammars to generate readable texts [16].

### Image Steganography

Image Steganography often involves hiding information in the naturally occurring “noise” or LSB within the image and provides a good illustration for such techniques; most kinds of information contain some



kind of noise. Noise can be described as unwanted distortion of information within the signal. Within an audio signal, the concept of noise is obvious. For images, however, noise generally refers to the imperfections inherent in the process of rendering an analog picture as a digital image [17].

## Audio and Video Steganography

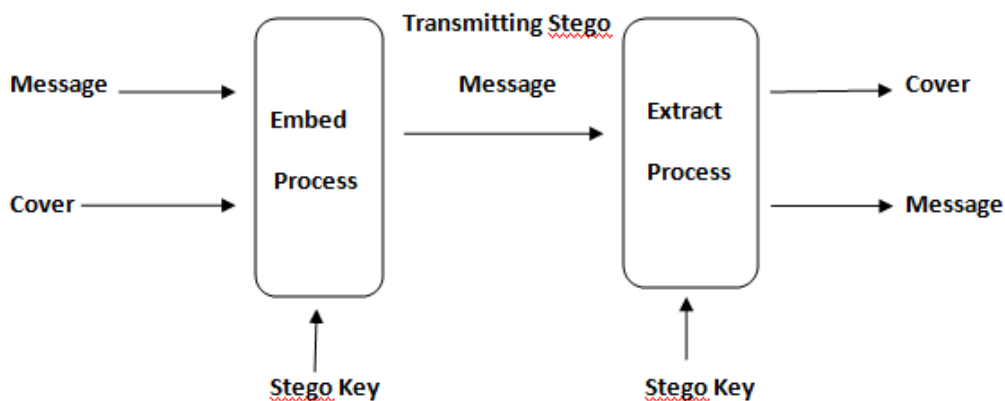
In audio Steganography, secret message is embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio file [18].

### Protocol Steganography

The term protocol Steganography refers to the technique of embedding information within messages and network control protocols used in network transmission. In the layers of the OSI network model, there exist covert channels where Steganography can be used. An example of where information can be hidden is in the header of a TCP/IP packet in some fields that are either optional or are never used [11].

### 1.9: The Information-Hiding Process in a Steganography System

The information-hiding process in a Steganography system begins by identifying a cover medium; the embedding process creates a stego medium by hiding secret data in cover medium [19]. Figure (1.7) shows the main steps of Steganography.



## Figure (1.7): Steps of Steganography.

As a consequence of all the developments that took place in the field of telecommunications and provided the wireless network everywhere from around the world which increased the importance of mobile for increased portability, as large size memory; large process power and internet browsing, declining costs and added value-added services, this services help users in their everyday life and them use it in many fields such as, electronic trade, business and the market.

Also, it is used in the e-commerce, e-government, financial payment, and other business applications and banking as ATM, it is also used in many fields such as medicine, engineering, science, and transactions business and shopping from around the world, as well as a large expansion of the role of financial transactions between users mobile. Users now can watch movies, play video games, and listen to music, pay for goods and bills by using mobile device.

### **1.10: Steganography Classification of Techniques**

There are many methods to classify Steganography systems, which are classified according to the cover used in secret communication and according to cover mutations applied in the process of embedding. Steganography techniques as follows [20]:

Substitution systems: replaces additional parts of the cover letter secret.

Transform domain techniques: includes confidential information in a vacuum signal conversion.

Spread spectrum techniques: apply ideas from spread spectrum.

Statistical methods: encode information by changing the properties of several statistical cover and the use of hypotheses examined in the process of reclamation

Distortion techniques: store information by noise signal and measuring the deviation from the original cover in a move to open codec.

Cover generation methods: symbol information in the manner in which they are configured to cover a confidential communication [20].

### **1.11: The Statement of Problem**

Mobile phones are considered from the most common communication devices recently and vulnerable to unauthorized access and invade privacy and security. This will cause a big problem that threat privacy and security, and the all security threats existing in mobile phone network could range from passively eavesdropping to stealing data thus threatening the privacy and security of messages and all risk associated with the sensitive information. That will make users need to work towards minimizing both privacy loss and information loss and improve the privacy and security during the send and receive messages.

We suggested the Steganography software for mobile application, are trying to send hidden secret messages through embedding in (image or text) and send secret messages to many users, and it is possible to extract directly the hidden message by the receiver. In the proposed work three algorithms will be used to hide the secret message inside stego covers

### **1.12 Contribution**

In the recent years, mobile phones play a major role in facilitating communications because the recent development that has operated on mobile phones such as large size memory, large process power and internet browsing, makes people use them in several field such as, electronic trade, business and the market, and all electronic trading via mobiles done through sending messages to server which responds to the user by messages, and issuing Internet Protocol Version 6 (IPV6) that increased from the importance of the mobile, but all services are vulnerable to unauthorized access and thus invading privacy and security.

For that, we propose some ways to protect sensitive information by hiding the message inside a message or a message inside image; this will increase security, privacy and integrity and give the users more confidence during the sending and receiving messages and protecting personal information.

### **1.13: Research Hypothesis**

We are trying to design identical software to the mobile phone system.

We assume that we use the same menu of the messages of the mobile phone.

We assume that we use three algorithms where the first simple object access protocol (SOAP) algorithm is used to hide the secret information dependence of to embedded secret information into cover message and generate Stego text (SMS). While the second Least Significant Bits (LSB) algorithm is used to embedded message inside cover image and generate Stego image (MMS) and three algorithms the Discrete Cosine Transform (DCT) algorithm are used in image compression. The other hand, the software has to be able to extract the secret message from text directly and extract the secret message from image directly.

We are trying to minimize the amount of information moving between the sender and the recipient which increases the efficiency of the algorithm.

We are trying to protect the message against the destruction during the image processing.

### **1.14: Research Tools**

The implementation of algorithms for hiding information will be done using J2ME (Java 2 Micro Edition) programming language to work in mobile phones.

The following are among the tools used in search three algorithms; first simple object access protocol (SOAP) algorithm used to hide information dependence of lightweight protocol uses XML technologies to define a messaging framework; the second is Least Significant Bits (LSB) algorithm used to hide information into digital image; and the third is the Discrete Cosine Transform (DCT) algorithm used in JPEG compression.

### **Hide secret information used simple object access protocol (SOAP) algorithm**

The SOAP protocol is designed to enable the exchange of structured information (i.e. SOAP messages) over a variety of underlying protocols in decentralized and distributed environments. This lightweight protocol uses XML technologies to define a messaging framework that is independent of any specific programming languages or implementation semantics [22].

A SOAP message is an XML document, which mainly consists of an envelope, a header, a body and fault elements. The “Envelope” is the root element that defines the XML document as a SOAP message. Also, it indicates the start and the end of the message. Application specific information (like security, reliability, etc) is usually defined within the optional “Header” element. Additionally, headers may contain commands to SOAP processors either to understand these headers or to reject the SOAP message. However, the actual data is defined within the required “Body” element. Thus, mandatory information that must be delivered to the intended recipient should be included within the body part of SOAP message. The optional “Fault” element is used to identify error messages. If an error occurs during SOAP processing, a SOAP fault element will be emerge in the body of the message.

Hiding secret information in a SOAP message means that the object that is used to transfer the secret message is the communication protocol itself that controls the actual data path over a network instead of using the actual data itself as a cover. This idea can overcome many of the trammels that the conventional Steganography techniques faced. In addition, a secret piece of information can be divided into multiple smaller messages and transmitted over several SOAP messages to overcome the size limitation as well[23].

**Process embedding secret information in SOAP message, the process of hiding a secret message within SOAP consists of the following six steps as follows**

Capture the SOAP message after its serialization.

Analyzing its contents to identify all the elements with contents that can be rearranged to determine if the SOAP message is suitable for embedding (i.e. has elements with contents that can be rearranged).

Calculating the number of elements that can be used to hide data (N).

Permuting every set of sub-elements to reflect a status of a symbol from the secret message.

If all the symbols of the secret message can be hidden in one SOAP message (the number of available seats N is greater than the length of the secret message M), then the sub-elements of the set M+1 will be rearranged to indicate the end of secret message.

Otherwise, if  $M > N$ , only a part of the secret message is sent in this SOAP message and the last set of sub-elements is rearranged to indicate that more hidden data are to arrive within the next received SOAP message[23].

**Process extract secret information from SOAP message, the process of extract a secret message from SOAP consists of the following five steps as follows**

The receiver, on the other hand extracts hidden information by analyzing the contents of each eligible element using same algorithm approach reverse (extract) reveal the hidden symbol, capturing the SOAP message, and checking its validity and capability to be a stego SOAP message.

Calculating the number of elements that might be used for data hiding (N).

Extracting the hidden symbols by analyzing the sub-elements order of each element in the stego SOAP message.

Stop the process either if the extracted symbol indicates that the message is not a stego SOAP or if the extracted symbol means “end of message”.

If the extracted symbol means "to continue", a new SOAP message has to be captured and analyzed.

Otherwise, the next symbol will be extracted and so on until we get the entire secret message embedded [23].

### **Hide secret information used the Least Significant Bits "LSB" Algorithm**

The LSB as one of the Steganography techniques, the simplest Steganographic techniques embed the bits of the message directly into least significant bit plane of the cover-image in a deterministic sequence [24].

## **Process embedding and extracting secret information into digital image used LSB algorithm**

Hiding secret information involves embedding the message in to the digital image. Each pixel typically has three numbers associated with it, each one for red, green, and blue intensities, and these values often range from 0-255. In order to hide the message information, is first converted into byte format and stored in a byte array. The message embeds each bit into the LSB position of each pixel position. The LSB of each 8bit byte has been co-opted to hide a text message; it uses the first pixel (at spot 0) to hide the length of message the (number of characters) [25].

The embedding process consists of choosing a subset  $\{j_1, \dots, j_i(m)\}$  of cover elements and performing the substitution operation  $LSB(C_{j_i}) = m_i$  ( $m_i$  can be either 1 or 0). One can also change more than one bit of the cover-element – for example by storing two message bits in the two least significant bits of one cover element.

In the extraction process, the LSB of the selected cover-elements are extracted and used to reconstruct the secret message. This can be done by extract the pixels of output image in one array, decoding in same manner as the reversal of encoding process i.e. first pixel value gives number of character in the message [26].

## **The Discrete Cosine Transform (DCT) algorithm used in JPEG compression**

DCT coefficients are used for JPEG compression. It separates the image into parts of differing importance. It transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into high, middle and low frequency components, as shown in Figure (1.8).



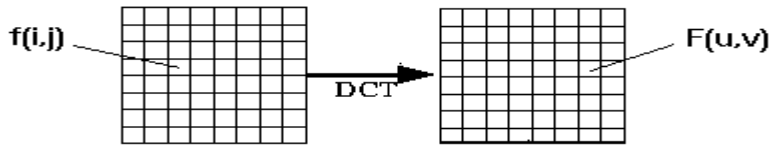


Figure (1.8): Discrete cosine transform of an image.

### DCT Encoding

The general equation for a 1D (N data items) DCT is defined by the following equation:

$$C(u) = a(u) \sum_{x=0}^{N-1} f(x) \cos[(2x + 1)u\pi/2N] \dots \dots \dots (1)$$

For u=0, 1, 2,....., N-1

The general equation for a 2D (N by M image) DCT is defined by the following equation:

$$C(u,v) = a(u)a(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) \cos[(2x + 1)u\pi/2N] \cos[(2y + 1)v\pi/2N] \dots \dots \dots (2)$$

For u, v=0, 1, 2,....., N-1

Here, the input image is of size N X M. c (i, j) is the intensity of the pixel in row i and column j; C (u, v) is the DCT coefficient in row u and column v of the DCT matrix. Signal energy lies at low frequency in image; it appears in the upper left corner of the DCT. Compression can be achieved since the lower right values represent higher frequencies and generally small enough to be neglected with little visible distortion. DCT is used in Steganography as- Image is broken into 8x8 blocks of pixels. Working from left to right, top to bottom, the DCT is applied to each block; each block is compressed through quantization table to scale the DCT coefficients, and the message is embedded in DCT coefficients [27].

### **1.15: Thesis Organization**

In this thesis, the background on mobile and literature reviews survey will be discussed in chapter two. The proposed system design for Steganography in mobile application software will be shown in chapter three. Chapter four contains the implementation of the proposed Steganography system in mobile application. The results of the implemented system will be shown in chapter four. The conclusion and future works will be given in chapter five.

## Chapter Two Literature Review

### Background on Mobile and Literature Survey

#### 2.1. Introduction

A mobile phone is not only a phone but also a small and portable computer. We can contact the Internet; it can be used as electronic trade and all transactions business and banking as ATM. More over through mobile we can reserve tickets and shopping. Users now can watch movies, play video games, and listen to music, pay for goods and bills, produce or show digital images, generate and play movies and music, etc. Mobile phone has the feature to send and receive messages safely through Bluetooth but that is not enough; and can be tapped because many hackers and intruders try to attack mobile phones and the security threats. The extensive use of these systems increases the possibility of the intrusion. Therefore, the security of the information transferred into these devices has become a major issue for users and developers to protecting the information by using Steganography [8].

Steganography, in today's electronic era, is the ability of hiding information in redundant bits of any unremarkable cover media, so nobody notice the existence of the secret information. Its objective is to keep the secret message undetectable without destroying the cover media. Steganography replaces unneeded bits in image, sound, and text files with secret information [19].

## 2.2. Literature Reviews

We provide a review of references that were used to conduct this study.

**Fabien**, et al, 1999 [28] proposed information hiding techniques that recently becomes important in a number of application areas. This technique contains a hidden copyright notice or serial number or even helps to prevent unauthorized copying directly. Military communications systems make increasing use of traffic security techniques which, rather than merely concealing the content of a message using encryption, seek to conceal its sender, its receiver, or its very existence. Similar techniques are used in some mobile phone systems and schemes proposed for digital elections. Criminals try to use whatever traffic security properties are provided intentionally or otherwise in the available communications systems.

**Lenti**, 2000 [29] suggested analyzed and tested several steganographic techniques on still images, and he shows embedding a large amount of data into the picture can by modify its visible properties , as well as compared to the RSA and the elliptic curve (ECC) based digital signatures, and we analyze their advantages and disadvantages in Steganography. In Steganography, it is important that the embedded data size should be minimized. Using ECC minimization of the embedded information is possible because the minimal block size is smaller than in the case of RSA.

In this paper several techniques are discussed, how to embed information in still images, and what the possible requirements in data hiding are, and what kinds of attacks are possible against Steganographic methods. Some Steganographic software was tested, studied, and the visible changes caused by the embedding process and their resistance against distortions were analyzed. The author proposed the usage of Elliptic Curves instead of RSA because it is more efficient in case of Steganographic application, because of the small size of digital signatures and encrypted small messages using this technique.

**Shahreza**, 2004[9] suggested an improved method for hiding data in images or Steganography. This method is used for securing data transfer from a computer to mobile phones. In this method a message can hide in an image on a PC using a password. The user can download this image from the computer to his mobile phone. The decoder program running on his phone will extract the hidden information by a Java program. The decoder program was installed on a Nokia 6600 mobile phone and tested by posting the students' grades over it.

The paper introduced an improved method of hiding information in image for mobile phones; this method allows a secure transfer of information between a computer and a mobile phone. In this implementation students connect to the course web site via Internet with their Nokia 6600 mobile phone and get their grades. It can use other kind of wireless communication such as Bluetooth to transfer data between computer and mobile phone. This method can be extended to hide data into video clips and sound clips that are common on new mobile phones.

**Chandramouli**, et al, 2004 [30] presented some general concepts and ideas that apply to Steganography and Steganalysis. Specifically are establishing framework and define notion of security for a Steganographic system. They are show how conventional definitions do not really adequately cover image Steganography and provide alternate definition. We also review some of the more recent image Steganography and Steganalysis techniques.

Such techniques essentially design a classifier based on a training set of cover-objects and stego-objects arrived at from a variety of different algorithms. Classification is done based on some inherent "features" of typical natural images which can get violated when an image undergoes some embedding process. Hence, designing a feature classification based universal Steganalysis technique consists of tackling two independent problems.

The first is to find and calculate features which are able to capture statistical changes introduced in the image after the embedding process. The second is coming up with a strong classification algorithm which is able to maximize the distinction captured by the features and achieve high classification accuracy. Typically, a good feature should be accurate, consistent and monotonic in capturing statistical signatures left by the embedding process. Prediction accuracy can be interpreted as the ability of the measure to detect the presence of a hidden message with minimum error on average. Similarly, prediction monotonicity signifies that the features should ideally be monotonic in their relationship to the embedded message size. Finally, prediction consistency relates to the feature's ability to provide consistently accurate predictions for a large set of Steganography techniques and image types. This implies that the feature should be independent on the type and variety of images supplied to it.

Paper reviewed some fundamental notions related to Steganography using image media, including security; they also described in detail a number of Steganalysis techniques that are representative of the different approaches that have been taken.

**Balan**, 2007 [21] suggested a Steganography method which is one of the

means of securing files, it allows one to hide files inside another file, through the design of STEALTH software. STEALTH: is file security for a mobile device is software that gives the intended users some option on how to secure their files. This software was developed using Microsoft .Net Framework, and C# as a tool for coding. It will run on mobile devices with windows- based operating system.

This study aimed to develop Steganography software that will run on mobile devices. Specifically, the study is able to design a file security for mobile devices, a program that implements Steganography,

is a very useful tool in embedding sensitive information in images and music. Research on Steganography becomes widely known today. It has to continue on growing and being enhanced to manage the increasing demand for security as the technology advances.

The application implements its main objective, which is to develop Steganography software that will run on mobile devices with windows-based operating system. This brought to a conclusion that steganography can demonstrate both reliability and portability at the same time. This also shows that Steganography applications can be further enhanced when used concurrently with other technologies. Another objective is to determine the file sizes that a definite cover file can accommodate. As a result, the researchers were able to arrive to a tangible conclusion that valid file sizes are ascertained through constant testing and iteration, and the developed system was tested and evaluated; and the results were documented. These were also included in the objectives of the study, which can be considered as successfully accomplished. There are many ways where Steganography can be applied. One is through integration of existing and new systems, which also means improving the application of Steganography in the industry.

**Soram**,2009 [31] proposed a system to prevent the security loopholes in SMS banking has been investigating and proposes a system to make mobile SMS banking secure using Elliptic Curve Cryptosystem (ECC), Also, another aim is to design an API to implement ECC algorithm.

This paper is study to mobile SMS banking security by means of elliptic curve cryptographic technique. Approaches based solely on data encryption provide a security that depends on the place encryption/decryption is actually performed. As the security of the proposed system is very hard, it is very clear that the proposed mobile SMS banking will dominate banking sector in India. It has been mentioned in many literatures that a considerably smaller key size can

be used for ECC compared to RSA. Also mathematical calculations required by elliptic curve cryptosystem are easier, hence, require a low calculation power. Therefore ECC is a more appropriate cryptosystem to be used on small devices like mobile phones. An API has been developed that implements ECC, allowing it to be used in banking sectors.

**Kumar and Yadav**, 2009 [32] proposed a method of hiding the data in mobile devices from being compromised. They use two level data hiding technique, where in its first level data is encrypted and stored in special records and the second level being a typical password protection scheme. The second level is for secure access of information from the device.

In the first level, encryption of the data is done using the location coordinates as key. Location Coordinates are rounded up figures of longitude and latitude information.

In the second phase the password entry differs from conventional schemes. They have used the patterns of traditional Angola for the specifying password and gaining access, thus minimizing the chances of data leak in hostile situations. In this paper, the suggested method a new data hiding technique for information on mobile devices is presented. This technique imposes a two level data hiding mechanism, where in the first level implements the storing techniques and the second level implements the accessing mechanisms.

The use of a predefined pattern for password entry will enhance the security of data in case of device theft or during hostile situations and the use of multiple records for saving the parts of a message protects the data from being stolen in case of device being hacked.

**Singh and Agarwal**, 2010[25] proposed technology to generate cross-platform that can effectively hide a message within a digital image file. Image is a mix of multiple pixels and every pixel has three numbers and color image consists up of millions of numbers. And thereby the



change in a low numbers the resulting color image that perhaps will look lots like the original image. This technique, which works by changing color pixel low value; and will be used in terms of value select pixels to represent characters instead of the color value. Obviously that the image still sounds mostly output as the original but some points seemed a little place if we look closely. Their results to create a cross-platform that can effectively hide a message within a digital image file. There are also many applications such as image hide information that allow the parties to communicate secretly and in secret.

**Jagdale**, et al, 2010 [33] proposed a method which is using steganography, which is the process of hiding secret information inside some carrier. SMS and MMS can be used as carriers for hiding information on mobile devices. For insisting more security, encrypted data will be hidden inside MMS. As the mobile devices have less memory and less processing power, we cannot use computation intensive encryption algorithms like AES, DES, and RSA. Elliptic Curve Cryptography (ECC) is emerging as an attractive alternative to traditional public-key cryptosystems.

ECC offers equivalent security with smaller key sizes resulting in faster computations, lower power consumption, as well as memory and bandwidth savings, in this paper; they are proposing method of encrypting text with ECC and then hiding encrypted text in MMS. SMS are limited to 160 character messages while MMS has no size limit. The biggest use of MMS is likely to be for companies for sending MMS messages to subscribers, enquirers or customers or for banks for sending secret information like PINS/Passwords etc. The computational burden of ECC can be minimized by executing ECC with multiple threads.

**Bachar**, et al, 2011[23] proposed a method to discuss and analyze a number of Steganography studies in text, XML as well as SOAP messages. Also, they proposed a novel Steganography method to be used for SOAP messages within web services environments.

The method is based on rearranging the order of specific XML elements according to a secret message. This method has a high imperceptibility; it leaves almost no trail because of using the communication protocol as a cover medium, and it keeps the structure and size of the SOAP message intact.

This method monitors a SOAP message just after its serialization in the sender endpoint and before it is sent. It analyzes the SOAP elements and embeds a secret message accordingly by rearranging the order of the contents and attributes of specific elements in a SOAP message, where every permutation represents a specific symbol according to a secret key shared between the sender and the receiver. As a result, the provided method has a high resistance against detection since it uses the communication protocol as a cover medium rather than the traditional digital files. The stego SOAP message has the same size of the original message; the method is tested and validated using a feasible scenario so as to demonstrate its utility and applicability. But the disadvantages of this method, anyone on the Internet can intercept the data transmitted between different sites. Thus, distributed applications require higher security levels than internal applications [29].

**Kiah, et al**, 2011[34] implemented a non-server (that is, P2P), architecture public key cryptography to secure the mobile communications. The proposed implementation of public key cryptography can provide confidentiality, authentication, the safety and non-repudiate security services needed for mobile communication. Compared with the server based architecture, the non-server based architecture has lower risk and the security has been improved, to avoid many kinds of attacks.

They discussed the impact of implementing public key cryptography on the non-server architecture and public key cryptography implementation for non-server architecture mobile security system has been proposed. NTRU algorithm is selected for public key cryptography implementation.

The results for NTRU tests on real equipment have been presented. The proposed solution security and the potential risks have been discussed.

**Kumar**, et al, 2011[35] proposed technology through the use of Cryptography and Steganography to secure information via mobile phone in the MMS; it is very common to hide data in the LSB of pixels. Spatial and frequency domains are generally used for image processing. Spatial domain has many accounts relatively frequency domain. But they are use the Discrete Cosine Transform (DCT) for image steganography and tiny encryption algorithm for cryptography. Tiny Encryption Algorithm (TEA) is block cipher algorithm. It is simple and fast but best for mobile application.

Previously Steganography was implemented for Steganography in MMS using JPEG over mobile communication. It is too much secure because data which has to be hiding is encrypted first than embed in to message in both text as well as image. We can also develop the algorithm using wavelet transformation.

**Wesam S Bhaya**, 2011 [35] propose a method to hide information (0, 1) in a cover SMS message by changing the fonts of each character by one of those two fonts (0 represented the system font and 1 represented by proportional fonts). After embedding secret information in a cover message and the Stego message looks like a normal message, but each character is drawn in one of these fonts of similarity.

The proposed system can be defined as a secret key Steganography system. There is a secret key between sender and receiver. The represented stego key is by using two types of fonts in J2ME, for example "system and proportional ". Without knowing the stego key, receiver cannot extract the original message. The similarity between the stego text and cover text can be considered very well

### 2.3 The Proposed Work

From the literature reviews we can suggest a new method that proposed from the previous researchers in this field to develop a new application in the area of mobile phone. The advantages will be taken from their experiences and mix it with the work that will be suggested to help in solving the problem of transferred secure data.

All methods of information hiding techniques of the previous researches are successful but have from some drawbacks. The proposed software used in the mobile hide the secret messages into SMS and MMS covers, and they are appropriate for its memory capacity and the availability of mobile SMS and MMS techniques. The proposed software loading does not need an modification in mobile architectural and the software loading on any types mobiles that have the a property of the send messages (SMS, MMS) used software in all type of mobiles because it is for flexibility and easy capacity, and gives the users more confidence during the send and receive messages and protect personal information.

## Chapter Three

### The Developed System Design

#### 3.1. Introduction

As a consequence of the developments that took place in the field of Information and Communications Technology (ICT) and provided the wireless network everywhere from around the world, which increased importance of mobile for increased portability, as large size memory, large process power and Internet browsing, declining costs and added value-added services. These services help users in their everyday life and then use it in many fields such as, electronic trade, business and the market.

Modern mobile devices are some of the most technologically advanced devices that people use on a daily basis, and the current trends in mobile phone technology indicate that tasks achievable by mobile devices will soon exceed our imagination [37].

The use of mobile in all the above areas is through the exchange of messages (SMS, MMS) between the server and the clients, but this process needs to increase security and privacy during the exchange of these messages to minimize the threats that threatens the security and privacy for users. Therefore, the goal of this thesis is to develop new design for Steganography in mobile application software that will be able to improve the privacy and security. The implemented Steganography in mobile application software is very useful tool in embedding sensitive information in images or text.

This is done through the use of three algorithms, the first algorithm to hide the message inside the text and the second is to hide the message inside the image and the third is using double techniques (hiding the result in another image). The suggested methods will be used in data transmitted between mobiles. Due to the importance of mobile in daily life, it is valuable to protect its transmitted information.

### **3.2 The Developed Steganography Software Design on Mobile Application**

Steganography software for mobile application is designed upon using the mobile phone messaging architecture system; we use the same menu for the messages of the mobile phone (SMS, MMS) to send messages to one or more users, the developed Steganography software design for mobile application using J2ME language to hide information of covers (text, image).

The researcher takes into account that the developed design needs to meet the following requirements:

- The developed Steganography software for mobile application does not need a secret key between the parties connection (the sender and receiver) to send a secret messages.
- The Process of sending the secret messages is by using the same facility for mobile system short message peer-to-peer, and this allows us to send the message for one person or more, insert a new contact, or select as many as wanted from the stored names in the Mobile.
- The Selection of the covers for the two types (SMS, MMS) can be done in two ways, either through stored covers in mobile or by directly entering a new one.
- Extraction process is adversely embedding process, so it must contain the same algorithm in both of the sender and receiver mobile.
- The developed software loading does not need any modification in mobile architectural or in its software.

- Providing a high security as a result of the flexibility of the programming process and change continually.

The developed software design programming use J2ME, Figure (3. 1) displays the class diagram the life cycle of the developed design for software:

Software application for the Mobile Information Device Profile (MIDP) must be derived from a special class, MIDlet. The MIDlet class manages the life cycle of the application. It is located in the package javax.microedition.midlet. The application manager is responsible for managing the MIDlets' life cycle.

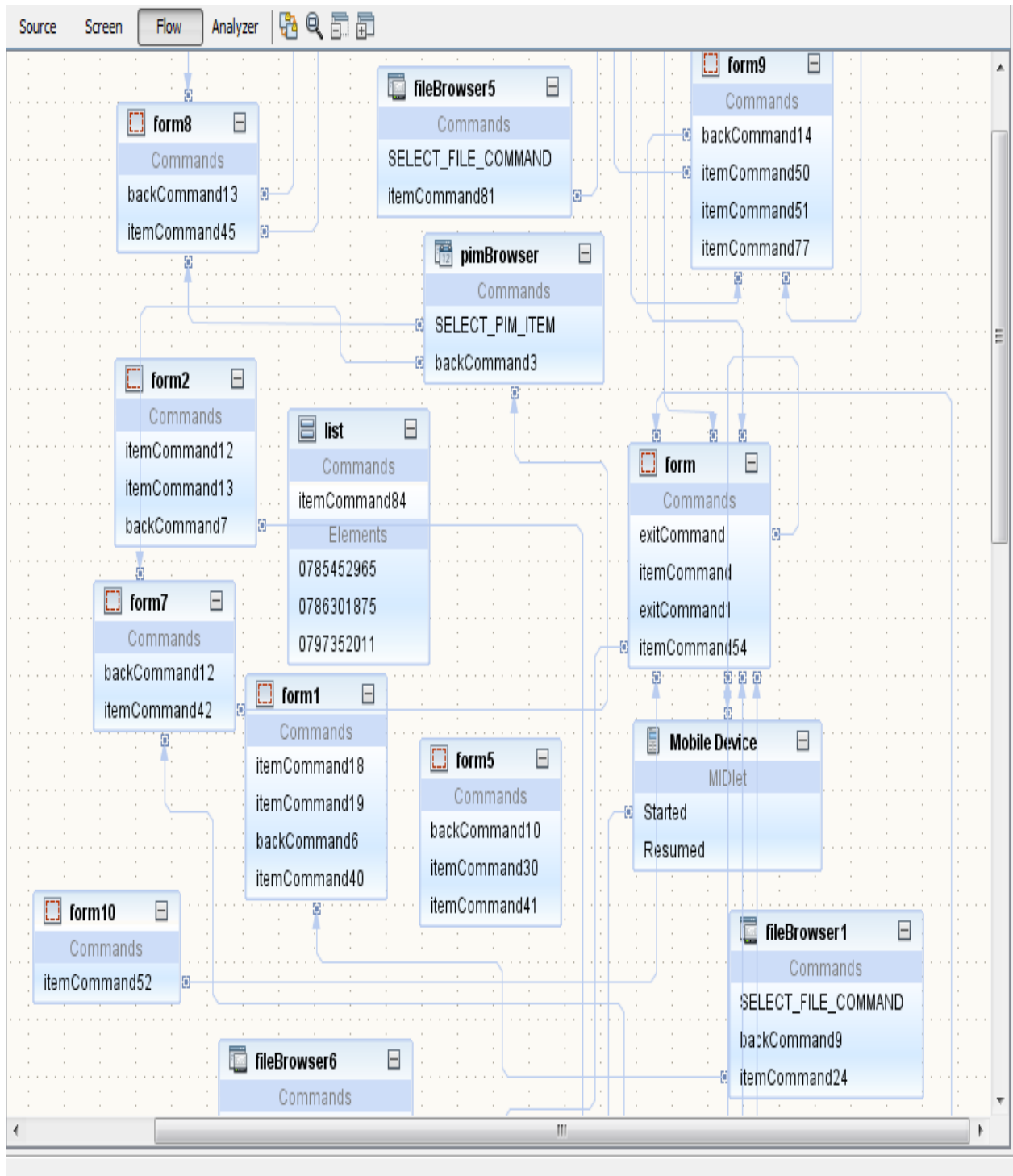


Figure (3.1): Class diagram of the developed software design programming.



For example, SMS form contains the following:

Text field called “secret text”: this textbox is used to write secret message and fill selected template.

Text field called “cover text”: this textbox used to select the cover text from existing template.

Select cover button: to embed the text message typically via SOAP messages.

Send button: to send result of embedding SMS.

**The System Activity Diagram is shown in Figure (3. 2)**

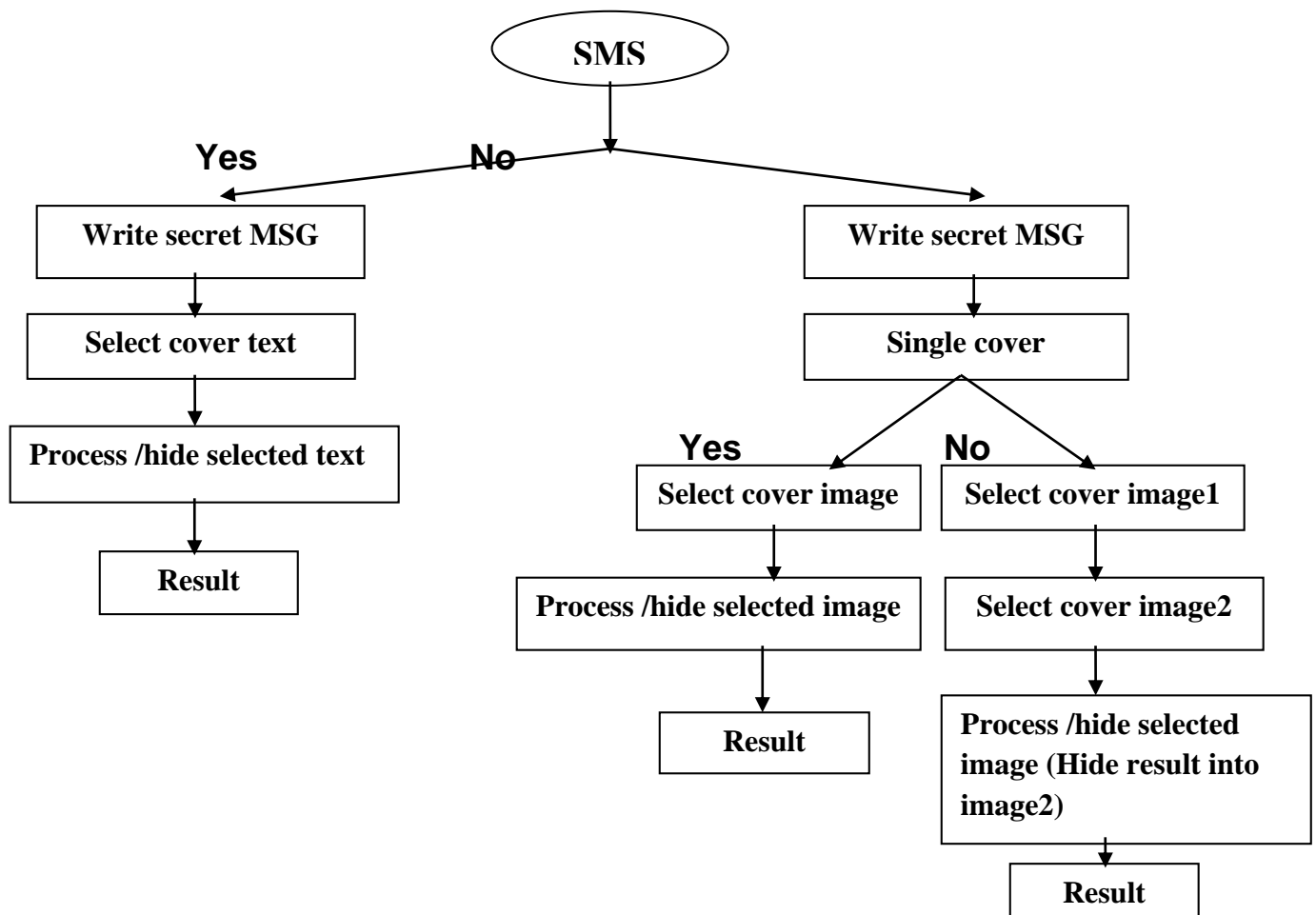


Figure (3.2): Activity diagram of the developed software design.

### 3.3 Project Environment (Net beans 7.0.2 “J2ME”)

Java ME is a collection of technologies and specifications that implementers and developers can choose from and combine to construct a complete Java runtime environment that closely fits the requirements of a particular range of devices and target markets [38].

J2ME is divided into configurations, profiles, and optional APIs, which provide specific information about APIs and different families of devices. A configuration is designed for a specific kind of device based on memory constraints and processor power. It specifies a Java Virtual Machine (JVM) that can be easily ported to devices supporting the configuration. It also specifies a strict subset of the Java 2 Platform, Standard Edition (J2SE) APIs that will be used on the platform, as well as additional APIs that may be necessary [39].

#### **Configurations**

Configurations are specifications that detail a virtual machine and a base set of class libraries which provide the necessary APIs that can be used with a certain class of device.

A configuration specifies a JVM and some set of core APIs for a specific family of devices. Currently, there are two: the Connected Device Configuration (CDC) and the Connected Limited Device Configuration (CLDC).

**The Connected Limited Device Configuration (CLDC):** Defines the base set of application programming interfaces and a virtual machine for resource constrained devices like mobile phones, pagers, and mainstream personal digital assistants.

When coupled with a profile such as the Mobile Information Device Profile (MIDP); it provides a solid Java platform for developing applications to run on devices with limited memory, processing power, and graphical capabilities.

**Connected Device Configuration (CDC):** Developed within the Java Community Process (JCP), it is a framework for using Java technology to build and deliver applications that can be shared across a range of network-connected consumer and embedded devices, including smart communicator's high-end personal digital assistants (PDAs), and set-top boxes.

## **J2ME Profiles**

Profiles complement a configuration by adding more specific APIs to make a complete runtime environment for running applications in a specific device category.

A profile is a set of higher-level APIs that further define the application life-cycle model, the user interface, persistent storage and access to device specific properties [38].

### **3.4 Steganography for Mobile Application Contents**

Focusing in design Steganography for mobile application contents on two menus to send the type of messages (SMS, MMS) as the following:

SMS\_ Menu.

MMS\_ Menu: That contain on (MMS\_ Single cover Menu, MMS\_Double cover Menu).

The Steganography software for mobile application contains on sender application "embedding" and receiver application "extracting ", both of senders and receiver applications exist in same device, and be exploited the same formats mobile application messages to send messages to more users.

### **3.5 SMS Menu**

In SMS service the user write secret message, and then selection of user to template or type cover message, then process to hide secret message into cover text.

SMS form (the sender application to embedding secret message) and contains the following objects:

Text field is called “secret text”: this textbox to write secret message and fill selected template.

Text field is called “cover text”: this textbox use to select the cover text from existing template.

Select cover button: to embedding the text message typically via SOAP messages.

Send button: to send result of embedding SMS.

SMS form (the receiver application to extracting secret message) and contains the following objects:

Text box called the result: to show original message after extracting.

Text box to show received message (embedding SMS).

Process button to extracting the secret message and return the (text).

### **Process to hide secret message into cover text “SMS”**

When the user wants to send message to destination environment she/he will browse the messages and select text cover.

Next step the user will insert secret message into text box.

The sender application will process the secret message and embedding into selected cover text via SOAP. See Figure (3. 3).

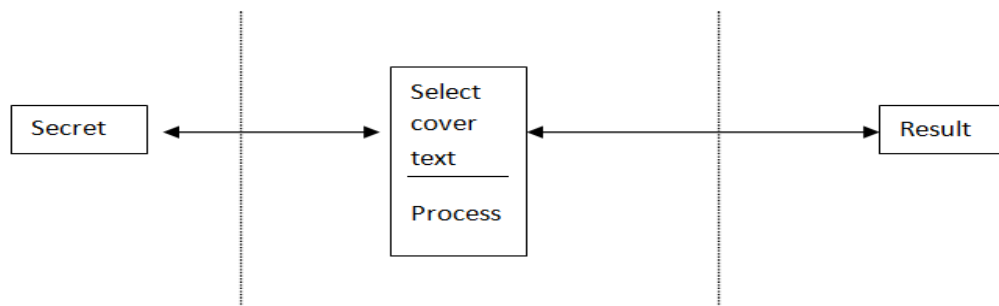


Fig (3. 3): Process send SMS message.

### 3.5.1 Process embedding secret information within SOAP consists of the following

Steps	Implementation	Remarks
N==number of bits	let N== number of bits	The number of available bits(N) to hide into cover
M==length of message	let M== length of secret message	Length secret message
I==number of elements	let I== Number of elements	Number of Characters
Text cover	<pre> for I   While     return the decimal     return the binary value   stop </pre>	Templates to text bix1 and convert cover message to concatenated binary string using the ASCII representation of the individual characters as the follow "01110111011101110"

Text secret	<pre> read M for i = 1 to M   Do     value for i   i+1 end while next </pre>	<pre> for While return the decimal return the binary stop </pre>	<p>Write into text box2, and convert text message to concatenated binary string using the ASCII representation of the individual characters as follows:</p> <pre> "000111000111000111 " </pre>
Divide the binary messages into 4 bits	<pre> read binary values for i for i = 1 to M   for s = 1 to 4     While i &lt;= M Do       get the first 4 ( binary value for i )     i+1   end while   stop next s next i </pre>	<pre> next s </pre>	<p>Converting text to binary divide the binary message into slice of size that match supported as "0111 0111011 1..." , "00011100 0111.."}</p>
Analyzing the content of secret and cover	<pre> for i=1 to 4 calculating the number of elements that can be used to hide data (N) next i </pre>	<pre> next </pre>	<p>Analyzing slices</p>
Determine first bit to hide	<p>let f The first bit to hide = "0" "ordering of the combination</p>		<p>Depends on analyzing method</p>

<p>Moving first character value to second value</p>	<p>for I = 1 to 4  moving first character value behind second next character value  I</p>	<p>Shifting values</p>
<p>if N&gt;M</p>	<p>if N&gt;M then  the end of secret message (stego-message)  else  save remaining value  repeat  if  end</p>	<p>Authentication for remaining values of secret message and the end of secret message, else part of the secret message is sent in this SOAP message and the last set of sub-elements will arrive within the next received SOAP message</p>

### 3.5.2 Process extracting secret information within SOAP consists of the following

Steps	implementation	Remarks
N==number of bits	let N== number of bits	The number of available bits(N) to hide into cover
M==length of message	let M== length of secret message	Length secret message
l==number of elements	let l== Number of elements	Number of Characters
Result	<pre> read M for l = 1 to M While i&lt;=M Do return the decimal value for l return the binary value for l l+1 end while  stop next l </pre>	Convert cover message to concatenated binary string using the ASCII representation of the individual characters as the follow "01110111011101110"



Divide the binary messages into 4 bits	<pre> read binary values for l = 1 to M for s = 1 to i&lt;=M While Do get the first 4 ( binary value for l ) l+1 end while stop next s l </pre>	<p>Converting text to binary</p> <p>divide the binary message into slice of size that match supported as "0111 0111011 1..." , "0001 11000111 ..."</p>
Analyzing the content of secret and cover	<pre> for l=1 to 4 calculating the number of elements that can be used to hide data (N) next l </pre>	Analyzing slices
Determine first bit to extract	let f The first bit to hide ="0"	Depends on analyzing method

Moving elements	for l = 1 to 4 character value behind next	moving second first character value	Extracting the hidden symbols by analyzing the sub-elements order of each element in the stego SOAP message
if N>M	if extracted symbol== stego SOAP then stop else end if	repeat	Authentication for remaining values of secret message and the end of secret message else a part of the secret message is sent in this SOAP message and the last set of sub-elements will arrive within the next received SOAP message set of sub-elements will arrive within the next received SOAP message

### 3.6 MMS Menu

In MMS service, the user writes a secret message (selection of the user to MMS single or MMS double): If selection of the user to MMS single cover, then the process to embedding secret message into selected cover image by “LSB” and information hiding using “DCT”, or if selection of the user to MMS double, are the process to embed secret message into selected cover image1 “LSB” and information hiding using “DCT” ,then result processed to embedding into image 2 using “LSB” and information hiding using “DCT”.

#### 3.6.1 MMS\_ Single Cover

MMS\_ single forms (the sender application to embedding secret message) and contains the following objects:

Text field called “secret text”: this textbox is to write secret message and fill selected template.

Image box “cover image”: this image use to select the cover image from existing folder.

Select cover: to embed the text message into cover image using LSB.

Send button: to send result of embedding MMS.

MMS\_ single form (the receiver application to extracting secret message) and contains the following objects:

Text box called the result: to show original message after extracting.

Image box to show received message (embedded message with cover1).

Process button to extracted the secret message and return them (text).

### 3.6.1.1 Process embedding secret information into digital image used LSB algorithm and DCT algorithm

Steps	Implementation	Remarks
N==number of bits	let N== number of bits	The number of available bits(N) to hide into cover
M==length of message	let M== length of secret message	Length secret message
l==number of elements	let l== Number of elements	Number of characters
s== number of pixels	let s== number of pixels	The number of variable pixels(s)

Image cover	For $l = 0$ to $M$ Arrange bits in a manner of placing the hidden bits before the pixel next $l$	Phone storage in image box and read pixels number $N$
Text secret	read $M$ for $l = 1$ to $M$ While $i \leq M$ Do return the decimal value for $l$ $l+1$ end while stop next $l$	Write into text box1, and convert text message to concatenated binary string using the ASCII representation of the individual characters as the follow "01110111011101110"
$Y=1$ 5	to convert characters to binary	Add value to characters

Embedding process	use two adjacent bits to hide one character ,get the 4 least significant bits alone , get the 4 upper significant bits alone , hide each character of secret message using two pixels	sender application
Read DCT	read DCT of image	DCT for image
set count of DCT	set count: = total bit to hide	DCT of image
Let X array	let X is array of bit to hide	Data to hide
Let A array	Let A is array of DCT coefficient	DCT array
Let n count	repeat n count =1,where 1 is initial value	Counter
Bit to hide	get bit to hide in text message from position x1,x2, x3	Secret bit
Remaining it in X	get remaining bit in array x from message bit	Authentication array X
n coefficient in A	get n coefficient in A array	Array A

m count==0	m bit count:=0	Count of A
Sum (m)	sum: = ((a [1] + a[3]) + x[1]) *1 )+ ( (a2 + a3) + x2) *2)	remaining in X
IF sum ==0	<pre> If (sum==0)then     change a[sum] bit in buffer else     change a[sum] bit in buffer end If count= n count +sum </pre>	X remaining value
m==m+2	m bit count= m bitcount+2	Remaining in X
Read next 2 bits	read next 2 bit in a array	Array A
IF m==count	<pre> If m bit count== count then     stop else     change a[sum] bit in buffer n count=n count sum end If </pre>	Count(m)

IF m==m +2	If m bit count=m bit count + 2 then in a array ; If m bit count == count then else repeat If	Count er       end
------------------	---	--

### 3.6.1.2 Process extracting secret information from digital image used LSB algorithm and DCT algorithm

Steps	Implementation	Remarks
Extracting result	reversing the process used to insert the secret message in the cover image	Received application
X=two adjacent pixels	shift the first pixel by 4 to right	Resulting image
Y=15	perform and operation with 15 to the second pixel	Add value to character
concatenation values	add the result of X and Y together and we get the character	Shifting pixel and added value
A array	starting from declaring a binary matrix having dimension, the first byte , till to the end byte, store the bits in the declared matrix	Binary matrix



compare result with cover	the final image is compared with the cover image to obtain the matrices	To declaring the matrix
number to matrix columns	the number of columns of the matrices gives the digits	Give number of digits
first digital serially in A	the digits are first serially obtained from those matrices which are placed 1 pixel apart. The digits for the next code are obtained from the matrices which are placed after 2 unchanged pixels	Placed 1 pixel apart
function $\varphi(p)$	the mathematical function $\varphi(p)$ is again used on the embedded code but with opposite mathematical operation to obtain the original number for the text, convert the numbers to obtain the original text	Used to extract original number for the text

### 3.6.2 MMS \_Double Cover

MMS \_double form (the sender application to embedding secret message) and contains the following objects:

Text field called “secret text”: this textbox is to write secret message and fill selected template.

Image box “cover image1”: this image is used to select the cover image from existing folder.

Image box “cover image2”: this image is used to select the cover image from existing folder.

Select cover 1: to embed the text message into cover image 1 using LSB.

Select cover 2: to embed the result of process button1 into cover image2 “LSB”.

Send button: to send result of embedding MMS.

MMS \_double form (the receiver application to extracting secret message) and contains the following objects:

Text box called the result: to show original message after extracting.

Image box to show received message (embedded message with cover2).

Image box to show received message (embedded message with cover1).

Process button to extracted the secret message and return them (text).

## Process to hide secret message into image covers “MMS”

When the user wants to send text message to destination environment she/he will browse the image folders and select image cover1.

Next step the user will insert secret message into text box.

The sender application will process the secret message and embedding into selected cover text using LSB.

If the user wants to get the message more privacy, she/he will browse the image folders and select image cover2.

The sender application will process the secret message and embed into selected cover text using LSB as in figure (3. 4).

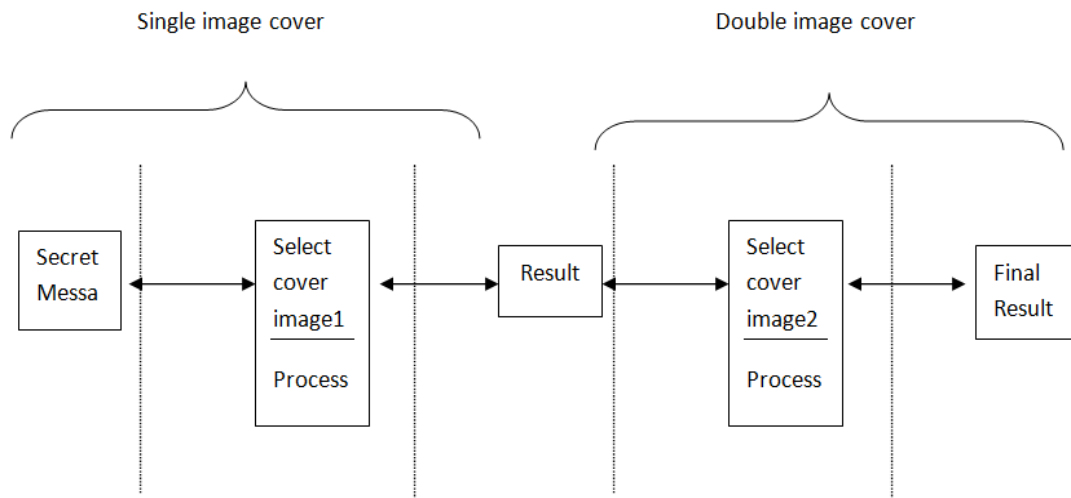


Figure (3. 4): Process send MMS message.

### 3.6.2.1 Process embedding secret information into two digital images used LSB algorithm and DCT algorithm

Steps	Implementation	Remarks
Image cover	the pixels are arranged in a manner of placing the hidden bits before the pixel of each cover image	Phone storage image box
Image cover	the pixels are arranged in a manner of placing the hidden bits before the pixel of each cover image	Phone storage image box
Text secret	convert each character of the secret message to decimal number	Write in text box

Y=15	to convert characters to binary	Add value to characters
Embedding process	use two adjacent bits to hide one character , get the 4 least significant bits alone , get the 4 upper significant bits alone , hide each character of secret message using two pixels	Single cover
substitute LSB with data	a few least significant bits (LSB) are substituted with in data to be hidden	LSB substitute
Let LSB substituted	let n LSBs be substituted in each pixel	LSBsubstituted (n)
Let d==pixel value	let d= decimal value of the pixel after the substitution	d== decimal value
Let d1 ==d(n)	let d1 = decimal value of last n bits of the pixel	d1= last n bits
Let d2==hidden d1	let d2 = decimal value of n bits hidden in that pixel	d2=hidden d1
If(d1~d2)<=(2^n)/2 then	no adjustment is made in that pixel If (d1<d2) → d=d-2^n Else If(d1>d2) → d=d+2^n	Determine adding pixels position to determine the columns to hide

Read DCT	read DCT of image	DCT for image
set count of DCT	set count: = total bit to hide	DCT of image
Let X array	let X is array of bit to hide	Data to hide
Let A array	Let A is array of DCT coefficient	DCT array
Let n count	repeat n count =1,where 1 is initial value	Counter
Bit to hide	get bit to hide in text message from position x1,x2, x3	Secret bit
Remaining it in X	get remaining bit in array x from message bit	Authentication array X
n coefficient in A	get n coefficient in A array	Array A
m count==0	m bit count:=0	Count of A
Sum (m)	sum: = ((a [1] + a[3]) + x[1]) *1 )+ ( (a2 + a3) + x2) *2)	Remaining in X
IF sum==0	If (sum==0)then , no change else change a[sum] bit in buffer n count= n count sum end If	X remaining value
m==m+2	m bit count= m bitcount+2	Remaining in X

Read next 2 bits	read next 2 bit in a array	Array A
IF m==count	If m bit count== count then stop else change a[sum] bit in buffer count=n count sum  end If	Count(m)
IF m==m+2	If m bit count=m bit count + 2 then read next 2 bit in a array ; If m bit count == count then else repeat to cover2 end If	Counter
Repeat	repeat DCT steps for cover2	

### 3.6.2.2 Process embedding secret information into two digital images used LSB algorithm and DCT algorithm

Steps	Implementation	Remarks
Extracting result	reversing the process used to insert the cover image in the cover image	Received application
(W,H)dimensions of the hidden image and the number of bits	dimensions of the hidden image(W,H), and the number of bits chosen to hide the image (k)	Resulting image
k==number of bits n==number of pixels	assuming that k {1, 2, 3, 4}, there are only (n <sup>2</sup> ) possible values, where n is the number of pixels in the image, making a brute force search feasible	To choose the hide the image
I(x,y)==the pixel value in I m==bits of the pixel value	I(x, y) is the pixel value in I at location (x, y), I <sub>m</sub> (x, y) denotes the lower m bits of the pixel value while I <sub>u</sub> (x, y) denotes the upper m bits of the pixel value	Pixel location



F is binary function Fx is binary function of x fy is binary function of y	$F_x(x, k) = \sum F_y(x, y, k)$ where f is binary function $f_y(y, k) = \sum F_x(x, y, k)$	Function to extract bits value and location
Read DCT	read DCT of image	DCT for image
set count of DCT	set count: = total bit to hide	DCT of image
Let X array	let X is array of bit to hide	Data to hide
Let A array	Let A is array of DCT coefficient	DCT array
Let n count	repeat n count =1, where 1 is initial value	Counter
Bit to hide	get bit to hide in text message from position x1,x2, x3	Secret bit
Remaining it in X	get remaining bit in array x from message bit	Authentication array X
n coefficient in A	get n coefficient in A array	Array A

m count==0	m bit count:=0	Count of A
Sum (m)	sum: = ((a [1] + a[3]) + x[1]) *1 )+ ( (a2 + a3) + x2) *2)	Remaining in X
IF sum==o	If (sum==0)then , no change else a[sum] bit in buffer n count sum end If change count= n	X remaining value
m==m+2	m bit count= m bitcount+2	Remaining in X
Read next 2 bits	read next 2 bit in a array	Array A
IF m==count	If m bit count== count then stop else a[sum] bit in buffer sum end If change n count=n count	Count(m)
IF m==m+2	If m bit count=m bit count + 2 then bit in a array ; read next 2 If m bit count == count then else repeat to cover2 end If	Counter

Extracting result	reversing the process used to insert the secret message in the cover image	Received application
X=two adjacent pixels	shift the first pixel by 4 to right	Resulting image
Y=15	perform an operation with 15 to the second pixel	Add value to character
concatenation values	add the result of X and Y together and we get the character	Shifting pixel and added value
A array	declare a binary matrix having dimension, starting from the first byte till to the end byte and store the bits in the declared matrix	Binary matrix
compare result with cover	the final image is compared with the cover image to obtain the matrices	To declaring the matrix
number to matrix columns	the number of columns of the matrices gives the digits	Give number of digits
first digit serially in A	the digits are first serially obtained from those matrices which are placed 1 pixel apart. The digits for the next code are obtained from the matrices which are placed after 2 unchanged pixels	Placed 1pixel apart
function $\phi(p)$	the mathematical function $\phi(p)$ is again used on the embedded code but with opposite mathematical operation to obtain the original number for the text and convert the numbers to obtain the original text	Used to extract original Number for the text

## Chapter four

### Results and Discussions

#### 4.1 Introduction

In this chapter the actual system (the Steganography software for mobile application) has been programmed using J2ME programming language for mobile devices that suggested for protecting security and privacy during the exchange of the secret messages between sender and receiver and the results will be discussed.

Design Steganography for mobile application contents on two main menus to send the type of messages (SMS, MMS) as the following:

SMS \_ MSG Menu.

MMS\_MSG Menu: are divided into (single cover, double cover).

Both two main menus included on the sender application "embedding" and the receiver application "extracting", both of sender and receiver applications are exist in same device, such as password between the sender and the receiver the secret messages.

In the developed software Steganography for mobile application we use the same facility of the messages in the mobile phone (SMS, MMS) to send messages to more users. The developed software enables the user to writing the message by using mobile keyboard and thus gains the advantage of the efficiency of mobile to send messages.

Steganography Software for Mobile Application Contents

(Steganography in mobile application) solution contains tow mine menu as the following:

## SMS\_MSG Menu.

MMS\_MSG Menu: are divided into (single cover, double cover).

### 4.2 SMS\_MGS Menu

Figure (4. 1) shows that the main menu will browse to Steganography in mobile phone application that contains two buttons SMS\_MSG, MMS\_MSG.

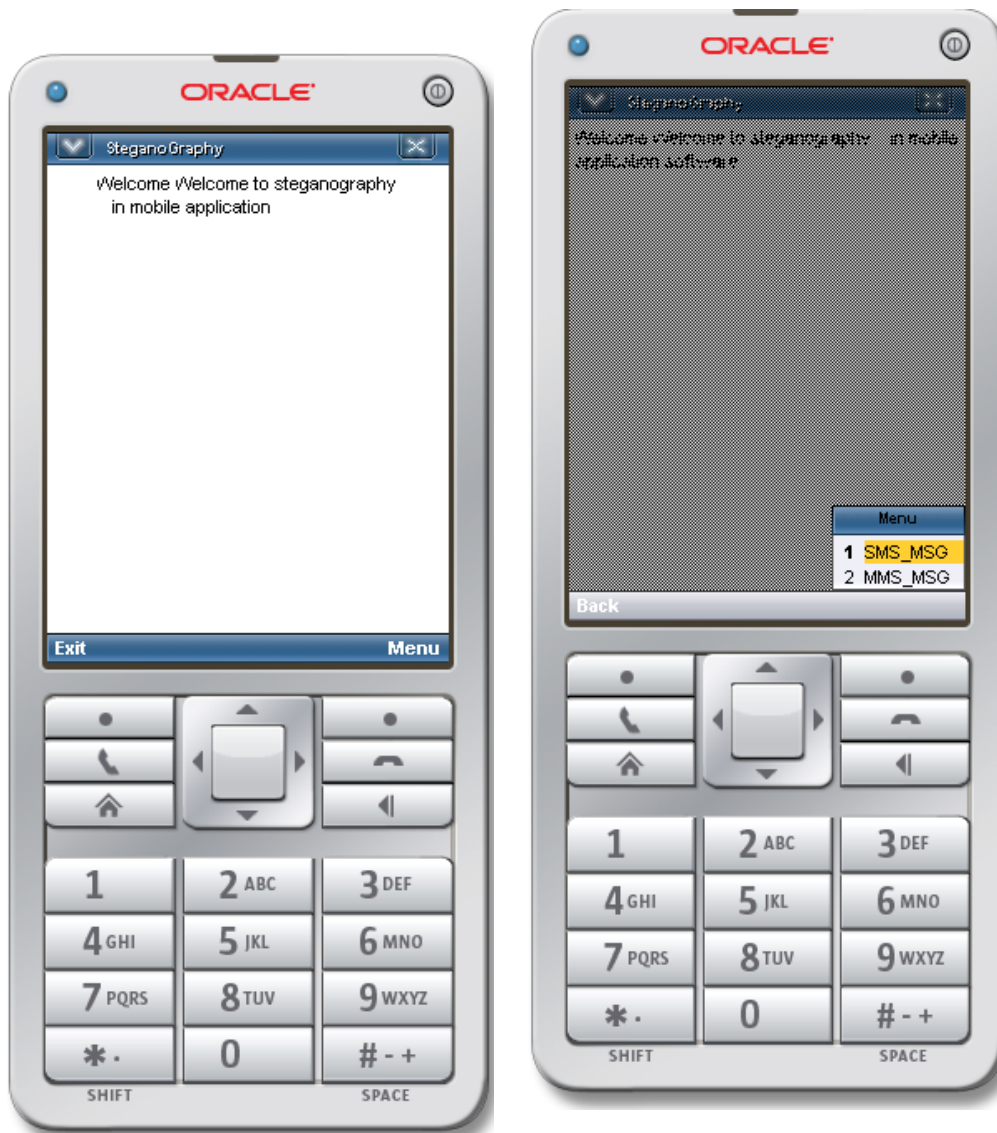


Figure (4. 1): Steganography in mobile application software and two main menus (SMS, MMS).

Figure (4. 2) shows the option user to SMS\_MSG menu: the selected senders to" select cover".

SMS sender form as the following:

Text field called "secret text": this textbox is to write secret message and fill selected template.

Text field called "cover text": this textbox is used to select the cover text from existing template.

Select cover button: to embedding the text message typically via SOAP messages.

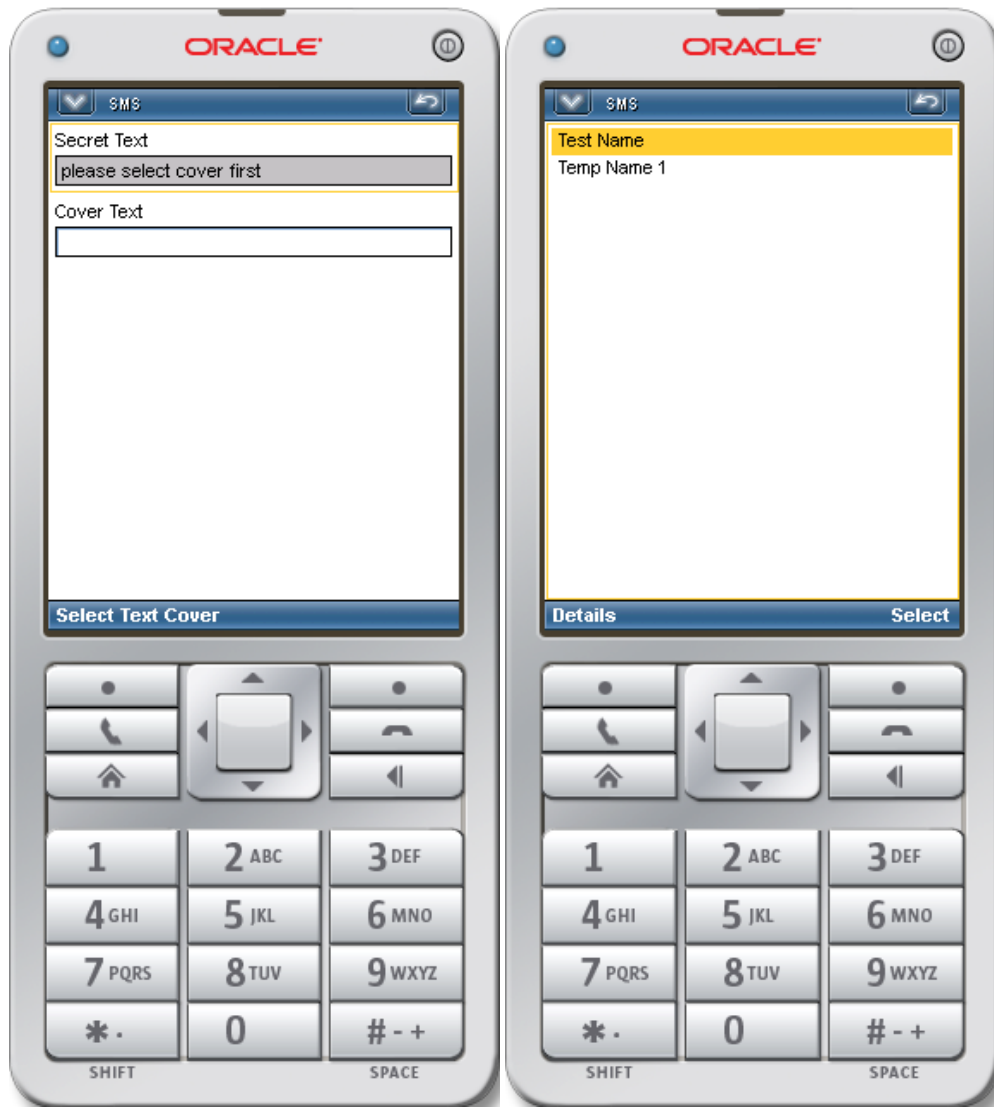


Figure (4.2): the sender select text covers SMS.

Figure (4.3) shows the sender selected to cover text "welcome to steganography".

The selected cover will be through a collection of covers that stored in a mobile device. The "welcome to steganography "cover is not the only one, but the sender can select another covers that stored in a mobile device, thereafter the sender be able to write the secret message such as (we are meeting today) and fill selected template.

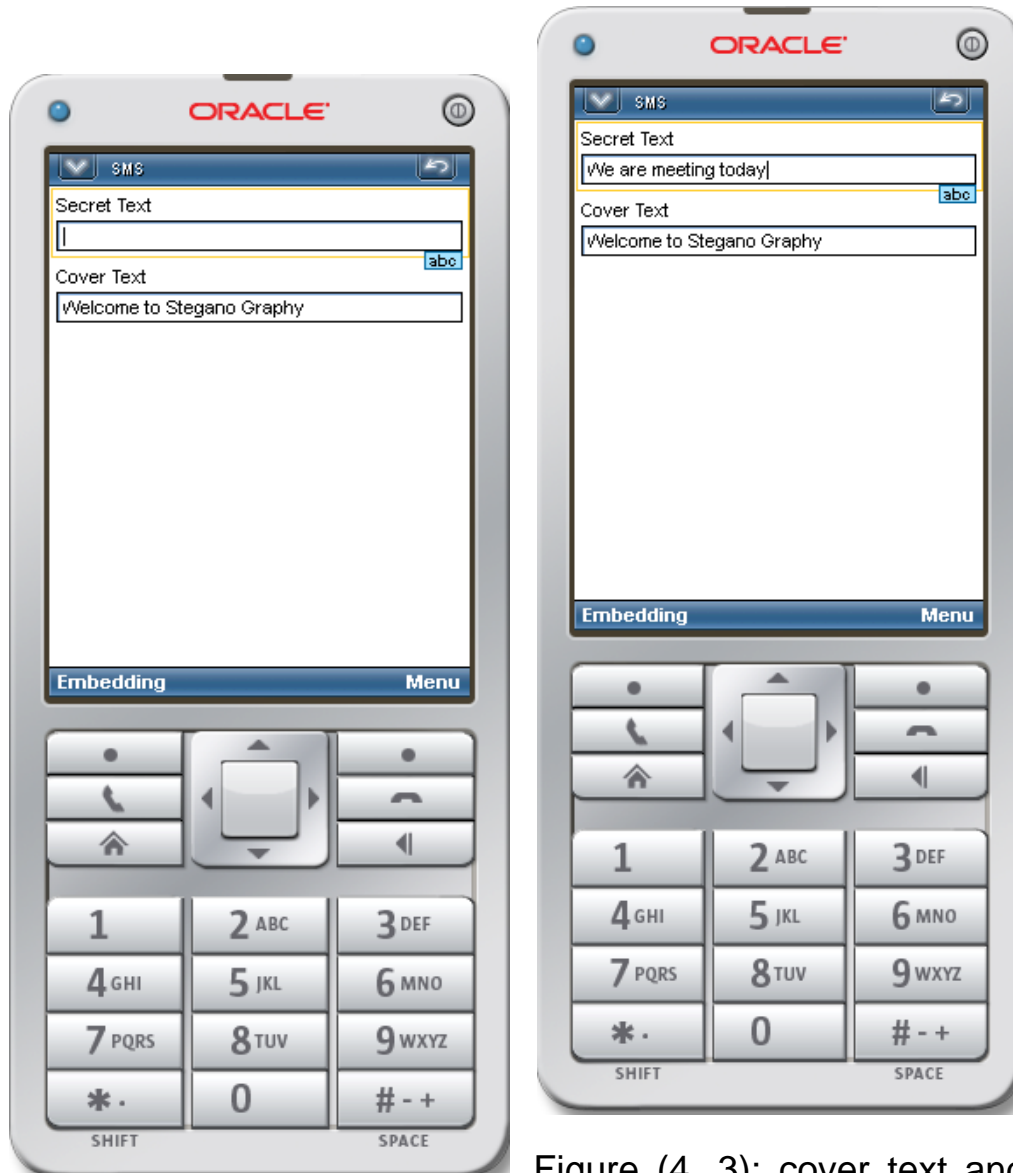


Figure (4. 3): cover text and the senders write the secret message.

The SMS screen contains the embedding option (process to embedding secret message inside text cover) and menu contains send option and another save option for by the sender, and finally the extract option for secret message by the receiver.

Figure (4. 4) shows selection of the sender to the embedding option (process to embedding the cover into secret message typically via SOAP messages), and its result.

This figure shows the result which contains the secret message inside the cover text and the selection of the sender to save option when the sender is unwilling to be sent to the receiver.







Figure (4. 4): process embedding and menu contains send and save options by the result.

Figure (4. 5) shows the saved result when the sender is unwilling to send the message to the receiver in mobile device, as well as the receiver can save the result that sent him. This means that the save option is available for both of sender and receiver.



Figure (4. 5): the option saves to save result in the mobile.

Figure (4. 6) shows the send option to help the sender to send the secret messages to one receiver or several receivers; Figure (4.6) shows the send process for the result to one receiver or several receivers.



Figure (4. 6): process sends to the result.

The result will be sent by using the same mobile system, and there is no need to complete the send process. The result is sent by mobile messaging system to one or several users.

Figure (4. 7) shows the arrival of result to the receiver followed by the process of extracting of the secret message.

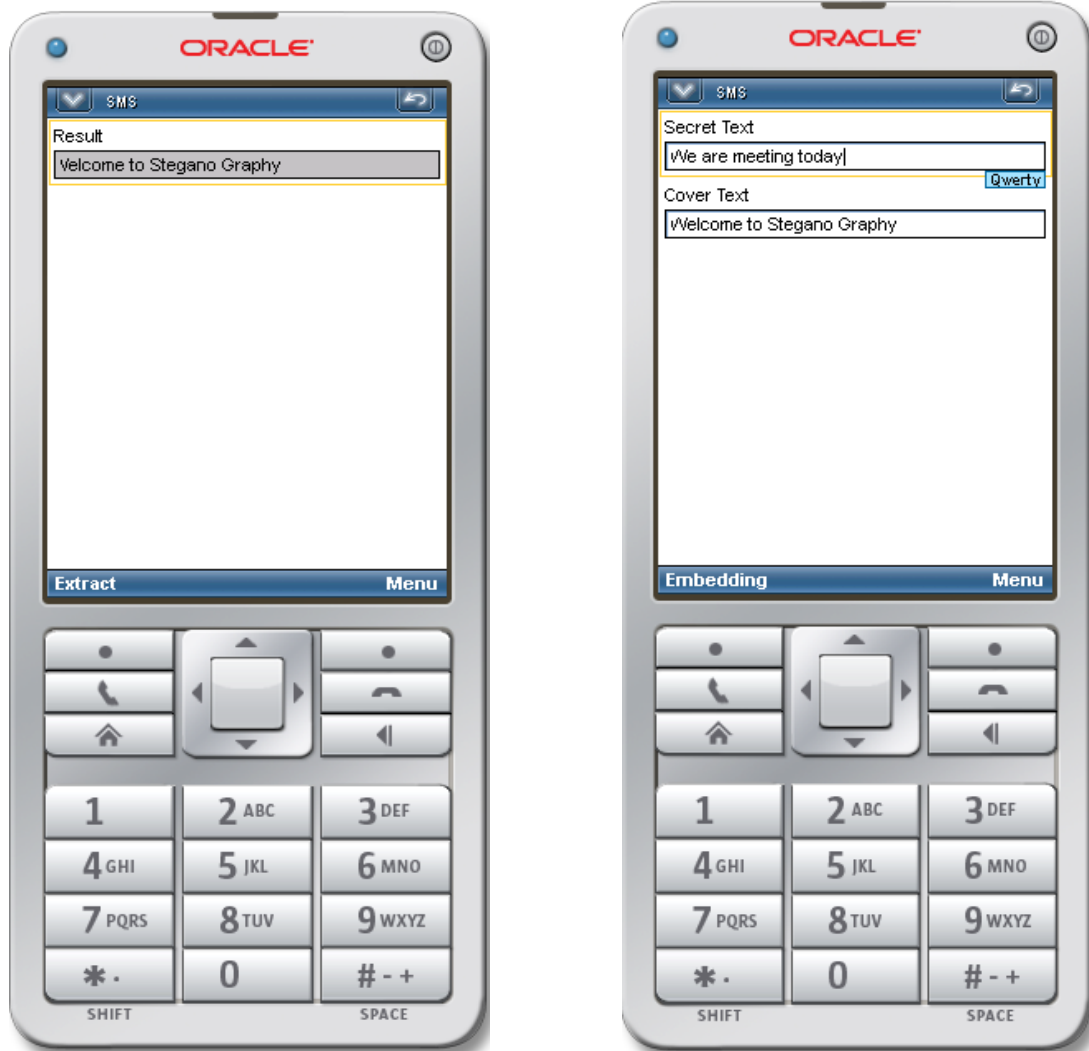


Figure (4.7): process extracts the secret message.

### 4.3 MMS\_MSG Menu: are divided into (Single cover, Double cover)

In MMS main menu display two options (single cover, double cover).

#### 4.3.1 MMS \_Single cover

MMS \_single cover sender form as the following:

Image box “cover image”: this image is used to select the cover image from existing folder.

Text field called “secret text”: this textbox to write secret message and fill selected template.

Embedding command: to embedding the text message into cover image 1 using LSB.

Send button: to send result of embedding MMS.

Figure (4. 8) shows the screen display when the sender selects single cover, and after the sender is selected the cover message; thereafter be able to write the secret message.

In this figure the selected image is done through a collection of images that stored in a mobile device. The selected image is not the only one which is stored, but the sender can select another image that stored in a mobile device.

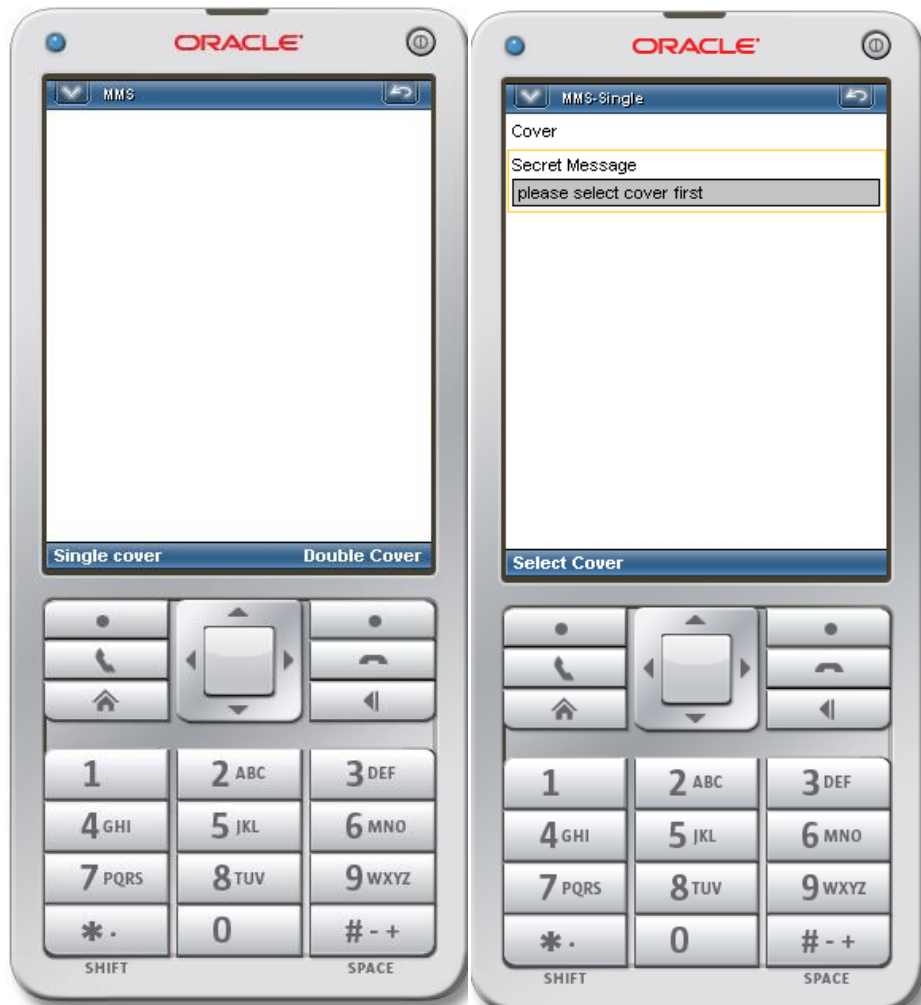


Figure (4. 8): when the sender selects single cover and next select cover (image).

Figure (4. 9) shows the selected image and thereafter be able the sender to write the secret message such as (Hello meeting today at seven o'clock) and fill the selected template.

So this figure also shows the selection of the sender to embedding option (process to embedding the image into a secret message typically LSB algorithm) and its result.

So this figure shows the result which contains the secret message inside the image. The selected option of save result when the sender is unwilling to the sent the message to the receiver.



Figure (4.9): the image cover and the sender to write secret message, so show result to process embedding.

Figure (4.10) shows that the option saved the result when the sender is unwilling to sent it to the receiver in mobile device, as well as the receiver can saved the result that sent to him. This means that save option is available for both of sender and receiver.



Figure (4. 10): option save the result when the sender is unwilling to be sent to the receiver.

Figure (4. 11) shows the option send to help the sender in sending the secret messages "result" to one receiver or several receivers at the same time.





Figure (4. 11): process sends to the result.

Figure (4. 12) shows the result that received by the receiver and then the process of extracting the secret message.

When receiver picks the result, the receiver selects option extract, which leads to extract the secret message of the cover.

MMS \_single receiver form as the following:

Text box called the result: to show original message and cover image after extract.

Process button to extract the secret message and return them (image).



Figuer (4.12): process extract secret message from the image .

#### 4.3.2 MMS \_Double cover: MMS \_double cover sender form as the following:

Image box “cover image1”: this image is used to select the cover image from existing folder.

Select cover 1: to embedding the text message into cover image 1 using LSB.

Text field called “secret text”: this textbox is to write secret message and fill selected template.

Image box “cover image2”: this image is used to select the cover image from existing folder.

Select cover 2: to embedding the result of process button1 into cover image2 “LSB”.

Send button: to send result of embedding MMS.

Figure (4. 13) shows the screen display when the sender selected double cover "double images ". First is selected the sender option select for cover1 , and the next step is the selected option select cover2.



Figure (4. 13): mine screen MMS \_double, and select cover1.

Figure (4. 14) shows when the sender selects cover1, then the screen will show the text box to write secret message. Thereafter the sender will be able to write the secret message such as

(I will go to the market). The next step is selected embedding option (process embedding secret message inside cover1 use" LSB" algorithm), and its result.

So these figures show select the sender select cover2 option to embed the previous result into cover image2 "LSB", and its final result.



Figure (4.14): writes MGS and the embedding cover1, and embedding result into cover2.

Figure (4. 15) shows the saved result when the sender is unwilling to send it to the receiver in mobile device.

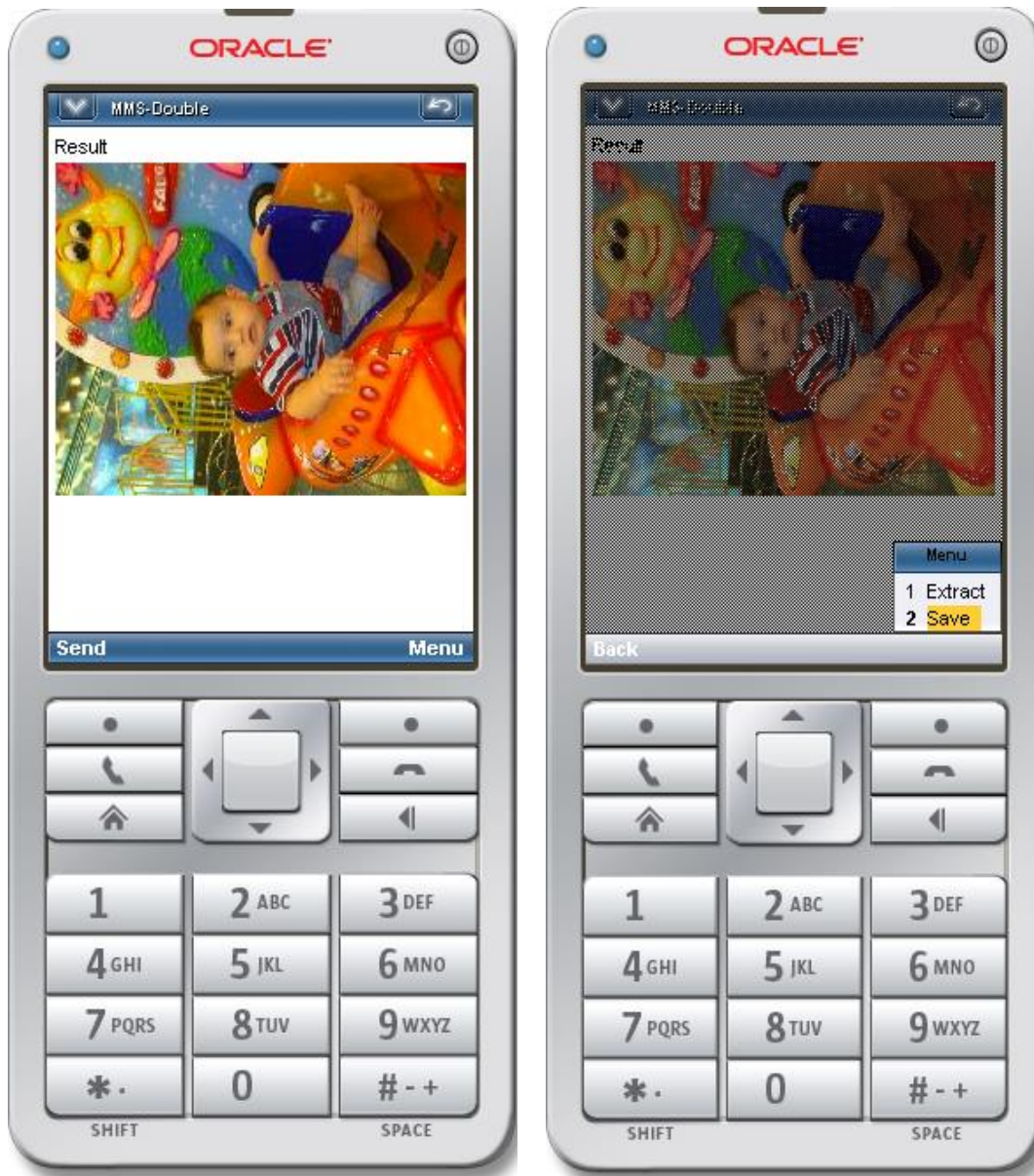


Figure (4. 15): save the final result when the sender is unwilling to be sent to the receiver.

Figure (4. 16) shows the option send to help the sender in sending the secret messages "final result" to one receiver or several receivers at the same time.

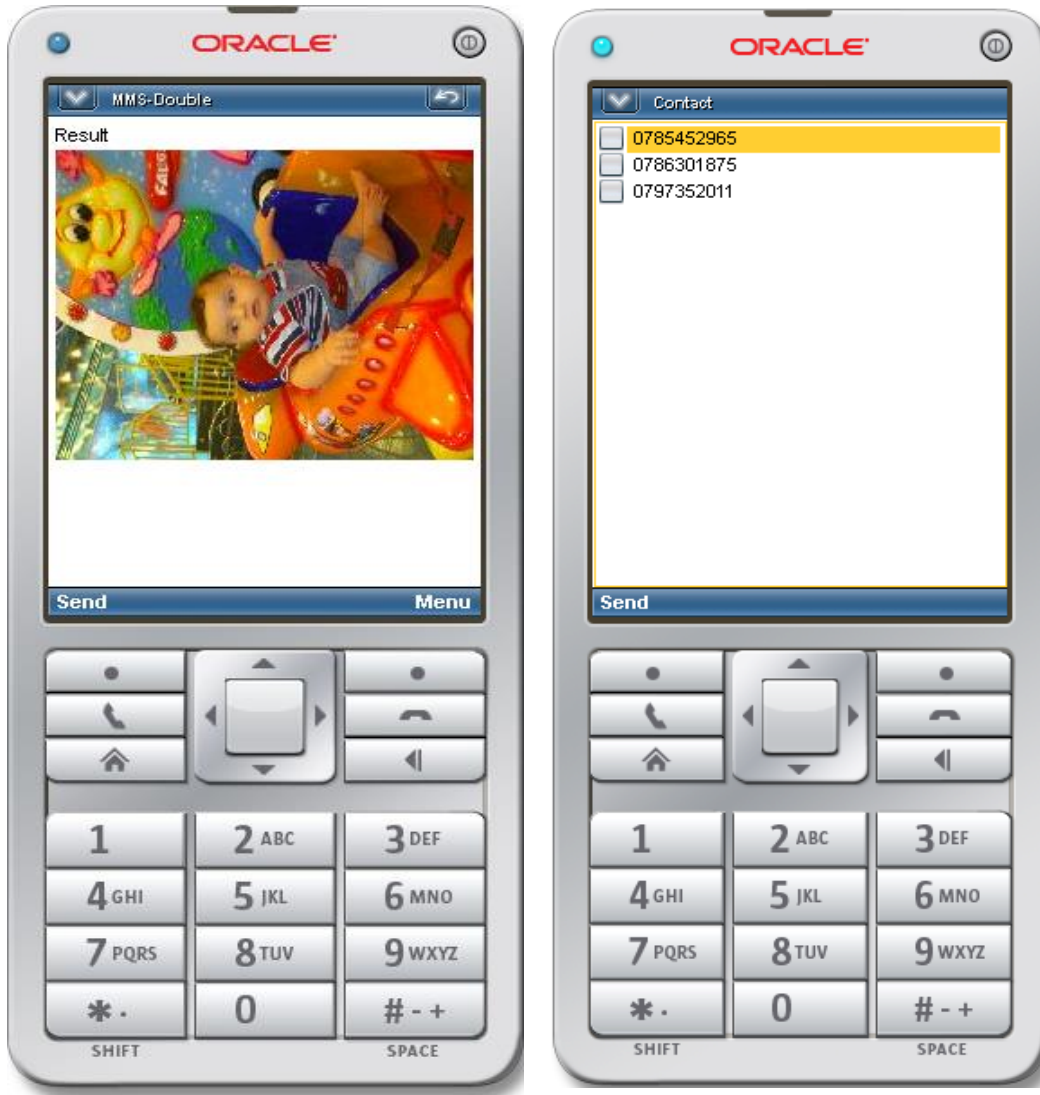


Figure (4. 16): process sends to the final result.

Figure (4. 17) shows the message received by the receiver after the process of extracting the secret message. In this figure the sender can sent the result to the receivers.

MMS \_double cover receiver form as the following:

Text box called the result: to show original message after extract.

Image box to show received message (embedding MSG with cover1).

Image box to show received message (embedding MSG with cover2).

Process button to extract the secret message and return them (text).



Figuer (4.17): process extract secret message from the cover .

#### **4.4 Conclusion:**

The implemented software provides the mobile users more security and privacy during the exchange of secret messages and authorization access to secret messages because of hiding the secret message and made it concealed during the transmission. One of the advantages of the implemented software is there's no need to a shared key between the two parties and the use both of the sender and receiver to the same software that provides flexibility more security, privacy and authorization access to secret messages. Also, the implemented software hides secret messages inside SMS and MMS without any doubts during the process of sending secret messages that look like the normal messages of SMS, MMS using the same menu the mobile phone messaging architecture system to send messages to one or more users.



## **Chapter Five**

### **Conclusions and Recommendations for Future work**

#### **5.1. Introduction**

In this thesis the most important topics is protecting both the security and privacy during the exchange of secret messages and users authorization access to secret messages. Authorized users used Steganography software in mobile application, and both of the sender and receiver are using the same software so without the need to a secret key between the parties. This leads to more security and more privacy because both the sender and receiver use their same algorithm, during the process of sending and receive secret messages and provide high flexibility, which enables us to the software loading on all types mobiles that have the property of the send messages without any modification or conditions and provide reliability and portability at the same time.

Advantage of used Steganography software to hide sensitive information into covers (texts and images) to gain more security, privacy and authorization access to sensitive information.

#### **5.2. Conclusions**

Given the importance of mobile in the daily life of users mobile, and the importance of the messages and frequent used among users to its cheap price, for privacy during the exchange secret messages, not to attract the attention of the intruders, or suspicion them during the exchange secret messages. As well as messages enables users to store sensitive information for a long time on the mobile and return them at any time possible.

So the developed software is to enhance security and increase privacy and authorized access to sensitive information of the parties to contact. That was through the use of steganography technology to hide sensitive information for mobile in the cover (SMS, MMS) and reduce the detection and infiltration information to the intruders and the reduction of all threats which threaten this information.

We implemented the developed system on mobile with our attention the following things:

The Steganography software for mobile application can demonstrate both reliability and portability at the same time.

The result of the Steganography software shows that using the Steganography technique in SMS and MMS has proved its flexibility, performance, security and integrity through using a friendly interface to easy the application.

Do not change the mobile phone messages (SMS and MMS) architecture system to commensurate the developed software system.

Use SMS system to send messages to take advantage of the characteristics of the service to be sent to several users.

To maintain the security or secret the hidden messages and the lack of clarity to intruder during transmission.

Use SMS and MMS to send secret messages without any additions to content messages or general form.

We assume that we use three algorithms to check if the users who receive the information are authorized or not. If the user is authorized the algorithm will continue the extraction process until getting the secret message. If the user is unauthorized, the algorithm will stop the extraction process.

The developed software loading does not need any modification in mobile architectural.

The developed software loads on all types mobiles that have the property of the send messages without any modification or conditions

### 5.3 Future Works

The implemented solution satisfied the desired requirements, and it can be improved by the following:

It is possible to use complex algorithms in the implemented Steganography software for mobile applications and not only LSB algorithm.

The implemented Steganography software for mobile application to hiding secret image inside image and hiding secret image inside double images. It is possible to use different method for embedding such as video and sound.

Increase the capacity of mobile leads to an increase in computations , which would lead to complex methods used in the process of embedding the secret messages(SMS,MMS ) into the covers and too the process of extract the secret messages from the covers .

## Reference:

[1] Rich Ling and Per E. Pedersen (Eds.), "**Mobile Communications**" Book, Re-negotiation of the social sphere, Mobile Phone addiction, chapter 17.

[2] <http://searchmobilecomputing.techtarget.com/definition/cellular-telep-honesearchmobilecomputing.techtarget.com/definition/cellular-telephone>, access on 8/12/2011.

[3] Wikipedia, <http://en.wikipedia.org/wiki/Telecommunication>,  
^ a b ATIS Telecom Glossary 2000, ATIS Committee T1A1 Performance and Signal Processing (approved by the American National Standards Institute), 28 February 2001.

[4] [http://www.webopedia.com/TERM/M/mobile\\_phone.html](http://www.webopedia.com/TERM/M/mobile_phone.html) , access on  
10/12/2011.

[5] Lagretteria .B. R u there February, "**The Wall Street Journal Europe**" Book, 14th 2005.

[6] Petros Zerfos, Xiaoqiao Meng, Starsky H.Y Wong, Vidyut Samanta, Songwu Lu, " **A Study of the Short Message Service of a Nationwide Cellular Network**", IMC'06, October 25–27, 2006, Rio de Janeiro, Brazil. Copyright 2006 ACM 1-59593-561-4/06/0010.

[7] Multimedia messaging service routing system and method R Skog, E Torok - US Patent 6,947,738, 2005 - Google Patents, US006947738B2

" **United States Patent**" (12)(10) Patent N0: **US 6,947,738 B2** Skog et al ... US Patent Sep ... US 6, 947, 738, B2," **Multimedia\_Message Service Routing Ststem and Method**" This application claims priority under 35 USC §119 to US Provisional.

[8] Mohammad Shirali-Shahreza, Sharif University of Technology, Tehran, IRAN," **Steganography in MMS**".

[9] Mohammad Shirali Shahreza , "**An Improved Method for Steganography on Mobile Phone**", Allameh Helli Pre-University, Ghafari Street, South Kargar Street, Tehran , Iran, <http://mohammad.shirali.ir>.

[10] Peter Gothard, "Are Mobile Phone the Next Target for Data Criminals", Portable Device News, in1988, <http://www.techradar.com>.

[11] Morkel .T, Eloff .J.H.P, Olivier .M.S, "**An Overview of Image Steganography** ", Information and Computer Security Architecture (ICSA) Research Group ,Department of Computer Science ,University of Pretoria, 2002, Pretoria, South Africa.

[12] **Wikipedia**, <http://en.wikipedia.org/wiki/Steganography>.

[13] Zaidoon Kh, A. Zaidan,A.A. Zaidan,B.B & Alanazi.H.O., 2010. "**Overview: Main Fundamentals for Steganography**". Journal of Computing, 2(3), pp 40-43.

[14] Currie, D.L. & Irvine, C.E., "**Surmounting the Effects of Lossy Compression on Steganography**", 19<sup>th</sup> National Information Systems Security Conference, 1996.

[15] Anderson, R.J. & Petit colas, F.A.P, "**On the Limits of Steganography**", IEEE Journal of selected Areas in Communications, May 1998.

[16] "Spam Mimic", <http://www.spammimic.com>. 2000.

[17] Wayner, Peter. Disappearing Cryptography: "**Information Hiding: Steganography & Watermarking**".

[18] Soumyendu Das & Subhendu Das, Bijoy Bandyopadhyay, "**Steganography and Steganalysis: Different Approaches**",

<http://books.google.jo/books?hl=ar&lr=&id=qMB9AiFUWF0C&oi=fnd&pg=PP1&dq=Wayner,+Peter.+Disappearing+Cryptography:+Informati on+Hiding:+Steganography+%>

[19] Provost, N. and P. Honey man, 2003. "**Hide and Seek: An Introduction to Steganography**". Securi. Priva. 1: 32-44. DOI: 10.1109/MSECP.2003.1203220.

[20] Alaa Hussein Al-Hamami and Mohammed Alaa Alhammi, "**Information Hiding –Steganography and Watermark**", Dar Ithraa for Publishing and Distribution, Jordan, 2008.

[21] Ariel Kelly D. Balan [akdbalan@mapua.edu.ph](mailto:akdbalan@mapua.edu.ph) , "**Applicability of Steganography to Mobile Devices**", Aeriane Charmaine C. Dizon, Leon Isaac E. Guevarra, Mark Kevin R. Villanueva, July 2007.

[22] Newcomer .E, "**Understanding Web Services: XML, WSDL, SOAP and UDDI**", Addison Wesley, 2002.' Book".

[23] Bachar Alrouh, Adel Almohammad, and Gheorghita Ghinea, "**Information Hiding in SOAP Messages: A Steganographic Method for Web Services**", International Journal for Information Security Research (IJISR), Volume 1, Issues 1/2, March/June 2011.

[24] Muhalim Mohamed Amin,Subariah Ibrahim, Mazleena Salleh,Mohd Rozi," **Information Hiding Using Steganography**", Department of Computer System & Communication Faculty of Computer Science and Information system ,UNIVERSITI TEKNOLOGI MALAYSIA 2003.

[25]Saurabh Singh, Gaurav Agarwal ,"**Use of Image to Secure Text Message with the Help of LSB Replacement**", International Journal of Applied Engineering Research, Dindigul Volume 1, No1, 2010.

[26]Neil F.Johnson and Stefan C .katzenbeisser ,"**A Survey of Steganographic Techniques** ", chapter3.

[27] Ekta Walia a, Payal Jainb, Navdeepc , "An **Analysis of LSB & DCT based Steganography** ", Global Journal of Computer Science and Technology, April 2010.

[28] Fabien A. P. Petit colas, Ross J. Anderson and Markus G. Kuhn , " **Information Hiding |A Survey**", Proceedings of the IEEE, special issue on protection of multimedia content, 87(7):1062{1078, July 1999.

[29] József LENTI," **Steganographic Methods**", Department of Control Engineering and Information Technology, PERIODICA POLYTECHNICA SER. EL. ENG. VOL. 44, NO, 3–4, PP. 249–258 (2000).

[30] Chandramouli .R, Kharrazi .M and Memon .N "**Image Steganography and Steganalysis: Concepts and Practice**", T. Kalker et al. (Eds.): IWDW 2003, LNCS 2939, pp. 35–49, 2004, c Springer- Verlag Berlin Heidelberg 2004.

[31] Ranbir Soram , " **Mobile SMS Banking Security Using Elliptic Curve Cryptosystem** ", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.6, June 2009.

[32] Prabu Kumar M and Praneesh Kumar Yadav K, "**Data Security In Mobile Devices by GEO Locking** ", International Journal of Network Security & Its Applications (IJNSA), Vol.1, No.3, October 2009.

[33] Jagdale .B .N, Bedi .R.K, Sharmishta Desai, "**Securing MMS with High Performance Elliptic Curve Cryptography**", International Journal of Computer Applications (0975 – 8887) Volume 8– No.7, October 2010.

[34] Sameer Hasan Al-Bakri<sup>1,4</sup>, M. L. Mat Kiah<sup>1,4</sup>, A. A. Zaidan<sup>2,4</sup>, B. B. Zaidan<sup>2,4</sup> and Gazi Mahabubul Alam<sup>3\*</sup>, "**Securing Peer-to-Peer Mobile Communications Using Public key Cryptography: New Security Strategy**", International Journal of the Physical Sciences Vol. 6(4), pp. 930-938, 18 February, 2011.

[35] By Yogendra Kumar Jain, Roopesh Kumar, Pankaj Agarwal , "**Securing Data Using Jpeg Image over Mobile Phone**", Global Journal of Computer Science and Technology Volume 11 Issue 13 Version 1.0 August 2011.

[36] Wesam S. Bhaya, "**Text Hiding in Mobile Phone Simple Message Service Using Fonts**", Department of Information Network, College of Computer Technology (2011), University of Babylon, Iraq, Journal of Computer Science 7 (11): 1626-1628, 2011.



[37] Reiner Creutzburg , I, Jarmo H. Takala, Chang Wen Chen, "**Wireless Steganography**", Monday 16 January 2006, San Jose, CA, USA ,Multimedia on Mobile Devices,

[http://spie.org/x648.html?product\\_id=650263](http://spie.org/x648.html?product_id=650263) access to 22/7/2012.

[38] Peter Salhofer, FH JOANNEUM, Mobile Application Programming Java Editions - IP-MAD "**Mobile Application Programming**", Java 2 Micro Edition, mad-ip.eu/files/J2ME.pdf.

[39] Sing Li and Jonathan Knudsen," **Beginning J2ME: From Novice to Professional, Third Edition**", © 2005 by Sing Li and Jonathan Knudsen.' BOOK'.