**1. Steganography:** Steganography is a method in which secret message is hidden in a cover media. Steganography means covered writing. Steganography is the idea to prevent secret information by creating the suspicion. Steganography is less popular than Cryptography. In steganography, structure of data is not usually altered. The forms of steganography are:

**1.** Text

**2.** Audio

**3.** Video

**4.** Images

**5.** Network or Protocol

**2. Cryptography:** Cryptography means secret writing. In cryptography, sender does not send message directly to the receiver, before sending information to the receiver information or plain text is converted into cipher text by using some encryption algorithm then send to the receiver and receiver decrypt the cipher text into plain text to read the original information. It is of two types:

**1.** Symmetric key cryptography

**2.** Asymmetric key cryptography

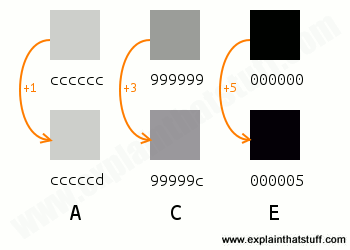
**1.** Symmetric key cryptography

2. Asymmetric key cryptography

**How does steganography work?**

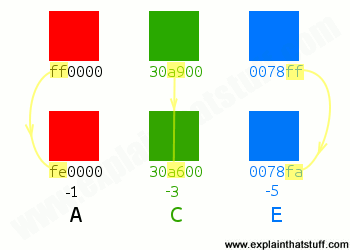
If you want to hide information in a picture, you can do it by subtly adjusting the color or brightness of each successive pixel (the squares that make up a digital image). That's barely noticeable to human eyes, but very easy for computers to detect.

Suppose the brightness value of a pixel is a number between 0 (black) and 255 (white). If you want to code an A, you could add 1 to the brightness of a pixel (since A is the first letter of the alphabet); if you want to code E, you would add 5; and so on. In that way, with very subtle adjustments to the brightness values, you could hide a whole string of text in an image: for example, if you changed the brightness of three successive pixels by 1, 3, and 5, you could invisibly send the code word "ACE." You can also hide one image inside another. If you're concealing information in music files, you take advantage of the way the [MP3](https://www.explainthatstuff.com/how-mp3players-work.html) algorithm (mathematical process) converts and compresses analog audio into digital form. In this case, your secret information is not only hidden but encrypted as well, so it's very hard to detect and decrypt.



*Artworks: How to hide the word "ACE" by changing the brightness or color values of pixels.*

Suppose I have an extremely simple picture made of just three pixels (top), which happen to be various shades of gray. In things like web pages, colors are represented by three pairs of two [hexadecimal](https://www.mathsisfun.com/hexadecimals.html) (base-16) codes, each made from the numbers 0–9 and the letters A–F. The first pair represents the red content of the pixel, the second pair the blue content, and the third pair the green content. In gray shades, the red, blue, and green values are equal. If I add 1 to the first pixel, 3 to the second pixel, and 5 to the third pixel, I get three new pixels that look virtually identical to a human eye (bottom). But if I compared the two images, or used a computer to subtract the color values, I could easily figure out that the difference between them is 1—3—5, representing the word ACE with a simple substitution code (A=1, B=2, C=3, and so on). It's a trivial example, but it illustrates the idea very clearly: I can hide information by changing the colors in an image so slightly that no-one would notice.



I can do the same thing in a slightly more complex way by changing the red, green, and blue part of each pixel separately. If I subtract 1 from the red value of the red pixel (FF−1 = FE), 3 from the green value of the green pixel (A9−3 = A6), and 5 from the blue value of the blue pixel (FF−5 = FA), I get three new pixels that, again, look virtually identical to the human eye, but still hide my secret message (ACE). This is slightly harder to detect than my simple brightness change because I'm hiding the code in a different "place" (a different part of the color value) each time. If you'd spotted and cracked the steganography trick I used in the black and white example, you wouldn't immediately be able to figure out what I'd hidden in the color example: I'm doing something slightly different this time!

# **What are the application of Steganography?**

Steganography is also represented as the art and science of hiding data by embedding messages within apparently harmless messages. Steganography works by restoring bits of useless or unused information in regular computer files. This hidden data can be plaintext or ciphertext and even images.

Steganography hides the covert message but not the fact that two parties are connecting with each other. The steganography procedure frequently includes locating a hidden message in some transport medium, known as the carrier.

The secret message is embedded in the carrier to form the steganography channel. The need of a steganography key can be employed for encryption of the hidden message and for randomization in the steganography design.

There are various application of steganography which are as follows −

**Digital Watermarking** − Digital watermarking is the procedure of embedding data into a digital signal in a way that is complex to delete. The signal can be audio, pictures or video.

For example, if the signal is copied, and then the data is also carried in the copy. A signal can carry several multiple watermarks at the same time.

**Visible Watermarking** − In this visible watermarking, the information is visible in the picture or video. Generally, the information is text or a logo which recognizes the owner of the media. When a television broadcaster insert its logo to the corner of transmitted video, and this is also a visible watermark.

**Invisible Watermarking** − In this invisible watermarking, information is inserted as digital data to audio, picture or video, but it cannot be perceived as such (although it can be possible to recognize that some amount of data is hidden).

The watermark can be pre-determined for extensive use and is therefore create simply to fetch or it can be a form of Steganography, where a party connects a hidden message installed in the digital signal.

In invisible watermarking, the goals is to connect ownership or other descriptive data to the signal in an approach that is complex to remove. It is also applicable to use hidden embedded data as a means of covert connection between individuals.

Digital Watermarking can be used for a broad range of applications including Copyright protection Source Tracking (there are multiple recipients have differently watermarked content). The numbers of possible applications for digital watermarking technologies are developing very quickly.

For instance, in the field of data security, watermarks can be used for certification, authentication, and conditional approach. Certification is an important problem for official files, including identity cards or passports.

Digital watermarks are generated by transforming copyright information into apparently random digital "noise" utilizing an algorithm that is imperceptible to all but special watermark reading application. So while a JPEG document that is read by an internet browser can display a good picture, that same file will show the copyright when read by the watermark application.

Encryption is the process of converting normal message (plaintext) into meaningless message (Ciphertext). Whereas Decryption is the process of converting meaningless message (Ciphertext) into its original form (Plaintext). The major distinction between secret writing associated secret writing is that the conversion of a message into an unintelligible kind that’s undecipherable unless decrypted. whereas secret writing is that the recovery of the first message from the encrypted information.   
