CONTENTS

S.NO	TITLE	PAGE No.
1.	Introduction	2
2.	History of Steganography	2-3
3.	Steganography VS cryptography	3-4
4.	Uses of Steganography	4-5
5.	Different type of Steganography	5
6.	A. Physical Steganography	5
7.	(a). Invisible ink	5
8.	(b). Null cipher	5
9.	(c). Becon's cipher	6
10.	(d). Microdot	7
11.	(e). Printer Steganography	7-8
12	B. Digital Steganography	8
13	(a). Video	9
14.	(b). Picture	9
15.	(c). Audio	10
16.	(d). Text	11
17.	(e). Hiding data in plain site	11
18.	C. Detecting Steganography	12
19.	(a). Detecting physical steganography	12
20.	(b). Detecting digital steganography	13

1. INTRODUCTION

Steganography is an ancient practice. When spies in revolutionary war wrote in invisible ink or When da Vinci embedded secret meaning in a painting that was steganography. This work in digital in the digital world too where a file like an images can be stealthily encoded with information. For example, pixel values, brightness and filter setting for an images are normally changed to affect the image's aesthetic look. But hackers can also manipulates them based on a secret code with no regard for how the inputs make the images look visually. This technique can be used for ethical reasons, such as to evade censorship or embed message in Facebook photos .But these methods can also be used nefariously. For security defenders the question is how to tell the difference between an image that's been modified for legitimate reasons and one that's been changed to secretly contain malicious information.

"Nothing is the same twice, there's no pattern to look for, and the steganography itself is completely undetectable," says Simon Wiseman, the chief technology officer of the British network security firm Deep Secure, which is working on steganography defence. "With advanced statistics, if you're lucky, you might be able to get a hint that something's strange, but that's no good as a defence, because the false positive and false negative rate is still enormous. So detection does not work."

Steganography techniques can be applied to images, a video file or an audio file. Typically, however, steganography is written in characters including hash marking, but its usage within images is also common. At any rate, steganography protects from pirating copyrighted materials as well as aiding in unauthorized viewing.

Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text, HTML, or even floppy disks) with bits of different, invisible information .This hidden information can be plain text, cipher text, or even images.

Steganography somethings is used when encryption is not permitted. Or, more commonly, Steganography is used to supplement encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered the hidden message is not seen.

There are a large number of steganographic methods that most of us are familiar with (especially if you watch a lot of spy movies!), ranging from invisible ink and microdots to secreting a hidden message in the second letter of each word of a large body of text and spread spectrum radio communication.

2. HISTORY OF STEGANOGRAPHY

The first written case of steganography is found in **Histories** by Herodotus. He writes that happened during the Lonian Revolt, an uprising of some Greek cities against Persian rule at around 500 BC. Histiaeus, the ruler of Miletus was away from his city, acting as an adviser to the Persian king.

He wanted to go back to Miletus, which was under the control of his son-in-law, Aristagoras, so he planned to stage a revolt in Ionia as a pretext for his return. This is where the steganography comes in. He shaved the head of one of his slaves and tattooed a message on his scalp.

Histiaeus then waited for the slave's hair to grow back and hide the message, then sent him to Aristagoras with instructions to shave the slave's head once more and read the message. The concealed text told him to rise up against the Persian rule, which kicked-off the uprising against their conquerors.

Herodotus tells another story about steganography that occurred several years later, when the Spartan king Demaratus sent a seemingly blank wax tablet back to Sparta. Hidden beneath the wax was a message that warned the Spartans of Xerxes' planned invasion.

Herodotus is known for his tall tales, so we can't be sure of how truthful these stories are, but they're the earliest records of steganography we have.

It wasn't long before more sophisticated forms of steganography were recorded. In the 4th century BC, Aeneas Tactics made mention of a hole punching technique Philo of Byzantium **was the first to discuss invisible inks**, writing about them in the third century BC. His recipe used gall nuts to write text and a copper sulfate solution to reveal it

.The term steganography was first used in a book called steganographia by Johannes Trithemius. The word combined the Greek *steganos*, which means concealed, with *graphein*, which means writing.

Steganographia was a clever book that was purportedly about magic and the occult, but used cryptography and steganography to hide its real subject matter, which centered around cryptography and steganography.

Steganographia was followed up by *Polygraphia*, which was first published after Trithemius' death in 1518. This was a more straightforward book about steganography and its practice.

Another key development in steganography came in 1605, when Francis Bacon devised Becon cipher's. This technique used two different typefaces to code a secret message into a seemingly innocent text.

Microdots were first developed in the latter half of the 19th century, but they weren't used heavily for steganography until World War I. They involve shrinking a message or image down to the size of a dot, which allows people to communicate and pass on information without their adversaries knowing.

There have been a wide range of other steganographic developments and techniques over the years. Steganography continues to be practiced to this day, with low tech versions often used by prison gangs, and digital methods harnessed to hide data in pictures, audio and other media.

3. STEGANOGRAPHY VS CRYPTOGRAPHY

Steganography is focused on hiding the presence of information, while cryptography is more concerned with making sure that information can't be accessed. When steganography is used properly, no one – apart from the intended recipient – should be able to tell that there is any hidden communication taking place. This makes it a useful technique for situations where obvious contact is unsafe.

In contrast, cryptography tends to be used in situations where the participants aren't concerned if anyone finds out that they are communicating, but they need the message itself to be hidden and inaccessible to third parties.

Let's go through some examples to understand the differences. If you were a political activist who's been imprisoned and you need to communicate with your organization, the logistics can be challenging. The authorities may monitor everything going in and out of your cell, so you would probably have to hide any communication that takes place.

In this kind of situation, steganography would be a good choice. It may be challenging with the resources you have at hand, but you could write a plain sounding letter with a hidden message concealed with different font types or other steganographic techniques.

Alternatively, let's say you're a diplomat discussing secret details with your home country. It's normal for diplomats to talk with officials from their own nation so the communications themselves don't raise any suspicions. However, since the content of the conversation is top secret, the diplomat may want to use cryptography and talk over an encrypted line.

If spies or attackers try to intercept the conversation, they will only have access to the ciphertext, and not what the two parties are actually saying.

Let's flip things over to examine the differences even further. If the political activist used cryptography to communicate with their organization, the authorities would most likely have intercepted it.

The officials would see the ciphertext and know that the activist was trying to send encoded messages, then they would most likely stop its delivery and interrogate the activist about it. This could end very badly, in beatings, torture, or even the activist's death. That's why steganography would be more suitable in such a scenario.

Conversely, diplomats are often monitored by their host countries. If a diplomat tried to send steganographically concealed messages back home, they could be intercepted, analyzed and the content may be uncovered. In this situation, cryptography is more suitable, because although interceptors will know communication is taking place, they won't be able to find out what it concerns.

4. USES OF STEGANOGRAPHY

Steganography has a number of surprising applications, aside from the obvious one of hiding data and messages. Hackers use it to conceal code in MALWARE ATTACKS. Printers use steganography as well, hiding imperceptible yellow dots that identify which printer created a document and at what time. Steganographic techniques are also frequently used in watermarking and fingerprinting to prove ownership and copyright.

5. DIFFERENT TYPE OF STEGANOGRAPHY

There are many type of steganography to cover each one, so we will stick to more commonly used and interesting forms, giving examples

- **Physical Steganography**
- **Digital Steganography**
- **Detecting Steganography**

6. (A). Physical Steganography

Steganography was developed well before computers, so there are a range of non-digital techniques that we can use to hide information

Examples of Physical steganography:-

7. (a). Invisible ink

Throughout history, invisible ink has been one of the most common steganographic practices. It works under the principle that a message can be written without leaving any visible marks, only to be revealed later after a certain treatment is applied.

A wide range of substances can be used as invisible inks. Some of these include lemon juice, cola, wine, vinegar, milk, and soapy water, all of which can be made visible by heat. Laundry detergents, sunscreen, soap and saliva are also invisible inks, but they are revealed by ultraviolet light instead.

8. (b). Null ciphers

Null ciphers hide their real messages amid seemingly normal text, using a range of different techniques. Common examples include creating a mundane text, where every nth word, or even letter, is part of the secret message.

For example, if we use a null cipher where every fifth word is our real message, we can take a message like:

I don't want any **dogs** because they stink and **are** not known for being **great**.

And find the hidden text:

"**dogs are great**"

Another example of null ciphers

If you **h**ate being so **a**nxious, buy a **p**uppy, or a **p**ony, it'll help **y**ou.

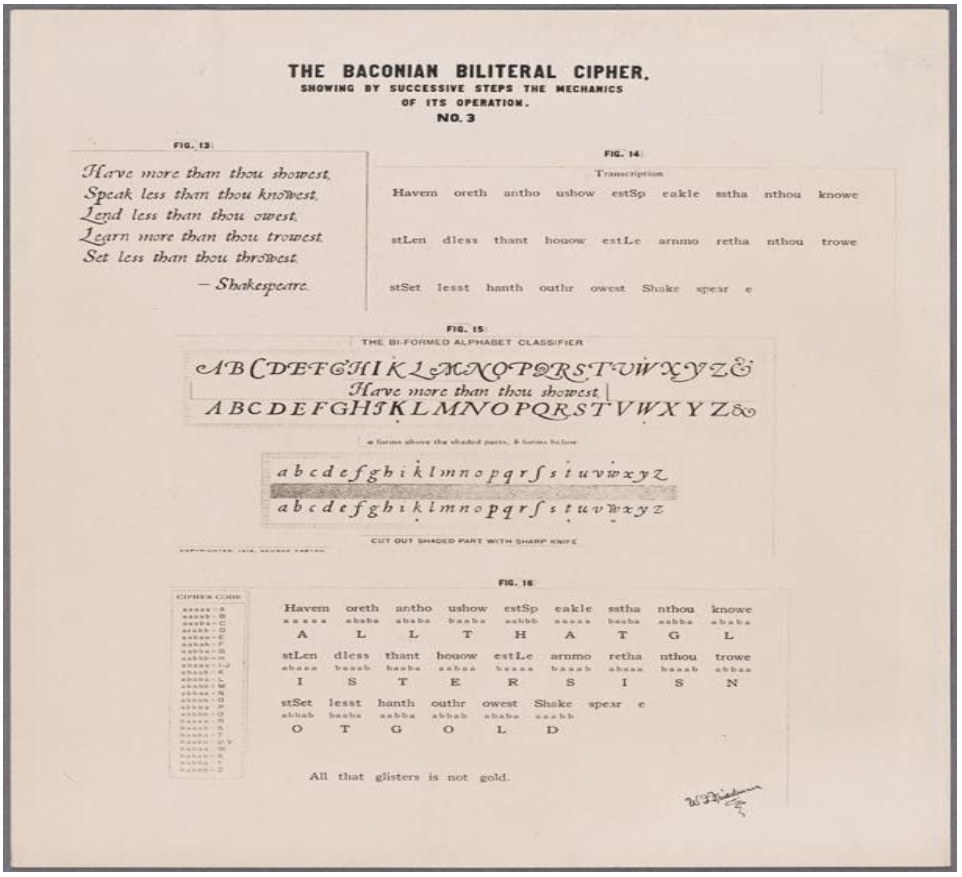
Contains a secret message of:

"**happy**"

9. (c). <u>Bacon's cipher</u>

Another early steganography scheme was Bacon's cipher, invented by the philosopher and politician, Francis Bacon, in the seventeenth century. It was an interesting development, because it hides the secret message in the format of the text rather than its content.

Bacon's cipher is a steganographic technique rather than a cryptographic one because the message is hidden by seemingly normal text, rather than appearing as a jumble of cipher text in plain view. Look at the images below as an example



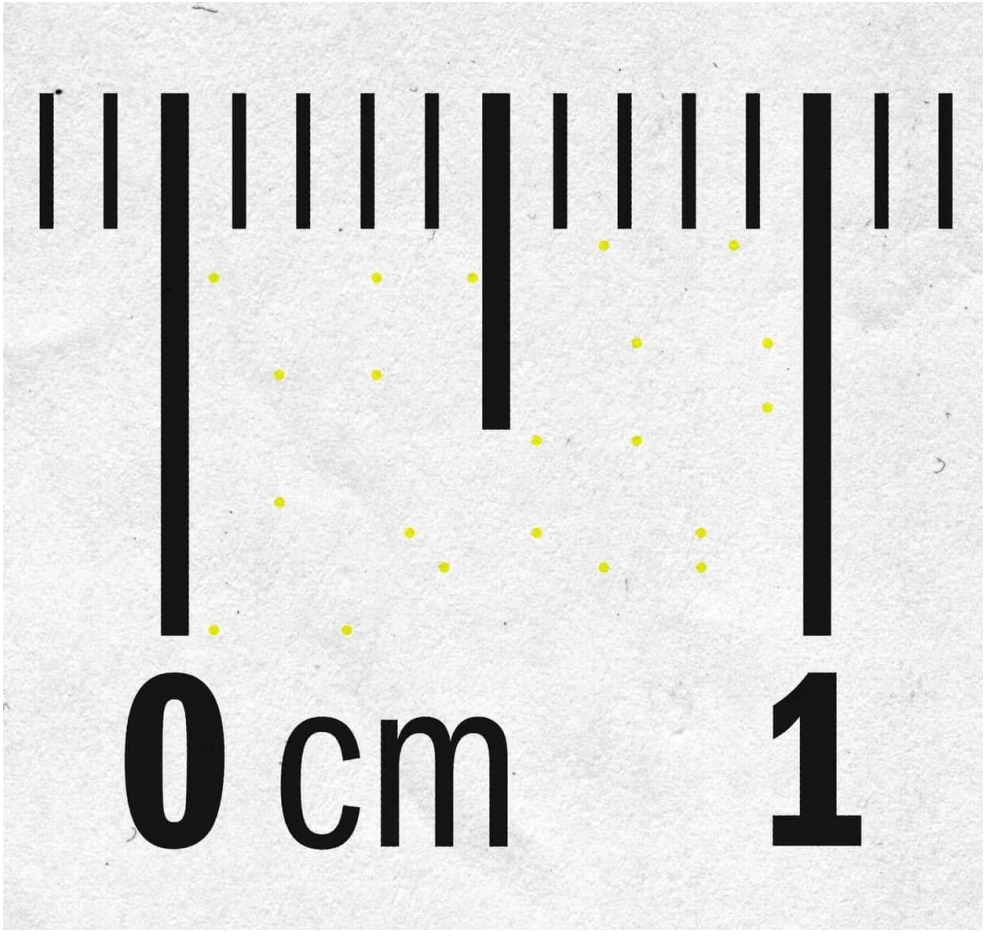
10. (d). <u>Microdots</u>

If you want to hide messages or other information, one of the best techniques is to make it invisible, or at least as close as possible. This is the school of thought behind microdots. They were first developed in the late 19th century and improved upon during the 20th.

Photographic techniques can shrink down images or text to a tiny fraction of the original size. By 1925, a method developed by Emanuel Goldberg was so sophisticated that a regular printed page could be shrunk down to one hundredth of a square millimetre.

Microdots allowed people to hide large amounts of information without any obvious trace. Spies could hide them on their person, send them through the mail, or keep information stored on them. Unless an adversary is already suspicious, microdots are almost impossible to detect, due to their tiny nature.

11. (e). Printer Steganography



An example of the code left behind by printers. Printer Steganography by Parhamr licensed under CC0.

Since the 1980s, various printer manufacturers have programmed their machines to print out a series of almost imperceptible yellow dots on every single page. Each dot is only a tenth of a millimetre in size, and their arrangement is coded to display the printer's serial number, as well as its date and time.

This information is repeated again and again across the page, so that the information can be recovered even if only a fraction of a page is found, or if the printed code is damaged due to printer error, moisture, or other problems.

This steganographic practice is ostensibly used to crack down on currency counterfeiters – if authorities seize the notes, they can figure out which machine they was printed by. It's assumed that the dots are also used to track down the perpetrators of other crimes, with some speculating that the NSA whistle-blower Reality Winner would have been caught using this method, had she not made other mistakes.

The secret dots weren't made public until 2004, when PC World published an article stating that Dutch authorities were using the codes to try and track down a gang that was counterfeiting train tickets.

There are a number of different coding schemes. Most big printer brands have been confirmed to use at least one of them. At this stage, researchers from the EFF aren't sure if every printer model secretly hides some kind of information that can be used to trace when and where a document was printed. Because of this, it's considered safest to assume that every printer does leaves a trace.

In 2018, researchers from the University of Dresden released a program that adds extra yellow dots, scrambling the code. This prevents anyone from being able to trace when and where a document was printed. The software was developed to help whistle-blowers and other activists retain their anonymity.

The software has some limitations, including that it must be used with a printer that's programmed with the same yellow dot encoding technique. Because there are a range of other identification codes in use, there is still a chance that a person's printer leaves other markings on the page which can be used to identify them.

12. (B). Digital Steganography

Like just about everything else in our lives, steganography has made its way into the digital realm. It's possible to hide information in different file types, in a range of

online venues, and even in places you'd never suspect, such as by varying the timing between data packets being sent over a network protocol.

Media files are some of the most popular places to hide information, because their large size means that more secret data can be stuffed inside them without raising suspicion. There are three separate ways that information can be hidden in files:

- By adding it to the file, such as in unused header space.
- By substituting part of the information within the file. One of the most common ways to do this is by altering the Least Significant Bit (LSB). In image, audio and other files, the last bits of information in a byte aren't necessarily as important as the beginning ones. For example, 10010010 might be a shade of blue. If we only change the last two bits to 10010001, it could be a shade of blue that's almost exactly the same. This means we can hide our secret data in the last two bits of every single pixel in a picture, without noticeably changing the image. If we change the first bits, it would alter it significantly.
- By creating a new seemingly benign file, which is actually just a cover for the steganographic text.

13. (a). <u>Video steganography</u>

Videos are relatively large files, so they can hide more data than most alternatives. Some of the most common techniques include a variety of different schemes for substituting the least significant bits (polynomial equations, hash-based, etc.). Alternatively, data can also be embedded into each frame, or filtering and masking data can be used as well. There are a range of video steganography programs available online.

One of the most interesting cases of video steganography was uncovered when the German authorities arrested a suspected al-Qaeda member in 2011. Officers searched the man and found a flash drive as well as memory cards in his underwear. Among the other files was a pornographic video called *Kick Ass*.

Because he was suspected of being involved in terrorism, the authorities investigated the video further to discover that steganographic techniques had been used to hide more than one hundred al-Qaeda documents. These included terrorist training manuals and plots for future attacks.

As un-Islamic as having pornography may seem, it's actually quite a clever scheme. When the authorities find encrypted files, their suspicions are often raised, wondering why the file was encrypted in the first place.

If they were to compel a suspect to hand over their key and discovered that the target had encrypted children's TV shows, it would seem fishy. The authorities would know something is up and be more likely to inspect the data further and discover the hidden information.

Because pornography is generally taboo, particularly for Muslims, the authorities might view the content, then just wave the person off as a sexual deviant filled with shame, rather than inspecting the data further. Fortunately for the world, the German officials weren't tricked.

14. (b). Picture steganography

Data can be hidden in pictures with a variety of techniques. These include:

- Least significant bit – We discussed this earlier under the Digital steganography section.
- Bit plane complexity segmentation (BPCS) – This technique replaces complex data with hidden information in a way that isn't perceptible to the human eye.
- High capacity hiding in JPEGs – This is essentially an adaptation of least significant bit that compensates for the compression involved in JPEG files.

In 2010 a Russian spy ring was busted by US authorities. As part of their communications process, they would encrypt data, use steganography to hide it in pictures, then post them on public websites. The communication technique was

discovered after the suspect's homes were raided and some of their computers were found to contain steganography software.

Steganography has also been used to steal intellectual property. In 2018 a GE engineer conspired with a business partner based in China to steal company secrets related to steam and gas turbines. At first, he just copied files to a flash drive. He was caught, and the company blocked USB ports and banned flash drives from being used.

Remarkably, he wasn't fired, and was given another opportunity to steal files. He took data from 40 Matlab and Excel files, used steganography to hide it in a picture of a sunset, then emailed it to himself, before forwarding it on to his business partner. He was caught by GE, then charged with six counts of economic espionage.

In a worrying trend, steganography is also becoming more common among hackers. Researchers from Trend Micro analyzed the efforts of a Twitter account that posted malicious memes in October 2018.

Once the malware was running on a device, it downloaded the memes from the Twitter account, then extracted a malicious command hidden inside them. It took a screenshot of the infected computer, and sent the information back to the attacker after it collected the control server details from Pastebin.

15. (c). <u>Audio steganography</u>

Audio steganography also comes with a range of different methods. As with all kinds of steganography, it's important for the techniques to be robust, to be able to carry a reasonable portion of hidden data, and for any changes to be as imperceptible as possible. Some of the most common techniques include:

- Least significant bit coding – Just like the other types of least significant bit that we mentioned, it's possible to alter less important parts of the audio data without making any obvious differences to the way a file sounds.
- Echo hiding – Data can also be masked in an echo.

- Tone insertion – Since it's hard to detect lower energy tones when they are near those that are much more powerful, these lower energy tones can be used to conceal data.

A Polish researcher used audio steganography in an interesting project. He took the song *Rhythm is a Dancer* by Snap! and then modified the tempo. When a beat was slowed down, it represented a dash in Morse code, and when a beat was sped up, it signified a dot. He used this system to spell out "steganography is a dancer!"

He then played the song to a mix of professional musicians and laymen. With a one percent tempo discrepancy, no one noticed that anything was amiss. It was only at around two percent that the professional musicians knew that something was up, and around three percent for everyone else.

His results show that it's quite easy to hide information in dance songs without anyone noticing. Despite this, his method isn't a particularly efficient way of communicating, because it only transmitted three words over a whole song.

16. (d). Text

When it comes to text, there are many different ways to hide information. However, because text files are generally quite small, they aren't particularly useful for sending large amounts of data. One simple technique involves opening Microsoft Word, typing out your secret message, then changing the text color to white.

Over the white background of your word processor, it'll look like nothing's there. You can then save it and send it to your co-conspirator, making sure that you instruct them over a secure channel on how to access the information.

Otherwise, they might be perplexed at why you keep sending them blank documents. This isn't a very secure method, because anyone who intercepts the messages will become suspicious about why you are always sending blank documents. All they have to do is select the text and your plot is foiled.

Spammimic offers another steganographic technique to communicate in secret. The website's tool allows you to encode a message so that it looks like spam. Because we are so used to ignoring spam, a message like this could easily fly under the radar and allow you to communicate without being detected. The usefulness of the software is debatable, but at the very least, it shows that messages can be hidden in a wide range of ways – you just have to think outside the box.

17. (e). <u>Hiding data in plain site</u>

The internet is incomprehensibly large, containing a wealth of strange and nonsensical information. This leaves a lot of opportunities to hide secret messages in public without raising any suspicions.

As long as two people aren't already being closely monitored, they can easily post their communications to each other on popular or obscure websites without being caught. They just have to make sure that their actual intentions aren't clear to any onlookers.

Just think of all of the absurd comments you have come across on forums or social media, and the thousands of blog posts that made absolutely no sense. We tend to either brush them off or read them for our own amusement, but never consider that there could be something more to them than lunacy.

The intercept claims that even the NSA has been in on the practice, using its official Twitter account to communicate with Russian spies. In a clandestine operation, the Intercept reports that some of the participants leaked the details of NSA Tweets to Russian operatives before they were posted. According to the report, this acted as confirmation that they were in fact representatives of the NSA, and not just scammers.

Steganography can be incredibly difficult to detect, especially when there is no reason to be suspicious. In the online world, so much information passes before our eyes, that we simply can't spare the time or effort to scrutinize every anomaly, let alone the things that appear legitimate.

This is what makes it so hard to talk about good steganography. All of the examples we've talked about have been failures, because they are now public knowledge. Techniques are actively being researched and the technology is improving, but its very nature makes it impossible to detect successful steganography in the wild.

There may also be a variety of techniques developed outside of the public sphere, by intelligence agencies, terrorist networks and criminal gangs. We really can't know unless we come across examples of them.

Despite this, a lot of analytical tools we can be applied when we suspect that steganography is being used to hide messages. However, the right tool depends on which techniques concealed the data in the first place.

18. (C). Detecting physical steganography

When it comes to invisible ink, the detection methods depend on what kind of invisible ink was used. If it has been done poorly, there may be scratch marks on the paper, a change in its texture, or a differing reflection where the writing has been hidden.

If a message is suspected to contain invisible ink, you can first inspect it visually and smell it for any irregularities. The next step is to pass it under an ultraviolet light, which shows several types of invisible ink. The message can then be exposed to heat, which may reveal other kinds of ink. If you still haven't found the message, exposing it to iodine fumes may do the trick.

If none of these techniques work, you can't prove that there is no message there just that there is unlikely to be one. Your adversary may be using a sophisticated invisible ink solution that you are unaware of.

Null ciphers can often be detected by anomalies in the text. They sometimes use strange turns of phrase as the creator tries to mold their secret message into the cover text. However, if the null cipher is done well and you have no reason to scrutinize it heavily, it can be simple for people to slip hidden messages past you.

Likewise, Bacon's cipher can be detected by looking for anomalies. In suspicious text, interceptors should examine the fonts, spacing, sizing and many other factors. Once again, if it's done well, it can be hard to tell if a secret message is present.

The tiny size of microdots makes them almost impossible to detect, unless the interceptor is already wary. On the other hand, because we know that printers leave codes on every single page, it's pretty easy to detect them.

One method involves taking a high quality scan of the page, then zooming in on some of the white space. If you invert the colors, it should make the yellow dots more apparent. Once you have done that, you can use this tool from the University of Dresden to try and decode the dots.

19. (a). <u>Detecting digital steganography</u>

Digital steganography can also be incredibly difficult to uncover. Unless you are already suspicious, or the steganography has been done poorly, you are unlikely to inspect someone's files in any serious way.

One of the biggest clues is when steganographic software is discovered on someone's computer, or if they have a history of visiting steganography-related sites. This is a good indicator that they may be hiding files with steganography, and can even give clues as to how they are doing it.

If the original version of a file is available, detecting steganographic modifications is relatively straightforward. You can take a hash of the original file and compare it to the suspicious file. If they are different, then the file has been altered and it may include hidden data.

If the above method is not possible, steganography can also be detected through statistical analysis. While our eyes and ears can't generally detect hidden information in pictures and audio, the secret data can often be easily discovered by looking for statistical anomalies and inconsistencies.

Detecting steganography is only part of the process. If steganography is suspected, and the investigator feels almost certain that it contains hidden information, they still might not be able to uncover the data. They may not have the right steganographic tools, could be unable to figure out the algorithm, or the data may have been encrypted beforehand.

If steganography is detected by an interceptor, this may or may not mean failure for the communicators. It depends on their initial reason for sending the message. If it was absolutely critical that communication remain unnoticed, then the detection would compromise their plan. In other cases, communicators may be safe as long as the data itself can't be accessed by the adversary.

CONCLUSION

Steganography transmits secrets through apparently innocuous covers in an effort to conceal the existence of a secret. Digital image steganography and its derivatives are growing in use and application.

In areas where cryptography and strong encryption are being outlawed citizens are looking at steganography to circumvent such policies and messages covertly.

As with the other great innovations of digital age the battle between cryptography and cryptanalysis security experts and hackers records companies and pirates . Steganography and steganalysis will continually develop new techniques to counter each other .

REFERENCES

1. Shahrin Bin Sahib, (26 JAN 2012), "An Introduction to Image SteganographyTechniques" https://ieeexplore.ieee.org/document/6516338/figures#figures, (20 JAN 2020).

2. Josh Lake, (12 JULY 2019), "What is steganography and how does it differ from cryptography", https://www.comparitech.com/blog/information-security/what-is-steganography/#The_different_types_of_steganography**,** (20 JAN 2020).

3. Lily Hay Newman, (6 JUNE 2017), " What Is Steganography?" https://www.wired.com/story/steganography-hacker-lexicon/, (22 JAN 2020).

4. Petitcolas, Fabien A.P., Katzenbeisser, Stefan (2016), "Steganography", https://en.wikipedia.org/wiki/Steganography,(21 JAN 2020).

5. Margreat Rouse,(29 MAY 2007), "Steganography", https://searchsecurity.techtarget.com/definition/steganography,(22 JAN 2020).

6. Alexey Shulmin, Evgeniya Krylova, (3 AUG 2017), "Steganography in contemporary cyberattacks", https://securelist.com/steganography-in-contemporary-cyberattacks/79276/,(25 JAN 2020).

7. Gary C.kessler,(1SEPT 2001), "Steganography: Hiding Data Within Data", https://www.garykessler.net/library/steganography.html,(23 JAN 2020).

8. Cory Janssen, (3 AUG 2019), "Steganography",https://www.techopedia.com/definition/4131/steganography, (25 JAN 2020).