SECURE COMMUNICATION WITH STEGANOGRAPHY TECHNIQUES

Belarusian State University of Informatics and Radio-electronics
Minsk, Belarus

Seyyedamin Seyyedi

Professor: Ivanov N.N.

In the past people used hidden tattoos or invisible ink to transmit secret message. Today computer and network technologies provide easy to use communication channels. The difficulties in ensuring communication security become in network technologies increasingly challenging. Communication security is an application layer technology to guard any transmitted secret message against unwanted disclosure as well as to protect the data from unauthorized modification while in transit.

Encryption is a well-known procedure for secure data transmission. Another approach is steganography. The main advantage of steganography over cryptography is that, messages do not attract attention to hackers. Steganography is the art of hiding information into digital image, text, audio, video and etc. In steganography secret message (text or image) is the data that the sender wishes to remain confidential. The cover or host is the medium in which the message is embedded and serves to hide the present of the message. Figure 1 is shown the steganography structure.

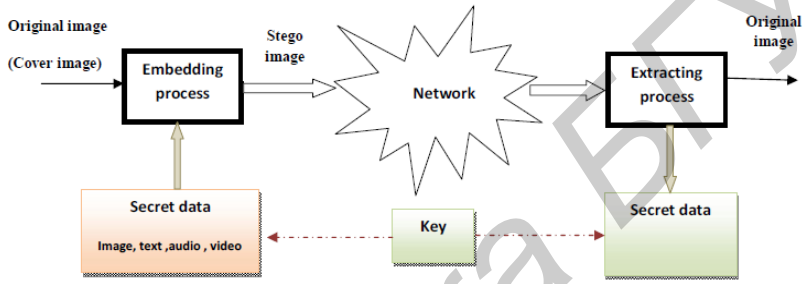

Figure 1 steganography structure

The steganography techniques are mainly classified as spatial domain techniques and transform (frequency) domain techniques. In the spatial domain approach, the secret message is embedded directly into intensity of image pixels of cover image. Least Significant Bit (LSB) based hiding strategies are most commonly used. It is simple to implement, the high hiding capacity and provides a very easy way to control stego image quality. But the limitation of this approach is vulnerable to every slight image manipulation. Frequency domain approach which appeared to overcome robustness and imperceptibility problems found in LSB and more robust to signal processing operation such as filtering operation and image compression. In this approach the cover image and /or secret message are converted into frequency domain and the secret message is embedded into the some coefficient of cover image to derive stego image. The various transform domain techniques are Fast Fourier Transforms (FFT), Discrete Cosine Transforms (DCT), and Discrete Wavelet Transforms (DWT).

There are three aspects to be considered when designing a steganography system :(i) Invisibility: Human eyes cannot distinguish the deference between the original image and stego-image (the image with confidential data). (ii) Capacity: amount of information that can be hidden in the cover image. Large embedded data usually degrade the image quality significantly. How one can to increase the capacity without ruining the invisibility is the key problem. (iii)Robustness: The embedded data should endure any reprocessing operation that cover may be subjected to and still remain intact.

The adaptability of the human visual system is advantage in wavelet transform. . In DWT, time domain is passing through low pass and high pass filter to extract low and high frequencies of the input image. The input image decomposes in four sub bands. This process is repeated for several times and each time a frequency section of the signal is drawn out. The two level wavelet decompositions are shown in figure 2.

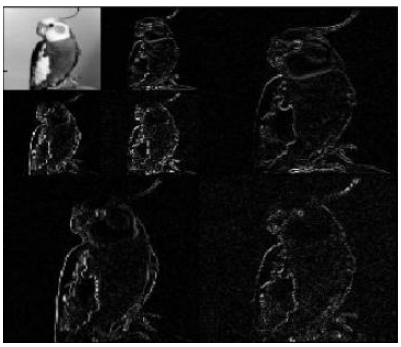

Figure 2 two level wavelet decompositions

The stenographer can to embed secret message in each sub bands. One of the major discoveries of this investigation was that each Steganography implementation carries with it significant trade-off decisions, and it is up to the stenographer to decide which implementation suits him/her best. Below, advantages and disadvantages to some Steganography techniques are discussed.

Table 1 Comparison some steganography techniques

Technique	Advantages	Disadvantages
Least Significant Bit (LSB) Encoding	Easy to detect. Original image is very similar to altered image. Embedded data resembles Gaussian noise.	Message is hard to recover if image is subject to attack such as translation and rotation.
Low Frequency Encoding	Hard to detect as message and fundamental image data share same range.	Significant damage to image appearance. Message difficult to recover
Mid Frequency Encoding	Altered image closely resembles original. Not susceptible to attacks such as rotation and translation	Relatively easy to detect
High Frequency Encoding	None	Message easily lost if image subject to compression such as JPEG

References:

1. Сейеди С.А , Садыхов Р.Х // Сравнение методов стеганографии в изображениях , Информатика , Беларусь, 2103-37,66,75 p.
2. Seyyedi S.A, Sadekhov R.KH // Digital image steganography concept and evolution, International Journal of Computer Applications, USA, 2013- 66, 17,23 p.
3. Iwata M, Miyake K and Shiozaki A // Digital steganography utilizing features of JPEG images, IEICE Transfusion Fundamentals, 2004- 4, 929,936 p.
4. Stephan M.G // a theory for multiresolution signal decomposition: the wavelet representation, IEEE Transaction on pattern analysis and machine intelligence- 11, 1980,674,693 p.