

Data hiding in anti-forensics – Exploit delivery through digital steganography

GHASHI, Hans, ZARGARI, Shahrzad <<http://orcid.org/0000-0001-6511-7646>> and JALALI, Setareh

Available from Sheffield Hallam University Research Archive (SHURA) at:

<https://shura.shu.ac.uk/32747/>

This document is the Accepted Version [AM]

Citation:

GHASHI, Hans, ZARGARI, Shahrzad and JALALI, Setareh (2024). Data hiding in anti-forensics – Exploit delivery through digital steganography. In: JAHANKHANI, Hamid, (ed.) Cybersecurity Challenges in the Age of AI, Space Communications and Cyborgs Proceedings of the 15th International Conference on Global Security, Safety and Sustainability, London, October 2023. Advanced Sciences and Technologies for Security Applications (ASTSA) . Cham, Springer. [Book Section]

Copyright and re-use policy

See <http://shura.shu.ac.uk/information.html>

Data Hiding in Anti-Forensics – Exploit Delivery through Digital Steganography

Authors: Hans Gashi, Dr. Shahrzad Zargari, Setareh Jalali

Abstract

“Developments in digital forensics investigations have occurred along with those in anti-forensics. Legal issues involving cybercrime are difficult to investigate and even more difficult to prosecute since a forensic investigator must often develop a case by examining artefacts left on a device or network. When cyber criminals became more aware of the techniques utilized in digital forensics, countermeasures to these approaches were developed. The goal of these procedures is to sabotage forensic investigations, and many of them are readily available and simple to use. The purpose of this research is to improve our understanding of these Anti-Forensic technologies by doing in-depth individual analyses and discussing the functionality and methods, as well as the possibilities of mitigation.

The topic of this Anti-Forensics study is within Data Hiding; there are different ways available; however, this project focuses on a steganography tool known as Stegosploit and looks to see if embedding JPG images with malicious code without visual distortion of the image is conceivable.”

Keywords: Anti-Forensics, Digital Forensics, Data Hiding, Steganography, browser exploit delivery

1. Introduction

In the digital era, with the rapid evolution of cybercrime, both in methodology and frequency of occurrence, digital forensics has become a crucial element of the judicial system. While digital forensics aims to legally acquire and examine collected evidence, Anti-Forensics aims to hinder that process by applying a variety of methods such as manipulating, hiding, or wiping data through respective tools. Cybercriminals may even aim to diminish the credibility of evidence as this is often enough to disrupt a forensic investigation. This work presents a data hiding method that allows for embedding images with undetected malicious code that can be later extracted. Hiding data in images is known as Steganography. The focus of this study is a steganography method called Stegosplit, this tool can deliver browser exploits while avoiding detection. Understanding the foundations of tools of this nature as well as the options available for mitigation is necessary in order to advance our understanding of Anti-Forensics.

Current research of individual Anti-Forensic tools is quite limited, this may be because efforts for countering AF are generally only made once necessary, for example, should a forensic investigator find evidence that an AF (Anti-Forensic) process has been used within a case, they may then proceed towards mitigation of that method. "The lack of true innovation in the forensic world is because there's no pressure to do so" (Foster & Liu, 2005). This is not the case for Anti-Forensics, as constant innovation is a requisite in order to reliably hinder forensic investigations.

This study aims to further our understanding of AF techniques and how they may impact the investigative process. For every new digital forensic technique developed, cybercriminals look to implementing a related counter-technique (Raghavan,2013). This creates an endless cycle, with this constant evolution of Anti-Forensics, it became necessary to consider as a part of DFIR (Digital Forensics & Incident Response). In order to achieve better results when countering Anti-Forensics, performing individual analysis of these tools is a vital step in understanding the underlying mechanisms, this will aid in the efforts for defining and categorizing of Anti-Forensics which began in the early 2000's (Garfinkel, 2007).

A data set of 308 known tools that can be considered as anti-forensic based on their characteristics was proposed by (Rogers, 2006) as part of an anti-forensic taxonomy that defines and categorizes these tools. (Conlan, 2016) devised an extended AF taxonomy in the hopes of facilitating a form of standardization for AF. However, while research on Data hiding & Steganography is plentiful, very little research could be found that investigates Stegosplit or any other Drive-by (malicious content that is able to exploit vulnerabilities in a browser without the users knowledge) browser exploits. This study aims to fill this gap in research and explicitly detail the mechanisms of Stegosplit and undetected payload delivery in browsers. Therefore, in contribution to these efforts, the following research questions have been formulated:

How can digital steganography techniques be utilized to embed hidden data into the pixels of a JPG file without altering the image, and what strategies can be employed to mitigate and categorize Stegosploit within a standardized taxonomy of Anti-Forensics (AF) tools?

The aim of this research is to address the research questions by pursuing several objectives and deliverables. The objectives include evaluating current literature on browser exploits to enhance our understanding of Anti-Forensics (AF) tools through individual analysis. Additionally, conducting the Stegosploit experiment in a secure virtual environment with simulated parameters to assess the feasibility of delivering hidden data through JPG files as carriers. Furthermore, measuring the effectiveness of the Anti-Forensic Tool and documenting the process of hiding, preserving, and delivering information using Stegosploit. Lastly, exploring countermeasures against this AF method and evaluating their success in detecting suspicious content. By accomplishing these objectives, this research aims to contribute to the field of tackling Anti-Forensics.

2. Literature Review

The following section highlights research material that was gathered to aid with the development of the study.

2.1 Introduction to Digital Forensics, Anti-Forensics & Current Challenges

Digital Forensics in simple terms, is the extraction of any information that may be useful to a forensic investigation contained on an electronic device (Etow, 2020). In 2001 the first Digital Forensic Research Workshop took place, this workshop intended to set the foundations of a wider community of specialists and academics for Digital Forensics. It aimed to set in motion works towards a clear definition of DF as well as furthering our understanding of the greatest challenges in the field. They would proceed to define Digital Forensic Science as:

“The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate unauthorized actions shown to be disruptive to planned operations.” (DFRWS, 2001).

Although AF is not a new or even recent concept, it lacks a universal standardized definition (Harris, 2006). A myriad of studies would posit that the bedrock of AF is the process a cybercriminal observes when attempting to hide their electronic footprint so that it remains undetectable during a forensic investigation (Mothukur, 2019). Whereas other studies such as (Foster and Liu, 2005) would suggest that AF is the act of avoiding detection and breaking tools or (Shirani, 2002) who defined AF as hiding attempts at system intrusion.

The relationship between Digital Forensics & Anti-Forensics has grown to a stage where should we fail to find a clear research strategy upon which collective works can be developed with a clear goal, advancements in DF (Digital Forensics) will start trailing behind those in AF. This was addressed by (Beebe,2009) which argues that DF is no longer a niche discipline, and it is now common knowledge that any action taken on an electronic device or network leaves a digital footprint. Comparatively, other sources would state that despite the development of AF tools, many of them freely available, AF largely remains present on only the most complex DF investigations (POST, 2016)

The “Golden Age” of DF is said to have occurred between 1990 – 2010. (Vincze, 2016) suggests that throughout those years DF could be defined by several characteristics such as:

- Relatively few file formats.
- Investigations would generally be within a single device.
- Majority of computer systems operating on Microsoft Windows.

However, the capabilities of DF developed over the last decade are at risk of becoming obsolete in the future due to the transformation of computing technology. (Garfinkel, 2010) when discussing challenges in DF in the next 10 years suggests that some of the contributing factors may be:

- Considerably larger storage on devices, increasing the time it takes when creating and processing a forensic image.
- Development of Embedded Storage, this makes it so storage on devices can no longer easily be removed & imaged.
- The propagation of different file formats and OS has greatly increased complexity when dealing with data processing tools.
- The scope of forensic investigations is largely defined by regulations and other legal challenges.

2.2 Anti-Forensics – Data Hiding

The practice of storing information in locations where it is unlikely to be found is known as Data Hiding. (Blunden, 2009) defines data hiding as “a method of security through obscurity”, this refers to act of integrating an obscure piece of data into a host source whilst maintaining the integrity of said source, this would operate through a different communication scheme when compared to how normal data transfer and communication occurs, meaning that hidden data relies on the host source for transmission (Sencar, 2005). The difference between normal data communication and communication of hidden data is that hidden data requires a host signal in which a secret message is embedded and then must be extracted upon transmission, whereas traditional data communication simply sends and receives message signals through a transmission channel.

There is a multitude of methods available to hide data, some of the more traditional methods include tampering with the metadata of certain file extensions, hiding data in unallocated or slack space, use of MBR (Master Boot Record), device driver registers and tables which may be allocated but are not in use or even partitions on a device hard drive that are potentially hidden & encrypted, however the vast majority of these methods can be discovered by forensic tools (Budimir & Slay, 2007).

In contrast to this, there is still methods of data hiding that make use of unreachable locations such as unallocated space that are ignored by available forensic tools, a compiled list of such methods is shown in Table 2.1.

Data Hiding Tool	Functionality	Source
Metasploit's Slacker	Hides data within slack space of NTFS or FAT file systems.	(Göbel & Baier, 2018)
FragFS	Hides data in the NTFS MFT (Master file Table).	(Garfinkel, 2007)
RuneFS	Stores data in “bad blocks”.	(Grugq, 2003)
Waffen FS	Hides data within ext3 journal file.	(Eckstein and Jahnke, 2005)
KY FS	Stores data in directories.	(Grugq, 2003)
Data Mule FS	Hides data in inode reserved space.	(Grugq, 2003)

Table 2.1 Data Hiding - Available File System Tools

2.3 Steganography Techniques

An example of one of the earliest effective methods of data hiding is Steganography. It can be summarized as the act of hiding secret information inside a carrier file (Abboud et al., 2010). These carrier files can consist of a variety of different file types, including, audio or image files, certain video file types and executable files (StegoArchive.com, 2005).

As the scope of this study is steganography in images and whether it's possible to encode and deliver exploits without affecting the image itself, a review was conducted examining research on the effectiveness of known methods of image steganography. The most popular survey of steganography techniques is that of (Johnson, 2000), while the majority of the techniques discussed in that survey are still relevant today, we must factor in that this work was published over 20 years ago. We can reasonably assume that in that time digital steganography has developed drastically and new methods have become available. This was addressed by (Hamid, 2012) who would devise a more current taxonomy of image steganography methods. In comparison, whilst (Johnson, 2000) discussed the ability of the reviewed techniques to hide information, (Hamid, 2012) took a more in-depth approach by also accounting for how much information could be hidden and the robustness of these image processing tools. Referring to this paper's research gap, regardless of in-depth surveys such as these, little research is available that individually analyzes and investigates available steganography tools beyond the most popular options.

When discussing the effectiveness of image steganography methods, (Lin, 1999) states that each technique can be weighed against the following characteristics:

- Robustness – This is the ability of an image to remain intact should it go through a process that changes the image itself such as resizing or cropping after embedding.
- High-Capacity Perceptual Transparency – Refers to the amount of degradation a carrier image undergoes after the maximum amount of information has been embedded into the image, meaning the perceived quality of the embedded image when compared to the original.
- Temper Resistance – This is how difficult it would be to change the information after embedding into an image.
- Computation Complexity – Measures how expensive or resource intensive the process of embedding and extracting a hidden message is.

Though there are many methods of image steganography such as Marking & Filtering, Distortion Techniques and Domain Transformation Techniques, the work performed on this paper looks to make use of hiding data by changing the least significant bit (LSB) values within the image pixels. This technique is known as Spatial Domain. During his work surveying image steganography techniques Hussain (2013) would broadly classify Spatial Domain Techniques into the following categories:

- Random Pixel Embedding (RPE)
- Pixel Value Differencing (PVD)
- Least Significant bit (LSB)
- Histogram Shifting method
- Pixel intensity-based methods

The developments made in the field of AF in recent years through constant updates and release of new methods have created an ever-growing gap between those in Digital Forensics. The major gap identified in the research stage of this study is the lack of in-depth individual analysis of current AF tools, beyond proposed taxonomies and surveys that aim to categorize AF tools in the hope of aiding our understanding, minimal research is available that sufficiently inquires about the fundamental mechanisms of these tools or that discusses specific mitigation methods. This gap further widens when discussing methods developed in recent years. Therefore, this study will focus on the examination of a Steganography tool known as Stegosplit of which no current research papers could be found, in addition to this, this paper also looks to investigate the possibility of mitigation of this tool in the hopes of aiding future forensic investigations being confronted by this AF method.

Throughout this literature review, much new information relating to the broad spectrum of data hiding as well as steganography itself was gained, it was interesting to delve into the current steganographic techniques and discover the true depth of this field. The sheer number of techniques available only highlights the problem digital forensics faces. Another interesting aspect was the consideration that AF should not be considered as a tool used exclusively by the criminal class and that it does in fact have legitimate uses by those seeking to protect their own privacy. Whether it is beneficial to excuse the use of some tools despite them being AF in nature is yet to be seen. For example, one might ask what possible use an average user could find in Digital Steganography except for acting on malicious intent.

Furthermore, it was interesting to find that despite AF being an issue shared by the entire digital forensic community, there is still many differences of opinions when attempting to define AF itself, its objectives and whether its existence serves only to hinder forensic investigations.

3. Results & Discussion

Any digital image in essence is simply a correlation of pixels that have been arranged so that the desired output is displayed. Every individual pixel is characterized by 3 color channels known as RGB (Red, Green, Blue), where each of these channels is represented by its own 8-bit value, which in turn allows for a total of 256 possible levels of color. For example, if we were to analyze an image with only a black & white or greyscale color scheme, we would find that the values for RGB would be the same throughout each pixel. In order to aid with the visualization of this, consider an image that has been sliced into 8 separate panes where each individual pane is its own bit layer. The first bit layer (Bit layer 0) naturally has the least impact on the overall image and is therefore known as the image's LSB (Least-Significant Bit). Thus pixels in bit layer 1 are composed of values of the second least-significant bit. This in turn would make bit layer 7 the most important layer as it has the most effect on the output of the image itself, for this reason, it is called the Most-Significant Bit (MSB) (Rustad, 2021).

Accordingly, encoding an exploit onto the higher bit layers of an image (Layers 3,4,5,6 & 7) will result in distortion of the image, significant enough that it will be noticeable to the human eye. Therefore, encoding the exploit into the lower bit layers should show minimal or possibly no aberration of the image, even to close inspection.

When replacing values of the LSB with the code representing the hidden data, in our case a JavaScript exploit, individual binary bits of the image pixels are changed to fit the encoded hidden data so that the visual aberration of the image is negligible to the human eye. If we were to select a specific pixel color channel bit stream from the original image such as:

```
10010101 00001101 11001001
```

```
10010110 00001111 11001010
```

```
10011111 00010000 11001011
```

Taking the following random 8 bits from the converted hidden data embedded as an example,

```
101101101
```

Hiding those 9 bits from a segment of our hidden data in a selected pixel is simply a matter of changing the last bit in each sequence of 8 bits from the original image pixel bit stream as needed. Resulting in:

```
10010101 00001100 11001001
```

```
10010111 00001110 11001011
```

```
10011111 00010000 11001011
```

By using the method this example shows that it is only necessary to change the four out of the nine LSB in those nine bytes (Warkentin,2008). Changing the last bit results in a slightly different colored pixel but remains indistinguishable from the original when viewing the image.

However, regardless of bit layers, pixel loss is always a possibility when altering the bits of an image. To overcome this, an iterative encoding technique is used which allowed for error-free decoding of the exploit code.

The study specification set out at the beginning of this work was to determine “Can digital steganography be used to embed hidden data into pixels of a JPG file without affecting the image?”. This research question remained the same throughout this study as the existing literature review conducted showed that there currently a gap in research when discussing individual analysis of AF tools that sufficiently evaluates their mechanisms in order to better understand how they can affect DF investigations. No research could be found that relates to Stegosploit and the data hiding method that it employs.

To ensure that this research question is answered, and the stated research gap addressed, the experiment conducted in this study provides a detailed overview of the process that Stegosploit uses to embed an image with hidden data, discussing the intricate mechanisms of the tool such as the process it undertakes when encoding and decoding hidden data in a JPG image via conversion of the data into a bit stream that is then sporadically hidden within its pixels in the form of a grid. In order to adequately analyze this AF tool so that future DF investigations concerning this steganography technique are able to efficiently recognize when these actions have been appropriated, in addition to detailing the process that this AF tool undertakes, the experiment also demonstrates how a cybercriminal may then use a stenographically encoded image to initiate an attack. For this purpose, the embedded image is used as a part of a browser exploit delivery method where the embedded JavaScript exploit is executed once the web page is visited, or the image is clicked.

From the results gained in the experiment it was found that the embedded exploit code becomes much more visually apparent on pixel layers 3,4,5,6 & 7, therefore it is safe to assume should an attacker employ this tool, they would naturally hide their data in the lower layers of an image as to make it impossible to notice only through visual inspection of the image.

Addressing the research question of this study and the initial hypothesis: Encoding JPG images with hidden data is possible with no noticeable visual distortion of the image.

The results show that the hypothesis was correct when stating that it is possible to encode JPG images with hidden data with no visual aberration of the image provided that the data being hidden is encoded onto Bit-Layers 0 to 2, as using layers above those has a more prominent effect on the overall image, so much so that even a visual inspection of the image in passing is enough

to detect that the image has been tampered with defeating the primary purpose of this stenographic technique.

Stegosplit is a relatively new AF tool, only a handful of researchers have ever conducted works involving it. While there is plentiful research available when discussing the methods available for steganalysis and detecting stenographically altered content, techniques that look to counter images generated by Stegosplit are practically non-existent. In relation, (Park, 2015) published works showing possible methods available to protect networks from hidden exploits and Jeysekar (2016) discussing their analysis of Stegosplit images or (Harblson, 2015) who analyses techniques for hacking with images through Stegosplit. However, these authors all discuss in detail various characteristics of Stegosplit, there is no focus on the means of mitigating of this tool.

As Stegosplit hides the malicious data within an image acting as a carrier file, it can easily evade even modern anti-virus software as it is treated as a regular JPG file that does not raise any flags, this is due to the malicious code embedded into the image not being directly visible.

The main focus of this study being an in-depth analysis of the functionalities of Stegosplit, showing its mechanisms as well as how it may be used maliciously, so that future forensic investigations are able to efficiently respond. It is beyond the scope of this study to establish how direct mitigation of Stegosplit can be implemented. Regardless of this, some research was conducted in order to allow future researchers an avenue in which they may develop a fixed method of mitigation.

Countering and mitigation of Stegosplit may prove more successful if the focus is shifted from attempting to directly detect encoded images to the detection of polyglots as this is the primary route Stegosplit takes for browser exploit delivery. An example of this is the work conducted by Vaidya & Rughani (2019), who presented a method of polyglot detection by analyzing signatures of both a regular JPG and one that has been stenographically encoded through HxD (Hex Editor) and designing a python script that detects polyglots based on this observation.

The initial goals of this study were to contribute to the immense work that is required to create a standardized definition and understanding of Anti-Forensics so that we may allow for purposeful development of Digital-Forensics tools and techniques. This is outlined in the work of many authors who looked to create a grand taxonomy of Anti-Forensic tools so that a systematic analysis of these methods could be performed. It is only by inquiring about individual tools available through collective works that are frequently adapted that we may hope to truly bring to light the scale of the threat that Anti-Forensics poses to forensic investigations.

The experiment performed in this study successfully detailed the processes that the Anti-Forensic tool Stegosplit undertakes when stenographically hiding data in the pixel layers of JPG file. An in-depth analysis was performed of the encoding and decoding mechanisms of the tool as well

as how it is able to deliver malicious code without user knowledge via polyglots. This meticulous work along with the options available for mitigation to the best of the researcher's ability, allows for this tool to be added to future granular taxonomies of Anti-Forensic tools hoping to further digital forensic science or already available works such as that of (Conlan, 2016) extended granular taxonomy of Anti-Forensic tools or (Katamara, 2020) taxonomy of countermeasures to Anti-Forensic tools.

3.1 Limitation of Study and Future Work:

Throughout this study, a number of unanticipated obstacles were met. The most apparent was the researchers lack of experience with the JavaScript programming language which affected the ability to use JavaScript exploits when embedding the image. Some difficulty was found when attempting to appropriate the syntax to fit Stegosplit. Due to this, a simple JavaScript alert was used in the place of an exploit to show the execution of the code upon delivery. Future researchers more familiar with JavaScript should have no issues when implementing exploits into the tool following the methodology shown in this paper. Another limitation of the study is the tools lack of support for other file types such as PNG or GIF files, Stegosplit is unable to encode and decode JavaScript exploits on any other file type excluding JPG due to the differences in file infrastructure. Lastly, there are some browsers available that do not support JavaScript and therefore inhibit the process that Stegosplit takes, making it impossible to execute exploits in the manner in which the tool is designed.

Future research in the field of Anti-Forensics and Steganography tools should look towards establishing a direct mitigation and detection method of malicious images as well as conceptualizing an expanded steganography subcategory for tools akin to Stegosplit in order to aid with categorization in future Anti-Forensic tool taxonomies. Regarding Stegosplit, future directions for research could include discovering a method that allows multiple browser compatibility for steganographically embedded JPG images as well as how these images can withstand resizing and compression without data loss.

4. Conclusion

To conclude this study, the initial aim of this research was to aid in the understanding of Anti-Forensic techniques through in-depth individual analysis so we may then be able to better recognize how they affect forensic investigations. From the literature review conducted, it was noted that the availability of research that looks to examine the intricate functionalities of specific tools was lacking. This was even more apparent when delving into Anti-Forensics through Steganography. Minimal Research was available that thoroughly discussed the relevant parameters such as the purpose, functionality and mitigation. Many authors discussing current Anti-Forensic tools would postulate that in order to close the gap between developments made in Anti-Forensics to those in Digital forensics, a comprehensive study of specific tools is necessary. Therefore, this study attempts to fill this gap in research having thoroughly analyzed the steganography tool Stegosplit, meeting all the relevant parameters mentioned above so that our understanding of this tool is adequate enough that it is ready to be added to taxonomies of Anti-Forensic methods easing the transition into real world application should a digital forensic investigator be met by this data hiding tool.

When referring to the research question proposed at the beginning of this study as well as the hypothesis, it can be said that they have been answered successfully and the objectives met. The initial hypothesis stating: "Encoding JPG images with hidden data is possible with no noticeable visual distortion of the image", upon experimenting the results showed that the hypothesis was correct in that it is possible to hide data within a JPG file without distortion noticeable to the human eye. However, it was found that this only remains true should the data be hidden in the lower bit-layers of the image (LSB) as embedded data into the higher layers or the MSB causes significant aberration of the image and would therefore defeat the purpose of the tool by making it considerably easier to discover that the image has been tampered with.

This research also looked further to inquire the mitigation methods available for Stegosplit as well as how it may be categorized in taxonomies looking to standardize Anti-Forensic tools and methodologies. Upon research, it was found that at the time of this study, options targeting direct mitigation of this tool are currently widely unavailable, this may be due to the fact that it is a relatively new Anti-Forensic method and remains a somewhat niche technique for cyber criminals to implement. However, it is safe to assume that this will change in the future and that options for mitigation need to be considered. The possibility of implementing a method that looks to shift the focus from detecting malicious images to the detection of polyglots for Stegosplit is mentioned as upon analysis of the tool, this mitigation method is the most appropriate. When looking towards categorization, Stegosplit falls under Steganography related Anti-Forensic tools, however, based on the work conducted on this report, creation of further subcategories for Steganography tools should be considered. This is due to the nature in which Stegosplit performs its stenographic process by altering specific pixels and the means by which it exploits vulnerabilities.

References

1. Abboud, G., Marean, J., & Yampolskiy, R. V. (2010). Steganography and Visual Cryptography in Computer Forensics. 2010 Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering. <https://doi.org/10.1109/sadfe.2010.14>
2. B. Blunden, (2009) The rootkit arsenal escape and evasion is the dark corners of the system, Wordware Publishing.
3. Beebe, N. (2009, January). Digital forensic research: The good, the bad and the unaddressed. In IFIP International conference on digital forensics (pp. 17-36). Springer, Berlin, Heidelberg.
4. Budimir, N., & Slay, J. (2007). Identifying Non-Volatile Data Storage Areas: Unique Notebook Identification Information as Digital Evidence. *Journal of Digital Forensics, Security and Law*, 2(1), 75-91.
5. Conlan, Kevin & Baggili, Ibrahim & Breitingner, Frank. (2016). Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. *Digital Investigation*. 18. 10.1016/j.diin.2016.04.006.
6. DFRWS Technical Committee (DFRWS) (2001) A road map for digital forensic research: DFRWS Technical Report. DTR-T001-01
7. Etow, T. R. (2020). IMPACT OF ANTI-FORENSICS TECHNIQUES ON DIGITAL FORENSICS INVESTIGATION. Available from: <http://urn.kb.se/resolve?urn=urn:nbn:se:lnu:diva-97116>
8. Foster, M. A., & Liu, V. (2005). *Catch Me If You Can*. Congressional Research Service.
9. Garfinkel S., (2007), "Anti-forensics: Techniques, detection and countermeasure," 2nd International Conference on i-Warfare and Security, vol. 20087, pp. 77–84.
10. Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *digital investigation*, 7, S64-S73.
11. Hamid, N., Yahya, A., Ahmad, R. B., & Al-Qershi, O. M. (2012). Image steganography techniques: an overview. *International Journal of Computer Science and Security (IJCSS)*, 6(3), 168-187.
12. Harblson, C. (2015). Hacking with pictures; new stegosplit tool hides malware inside internet images for instant drive-by pwning

13. Harris, R. (2006). Arriving at an Anti-Forensics Consensus: Examining How to Define and Control the AntiForensics Problem. Proceedings of the 2006 Digital Forensics Research Workshop. Digital Investigation, 3(S), S44-S49. Available from: <http://dfrws.org/2006/proceedings/6-Harris.pdf>
14. Johnson, N. F., & Katzenbeisser, S. (2000). A survey of steganographic techniques. In Information hiding (pp. 43-78).
15. Katamara, Ziada, "Taxonomy for Anti-Forensics Techniques & Countermeasures" (2020). Culminating Studys in Information Assurance. 109. Available From: https://repository.stcloudstate.edu/msia_etds/109
16. Mothukur, Abhinav & Balla, Akhil & Taylor, Dandy & Sirimalla, Shiva & Elleithy, Khaled. (2019). Investigation of Countermeasures to Anti-Forensic Methods. 1-6. 10.1109/LISAT.2019.8816826.
17. Park, B., Kim, D., & Shin, D. (2015). A Study on a Method Protecting a Secure Network against a Hidden Malicious Code in the Image. Indian Journal of Science and Technology, 8(26).
18. Rogers, M, (2006). Anti-forensics: the coming wave in digital forensics.
19. S. Raghavan, (2013) "Digital forensic research: current state of the art," CSIT 1, pp. 91-114.
20. Shirani, B. (2002). Anti-forensics. High Technology Crime Investigation Association, <http://www.aversion.net/presentations/HTCIA-02/anti-forensics.ppt>.
21. StegoArchive.com. (2005). Stego Archive Web site. Available from <http://www.stegoarchive.com>
22. Vaidya, N., & Rughani, P. (2019). An Efficient Technique to Detect Stegosploit Generated Images on Windows and Linux Subsystem on Windows. International Journal of Computer Sciences and Engineering, 7(12), 21–26. <https://doi.org/10.26438/ijcse/v7i12.2126>
23. Vincze, E. A. (2016). Challenges in digital forensics. Police Practice and Research, 17(2), 183-194.