

Steganography, which literally means “*covered writing*” differs from encryption in that while encryption uses cipher or code to protect or conceal the contents of a message by scrambling them before transmission, steganography works by concealing the very existence of the message. Clearly, detection of an encrypted communication between an unsavoury party (known terrorist or enemy agent) and a previously unsuspected person is going to put this person under suspicion. This is would be adequate reason for criminals to use steganography tools.

Simon Singh describes some historical methods of steganography in *The Code Book*. These included shaving the head of a courier, writing the message on his scalp and letting the hair grow; writing a message on a wooden writing tablet and coating it with wax. In later times, people would make pinpricks below certain words in a newspaper cutting and then mail the cutting to the recipient.

But nowadays, electronic methods of hiding information have evolved. At its core, electronic steganography hides or embeds a message inside another file which is called “cover image file” or “cover text”. Together, the two are called “stegotext”. Encrypting the message and then embedding it is common. Many programs are freely available on the internet that allows one to embed a text message inside a picture. The container file can be a text file, or a picture or audio/video file. Similarly the embedded message can also be a text or picture.

Here is how one common technique of hiding one image inside another image works. First, the image is represented in the RGB format, i.e., each pixel is represented as a (R, G, B) triple and there are three bytes per pixel. Changing the least significant bit has the smallest impact on the value of the 8-bit number (byte). Therefore if we embed an image in the least significant bit of each pixel of the container image, the changed value of each of the three bytes in the (R, G, B) triple will not change too much. Hence, the stego'd image (container image + embedded image) will not be visually too different from the original container image. To recover the hidden image, one performs the reverse operation, i.e., the stego image's least significant bits are used to re-construct the hidden image. The reconstructed image is degraded but sufficiently clear for many purposes. The following link explains it quite well.

<http://www.infosyssec.com/infosyssec/Steganography/techniques.htm>

To check if I understood the basic concept of electronic steganography, I wrote very simple, crude code to perform a do-it-at-home version of electronic steganography. The code is in MATLAB, a language well suited for the task at hand since it lets one perform bitwise operations very easily. I have used only the least significant bit but one could use the two least significant bits for the task.

One can see pictures of the [cover image](#), the [image that will be embedded](#), the [stego image](#) (cover + embedded image) and the [recovered image](#). The MATLAB [code](#) to do this also included.

Detecting the presence of hidden messages has also been the focus of much research. As the insertion percentage increases the statistical nature of the jpeg coefficients differs

from usual and this can be basis for detection. For example, it is known that in monochrome images, the entropy is usually between 4 to 6 bits per pixel. An image with an embedded message such that the observed entropy value observed is to have deviated from the usual by chance alone, is the basis of an approach. Some detection systems actually test the properties of least significant bits for departures from usual. Other approaches utilize knowledge of the statistical properties of JPEG images – certain transforms of an image are taken and chi-square tests on the resulting coefficients are performed. The resulting chi-square statistic indicates the probability of embedding.

What can we learn from a study of steganography? First, the least important places might make good holes to hide stuff. But as in any scheme of deception, once the adversary knows we might go for the least obvious approach, the least obvious will become the first place the adversary will look for. Secondly, what appears innocuous to the eye may actually be important; and we should rely on statistics rather than visual examination to guard against the possibility of deception - looking at charts to make investment decisions is dangerous. Paying attention to measures like entropy or moments can signal departures from the usual. And of course, deception might be particularly effective when its very existence is not suspected.

Saurabh