Survey of the Use of Steganography over the Internet

Lavinia Mihaela DINCĂ
Academy of Economic Studies, Bucharest, Romania
Lavinia.dinca@gmail.com

This paper addressesthe use of Steganography over the Internet by terrorists. There were rumors in the newspapers that Steganography is being used to covert communication between terrorists, without presenting any scientific proof. Niels Provos and Peter Honeyman conducted an extensive Internet search where they analyzed over 2 million images and didn't find a single hidden image. After this study the scientific community was divided: some believed that Niels Provos and Peter Honeyman was conclusive enough other did not.
This paper describes what Steganography is and what can be used for, various Steganography techniques and also presents the studies made regarding the use of Steganography on the Internet.
Keywords: *Steganography, Secret Communication, Information Hiding, Cryptography*

1 Introduction

Steganography is the art of secret communication. The difference between Steganography and Cryptography is that the latter will make the message unreadable, but the existence of secret communication will be there. Steganography on the other part hides the message and "erases" the existence of any communication. In modern times Steganography and cryptography are complementary: first the message is encrypted and then is hidden using Steganography.
On February 2000, USA Today reported that terrorists are using Steganography to post secret communication on the Internet [1]. The newspaper article didn't contain any scientific proof or technical information that will permit the reader to verify the claims. Other news agencies reported that images posted on eBay and Amazon contained hidden messages [2].In their paper Niels Provos and Peter Honeyman [3] tried to verify the claims by analysing over two milion images downloaded from eBay and one milion images downloaded form USENET arhives and they didn't discover a single hidden message. For image analysis they used a open source framework created by them. Recent studies show that the proposed framewok can't detect all hidden messages in images. This paper will examine the research done in this area.

2 Steganography

Steganography derives from the Greek word "steganos", meaning secret and "graphy" meaning writing. Steganography represents a hidden writing. The message is visible, but remains undetected because we are not aware of its existence. A usual description of Steganography is "Hiding in plain sight".
Sometimes encrypted messages have been intercepted but never decrypted. Even so the damage was done, because the existence of an encrypted message shows that someone is communicating confidential information. This is the reason nowadays Steganography is used combined with cryptography. This way the existence of a secret communication is erased.
The basic structure of Steganography is made up of three components: the"carrier", the message, and the key [4]. The carrier (or cover) can be a digital image, an audio file, even a protocol (like TCP/IP packet). The cover will conceal the hidden message.
When a Steganography algorithm is evaluated the following are taken into consideration:

- **Capacity** – the amount of information that can be hidden without altering the cover medium in such way that will attract suspicion
- **Security** – the difficulty of detecting the hidden information. Usually security relates with capacity – if we hide a large

amount of information in a cover medium it will be easier to detect.
- **Robustness –** the amount of modification that the cover medium can endure before the hidden information will be destroyed.

How Steganography can be used [5] for:
- Enhanced Data Structures: hide extra information with the standard medium such as hiding information about a photo (like the year and place it was taken) in the photo itself, this way the information will "travel" along with the photo.
- Strong watermarks: used mostly for copyright of digital content such as books, movies and audio files. Some watermarks are meant to be visible such as a word in the background of a document and others are not. The invisible watermarks are used for identification purposes mostly to know how originated the document, who bought that file and distributed illegally. Watermarking technology has been embedded into DVDs and DVDs/CDs, nowadays if a DVD/CD bears a DO NOT COPY watermark, some DVD/CD writers might refuse to create a copy.
- Document-Tracking tools –the hidden information inside of a document can identify the legitimate owner of the document or the person the document was issued to - this type of identification is used mostly in digital libraries who generate a watermark barring the users id, if the file is posted over the Internet it can be tracked to the person who illegally published it.
- File Authentication –the hidden information embedded into a file can certify file authenticity.
- Private Communications – Steganography can be used for private communications by embedded information into a harmless cover.

There is a difference between Steganography and watermarking, in Steganography the message is important, any alteration to the message will make it unreadable. In watermarking it is important that at least one watermark is preserved during and attack, it doesn't matter if the other marks are destroyed.

3 Different kinds of Steganography

There are different kinds of Steganography which are going to be briefly described for information purposes. Due to the papers topic, the emphasis will be on Steganography in images and in protocols (on web); the other domains will be briefly mentioned.

- *Steganography in Images*

Images are the most popular carriers for Steganography. The techniques of hiding messages into images can be divided into Image Domain and Transform Domain[6]. The Image Domain (or spatial domain) techniques embed the message directly into the image, while the Transform domain the image is first transformed and then the message is embedinto the file.

A digital image is represented as a collection of numbers that makeup different light intensities in different areas ofthe image [7].

The selection of the cover image is very important. It is advisable not to use well known images because the hidden message can be found very easily (please refer to section 4 Methods of attack on Steganography, for more information about the attacks on Steganography). The best cover images are the ones with many details, which don't have large portion with the same color.

It must be clear that changing a bit in an image might represent switching form a color pixel to another color one (like red to blue). Such a change will be immediately detected in the cover picture, imagine a red pixel in the middle of the sky.

Another thing we must be aware when we select the cover image is the image compression and how the image is going to be transmitted. There are two types of images compression "lossless" and "lossy". The difference between them is that "lossless" data compression is a type of algorithm that allows the exact original data to be reconstructed from the original data contrast to lossy algorithm which only allows an approximation of the original data to be recon-

structed [8].The "jpeg" images uses lossy-compression while "bmp", "giff" uses the lossless compression.
Due to the fact that the transmission medium for the Steganography is mostly the Internet, the preferred compression algorithm is the lossy compression because it offers bigger compression rates.

The most common method of embedding information into an image is LSB algorithm (Least Significant Bit). The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message [9]. For example a grid for 3 pixels of a 24-bit image can be as follows:

```
(00101101   00011100   11011100)
(10100110   11000100   00001100)
(11010010   10101101   01100011)
```

Fig. 1. Example of 3 pixels of a 24-bit image [9]

If we embed the number 200, which has the 11001000 binary representation, using LSB techniques we obtain the following grid:

```
(00101101   00011101   11011100)
(10100110   11000101   00001100)
(11010010   10101100   01100011)
```

Fig. 2. Example of 3 pixel with 200 number embedded [9]

A practical example of Steganography is the following image:

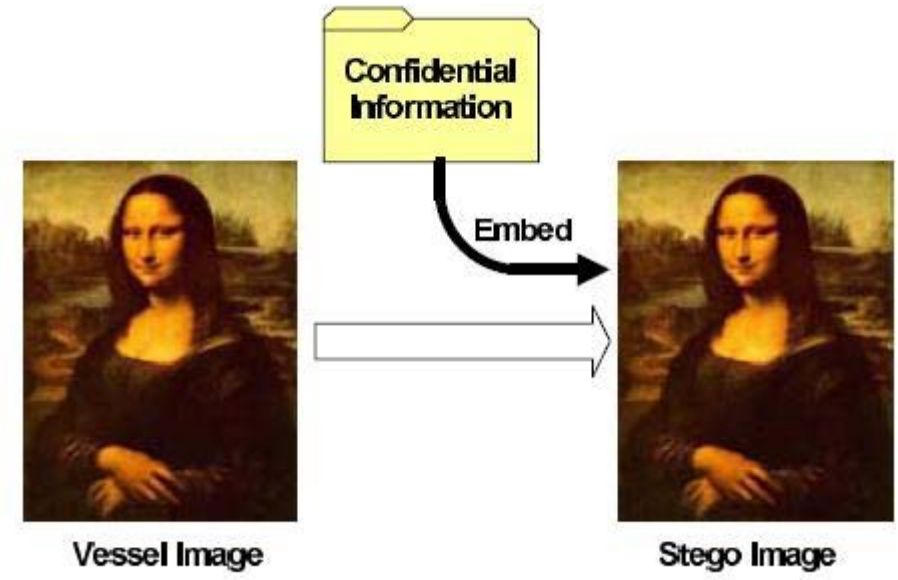

Fig. 3. Example of image Steganography [10]

The image above was used as an example, even if it contradicts what was stated earlier in this paper – not to use popular images, because the original can be found and then compared with the "fake" copy. As you can see there is no way you can detect by observation that there is something "wrong" with that picture.

- *Steganography in Audio*

This type of steganography is very difficult because the human auditory system is perceptible to background noises. The weakness of the human auditory system is that it can't differentiate between the sounds high and

low sounds. It is clear that this weakness must be exploited when hiding data into audio files.

There are several methods of data hiding in audio files:

- Low bit encoding which issomewhat similar to LSB that is generally used in Images.The problem with this technique is that the human ear can notice it.
- Spread Spectrum this method addsrandom noises to the signal and the information is concealed inside acarrier and spread across the frequency spectrum [11].
- Echo data hiding this method uses the echoes in sound files in order to try and hide information [11].

If we hide information inside an image we risk damaging the file, the exact opposite happens in audio files. When information is inserted into an audio file sound can actually improve.

- *Steganography in Video*

The most commonly used method for hiding information inside a video is DCT (Discrete Cosine Transform). DCT works by slightly changing the each of the images in the video, only so much though so the human eye can't notice [12]. Steganography in Video works like the steganography in images, the difference is that the data is hidden in video frames.

Westfeld and Wolf have described a method for data hiding in a videoconferencing system[13]. Because of the bandwidth necessities the videoconference systems have a special transmission system. Because of bandwidth necessities the videoconferences systems transmit only the differences between successive frames. If the information is hidden when these differences are transmitted it is very hard to detect because there is no "whole" image to compare only frames differences.

- *Steganography in text*

There are several methods of hiding data into text or documents, sometimes called linguistic Steganography. The most common methods are:

- Open text methods like inter-sentence spacing, end of line spacing, inter-word spacing. The problem with these methods is that they can be easily removed from the text by a simple reformatting.
- Syntactic method – manipulates the punctuation to hide information.
- Semantic method – this method uses synonyms for primary and secondary value.For example, the word "beautiful" could be considered primary and "exhilarating" secondary. Whether a word has primary or secondary value bears no relevance to how often it will be used, but primary words will be read as ones, secondary words as zeros when decoding [14].
- New file generation – new files are generated in order to create the message.

This latest method described is the best way to hide information inside documents because it doesn't use o cover document, but rather creates one. A popular program that can do that is: spam mimic [15].

If we encode the following text "hidden message" we obtain the following spam message:

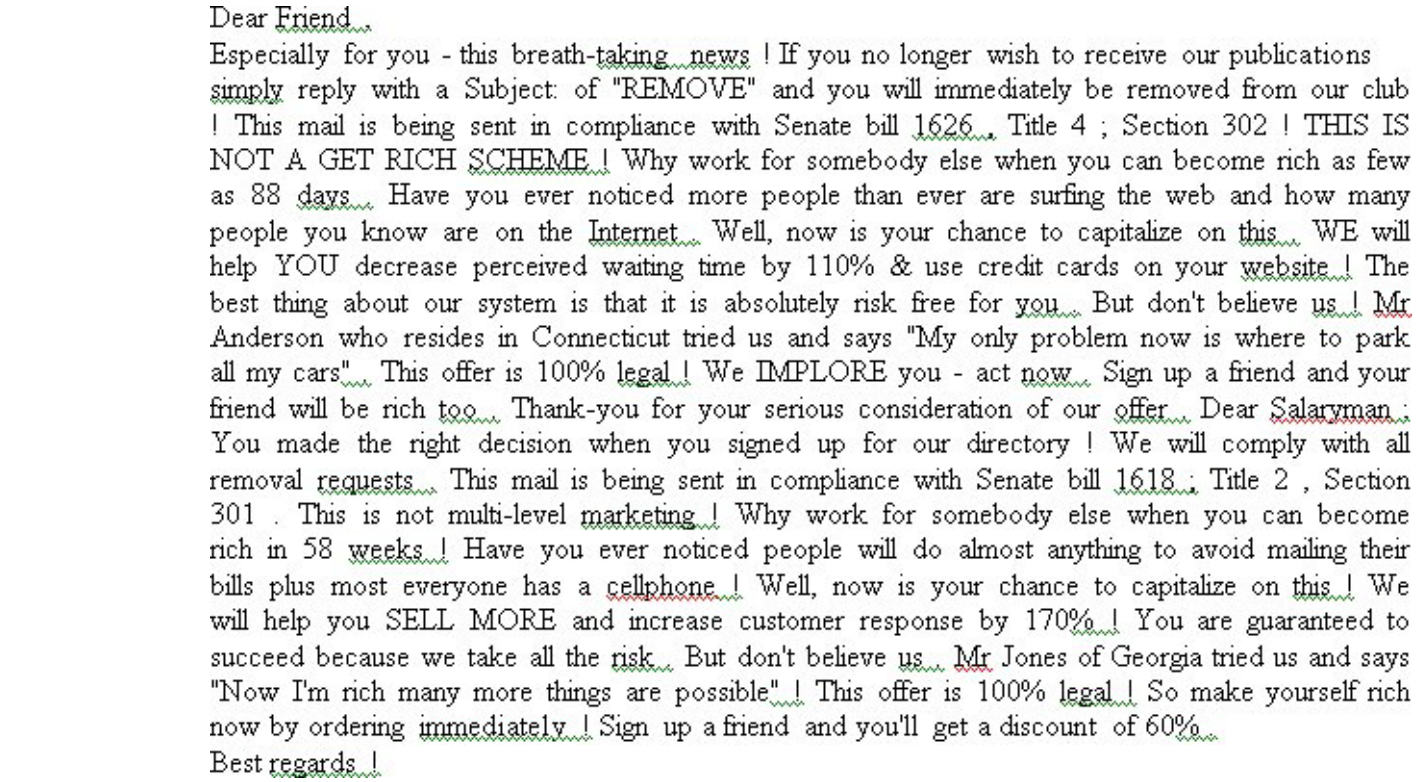
Dear Friend ,
Especially for you - this breath-taking news ! If you no longer wish to receive our publications simply reply with a Subject: of "REMOVE" and you will immediately be removed from our club ! This mail is being sent in compliance with Senate bill 1626 , Title 4 ; Section 302 ! THIS IS NOT A GET RICH SCHEME ! Why work for somebody else when you can become rich as few as 88 days . Have you ever noticed more people than ever are surfing the web and how many people you know are on the Internet . Well, now is your chance to capitalize on this . WE will help YOU decrease perceived waiting time by 110% & use credit cards on your website ! The best thing about our system is that it is absolutely risk free for you . But don't believe us ! Mr Anderson who resides in Connecticut tried us and says "My only problem now is where to park all my cars" . This offer is 100% legal ! We IMPLORE you - act now . Sign up a friend and your friend will be rich too . Thank-you for your serious consideration of our offer . Dear Salaryman , You made the right decision when you signed up for our directory ! We will comply with all removal requests . This mail is being sent in compliance with Senate bill 1618 ; Title 2 , Section 301 . This is not multi-level marketing ! Why work for somebody else when you can become rich in 58 weeks ! Have you ever noticed people will do almost anything to avoid mailing their bills plus most everyone has a cellphone ! Well, now is your chance to capitalize on this ! We will help you SELL MORE and increase customer response by 170% ! You are guaranteed to succeed because we take all the risk . But don't believe us . Mr Jones of Georgia tried us and says "Now I'm rich many more things are possible" ! This offer is 100% legal ! So make yourself rich now by ordering immediately ! Sign up a friend and you'll get a discount of 60% .
Best regards !

Fig. 4. Example hidden message by generating a spam message

We notice that the generated message is actually a “normal” spam message that mostly will be ignored. The advantage of this technique is that the generated spam can be send to millions of users and it will be quite impossible to know to whom that message was addressed.

- *Steganography in networks*

Usually the Steganography in networks can be divided into the following categories [16]:

- Hiding in an attachment - is the basic form of sending Steganography files to another person. The message contains an attachment, a file, which has a secret message hidden inside it. The file can be an image, a audio file, video file, a document. The best transmission methods are via email, ftp, website posting.
- Hiding in a transmission – it uses special programs that hide the data into a file and then transmit the message. The previous method needed two steps: first hide the data into the cover file, and then transmit the data.
- Hiding in an overt protocol – involves camouflaging data like so it looks like something else. For example the data transmitted can be masked so it looks like normal web traffic, even though is not.
- Hiding in network headers – it uses the headers of the TCP/IP protocol to hide data. The IP protocol header contains the necessary information for packets to be routed where is needed, so when we insert or change the data into the header we must do so we do not affect communication.

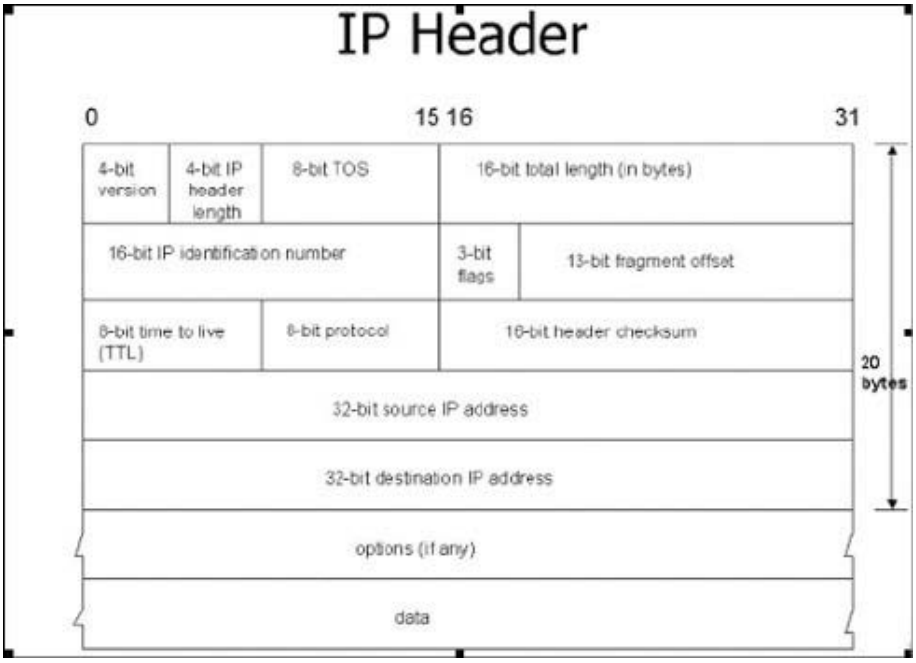

Fig. 5. Example IP header

Some fields in the IP header must contain specific values such: header length version number. If we change those numbers the communication will fail. One field in the IP header thatcan be changed without affecting the communication is the IP identification number. Usually this number is incremented by one when large packets are sent (the large packets are broken down into smaller one). A different number can be used as long as the order of the packages is respected and the protocol will work properly.

4 Methods of attack on Steganography

The most common attacks on Steganography are[5]:

- File only –an attacker must determine if the file in question contains a secret message hidden in it. Many of these basic attacks rely on statistical steganalysis (covered in section 5 of this article) to detect a possible hidden message in the file.
- File and Original copy – this is the case when the attacker is in possession of the original file and the file containing the secret message. In this case detecting the existence of a secret message is very easy, because the two files can be compared. This is the reason that whenever Steganography is used it is recommended that the cover medium be an "original one" like: a picture taken with your own camera etc. If this is not possible it is advisable to take the original cover (a picture, video, document etc) and alter it prior to information hiding. This way we ensure that there is no "original" file.
- Multiple encoded files – the attacker gets multiple files, same cover with different messages embedded into it. This might occur especially in watermarking a digital file with copyright information. Let's assume that and attacker gets multiple copies of a book that contains different user information (each copy of the book has embedded information about the user who received the copy). In this case the simplest attack is to blend the files together and create a hybrid.
- Access to file and algorithm – if the attacker has access to the file containing the secret message and algorithm used to hide the information; it might be easier to retrieve the hidden message. Some Steganography algorithms safeguard against this method by using the same principle as cryptography systems use: public and private keys – without the private key it is impossible to retrieve the message.
- Destroy everything attack –this type of

attack aims in destroying the message completely and the attacker might not even try to retrieve the message.
- Random tweaking attacks –adding small changes in the files hoping that the message will be unreadable. As the previous form of attack the goal is to make the hidden message unreadable, not retrieving it.
- Add New Information – in some cases the attackers might use the same software to hide a new message into the file. The original message might be overwritten.
- Reformat attack – a common way to destroy the information hidden in a file is by changing the file format. This type of attack can produce a lot of damages to the hidden message.
- Compression attack – the attacker might compress the file which might result in the total loss of the secret message embedded in the file, because the compression algorithms tend to remove extra information during compression. It is obvious that "hidden message" equals extra information.

From what stated above it is clear that if an attacker wants only to destroy the hidden message, he/she can do that very easily by combining some of the methods of attack presented above.

5 Statistical analysis

In order to analyze large quantities of images statistical analysis can be used. When we embed information into an image some statistical properties might deviate from the norm.

For example embedding encrypted message into a GIF image changes the histogram of its color frequencies [17].

Figure belowpresents two images with a resolution of 640 ×480 in 24-bit color. The original image was about 1.2 Mbytes, while the two JPEG images shown are about 0.3 Mbytes. Figure 6a is compressed original; Figure 6bcontains the first chapter of Lewis Carroll's The Hunting of the Snark. After compression, the chapter is about 15Kbytes. The human eye cannot detect which image holds steganographic content [18].

(a) (b)

Fig. 6. Example of image that contains steganographic content [18]

Even though the human eye can't detect the message, the statistical analysis software can detect modification in the DCT coefficients. The DCT is used in JPEG image compression. JPEG divides the image into 8 by 8 pixel blocks, and then calculates the DCT of each block. The modification of a single DCT (while hiding the data) will affect all 64 image pixels.

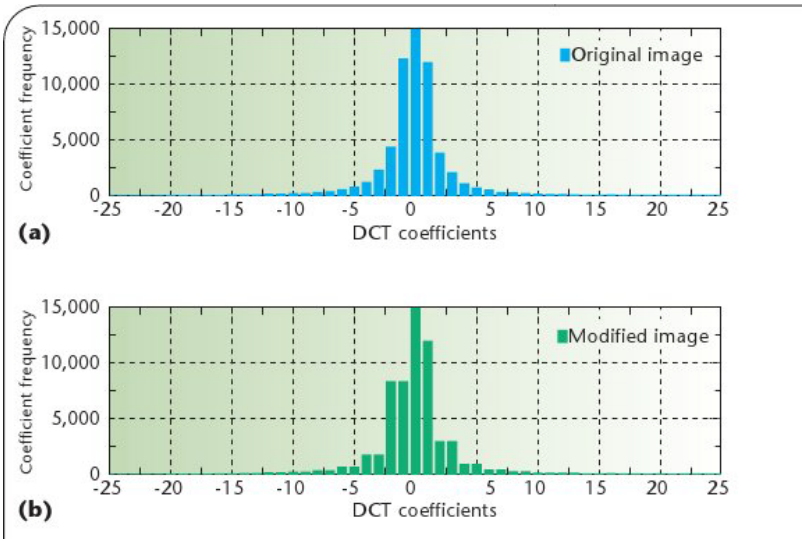

Fig. 7. Modification of DCT coefficients [18]

The picture above shows the modification of DCT coefficients when a hidden message is inserted.

To prevent detection by statistical tests the statistical properties of the cover medium must be preserved. To do that the user can estimate, prior to data hiding, the amount of data that can be hidden in an image while maintaining the correct statistics [19]. This way the "correct" image can be chosen – an image where the needed amount of data can be hidden "with the correct statistics".

6 Detection framework and results

At the beginning at the article, it was mentioned that in order to prove or disprove the allegations that terrorists were using Steganography to hide messages in images posted on eBay, Niels Provos and Peter Honeyman-conducted an extensive Internet search where they analyzed over 2 million images and didn't find a single hidden image[3].

This section presents the Steganography software analyzed, the detection framework used for analyzing the images, the image selection method and their results.

The open source Steganographic systems analyzed were:

- **JSteg**is a program by Derek Upham which hides data in the ever popular JPG image format. Version 1.0 has a number of new improvements, including 40 bit RC4 encryption, determination of the amount of data a JPG can hide beforehand, and user-selectable JPG options (ie. degree of compression). JSteg Shell is the interface for the JSteg program.
- **JPHide** is a program which hides a file in a jpeg visual image.The design objective was not simply to hide a file but rather to do this in such a way that it is impossible to prove that the host file contains a hidden file. Given a typical visual image, a low insertion rate (under 5%) and the absence of the original file, it is not possible to conclude with any worthwhile certainty that the host file contains inserted data. As the insertion percentage increases the statistical nature of the jpeg coefficients differs from "normal" to the extent that it raises suspicion.[20].
- OutGuessis a steganographic system available asUNIX source code. The last released version includes the ability topreserve statistical properties of the cover image [21].

The proposed framework is StegDetect – a program developed by the authors which can detect content hidden with the above mentioned programs.

Stegdetect is an automated tool for detecting steganographic content in images. It is capable of detecting several different steganographic methods to embed hidden information in JPEG images. Currently, the detectable schemes are

- jsteg,

- jphide (unix and windows),
- invisible secrets,
- outguess 01.3b,
- F5 (header analysis),
- appendX and camouflage.

The images for analysis were obtained from the eBay site (since that was the site in question, which appeared in the newspapers reports) and form a USENET archive.

For obtaining the JPEG images form eBay a web crawler was needed. Since at the moment when the study was conducted, there was no suitable web crawler available, one was written by the authors named "Crawl"

The Crawl web crawler starts a depth-first traversal of the web at the specified URLs. It stores all JPEG images that match the configured constraints [22].

Main features:

- Saves encountered images or other media types
- Media selection based on regular expressions and size constraints
- Resume previous crawl after graceful termination
- Persistent database of visited URLs
- Very small and efficient code
- Asynchronous DNS lookups
- Supports robots.txt

The web crawler was automatically integrated with Stegdetect creating an automatic detection framework.

Over two million images downloaded from eBay and over one million from USENET discussion forums and failed to find a single genuine hidden message [3]. The conclusion of the study was obvious: the terrorists didn't use steganography to communicate among them.

This study divided the scientific community in two: some believed that the study was relevant and the result was proof enough others did not.

7 Other studies

Some of the people, who opposed the study conducted by NielsProvos and Peter Honeyman, stated that Stegdetect is not an accurate tool to detect Steganography, because it was designed to detect hidden content created with open source software. Since the commercial programs are more powerful and implement "better" algorithms, there was a chance that Stegdetect will not be able to detect content hidden with commercial programs.

This assumption might be accurate, mainly if we take into consideration that commercial Steganography software is not that expensive and that large terrorist organizations are well funded. Not to mention thy can actually invest in their own Steganography framework.

So "Stegdetect" was "tested" against commercial versions of steganography software [23].

The following commercial software was evaluated:

- SecurEngine Professional by AdrienPinet
- Computer security from Adolix
- Steganography from Secure Kit Incorporated

The "Computer Security" software was used in the experiment due to its extensive list supported of cryptographic algorithms.

The above software was used to create an image with steganographic content. The image was tested with StegDetect. The result of the test was negative; StegDetect wasn't able to detect the hidden message created with a commercial on the shelf program.

From the results of the experiment the following conclusions can be drawn:

- StegDetect can't detect images using commercial software, in this case Computer Security
- A better detection framework is needed in order to accurately detect hidden messages on the web
- Assure the integrity of the data files in order to certify that they haven't been modified – a legitimate image was switched with one containing steganographic content
- Close monitoring of free web hosting servers, so they will not be used for posting steganographic content.

8 Prevention methods

It is clear that something must be done to prevent the use of Steganography. Authorities have realized that and have started to include Steganalysis in the list of prevention measures to be taken against vicious persons using the Internet.

The majority of the developed countries, EU, USA and other countries, alliances or security structures are making intense efforts in order to identify, supervise, optimize and protect their vital critical infrastructures [24].

For example the European Commission began to realize that classical security solutions are getting obsolete and that we must adapt to new trends – steganography being one of them. In order to counteract the European Commissionlaunched the Future Internet Initiative [25] as vital for economic growth in Europe. The initiative refers to the need to secure the Small Medium Enterprises (SME) against vicious uses of their resources – that being a huge security thereat. It is believed that governmental and large enterprises can protect their Internet resources, while the SMEs (including open source communities) can't.

The EU economy is based on SMEs, so it is clear that the SMEs must be protected against malicious uses of their resources.

The major security challenges identified by the EU for SMEs can be broken into the following categories [26]:

- Access Control

There is a growing need for monitoring solutions (logs monitoring), smart passwords, latest firewalls, updated computers. All of that will ensure that no one is misusing the resources. A common tactic is to penetrate a network and use its resources outside the office hours – this type of attack can go undetected for months. So the monitoring solutions must take this practice and many more into consideration.

- Steganalysis

Due to the increase necessity of large bandwidths for common business the SMEs are susceptible to steganography. Nowadays the email systems are not limited to a few megabytes per email, so a simple email can be used to sent multimedia files (such and image, video, audio) to multiple persons. It is a common practice to receive "funny" messages from friends and forward them to another list of friends. These "friendly" messages can contain steganographic content and can be used for corporate espionage even by terrorists. It is important to implement Steganalysis tools as an internal LAN defense measure.

- Multi-tenancy

Multi-tenancy is quite new concept that refers to the architectural principle, where a single instance of the softwareruns on a software-as-a-service (SaaS) vendor's servers, serving multiple client organizations[26].The old concept implied the security of the application by installing it into a controlled environment, on a server in your own LAN. This tendency is starting to change as many companies, especially SMEs, use SaaS. Some of the SMEs have renounced in having their own servers, some have even rented personal computers.

9 Conclusions

The use of Internet for communication is still open for debate. There are two groups in the scientific world: one agrees with fact that terrorists are using steganography to communicate with each other the other group does not. Nowadays there is sufficient evidence or lack of it to support both theories, but not enough to reach a definite conclusion.

The most extended study on this topic was conducted by Niels Provos and Peter Honeyman where they analyzed over 2 million images from eBay and one million from USENET archives and didn't find a single hidden image. They used their own framework to analyze the images.The framework was design to analyze hidden content created by the most popular steganography open source software at the time.

Due to that fact, some people argued that the analysis framework was not effective and that commercial steganography software was more powerful. A study was made and it was proven that the steganographic framework used by Niels Provos and Peter Honeymancan't detect content hidden with commercial

steganography software. This represents a problem because possible terrorists groups have the capacity to buy commercial steganographic software which is not that expensive. Another problem might be the images selection; possible terrorists might use popular web sites or might not – which will make the target images harder to find in order to be analyzed (we can't scan the entire Internet).
One thing is clear: the authorities have realized the security threat posed by steganography and they began implementing measures and proposals to defend it. The EU has recognized steganalysis as an important tool in the proposal made for by the Future Internet Initiative. The most important measure was implemented by the USA after the 9/11 terrorists attacks by implementing the controversial Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 known as the USA PATROT act, which allows the Federal Bureau of Investigation (FBI) to search telephone, e-mail, and financial records of suspected terrorists without a court order.

References

[1] K. Jack,*www.usatoday.com.* [Online] USA Today, February 05, 2000. [Cited: January 29, 2011.] http://www.usatoday.com/tech/news/2001-02-05-binladen.htm

[2] D. McCullagh, Secret Messages Come in .Wavs. *www.wired.com.* [Online] February 20, 2001. [Cited: January 29, 2011.] http://www.wired.com/politics/law/news/2001/02/41861

[3] N. Provos, P. Honeyman.*Detecting Steganographic Content on the Internet.* San Diego : CITI Technical Report, 2001.

[4] G.C. Kesslet, "An Overview of Steganography for the Computer Forensics Examiner,"Forensic Science Communications, 2004.

[5] P. Wayner, *Dissappearing Cryptography: Information hiding: Steganography & watermarking*, Elsevier Inc, 2009, ISBN 978-0-12-374479-1

[6] J. Silman, *Steganography and Steganalysis: An Overview*, SANS Institute, 2001.

[7] N. F. Johnson& Jajodia,"Exploring Steganography: Seeing the Unseen,"*Computer Journal*, 1998.

[8] Lossless data compression. [Online] [Cited: 01 20, 2011.] http://en.wikipedia.org/wiki/Lossless_data_compression.

[9] T. Morkel, J.H.P. Eloff, M.S. Oliver,*An overview of image steganography*, Pretoria, South Africa, Information and Computer Security Architecture (ICSA) Research Group, 2005.

[10] Steganography. [Online] [Cited: 01 04, 2011.] http://sites.google.com/site/itworldtricks/steganography.

[11] Steganography, *Web Technology and security tips.* [Online] [Cited: 01 20, 2011.] http://somasish.blogspot.com/.

[12] A. Mangarae, Steganography FAQ. *Slideshare.* [Online] 03 18, 2006. [Cited: 01 20, 2011.] http://www.slideshare.net/NLDT/steganography-faq.

[13] A. Westfeld, G. Wolf,*Steganography in a Video Conferencing System*, Information Hiding, LNCS - Lecture Notes in Computer Science, 1998, Vols. 1525/1998;32-47.

[14] G. Kipper,*Investigators guide to Steganography*, Auerbach Publications, 2004.

[15] [Online] [Cited: 01 04, 2011.] https://www.spammimic.com/.

[16] E. Cole, *Hiding in plain site: Steganography and the Art of Covert Communication.* Indianapolis, Indiana, Wiley Publishing Inc, 2003. ISBN 0-471-44449-9.

[17] A. Westfeld, A. Pfitzmann,"Attacks on Steganographyc Sytems,"*Proceedings of*

Information Hiding - Third International Workshop, Springer, 1999.
[18] N. Provos and P. Honeyman,*Hide and Seek: An Introduction to Steganography*, IEEE Computer Society, 2003.
[19] N. Provos,*Defending Against Statistical Steganalysis.* Center for Information Technology Integration University of Michigan, 2001.
[20] Download for JPHide. [Online] [Cited: 01 15, 2011.] http://www.freewr.com/freeware.php?download=jphide-and-jpseek&lid=258.
[21] N. Provos. [Online] [Cited: 01 25, 2011.] http://www.outguess.org/.
[22] N. Provos. Crawl. [Online] [Cited: 01 29, 2011.] http://monkey.org/~provos/crawl. .
[23] R. Goel, M. Garuba, C. Liu, T. Nguyen,"The Security Threat Posed by Steganographic Content on the Internet,"*International Conference on Information Technology*, 2007.
[24] C.D. Tofan,"Protection of Information Technology Critical Infrastructures in UE,"*Simpoziului international al tinerilor cercetatori(Editia a VIII-a)*, 2010.
[25] Future Internet Assembly (FIA). [Online] [Cited: 01 27, 2011.] http://www.future-internet.eu.
[26] S. Naqvi, G. Dallons, C. Ponsard,"Applying Digital Forensics in the Future Internet Enterprise Systems - European SMEs perspective,"*2010 Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering*, IEEE Computer Society, 2010. ISBN 978-0-7695-4052-8/10.

Lavinia Mihaela DINCA has graduated the Romanian American University and currently holds two master degrees in: "Business Excellence Models" from Academy of Economic Studies Bucharest and "Computer networks" from University of Bucharest. She is currently enrolled in the doctoral programme at the Academy of Economic Studies Bucharest. She has experience in managing software complex projects being PMP certified. Her main interests are: steganography, cryptography, computers security, Linux and open source software.