Rukmini Devi Institute of Advanced Studies

Madhuban Chowk, Rohini, Delhi-110085

(Approved By AICTE &Affiliated With GGSIP University)

DOSSIER

On

Guest Lecture

On

"Graph Theoretical Approach to Steganography"

on

11th February, 2013

Ms. Pallavi Joshi
(Member, Literary Club)

Ms. Upasana Diwan
(Chairperson, Literary Club)

Prof. Col. (Retd.) Mahander Singh
Director General, RDIAS

FORM A

Proposal:

- **Name of the event to be organized**: Guest Lecture on Graph Theoretical Approach to Steganography

- **Date:** 11th Feb , 2013

- **Time:** 2:00 PM-3:30 PM

- **Venue:** Lecture Theatre, RDIAS

- **Motivation for the activity**: This lecture was conducted with the motive to make the students of MCA aware of concepts of steganography and its implementation.

- **Organized by**: MCA Department

FORM B

Part 1

Aim of the event: The aim of this event was to introduce everybody with Steganography and its functionalities. Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity

Hence it is important for the students to be well acquainted with the field and should be aware of the intricacies of implementing this technology. Keeping this in mind a guest lecture was organized for the students of MCA.

Part 2

Abstract:

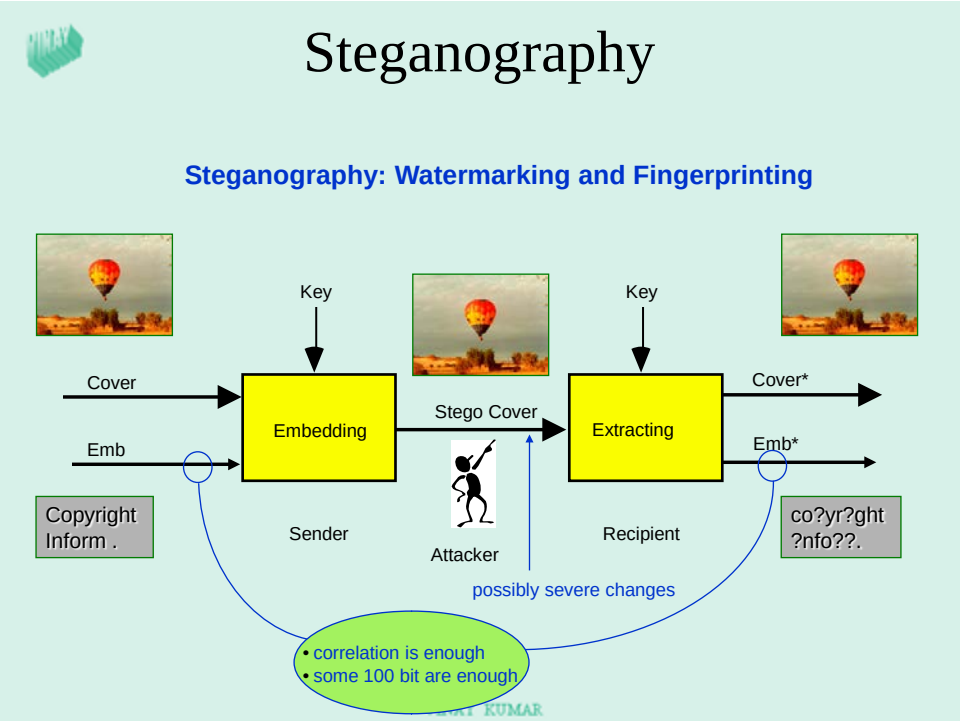
The session was conducted by Dr. Vinay Kumar, Scientist in National Informatics Centre, MoCIT, Government of India.

His presentation contained the following discussion points:

1. What is Steganography?
2. Steganography example
3. Cover Object
4. Various methods of Steganography
5. Two ways of using graphs for hiding information
6. Application and future directions

Many real world anecdotes were shared with the students in the course of this discussion:

Mr.Vinay Kumar started the discussion by explaining the basic meaning of Steganography. **Steganography** is hiding information within a more obvious kind of communication.



He told how **Steganography** was used in earlier centuries by roman peoples. Following procedure was used by them to maintain the secrecy of data.

- messenger shaved his head
- tattooed a message on it
- waited for his hair to grow back
- travelled to his destination
- shaved off his head to reveal the message.
- Also used invisible ink etc.

Then he explained about cover channels also known as covert channel and gave two categories of covert channels: storage & timing

Storage channel are all vehicles that allow direct/indirect writing of a storage location by one process and direct/indirect reading of it by another process.

Timing Channel: All vehicles that allow one process to signal information to another process by modulating its own use of system resources in such a way that the change in response time observed by the second process would provide information.

Sir gave various Digital Steganographic Methods:

1. Injection Steganography: The payload or embedded data is placed inside the cover object/covert channel e.g. image, audio, program file. The resultant file is called stego object in general. Size of stego object in this case is larger than that of cover object.

2. Substitution Steganography: The *payload* is placed inside the cover by replacing the redundant/insignificant part of it. It is done in such a way that it must survive a detection by maintaining almost similarity between stego and cover object.

3. Propagation Steganography: An output is generated from the payload. The content of this file, also referred as mimic, may appear as freeform graphic or any other type of file.

Sir described what is Graph-Theoretic Approach to Steganography, along with two ways of using graph for information hiding

1. Generate graph (node and exchange relationship) from payload and digital cover then hide the graph into that cover which may be image, audio or video file…(S. Hetzl and P. Mutzel)

2. Use a graph as cover object and find redundancy in its feature like node or segment or its attributes and embed payload in it.

Sir also gave various examples like hiding message in a map along pre Hamiltonian path, hiding information in a sustainable way.

Part 3

Conclusion:

Sir concluded the session by giving various applications and future directions of Steganography:-

1. A recursive or explicit mathematical function $f(k_s)$ may be derived to divide the image based cover in different blocks of different size k_s (s = 1, 2, 3 ..) so that the cover image may carry the secret information in natural way only. The mathematical formula $f(k_s)$ will be then stego key.
2. The rich resources of spatial data available under national spatial database project may be used for the purpose of steganography by developing suitable protocols using GTA.
3. More rigorous work is required to explore the method to hide information in a map so that almost entire secret message is hidden in node only. In this way no intermediate points is to be nagged.
4. Watermarking a digital data in reliable and secure way is still a challenge. The protocol presented in this thesis to watermark vector map can be further extended to watermark other spatial and non-spatial digital data.
5. Since the graph isomorphism and complementation of a subgraph provides large domain for stego key, a public key steganography can be explored using GTA.

Students of MCA showed great enthusiasm by attending the session and actively participating in question answer sessions. Some curious questions were raised by the students . All were answered by the speaker in a very explicable manner.

Lecture Moments

Student from MCA-4th sem (Mankunvar) introducing Dr. Vinay Kumar !!

Dr. Vinay Kumar giving the lecture!!

Students listening about steganography!!