MULTIMEDIA AND CRYPTOGRAPHY

Dorin Iordache

Eng, IT Departament, Romanian Navy Staff,
Bucuresti - Ploiesti Av., 13.5 Km, Bucharest
e-mail: dorin.iordache@fortele-navale.ro,

Abstract: In computer's world is a permanently care of preserving secret an information, to hide an individual information or to preserve the author's right over the respective data. To be complete this desideratum that in the time catches new dimensions and difficulty grades, appear new methods base in principal on the stenography principle who was been developed and improve.

Keywords: information technologies, criptography, steganalys, multimedia.

1. INTRODUCTION

The principal object of the stenography is to incorporate in an original (clear) form inside of others data. When I think at an information (in an original form) I have in clear the message (data, information) who must be persevering in secret.
The cryptography's object is to imprint an undecipherable character of certain information in clear. The stenography has as an object to hide of the existent and original data, the information in clear. If an outsider is able to find the hide data, then the stenography method that was utilized has failed.
In many cases, in practice, the stenography is use in combination with the cryptography. For example, trough the crypt of the data, before they are hides in a picture, they use the cryptography technologies in order to decide were will bee hide the information. Trough those methods the analysis process became hard.
The hide of some information is one of the most utilized method of the stenography. Same method can be use with the scope to watermark certain information, for example: a melody, a film, a picture, etc. The musical or the film's industry are permanent concerned for the protection of the personal benefits, trough the property right over the multimedia information.
To be complete this cryptography, the stenography's techniques are often use for watermark the data against the piracy.
The watermark constituted a subject of preoccupation for the stenography attacks, too. In reality, the secret date in the watermark setting it must not be detected, it must be eliminating.
The watermark who can be easily eliminate without to affect the date quality who was enclosed can be consider as a failed of the stenography

2. THE INFORMATION HIDES

In our days the communications are realized trough the help of some progressive technologies (e-mail, office system, etc.). The kipping secret some information like this must be taking in care for its save and protection.
The cryptography can be apply to the message communications, but sometimes the send message have reduce dimensions and the crypt/decrypt process as well as the keys transfer became much complicate. In this case, a solution is the existent hide of this message, "watermark".

To go on, I will present some aspect of the information's hidings in the sound and picture file setting.
I will use the next terms: file/data logging MHF (Multimedia Host File) and file/data hide MWF (Multimedia Watermarked File).
File/date logging MHF is represent by the non-modification file, were will bee hide the information content by the clear message M. File/data hide MWF represents the file which contains the message who want to be kept in secret.
In the computer's world (we) will find an abundance of format files. From the data content by an unformatted diskette, to the performer files, the files who content pictures, encode data, compact data, sound files, etc. All these are examples for some kind of data which it can be found without classification in some way. Those kinds of files represent exactly medium that needs stenography man to hide the data.
This stenography communication can be imperceptible for a cryptography man exactly thanks to these aleatory structures of data. If the hide data look as they are aleatory and enclosed the information without affect his aleatory structure, then (we) can talk about stenography.

2.1. Picture files

The existent data in a picture file are very aleatory and that brings us to the idea of using those files for stenography. That why it is welcome. Any octet of data who is enclosed in a picture file designate the color cod for each pixel, or group of pixel. The each octet can content any kind of value, so we can say that it has an aleatory structure.
Trough the change of the low significant bit (LSB) of any octet content by the picture file, this became imperceptible modification for the human eyes that looks at the picture.
In this way, we have a system which can hide information inside of a picture file. Because we can use just a single bit, LSB, the message hides in a picture file has a dimension very good determined that can't pass. From the simple estimation, trough that for any octet from MHF we can hide just one bit from MWF, result a rate of 1 MHF at 8 from MWF.

Bit	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
octet	1								2								3							
MHF	1	0	1	1	1	1	0	0	0	0	1	1	0	1	0	0	1	1	1	1	0	0	0	1
XOR								⊗								⊗								⊗
M								0								1								1
MWF	1	0	1	1	1	1	0	**0**	0	0	1	1	0	1	0	**1**	1	1	1	1	0	0	0	**0**

The operation rule XOR (or exclusive) as is describe below.

A		**B**		**C**
0	⊗	**0**	=	**0**
0	⊗	**1**	=	**1**
1	⊗	**0**	=	**1**
1	⊗	**1**	=	**0**

- The above process can be use with the information content in message M.

This report it doesn't mean to much if we think that inside a file MHF of 128 octets will hide 128/8 = 16 octets from MWF. All this is happening when we want to keep visible the original picture. Too much modification of MHF will generate a diffuse picture with distortions or other unexpected effects. This shortcoming can constitute a sign of present stenography man action and can be explored by a cryptography man.

It's presuming the next scenario:

Data in:

- MHF, is a .BMP file, picture dimensions 320/480 pixels and his length 153600 octets. This is the effective aria of information's hide, which is less than the total dimension of file, because it must be eliminated the bites of file antet. As a result, we can store in this file 153600/8=19200 bites (characters) of information, approximate 19 Ko.
- The message which has to be enclose, M. Let's suppose that is a file of 2502 bites.

Data out:

- MWF is the MHF that has any bites LSB of each modified octet and content hide information.

The process utilized:

- In the first 32 bites of the file MHF, in the aria of the affective data trough the modifications of any LSB, it will be stored the message dimension M. In this way it can be stored a message which has the maximum length equal with 2^32=4.294.967.296 bites/8 = 536.870.912 characters.
- In the same way we must hide the insertion of those information using an extern crypto process or to realizing a logic operation at the same level of a bite between the modification bite and the second bite from the 32 bites setting, as follow for example:

The problem which is appearing in this situation is represented by the dispersion of the message's bites content M, produced by the increasing the dimension of the picture file. If the hider is load with large quantities of the proportion 1 bite at 1 octet, then the resulted picture can have distortions, light spot of other colors, etc. All this can constitute indicators of the stenography proceedings. So, the most helpful in hide of information in a picture file is using black-white pictures. In this way it's touched a good threshold of maximization the security.

2.2. Sound files

As I presented before, the sound file can be use for the information hide, too. Trough their nature, the sound files can't be correctly indentificate if we look for the exactly value of the signal octet which content. This fact allow a big commodity in those files use for the hide of data, namely the sound files have an aleatory structure.

In order to experiment this theory, I created a personal application where I used an audio file in formatting WAV on post of MHF where inside it are hide the information. The file MHF can have the audio signal structure, on 8 or 16 bites in function of the play-back kind on the sound disk, respective mono or stereo.

If it is used the same algorithm as the picture files we can replace one bit of message M at the all octet from MHF so will obtain a good hide of the information, but a reduce quantity. In the experiment that I realized, I used the replaces to the level of one message's octet M till one octet of MHF, with the following observation: in case of stereo message the sound is represented by 2 octets. If it's replace the low significant octet, the modification isn't major and imperceptible to the human ears, practically, the modification of the respective octet is imperceptible.

The disadvantage of this replace at the octet level is represented by the "visibility" of replacing that octet just when is make analyzes at a logic level of the file.

Trough the combination with cryptographic algorithm and an aleatory relative disposing, after an algorithm before established, it can be heavy the proceeding in determination of the message M content, in clear.

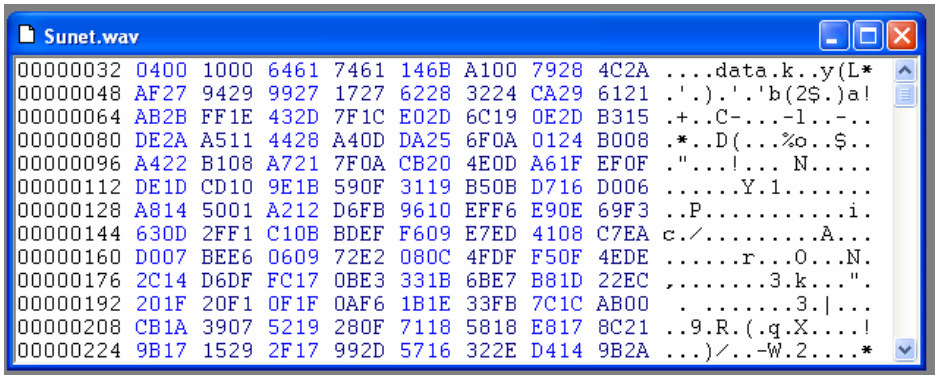

Fig.1. The original sound file

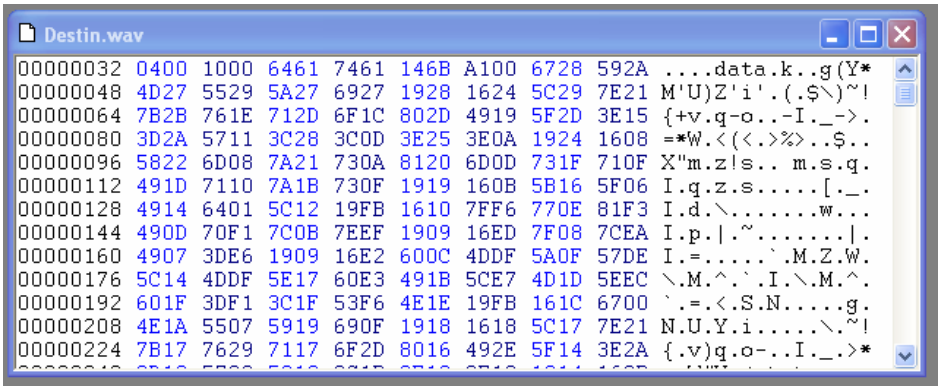

Fig.2. The file with modificated sound

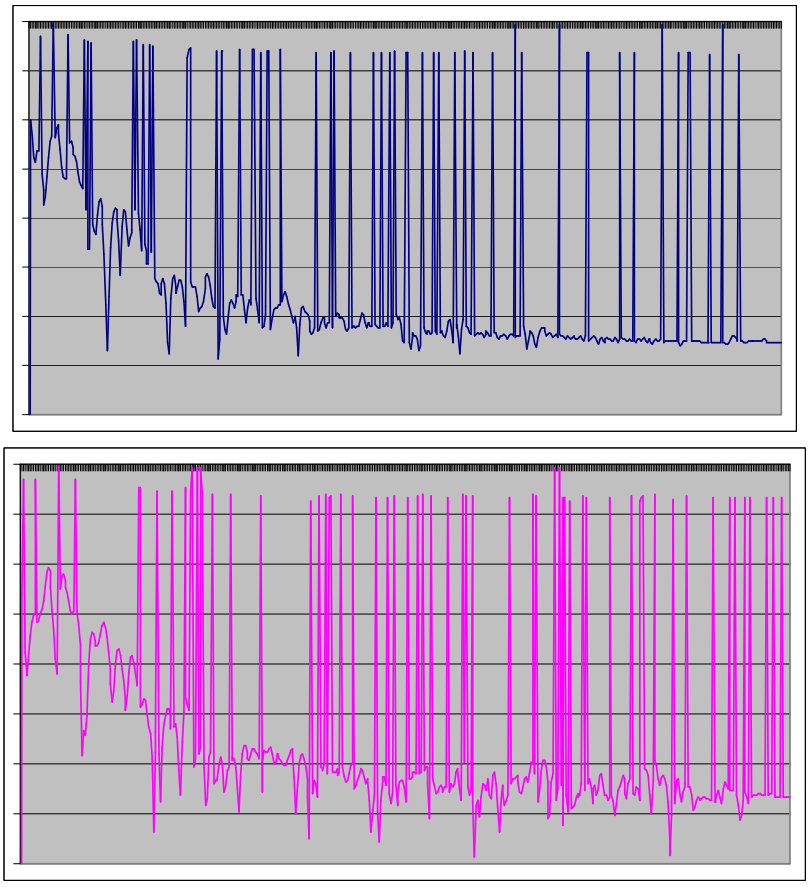

Fig. 3 Source file MHF left and right channel charts

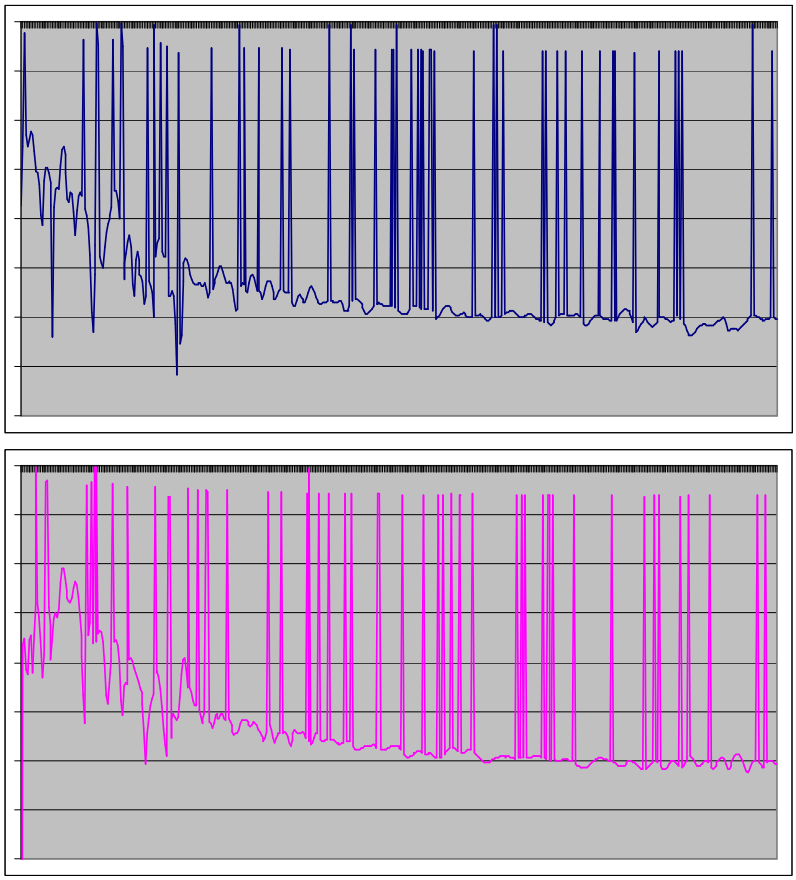

Fig. 4 Destination file MWF left and right channel charts

In the fig. 1 and 2 I presented a small portion of MHF an MWF where it can be visible the difference between them, at the low level read of those files.

In the fig. 3 and 4. I represented the chart (Microsoft chart) for a half a second of the source and destination files, for left and right channel of wave sound format.

In both way of representing of MHF and MWF it is visible the alteration of file, because the process take place at the octet level where it is altered only low significant octet.

The methods before mentioned, at the sound and picture files level, represent methods of hide the information in the multimedia files. With some intelligent modifications, those methods can be use in "transporter" of the secret information in a transparent way for the accustom people.

3. STEGANALYSIS

In the content of this article I described and tested some methods that can be used to hide information inside of multimedia files: picture and sound.

Obviously, that information is exposing to a stenographic and cryptographic analysis.

So, the steganalysis represents the final process of the hide information, using the perfect proceedings, but it can say if inside a file was or not enclose a "watermark", utilized with the scope to protect the author's right. The steganalysis goes much further then an analysis when it is find if is or not modifications the bit from a file, or where the watermark information is present. For example, the statistic analysis of a picture can be realized for finding of the hiding message presence.

Some of these instruments live specific "trace" in the hide data and that make easily the steganalysis job. In normal way, the remake of the original message, in special way, in case of an aprioristic crypto can be very difficult, but not impossible.

4. CONCLUSION

The hide of some information in the multimedia files: picture, sound or movie background, realized into a little installment message M at an octet MHF level, is real and viable, because those little modifications are imperceptible for the human eyes and ears.

Many times those modifications can be interpreted like „little errors" or "noises" in the multimedia file.

The stenography can be used in hiding of information process with success, so we can

„mark" the multimedia files, and others forms of data, the database file for instance.

Trough the using of those methods it is obtained a new form of security communication, where the implicate sides benefit of the propriety that the modification data are total irrelevant for an outsider.

If it is used the analysis proceedings of the signal or of the absorb power, the steganalysis process became more and more easily to transfer a file and to register a big quantity of information in a relative short time.

The battle in this domain it's going between cryptography man and cryptanalysis man, security experts and hackers, the media register company and „pirates". So, the stenography and the steganalysis will exist and continue to develop trough new technical to counteract reciprocally.

The multimedia offers a perfect medium as a manifestation space of the protection and security of data.

REFERENCES

[1] Naor M. şi Shamir A., *Visual Cryptography*, Lecture Notes in Computer Science LNCS 950,

Advances in Cryptology: EUROCRYPT'94, Springer-Verlag, 1994, pp. 1-12.

[2] Stinson D., *Visual Cryptography and Threshold Schemes*, Dr. Dobb's Journal, April 1998, pp.36-43.

[3] R. Agrawal, P. Haas, and J. Kiernan, "Watermarking relational data: framework, algorithms and analysis", VLDB, vol. 12, issue 2, 2003.

[4] M. Bocko, "Data Hiding in Digital Audio Files", IEEE SPS, March 5, 2003.

[5] P. Davern and M. Scott, "Steganography: Its History and Its Application to Computer Based Data Files", Working Paper, Dublin, Ireland, 1995.

[6] J. Dittmann, M. Stabenau, and Ralf Steinmetz, "Robust MPEG video watermarking technologies", ACM International Conference on Multimedia, p.71-80, September 13-16, 1998, Bristol, United Kingdom.

[7] J. Fridrich and M. Goljan, "Practical Steganalysis of Digital Images -- State of the Art", Security and Watermarking of Multimedia Contents, vol. SPIE-4675, pp. 1-13, 2002.

[8] J. K. 'O Ruanaidh, W. J. Dowling, and F. M. Boland. "Watermarking digital images for copyright protection", IEE Proceedings on Vision, Signal and Image Processing, 143(4):250--256, August 1996.

[9] http://www.digimarc.com

[10] N. Provos and P. Honeyman, "Detecting Steganographic Content on the Internet", ISOC NDSS'02, San Diego, CA, February 2002.

[11] Iordache D., "A*plicaţii ale criptografiei vizuale"*, Sesiunea jubiliară de comunicări ştiinţifice cu participare internaţională "130 de ani de învăţământ de marină", 14-16 noi. 2002, Secţiunea V/155

[12] Iordache D., "*Metoda de autentificare vizuală pe WEB",* Computers and Electronics Romanian Fair –DOBROGEA, 2 iulie 2001