STEGANOGRAPHY

B Tech CSE- IV Sem

TCS 491

Introduction to Cryptography

Jan- Jun 2022

STEGANOGRAPHY

- The word **Steganography** is derived from two Greek words- ‘stegos’ meaning ‘to cover’ and ‘grayfia’, meaning ‘writing’, thus translating to ‘covered writing’, or ‘hidden writing’. **Steganography** is a method of hiding secret data, by embedding it into an audio, video, image or text file. It is one of the methods employed to protect secret or sensitive data from malicious attacks.

STEGANOGRAPHY

- We conclude with a discussion of a technique that (strictly speaking), is not encryption, namely, steganography. A plaintext message may be hidden in one of two ways. The methods of steganography conceal the existence of the message, whereas the methods of cryptography render the message unintelligible to outsiders by various transformations of the text.

- A simple form of steganography, but one that is time-consuming to construct, is one in which an arrangement of words or letters within an apparently innocuous text spells out the real message. For example, the sequence of first letters of each word of the overall message spells out the hidden message. Figure 3.9 shows an example in which a subset of the words of the overall message is used to convey the hidden message. See if you can decipher this; it's not too hard.

Some examples:

- Various other techniques have been used historically; some examples are the following :
- ■ Character marking: Selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held at an angle to bright light.
- ■ Invisible ink: A number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.
- ■ Pin punctures: Small pin punctures on selected letters are ordinarily not visible unless the paper is held up in front of a light.
- ■ Typewriter correction ribbon: Used between lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light.

Other Points

- Although these techniques may seem archaic, they have contemporary equivalents. Some academicians propose hiding a message by using the least significant bits of frames on a CD. For example, the Kodak Photo CD format's maximum resolution is 3096 * 6144 pixels, with each pixel containing 24 bits of RGB color information.
- The least significant bit of each 24-bit pixel can be changed without greatly affecting the quality of the image. The result is that you can hide a 130-kB message in a single digital snapshot.
- There are now several software packages available that take this type of approach to steganography. Steganography has several drawbacks when compared to encryption. It requires a lot of overhead to hide a relatively few bits of information, although using a scheme like that proposed in the preceding paragraph may make it more effective. Also, once the system is discovered, it becomes virtually worthless. This problem, too, can be overcome if the insertion method depends on some sort of key. Alternatively, a message can be first encrypted and then hidden using steganography. The advantage of steganography is that it can be employed by parties who have something to lose should the fact of their secret communication (not necessarily the content) be discovered. Encryption flags traffic as important or secret or may identify the sender or receiver as someone with something to hide.

How is it different from cryptography?

- Cryptography and steganography are both methods used to hide or protect secret data. However, they differ in the respect that cryptography makes the data unreadable, or hides the *meaning* of the data, while steganography hides the *existence* of the data.
- In layman's terms, cryptography is similar to writing a letter in a secret language: people can read it, but won't understand what it means. However, the existence of a (probably secret) message would be obvious to anyone who sees the letter, and if someone either knows or figures out your secret language, then your message can easily be read.
- If you were to use *steganography* in the same situation, you would hide the letter inside a pair of socks that you would be gifting the intended recipient of the letter. To those who don't know about the message, it would look like there was nothing more to your gift than the socks. But the intended recipient knows what to look for, and finds the message hidden in them.
- Similarly, if two users exchanged media files over the internet, it would be more difficult to determine whether these files contain hidden messages, than if they were communicating using cryptography.
- Crpytography is often used to supplement the security offered by steganography. Crypography algorithms are used to encrypt secret data before embedding it into cover files.

Thank You

&

Best Wishes