Relevance of Steganography, in General, and Graph Theoretic Approach in Particular, in Indian Security Concern and Measure

Vinay Kumar*, Scientist ‘D’, NIC, DIT, MoCIT, GOI, New Delhi, India, e-mail: rakvi@hotmail.com and S. K. Muttoo, Department of Computer Science, University of Delhi, India e-mail: skmuttoo@hotmail.com

* Corresponding Author

ABSTRACT
A tool finds different usage in different hands. All usage may or may not be good for the civilized world. The case is same with a technology too. Steganography is not an exception. In this paper, we present how steganography (covert communication) can be both bane and boon for a nation, particularly in the context of the hostile situation we are living in. Steganography is a science of hiding information with the purpose of retaining privacy and secrecy of the information. In a utopian state, there is no need for any covert communication. The availability of large resources in the form of audio, video, graphs and general texts and their suitability to be used as cover object in steganography has posed an enormous threats and challenges to those involved in maintaining external security and internal law and order in any nation. The paper suggests some measures to tackle the possible menace due to this technology and risk involved in ignoring or delaying the due consideration that this science needs to be given.

KEYWORDS
Cover object, covert writing, steganography, spatial resource, data format, steganalysis, graph.

1. INTRODUCTION
In a digitized world where massive amount of data can be compromised by lost of a single laptop or a hard disk or a pen drive or an individual's identity can be swiped by an online "phishing" expedition, the need for information security is vital. Most of the concerns of data security, today, often focus on physical solution or cryptography. Very little is being thought about the use of steganography in ICT world. Over the past three to four years, it has been the source of lot of discussion, particularly as it was suspected that terrorists connected with September 11 or December 24 attacks might have used it for covert communication. While no such connection has been proved, the concern brings forth the effectiveness of the steganography as a means of obscuring data.

The purpose of the Steganography is to conceal the fact that some communication is taking place. This is achieved by hiding of secret message within another seemingly innocuous message, or carrier. Steganography, like cryptography, is a means of providing secrecy to the data under transmission. Yet steganography does so by hiding the very existence of the data, while cryptography does so by scrambling the data so that it cannot be understood by the third party.

Looking back historically, steganography was originally formalized by Simmons as the prisoners’ problem. Alice and Bob were prisoners in separate cells who wanted to develop an escape plan. They were allowed to exchange messages, but a warden looking for suspicious activity monitored their communication. Alice and Bob resorted to steganography by hiding the details of the escape plot in innocuous looking messages. The prisoners’ goal was to hide the secret data so that the warden could not tell whether the exchanged messages were genuine or contain hidden data.

For clarity of the concept, we may visualize that the messages exchanged by the prisoners are digital images. Most steganographic schemes for digital images hide secret data by slightly perturbing the values representing the numerical values of individual pixel colors. For example, the secret data may be communicated in the least significant bits (LSB) of colors of selected pixels. The main requirement of any steganographic technique is undetectability. The intruder should not be able to distinguish between cover objects (original unmodified messages) and stego objects (cover embedded with data) with success better than random guessing given a complete knowledge of the steganographic algorithm and the source of cover objects and possibly a key. The detectability of data hidden in a stego object is mainly influenced by four factors:

- the choice of the cover object,
- the selection rule used to identify individual element of the cover that could be modified during embedding,
- the type of embedding operation that modifies the cover element, and
- the number of embedding changes.

There is large number of steganographic methods that most of us are familiar with. Familiar examples are invisible ink, microdots, plain text, images stored in different file formats, audio files etc. With the advent of Information Communication Technology (ICT), there are many other ways of hiding information, such as:

- Covert channels (e.g., Loki and some distributed denial-of-service tools use the Internet Control Message
Protocol, or ICMP, as the communications channel between the "bad guy" and a compromised system

- Hidden text within Web pages
- Hiding files in "plain sight" (e.g., what better place to "hide" a file than with an important sounding name in the c:\winnt\system32 directory?)
- Null ciphers (e.g., using the first letter of each word to form a hidden message in an otherwise innocuous text)

With the abundance of available downloadable multimedia resources on the various web sites, Steganography today, however, has significantly more sophisticated cover media to use from. This in turns allowing a user to hide large amounts of information within image and audio files. These forms of steganography often are used in conjunction with crypography so that the information is doubly protected; first it is encrypted and then hidden so that an adversary has to first find the information -difficult task in itself, and then decrypt it.

This method can be employed not only to cover data to hide from eavesdropper but also to uncover such devious tactics, but the first steps are awareness that such methods even exist. There are many good reasons as well to use this type of data hiding, including watermarking or a more secure central storage method for such things as passwords, or key processes. The technology is easy to use and difficult to detect. The more that we know about its features and functionality, the more ahead we will be in the game. The basic objective of the paper is:

- To highlight the potential use of the National Spatial Database as secret repository of strategic information, plan, execution methodologies etc. using graph theoretic approach.
- To mention potential threats that this science may pose to India’s security concern due to inability to use the information available in stego form.
- To suggest that some financially supported Research and Development activities should be initiated as early as possible.

2. PRESENT SCENARIO

"The terrorists know that if they use machines at home, they can be caught. Cyber cafes therefore give them anonymity," says Vijay Mukhi, President of the Foundation for Information Security and Technology. This is reported under the title "Police to monitor Cyber Cafes" dated September 5, 2007 that is available on http://www.schneier.com/blog/archives/2007/09/police_to_monit.html.

He further adds, "The police needs to install programs that will capture every key stroke at regular interval screen shots, which will be sent back to a server that will log all the data. The police can then keep track of all communications between terrorists no matter, which part of the world they operate from. This is the only way to patrol the net and this is how the police informer is going to look in the e-age."

Is anyone talking about the societal implications of this sort of wholesale surveillance? Even at the cost of breach of individual privacy, will it be a sufficient mechanism to deal with cyber crimes? Certainly not! This simply explains our preparedness and line of thinking to deal with such larger issues which adds a new dimension to it every passing day with the very rapid developing Information Communication Technology.

Terrorists have already demonstrated that they can use the Internet in such a way as to not get caught or compromised. This came out I think more than a couple of years ago. Cyber terrorism can be understood as the activity that uses the ICT with the intention to disrupt social, religious, political or similar order in furtherance of so called ideological objectives. An example may be found in the way of use of klem_kaddiddlehopper@yahoo.com, which was opened by an operative using a fictitious identity, and is thus traceable to no one. Once logged in, each opens the mail service, deletes all the spam built up, and views and then edits one of the drafts of a message which will never be sent. It contains the secret message, hidden by steganographic methods.

Steganography is the science of information hiding. It wonderfully conceals a file inside a digital cover. More is the redundancy in the file format of a cover file, much larger a file can be concealed in it. It is simple to have a central repository of messages where people can post pictures or shots of purported UFOs so that the knowledgeable can post messages and read those of others by uploading and downloading the correct files. Imagine the size of a file that could be hiding inside of a video posted on YouTube.

At present, there are many online depositories of the various multimedia objects created, maintained and marketed by different independent agencies. The government agency responsible for providing intelligence input to organs accountable for maintaining internal law & order and external security has virtually no clue that how these sites can play havoc in spreading premeditated message through covert writing. Steganography can be used for peer to peer private communication in order to share any intelligence input. It can also be used to post secret communication on the web to avoid transmission for sharing of information through a secured common platform. On the other hand steganalysis can be used to unearth any hidden information in UFOs (cover object which is usually multimedia object) that may lead to social and economic damages. Keeping an eye on these sites can help in taking preemptive measure against any subversive effort of ill minded group of people. In order to do that it is essential to know the resources that can be used for this purpose and the way it can be used. We discuss some possible measure that can be taken in this regard in section 4 of this paper.
In India, a lot of work has been initiated and completed towards development of National Spatial Databases (NSDB). It hosts geographical details in digital form using various data formats. These details are available in both vector and raster form. This repository may be put to use for not only covert communication among security agencies but also among the strategic planner who would like to keep the plan secret until proper time to reveal that. At present the scenarios is evident from the recent statement of the Union Home Minister. On 4th October, 2007 he said that intelligence agencies of the states were not strong and adequate enough to meet the challenges of terrorism. It is also true that it is not also steganographically equipped to deal with. It is irony that many governments in the world have created laws that either limit the strength of cryptosystems or prohibit them completely primarily because of the fear of not been able to gain intelligence from it. It is like forcing not to communicate in the medium that our intelligence agencies do not understand! If there is no activity, no discussion, no exchange of ideas and communication, there will not be any source of intelligence. Steganographic technologies are a very important part of the future of Internet security and privacy on open systems such as the Internet. Early it is known that how to use the technology and how other may use or misuse it, better will be for the nation in particular and mankind as a whole.

3. POTENTIAL THREAT

Imagine a situation of inaugural function for release of compilation of some events on DVD. A very high dignitary of India is chief guest and he has to release the DVD. The preface of the DVD contains a message from Head of state containing his/her excellency’s recent photographs in some digital format. Suppose the place where the DVD has been made (copied with the contents) the photograph has been steganographed with the message that may create some diplomatic row with some otherwise friendly nation! The extent of damage caused can be devastating. The practice of steganography has its own distinguished history; modern technology is only facilitating it as how beautifully it can be used or hatefully be misused.

For illustration, figure 1 is of the corresponding author of this paper. Figure (a) is used as a cover object to hide the message “I am not doing the thing what I can do in much better way” approximately around frame of the spectacle on the face. The stego image is (b). The image is in 24 bits BMP format.

In a daily news paper, recently it has been reported that the militant responsible for the Red Fort attack were running a cybercafé and using electronic mail to receive instructions from abroad. When the police seized their computers and e-mail messages, they found a vast amount of pornographic films and photographs on the hard disks. Assuming that the militants might have stored pornographic collection for personal enjoyment, it dumped it into the *maalkhana* as case property.

A few weeks later, a police officer in Delhi read in the ‘USA Today’ about the testimony furnished by George Tenet, Director, CIA, to the US Congress. It stated that extremists were hiding their messages within pornographic and sports images and movies, as well as in music files, and were utilizing heavily-visited electronic chat rooms and bulletin boards as drop sites. The modus operandi is to download the file and decrypt the hidden message. To all others who would download that file, it would seem to be an innocuous image. The first organizations to recognize the utility of steganographic algorithms developed in European universities were, as suspected, the terrorist groups known by different names in different parts of the globe. It is further assumed that Al Qaida was the first to practice the research results of Professors Ross Anderson and Fabien Petitcolas of Cambridge University, and conceal its messages in dense packet internet traffic, and large bandwidth uncompressed audio, video and image files. These files are located at heavily visited pornographic sites, music download sites, chat rooms and bulletin boards. Al Qaida began to use these as message drop sites for their agents. A security analyst detected steganographic activity even on heavy-traffic commercial portals such as Amazon and eBay, who were not even aware that their web sites were being used for such purposes.

A security analyst recounted the case of a suspected militant. The security analyst, which had placed him under surveillance using its packet-sniffing tool Carnivore, was intrigued that while he kept e-mailing photographs of his family to e-mail addresses that appeared to be those of relatives, he never received any replies. It was found that he was sending instructions to his agents using DEMCOMs Steganos. It simple passed undetected by a package called Carnivore used...
by the security analyst. There is software that combines technical excellence with human psychological factors to avoid suspicion. One such example is Texto, developed in Finnish universities, which converts messages into blank verse poetry. Another is Spam Mimic, which encodes messages into what looks like a junk e-mail. So if steganography is so popular, is there anything the government can do about it?

While round one has gone to the terrorists, Indian security agencies can fight back. Compressed video, music and image, graphs, maps, sketches, cartoons etc. are stored into binary files having predictable patterns that would be disrupted when a message is inserted. It is possible to develop a stego scanner program, akin to a virus scanner, to examine hard drives and identifies the electronic fingerprints and signatures left behind by steganographic applications.

4. A POSSIBLE COMBATIVE MEASURE

Steganalysis is the art of detecting and breaking steganography. One form of this analysis is to examine the color palette and adjacency pattern of a graphical image. A detailed work is to be carried out to support/compliment the graph theoretic approach to steganography. A possible steganography roadmap for future efforts can be outlined as below:

- A comprehensive and cooperative zeal among the agencies having the spatial resources to share for the national cause.
- Collection of all possible formats in which a potential cover object (graph, image, audio, video etc.) can be stored. It is continuous process. It may stabilize and saturate after sometime. Till then sustainable effort should be continued.
- The change of mindset among the planner and intelligence agencies that means of information gathering has changed a long way over the period of time and is still changing with the advancement of the technology, particularly IT.
- Derive the signatures/indicators associated with each steganographic package and write a scanner. The harder part is picking up the dead drops. This would require involvement of many accountable officers to continuously monitor the web sites, bulletin boards and chat rooms.
- The next stage is difficult. Once such sites are identified, develop a Trojan horse that would sit in the machines and scan all activity.

If terrorist group can put into practice the latest technological breakthroughs from European universities for ill effect to the human beings there is no reason why India should not use its resources for the betterment of the human beings and to provide better security to the nation. The intelligence agencies should, for instance, examine the hard drives of those militants who are being caught. A schematic diagram for the development and implementation of the suggested roadmap is shown in the figure 2. India’s security agencies should utilize the latest steganographic technologies for their internal communications as well, in contrast to the insecure channels they use at present. They should also develop the futuristic science of detecting these hidden messages and decrypting them, in order to trace sensitive information being leaked out under innocuous guises. For these, they should work together with the Universities/research institution just as the Center for Secure Information Systems in the US is a joint venture between the National Security Agency and the George Mason University. The Pentagon and CIA are funding steganalysis research at the Carnegie Melon.

What is suggested through this paper is to develop and utilize own format to store and use spatial data. The expertise of the Indian scientist working in the area of the development of national spatial database can be utilized to develop one such format. The format so developed can be used to store a graph, map, sketch etc. and then to use it as cover object in steganography for secured communication by the intelligence agencies. In fact there exist a few such data formats to store a planar graph or map. Authors of this paper have written a research paper on this. Currently this paper is submitted to International Journal of Communication Network and Distributed Systems.

Modern steganography works by replacing bits of unused (or at least significant) data in regular digital files with bits of invisible information. To embed hidden information into a graph requires two files - the cover graph that will hold the hidden data and the secret message file. A message may be
Relevance of Steganography, in General, and Graph Theoretic Approach in particular, in Indian Security Concern and Measure

plain text, cipher text. When combined, the cover object and the hidden message make a stego object. A stego-key or password may be used to hide and decode the message. Special software is needed for steganography.

As common in the GIS (Geographical Information Systems) a feature called metro line from the above map can be extracted. A track between any two metro stations, in the extracted feature, can be embedded with the secret message and can be sent to the concerned authority to convey the potential threat and possible measure that can be initiated to avoid any such mishap. Possibly then figure 3(a) will look like 3(b). Obviously it is very difficult to detect unless the graph is zoomed by a large factor. Initial institutional support is required to carry out the research and to conduct follow up training programs to the concerned agencies.

A concerted cooperative approach among academics, industries and research institution should be initiated in this direction to fight these possible cyber crimes before it takes its toll. Also, on the line of anti spam, anti virus group, a group dedicated for steganalysis should be considered to carry out research and development in this direction. Early the steps are taken better will be for the country.

5. CONCLUSION
Steganography is a fascinating and effective method of hiding data that has been used throughout history. One of the oldest steganography schemes was to shave the head of a messenger and tattoo a message on the messenger's head. After the hair grows back, the messenger can be sent to the intended recipient, where the messenger's head can be shaved and the message recovered. This method is deceivingly clever, patient, and very low-tech, and goes right to the heart of steganography's literal meaning of "covered writing."

Steganography doesn't just apply to written forms of communication. Radio and TV messages, from World War II to today, can be used to hide coded or hidden messages. Some government sources even suspect that Osama bin Laden's pre-recorded videos that are re-played on TV stations around the world contain hidden messages.

In a democratic world, where any control on the flow of information is taken as encroachment on freedoms, a persistent vigil is essentially and urgently needed to track any such covert communication taking place to disturb peace and harmony in the civil society. News posting on a newspaper web site may carry a photograph of a national leader lying in some hospital bed. A motivated hacker may download the image together with the news text. It can then steg a message to do some harm to the leader and send the news as it is to its accomplices to carry out the task as planned and directed. The entire message may go undetected to the recipient leaving the security agency in lurch. What is needed is to scan such images even if it is not suspicious to see whether it contains any hidden information.

A lot of research is required to find out ways in which message can be hidden in digital cover media. It can be used for the benefit of the society as well as for better administrative management by keeping any secret information secret and beyond the reach of spoiler by maintaining its utmost privacy. The rich resources of spatial data available under national spatial database project may also be used for the purpose of steganography using graph-theoretic approach to steganography. Authors of this paper are currently working in this area. A cover graph is slightly distorted in a way that human eye cannot recognize it by ensuring that the visual changes introduced by the embedding remains as minimum as possible.

6. ACKNOWLEDGEMENT
Inspiration comes from many sources. In fact it is always there. One has to look around to know the presence of something worth noticing. The paper is result of the present potential threat, the world in general and India in particular is facing from the intelligent and technically expert group of people who are driven by some motivations. Different names are given to such motivations and to the group of people who are involved in it. It is not the place to discuss about that. What is important is to find a way to tackle these problems for the sake of the safety of human life. We are grateful to almighty for keeping us in good mental health to think about it.

Further, we are very grateful to all those who have been constantly encouraging us to go for such scientific and social research work besides the regular work which we are doing in our respective departments.

7. REFERENCES
8. A number of web sites through google search engines provide rich source of texts and materials.

8. Biographical notes
1. **Vinay Kumar** is a postgraduate in mathematics. He did his MCA in 1990 from School of Computer and System Science, Jawaharlal Nehru University, New Delhi. He is working as a scientist in National Informatics Center, MoCIT, Government of India. Recently a paper by him is published in ‘International Journal of Information Technology and Management’ on ‘Overcoming 64kb data size limit in handling large spatial data in GISNIC while cleaning and building topology’. He has authored a book on **Discrete Mathematics** published by BPB, India in Oct-Nov 2002.

2. **Dr. Sunil K. Muttoo** is Reader in Department of Computer Science, University of Delhi, India. He completed his M. Tech from IIT Kharagpur, India. His specialized area is coding theory, encryption, data security and privacy. He has been Research Scholar of ISRO sponsored Project (ii) "Gross Migration Scheme" Fellow (for doing M.Tech.).