RESEARCH ARTICLE OPEN ACCESS

Comparative Study on Different Embedding and Steganography Technique for Text Data and Image Security

Kavita Choudhary [1], Brij Kishore [2]

[1] M.Tech Scholar, Department of Computer Science and Engineering,
[2] Assistant Professor, Department of Computer Science and Engineering,
Apex Institute of Engineering and Technology, Jaipur, Rajasthan - India

ABSTRACT

Information security has been a serious challenge in communications since the arrival of the internet. With the enhancement of information technology and internet, digital media has become one of the most popular data transfer tools. This digital data includes text, images, audio, video, and software transferred over the public network. Most of this digital media takes the form of images and is an important element in various applications such as chat, news, website, e-commerce, e-mail and e-books. Today's huge demand for Internet applications requires data to be transmitted in a secure manner. Data transmission in public communication systems is not secure due to interception and improper manipulation by eavesdroppers. So a tantalizing solution to this problem is digital data security in which Steganography, embedding and cryptography is most popular techniques. In this paper present the comparative analysis of different Steganography and embedding techniques that are used for text data and digital image security purpose.

Keywords — LSB, DCT, DWT, Embedding, Steganography, Secrete Image, Secrete Text Data.

I. INTRODUCTION

In the today going on technology, for the data exchange the Internet is the most popular and important medium. With advances of the internet and information technology, the digital media has become one of the most popular and best-known data transfer tools. This digital data includes text, images, audio, video and software transferred via the public network [1]. Digital Data are the most widely used modes of communication in very field usually, such as the research, industry, medical, military etc. Significant image transfers take place over an unsecured web network. Therefore, it is necessary to establish adequate security so that the digital picture or digital image prevents from the unauthorized persons to accessing secrete information. steganography and cryptography are the most popular techniques for data security [2]. Data protection has come to be a heavy digital verbal exchange drawback through the internet or the alternative medium. Cryptography and stenography are the widely used technique for data security. In cryptography data is change one form to another form and in steganography secret data is hidden into cover data [3]. The word Steganography comes from the Greek word "stegos", which meaning "cover" and graphic meaningful writing that designates it as a cover writing [4]. In Image Steganography, data is hidden solely in cover image or picture. Steganography is the science and art of secret communication [5]. Hiding information is important to secure online communication, especially in the military and commercial areas, and copying and unauthorized access. Correspondence between two gatherings, security offices, any knowledge association, or some other private trade of data must be secure.

The main goal of hiding information to pictures is to transfer information safely over the Internet [6]. Steganography is mainly cauterized into four types that are text, image, audio and video steganography. Steganography is widely used for secret communications, feature tagging and copyright protection.

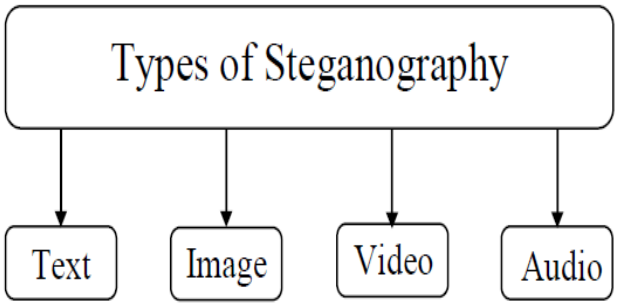

Fig 1: Types of Steganography

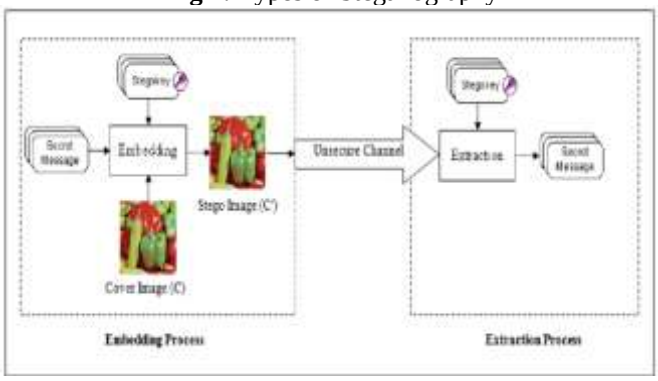

Fig 1: Embedding Process

II. LITERATURE REVIEW

Sharaf et. al. 2021 [7], Discussed that with the advancement of the wireless access network the information security become more and more serious issue. So here it is necessary to develop more secure method to transfer the information through the internet then the existing techniques. In the most of the communication system image is the one of the most popular and widely used in wireless communication format. In this present a new method of image steganography that is hybrid of chaos map and discrete transforms methods.

Rustad et. al. 2021 [8], discussed the different image steganography techniques have been created to improve the nature of the stego image, for example intangibility, ability and security. This examination proposes a versatile technique which can choose the most ideal model to limit the error rate because of the embedding of messages. This versatile model can improve the presentation of the converse LSB substitution technique, in view of the two bits + LSB model in the compartment image. Prior to inserting, the holder and message image bits are tested and the error rate is determined utilizing the converse LSB substitution strategy for a few potential models. The model with the most reduced lowest error rate is chosen to incorporate the message. The utilization of this versatile model in LSB turn around image Steganography significantly builds intangibility.

Karakus et. al. 2020 [9], presented a new image steganography method with optimum pixel similarity for data hiding in medical images. Steganography is one of the most popular approaches to hide the data. The capacity of data hiding and quality of the image of cover object are most important factor in the image Steganography. In the human vision system the quality of image can be noticed and it attracts the attacker attention. So the purpose of this study to increase the hidden data amount and ensure the quality of the setgo image is high quality. In this proposed optimization based technique making the use of the pixel similarities. In this proposed technique the performance of the test data has been used visual quality of merit analysis such as PSNR, MSE etc.

Soni et. al. 2020 [10] Proposed a grayscale medical image encryption technique with hiding the patient information in the form of 2D barcode into the gray scale medical using LSB technique and encrypted that grayscale image after hiding the patient information using Genetic Algorithm. İt improve the security of the patient information with medical image also.

Watni et. al. 2019 [11], discussed different steganography techniques that was showed in previously and give us a comparatively analysis for jpeg image steganography. In this a portion of the methods recommended by the specialists was discussed. To apply jpeg steganography, three significant boundaries of image steganography are considered, in particular joining, heartiness and imperceptibility.

Benedict et. al. 2019 [12], Present the data bits of the message to be veiled are organized arbitrarily and the pixel bits of the picture are likewise made interesting, making the example garbled to recognize.

Table 1. Comparative Analysis of Different Steganography and Embedding Technique

Ref No.	Year of Publication	Technique Used	Description	Advantage
[8]	2021	LSB	In this work proposed a secure image steganography technique in which hide an image in an image using the LSB technique and measure the security of the hiding in the term of MSE and PSNR.	Get low MSE and high PSNR Value.
[9]	2020	Optimum Pixel Similarity	In this discussed the human vision system the quality of image can be noticed and it attracts the attacker attention. So the purpose of this study to increase the hidden data amount and ensure the quality of the setgo image is high quality.	Quality of merit analysis such as PSNR, MSE is better.
[10]	2020	LSB, Genetic Algorithm	Protect digital medical image using pixel based image protection using LSB water marking and AES algorithm.	Difficult to creak. Apply steganography and cryptography together to enhance the security.
[11]	2019	DCT	Discussed a portion of the methods recommended by the specialists.. To apply jpeg steganography, three significant boundaries of image steganography are considered, in particular joining, heartiness and imperceptibility.	Improve the security of the secret data stored in smart device or framework.
[12]	2019	LSB	Used pixel based technique for file security purpose.	the pixel bits of the image are also made unique, making the pattern unintelligible to recognize

III. CONCLUSION

In this, many important stenography techniques have been introduced and analyzed to become familiar with the different stenography algorithms that used for the image that has been transferred to the network. According to the survey of recent research, it has been said that security is the main concern in the transmission of images. The security issue is expanding quickly with devices created for hacking image information. Numerous analysts have proposed answers for the security issue; however have not had the option to get total security on the unstable organization. Stenography sends privileged insights through apparently innocuous covers to hide the presence of a secret. Hide advanced data, images and their subordinates is progressively utilized and applied. In this give an overview and comparative analysis of different stenography techniques for image, data or information hiding.

REFERENCES

1. H. Arora, G. K. Soni, R. K. Kushwaha and P. Prasoon, "Digital Image Security Based on the Hybrid Model of Image Hiding and Encryption," 2021 6th IEEE International Conference on Communication and Electronics Systems (ICCES), pp. 1153-1157, 2021.
2. Gaurav Kumar Soni, Himanshu Arora and Bhavesh Jain, "A Novel Image Encryption Technique Using Arnold Transform and Asymmetric RSA Algorithm", In. Springer International Conference on Artificial Intelligence: Advances and Applications 2019, Algorithm for Intelligence System, pp. 89-90, 2020.
3. Matted S., Shankar G., Jain B.B., "Enhanced Image Security Using Stenography and Cryptography", Computer Networks and Inventive Communication Technologies, Lecture Notes on Data Engineering and Communications Technologies, Vol-58, Springer, Singapore, 2021.
4. Arpita Tiwari, Gori Shankar, Bharat Bhusan Jain, "Comparative Analysis of Different Steganography Technique for Image Security", International Journal of Engineering Trends and Applications (IJETA), Volume-8, Issue-2, Mar-Apr 2021.
5. Vipin Singh, Manish Choubisa and Gaurav Kumar Soni, "Enhanced Image Steganography Technique for Hiding Multiple Images in an Image Using LSB Technique", TEST Engineering & Management, vol. 83, pp. 30561-30565, May-June 2020.
6. Arpita Tiwari, Gori Shankar, Dr. Bharat Bhushan Jain, "Digital Image and Text Data Security Improvement Using the Combination of Stenography and Embedding

Techniques", Design Engineering, Issue-7, pp. 8592-8599, 2021.

7. J. Sharafi, Y. Khedmati, M.M. Shabani, "Image steganography based on a new hybrid chaos map and discrete transforms", Optik, Volume-226, Part-2, PP-1-34, 2021
8. Supriadi Rustad, De Rosal Ignatius Moses Setiadi, Abdul Syukur and Pulung Nurtantio Andono, "Inverted LSB image steganography using adaptive pattern to improve imperceptibility", Journal of King Saud University – Computer and Information Sciences, PP-1-10, 2021.
9. Songul Karakus, Engin Avci, "A new image steganography method with optimum pixel similarity for data hiding in medical images", Medical Hypotheses, Volume 139, PP-1-8, 2020.
10. G. K. Soni, A. Rawat, S. Jain and S. K. Sharma, "A Pixel-Based Digital Medical Images Protection Using Genetic Algorithm with LSB Watermark Technique", in Smart Systems and IoT: Innovations in Computing: Springer. pp. 483-492, 2020.
11. Dipti Watni and Sonal Chawla, "A Comparative Evaluation of Jpeg Steganography", 5th IEEE International Conference on Signal Processing, Computing and Control (ISPCC 2k19), pp-36-40, 2019.
12. Arnold Gabriel Benedict, "Improved File Security System Using Multiple Image Steganography," IEEE International Conference on Data Science and Communication (IconDSC), Bangalore, India, pp. 1-5, 2019.