**Steganography :-**

**Steganography** is the practice of concealing a file, message, image, or video within another file, message, image, or video. The word *steganography* combines the [Greek](https://en.wikipedia.org/wiki/Greek_language) words *steganos* meaning "covered, concealed, or protected", and *graphein*  meaning "writing".

The first recorded use of the term was in 1499 by [Johannes Trithemius](https://en.wikipedia.org/wiki/Johannes_Trithemius) in his *[Steganographia](https://en.wikipedia.org/wiki/Johannes_Trithemius" \l "Steganographia" \o "Johannes Trithemius)*, a treatise on cryptography and steganography. Generally, the hidden messages appear to be (or be part of) something else: images, articles, shopping lists, or some other *cover text*. For example, the hidden message may be in [invisible ink](https://en.wikipedia.org/wiki/Invisible_ink) between the visible lines of a private letter. Some implementations of steganography that lack a [shared secret](https://en.wikipedia.org/wiki/Shared_secret) are forms of [security through obscurity](https://en.wikipedia.org/wiki/Security_through_obscurity), whereas key-dependent steganographic schemes adhere to [Kerckhoffs's principle](https://en.wikipedia.org/wiki/Kerckhoffs%27s_principle" \o "Kerckhoffs's principle).

The majority of todays steganographic systems uses multimedia objects like image, audio, video etc as cover media because people often transmit digital pictures over email and other Internet communication. Modern steganography uses the opportunity of hiding information into digital multimedia files and also at the network packet level. Hiding information into a medium requires following elements . 1. The cover medium(C) that will hold the secrat message. 2. The secret message (M), may be plain text, digital image file or any type of data. 3. The stegonographic techniques 4. A stego-key (K) may be used to hide and unhide the message. In modern approach, depending on the cover medium, steganography can be divided into five types: 1. Text Steganography 2. Image Steganography 3. Audio Steganography 4. Video Steganography 5. Protocol Steganography.

**• Text steganography**

Hiding information in text file is the most common method of steganography. The method was to hide a secret message into a text message. After coming of Internet and different type of digital file formats it has decreased in importance. Text stenography using digital files is not used very often because the text files have a very small amount of excess data .

**• Image steganography**

Images are used as the popular cover medium for steganography. A message is embedded in a digital image using an embedding algorithm, using the secret key. The resulting stego-image is send to the receiver. On the other side, it is processed by the extraction algorithm using the same key. During the transmission of stego- image unauthenticated persons can only notice the transmission of an image but cant see the existence of the hidden message.

**• Audio steganography**

Audio steganography is concerned with embedding information in an innocuous cover speech in a secure and robust manner. Communication andtransmission security and r obustness are essential for transmitting vital information to intended sources while denying access to unauthorized persons. An audible, sound can be inaudible in the presence of another louder audible sound .This property allows to select the channel in which to hide information . Existing audio steganography software can embed messages in WAV and MP3 sound files. The list of methods that are commonly used for audio steganography are listed and discussed below.

• LSB coding

• Parity coding

• Phase coding

• Spread spectrum

• Echo hiding .

**• Video steganography**

Video Steganography is a technique to hide any kind of files in any extension into a carrrying Video file.

**• Protocol steganography**

The term protocol steganography is to embedding information within network protocols such as TCP/IP. We hide information in the header of a TCP/IP packet in some fields that can be either optional or are never used.

**Applications of Steganography**

**• (i)Secret Communications**

The use steganography does not advertise secret communication and therefore avoids scrutiny of the sender, message and recipient. A trade secret, blueprint, or other sensitive information can be transmitted without alerting potential attackers.

**• (ii)Feature Tagging**

Elements can be embedded inside an image, such as the names of individuals in a photo or locations in a map. Copying the stego-image also copies all of the embedded features and only parties who possess the decoding stego-key will be able to extract and view the features.

**• (iii)Copyright Protection**

Copy protection mechanisms that prevent data, usually digital data, from being copied.The insertion and analysis of watermarks to protect copyrighted material is responsible for the recent rise of interest in digital steganography and data embedding.

**Image steganography**

An image is a picture that has been created or copied and stored in electronic form. An image can be described in terms of vector graphics or raster graphics . An image stored in raster form is sometimes called a bitmap . An image map is a file containing information that associates different locations on a specified image with hypertext links.An image is a collection of numbers that constitute different light intensities in different areas of the image. This numeric representation forms a grid and the individual points are referred to as pixels (picture element).Greyscale images use 8 bits for each pixel and are able to display 256 different colours or shades of grey. Digital colour images are typically stored in 24-bit files and use the RGB colour model, also known as true colour . All colour variations for the pixels of a 24-bit image are derived from three primary colours: red, green and blue, and each primary colour is represented by 8 bits . Thus in one given pixel, there can be 256 different quantities of red, green and blue .

**Image Compression**

In images there are two types of compression: lossy compression and lossless compression. In Lossless compression,With lossless compression, every single bit of data that was originally in the file remains after the file is uncompressed. All of the information is completely restored.The most popular image formats that use lossless compression is GIF (Graphical Interchange Format) and BMP (bitmap file). lossy compression reduces a file by permanently eliminating certain information, especially redundant information. When the file is uncompressed, only a part of the original information is still there. In this case the resulting image is expected to be something similar to the original image, but not the same as the original. An example of an image format that uses this compression technique is JPEG (Joint Photographic Experts Group) .

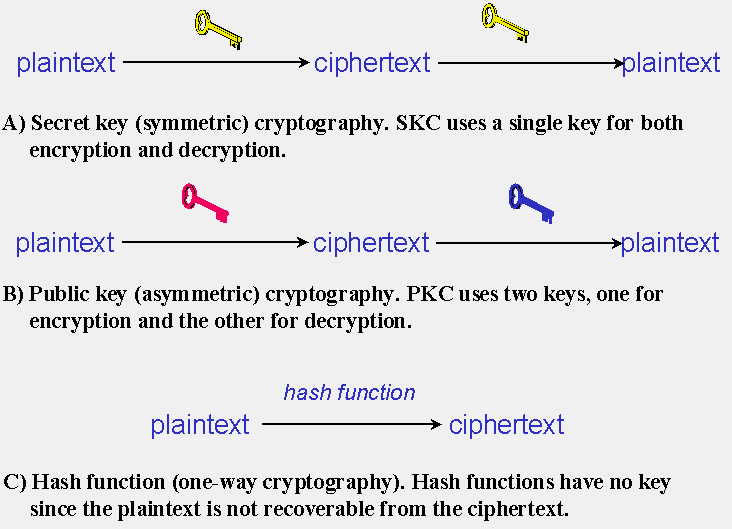
**Cryptography**

Cryptography the art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form . **Plaintext** - the original intelligible message n. **Ciphertext** - the transformed message. **Cipher** - an algorithm for transforming an intelligible message into one that is unintelligible by transposition and substitution methods . **Key** - some critical information used by the cipher, known only to the sender & receiver.

**Encipher (encode) -** the process of converting plaintext to ciphertext using a cipher and a key . **Decipher (decode)** - the process of converting ciphertext back into plaintext using a cipher and a key .**Cryptanalysis** - the study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key.

There are several ways of classifying cryptographic algorithms. For purposes of this paper, they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The three types of algorithms that will be discussed are (Figure 1):

* **Secret Key Cryptography (SKC):** Uses a single key for both encryption and decryption
* **Public Key Cryptography (PKC):** Uses one key for encryption and another for decryption
* **Hash Functions:** Uses a mathematical transformation to irreversibly "encrypt" information



**FIGURE 1: Three types of cryptography: secret-key, public key, and hash function.**

RSA Algorithm :-RSA algorithm is more secure cryptography algorithm. In cryptography we use two keys i.e; private key and public key.

Sender used public key to encrypt the message.

Receiver used private key to decrypt the message.

(1)Select P & Q (P & Q are two large prime numbers)

(2)Calculate the product of P & Q.

N=P\*Q

(3)Select public key .It is the factor of

Z= (P-1)(Q-1)

(4)1<e<Z

(5)(d\*e)mod Z = 1

(6)Encrypt C= m pow (e)mod n

(7)Decrypt C pow (d)mod n =m