Steganography and Cryptography: Challenge to Digital Forensics

Mr. Navin D. Bhanushalee, Assistant professor, ROFEL BBA & BCA College, Vapi, India, navindbhanushali9033@gmail.com

Mrs. Zinkal Patel, Assistant professor, ROFEL BBA & BCA College, Vapi, India, zinkal.patel121@gmail.com

Abstract : In today's digital era, the internet is an essential part for communication and information interchange. The security of data transfer via internet and digital media has become a fundamental issue so the confidentiality and integrity are required to protect data from unauthorized access. The use of Steganography and Cryptography is increasing in daily life in order to protect our digital data because as we all concern about our security. There are various types of Cybersecurity technique but Steganography and Cryptography are most useful of them. Both of them have their specific goals of improving security, compatibility, reliability and efficiency. This paper gives basic details about Steganography and Cryptography, their methods and their applications. Comparison of both of these techniques is also done in this paper. The use of cybersecurity technology to protect computer data is growing day by day and that may create a challenge for forensic investigators in their examinations.So, in addition of details about techniques, here we have also discussed challenges may be faced by Forensic Investigators while analysing Digital evidence.

Keywords : Challenges in Digital Forensic, Cryptography, Cybersecurity,Diffrence between Cryptography and Steganography,Digital Forensic, Steganography

I. STEGANOGRAPHY

Steganography is the art and science to hide any type of information or file within another file or cover medium. The purpose of steganography is to protect confidential data from a third person. Steganography hides the covert message it doesn't means that two persons or two parties are communicating with each other. Some person may also use steganography to hide sensitive or personal data from others and store it them into any digital device. A *stego-system* is the mechanism that is used to perform steganography.

There are various components which make up stego-system :

Embedded Message:the original secret message or file to be hidden behind the cover medium

Cover medium:the medium used to hide the message or file

Stego-key:the secret key used to encrypt and decrypt the message

Stego-medium:the combined cover medium and embedded message is called Stego-medium. [4]

II. PROCESS OF STEGANOGRAPHY

First, the cover medium is choosed to hide message within it. Then software are used to hide text behind the cover medium using key or password. This key or password is called as Stego-Key. Stego key is used to embed message in cover and extracting the message from cover medium also.

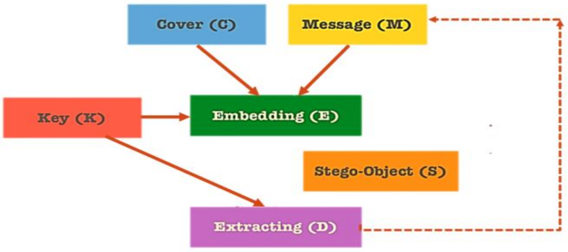


Figure1 : Process of Steganography

Objectives of Steganography

Steganography fulfils the goal like Confidentiality and Authentication. In simple terms confidentiality ensures that the information can't be understood by anyone for whom it was intended. Authentication ensures that the sender and the receiver can confirm each other's identity and source/destination of the message.

Goals like Data Integrity and Non-Repudiation is not fulfilled by Steganography.

Steganography in Past

Steganography isn't just limited to text-based communications. From the second world-war until now, broadcast as well as television communications could be utilized to disguise encoded or disguised information.

According to certain intelligence authorities, Laden's previously taped movies, which were re-broadcasted on television networks throughout the globe, might have included secret messages. [1]

Many contend that perhaps the United States is a rogue state. WWII Marine Corps Navaho coding conversationalists are an example of cryptography. The content of the communications wasn't encoded; it was merely written in a dialect which the Asians didn't understand. Additional techniques to hide communications from the neutral onlooker included vanishing ink or even diminutive marks. [1]

One of the earliest steganographic ideas involved shaving a sender's hair and tattooing a text on it. The envoy could be delivered to the desired destination once his head grows the hair back. Once arrived at the destination the message bearer's head could be cut-off and the text could now be documented. This approach is deftly smart, painstaking, but crude and deprives of any technology, and it gets directly into the very core of stenography's strict definition which is concealed writing. [1]

III. Classification of Steganography

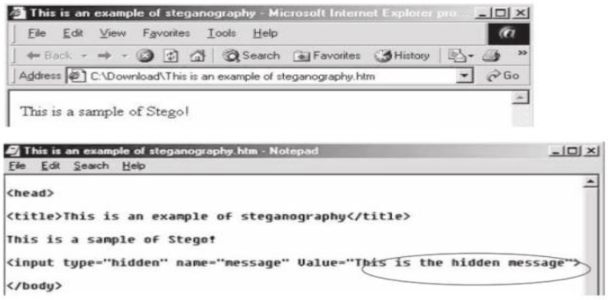
Steganography is classified into mainly three categories: Technical Steganography, Linguistics Steganography and Digital Steganography.Our focus is more on Digital Steganography.

Digital Steganography can be done using Text Files, Image Files, Audio Files and Video Files and etc. So, we can say that Digital Steganography can be performed using any type of Digital Files.

Techniques Used in Digital Steganography

1.Insertion

- In injection technique, the secret message is placed inside a cover file. The secret message is directly inserted into a cover medium using various software, cover medium could be an image file, video file or text file, etc.


This is an example of steganography - Microsoft Internet Explorer pro...
File Edit View Favorites Tools Help
Back Search Favorites History
Address C:\Download\This is an example of steganography.htm
Go
This is an example of steganography.htm - Notepad
File Edit Search Help

This is a sample of Stego!

```
<head>
<title>This is an example of steganography</title>
This is a sample of Stego!
<input type="hidden" name="message" Value="This is the hidden message">
</body>
```

Figure2 : Shows Insertion Technique of Digital Steganography[4]

- In insertion technique, we are inserting an extra information or data in a file so the size of the cover file increases and making it easy to detect, so this is the drawback of this technique. This can be overcome by deleting the original file after the file with the hidden message is generated. Then it is difficult to detect that the file contains any hidden information or not once the original file is deleted.

2.Substitution

The rightmost bit of the binary notation has very least significance. So, Least-Significant-Bit (LSB) technique is used.In that technique the rightmost bit of the binary notation which has very least significance is substituted with a bit from the embedded message and it doesn't affect the original file because the rightmost bit has the least impact on the binary data.

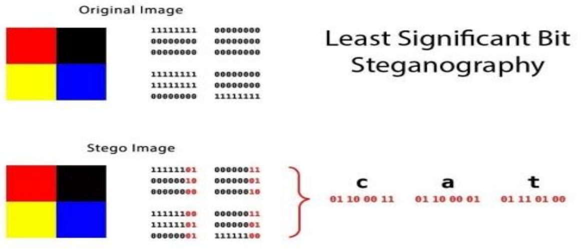


Figure3 : Shows Substitution Technique of Digital Steganography

- If an attacker knows that this technique is used, then the data are vulnerable because he can use any hex editor and see the binary notation of file.

3.Generation

- This technique generates a new cover file exclusively for the purpose of hiding data instead of selecting a cover file to hide a message.
- A picture is created that has a hidden message in it. In the modern form of file generation, a spam-mimic program is used. Spam mimic embeds the secret message into a spam message that can be e-mailed to any destination.

IV. Applications of Steganography

Steganography can be used in following fields:

- In Hospital to maintain Medical Records of Patients
- In Workplace communication
- In Digital Music
- Terrorism
- The Movie Industry
- Secret Communication, etc.

Steganalysis and Stego-forensics

- Steganalysis is the reverse process of steganography. Steganography hides data, while steganalysis is used to reveal hidden data. Steganalysis detects the encoded hidden message and, if possible, recovers that message.

- Stegoforensics is an area of forensic science dealing with steganography techniques to investigate a source or cause of a crime. Different methods of steganalysis can be used to reveal secret communications between antisocial elements and criminals.

V. CRYPTOGRAPHY

- Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.[7]
- The prefix **"crypt-"** means "hidden" or "vault" and the suffix **"-graphy"** stands for "writing." [7]
- In short, we will know cryptography as Hidden-writing.

Basic Terminology of Cryptography [6]

- Plain Text : A message that sender wants to sends
- Cipher text: coded message which generated after encryption
- Enciphering/Encryption: mechanism of converting plaintext to cipher text
- Deciphering/ Decryption: convert the plain text from the ciphertext
- Key: the secret variable strings used for performing encryption/decryption

- Nowadays cryptography is becoming more popular because of the security challenges which are faced by users on the internet. Cryptography helps us to protect our sensitive information from intruders or hackers, which is transmitted over the internet. Cryptography is the mechanism of safe communications that allow only the sender and receiver of a message to view its contents. This process is closely associated with encryption, which is the process of converting original content into meaningless text and vice-versa.
- Cryptography not only protects data but can also be used for authentication along with data integrity and non-repudiation.

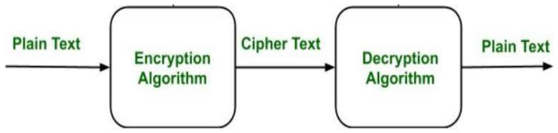


Figure 4:Shows the Process of Cryptography

Objectives of Cryptography

It Fulfils the security goals like Confidentiality, Integrity, Non-repudiation and Authentication. **Confidentiality** ensures that the information will only reach the person for whom it is sent no other person can get it. **Integrity** ensures thatthe information not be modified while transmission between sender and receiver. **Non-repudiation** ensures that the sender of information later on can't deny his intention of sending a message. **Authentication** ensures that the sender and the receiver can confirm each other's identity and source/destination of the message. [5]

Types of cryptography:

In total there are 2 types of Cryptography available:

1. Symmetric Key Cryptography

In this type of cryptography, the sender and receiver of a message share the same key for encryption as well as decryption also. In Symmetric key Cryptography the process is quite simple and faster, but the issue is that the sender and receiver have to transfer the key in a very secure way. DES(Data Encryption System) is the type of Symmetric key cryptography.This type of cryptography is also known as Secret Key/ Private Key cryptography.[3]

Advantages:

Complexity is very less as it uses only one key and it is very easy to use.

Disadvantage:

If any attacker gets the secret key, then he can easily decrypt the message and your confidentiality can be affected.

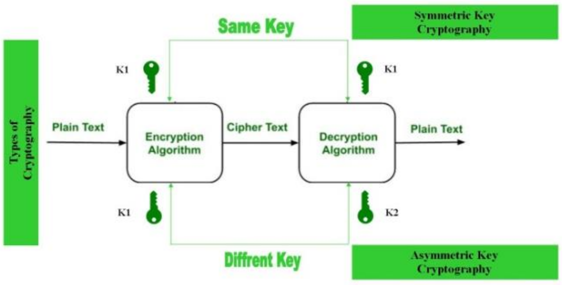


Figure5 : Shows the Different Process of Two types of Cryptography

2.Asymmetric Key Cryptography

In this type of cryptography, the sender and receiver of a message have different keys for the encryption and decryption. Here the sender encrypts the message with the public key and the receiver decrypts the message with its private key. As compared to Symmetric Key Cryptography this processes the data slower than usual. This type of cryptography is more secure than Symmetric Key cryptography. RSA and DSA are the types of Asymmetric key cryptography. This type of cryptography is also known as Public key cryptography. [2]

Advantages

The major advantage of Asymmetric Key cryptography is unbeatable security because here we are removing the key distribution problem.

Disadvantage:

The process is slow compared to other cryptography systems.

DOI : 10.35291/2454-9150.2021.0539

Cryptanalysis:

Cryptanalysis is the process of observation in order to breach a cryptographic secure system and gain unauthorized access over encrypted data. Cryptanalyst is the person who decrypts the encrypted message without prior knowledge of any keys.

III. Difference between Cryptography and steganography [8]

Steganography	Cryptography
Steganography means protected or hidden writing.	Cryptography means confidential or secret writing.
The attack which is performedin steganography is known as steganalysis.	The attack which is performed in cryptography is known as cryptanalysis.
In steganography information is not changed.	In cryptography information is changed.
Steganography provides only Confidentiality and authentication type of security measures	Cryptography provides all the security measures like authentication,confidentiality,non-repudiation and integrity.
steganography doesn't involve any mathematical transformations.	Cryptography involves various number theory and complex mathematical formulas to modify data.

Table1 : Shows the Difference between Steganography and Cryptography

On the bases of above table we can conclude that the Steganography and Cryptography both of the technologies are used for data security. Steganography provides only confidentiality and authentication in information security whereas Cryptography satisfies all the four needs of information security including Non-repudiation and Integrity also.

Steganography is the science deals with how communication can be disguised while cryptography is the science of transforming the content of the communication and making it obscure. It also implies the difference between breaking the system, the steganography is defeated if the presence of steganography is disclosed, whereas in cryptography the attacker must not be able to read the secret message otherwise the system is broken. The security of the steganography depends on the secrecy of the data encoding system.[10]

IV. Impacts of Cryptography & Steganography on Forensic Investigation and Challenges Faced by Investigators

The use of cryptography and steganography to protect digital data is growing and that creates challenges for forensic investigators. Without a key or password, digital forensic tools can't be used to search ad analyse digital evidence. Even if investigators have key or password, searching and analysing encoded data which is protected using steganography and cryptography can be tricky, tough and very time consuming.

Forensic Investigators have limited access to the information on the device that they can access. If any storage media is fully encrypted, then forensic investigators can't get access easily on data and so that investigative options become limited. If the storage media or device in encrypted in that case the first thing an investigator have to do is to determine the level and extent of the encryption. [9]

If user has set weak passwords, then it can be easily cracked by brute force attacks, but if the user has set a strong password, it becomes almost impossible to crack password and access the data. [9]

There are chances that digital evidence can be damaged or corrupted of while working with them.

The other thing is that if the whole drive is encrypted it must be decrypted in order to analyse the data and that can take hours. And there may be chances of drive decryption fail, etc. and which can be damage your drive.

In such cases, Forensic Investigators spend too much time in trying to decrypt a storage media where files are encrypted and so that it may affect the overall time of analysis of case. [9]

VI. References

[1] Kessler, G., 2001. Steganography: Hiding Data Within Data. [Blog] Available at: <https://www.garykessler.net/library/steganography.html> [Accessed 5 August 2021].

[2] Francis, N., 2015. Information Security using Cryptography and Steganography. *International Journal of Engineering Research & Technology (IJERT)*, [online] 3(28). Available at: <https://www.ijert.org/> [Accessed 3 August 2021].

[3] Abboud, G., Marean, J. and Yampolskiy, R., 2010. Steganography and Visual Cryptography in Computer Forensics. *IEEE Computer Society*, [online] pp.25-30. Available at: <https://ieeexplore.ieee.org/Xplore/home.jsp> [Accessed 8 August 2021].

[4] 2010. *Investigating Data and Image Files, EC-Council | Press*. Course Technology/Cengage Learning, pp.1.1 - 1.20.

[5] KOTHARI, J. (2020). Cryptography and its Types. Retrieved 9 August 2021, from https://www.geeksforgeeks.org/cryptography-and-its-types/

[6] Shunmugapriya. (2020). Basic Terminology. Retrieved 8 August 2021, from https://www.eezytutorials.com/Cryptography-And-Network-Security/Basic-Terminology.php#.YRNUHd_hVPY

[7] Richards, K. (2020). Cryptography [Blog]. Retrieved from

DOI : 10.35291/2454-9150.2021.0539

https://searchsecurity.techtarget.com/definition/cryptography

[8] MKS075. (2020). Difference between Steganography and Cryptography. Retrieved 9 August 2021, from https://www.geeksforgeeks.org/difference-between-steganography-and-cryptography/?ref=rp

[9] Spruill, A. (2021). Digital Forensics and Encryption. Retrieved 9 August 2021, from https://www.evidencemagazine.com/index.php?option=com_content&task=view&id=656

[10].Difference between Steganography and Cryptography, from https://techdifferences.com/difference-between-steganography-and-cryptography.html

DOI : 10.35291/2454-9150.2021.0539