CHAPTER 1

INTRODUCTION
1.1. Cyber crimes

The Cambridge dictionary defines Cyber Crimes as Crimes committed with the use of computers or relating to computers, especially through the Internet. Universally, Cyber Crime is understood as "an unlawful act where in the computer is either a tool or a target or both".

Cyber Crimes are different from conventional crimes as in cyber crimes; the crime is committed in an electronic medium and here mens rea is not a requirement but is rather a general rule under the penal provisions of the Information Technology Act. The element of mens rea in Internet crimes is that the offender must have been aware at the time of causing the computer to perform the function that the access thus intended to be secured was unauthorized. [1]
1.2 Evolution of Mobile Phones

Mobile phones have evolved very fast in last few years. In the early days a typical wireless handset was launched for mobile communication and after continuous innovations in the technologies it has become more fascinating device with multiple features.

Not only from customer's point of view, but mobile market has grown like anything for manufacturers of hardware and software. As end users are using phone regularly they are expecting power and speed of traditional computers in mobile phones, which makes scientists and manufacturers to provide new features in each new version.

With latest inventions and rich features the ordinary mobile phones are now replaced with so called smart phones. Smart phones are being used by millions of people in their day to day life. Features available in current smart phones help end user in performing certain routine tasks from the phone itself.

In early days of smart phones only few competitors were there and market was dominated mainly by IOS and Blackberry. But with the launching of Android open source project by OHA (Open Handset Alliances) the market became more competitive and many new companies has started investing in this domain.

As per the latest survey by comscore\textsuperscript{[24]} Android has major share in the smart phone market and will continue dominating for next few years. Android is open source and that is the main reason behind success of Android in Smart Phone market.

If we consider current scenario then there are variety of manufacturers and mobile operating systems who are competing with each other to serve the users with the best experiences at affordable cost. The competition has not only opened a market for all, but has also benefited users with unexpected features in a small device called smart phones.
Some of such features include integration of Camera into mobile phone. It allows users to capture and store images from their mobile phone and eliminated use of special camera with others like clock and address book.

With increasing demands manufacturers have started providing Higher storage (in GBs) and high resolution cameras (In mega pixels) within the phone. These facilities have made it possible for users to capture digital pictures and carry them wherever they go. Not only still images, it is now possible to record videos/movies and store them in the mobile phone.
1.3 Mobile Phone Related Cyber Crimes

All these features and facilities with availability of Internet have made the mobile phone very useful and people are spending majority of their time on mobile phones. In fact one can say that people are now addicted to mobile phones.

As the mobile phone is staying with a person most of the time it is one of the place where that person would like to store or keep all the required information or data for day-to-day usage. And it is very common that people carry all such critical information in the mobile phones. Since mobile is with a person he/she is used to store things like important contact numbers, addresses, tasks or even credentials of banks/credit cards with of course images/videos captured by mobile phone camera.

It is in true sense very handy to have such device available with us, but from the other aspect it is more vulnerable also. Looking at the craze and usage of mobile phone among people around the world hackers from different parts of the world have started targeting them. The features which make a mobile phone smarter are also opening doors for hackers to get-in to the phone and steal crucial information from the device.

As per latest survey mobile phone malware have been increased in huge number these days. There are many cases where mobile phones have been targeted or used to carry out Cyber crimes.

If we specifically consider smart phone malware then following detail provided by Kaspersky Lab during March 2013 gives us how vulnerable these devices and especially Android phones:

Kaspersky Lab in a recent statement said that mobile users were actively searching for software from suspicious sources and taking no precautions when launching an unknown programme - all of which makes it easier for cyber criminals to infect devices.
Kaspersky Lab's key mobile forecast\textsuperscript{[25]} for 2012 had said that cybercriminals indeed focused their attention on the highly popular Android platform, and the number of threats for it continued to grow at a rapid pace. In January 2012, the lab had less than 6,000 unique malware samples for Android in its database, but the year ended with an astounding figure of 43,000+ malicious programmes. Over 99% of new threats found in 2012 targeted Android-based smartphones and tablets, with less than 1% aimed at devices running Symbian and BlackBerry operating systems or Java supported mobile phones.

It clearly indicates Android is highly selected target for hackers compare to other competitors from same domain. The reason behind this is open source of the Android. As android is open source and intruders can easily get into it by using its loopholes.
1.4 Steganography and Mobile Phone Related Cyber Crimes

Steganography refers to a process (art and science) of concealed communication. The term *steganography* is derived from two Greek words *steganos* ("covered or protected"), and *graphei* ("writing").[3]

This is an ancient technique used by many people including kings to communicate protected message to intended recipient. Most of the time except sender and receiver no one else know about existence of such message. It is very powerful technique to share critical messages as there are less chances of disclosure of the content.

Use of steganography varies in different conditions. May users use it for securing transactions while many use it for spreading malware in hidden way. Unfortunately it is used very frequently by hackers in committing cyber crimes. The strength of steganography is highly misused in many crimes and it is discussed in next chapter.
1.5 Literature Review

Many research scholars and scientists around the world are working on different aspects to either overcome or reduce cyber crime. The objective of the research work is to either create a solution which can secure the system (a computer, network or an organization) from cyber attacks or to detect the possible cyber attacks and reduce the damage done by such activities.

So far many innovations are done in this field and one of the major similar work done so far is use of EXIF data or meta data to find the source of an image.

Digital camera pictures may contain an Extended File Information (EXIF) header, which saves information about the camera that took the picture. The EXIF format was created by the Japan Electronic Industry Development Association and is referenced as the preferred image format for digital cameras in ISO 12234-1 [2]

This EXIF information can give details like date / time, camera used and other camera related properties. These details help a Digital Forensic Analyst to find out date on which image was captured and many times even the camera which was used. Though it provides basic details it is insufficient when the root of the image needs to be identified.

Few smart phones provide location (mostly lat and long) as an additional detail to EXIF information, which allows investigators to know about the location from where the image was captured.

But all these informations do not provide rock solid data about the person who captured the image. Even a user can disable or manipulate EXIF information easily.
1.6 Topic Selection

While I had to decide my subject topic for Ph. D. I had broad idea that I will work on mobile phone related cyber crimes. As it was fastest growing at that time and it was expected that there will be many cyber crimes which will involve use of mobile phone in coming future.

After looking at the need I observed that one of the common crime related to mobile phone was of capturing and distributing offensive MMS / SMS. This crime is generally carried out for different reasons like:

1. Creating hatred in specific group of people.
2. Blackmailing innocent victims.
3. Abusing Girls/Women
4. Spreading such content for fun.
5. To hurt someone intensionally.
6. To spoil reputation of a person.

While I was analyzing this crime, I observed that when such content spreads in the society the victim suffers a lot mentally and socially. One of the challenges in resolving this type of crimes is difficulty of detecting the original sender / creator of the content.

As per the current technique you can get detail of the sender who sends you such MMS, but you can't see from whom the sender has received. And as it starts circulating among different people once cannot trace out origin of the content.

Based on above study, I decided to work on this requirement of detecting origin for such mobile phone related cyber crimes. The decision needed some technical skill to be used and I explored many techniques to see which suits the need.
After studying variety of options, I decided to select steganography for achieving my objective. Steganography can be used to hide information in media and so the identity of originator of such content.
So I decided title for my Research topic as

“DEVELOPING A STEGANOGRAPHIC TECHNIQUE TO DETECT ORIGIN OF MOBILE PHONE RELATED CYBER CRIMES”
1.8 Objectives

✓ To develop a technique using steganography to detect source of offensive MMS and mobile crime.

✓ To assist cyber crime investigator to detect source of any mobile related crime.

✓ To keep mobile phone safe and secure device to store personal information.

✓ To make sure innocent does not become victim of the crime and criminals can be traced easily.
1.9 Details of the Remaining Chapters

Chapter 2
Contains details about digital steganography and different techniques to implement it. The chapter includes data representation of different types of images. There are limitations in implementing steganography in mobile phones and these limitations are discussed in this chapter.

Chapter 3
Chapter 3 contains introduction and detail about Android. The chapter also includes detail about android architecture and AOSP (Android Open Source Project).

Chapter 4
This chapter contains implementation of steganography technique and customization of android code. There are several sub topics in this chapter and it is core of the thesis. It includes detail about each folder of android 2.2 source with complete explanation of downloading, and customizing android source.

Chapter 5
Contains testing of customized Android OS on emulator. The customized code here contains steganographic technique and the steps to test it in emulator are described in this chapter. The chapter also checks work by extracting hidden mobile number from captured image using an independent application to confirm results.

Chapter 6
Final chapter contains conclusion statement on the research work. It also includes future scope and extension to this research from different perspectives.