Modern Steganography

Johann Barbier
Centre d'ÉLectronique de l'ARmement
Département de Cryptologie
BP 57419, 35 174 Bruz Cedex, France.
johann.barbier@dga.defense.gouv.fr
Associated researcher at ESIEA
Laboratoire de Cryptologie et Virologie Opérationnelles
38, rue des docteurs Calmette et Guérin, 53 000 Laval, France.

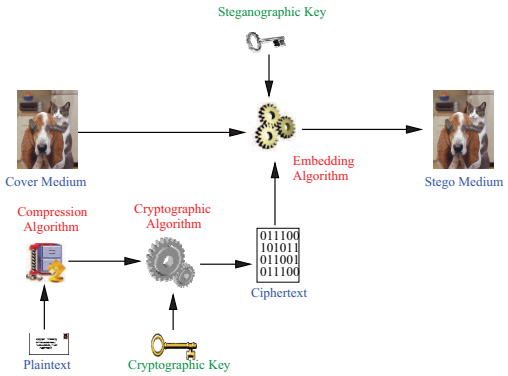
1 Introduction

As ancient as cryptography, steganography takes its roots in the antiquity. Whereas the former enables confidential communications, the latter provides invisibility. With the popularization of the Internet, steganography has become accessible to everyone. In the same time as the development of steganography tools, the scientific community got itself organized in the middle of the 90's and now proposes advanced steganography schemes but also advanced detectors. Nevertheless, the huge amount of media available on the Internet gives the opportunity to the steganographer to send stego media that are quasi-undetectable by analyzers.

In 1983, G.J. Simmons laid the foundations of modern steganography and introduced the concept of *subliminal channel*. To illustrate it, he drawn on the *prisoner's problem*. Alice and Bob are two prisoners who communicate thanks to the warden, Wendy. If Wendy suspects them to set up a plan to escape, she sends them to high security jails. If Alice and Bob use cryptography for communication security (COMSEC), Wendy will notice it and may force them to disclose their secret key. Their only way to communicate securely is to send an innocuous message and embed the compromising information in it. The transmission channel is no more visible by Wendy; it is a *subliminal channel*. Steganography extends classical techniques of transmission security (TRANSEC) to any kind of data.

2 Modern steganography

To send Bob a message, Alice first compresses it, keeping in mind that the longer the message is, the easier Wendy detects it. Moreover, Alice wants to guarantee the confidentiality of her message even if it is detected; so she encrypts the plaintext. Then, she embeds the ciphertext in an innocuous cover medium. She randomly selects positions, according to a secret stego key and a Pseudo-Random Number Generator (PRNG) and inserts the ciphertext at these positions.



Steganography scheme

The steganography scheme is symmetric. Bob retrieves the ciphertext by selecting the positions according to the secret stego key and the PRNG and "reads" it at these positions. The ciphertext is then decrypted and uncompressed. Each steganography scheme is entirely determined by its way to "write" the message in the cover medium. The embedding algorithm depends on the format of the cover medium (pictures, sound, video, html, text, *etc* ...) but also on the personal experience of the steganographer (LSB, $+/-k$, spread spectrum steganography, *etc* ...).

For a non compressed image coded with 24 bits, each pixel is defined by 3 bytes.

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)
!

To embed the binary stream 10000011 we use the Least Significant Bit of each byte.

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)
!

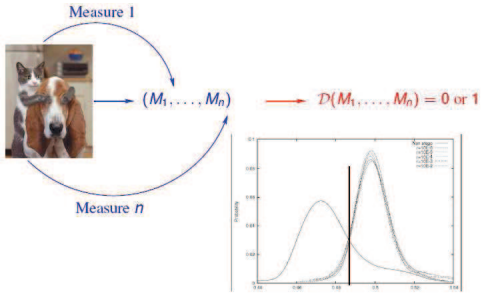
LSB steganography adapted to non compressed pictures

Some rules must be respected to correctly use steganography. First, Alice must generate her own cover medium, use it only once and finally destroy it after using it. Otherwise, a simple comparison with the original medium reveals that at least one of the two contains hidden data. The secret message should be encrypted before embedding. Indeed, embedding algorithms work under the hypothesis that hidden texts are random. The detection rates of the attacks increase when the payload increases. Hence, the (compressed) message must be as short as possible (with compression) and eventually must be splitted in small parts and be hidden in different media.

3 Technical stakes

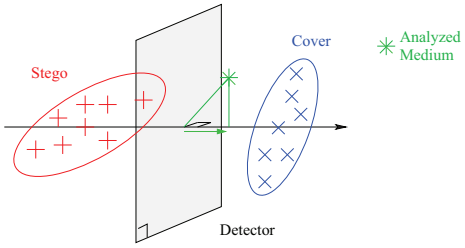
To have access to the information exchanged by Alice and Bob, Wendy has first to detect which medium contains the hidden data. Then, she has to extract the ciphertext and finally to cryptanalyze it. This is a complete breaking scheme. In steganography, models of security only consider adversaries who answer the following question. Given an unknown medium, "*Is the medium is a stego one or not ?*". To achieve this, most of techniques are statistical ones.

The adversary computes n measures on the analyzed medium. Each of these measures can be considered as a random variable. If the adversary is successful, at least one probability law or one marginal probability law associated with the measures is not the same when the measures are processed on cover media and when they are processed on stego media. In that case, he is able to calibrate a detector, *i.e.* a two-classes classifier, which outputs 0 for cover media and 1 for stego media.



Statistical analysis of a medium

To calibrate a statistical detector, we process the following steps. First, we compute the n measures for a set of cover media and a set of stego media. These n measures define a vector associated with a medium in a n-dimensional space. In this space, different statistical approaches (Fisher Analysis, Support Vector Machines, *etc*...) output the equation of a surface which separates at best the group of vectors associated with stego media and the group of vectors associated with cover media. Finally, when we analyze a given medium, we compute the associated vector. If this vector is in the same side of the surface as the group of cover media, then the detector outputs 0 and it ouputs 1 otherwise.



Conception of a linear statistical detector for 3 measures

The statistical techniques are very limiting for forensics applications. Indeed, let us consider that Alice embeds in a same cover medium an innocuous message with a key K_1 and a compromising one with a key K_2. If the medium is detected as a stego one by a detector, she may be constrained to reveal the hidden text. In that case, Alice may reveal K_1 and so the innocuous hidden text and the detector is unable to say if there is more than one hidden text in the medium. The doubt benefits Alice. For very specific steganographic schemes, some powerful analysis succeed in estimating the amount of hidden data in a medium. Such techniques are very few but defeat Alice's strategy. In the previous context, giving K_1 does not reveal enough hidden data.

4 Conclusion

Modern steganography schemes provide a complementary goal of security for the privacy of digital data: The TRANSEC. The global security of steganography techniques is composed of a security level against detectors, the security of the extraction which is equivalent to exhaustively search the steganographic key and finally, the classical cryptographic security. The experience shows that the steganographer can choose to spend more time during the embedding step so that the detection security is improved, whereas the accuracy of detectors does not increase with the time. Moreover, the Internet provides a huge amount of data of a given format and for each format of cover media, many specific steganography schemes exist. The fight between steganographers and steganalysts appears to be unequal in favor of steganographers while steganalysts are looking a needle in a haystack.