MEDWIN PUBLISHERS
Committed to Create Value for Researchers

International Journal of Forensic Sciences
ISSN: 2573-1734

JPEG Steganography: Hiding in Plain Sight

Hasan Fayyad-Kazan[1]*, Elissa Saba[2], Hussin J Hejase[3], Ali El Dirani[4] and Hassan Rkein[4]

[1]Information Technology, Al Maaref University, Lebanon
[2]Department of Forensic Sciences, Lebanese University, Lebanon
[3]Senior Member IEEE, Researcher and Professor, Lebanon
[4]FBA, Al Maaref University, Lebanon

Research Article
Volume 6 Issue 1
Received Date: January 29, 2021
Published Date: March 15, 2021
DOI: 10.23880/ijfsc-16000223

***Corresponding author:** Hasan Fayyad-Kazan, Information Technology, Al Maaref University, Beirut, Lebanon, Email: hasanfkazan@gmail.com

Abstract

Steganography and steganalysis are important topics in hiding data. Since antiquity steganography has existed in protecting sensitive information against unauthorized unveiling attempts, it hides messages in plain sight. On the flip side, steganalysis tries to detect the existence of the message or even more to retrieve the embedded data. Nevertheless, internet's growth, reveals that steganography has been used as a tool for illegal acts such as child pornography or terrorism. Given this background, both steganography and steganalysis received a great deal of attention, especially from law enforcement. On the other hand, universal steganographic methods adjustable to real-world applications are practiced on a large scale using different softwares and algorithms. Thus, it is necessary to set up even more accurate steganalysis techniques capable of detecting the hidden data. Considering this, this work is intended as technical introduction to steganography for those unfamiliar with the field and delivers a practical understanding of it without delving into the mathematics. It also provides a historical context alongside a detailed review for steganography and steganalysis of digital images, mainly in JPEG format. Examples of software tools to hide secret data inside JPEG images as well as software to detect such hidden files will also be presented.

Keywords: Steganography; Steganalysis; JPEG; LSB; DCT; Stego-Image

Abbreviations: JPEG: Joint Photographic Experts Group; HVS: Human Visual System; MSE: Mean Square Error; PSNR: Peak Signal to Noise Ratio; IS: Image Steganography; UED: Uniform Embedding Distortion; DCT: Discrete Cosine Transform; LSB: Least Significant Bit, BBC: Block Boundary Continuity; BBM: Block Boundary Maintenance; GIF: Graphical Interchange Format; BMP: Bitmap File; OSNs: Online Social Networks.

Introduction

The word Steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing", and is a long-practiced form of hiding information, and it has long been regarded as a tool used for illicit and destructive purposes such as crime and warfare [1].

With the outrageous evolution of the digital media, people are easily using it today as a form of invisible communication, in such a way that no one apart from the sender and the intended receiver could possibly know that a message has been sent, nor detect it using his human visual system (HVS). It is the science and art of secret communication between two sides that attempts to conceal the existence of the message [2]. So it's hiding confidential

information in plain sight.

Steganography concept is often confused with the one of cryptography and that's because both were used throughout history as a way to protect valuable data. The difference between two is that cryptography simply encrypts the information without hiding its presence, steganography, on the other hand, hides the message and its existence so it appears that no information is hidden at all. One conceals the contents of the message, whereas the other conceals the existence of the message.

Steganography has a long history, going back to the ancient Greek and Roman Civilizations. Messengers tattooed messages on their shaved heads and the messages remain invisible when their hair grows [3], other practices used waxed tables where messages were etched on wood then covered with wax, invisible inks were also used to accomplish the same goal.

The basic structure of Steganography is made up of three components, The "Carrier", the "Message", and the "key" [4]. A key can be used to assure more security. Today, thanks to modern technology, steganography is used on text, images, sound, signals, and more [5]. Digital images are large enough used as cover media due to their high degree of redundancy in modern communication and on the worldwide Internet. JPEG images are widely used in image steganography as there are various JPEG steganographic tools freely available to use. F5, Outguess, StegHide, MBSteg, JSteg, JSteg-Shell, and JPhide [6], are steganographic programs that have been developed recently for hiding data inside JPEG image format.

With the widespread illicit usage of steganography, steganalysis has garnered much attention from researchers. The aim of steganalysis is to identify the existence of the hidden message. It is mainly done by comparing the encrypted cover with the original copy.

This paper intends to critically review how a secret communication is carried on between a sender and a receiver, using a LSB steganographic method, the outguess algorithm. Thus the process of embedding secret data inside the DCT coefficients of JPEG image file, and its extraction.

Related Work

There are many research work on data hiding methods in DCT coefficients. A brief overview of some of those methods conducted in the past 10 years is given in this section.

In 2012, Gurmeet, et al. presented a comparative analysis by computing Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR), Processing time, and security. The analysis shows that the BER and PSNR is improved in the LSB Method but security sake DCT is the best method [7].

In 2013, Sohag, et al. analyzed various existing system and implemented a dynamic substitution based Image Steganography (IS) with a secret key. The proposed method is more difficult to attack because of message bits are not inserted into the fixed position but into deeper layer depending on the environment of the host image and a secret key resulting increased robustness. The robustness specially would be increased against those intentional attacks which try to reveal the hidden message [8]. At the same year, Eltyeb, et al. compared and analyzed Least Significant Bit algorithm using the cover object as an image with a focus on two types: BMP and JPEG. The comparison and analysis are done with respect to a number of criteria to understand their strengths and weaknesses [9].

In 2014, Pan, et al. presented a class of new distortion functions known as uniform embedding distortion function (UED) for both side-informed and non-side-informed secure JPEG steganography. By incorporating the syndrome trellis coding, the best code word with minimal distortion for a given message is determined with UED, which, instead of random modification, tries to spread the embedding modification uniformly to quantized discrete cosine transform (DCT) coefficients of all possible magnitudes. In this way, less statistical detectability is achieved, owing to the reduction of the average changes of the first- and second-order statistics for DCT coefficients as a whole. The effectiveness of the proposed scheme is verified with evidence obtained from exhaustive experiments using popular steganalyzers with various feature sets on the BOSS base database. Compared with prior arts, the proposed scheme gains favorable performance in terms of secure embedding capacity against steganalysis [10].

In 2015, Hiney, et al. explored a method to minimize the disruption so JPEG images can be used as steganography carriers on Facebook [11].

In 2016, Sugandhi, et al. proposed a new steganography approach for data hiding. In this approach they hide data in the encrypted image using LSB (least significant bit) technique. The hidden data in the binary form is replaced to the LSB position of the encrypted image binary data. The hidden data will be recovered by the receiver using the secret key. Thus this method provides double staging security. Thus it will be used to reduce the chance of detecting the encrypted image and then provides advanced security level of the encrypted image [12].

In 2017, Denemark, et al, imposed multivariate Gaussian model on acquisition noise and estimated its parameters

from the available precover. The embedding is then designed to minimize the KL divergence between cover and stego distributions. In contrast to existing heuristic algorithms that modulate the embedding costs by 1–2|e|, where e is the rounding error, in their model-based approach the sender should modulate the steganographic Fisher information, which is a loose equivalent of embedding costs, by (1–2|e|)^2. Experiments with uncompressed and JPEG images show promise of this theoretically well-founded approach [13].

In 2018, Li, et al. inspected the embedding change from the spatial domain and propose a principle of Block Boundary Continuity (BBC) for defining JPEG joint distortion, which aims to restrain blocking artifacts caused by inter-block adjacent modifications and thus effectively preserve the spatial continuity at block boundaries. According to BBC, whether inter-block adjacent modifications should be synchronized or desynchronized is related to the DCT mode and the adjacent direction of inter-block coefficients (horizontal or vertical). When built into $DeJoin$, experiments demonstrate that BBC does help improve state-of- the-art additive distortion schemes in terms of relatively large embedding payloads against modern JPEG steganalyzers [14].

In 2019, Ansari, et al. presented the comparative study and performance analysis of different image Steganography methods using various types of cover media (like BMP/JPEG/PNG etc.) with the discussion of their file formats. We also discuss the embedding domains along with a discussion on salient technical properties, applications, limitations, and Steganalysis [15].

In 2020, Giboulot, et al. proposed a method to better estimate the variances of DCT coefficients by taking into account the dependencies between pixels that come from the development pipeline. Using this estimate, we are able to extend statistically-informed steganographic schemes to the JPEG domain while significantly outperforming the current state-of-the-art JPEG steganography. An extension of Gaussian Embedding in the JPEG domain using quantization error as side-information is also formulated and shown to attain state-of-the-art performances [16].

In 2021, Wang, et al. presented a new principle, called block boundary maintenance (BBM), to minimize the modifications on the spatial block boundaries. In theory, they deduced the BBM principle on how to modify a pair of DCT coefficients of the intra-block to reduce the modifications on the spatial block boundary. According to the BBM principle, they designed a new strategy to define non-additive cost functions for JPEG steganography by exploiting the coefficient correlation of the intra-block in the DCT domain. The experimental results show that the BBM-based strategy can minimize modifications on the spatial block boundaries and thus achieve a high-security level when resisting modern JPEG steganalysis. Furthermore, the two principles of BBC and BBM can be fused to further improve the empirical security [17].

Background

In this section, we will provide a general overview of image steganography, image definition as well as image compression.

Image Steganography

Image Steganography hides confidential data within the image in such a way that prevents anyone other than the receiver from the detection of the hidden information or data. Figure 1 shows how the process is done.

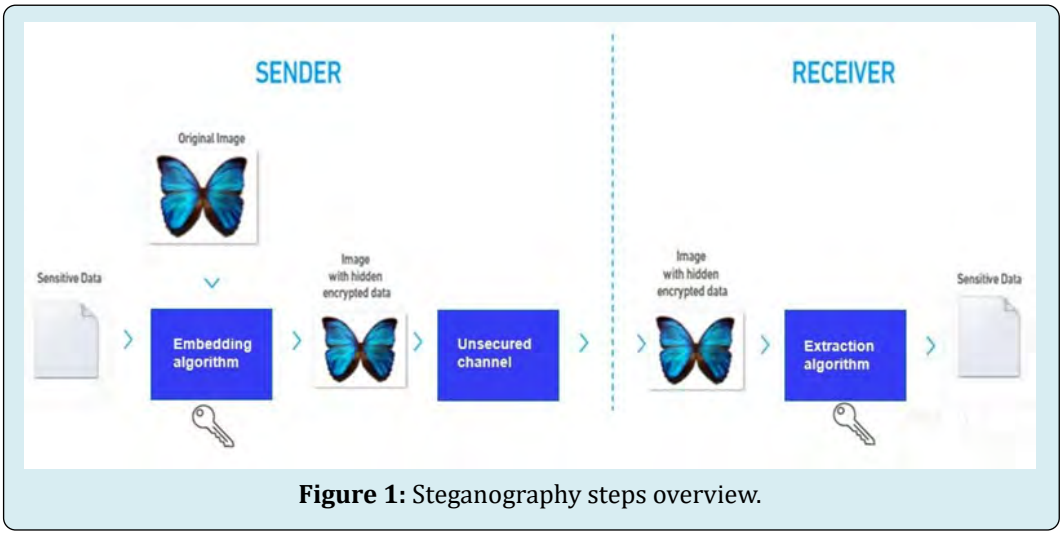

Figure 1: Steganography steps overview.

Based on the way of embedding data into an image, image steganography techniques can be divided into the following groups: Spatial domain and Transform domain.

- Spatial domain: This technique embeds the secret message bits in the pixel's color values directly without perceptible distortions. Least significant bit (LSB)-based steganography is one of the spatial domain techniques.
- Transform domain: It is a complex and very strong method based on frequency components, image pixels are first transformed to frequency domain components in order to embed the secret message bits into it. The Discrete cosine transformation technique (DCT) is a transform domain steganographic method.

Image Definition

An image is a collection of numbers that constitute different light intensities in different areas of the image. This numeric representation forms a grid and the little dots are called pixels (picture element).

8 Bit and 24-bit images are very common. Grayscale images are an example of 8-bit image form, which means each pixel has a gray intensity, presented as 1 byte that is equal to 8 bit, and can range from 0 (zero level intensity of light, black) to 255 (full intensity, white) so that's a total of 256 different shades of gray. Whereas for a 24-bit color image as shown in figure , it is well known that any color is a combination of red, green, and blue, thus each pixel is represented as 3 bytes –one for Red, one for Green and one for Blue (RGB color model). Each color have different intensities, exactly the same as in grayscale images, that range from 0 (zero intensity of color) to 255 (highest level of the color).

Thus in one given pixel, there can be 256 different quantities of red, green and blue, adding up to more than 16-million combinations, resulting in more than 16-million colors so the larger the image size, the more information you can hide [18].

Image Compression

Image compression is divided into two types of compression as follows.

- Lossless compression: it maintains every single bit of data exactly as it was originally in the file, when uncompressed all the information is completely restored. The most popular image formats that use lossless compression is GIF (Graphical Interchange Format) and BMP (bitmap file) [18].
- Lossy compression: the data in this type of compression is not conserved, portion of the information is eliminated, especially redundant information [19]. Therefore, the compressed image will not be the same as the original after decompression. JPEG (Joint Photographic Experts Group) image format is an example of lossy compression.

LSB Steganography

Least significant bit (LSB) substitution is mostly used to embed information within the last bit holding the least value in pixel byte of an image file. This technique works well for image steganography. The human visual system won't be able to detect the difference between the stego image and the cover image. In this method, we take the binary value of the secret information and overwrite the LSB of each byte within the cover image.
E.g. consider the following color encoding:

10100011 11100010 11111001
11000010 10101110
11100000 10010010
10000011

The LSB algorithm can hide the letter E having a binary value based on the ASCII code equal to 01000101, by changing the last bit in each byte as needed. This results in
10100010 11100011 11111000
11000010 10101110
11100001 10010010
10000011

This example demonstrates that to hide eight bits of data, only four of the eight least significant bits needed to be changed by the algorithm according to the embedded image.

The LSB substitution method introduces a very small change in the color of the pixel the change in the image is undetectable with the human visual system.

This technique can be directly applied on digital image in bitmap format as well as for the compressed image format like JPEG. In JPEG format, each pixel of the image is digitally coded using discrete cosine transformation (DCT). The LSB of encoded DCT components can be used as the carriers of the hidden message [20].

Steganography in JPEG

In the compressed JPEG image, the spatial domain is transformed into a frequency domain, thus we cannot modify pixel values in the spatial domain because the JPEG compression algorithm is lossy and causes too much noise. This means if we try embedding data on the LSB of pixel values we may not get the same pixel value after decompression. JPEG encoding has lossy and lossless stages. The Discrete cosine transformation (DCT) to the frequency domain and the quantization steps are lossy, whereas the entropy coding

that occurs after this point is lossless compression. Hence, a solution will be in hiding data after the Quantization stage. By embedding the information at this stage, in the transform domain, it is quite hard to detect the message because the embedding no longer takes place in the visual domain. The data embedding can take place by using LSB techniques, first the least significant bit of a JPEG coefficient is modified in order to embed one bit of confidential information, and then the embedded image coefficients are compressed using entropy encoding to finally produce the JPEG stego image as shown in Figure2. We should note that the receiver extracts the hidden message bits by reading the coefficients in the same sequence that the sender has used to embed it into the cover image and by using the same embedding algorithm.

Experiments and Results

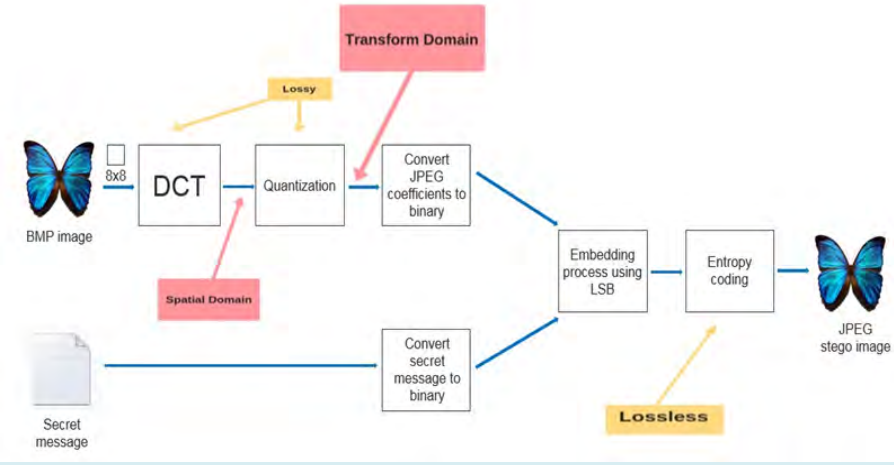

Figure 2: LSB steganography in JPEG.

We are going to show you how terrorists communicate online; a sender using the outguess algorithm to hide messages inside JPEG image files. And a receiver retrieving the message using the same algorithm. Experiments were conducted on an image dataset consisting of three JPEG images freely available in public domain on internet. The JPEG image's properties are shown in Table 1.

Picture name	Dimensions
Pic1.jpg	807x730 pixels
Pic2.jpg	500x477 pixels
Pic3.jpg	1892x1773 pixels

Table 1: Description of JPEG pictures used.

It is important to note that for our experiments, Oracle Virtual box version 5.2.8.21009 was used. Before selecting the steganographic algorithms to be used, it is important to consider the aspect of algorithm reputation either in spatial or transform domain, and the type of images we are using. Taking this information into consideration, the selected method is: Outguess, direct command in Ubuntu Linux.

The OutGuess steganographic algorithm was proposed by Neils Provos [21] to counter the statistical chi-square attack [22]. It hides messages in JPEG files, and works in two phases- embedding and correction steps. In the first pass, OutGuess embeds message bits along a random walk into the LSBs of quantized DCT coefficients while skipping 0's and 1's and flips the LSBs of coefficients to match them with the secret data bits. The embedding process will change the histogram of the quantized DCT coefficients, thus, the image is processed again while correcting the coefficients to make the stego image histogram match the cover image histogram. The chi-square attack and its generalized versions cannot detect messages embedded using OutGuess.

File Encryption, by the Sender

Because we already have a JPEG image, outguess will decompress it first, then recompresses using a user defined quality factor, in order to embed the message bits. The double compression applied here will make the detection very complicated.

Input: JPEG image, secret message.
Output: stego-image.

The command line used to embed the secret message into the cover image is the following:
$ outguess -d examplefile.txt image.jpg image-output.jpg

In case you want to specify a secret key, use the following syntax:

$ outguess –k "secret key" -d examplefile.txt image.jpg image-output.jpg

The "image-output.jpg" file is the final stego-image containing our confidential data which is shown in (figure 3).

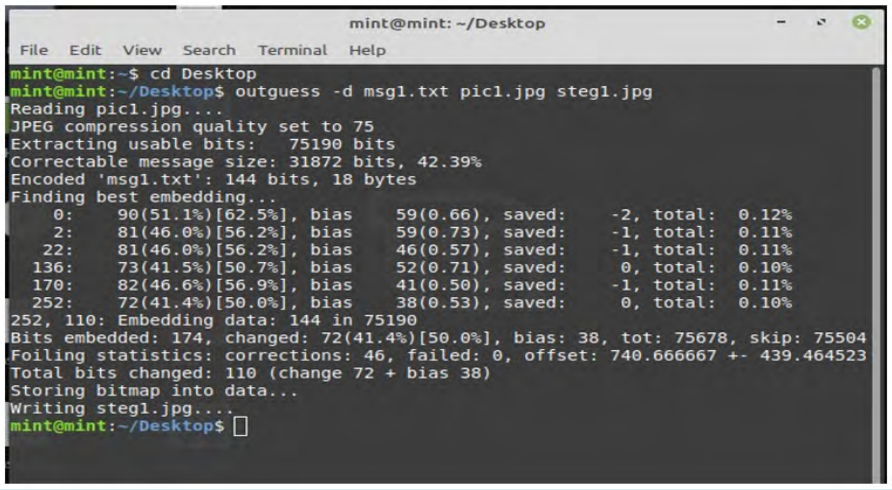

Figure 3: outguess embeds a message in an image in a matter of seconds.

File Extraction, by the Receiver

The recipient can use the following syntax in order to extract the original confidential file from the output image file it was embedded into (Figure 4):

$ outguess -r image-output.jpg secret.txt

$ outguess -k "secret key" -r image-output.jpg secret.txt (when a secret key was specified during encryption)

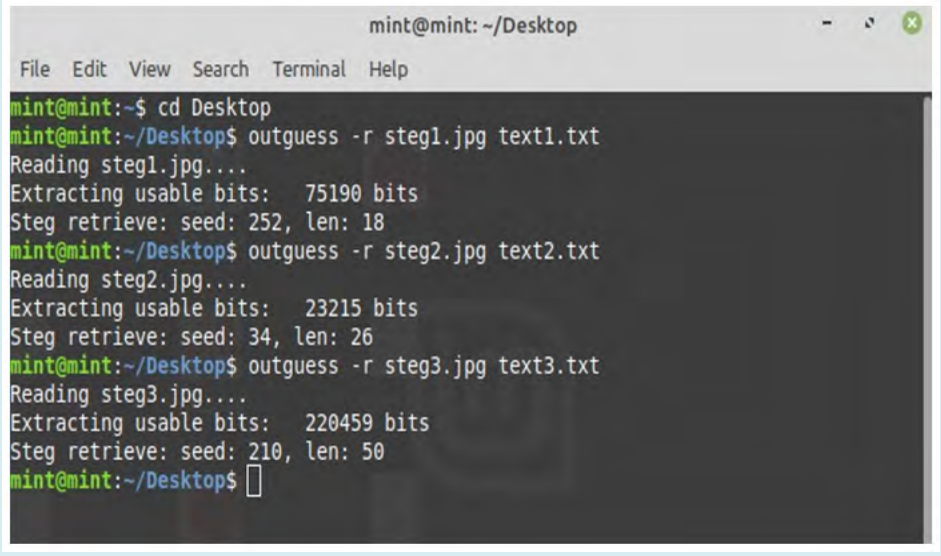

Figure 4: Extracting the hidden message using Outguess.

The Resulting Stego-Images

Figure 5: Left hand side images is the original JPEG cover images, where as right hand side we have the stego images containing the embedded message.

Steganography in Real Criminal Cases

Secret information exchange has been taking place since ancient times but the present digital and technological era provides numerous ways and choices to share such confidential messages. Criminals today are using steganography in order to communicate with other criminals, to share classified information and even to perform computer hacks, it is also used for illegal purposes such as crime, child pornography, cash drops and organizing terrorist attacks. In the business world steganography can be used to hide a secret chemical formula or plans for a new invention [23]. All of this is done in a way to make the information sharing inaccessible to law enforcement and to prevent any unauthorized persons to be aware of its existence. Currently, digital tools are widely available to ordinary computer users with basic computer skills also. The stego images can be shared using Social Media Sites such as Instagram, Facebook and Twitter or Online Social Networks (OSNs), which make them available to a very large number of individuals. We will be presenting specific cases in which steganography was used.

The first confirmed case of data concealment in real life was reported in 2010 by NBC [24]. Russian spies were using steganography to embed messages inside images then the stego images were uploaded to public websites. The huge number of pictures on the web and the endless stream of communications transmitted daily through it makes it hard for an investigator to detect the presence of the message and who it is aimed at.

Many articles claimed that after the September 11, 2001 attacks there were rumors that al Qaeda members used steganography to coordinate their actions, and for promoting child pornography although it was never confirmed.

NBC reported that German security officials caught a Pakistani Al Qaeda operative with a memory disk containing a pornographic video that embedded over 100 documents outlining plans for terror attacks through Europe [25].

An internet pedophile ring known as the "Shadowz Brotherhood" used steganography to transfer child pornographic material [26].

Digital steganography has been used by terrorists to facilitate secret intra-group communication as has been claimed. This is because terrorist use of digital steganography is both technically and operationally implausible [27].

Steganalysis Techniques for Computer Forensic Investigation

In today's society crime and cybercrime are considered as very challenging topics for law enforcement. Studying steganography covers and how they are transferred on online social networks is important because most of the time they are used for causing harm and for illicit purposes. Social media has become increasingly important and useful in solving crimes. Understanding how people might use steganography and social media for harm or even just as a means of communication could lead to breakthroughs in cases [28].

Steganalysis is emerging out as a process of detecting steganography. We should note that Steganalysis is mostly about discovering and identifying the existence of a concealed message, it essentially deals with the detection of hidden data. Digital forensics is the investigation of the steganography practiced by criminals on the network channel like TCP/IT protocol, to perform criminal communications, fraud, hacking electronic payments, gambling and pornography, harassment, viruses, pedophilia. So the first step for a forensic examiner would be to identify

the existence of the hidden message, and for the extraction considered as a second step it may be indeed complex and difficult, sometimes impossible if we have no idea about the tool or technique used for the steganopgraphy. Even if the steganographic tool was somehow discovered, extracting the hidden information can prove to be rather daunting as most algorithms employ cryptographic techniques to scramble the secret message when it is embedded [29]. Therefore it would be so challenging for the forensic investigator to recover the hidden information.

There are several types of steganographic attacks based on the information available for analysis. Some of them are as follows:

- Known carrier attack: The original cover file and stego object are both available for analysis. Steganography only attack: only stego object is available for analysis.
- Known message attack: The hidden message is known in this case.
- Known steganography attack: The cover file, stego object as well as the steganographic tool or algorithm, are known.

However in forensic investigations, the most likely situation the investigator will be in is when only the steganographic object is available, and that is assuming if an object can be classified as a steganographic object in the first place [29].

Steganalysis and steganography are two sides of the same coin, similar to cryptography and cryptanalysis, and computer viruses and antivirus software. The threat today is so serious because cybercrime is continuing to grow and the criminals are getting smarter and looking for ways to create malicious tools and software without getting exposed. Research in steganography involves both developing new techniques for hiding content and developing new tools for the detection and deciphering of hidden content. This duality is similar to biologic warfare, where the development of new biological weapons goes hand in hand with the research of their antidotes.

Forensic Tools for Steganography Detection

The plausibility of steganographic target formats increases with the amount of data transmitted in the respective format. JPEG images are widely used over internet and therefore they are an ideal target format for steganography [9]. Most of the steganalytic methods concentrate on one operation; feature extraction. We will show some examples of currently available softwares that can detect the presence of steganography programs, detect suspect carrier files, and disrupt steganographically hidden messages.

StegoArchive.com lists many steganalysis programs [30].

Guidance Software, Inc.

http://www.guidancesoftware.com

"Award winning and validated by the courts, EnCase allows law enforcement and IT professionals to conduct a powerful, yet completely noninvasive computer forensic investigation. EnCase features an intuitive GUI that enables examiners to easily manage large volumes of computer evidence and view all relevant files, including "deleted" files, file slack and unallocated space. The solution effectively automates core investigative procedures, replacing archaic, time-consuming and cost-prohibitive processes and tools."

Guidance Software, Inc.

ILook Investigator

http://www.ilook-forensics.org/

"ILook Investigator © is a forensic analysis tool used by thousands of law enforcement labs and investigators around the world for the investigation of forensic images created by many different imaging utilities."

ILook Investigator

Stegdetect and Xsteg (freeware)

Stegdetect was written by Niels Provos in 2001, the author of the steganography program called Outguess. Stegdetect is reliable in detecting JPEG images that have content embedded with JSteg, JPHide and OutGuess [21].

Stegdetect can find hidden information in JPEG images using such steganography schemes as F5, Invisible Secrets, JPHide, and JSteg [30].

Access Data's Forensic Toolkit and Guidance Software's EnCase

These softwares can use the HashKeeper, Maresware, and National Software Reference Library hash sets to look for a large variety of software. In general, these data sets are designed to exclude hashes of known "good" files from search indexes during the computer forensic analysis [30].

Forensically Beta

Forensically beta is a website used for JPEG steganalysis (Figure 6).

This website allows to detect differences between the original JPEG cover image and the embedded one, therefor no analysis is possible without the original JPEG.

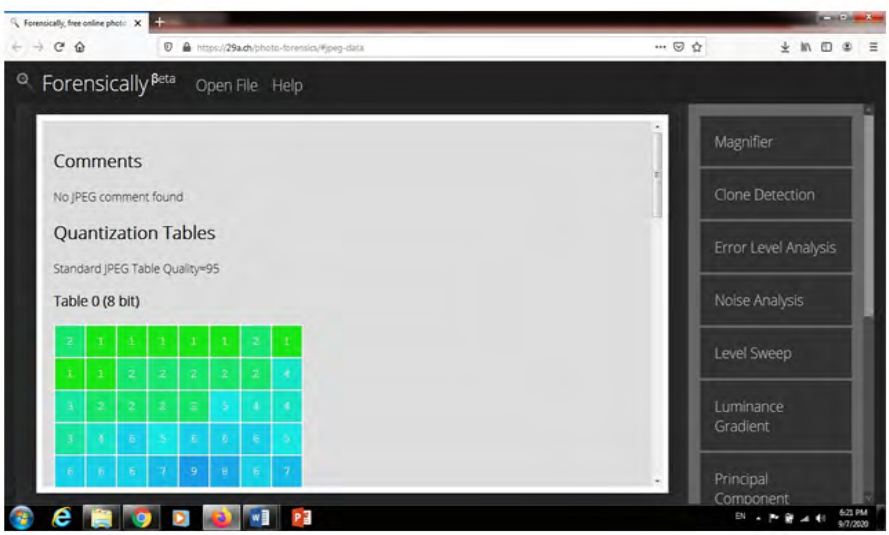

Figure 6: Forensically beta. https://29a.ch/photo-forensics/#jpeg-data

We tried several tools available on the website and we will present the figures showing the differences between the original JPEG file pic1.jpg and the stego-image steg1.jpg.

Figure 7: pic1.jpg principal component analysis.

Figure 8: steg1.jpg principal component analysis.

Figure 9: steg1.jpg Noise analysis.

Figure 10: pic1.jpg Noise analysis.

Figure 11: pic1.jpg clone detection.

Figure 12: steg1.jpg clone detection.

Discussion

Our experimental study has shown how easy hiding secret information using steganography methods are. It doesn't require so many skills, just some basic research and knowledge about the subject, what made it available and possible for any normal person to use. But the question remains, how far a forensic examiner can detect the presence of the hidden messages using forensic steganalysis methods because the variety of steganographic methods may be considered as an obstacle and the steganalysis techniques might be able to detect some of the embedding methods and not detect others. Some methods with a very good performance for detecting exclusively transform domain steganographic methods [31,32] are available. We have other methods that outperform one steganographic method and underperform over another [33]. Steganalysis methods may be capable to reliably detect steganography only for specific embedding rates. For instance, this can be shown in the results of a recent experiment [34]. Many steganalysis software and tools are available but they show numerous challenges and difficulties so it would be of great value to check even more and more of them.

Conclusion

In recent years, Steganography has emerged as a growingly active research topic. The past few years have seen an increasing interest in using images as cover media for steganographic communication, mostly JPEG image file format.

However, while implementing image steganography is important, the steganalysis methods to detect and embed the secret message are far more complex than actually doing the steganography itself and it needs to be an area of ongoing research. Today's steganographic programs can hide any type of secret data into various types of cover media. It is so difficult, nearly impossible to predict whether there is a secret message to begin with at first place. Given this fact, there is a lot of research working on discovering new techniques for steganalysis, and it would be interesting to see how accurate they will be at detecting Steganography.

Finally, it is clear that the use of steganography by terrorists and criminals is likely to increase in the future, posing a problem for law enforcement agencies. Steganalysis needs to be further developed to help counter high tech terrorism and cases of child pornography and others.

References

1. Warkentin M, Bekkering E, Schmidt MB (2008) Steganography: Forensic, Security and Legal Issues. ADFSL 3(2): 17-34.

2. Attaby AA, Mursi Ahmed MFM, Alsammak AK (2018) Data hiding inside JPEG images with high resistance to steganalysis using a novel technique: DCT-M3. Ain Shams Eng J 9(4): 1965-1974.

3. Yunus YA, Rahman SA, Ibrahim J (2013) Steganography: a review of information security research and development in Muslim world. Am J Eng Res 2(11): 122-128.

4. Singhal V, Yadav D, Bandil DK (1956) Steganography and Steganalysis: A Review. Int J Electron Comput Sci Eng 1(2): 399-404.

5. (2015) Least Significant Bit (LSB) and Discrete Cosine Transform (DCT) based Steganography 2(1): 31-36.

6. Zakaria A, Chaumont M, Subsol G (2018) Quantitative and binary steganalysis in JPEG: A comparative study. Eur Signal Process Conf, pp: 1422-1426.

7. Kaur G, Kochhar A (2012) A Steganography Implementation based on LSB & DCT. International Journal for Science and Emerging, Technologies with

Latest Trends 4(1): 35-41.

8. Sohag SA, Islam K, Islam B (2013) A novel approach for image steganography using dynamic substitution and secret key. Am J Eng Res 2(9): 118-126.

9. Bed Elgabar EEA (2013) Comparison of LSB Steganography in BMP and JPEG Images. Semantic Scholar.

10. Pan Y, Ni J, Su W (2016) Improved uniform embedding for efficient JPEG steganography. Lect Notes Comput Sci 10039(5): 125-133.

11. Hiney J, Dakve T, Szczypiorski K, Gaj K (2015) Using Facebook for image steganography. Proc. - 10th Int Conf Availability, Reliab Secur ARES, pp: 442-447.

12. Wang Y, Zhang W, Li W, Yu N (2021) Non-Additive Cost Functions for JPEG Steganography Based on Block Boundary Maintenance. IEEE Trans Inf Forensics Secur 16: 1117-1130.

13. Denemark T, Fridrich J (2017) Model based steganography with precover. Society for Imaging Science and Technology 11: 56-66.

14. Li W, Zhang W, Chen K, Zhou W, Yu E (2018) Defining joint distortion for JPEG steganography. IH MMSec 2018 - Proc. 6th ACM Work Inf Hiding Multimed Secur, pp: 5-16.

15. Sajid Ansari A, Sajid Mohammadi M, Tanvir Parvez M (2019) A Comparative Study of Recent Steganography Techniques for Multiple Image Formats. Int J Comput Netw Inf Secur 11(1): 11-25.

16. Giboulot Q, Cogranne R, Bas P (2020) JPEG steganography with side information from the processing pipeline. ICASSP, IEEE Int Conf Acoust Speech Signal Process Proc, pp: 2767-2771.

17. Sinha B (2015) Comparison of PNG & JPEG Format for LSB Steganography. International Journal of Science and Research 4(4): 198-201.

18. Css U, Jpegs P, Machines IB (2013) Images Best Practices Guide.

19. Taubman DS, Marcellin MW (2002) Image Compression Overview. JPEG2000 Image Compression Fundam Stand Pract, pp: 3-21.

20. Al-Shatnawi AM (2012) A new method in image steganography with improved image quality. Appl Math Sci 6(79): 3907-3915.

21. Richer P (2003) Steganalysis: Detecting hidden information with computer forensic analysis. SANS Inst Info Sec Read Room.

22. Chutani S, Goyal A (2019) A review of forensic approaches to digital image Steganalysis. Multimed Tools Appl 78(13): 18169-18204.

23. Doshi R, Jain P, Gupta L (2012) Steganography and its Applications in Security. Int J Mod Eng Res 2(6): 4634-4638.

24. (2010) Fbi: Russian spies hid codes in online photos. News.

25. (2012) How Al Qaeda Hid Secrets In a Porn Video. News.

26. (2002) Accessing the secrets of the brotherhood. BBC News.

27. Conway M (2003) Code wars: Steganography, signals intelligence, and terrorism. Knowledge, Technol. Policy 16(2): 45-62.

28. Trotter LK (2019) A case study involving creating and detecting steganographic images shared on social media sites.

29. Ibrahim A (2007) Steganalysis in computer forensics. Proc 5th Aust Digit Forensics Conf, pp: 98-108.

30. Kessler G (2004) An Overview of Steganography for the Computer Forensics Examiner. Forensic Sci Commun 6(3): 1-29.

31. Pérez JDJS, Rosales MS, Cruz Cortés N (2016) Universal steganography detector based on an artificial immune system for JPEG images. IEEE Trustcom/BigDataSE/ISPA, pp: 1896-1903.

32. Andriotis P, Oikonomou G, Tryfonas T (2013) JPEG steganography detection with Benford's Law. Digit Investig 9(3-4): 246-257.

33. Wu Y, Zhang T, Hou X, Xu C (2016) New blind steganalysis framework combining image retrieval and outlier detection. KSII Trans Internet Inf Syst 10(12): 5643-5656.

34. Yanping Z, Yang X, Kaveh G, Jingyuan Z, Hongmei D (2012) A survey of cyber crimes. Secur Commun Networks 5(4): 422-437.