CRYPTOGRAPHY AND STEGANOGRAPHY, METHODS TO HIDE INTELLIGENCE PRODUCTS

Major Adrian IVAN, PhD student*

Abstract: *Intelligence plays a very important role in supporting decision-making. Once intelligence has been collected, it must be sent as quickly as possible to the decision-maker, but prior to transmission, the intelligence product must be encrypted, hidden from view. Well-known and widespread techniques by which intelligence is manipulated for the purpose of encoding/encryption and hiding its existence are cryptography and steganography.*

Keywords: *intelligence; cryptography; steganography; key; code; encrypted message.*

Intelligence plays a very important role in supporting decision-making, always aiming to ensuring intelligence superiority. The quality of the decision is given by the quality of the available intelligence. The decision moves the force to fulfill the purpose, and can be characterized by a high or a low risk in terms of success or cost of operation. The decision based on timely information, both in terms of quality and time, ensures success under minimal risk conditions and to a minimal cost.

The informational activity, consisting of the succession of the organizing and execution activities, is carried out to „know" the operational environment, using its own resources, using the intelligence system and is concretized through an intelligence process. A classical intelligence process includes the following stages[1]: planning, collecting, processing, analyzing and disseminating intelligence products.

Once intelligence has been collected, it must be sent as quickly as possible to the decision-maker, but in order to keep the secret, it can not be delivered „*clearly*". Prior to transmission, intelligence product must be encrypted, hidden from view. Well-known and widespread techniques by which information is manipulated for the purpose of encoding/encryption and hiding of its existence are cryptography and steganography.

The purpose of this article is to highlight that cryptography and steganography are methods by which intelligence collected from different sources can be concealed and transmitted.

In the following lines, to understand the role of cryptography and steganography, I will present a brief history of their appearance, how information can be conveyed „hidden" through them, and a radiography of the main differences between the two methods.

Cryptography has followed man over the stages of evolution, dating back to 1900 BC, for example in ancient Egypt, when scribes used a non-standard hieroglyphic inscription. Between 500 and 600 BC Hebrew scribes used Atbash[2], a simple encryption solution based on the inverted alphabet.

During the long history of cryptography, steganography has developed and bloomed, the first steganographic technique being documented in ancient Greece, around 440 BC. The Greek leader Histaeus used a version of steganography that involved the use of human scalp as carrier object of the secret message: tattooing the message

[1] FM 2-0, *Intelligence*, Department of the Army, Washington, May 2004, USA, p. 4-1.

**** "Carol I" National Defense University***
Ministry of National Defense, Romania
e-mail: iandust77@yahoo.com

[2] The Atbash cipher is a particular type of monoalphabetic cipher formed by taking the alphabet and mapping it to its reverse, so that the first letter becomes the last letter, the second letter becomes the second to last letter, and so on.

on a slave's scalp after having previously removed his hair, waiting for a period of time for hair to grow and hiding the secret message, and sending the slave to the recipient of the message, who knew where to look, and doing the same to respond to the sender.

On the same epoch, another ancient form of steganography was often utilised. Demerstus, who wrote a message to the Spartans warning them about the imminent invasions of Xerxes, was a exponent of this method. The message was engraved in the wood of a wax tablet, and then covered with a fresh wax layer. This apparently empty, unwritten tablet was successfully sent.

Nowadays *„cryptography defines the art and science of transforming data into a seemingly random and unintelligible bit sequence for an observer or an attacker*[3]*"* while *„steganography is the practice, or better said the procedure of hiding or rendering a secret message, image or other file type in another message with different digital extensions, such as a self-image or video, files or applications with different endings – extensions*[4]*"*.

In my opinion cryptography consists in distorting the message in such a way that it cannot be understood, while steganography consists in concealing a message so that it cannot be seen. Even though both methods provide information security, there are attempts to combine the two methods into a single system for better privacy/ secrecy and security.

I consider that steganography and cryptography differ in the way how they are evaluated: cryptography fails when the „*opponent*" is able to access the contents of the encrypted message, while the steganography fails when the „*opponent*" detects the presence of a secret message in the steganographic environment.

The disciplines that study decryption techniques of encrypted messages and hidden messages detection are called cryptanalysis and steganalysis. The first is the set of methods for obtaining the meaning of encrypted information, while the second is the art of discovering hidden messages.

In the process of gathering and transmitting intelligence to the recipient, *cryptography* is considered to be an important element of any strategy designed to ensure security requirements in message forwarding. Cryptography allows the information to be conveyed in a hidden form so that only the right recipient can discover and read the message. It is practically the art of transforming messages or data in a different form so that no one can read them without having access to the „*key*".

The message can be converted using a „*code*" (in which case each character is replaced by another) or a „*cipher*" (in which case the entire message is converted). Cryptology is the science behind cryptography. Cryptanalysis is the science of discovering („*breaking*") the encryption scheme, for example, the discovery of the decryption key. Cryptographic systems are generally classified in relation to three independent dimensions/concepts:

1. The methodology of transforming a clear text in an encrypted text. All encryption algorithms are based on two general principles: the substitution, in which each element in the clear text is replaced by another, and the transposition, in which elements in the clear text are rearranged. The fundamental requirement is that no information be lost.

2. The methodology of using a number of secret keys. There are some standard methods[5] used in cryptography, such as secret key, public key, digital signature, and more.

- The secret key (symmetric). Secret key cryptography involves the use of a single key for both encryption and decryption. The sender uses the key to clearly encrypt the text and sends the text to the recipient. The receiver applies the same key to decrypt the message and discover the text in clear. Since one key is used for both functions (encryption and decryption), this encryption method also carries the name of symmetric encryption.
- The public key: public key cryptography was said to be the most important improvement in cryptography over the last 300-400 years. Modern public key cryptography was first publicly described by Professor Martin Hellman and his associates, in 1976. Their study described a two-key encryption system, in which two parties could engage a secret communication act over an unsafe communications channel, without having

[3] Joseph Raphael, Dr. V. Sundaram, „*Cryptography and Steganography – A Survey*", Int. J. Comp. Tech. Appl., Vol. 2 (3), p. 628.

[4] *Ibidem*, p. 629.

[5] Emil Simion, David Naccache, Adela Mihăiţă, Ruxandra Florentina Olimid, Andrei George Oprina, *„Criptography and Information Security"*, Matrixrom Publishing House, Bucharest, 2012, p.27.

to provide a secret key[6].

- Digital signature. Its use has come from the need to ensure authentication. The digital signature is more related to the stamp or signature of the issuer, which is encrypted with the private key along with the useful information, so that it can be transmitted to the correspondent. In addition, the digital signature ensures that the correspondent easily detects any changes made to the encrypted data.

3. Methodology of clear text processing.

steganography is to hide messages inside other harmless messages, in a way that does not allow detection of the fact that there is still a second message.

Once collected, the intelligence can be hidden and transmitted according to certain standard steps. The basic steganography model includes: the carrier, the message, the insertion/detection algorithm and the steganographic key. A model of the steganographic process for sending intelligence is presented in figure no. 1.

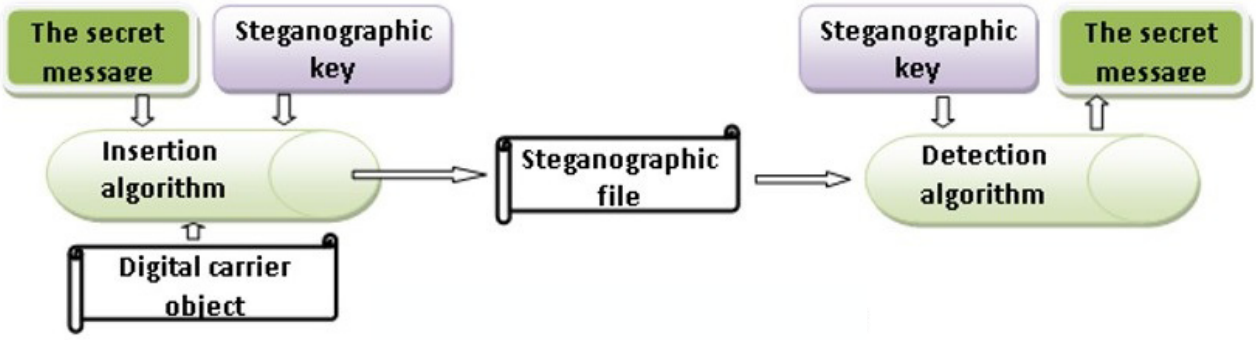

Figure no. 1. The steganographic process

A block encryption module processes one block of input elements at one time, making one corresponding block of elements at the output of the module. A flow encryption module processes the input elements continuously, producing individually processed items as they occur.

Regarding steganography, its main purpose is to communicate safely in a completely undetectable manner and to avoid creating suspicions about the transmission of hidden data. Specific to this method is that during the process there are changes in the structure and characteristics of the hidden data carrier, so that they cannot be identified with the naked eye.

In my opinion images/photos, video, audio, and other types of electronic files containing information that can be perceived as irrelevant or redundant can be used as „*masks*" or carriers of secret messages. After inserting a secret message into a cover-file, a so-called stego-file is obtained.

Thus, in my opinion, the purpose of

The usefulness of the process of transmitting information using steganography is influenced by the following three aspects: capacity, security and robustness.

Therby the capacity refers to the amount of information that can be hidden in the carrier object/medium. Security is closely linked to the impossibility of unauthorized persons („*curious*") to detect the existence of any message in the digital carrier (stego-file). Robustness lies in the level of changes the steganographic environment can endure before the opponent can destroy hidden information.

There are several types of steganography techniques, such as the steganographic system, the bit of substitution techniques, hide & seek: sequential approach, hide & seek: random approach and domain transformation technique. The field of informatics/IT is a complex one that changes from day to day and it can be said that new algorithm techniques are being introduced on a daily basis by changing at least a value in terms of steganography, but also other types of computer encryption.

As we can easily tell, current trends in the development of modern steganography techniques is

[6] Martin Edward Hellman, Whitfield Diffie and Ralph Merkle, „*New Directions in Cryptography*", Transactions on Information Theory, Vol. IT-22, No. 6, November 1976, USA.

using the twentieth-century inventions – computers and computer networks. Four main trends in the development of so-called digital steganography can be distinguished: digital media files steganography, linguistic steganography, system file steganography, and network steganography[7].

Recent developments in steganography, closely related to the pace of development of information and communication technologies, have resulted in its increased and diversified use as follows:

- Using „*craft*" files (small-size text files that can easily be distributed over the network) to hide some instruction messages;

- Print-steganography, „*data hide in data*", a technique developed by manufacturers of laser printers that adds to each printed page yellow dots that are imperceptible to the naked eye, representing the encoded form of machine/printer identification data and the print job moment;

- The use of photo-sharing web sites, some photos carry parts of secret messages that can only be rediscovered after having a number of appropriate photos;

- Microbial prints. Researchers at William Howard Tuft University have shown that it is possible to conceal information using bacteria with fluorescent capabilities. For example, certain strains of the genetically modified E-coli bacteria can shine in one of the seven specific colors when placed in a supportive growth environment;

- Malware, computer worms, or other malware information software started to use steganography to get functional commands or to perform unauthorized data transfers. Computer control instructions can be placed in HTML or JPEG files;

- Computer games. There is a suspicion that network/multiplayer games can be a good cover for hidden communications. Private chat rooms are not the subject of network monitoring, so they can be easily used as a meeting place for people with hidden intentions. For example, using PlayStation and Xbox you can communicate without being supervised (starting 2012).

In my judgment the modern steganography techniques follow the use of communication methods by circumventing common monitoring systems/activities, this being possible, as the variety of steganographic carriers is continually expanding.

Given the relatively small complexity of implementing this method, it is expected to remain a preferred mean of hidden communication.

In addition to what I have described above, I will present a comparative analysis of the two methods, with the common aspects and the differences between them.

Thus, in my opinion, the main difference between steganography and cryptography is that steganography protects the message by hiding it to other readers other than the container which it is addressed, instead of the cryptogram that displays all the information encrypted, which, however undisputable, attracts attention and curiosity.

At the same time steganography, unlike cryptography, requires the existence of surrogate data to be used in order to transmit and host the steganographic message. Regarding the choice of surrogate data, this can be done using the specific structure of some file formats or the architecture of data transmission protocols over the network.

A common example of surrogate formats for transmitting information gathered from various sources are media formats for storing images, sounds, or movies. Because of their considerable size, they can easily conceal messages without suspecting the changes.

In my opinion, the files chosen as a surrogate for hidden messages must meet the following conditions: to be as complex as possible, to present hatches or ways of inserting messages and to occupy considerable dimensions, in order for nobody to notice the insertion of some hidden texts.

Therefore, the common purpose of steganography and cryptography is to ensure secret communication. Steganography has until recently been a variant of performing a somewhat neglected secret communication, unlike cryptography whose evolution/development has been constant. At present, steganography is becoming more and more popular and develops directly in line with the pace of development of information technologies and the growing need to conduct communications with maximum confidentiality in the virtual environment.

[7] Elżbieta Zielińska, Wojciech Mazurczyk, Krzysztof Szczypiorski, „*Development Trends in Steganography*", Warsaw University of Technology, Warsaw 2012, Poland, p.00-665.

On the other hand, although the purpose of the two methods is common, they must not be mistaken, with the above definitions clearly showing the differences between them. Also, the methods of „*breaking*" the two systems are different.

In cryptography, the system is considered to be „*broken*" when the attacker can read the secret message, while in steganography the attacker must detect that steganography has been used and read the inserted message. In addition, the security of the classic steganographic system is based on the secrecy of the data encoding system. Once this system is known, the steganographic system is considered defeated. The distinction between cryptography and steganography is very important and is synthesized in the following table:

Steganography	Cryptography
Unobserved passage of the message	The passage of the message is visible
Prevents discovery of any form of communication	Prevents discovery of the content of a communication by an unauthorized person
Less known technology	Common / known technology
Technology still in development for some formats	Most algorithms are generally known
Once detected, the message can be read	The very strong current algorithms are resistant to attack, with higher computing power (and, implicitly, higher cost) needed to "break"
It does not affect the structure of the hidden message	It alters the structure of the secret message

Even if each of the known methods, used individually, offers good security, the application of several security levels to a protected object is always a superior security solution, as well as a good practice in the field.

A multi-level security solution represents the combined use of steganography and cryptography, termed crypto-steganography. By combining them, it is possible to encrypt data with software and then insert encrypted text into a carrier file (text, video, audio, images, etc.) using a keyhole.

Transmitting intelligence by combining the two methods will enhance the security of the inserted data. This combination will also meet requirements such as capacity, security and robustness in securing data transmitted through an open channel, and beyond.

A graphic representation of the combined concept of steganography and cryptography is presented in figure no. 2.

The Stego-file resulting from the combined crypto-steganography method can be transmitted without discovering that there is actually a secret information exchange. Moreover, even if an

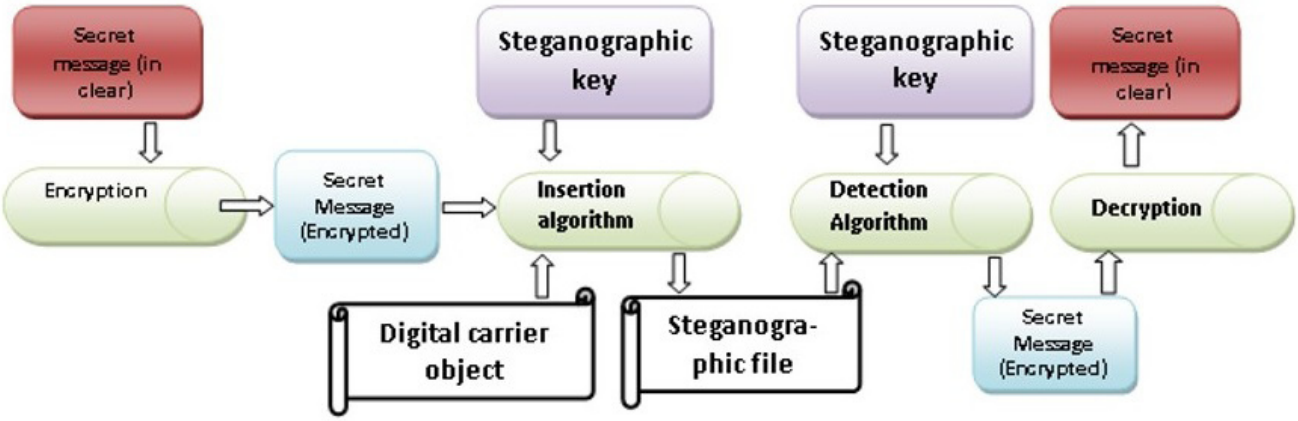

Figure no. 2. The crypto-steganographic process

attacker would pass the steganographic barrier to detect the message in the carrier file, he would also need the key to decrypt the encrypted message.

This solution of combining the two methods of hiding information has created new approaches to steganography, which can be divided into three types:

a. Simple steganography – technique that only uses a carrier object to conceal a clear message.

b. Secret key steganography – where the combination of cryptographic secret key technology and simple steganography is used. The idea of this type of approach is to encrypt the secret message with the secret key and conceal the resulting (encrypted) message into the carrier file.

c. Public key steganography – represented by the combination of the public key cryptography method with the simple steganography method. The idea behind this approach is to encrypt the secret message with the public key and to hide the resulting (encrypted) message in the carrier file.

I can conclude that through the cryptography and steganography the information collected from various sources: SIGINT (*Signal Intelligence*), IMINT (*Imagery Intelligence*), HUMINT (*Human Intelligence*) and OSINT (*Open Source Intelligence*)[8] can be quickly transmitted to a beneficiary without suspicion .

Also, in my opinion, the development trends of information hiding methods are in line with the increasing importance of preserving the confidentiality of information by most of the sectors of the current society, but are also imposed by its fast pace of development.

However the speed at which information can now be transmitted over the information and communications networks has put this communication medium first in the choices of society as a whole.

The information to be transmitted takes all possible forms, but those covered by this article are those that have a certain level of confidentiality required or imposed by the sending/receiving tandem in a legal, institutional, and organizational manner. This has led to the need to innovate/ develop methods of concealing information in line with the level of development of information technology, these methods being mainly applied to open communication channels, but their use can still be extended to computer networks and private communications, even if it may appear as a redundant solution.

[8] AJP 2.0 *Allied Joint doctrine for Intelligence, Counterintelligence and Security*, p. 1-2-5.

BIBLIOGRAPHY

1. *** AJP 2.0, *„Allied Joint doctrine for Intelligence, Counterintelligence and Security"*, 2003.
2. Berg, George; Davidson, Ian; Duan, Ming-Yuan and Goutam, Paul, *„Searching For Hidden Messages: Automatic Detection of Steganography"*, Computer Science Department University at Albany, Washington, USA.
3. FM 2-0, *„Intelligence"*, Department of the Army, Washington, May 2004, USA.
4. Groza, Bogdan, *„Introduction to Cryptography, Cryptographic Functions, Mathematical and Computational Foundations"*, Politehnica Publishing House, 2012.
5. Hellman, Martin Edward;Whitfield, Diffie and Merkle, Ralph, *„New Directions in Cryptography"*, Transactions on Information Theory, Vol. IT-22, No. 6, November 1976.
6. Konheim, A., *„Computer Security and Cryptography"*, Wiley Interscience, 2007.
7. Joseph, Raphael; Sundaram, V., *„Cryptography and Steganography – A Survey"*, Int. J. Comp. Tech. Appl., Vol 2 (3), USA.
8. Rausch, Peter; Sheta, Alaa; Ayesh ,Aladdin, *"Business Intelligence and Performance Management"* Theory, Systems, and Industrial Applications, Springer Verlag U.K., 2013.
9. Rațiu, Crina Anina, *"Optimization and Security of E-Business Systems"*, PhD thesis, Cluj-Napoca, 2016.
10. Zielińska, Elżbieta; Mazurczyk, Wojciech; Szczypiorski; Krzysztof, *„Development Trends in Steganography"*, Warsaw

University of Technology, Warsaw 2012, Poland.
11. Simion, Emil; Naccache, David; Mihaiţă, Adela; Olimid, Ruxandra Florentina; Oprina Andrei George, *„Criptography and Information Security"*, Matrixrom Publishing House, Bucharest, 2012.
12. Wayner, P., *„Disapearing Cryptography - Information Hiding: Steganography & Watermarking (Second Edition)"*, Morgan Kaufmann Publishers, 2002, USA.