COMP 8310

Steganography Forensics

Steganography and Steganalysis

- **Rifat Ahmed Khan** – 45847827
- **Tahsina Tamanna** – 45710449
- **Suman Ojha** – 45720401
- **Ashish Bhandari** – 45814155
- **Harshitha Reddy Rajanala** – 45546029
- **Avista Rijal** – 45534934
- **Panchhewa Nembang Limbu** - 46167243

1 Introduction

Due to the massive advancement of digital technology, secure communication has become a fundamental necessity in today's digital world. Steganography is a form of secret communication in which data is hidden within a cover item. Steganography allows a secret message to be hidden inside inconspicuous data and sent without anyone suspecting about it[1]. Steganography is needed for safe communication in a variety of settings, including banking and the military, and even by common people for various purposes. However, the popularity of steganography is due not only to its ethical uses, but also to certain unethical practices, such as cyber-criminals embedding malware, spam, and malicious links to files. Terrorists have also used steganography for their nefarious purposes[2].

Steganalysis is the process of detecting secret information in media files or network packets using a steganography method or technique. The need for steganalysis in digital forensics was first recognised in 1983, when the National Computer Security Center (NCSC) discussed the potential threats of hidden media. The primary task of a forensic specialist in steganalysis is to accurately identify and extract secret material from communications if it exists[2].

This report would first explore the different applications of Steganography and then analyze the different categories of Steganography. The report would then go on to analyze the different methods of Steganalysis processes used by forensic experts and would then demonstrate practical applications of some of the Steganalysis processes. The final part of the report would discuss the challenges and issues of Steganalysis faced by the forensic analysts in the due process.

2 Adverse effect of steganography

Steganography is one of the most important discovery which provides secrecy while transferring data or to protect against threats. In the same way, it can also be a lethal threat which can leave law enforcement and experts scratching their head. In today's modern world where everything is connected to internet, steganography technique has also evolved and now it has not just become a medium to deliver secret messages but also a medium to inflict harm on others. Some of the major adversarial field impacted by it are pornography, terrorism, data theft and harm.

Steganography could be effective in affecting PC with virus or spyware when it is hidden inside harmless pictures, videos or music[3]. In 2018, memes with hidden payload were distributed by a bad actor in Twitter, where the image contained remote command and control services for infected Pcs which extracted the country codes from the phone number which was associated to twitter account[4].

3 Steganography as a weapon

As we know steganography is a technique to hide data or message inside image, videos music and so on. The advancement of technology has given the steganography to take a different sides, as now a days steganography is widely used in order to perform various cyber attack or by terrorism group in order to deliver messages, attack tactics or some important documents. Some of the service providers allows a user to post pictures, videos and text messages like Facebook, twitter, Instagram and so on, an attacker tends to upload an infected image on such platform with a payload attached on it which executes when it is opened and affect multiple users in multiple location at once[5]. With the advancement of Internet, now a days criminal tends to hide data and malware in plan site like the ad banners, links, Gif image and so on[6]. Now a days, the steganography has become a major threat in

the society as a result of which some of the best researchers formed a Criminal Use of Information Hiding (CUIng) initiative in co-operation with Europol European Cybercrime Centre to find the best possible way to stop and detect such threats[7]. According to Steffen Wendzel, now a day use of a steganography has become a de facto standard for any ordinary malware[8]. Some of the most represented malware which were observed in between 2011 to 2017 are listed below with its purpose and the method used to hide information.

Malware/exploit kit	Information-hiding method	Purpose
Vawtrak/Neverquest	Modification of the least-significant bits (LSBs) of favicons	Hiding URL to download a configuration file
Zbot	Appending data at the end of a JPG file	Hiding configuration data
Lurk/Stegoloader	Modification of the LSBs of BMP/PNG files	Hiding encrypted URL for downloading additional malware components
AdGholas	Data hiding in images, text, and HTML code	Hiding encrypted malicious JavaScript code
Android/Twitoor.A	Impersonating a pornography player or an MMS app	Tricking users into installing malicious apps and spreading infection
Fakem RAT	Mimicking MSN and Yahoo Messenger or HTTP conversation traffic	Hiding command and control (C&C) traffic
Carbanak/Anunak	Abusing Google cloud-based services	Hiding C&C traffic
SpyNote Trojan	Impersonating Netflix app	Tricking users into installing malicious app to gain access to confidential data
TeslaCrypt	Data hiding in HTML comments tag of the HTTP 404 error message page	Embedding C&C commands
Cerber	Image steganography	Embedding malicious executable
SyncCrypt	Image steganography	Embedding core components of ransomware
Stegano/Astrum	Modifying the color space of the used PNG image	Hiding malicious code within banner ads
DNSChanger	Modification of the LSBs of PNG files	Hiding malware AES encryption key
Sundown	Hiding data in white PNG files	Exfiltrating user data and hiding exploit code delivered to victims

Figure 1: Some malwares with its purpose and the method used to hide information[9]

In 2016, a hacker used steganography technique as a main weapon to infect an e-commerce platform called Magento. In this, the hacker used an image steganography technique to hide credit card and payment details inside a JPG image which was sent back to the hacker server undetected and where the hacker would download the image and extract the hidden data[10]. Such similar or major hacks and exploits have increased drastically because of the misuse of steganography technique. It has been weaponized in order to extract critical information or to harm an individual mentally, financially or socially.

In the same way, steganography has also played an major role in world war 2. Different countries used different unique techniques to supply important messages and tactics without letting anyone know

about it. Invisible ink was also one of the most commonly used means to provide a message without letting any other countries or force detect it[11].

Similarly, Germany introduced a technique called microdots. This microdots were a complete documents, images and tactical plans which were reduced in size of a period and were attached to common paperwork. They also used null cypher cryptography technique to hide messages in a plan text, which is considered a genius tactics[11].

4 Categories of Steganography:

Steganography can be applied to various kinds of carrier medium. As technology advanced, so did the techniques of Steganography, and nowadays steganography can be applied on- multimedia, video conferencing, network, DNA etc. [2]. Current steganographic trends can be broadly categorized as follows:

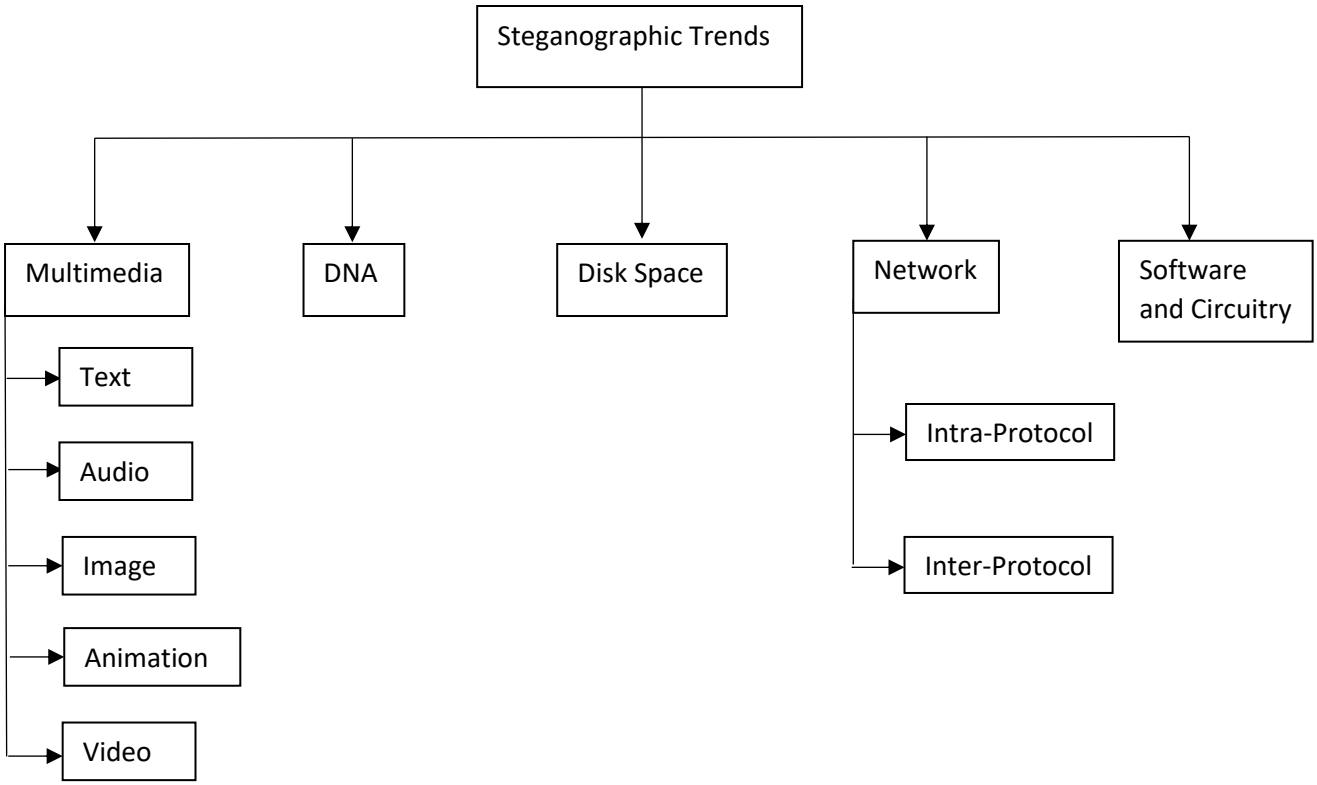

Figure 2: Categorization of Steganography [2]

The categories are described briefly as follows[2]:

- **Multimedia Steganography:**
  This kind of steganography hides data inside multimedia files. The most commonly used formats for this purpose include- images, videos, audios, etc. and data can be hidden inside them quite easily without being detected as they allow for high redundancy. Multimedia steganography can be achieved in various processes such as Spatial and Transform domain-based techniques.

- **DNA:**
  DNA steganography can be also called Genome Steganography. In DNA steganography, messages could be hidden in different regions of the Genome after being encrypted. This approach could be used to track cells and protect biological assets such as engineered cells.

- **Disk Space:**
  In this type of steganography, data is hidden in the slack space of hard disks. The logical channels of the disks, that are usually out-of-sight of forensic examiners, are used to hide data by using the redundant and unused fields, such as- the Master Boot Record of non-bootable hard disks and the slack spaces in disks caused by a mismatch of alignment of hard disk file and sector size.

- **Network Steganography:**
  Network Steganography is a comparatively newer field of steganography where redundant communication mechanisms are used to hide data. Protocols such as TCP, UDP, IP, etc. are used to create hidden communication channels for the purpose of hiding data. Network steganography can be further categorized into two different sub-categories- Intra-protocol and Inter-protocol. This type of steganography could be used to hide data in video conferences (Skype).

- **Software & Circuitry:**
  The software and the circuit system is another potential field for steganography. Data could be hidden in a software inside the code of the program and similarly in the electronic circuit layout.

The field of steganography is a vast area and could not be covered in whole in this paper. The scope of this paper is restricted to Multimedia and Network steganography and steganalysis only.

5 Steganography Techniques:

The primary goal of steganography techniques involves hiding data without degrading the quality of the cover medium. The basic steps of the process involve placing a secret message in some transport medium, known as the carrier. The carrier is embedded with the secret message to form the steganography medium. A steganography key can be employed during the process to either encrypt the hidden message or introduce randomization in the steganography scheme[2].

5.1 Multimedia Steganography:

5.1.1 Image Steganography:

Image steganography can be broadly generalized into two different categories based on their domains- transform and spatial domain. In the following section, 3 different techniques of Image steganography are discussed based on transform domain, spatial domain and adaptive steganography:

- **Spatial domain techniques**
  This technique for embedding secret data requires manipulation of direct pixel values of images. This is the most commonly used domain for Image steganography due to the ease and speed of its implementation. Various kinds of spatial domain techniques exist such as- Least Significant Bit (LSB), Pixel Value Differencing (PVD), Histogram shifting, etc[2]. The LSB and PVD methods are discussed below:

i. ***Least Significant Bit (LSB) based steganography:*** This method of image steganography is one of the most popular and the simplest. Using this method does not degrade the image quality after the secret bits of data are embedded, as LSBs usually contain noise or frail information. However, with increased capacity, the visual quality of the cover image degrades. Due to its easy implementation, LSB based techniques are highly susceptible to steganalysis attacks[2].

ii. ***Pixel Value Differencing (PVD) based steganography:*** PVD is another commonly used method of spatial domain-based image steganography where the secret data is embedded by comparing the values of successive pixels of the cover image. The advantage of this method over the LSB method is that after embedding, the visual quality of the carrier image does not degrade[2].

- **Transform domain techniques**
  The transform domain technique requires the secret information to be embedded in the transformed coefficients unlike the Spatial domain techniques, where it is done by directly manipulating the intensity values of the carrier images. There are several methods of transform domain technique used for image steganography such as- Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT)[2]. Even though the process of the embedding and extracting is computationally more complex in transform domain-based methods, they are much more resistant to steganalysis attacks and preserves the quality of the carrier with minimal or no degradation.

- **Adaptive Steganography techniques**
  Adaptive methods for image steganography target certain areas of the carrier image to increase the efficiency of steganographic techniques for embedding the secret information. These methods consist of targeting the Human Visual System (HVS) during embedding to reduce the probability of detection, using a threshold value or a combination of other fields to increase the security of the steganography techniques[2].

5.1.2 Video Steganography:

Video steganography can also be done using spatial and transform domain techniques. However, videos consist of much more features than images and those could be utilized to embed secret data to create a more complex structure, making the steganography more resistant to attacks. Videos are usually stored and transferred in compressed format and thus secret data could be embedded based on the video coding standard features such as- encoding schemes, Motion Vector (MV), bitstreams, etc[2].

5.1.3 Audio Steganography:

The general concept of audio steganography consists of hiding a message inside a cover signal of the embed and audio processing block by the means of a steganography key to create a stego audio signal. The key remains the same for both the sender and the receiver. The receiver then uses the key to retrieve the hidden message from the extract and audio processing block within the carrier audio file[13].

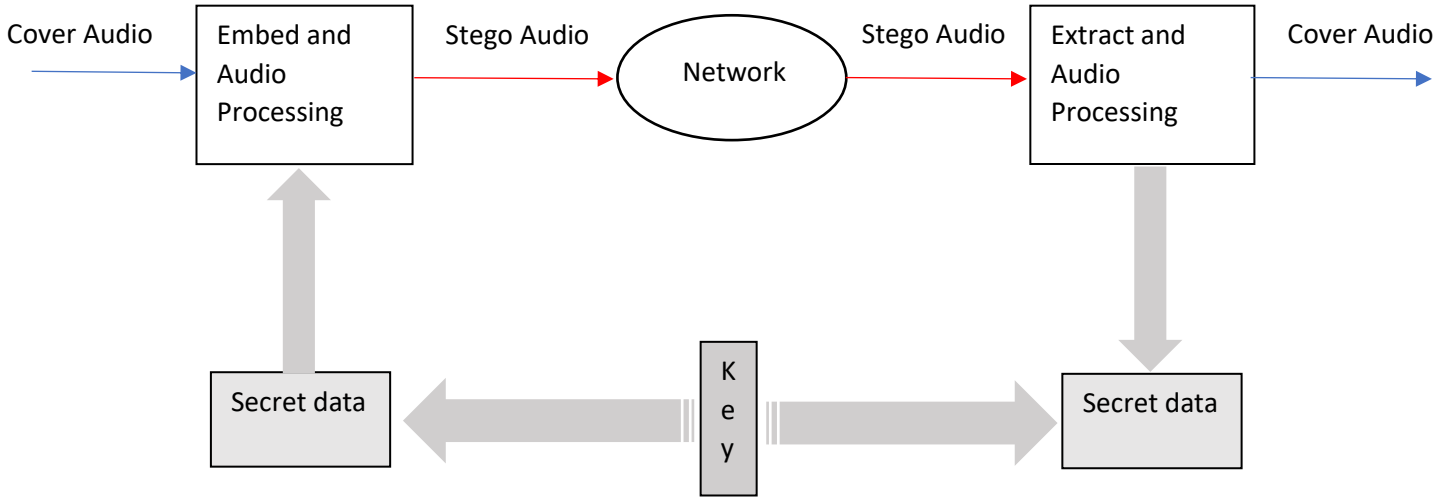

Figure 3: Block diagram of Audio Steganography[13]

5.1.4 Text Steganography:

Text steganography is the process of hiding a secret text message inside another text as a covering message or to generate a cover message related with the original secret message[14]. Text steganography is believed to be trickiest among all other steganography techniques due to deficiency of redundant information present in image audio and video files[15]. The structure of in text document is identical to what we observe, but in other types of document like video, the structure of document is completely different from that we observe. Therefore, in such documents hiding of information becomes easier. The structure can be changed without making any notable changes in the concern output[16]. In case of text even the small changes like adding blank space or comma can be identified by the normal user[17]. Beside this difficulty text steganography is easy to communicate and faster with less memory requirement which makes it more preferable in comparison with other steganography techniques[18].

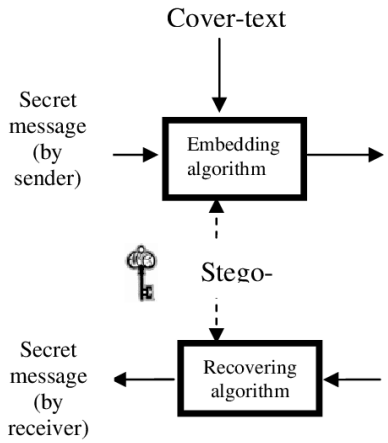

Figure 4: Mechanism of text Steganography [19]

Text steganography can be classified into three basic categories as follows:

5.1.4.1 Format Based Method:

In a format-based model basically a text is modified in order to hide steganographic text in it. This method uses formatting of physical text of text where information will be hidden [9]. Some of the methods used in format-based models are line spacing between the text, distribution of deliberate misspelling in the text, resizing fonts, formatting text etc[17].

An example of a message containing cipher text by German Spy in World War II:

"Apparently neutral's protest is thoroughly discounted and ignored. Is man hard hit. Blockade issue affects Pretext for embargo on by products, ejecting suet's and Vegetable oils."

Taking the second letter in each word the following message emerges:

"Pershing sails from NY June 1".

5.1.4.2 Random and Statistical Generation

The second approach is based on character sequence and word sequence of character. The sequence must appear to be random to the person who intercept it [9]. This method basically deals with generating cover text based on statistical property. This method is driven by realms of computer science and programming language by the way of natural language processing and computer-generated text[17]. Some examples of random and statistical generation of text are Markov Chain.

5.1.4.3 Linguistic Method

Linguistic steganography is a method that considers linguistic properties of modified or generated text. This steganography usage's linguistic structure is a combination of syntax and semantics. Syntax is used to ensure the structure is syntactically correct where as in semantic a value can be assigned to synonyms and that can be encoded into the actual word of text[17].

For example:

"The beginning of this week"

This phrase can be modified with the same meaning as

"This week in the beginning"

Both of the sentences look correct but they have different 0's and 1's encoded in them.

Techniques used in Text Steganography

- **Line Shifting**
  Line shifting methods use a vertical shifting approach of text to some degree where the secret message is hidden. For the detection of movement, the message has two unmarked lines one on either side of it to indicate the direction of movement [20]. To hide a 0-bit line is shifted up and to hide 1 bit the line is shifted down. Determining weather, the line has been shifted up or \down is done by measuring the distance of the centroid of marked lines and its control lines. The method requires the original image to be decoded[21]. This method works best for printed text[18].

- **Word Shifting**
  This technique of text steganography usages message hiding by shifting the location of words horizontally from left or right to represent bit 0 or 1 respectively[21]. This method is applicable where the distance between adjacent words varies [20]. When justifying text, the variable spacing is commonly used to obtain distribution of white space in the text document. Due to variable spacing, to decode the message, the original document is necessary[21].
- **Semantic Method**
  In this method, one can hide text using punctuation marks such as comma (,) and full stops(.) are used in between the text. The method requires placing punctuation marks in the proper place so that information can be hidden. The amount of information hidden in this method is trivial [20].
- **Feature Coding**
  This is a coding method that is applied either on a file or a bitmap image of the document. This method alters some of the features of text are altered or not altered depending on the codeword[18]. Using this method, a large volume of information can be hidden in text without making a reader aware of such hidden information embedded in the text [12]. In this method decoding requires the original image. For example, changing points on the letter "i" and "j" can be displaced or played with the length, size of text to hide information. The flaw of this method is re-typing or using OCR (character reorganization program) can destroy the information hidden[21].
- **Abbreviation**
  Another method by hiding information is by using abbreviations in the text [10]. This method of text steganography can hide a few amounts of information. Suppose in a kilobyte of text file it can hide a few bits of information using this method[20].
- **Open Space**
  The method of adding extra white-space in the text to hide the information is called open space text steganography method [9]. These white spaces can be placed carefully between the words or at the end of each line or at the end of paragraph or even between the words[22].

5.2 Network Steganography:

The main objective of network steganography is to use active network protocols as carriers to transmit secret data from host to its destination. Using the carrier, one can include digital videos, audios, and image files or even an ICMP message from a ping command. The reach of network steganography is constraint to all data hiding technologies which uses a communication network by providing a covert transmission channel to allow sharing of secret data, linked and all bound to the transmission process, and do not kill data carriers[23].

The key difference between a standard steganography and network steganography is that the standard depends on fooling human senses while the latter attempts to mislead network devices such as intermediate or end user network nodes.

In the case of network steganography, a carrier has at least one network traffic flow. Generally, a carrier is multidimensional, which means that it has more possibilities to hide information which are called subcarriers. In a carrier the secret data can be hidden using steganographic techniques using subcarriers which are identified as a place or time-based event such as padding, headers or sequence of packets.

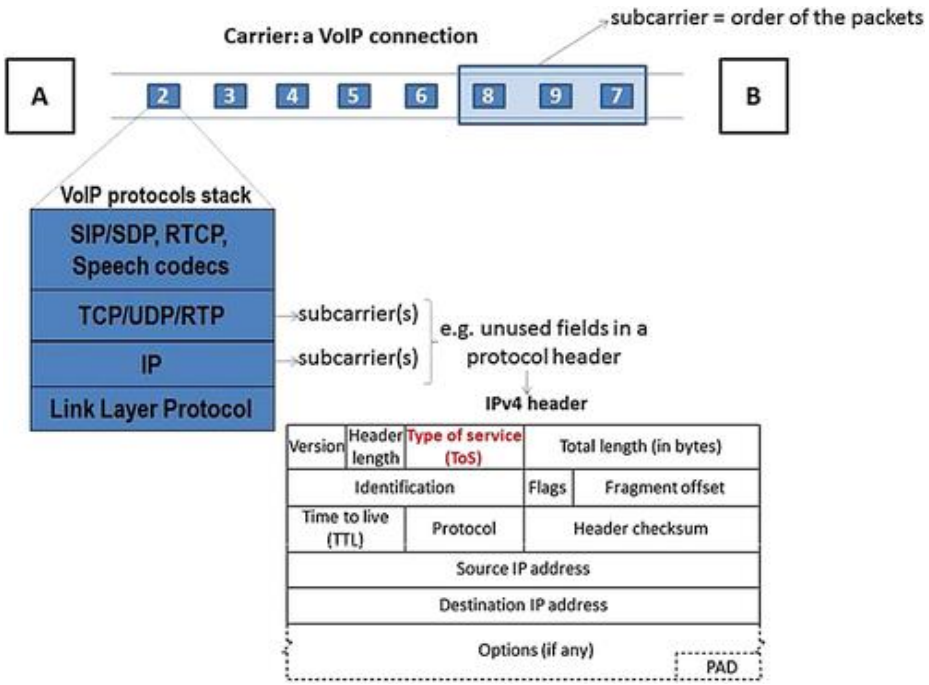

Figure 5: Network Steganographic technique

5.2.1 Classification and cases:

Network steganography can be classified into 3 categories utilizing the network protocols' header and payload, the second one using the structure/sequence of packet streams and lastly hybrid of the above two. Network protocols' header have several fields that must be sent from the source to the receiver to ensure correct delivery of the packets. Some of the fields are not used during transmission and are sometimes used during certain network conditions. So, the fields which are not used can be used as a carrier to transmit secret data[24].

- Craig H. Rowland[25] was the first to suggest the use of network protocols' header. In 1997, he used the ID field of the IP header for hidden communication. He had also proposed that the TCP header field which contains ISN (Initial Sequence Number) to be used to conceal data.
- Patel et al.[26] describes the use of network protocols' header by using 2 bits of the service field in IP the header as well as 6 unused bits of TCP header.
- B. Jankowski et al.[27] uses etherleak problem to which utilizes the Ethernet header and include the minimum length of frame padding bits. Standard cases of padding use 0s but in some cases NIC incorrectly incorporate arbitrary bits that are regarded as special cases. Using this flaw, secret data was added to the padding bits.

Another way of sending secret data is using the structure and sequence of package stream.

- Wojciech Mazurczyk[28] proposed using oversized data packets for sending secret data. When a packet is too big, it will be fragmented. When there are even number of fragments it holds secret 1 and similarly if the fragments are odd then it carries 0. In this way, 1 bit is secretly passed in the network.
- Using packet payload[29] , bits of secret data are transmitted by modifying packet payload size based on the number of 1s and 0s.

The hybrid schemes are a mix of the above two which introduced new and advanced techniques to network steganography. Some of the most popular techniques are as follows:

- **HICCUPS (Hidden Communication System for Corrupted Network)**
  In this technique[30], fields or content of the protocol are used. In this technique wrong checksums in the frame are deliberately used to send secret data. This method is usually used in wireless local area network (WLAN). This steganographic technique was the world's first tool to be recognized for wireless LAN.

- **LACK (Lost Audio Packets Steganography)**
  Lack is a hybrid approach which makes use of the time events and the contents of the voice packets [31]. The end of the sender receives the packets at a delay deliberately. When the packets are delayed and dropped by the end users who are not a part of the secret communication, the contents of the secret data is relayed in these packets.

- **TranSteg (Transcoding Steganography)**
  This technique uses IP telephony[32] where data is compressed to make room for the secret data. This uses a codec to find a voice stream of equal quality but lesser in size so that once the original data is encoded, the end size of the original sample and the one with secret data results in the same size.

6 Steganalysis

Steganalysis refers to the process of detection of the hidden information using steganography tools or techniques in media files. The main goal of a forensic examiner in this process is to detect and extract the hidden information reliably. This process requires knowledge of the original file, but that is not available in most cases. The features and characteristics of both the objects, stego- and cover-object are taken into consideration for steganalysis[2].

Steganography detection attacks can be classified based on how much prior information is known[33].

1. **Steganography-only attack:** The only item available is the steganography medium is for analysis.
2. **Known-carrier attack:** Both the carrier and steganography media are present for analysis.
3. **Known-message attack:** The hidden message or the secret is known.
4. **Chosen-steganography attack:** The steganography algorithm both are known.
5. **Chosen-message attack:** A steganography medium is created using a known message and steganography algorithm for future analysis and comparison.
6. **Known-steganography attack:** The carrier, steganography algorithm as well as the steganography medium are known for this analysis.

7 Steganalysis Techniques

Steganalysis techniques can be divided into six categories as follows[34]. It depends on the type of attacks a forensic examiner uses.

1. Visual steganalysis

2. Signature or specific steganalysis
3. Statistical steganalysis
4. Spread spectrum steganalysis
5. Transform domain steganalysis
6. Universal or blind steganalysis

7.1 Visual steganalysis

Visual steganalysis is to investigate visual properties of the steganographic file, where the visual difference is detected by analyzing the stego files[35].

Most common form of this steganalysis includes Least Significant Bit (LSB) steganography. Any image or video is converted to its binary form. Usually, for images, the odd values and the even values are equal. So, There are approximately as many 1's as 0's in the LSB plane. When any text is converted to binary and added with the image, more 0's than 1's creates a visual inconsistency which makes it easier for a forensic examiner to classify the image as a steganographic image[34].

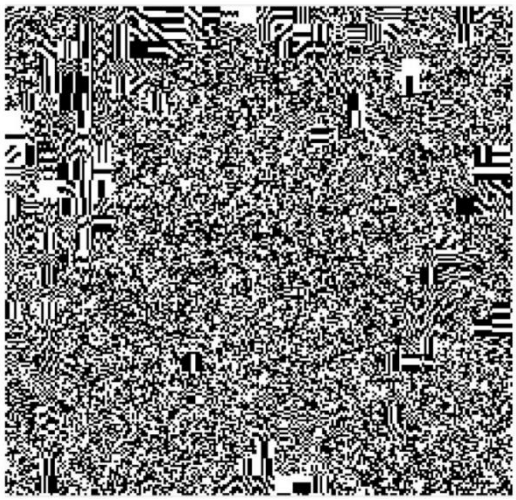

Figure 6: LSB of a Clean Image

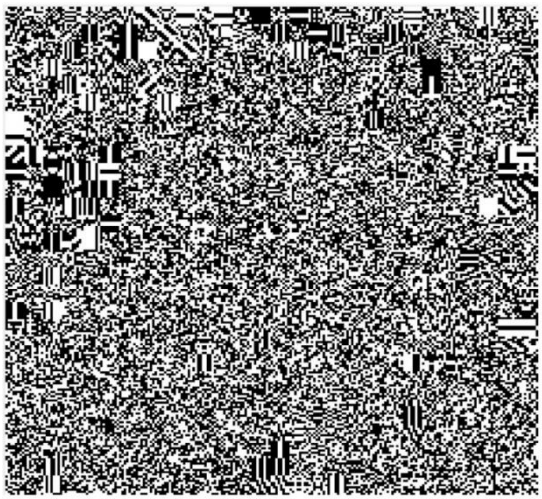

Figure 7: LSB of a Stego Image

Trying to detect blank spaces in possible steganographic files is also another method of detecting steganography. Some steganography algorithms crop and pad the file for it to be fitted to affixed size.

Differences in file size between original and steganographic files, variance in unique colors in steganographic files can also be analyzed for detecting hidden messages[36].

7.2 Signature Steganalysis

Steganography some of the properties of that file to create some form of unusual patterns or characteristics. These changes may act as signatures that broadcast the existence of hidden message. Observing these repetitive patterns (signatures) of a steganography software can determine presence of steganography in that file[36].

7.3 Statistical Steganalysis

Statistical models can be utilized in this steganalysis. Changes in patterns of pixels or LSB are analyzed. Two LSB approaches are described as follows[34]:

- *LSB replacement*
  The least important bits of the cover picture bytes are replaced by the hidden data in LSB Replacement. There are two different embedding schemes i.e. sequential and randomized.
  Sequential embedding means that the algorithm begins with the first pixel of the cover image and embeds the message data bits in sequence until the whole message is inserted.
  The locations of the values that will be changed to contain the bits of the embedded data are dispersed using randomised embedding.
- *LSB matching*
  Each hidden data bit is compared to the least significant bit of the corresponding cover byte in the LSB Matching embedding algorithm. If the two compared bits match, no difference is made, but if they do not, the cover byte is randomly incremented or decremented.

Histogram Analysis can also detect steganography in images, audio and video files. Frequency of the DCT coefficients are analyzed in this case and it has been found out that hidden messages cause noticeable changes to the DCT coefficient histogram[37].

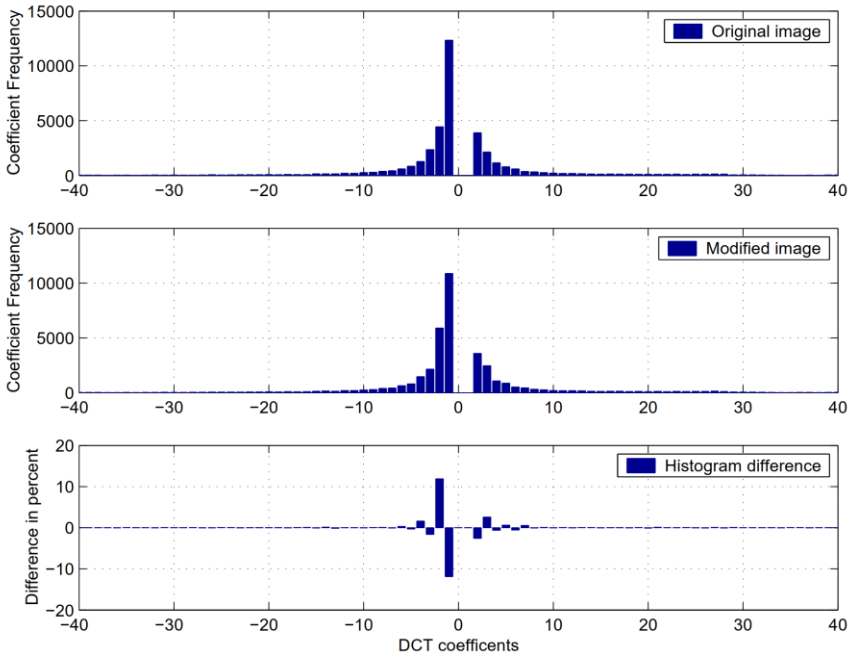

Figure 8: Histogram analysis of an image file[37]

7.4 Spread Spectrum Steganalysis

Spread Spectrum Steganalysis is basically embedding the hidden information within noise, which is then added to the original file. This noise is not distinguishable to the human eye if they are kept at low levels[34].

Chandramouli et al.[38] proposed two steganalysis schemes for spread spectrum steganalysis. Regression techniques are used in the first scheme to estimate original file from steganographic file. For getting an estimate of the hidden message, the estimated value is deducted from the steganographic file. The second exploits higher order statistics.

Fan et al. [39] proposed a technique for spatial domain based steganalysis to detect hash-based LSB video steganography. A cross-correlation feature of video frames was employed and a hash function was used to perceive the embedding sites.

7.5 Transform domain Steganalysis

To conceal details in the transform coefficients of the original files, various transform domains techniques such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Fast Fourier Transform (FFT) were used[36].

A neural network based steganalysis was proposed in [40]. The digital images, both clean and stego, are analysed using neural networks in the DFT, DCT, and DWT transform domains. The statistical features of images that are greatly impacted by data hiding are calculated using a neural network. Using quantization index modulation, the neural network is trained using the statistics of clean images and images with hidden messages.

7.6 Learning steganalysis

Learning steganalysis, also known as blind steganalysis is one of universal statistical steganalysis. Universal steganalysis techniques try to detect the hidden messages regardless the steganographic methods applied to the original file. Machine learning techniques are used afterwards in order to build a detection model from the training data[35].

Image processing, video processing, natural language processing, computer vision, speech recognition, and other applications of artificial intelligence have been around for a long time. Image/Video steganalysis using machine learning is a two steps process:

To distinguish the original file from the steganographic object, the first step is to extract statistical features from the stego and cover-object (image/video) for comparison. The hypothesis that embedding changes the image/statistical video features is the reason for depending on these statistical features [41].

The second step puts the plan into action using machine learning algorithms. In order to train a classifier, features are extracted from the steganographic and cover-image/video-frames, and the testing images/videos are fed into the machine learning classifier model for analysis[2].

The most popular classifiers used by researchers for image/video steganalysis are Support Vector Machines (SVM).

Aside from this two-stage machine learning method, newer techniques use deep learning algorithms like Deep Neural Networks (DNN), Convolutional Neural Networks (CNN), and others to automatically extract and select features.

Few researchers have used the CNN deep learning platform in image/video steganalysis, so it is still a new area. A CNN is made up of various hierarchical layers, such as feature maps and classification layers. The input data is fed into a convolutional layer, which is made up of a few filters for mapping of similar sizes. The processed data is passed to the next sampling layer after convolution operations, which reduces the size of subsequent layers[42]. Since CNN uses a variety of deep learning methods that are connected locally, it needs high-end GPU systems with several hundred cores.

7.7 Others

As the structure of the stego message is superimposed on the digital carrier data, analysis of distribution of known properties often reveals the presence of the hidden message. For instance,

bitmap files with more than 50 near-identical colors should be suspected of containing hidden messages[19]

With the original file in hand, differences in file properties/contents, size, hash value or date/time can also lead to modified files.

8 Stego tools

The identification of steganography software on a suspect device is crucial to the forensic investigation. Many steganography detection programmes work well when there are hints as to the form of steganography that was used in the first place, as the research shows.

The detection of steganography software on a suspect computer is important to the subsequent forensic analysis. As the research shows, many steganography detection programs work best when there are clues as to the type of steganography that was employed in the first place. Finding steganography software on a computer raises the possibility that the suspect computer contains steganography files containing secret messages.

Furthermore, any subsequent steganography research would be influenced by the form of steganography software discovered. For example, S-Tools may guide the analyst's attention to GIF, BMP, and WAV files, while JP Hide-and-Seek may direct the analyst's attention to JPEG files[43].

- **Gargoyle (formerly StegoDetect)**
  This tool can be used to detect the presence of steganography software[44]. Gargoyle compares the hashes of the files under quest to a proprietary data set (or hash set) of all the files in the documented steganography software distributions. Cryptography, instant messaging, key logging, Trojan horses, password cracking, and other malicious malware can all be detected using Gargoyle data sets.
- **Stegdetect**
  Niels Provos' Stegdetect[45] is a popular detection software. Stegdetect uses steganography schemes like F5, Invisible Secrets, JPHide, and JSteg to find hidden details in JPEG images (OutGuess 2003).
- **Stego Suite**
  Stego Suite is is comprised of Stego Watch, Stego Analyst and Stego Break. This tool can be used for investigation, detection, analysis, reporting as well as recovery of digital steganography.
  Stegowatch analyses collection of files to determine which are steganography media and the most likely algorithm for hiding them (which, in turn, provides clues as to the most likely software employed). The study employs a number of user-selectable statistical tests based on carrier file characteristics that may be affected by various steganography techniques. Stego break uses a dictionary attack to find the password of the hidden data against JSteg-Shell, JPHide, and OutGuess[46]
- **StegCracker**
  This tool can be used for dictionary attacks against steganographic files which are protected with passwords. After the attack, StegCracker automaticaaly writes the hidden data to an output file[47].

Listed below are some of the tools which are frequently used along with their functionality. The tools provide means of using the network protocol for controlling cyberspace to make hidden transmissions. Unlike some standard media which are based on integration of data in the carriers, the tools provide work directly and work in the actual network protocols[48].

Tool	*Year*	*Functionality*
CovertTCP	1997	Covert Channels using TCP and IP headers
StegTunnel	2003	Timing channel using TCP header fields
hCovert	2005	Covert channel using HTTP GET requests between webservers
VoVoIP	2007	Embedding data in PCM voice traffic exchanges
SteganRTP	2007	Uses RTP of VoIP as payload medium
Gary-World Team's	2008	Covert channel projects using TCP and IP headers
Steganography Studio	2009	Training suite on network steganography tradecraft
NetCross	2010	Utilizes the DNS protocol to establish covert comm.
OpenPuff	2011	Multiprotocol embedding toolkit
SoCat	2013	Network relay transfer between two independent data channels.

Figure 9: List of Common Network Steganography Tools [48]

9 Demonstration of Steganalysis

9.1 Image Steganalysis

We have used Steghide and Stegcracker for our demonstration of image steganalysis.

We used Steghide to embed a text to an image file. Here, 'cat.jpg' is the original file, 'msg.txt' is the secret information, and 'stego.jpg' is the steganographic image. We locked the file with the password 'pass'.

```
(base) kali@kali:~/Downloads$ steghide embed -ef msg.txt -cf cat.jpg -sf stego.jpg -p pass
embedding "msg.txt" in "cat.jpg"... done
writing stego file "stego.jpg"... done
(base) kali@kali:~/Downloads$
```

Figure 10: Hiding data with Steghide

Then we checked some properties to notice any changes. The Steganographic image was larger in size and their hash values were different.

```
(base) kali@kali:~/Downloads$ exiv2 cat.jpg
File name       : cat.jpg
File size       : 28278 Bytes
MIME type       : image/jpeg
Image size      : 620 x 372
cat.jpg: No Exif data found in the file
(base) kali@kali:~/Downloads$ exiv2 stego.jpg
File name       : stego.jpg
File size       : 28745 Bytes
MIME type       : image/jpeg
Image size      : 620 x 372
stego.jpg: No Exif data found in the file
(base) kali@kali:~/Downloads$
```

Figure 11: File properties

```
(base) kali@kali:~/Downloads$ md5sum cat.jpg
bca3c0a178327ae9f4026afa31d35f74  cat.jpg
(base) kali@kali:~/Downloads$ md5sum stego.jpg
9c91dbfae5349226ca2f6b4cc31d0ede  stego.jpg
(base) kali@kali:~/Downloads$
```

Figure 12: File hashes

We used Stegcracker to attack the file against a wordlist. We conducted a dictionary attack against the wordlist 'wordlist.txt'. We managed to get the secret from the steganographic file successfully.

```
(base) kali@kali:~/Downloads$ stegcracker stego.jpg wordlist.txt
StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2021 - Luke Paris (Paradoxis)

StegCracker has been retired following the release of StegSeek, which
will blast through the rockyou.txt wordlist within 1.9 second as opposed
to StegCracker which takes ~5 hours.

StegSeek can be found at: https://github.com/RickdeJager/stegseek

Counting lines in wordlist..
Attacking file 'stego.jpg' with wordlist 'wordlist.txt'..
Successfully cracked file with password: pass
Tried 201 passwords
Your file has been written to: stego.jpg.out
pass
(base) kali@kali:~/Downloads$
```

Figure 13: Steganalysis

Stegcracker automatically wrote the hidden information to a file 'stego.jpg.out'. Both information matched and the attack was successful.

```
(base) kali@kali:~/Downloads$ cat stego.jpg.out
This is the secret
(base) kali@kali:~/Downloads$ cat msg.txt
This is the secret
(base) kali@kali:~/Downloads$
```

Figure 14: Steganographic data comparison

9.2 Audio Steganalysis using MP3Stego

9.2.1 Embedding process:

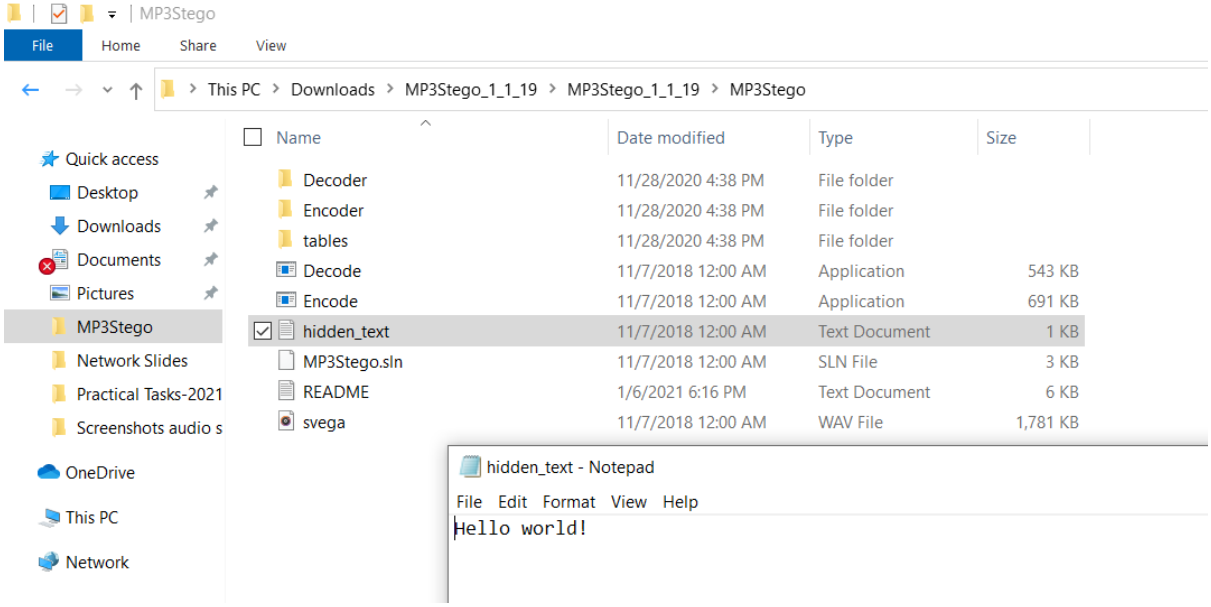

Figure 15: The text file containing the hidden message

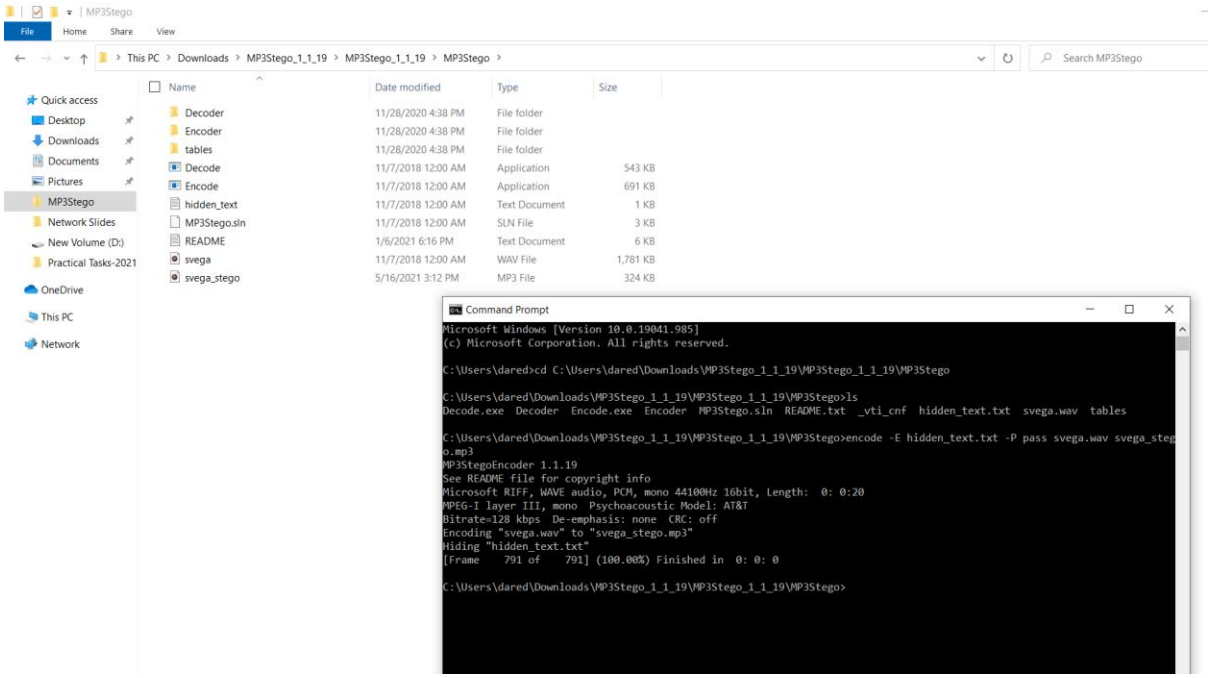

Figure 16: The mp3 file svega_stego created containing the hidden message

Command used:

encode -E hidden_text.txt -P pass svega.wav svega_stego.mp3

The command used compresses the svega.wav file and hides the secret message hidden_text.txt. The hidden text is encrypted using '*pass*' as a password. This produces the output called svega_stego.mp3.

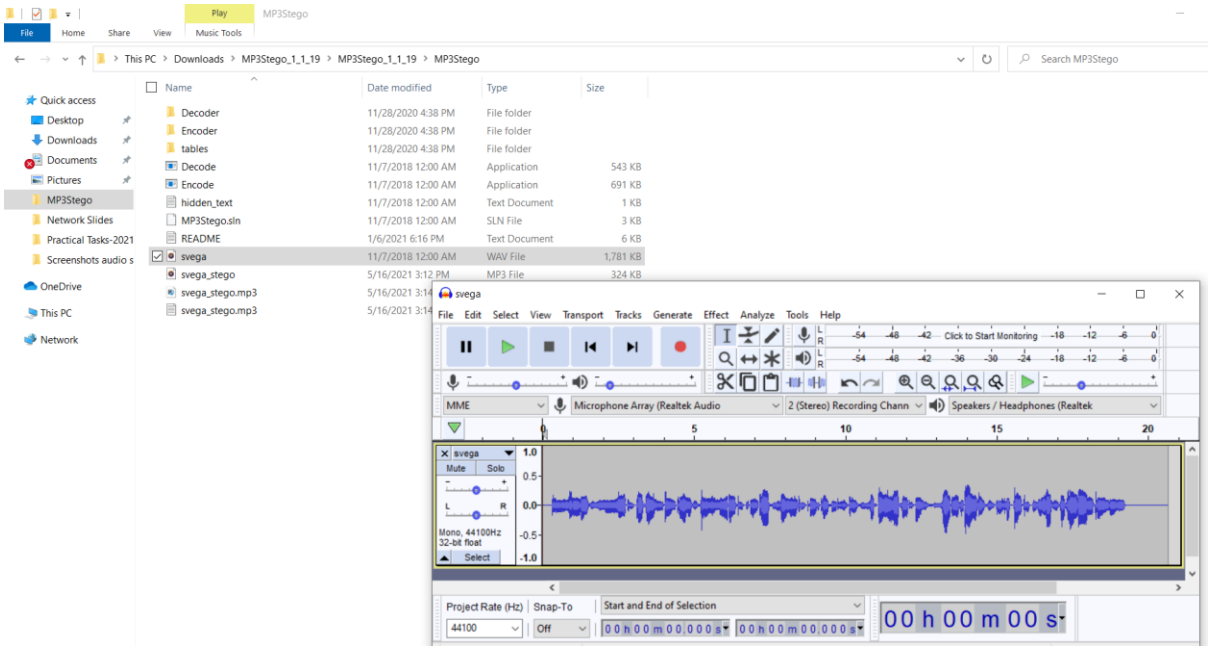

Figure 17: The waveform view of the svega.wav carrier file before embedding the secret message

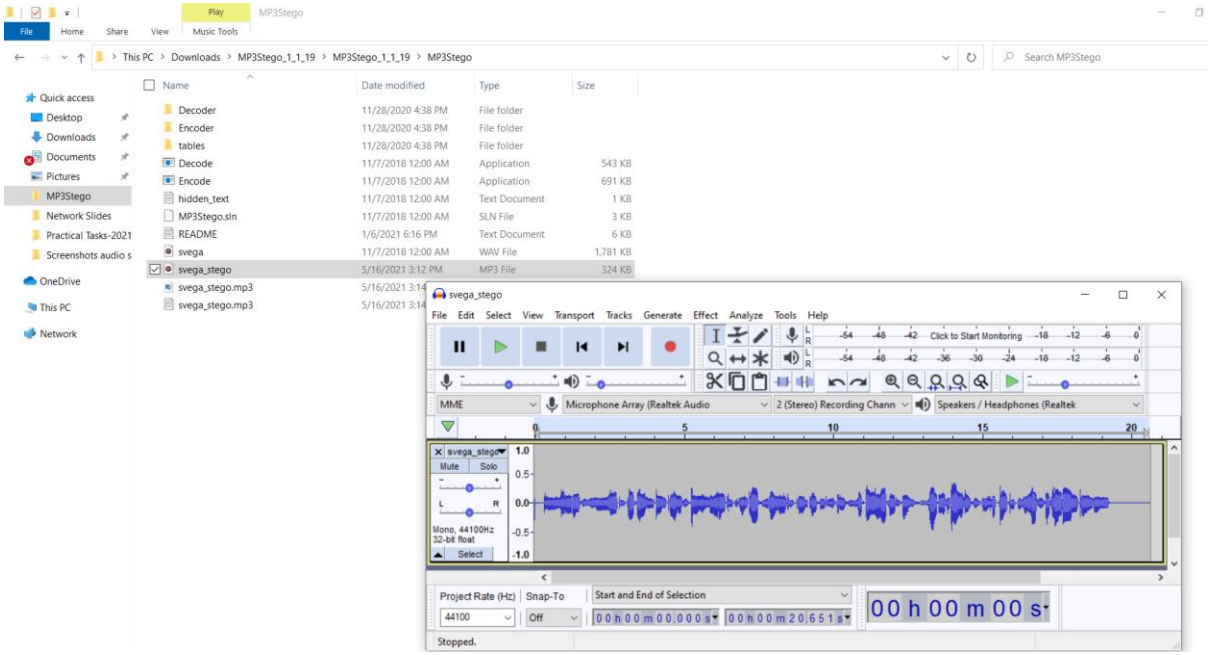

Figure 18: The waveform of the stego file svega_stego.mp3 after the secret message hidden_text.txt is embedded

When both the audio files svega.wav and svega_stego.mp3 are played, they sound exactly the same. However, when the waveform of both the files are analyzed, they seem almost identical, except for the stego file containing a slight variation at the beginning.

9.2.2 Extracting process:

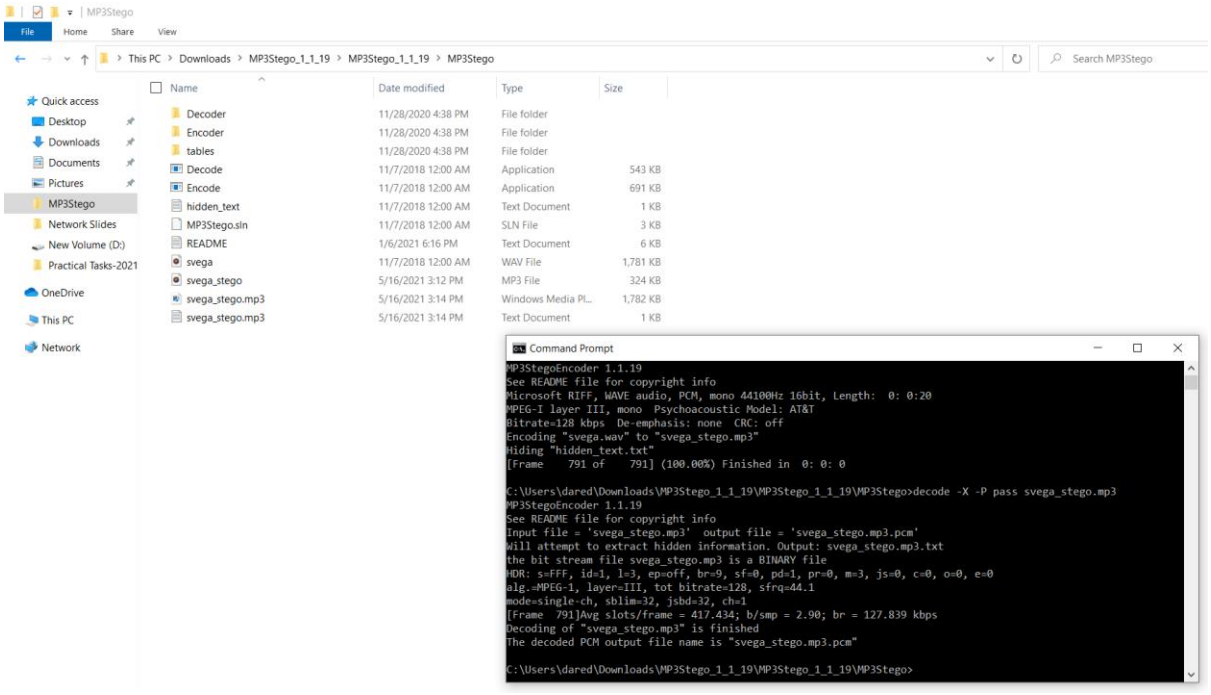

Figure 19: The secret file is extracted from the carrier file

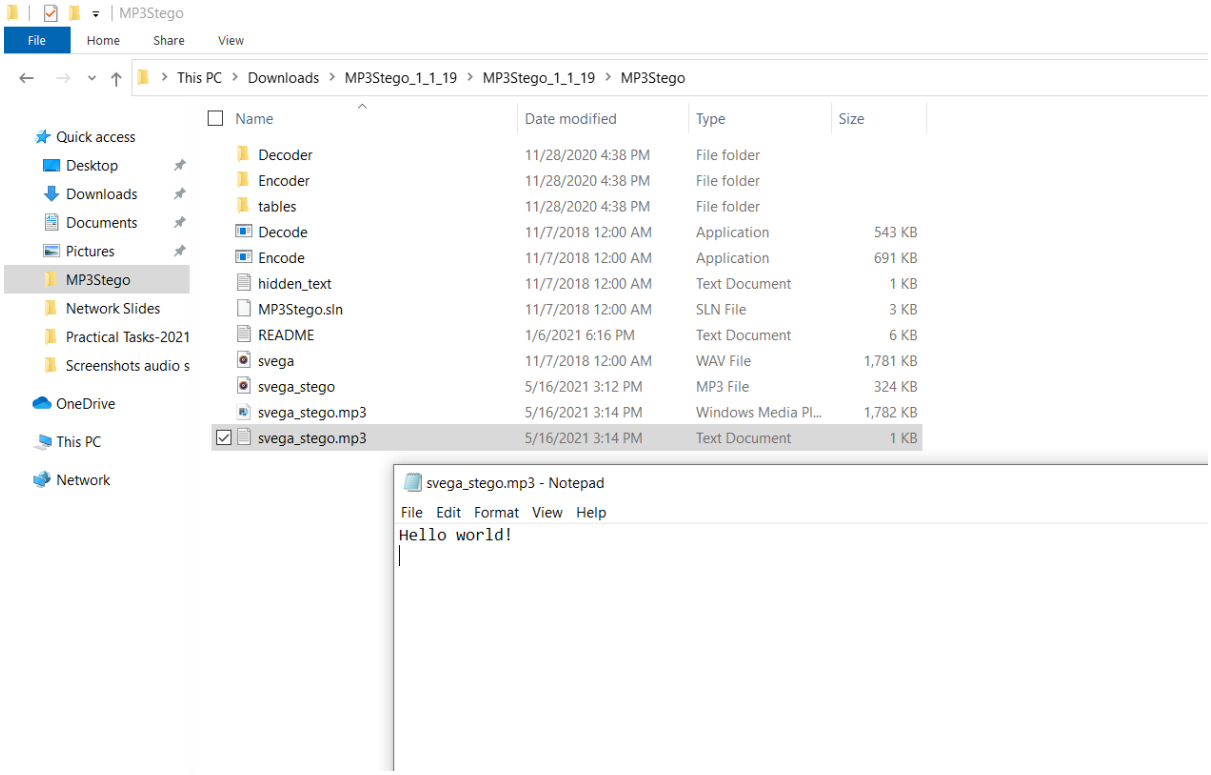

Figure 20: The secret text after extraction

Command used:

decode -X -P pass svega_stego.mp3

The command used uncompresses the stego file svega_stego.mp3 into svega_stego.mp3.pcm and extracts the hidden file by decrypting and uncompressing it and finally saving it into svega_stego.mp3.txt.

9.3 Video Steganalysis

It can be more difficult to crack the original information in case of video steganalysis at times, because time frame is comparatively less. Some generic steps can be used to hide the secret message into other authentication messages[49].

- Select any original format of video file.
- Open it by using any read file function.
- Now select all the frame files into “MOV” function from the video file.
- Observe all the frame data by playing MOV function.
- Hide the information from the authentication image by taking any number of frame.
- Now select the file and read it and save it with variable a.
- Next, select the other authentication image in video and read it and save it with variable b.
- We can extract the msb of frame by using bit and function with 240.

- Similarly, we can perform bit and with 240 for authentication image.
- Now reverse the msb with lsb by dividing with any element 8(consider 8 as another element factor).
- We can reshape the images in a row or column.
- Now the original images are reshaped in other authentication image by column wise by dividing with 8 elements in each authentication image.
- Now, we created a new Stego frame and we have over written the original data.

10 Challenges of Detecting Steganography:

10.1 Requirement of original file:

Some steganographic detections are very difficult without the original file despite noticeable distortions and noise. In most cases, a forensic investigator will not be presented with the steganographic and original file[50].

10.2 Lack of Effective Detection Tools:

Many of the current commercial tools that can be used for detecting steganography are not much effective. Rather than finding the hidden secret data embedded within a digital file, the tools emphasis on finding the artifacts that have been left by the steganographic tools. Even though such approach seems effective, it only works against well-known steganography tools. If a perpetuator uses proprietary data hiding tools to hide the data or if the device is infected with a malware capable of data hiding, it will be near impossible reveal its artifact or to determine the intent of the attacker[51]. As new and sophisticated tools and techniques are being developed for data hiding, it is very challenging for the forensic investigators to detect such hidden information using the current detection tools at their disposal. If a network is compromised, then detecting the use of steganography on such compromised network is very challenging. According to Barwise (2018),

"If an adversary is able to penetrate a network successfully and unsuspectingly install malware onto a system that uses digital steganography to hide its presence, then the network and all associated data contained therein should be considered entirely compromised (Theoretical Framework)."

Additionally, there is abundance of data hiding tools which makes use of various techniques to hide the information. With such variety of data-hiding tools, it has been a challenge for the existing steganalysis tools to detect steganography. The programs that are available for data hiding, considerably outnumber the programs that can be used to detect and extract such embedded/hidden contents. Easily available tools for data hiding means that even inexperienced users with minimal knowledge are able to use such tools for steganography for ill intents. Furthermore, it is nearly impossible to develop steganalysis tools or techniques which is able to detect steganography with hundred percent accuracy[52].

10.3 Machine learning based steganalysis:

The main difficulty in ML/AI based steganalysis is to find relevant features which are the main characteristics for stego images[34].

10.4 Network Steganalysis:

TranSteg is a tool for network steganalysis. It is hard to perform since the compressed message with the secret data is extracted before it reaches to the receiver and the data is restored to it original data by the time it reaches the end. The signal of the change are also not easily detectable without proper analysis[32]

10.5 Use of Encryption Technique:

With the development of steganalysis techniques, forensic officers have to ability to detect and extract hidden messages from embedded files. Perpetrators, in an effort to limit being detected and maintain their covert line of communication, can make use of encryption techniques to conceal actual information. It is one of the major challenges faced by the forensic officers to detect and decrypt steganography. Encryption technique makes use of secret key to encrypt and decrypt the message. If suspects encrypt the message before embedding it, it makes investigation much more complicated[52]. As the encryption technique gets more and more advanced and sophisticated, it is near impossible to detect and decrypt the hidden messages without the encryption key. If the suspect makes use of powerful encryption technique, then decrypting the message without key is impossible even using all the cryptanalysis attacks.

10.6 Legal Challenges:

Just like any other digital forensic investigation, steganography forensic also faces the legal challenges to conduct the investigation. In order to function properly in the field of science, the legal challenges surrounding digital forensics has to be addressed[33]. One of the challenges that digital forensic faces is during search and seizure. For search and seizure, officers need a clarification from a legal standpoint[53]. If any evidence is procured without set rules and procedures, then the evidence collected might be dismissible in the court of law. Another legal issue surrounding the investigation is that evidence or criminal communications might cross multiple state or even an international border. Any actions that are considered illegal in one state or country might be considered legal in another. Additionally, investigators' access to the evidence or conduction of investigation may be seriously impacted because of lack of jurisdiction overseas [2]. There are no specific laws that limits or prohibits the use of steganography[52]. Rapid advancement in digital technologies along with techniques and technologies to extract and analyse the data from digital devices poses serious legal concerns about its reliability[54].

10.7 Advancement in Digital Devices:

With the growth and rapid development of digital devices, another challenge facing forensic officers regarding steganalysis is the storage capacity of the device. As technology is evolving, digital devices are capable of storing huge amounts of data. Increased storage capacity adversely affects forensic officers to perform steganalysis with an aim to search steganography on digital medias (audio, video, image and text)[52]. Additionally, forensic examiners are required to manually scan through large amount of data in order to detect potentially illegal contents, which makes the process particularly time consuming and overwhelming[52]. The development of cloud services has only made the matter worse which means that investigators need to deal with exponential data load.

Additionally, development of digital devices can open up new ways for perpetrators to exploit and hide data which has not been discovered yet. One such possibility is the storing hidden data in IoT (Internet of Things) devices. It might be only a matter of time where IoT devices are exposed to steganography cybercrime. IoT devices offer whole new way to store hidden data in the memory of its actuators and embedded components. Hidden data on such devices cannot be found by employing existing methods, and there are not any tailored tools available which can be used to detect, extract and analyse data from such devices[51].

10.8 Growth of Social Media and Online Services:

The emergence and growth of social media have enabled millions of people around the world to easily communicate and share information over the internet. Social media have provided the platform for users to share various digital contents such as audio, video, image and text. Everyday millions of such

contents are uploaded and shared within the social media platform. The use of steganography tools on social media is on the rise. Criminals are able to use social media to transfer hidden messages with each other. Due to huge numbers of users, it has been challenging for the investigators to sort and analyse such high amount of data to detect hidden messages passed within the social media and its perpetrators[52]. Another issue in social media is that some of the social media sites change some of the property of the contents like auto re-sizing, changing pixel resolution and so on. Unanticipated modification that are applied to such digital contents can sometimes corrupt the embedded image which will limit steganalysis.

11 Conclusion

In this report, the adverse effects of steganography were discussed. The different categories of steganography were defined and the steganalysis processes for detecting steganography were explained and practical demonstrations were performed. Finally, the issues and challenges for the forensic investigators dealing with steganography were discussed.

Steganography has been a growing field of study in the recent years. Information can be concealed in photographs, recordings, and audios and many other carrier mediums. It opens up a wide range of possibilities for secret communication, more often than not, for unethical purposes. As a result, methods to detect secret communications are required. Steganography cannot always be identified due to utilization of different methods, so steganalysis is still a work in progress. Steganography not being an exact science amplifies the drawbacks of steganalysis. Steganographic software today can mask any form of binary data in a variety of carrier files. It's almost impossible to know if there's a hidden message to begin with; it's like searching for needles in a haystack! Terrorists and criminals are expected to rely on steganography even more in the future, creating a concern for law enforcement authorities. To combat high-tech terrorism and cases of industrial espionage, steganalysis must be further developed.

12 References

[1] J. R. Krenn, “Steganography and Steganalysis,” p. 9, Mar. 2004.

[2] M. Dalal and M. Juneja, “Steganography and Steganalysis (in digital forensics): a Cybersecurity guide,” *Multimed. Tools Appl.*, vol. 80, no. 4, pp. 5723–5771, Feb. 2021, doi: 10.1007/s11042-020-09929-9.

[3] “The Threats of Steganography,” *GFI Blog*, Jan. 11, 2010. https://techtalk.gfi.com/threats-steganography/ (accessed May 16, 2021).

[4] M. J. S. December 18 and 2018, “Twitter Sees Signs of State-Sponsored Attack.” https://www.databreachtoday.com/twitter-sees-signs-state-sponsored-attack-a-11869 (accessed May 16, 2021).

[5] “Steganography: A weapon of cybercriminals | Computing & Communications Services.” https://www.uoguelph.ca/ccs/infosec/steganography (accessed May 16, 2021).

[6] “Hackers’ latest weapon: Steganography,” *Computer Magazine|Flagship magazine of the IEEE Computer Society*,Nov.15,2018.https://publications.computer.org/computer-magazine/2018/11/15/how-steganography-works/ (accessed May 16, 2021).

[7] “Criminal Use of Information Hiding (CUIng) - An Initiative in Cooperation with Europol EC3.” https://cuing.org/ (accessed May 16, 2021).

[8] “The New Threats of Information Hiding: The Road Ahead.” https://ieeexplore.ieee.org/document/8378979 (accessed May 16, 2021).

[9] “Classification-of-information-hiding-techniques.gif (528×748).” http://publications.computer.org/it-professional/wp-content/uploads/sites/33/2018/08/Classification-of-information-hiding-techniques.gif (accessed May 16, 2021).

[10] C. Cimpanu, “Magento Malware Uses Steganography to Steal Payment Card Data,” *softpedia*. https://news.softpedia.com/news/magento-malware-uses-steganography-to-steal-payment-card-data-509388.shtml (accessed May 16, 2021).

[11] A. Siper, R. Farley, and C. Lombardo, “The Rise of Steganography,” *undefined*, 2005, Accessed: May 16, 2021.

[12] “Steganography: A New Age of Terrorism,” p. 9, 2004.

[13] P. P. Balgurgi and S. K. Jagtap, “Audio Steganography Used for Secure Data Transmission,” in *Proceedings of International Conference on Advances in Computing*, New Delhi, 2012, pp. 699–706. doi: 10.1007/978-81-322-0740-5_83.

[14] R. S. R. Prasad and K. Alla, “A new approach to Telugu text steganography,” *undefined*, 2011, Accessed: May 16, 2021. [Online]. Available: /paper/A-new-approach-to-Telugu-text-steganography-Prasad-Alla/bda7e9b79512f07728f3831a0b8a4bdafad4d9de

[15] M. Agarwal, “Text Steganographic Approaches: A Comparison,” *Int. J. Netw. Secur. Its Appl.*, vol. 5, no. 1, pp. 91–106, Jan. 2013, doi: 10.5121/ijnsa.2013.5107.

[16] M. Shirali-Shahreza and M. H. Shirali-Shahreza, “Text Steganography in SMS,” Nov. 2007, pp. 2260–2265. doi: 10.1109/ICCIT.2007.100.

[17] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, “Techniques for Data Hiding,” *IBM Syst J*, 1996, doi: 10.1147/sj.353.0313.

[18] M. H. Shirali-Shahreza and M. Shirali-Shahreza, “A New Approach to Persian/Arabic Text Steganography,” in *5th IEEE/ACIS International Conference on Computer and Information Science and 1st IEEE/ACIS International Workshop on Component-Based Software Engineering,Software Architecture and Reuse (ICIS-COMSAR’06)*, Jul. 2006, pp. 310–315. doi: 10.1109/ICIS-COMSAR.2006.10.

[19] S. Katzenbeisser and F. A. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*, 1st ed. USA: Artech House, Inc., 2000.

[20] M. H. Shirali-Shahreza and M. Shirali-Shahreza, “A New Synonym Text Steganography,” in *2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Aug. 2008, pp. 1524–1526. doi: 10.1109/IIH-MSP.2008.6.

[21] M. Nosrati, R. Karimi, and M. Hariri, “An introduction to steganography methods,” *World Appl. Program.*, vol. 1, pp. 191–195, Aug. 2011.

[22] J. T. Brassil, S. Low, N. F. Maxemchuk, and L. O’Gorman, “Electronic marking and identification techniques to discourage document copying,” *IEEE J. Sel. Areas Commun.*, vol. 13, no. 8, pp. 1495–1504, Oct. 1995, doi: 10.1109/49.464718.

[23] W. Mazurczyk, S. Wendzel, I. A. Villares, and K. Szczypiorski, “On importance of steganographic cost for network steganography,” *Secur. Commun. Netw.*, vol. 9, no. 8, pp. 781–790, 2016, doi: https://doi.org/10.1002/sec.1085.

[24] M. KShah, A. M. Virparia, and K. Sharma, “An Overview of Advanced Network Steganography,” *Int. J. Comput. Appl.*, vol. 118, no. 21, pp. 23–26, May 2015, doi: 10.5120/20871-3364.

[25] C. H. Rowland, “Covert channels in the TCP/IP protocol suite,” *First Monday*, May 1997, doi: 10.5210/fm.v2i5.528.

[26] J. Patel, R. Patel, and M. Shah, “Network Steganography for Hiding Data in IP,” *Int. J. Sci. Res.*, vol. 1, pp. 63–65, Jun. 2012, doi: 10.15373/22778179/DEC2012/26.

[27] B. Jankowski, W. Mazurczyk, and K. Szczypiorski, “Information Hiding Using Improper Frame Padding,” May 2010.

[28] W. Mazurczyk and K. Szczypiorski, “Steganography in Handling Oversized IP Packets,” Jul. 2009, doi: 10.1109/MINES.2009.246.

[29] O. I. Abdullaziz, V. Goh, H. Ling, and K. Wong, “Network packet payload parity based steganography,” *undefined*, 2013, Accessed: May 16, 2021. [Online]. Available: /paper/Network-packet-payload-parity-based-steganography-Abdullaziz-Goh/8f5cac775eea05291e9b64b3ab9cbc75b26ca4a4

[30] K. Szczypiorski, “HICCUPS: Hidden communication system for corrupted networks,” in *In Proc. of: The Tenth International Multi-Conference on Advanced Computer Systems ACS’2003, October 22-24, 2003 Międzyzdroje*, 2003, pp. 31–40.

[31] W. Mazurczyk and K. Szczypiorski, “Steganography of VoIP Streams,” in *On the Move to Meaningful Internet Systems: OTM 2008*, Berlin, Heidelberg, 2008, pp. 1001–1018. doi: 10.1007/978-3-540-88873-4_6.

[32] W. Mazurczyk, P. Szaga, and K. Szczypiorski, “Using transcoding for hidden communication in IP telephony,” *Multimed. Tools Appl.*, vol. 70, no. 3, pp. 2139–2165, Jun. 2014, doi: 10.1007/s11042-012-1224-8.

[33] K. Bailey and K. Curran, “An evaluation of image based steganography methods. Multimedia Tools and Applications,” *Multimed. Tools Appl.*, vol. 30, pp. 55–88, Jul. 2006, doi: 10.1007/s11042-006-0008-4.

[34] K. Karampidis, E. Kavallieratou, and G. Papadourakis, “A review of image steganalysis techniques for digital forensics,” *undefined*, 2018, Accessed: May 15, 2021. [Online]. Available: /paper/A-review-of-image-steganalysis-techniques-for-Karampidis-Kavallieratou/f5c427b655d33ab280ccfe93d846f2f2704fc93c

[35] K.-H. Jung, “A Study on Machine Learning for Steganalysis,” in *Proceedings of the 3rd International Conference on Machine Learning and Soft Computing - ICMLSC 2019*, Da Lat, Viet Nam, 2019, pp. 12–15. doi: 10.1145/3310986.3311000.

[36] A. Nissar and A. H. Mir, “Classification of steganalysis techniques: A study,” *Digit. Signal Process.*, vol. 20, no. 6, pp. 1758–1770, Dec. 2010, doi: 10.1016/j.dsp.2010.02.003.

[37] N. Provos and P. Honeyman, “Detecting Steganographic Content on the Internet,” Dec. 2001.

[38] R. Chandramouli and K. Subbalakshmi, “Active steganalysis of spread spectrum image steganography,” Jun. 2003, p. III–830. doi: 10.1109/ISCAS.2003.1205148.

[39] M. Fan, P. Liu, H. Wang, and S. Xingming, “Cross correlation feature mining for steganalysis of hash based least significant bit substitution video steganography,” *Telecommun. Syst.*, vol. 63, Dec. 2016, doi: 10.1007/s11235-016-0139-5.

[40] K. Koptyra and M. R. Ogiela, “Multiply information coding and hiding using fuzzy vault,” *Soft Comput. - Fusion Found. Methodol. Appl.*, vol. 23, no. 12, pp. 4357–4366, Jun. 2019, doi: 10.1007/s00500-018-3089-x.

[41] T. Aach, A. Kaup, and R. Mester, “Statistical model-based change detection in moving video,” *Signal Process.*, vol. 31, no. 2, pp. 165–180, Mar. 1993, doi: 10.1016/0165-1684(93)90063-G.

[42] B. Jan *et al.*, “Deep learning in big data Analytics: A comparative study,” *undefined*, 2019, Accessed: May 16, 2021. [Online]. Available: /paper/Deep-learning-in-big-data-Analytics%3A-A-comparative-Jan-Farman/407b4abb53dba1e7a91e0f8c1ea53a4380d08e7d

[43] G.C.Kessler, “Steganography for the Computer Forensics Examiner.” http://jeiks.net/wp-content/uploads/2014/estego/Steganography.html (accessed May 07, 2021).

[44] “Gargoyle Investigator™ MP: DFIR Tool for Advanced Malware Detection,” *WetStone Technologies*. https://www.wetstonetech.com/products/gargoyle-malware-detection-dfir/ (accessed May 16, 2021).

[45] A. Luck, *abeluck/stegdetect*. 2021. Accessed: May 16, 2021. [Online]. Available: https://github.com/abeluck/stegdetect

[46] “Ubuntu Manpage: stegosuite - Steganography tool to hide information in image files.” http://manpages.ubuntu.com/manpages/bionic/man1/stegosuite.1.html (accessed May 16, 2021).

[47] L. Paris, *Paradoxis/StegCracker*. 2021. Accessed: May 16, 2021. [Online]. Available: https://github.com/Paradoxis/StegCracker

[48] J. Collins and S. Agaian, “Trends Toward Real-Time Network Data Steganography,” *Int. J. Netw. Secur. Its Appl.*, vol. 8, no. 2, pp. 01–21, Mar. 2016, doi: 10.5121/ijnsa.2016.8201.

[49] M. Kaur and K. Dhindsa, “Enhancement of Data Security using Video Steganography,” *Int. J. Comput. Appl.*, vol. 181, pp. 34–38, Jul. 2018, doi: 10.5120/ijca2018917472.

[50] A. Ibrahim, “Steganalysis in computer forensics,” *Aust. Digit. Forensics Conf.*, Mar. 2007, doi: 10.4225/75/57ad58327ff2e.

[51] W. Mazurczyk and S. Wendzel, “Information hiding: Challenges for forensic experts,” *Commun. ACM*, vol. 61, no. 1, pp. 86–94, Dec. 2017, doi: 10.1145/3158416.

[52] D. E. White, “The Impact of Steganography and Steganalysis on Digital Forensics and Social Media,” M.S., Utica College, United States -- New York, 2017. Accessed: May 16, 2021. [Online]. Available: https://www.proquest.com/docview/1957425715/abstract/3C12972001464BD6PQ/1

[53] K. A. Cole, S. Gupta, D. Gurugubelli, and M. K. Rogers, “A Review of Recent Case Law Related to Digital Forensics: The Current Issues,” p. 11.

[54] S. E. Goodison, R. C. Davis, and B. A. Jackson, “Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence,” in *Digital Evidence and the U.S. Criminal Justice System*, RAND Corporation, 2015, pp. 1–32. Accessed: May 16, 2021.