RESEARCH ARTICLE OPEN ACCESS

Comparative Analysis of Different Steganography Technique for Image Security

Arpita Tiwari [1], Gori Shankar [2], Dr. Bharat Bhusan Jain [3]

[1] M.Tech Scholar, Department of Electronics & Communication
[2] Assistant Professor, Department of Electronics & Communication
[3] Principal, Jaipur Engineering College, Kookas, Jaipur, Rajasthan - India

ABSTRACT
In the age of information technology, the most vital part of information exchange and communication is 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. Content is still facing a number of challenges, including issues of modification, authentication, copyright protection. To ensure data, cryptography and Steganography are broadly utilized. Steganography shrouds the mystery information in another record so just the beneficiary knows the presence of the message. Steganography is characterized as the investigation of imperceptible correspondence. Steganography by and large arrangements with methods for disguising the presence of the imparted information so that it stays classified. Stay quiet between two questioners. Different types of the techniques or methods are used to hide the data in Steganography. In this paper present the comparative analysis of different Steganography techniques for data (image, text, audio, video etc) security.

Keywords: RSA, AES, LSB, DCT, DWT, Steganography, Secrete Image, Secrete Data.

I. INTRODUCTION

Data (text, image, audio, video etc) 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 [1]. 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 [2]. 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. Without causing the hacker to notice shrouded data, they ought to be sent. In the event that programmers notice this in any capacity, the concealed data must be in encoded structure all together not to be unscrambled. In this way, this data is remained careful [3].

II. STEGANOGRAPHY

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.

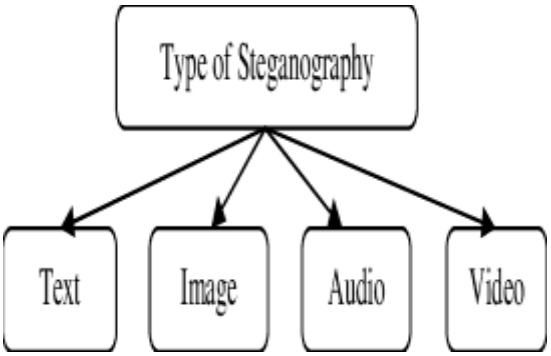

Fig 1: Types of Steganography

The three principle terms utilized in Steganography frameworks are: cover data, secret information message, and implanting algorithm. Secrete key terms can likewise be entered to give a safer association. An introductory letter is the mode of the message, for instance, a audio, video, text and picture or other computerized medium [5]. The secret message is the data that ought to be covered up in the proper advanced medium. The mystery key is commonly

used to implant the message as indicated by storing calculations. An integration algorithm is the real trick or strategy used to remember classified data for an introductory massage. 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.

III. RELETED WORK

Soni et. al. 2020 [5] 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**. Kini et. al. 2019 [2]**, Present the recent enhanced in computer security have shown that concealment info instead of encoding is that the best thanks to shield information. The LSB could be a wide used method of knowledge concealment and is at risk of attack owing to its simplicity. In this A 24-bit color image carrier is employed to cover the key image, and also the same is employed to cover the steno key. It compares the PSNR associated suggests that MSE and runs an analysis graph to work out to what level the steno image is hidden within the carrier image. **Watni et. al. 2019 [6],** discussed different steganography techniques that was sued in previously and give us a comparatively analysis for jpeg image steganography. **Benedict et. al. 2019 [7]**, 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. **Krishna et. al. 2016 [8],** It has been indicated that the proposed reversible steganography strategy utilizing the pre-prepared DES IMNP calculation permits better joining and picture quality qualities to be gotten contrasted with existing NMI and INP methods. **Shelke et. al. 2015 [9],** proposed conspire limits the contortion after data incorporation. The execution of this plan is straightforward. It is more affordable than the space domain methods recently utilized. The data concealing capacity is more prominent than that of DE and EMD. **Mousa et. al. 2013 [10],** proposed the random function strategy coordinates touchy data into a norm and non-standard host picture utilizing various random coefficients and boundaries.

Table 1. Comparative Analysis of Different Steganography Technique

Ref No.	Year of Publication	Technique Used	Description	Advantage
[5]	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.
[2]	2019	LSB	In this gives the details about the how to secret image is hide into the 24-bit color cover image using LSB technique	Gives an enhanced hiding technique that is difficult to crack easily

[6]	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.
[7]	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
[8]	2016	IMNP algorithm with DES	It has been demonstrated that the discussed reversible steganography technique using the pre-processed DES IMNP algorithm allows better integration and image quality values to be obtained compared to existing NMI and INP techniques.	decreasing the computational complexity of IMNP algorithm.
[9]	2015	DE, EMD, LSB	The proposed scheme limits the distortion after data incorporation. The execution of this scheme is very simple	More security than LSB from unauthorized user.
[10]	2013	Random Function	The random function strategy coordinates touchy data into a norm and non-standard host picture utilizing various random coefficients and boundaries.	Get high PSNR and low MSE values

IV. 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. 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, 89-90 (2020).
2. N. Gopalakrishna Kini, Vishwas G. Kini and Gautam, "A Secured Steganography Algorithm for Hiding an Image in an Image.", In. Springer Nature Singapore Pte Ltd., Integrated Intelligent Computing, Communication and Security, Studies in Computational Intelligence 771, 539-546 (2019).
3. Imra Aqeel and Muhammad Babar Suleman, "A Survey on Digital Image Steganography Approaches" In: Springer Nature Singapore Pte Ltd. INTAP, CCIS 932, 769–778 (2019).
4. R.Anderson and F. Petitcolas, "On the limits of Steganography" IEEE Journal of Selected Areas in Communications, Vol. 16, No. 4, (1998).
5. 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..
6. Dipti Watni and Sonal Chawla, "A Comparative Evaluation of Jpeg Steganography", 5th IEEE International Conference on Signal Processing, Computing and Control (ISPCC 2k19), 36-40, (2019).
7. 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.
8. Dr. Himanshu Arora, Mr. Manish Kumar and Mr. Sanjay Tiwari, "Improve Image Security in Combination Method of LSB Stenography and RSA Encryption Algorithm", International Journal of Advanced Science and Technology, Vol-29, No-8, 6167-6177, (2020).
9. S.G.Shelke and S.K.Jagtap, "Analysis of Spatial Domain Image Steganography Techniques", In. IEEE International Conference on Computing Communication Control and Automation, 665-667 (2015).
10. Hamdy M. Mousa, "Secured Steganography Algorithm Based Random Function", 2013 8th International Conference on Computer Engineering & Systems (ICCES), 228-232 (2013).