iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: https://doi.org/10.22214/ijraset.2022.44279

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

Types and Tools of Steganography

Dr. Nitika Arora
Assistant Professor of Computer Science, S.U.S Govt college Matak Majri, Indri

Abstract: ***Steganography is the practice of concealing a secret message inside of another message. It is a form of covert communication and can involve the use of any medium like a computer file, message, image, or video within the other file, message, image or video. It is not the same as cryptography where cryptography means secret writing and steganography which is not as popular as cryptography means covered writing. Many different file formats are often used but digital images or media files are the most popular due to their most-used on the web and the large size of media files. There exist many Steganography techniques for hiding secret information in images where some of them are more complex than others. Steganography works by changing bits of useless or used data in regular computer files such as graphics, sound, and text with bits of different and invisible information. Steganography technique refers to methods in which data hiding is performed directly on every hundredths or thousandths pixel value of cover image by replacing with corresponding to letter in the alphabet in such a way that the effect of message is not visible on the cover image and unnoticeable to someone. This paper is intended to illustrate the different steganography techniques and the purpose of techniques.***

Keywords: Cryptography, cover-medium, Watermarking, stego-message, LSB (least significant bits),

I. INTRODUCTION

Since the invention of the Internet one of the most important factors in home networks or professional networks is network security at all levels. In today's scenario, it is very easy to exploit networks because of one or more wireless routers so even if we have a solid network system to protect the computer network against unethical issues like hacking or unauthorized access to the system still there may be chances of loss of information or use of our personal information in the wrong way. So cryptography was used to secure the information and communication which allows only sender and receiver to know the exact messages in proper form. In this technique, cryptographic algorithms are used which take the original message and convert the original message to cipher text using a secret key which is not understandable, and then this encoded message and key is sent to the receiver to decrypt the message. The major objectives behind this technique are to maintain the integrity, confidentiality, and authenticity of the message.

In spite of having more advanced cryptographic techniques, there is a need to secure the data more at the deepest level and this race continues to create more advanced techniques so steganography is used where hiding of information takes place within the other file or message which is ordinary and non-secret in the form of image, text or video and then secret data is transferred to the destination. Basically, steganography means encryption with the extra step of hiding or secreting the information to protect the data [1].

There are many forms of steganography available for hiding a secret message which can be of any digital type including text, audio, image, or video and this data is to be hidden inside another digital type of content.

II. ORIGIN OF STEGANOGRAPHY

Steganography was developed in ancient Greece around 400 B.C .The word Steganography comes from Greek word steganographia where stegano means covered and graphia means writing .The Steganographia term was firstly used in 1499 by Johannes Trithemius in his discourse on cryptography and steganography. Steganography is defined by Markus Kahn as follows, "Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity". Steganography has been used for 2500 years for many purposes. The major use of these techniques is in the area of military, Banking, intelligence services, personal and Business world. Steganography is the means of sending information to someone without the fear of being grabbing the data by the interceptor.

Steganography is the technique of disguising the existence of an original message called cover. The cover medium in which we want to hide the data which needs to be protected for copyright reason. The hidden message is called embedded message which we want to cover or hide .The main digital carriers of the information on the internet are images, audio, video, text, etc. which hold the hidden information. The combination of hidden data and cover is known as the stego-object .Stego Key is an additional piece of information or secret information like password which is required to extract the embedded message from the stego medium where

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

stego medium is that information which receiver can see so decoding takes place at the receiver end on the secret Message by removing the cover Using the Stego Key and Receiver Reads Secret Message [2]
We can define this simple formula:
Cover-medium + embedded-message = stego-message

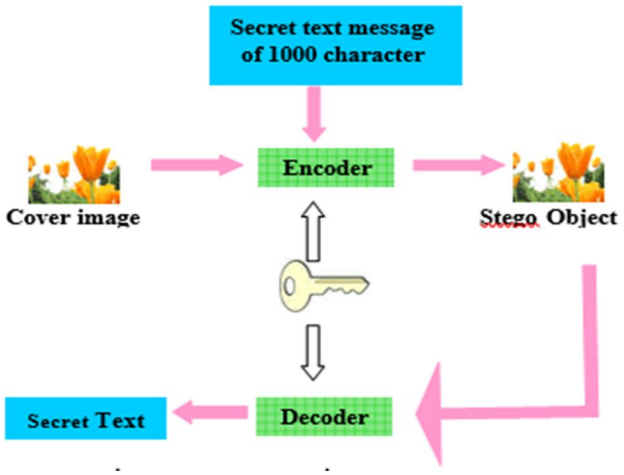


Figure 1: The basic Steganography model [14]

III. DIFFERENT FORMS OF STEGANOGRAPHY

There are many forms of steganography that have been used to hide a secret message .One of them is the usage of invisible ink which is unrelated to computer for hiding the secret messages by writing the message with clear ink and they can be seen only by other ink when applied on the another message .Invisible ink technique is in limited use today[3].
Then concept come under steganography is the technique which is mainly used for businesses called watermarking. Watermarking is the technique used for content authentication, copyright management and content protection. For example if I have created a document and I embedded that document with a watermark that identifies me as creator of that document so whenever that document shared or spread on the internet it shows that I am the owner of this document .so this technique is used by digital world for content protection .Watermarking is used to hide the proprietary data [4].So if someone tries to copy the image then that watermark also gets copied with that image and this watermark could be image, audio or video. There are two types of watermark: one is visible watermarking and other is invisible watermarking. Visible watermarking where logos or text is visible on the image, audio or video and in invisible information is not visible and need to be detecting by some other means.
The other techniques are null ciphers and microdot. Null ciphers is technique used in ancient times in which plain text is included with the cipher text .There are many options and patterns are there of using null ciphers like taking the last letter from each word or taking the letter from particular position as 1,2,3,....from each word.

A. Types of Steganography

1) *Text steganography:* It is the type in which the information is hidden within the text by changing the format of the text. Text steganography is most difficult to achieve because of less duplicates in text as compared to images, videos and audio files. The most used method for this is data compression where the form of text is changed to another. The various techniques used are Random and Statistical Generation, Format Based Method and Linguistic Method.
2) *Image Steganography:* It is the type in which information is hidden within the image. The reason of most used of image steganography is the large number of bits representation in digital form of the image. There are many techniques used in image steganography are [5] Least Significant Bit Insertion, Redundant Pattern Encoding, Masking and Filtering, Encrypt and Scatter and Coding and Cosine Transformation.. The most used method is the least significant bit insertion where we hide the message by replacing the least significant bit of the image such that no visible change is observed in the colour of the image[6].
3) *Audio Steganography:* It is the type in which information is hidden into audio files such as mp3 sound file, wav file or AU files and secret message can be of any form image, audio, text or video within the audio file. The methods which are used for audio

steganography are Hiding methods where insertion based, substitution based and Generation based are mostly used .The techniques which are used for audio steganography are Echo hiding, Phase coding ,Parity coding, spread spectrum ,Tone insertion and LSB(Least significant bit)[7].The process of sending secret message using audio steganography is most difficult.

4) *Video Steganography:* It is the type in which information is hidden within the frames of video. This type is most prominently used because a large amount of the data travelling on the internet is in the video format .In video steganography ,along with least significant bit (LSB) method, the other technique masking-filtering can be used to hide the secret message within the frame of the video. These both techniques are used for 24 bit images [8]. The video files are generally comprised of both audio and video so audio steganography techniques are used for audio part and video steganography techniques are used for video part which makes it more robust and secure. So two stage secret techniques are embedded to hide the secret message within the video file. One is least significant bit (LSB) for image steganography and the second is discrete cosine transform (DCT) for video steganography [9].
5) *Network Steganography:* In this type of steganography ,the secret information is hidden within the network .This method is more sophisticated in terms of usage of hiding the information in the header or packet of protocols depending on which method is being used in network steganography .In today's scenario people exchange information over social media like Face book ,Whatsapp, Skype , voice calling or video calling so there are numerous methods to hide the information over the network[10]. Network steganography can be categorized into two ways depending on the OSI model: One is Intra-protocol Network steganography and other is Inter-protocol network steganography. The methods used are HICCUPS (Hidden Communication System For Corrupted Networks),RSTEG (Retransmission Steganography) ,LACK (Lost Audio Packets Steganography),SCTP (Stream Control Transmission Protocol),PadSteg (Padding Steganography), SkyDe(Skype Hide),StegTorrent,Steg Suggest and TranSteg (Transcoding Steganography).

B. Tools used in Steganography

A number of tools have been created to use steganography and the different tools have different functions but the most widely used is hiding text or image in another image because images are harmless.

1) *Hide n send Steganography:* It is one of best steganography tools .It hides the data inside the jpeg image. It uses encryption and encrypts the data using the F5 steganography algorithm. It supports a lot of hashing, concealment and encryption algorithms. The procedure of hiding and extraction are available in respective tabs on interface. Selection of cover image and concealed file can be done using the hide tab [11].

Figure 2 Hide-n-send steganography [11]

Then you can apply concealment algorithm (M-F5, M-LSB, F5, LSB), Hash algorithm (SHA512, RIPEMD, MD5) and Encryption algorithm (AES, RC2, RC4) and then hide the data. Extraction of data is done by choosing the extract tab with the password set during hiding the data.

2) *Open stego:* It is steganography application that come with two functions:1)Hiding of Data Hide any data with Image file and 2.)Watermarking: To imprint an invisible mark on the image .It is used for detecting unauthorized copying of the file [12].It is open source and free tool developed using the Java. The output of hiding the file in openstego is the .png file.

Figure 3: Open stego tool [12]

3) SSuite Picsel: The use of this tool is very simple and does not require to be installed as it is a portable tool. It involves selection of image as key and no need of password .Then enter your message and encrypt the image and save the image with a different name [12].Now decrypt the message using the encrypted image and secret message will be displayed in your text editor.

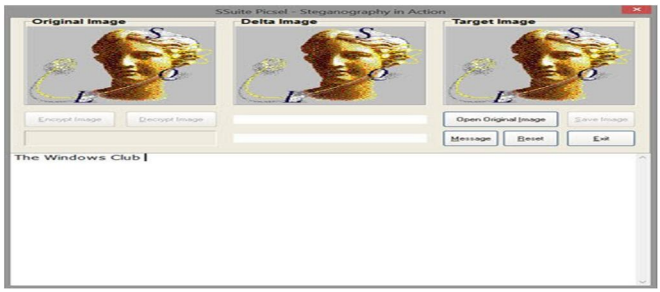


Figure 4: SSuite Picsel Steganography tool [12]

4) Xiao steganography: It is the best tool which is used both for image and audio files .The most used file formats for image is bmp and for audio file is wav.this tool starts with an option to load the target file for cover file and then it involves the use of loading the required secret message in the cover file by using the add files option [13]. A number of encryption and hashing algorithms are available according to requirement and then decrypt the whole process using the extract file option .It is a very easy and strong tool among the other tools.

Figure 5: Xiao steganography tool [13]

There are many other tools available such as Stegsolve, Exiftool, Exiv2, BinWalk, Zsteg, Wavsteg, Rsteg, Crypture, Our secret for steganography.

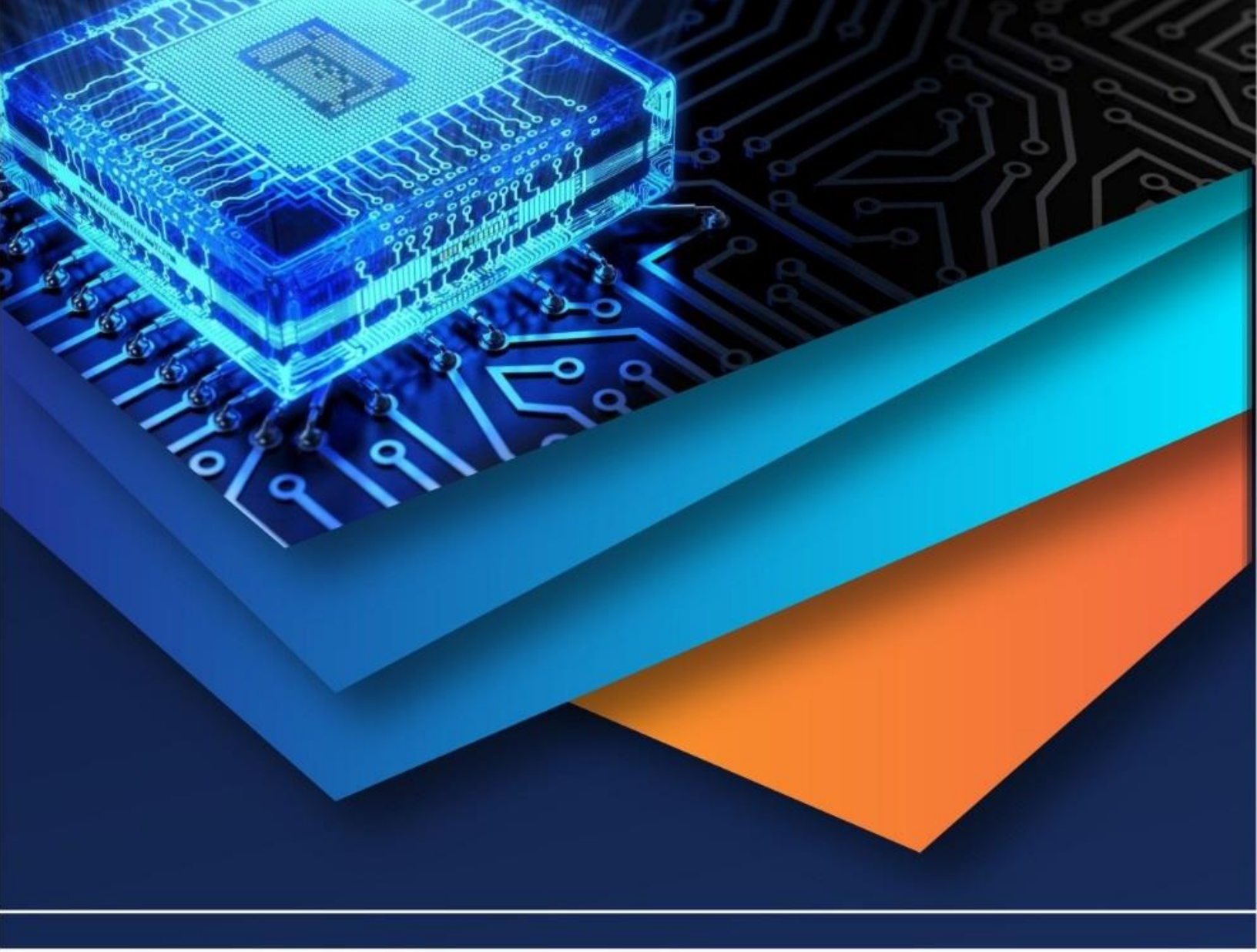
IV. CONCLUSION

In this paper, Introduction, Types and tools are discussed. Many different techniques are there and will continue to develop as there is no guarantee of securing the hidden information. A number of methods are being developed to defeat steganography. In today's scenario digital watermarking is influencing the users because there is a need to protect the information from copyright work and illegal distribution. A number of free tools exist for steganography and are very easy to use .So there are more chances for criminals

to use these for their communication. The methods used for steganography are basically for concealment and there is need for security with privacy to be incorporated.

REFERENCES

[1] UKEssays. (November 2018). Examining the Importance of Steganography Information Technology Essay. Retrieved from https://www.ukessays.com/essays/information-technology/examining-the-importance-of-steganography-information-technology-essay.php?vref=1
[2] UKEssays. (November 2018). Steganography: Uses, Methods, Tools and Examples. Retrieved from https://www.ukessays.com/essays/computer-science/steganography-uses-methods-tools-3250.php?vref=1
[3] (Amritha Sekhar, 2015)4. Huang, Chun-Hsiang & Chuang, Shang-Chih & Wu, Ja-Ling. (2006). Digital invisible ink and its applications in steganography. 23-28. 10.1145/1161366.1161372.
[4] Kaushik, N. (2012, May 7). Differences between Watermarking and Steganography. Difference between Similar Terms and Objects. http://www.differencebetween.net/business/product-services/differences-between-watermarking-and-steganography/.
[5] Arun Kumar Singh, J. S. (2015). Steganography in Images Using LSB Technique . International Journal of Latest Trends in Engineering and Technology (IJLTET) , 426-430.
[6] Kilic, Eren & Evrensevdi, Berke. (2020). A Review on the Different Types of Steganography.
[7] Kaur, N. (2014). Audio Steganography Techniques-A Survey. Int. Journal of Engineering Research and Applications, Vol. 4 (, Issue 6), pp.94-100.
[8] Rajkumar, Gat & Malemath, Virendra. (2017). Video Steganography: Secure Data Hiding Technique. International Journal of Computer Network and Information Security. 9. 38-45. 10.5815/ijcnis.2017.09.05.
[9] Abhishek Saxena, S. S. (2017). A Review of Video Steganography Methods. International Journal of Innovative Science and Research Technology, 2 (8).
[10] Namrata Singh, J. B. (2017). Network Steganography and its Techniques: A Survey. International Journal of Computer Applications (0975 – 8887) , September.
[11] Ahmed, W. (2012, June 7). Hide'N'Send: Conceal Sensitive Text Files Inside Images Through Steganography. Retrieved from https://www.addictivetips.com/.
[12] Kolla, a. (2020, june 11). List of 10 Best Steganography Tools to Hide Data. Retrieved from GEEk dashboard: https://www.geekdashboard.com/best-steganography-tools/
[13] Nidhi bhatia, g. K. (2019). Xiao Steganography. International Journal of Scientific Research in Computer Science Applications and Management Studies , 8 (1).
[14] Dr.E.N.Ganesh. (2017). Steganalysis of LSB Insertion Method in Uncommpressed Images Using Matlab. 3. 1-6.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY