Chapter 9
Digital Steganography Security

Parkavi R.
Thiagarajar College of Engineering, India

Anitha S.
Thiagarajar College of Engineering, India

Gayathri R.
Thiagarajar College of Engineering, India

ABSTRACT
Steganography has been considered as a major instrument used for an unauthorized and destructive purpose such as crime and warfare, and forensics has been used for a constructive purpose such as crime detection and fraud detection. Hence, the combination of both steganography and forensics plays a major role in the present internet era for information exchange between two parties. It has been propelled to the forefront of the current security techniques. The main objective of the technique is to provide an imperceptible way of transferring secret messages to the recipient. Another issue to be noted is that the term steganography completely differs from cryptography. The above-stated analysis is used in digital forensics. There are many steganography software tools available for ordinary computer users.

INTRODUCTION
The word “DATA” is more valuable than money. Nowadays Data is flooding over the internet via social media like Facebook, Twitter, YouTube and the web browser itself. Even a search query and history data of a search engine can able to describe one’s personal or societal status. Due to rapid increase in data mining, analytics as well as hacking technologies and tools, data can be easily processed to get valuable information.

DOI: 10.4018/978-1-7998-1558-7.ch009
information of a person or country like their favorites, daily routines, family and business, and even though unknown secrets which are not even known by the respective user. So the risky situation comes here to exchange data via the internet which is ineluctable in our fastest and modern world. There is a need for reliable techniques that helps to secure data roaming on the internet. Hence the security systems like Cryptography, Steganography comes to the digital world to secure the data, which is already used by our ancients to protect data that exist in physical matter.

**HISTORY OF STEGANOGRAPHY**

The word Steganography comes from the words “Steganos” means cover or secret and “graphy” means writing. The veiling of one form of data within another form of data is called Steganography. Many incidents are revealing that Steganography is not a new technique for this world. The first incident was, Ancient Greek Ruler Histaeus used to shave the head of his slave, tattooing in the scalp and wait for hair to grow. Then send the slave to recipients to convey the hidden message. The recipient would have shaved the slave’s head to see the message. In the second incident, Demestrus wrote a message to his friend in the wooden carve of the wax tablet that seemed to be simple. In the third incident, During the American & British Revolutionary, they use invisible ink to exchange information. In the fourth incident, during World War 2, Germans used microdots. Later, Null ciphers were used i.e. unencrypted message send within the real readable format. For example, Police report emergencies in downtown ending near Tuesday by taking the first letter on each word on the given sentence, it gives the result “PRESIDENT”. This is called null cipher. As the years have grown, Steganographic techniques also grow and emerge as the strongest technique to secure the data. (Siper, Farley, R & Lombardo, 2005)

**Cryptography vs. Steganography**

Cryptography is the most frequent usable technique for data communication in the network where Steganography is not in that case but it is also used for secured data sharing.

Cryptography uses a key to encrypt or decrypt the data. For example, Mr. X wants to send the message “Hello Mr.” to Mr. Y via the “ZZZ app”. The “Z app’s” security system encrypts the plain text of Mr. X i.e. altering the actual or original message to something like “HSJHDJHF SDKJSDJS” (just for example, not a real answer) as a ciphertext which is going to send in the network by using the public key of Mr. X. On another end, Mr. Y ‘s app receives the ciphertext sent by Mr. X and the security system decrypts the ciphertext into plain text by using the private