INFORMATION SECURITY PROJECT

**Submitted by:**

Aayush Gupta (9915103002)

Aksh Gupta (9915103003)

Nikhil (9915103018)

Paritosh (9915103021)



**Under the supervision of:**

Mr. Shariq Murtaza

Nov 2017

Department of CSE/IT

Jaypee Institute of Information Technology University, Noida

**ABSTRACT**

**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". Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the colour of every hundredth [pixel](https://en.wikipedia.org/wiki/Pixel) to correspond to a letter in the alphabet. The change is so subtle that someone who is not specifically looking for it is unlikely to notice the change. The advantage of steganography over [cryptography](https://en.wikipedia.org/wiki/Cryptography) alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which [encryption](https://en.wikipedia.org/wiki/Encryption) is illegal. Whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent as well as concealing the contents of the message.

**IMPLEMENTATION**

Data to be communicated is first read from a file and encrypted using Caesar Cipher. The encrypted data is then stored in an image. The ASCII value of each alphabet is stored at the red part of the RGB values of the pixel of the image. The image obtained after the process is stored and used for communication. The receiver uses the encrypted image to obtain the encrypted data. The value of the red part of a RGB pixel is converted into the character to get the encrypted message. The obtained message is decrypted and is stored in a file.

**CONCLUSION**

Steganography is beneficial for securely storing sensitive data, such as hiding system [passwords](http://searchsecurity.techtarget.com/topics/0,295493,sid14_tax299852,00.html) or keys within other files. However, it can also pose serious problems because it's difficult to detect. Network surveillance and monitoring systems will not flag messages or files that contain steganographic data. Therefore, if someone attempted to steal confidential data, they could conceal it within another file and send it in an innocent looking email.