International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 10 Issue 5 ǁ 2022 ǁ PP. 216-220

Image Steganography

[1]Neha Srivastava , [2]Namita Singh, [3]Prabhat Kumar Yadav , [4] Ankit Khare
[1&2]Research Scholar , [3&4]Assistant Professor
[1&2]Department of Information Technology , Shri Ramswaroop Memorial College of Engineering And Management,Lko
Dr. A.P.J Abdul Kalam Technical University, Lucknow,Uttar Pradesh,India

ABSTRACT – *With the fast improvement of data transfer methods through internet it has become easier to send the data accurately and faster to the destination point There are many channels to transfer the data to destination like electronic mails, social networking sites etc. Due to which it becomes easier to change or modify and exploit the sensitive data information through hacking. So, in order to transfer the data safely to the destination without any modifications, there are many approaches like steganography and cryptography.Steganography is the art of hiding the truth that communication is in process by hiding information in other information.There are different file formats that can be used but digital images are the most in demand because of their large frequency on the internet. There are several steganographic ways for hiding sensitive or private information in an image. Some of them are more difficult to use than others and they all have their advantages and disadvantages . Various applications may require complete invisibility of secret information, while other applications may require protection of large confidential messages. In this project report we focus on providing a the complete overview of image steganography, its uses and methods, also attempts to to find the needs and requirement of good steganographic algorithm and compactly shows us which steganographic methods are the best for particular application.*
Keywords: *Vision based technique, Steganography algorithm,Digital image hiding*

Date of Submission: 15-05-2022 Date of acceptance: 30-05-2022

I. INTRODUCTION

One of the common reason that the intruders can be successful is that most of the information they acquire from system is in the form that they can read and comprehend. Intruders may reveal that knowledge to others and,modify or misrepresent it to an individual or organization, or make use of it to attack. The simple solution to solve this trouble is, through the use of technique called steganography. Steganography is a technique of hiding data in digital media. In compare to cryptography, [1]it is not to keep others from knowing the hidden information but it is to keep others from knowing that some data or information even exist .Steganography is becoming more important as more and more people are joining the cyberspace revolution. Steganography is the art of concealing information in ways that stops the detection of hidden data messages. Steganography include an arrangement of secret communication methods that hide the message from being found or discovered.

Since rise of the Internet security of information in communication and information technology is a important factor. Cryptography was created for the purpose of r securing the secrecy of communication and many different ways have been invented to encrypt and decrypt informative data in order to keep the message secret. Unfortunately sometimes it is not enough to keep the contents of a message confidential, it is also necessary to keep the existence of the message a secret. The technique used to execute this kind of feature is called steganography.

Steganography is the capability of communicating in a way that lockup or hides the presence of the communication in progress. [2] The word Steganography is derived from two Greek words- ‘stegos’ meaning ‘to cover’ and ‘graphy’, means ‘writing’, thus translating something into ‘covered writing’, or ‘hidden writing. It includes a vast variety array of secret communication methods that conceal the message very existence. These methods include unnoticeable inks, microdots , character arrangement, electronic signatures, stealthy channels ,and spread spectrum communications. On the simplest level, steganography is hidden writing, whether it consists of invisible ink on paper or copyright information hidden in audio file,video file or text file. Where as cryptography scrambles a message into a code to obscure its meaning and make it unreadable steganography hides the message entirely. These two secret communication technologies can be used separately or together for example, by first encrypting a message, then hiding it in another file for transmission.

Today, the world has become more eager about the use of confidential communication, and due to the

regulations are created by governments to limit uses of encryption, steganography's role is gaining prominence.Steganography crucially makes the most of use of human perception, human being senses are not up skill to search for objects that have data concealed inside them[3],even though there are certain programs available that perform stegnalysis (Detecting the use of Steganography.). This regular/common use of image steganography is to conceal one file inside another. Steganography hides the secrete text within the host data set and presence imperceptible and is then very reliably communicated to the receiver. The host data set is intentionally damaged, but in a stealthy way, designed to be invisible in information analysis.

Steganography is the exercise of hiding sensitive or private information within something that appears to be nothing but very usual and common. Steganography is usually confused with cryptography because both of then are alike in the way that they both are used to safeguard the crucial information. The difference between steganography and cryptography is that steganography involves hiding information data such that it appears as if no information is hidden at all, for example if a person views the object that has the information hidden inside it he or she will not get even a pinch of idea that something is inside it, so they will not try to decrypt it.

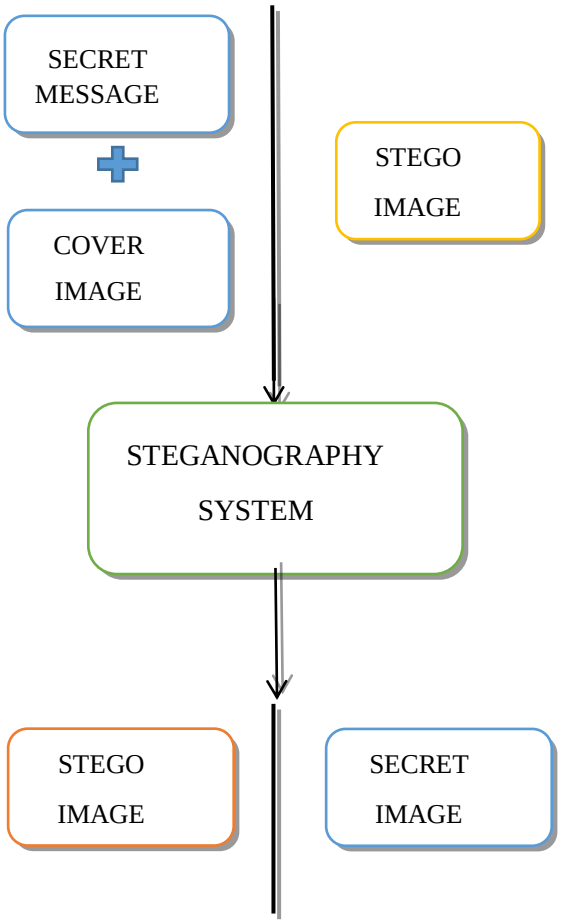
Due to advancement in ICT, most of importannt documents are kept electronically.So, the security of information has become a serious issue. Besides cryptography, streganography can also be employed to protect information. In cryptography, the secret messages or encrypted messages before being passed through the network are embedded indigital host, thus the existence of the message is unrevealed. Besides hiding data for confidentiality, this approach of information hiding can be stretched out to copyright protection for digital media like video,audio.

II. RELATED WORK

Mostafa Ahmad [6] proposed an enhanced medical image steganographic algorithm He used integrated wavelength filter to decompose image, arithmetic coding (AC) and data encryption Standard (DES) for information processing.[7] Rostam, Habib Esmaeelzadeh used combination of chaos functions image blocking method in which block centers are used to generate the initial key of the chaos function, then selected secret data bits are hidden in the pixels of randomly selected blocks.[8] Kurane, S.H. Harke, and S Kulkarni provided a high performance steganography method based on LSB1 and LSB2 algorithms which supports all kinds of image format.

[9]K. B. Raja in 2005 used the combination of LSB algorithms, DCT transformation, and compression using quantization and run length coding on raw images to obtain secure stego-image, this helpss secure transfer of payload with lower amount of MSE and BER as compared to earlier techniques. In the year 2013 Mohammad Javad KosraviI [10] launched a new way to improve the existing security of steganography using integer wave length and secret sharing method. His method had three phases: first cryptography phase which uses a secret sharing method, second data hiding phase using a novel integer wavelength based steganography method, and third date extraction phase. In 2007 Hong-Juan Zhang, Hong-Jun Tang [11] had proposed a novel LSB image steganography algorithm. Which avoided the weak points of classic LSB steganography algorithm, but maintains high insertion capacity and low computational complexity. It can also effectively withstand RS analysis, Chi-square test In the year 2015 Amritpal Singh and Harpal Singh [12] proposed an improved and advanced LSB technique for color images by embedding the information into three planes of RGB image in a way that enhances the quality of image with high embedding capacity. As compared to all the work done in steganography methods previously ,the proposed module has higher PSNR value. Gandharba Swani in 2011 [13] proposed a new LSB (least significant bit) array based image steganographic method using encryption by RSA algorithm is. In the image each pixel has 8 bits. There are four arrays, with the name LSB, LSB1, LSB2 and LSB3 which are put together by collecting the bits from the 8th (LSB), 7th, 6th and 5th bit locations of the pixels respectively. The cipher text is split into four blocks.In the year 2021 Nandhini Subramanian did[14] a research in which the main aim was explore and discuss various deep learning methods available in image steganography field. Deep learning techniques used for the purpose image steganography can be divided into three types - traditional methods, Convolutional, General Adversarial Network-based and Convolutional Neural Network-based

III. SYSTEM ARCHITECTURE



IV. METHODOLOGY

When the user starts the application the user has two options in front of him encrypt and decrypt. If user selects encrypt the application gives the screen to select image file, information file and option to save the image file. If user select decrypt option , the application shows screen to select only image file and ask path where user want to save the secrete file. This project is divided into two phases – encryption and decryption. In encryption process the secrete/important information is concealed inside any type of image file and in decryption the secrete information from image file is extracted The project has following objectives: To produce security instruments based on steganography methods. Find different ways to hide data using the encryption module, Use the decryption module to extract images with data. Project is a friendly, simple and effective application that truly hides the data of the image file of your choice. For Lsb, we get the same image as the cover image after performing encryption. We run a decryption function to extract the information (or hidden text in our case). In other words, the application extracts data from the image and achieves the main goal of the project.

V. MODULE DESCRIPTION

V[I] AUTHENTICATION

Authentication field consist of user and password, it helps us provides or gives the permission to view the project.The two operations in this field are Ok and Cancel,if the password and username are valid ok helps you to view the project else shows a error message.And cancel is used to stop user actions.

V[ii] EMBEDDING MESSAGE IN PICTURE

In this module the process of hiding data in image starts and file is saved in memory location, Encryption Key are provided by the user to hide message in the save file location.

Image location-The Image file, which already, exists in the system.Save the file -This is also an Image file, which is generated by the user. User has to save this new file in any location according to their wish. This file is used to embed the message in the image file.Encryption Key-This key is the private key. This is

confidential key between sender and receiver. This is also embedded in picture with message.Validation code-This is actual file size of the image location. This is in bytes. The message is added to the saved image location after this last byte.Hide-It is used to hide the message into saved image file. Messages are encrypted in unknown format and then embed in the saved image file.Send-The user to another user uses this button to send the saved image file, whichcontains the message hided.

V[iii] RETRIVING DATA

This phase has the following Extract Messages- This module is used to extract messages.Image Location-Downloaded images by the user are given as input in this text box.Encryption key- The key used to extract the message. This a secret key. Receiver should know this key to retrieve message.Validation Code-This is the offset of the file where actually the message is reside.Extract message- When receiver clicks this button the message is shown to the receiver. Encrypted messages are decrypted and then shown in the text box

VI. CONCLUSION AND FUTURE SCOPE

Steganography is a really interesting topic that goes beyond the basic encryption and system administration that most of us deal with on a daily basis. Steganography can be used for covert communication. We explored the limitations of the theory and practice of steganography. to provide a safe means of communication, we printed enhancements to our image steganography system using an LSB approach. Stego-key was put on to the system while encrypting the data in the cover image.

This steganography application software is designed to use image format to hide any type of file inside. The main and most important work of this system is in supporting all types of pictures without necessarily converting it in bitmap, and also reducing limitation on the size of file to hide, as it uses maximum space of memory to hide file inside a picture.Since long ago man has a desire to fine something from which he can secretly communicate. [4]In the recent time with the vast research in watermarking to protect intellectual property is proof that steganography is not only limited to military or surveillance applications. Like cryptography steganography will also play an increasing role in future to secure the communication in the world which is digitally growing. An ideal steganographic algorithm should have high precision, a higher level of security with good embedding capacity. Efficiency,simplicity and cost efficiency should also be considered. Thus, it is necessary to investigate steganographic problems and solve it with different approaches using different inputs. It is observed that the steganographic schemes designed in the transform domain are much better in terms of security as compared to the spatial domain schemes because in the transform domain, the secret message bits are embedded in the DCT or DWT coefficients rather than directly manipulating the pixels as happens in the spatial domain.

Due to the advancement of digital technology and the popularity of social media, people are becoming more vulnerable. So, to increase the security, future work may be continued in transform, compress or random domains.

[5]The design and implementation of the proposed strategy presented in this paper is novel. However, some restrictions still exist. There are some areas where the project can be stretched .further.. The concepts of steganography through PVD, weighted matrix, graph neighbourhood, DCT, and DWT are conventional

REFERENCES

[1]. Pahati, Omar J. "Confounding carnivore: How to protect your online privacy." AlterNet. Archived from the original on (2007): 07-16.

[2]. Hariri, Mehdi, Ronak Karimi, and Masoud Nosrati. "An introduction to steganography methods." World Applied Programming 1.3 (2011): 191-195.

[3]. https://www.scribd.com/document/131910082/What-is-Steganography

[4]. https://www.imaging.org/site/PDFS/Papers/1999/PICS-0-42/1043.pdf

[5]. Pal, Pabitra, Partha Chowdhuri, and Biswapati Jana. "Weighted matrix based reversible watermarking scheme using color image." Multimedia Tools and Applications 77.18 (2018): 23073-23098.

[6]. Ahmad, Mostafa A., et al. "Hiding patients' medical reports using an enhanced wavelet steganography algorithm in DICOM images." Alexandria Engineering Journal 61.12 (2022): 10577-10592.

[7]. Rostam, Habib Esmaeelzadeh, Homayun Motameni, and Rasul Enayatifar. "Privacy-preserving in the Internet of Things based on steganography and chaotic functions." Optik 258 (2022): 168864.

[8]. Kurane, S., H. Harke, and S. Kulkarni. "TEXT AND AUDIO DATA HIDING USING LSB AND DCT A REVIEW APPROACH."Natl. Conf."Internet Things Towar. a Smart Futur."Recent Trends Electron. Commun. 2016.

[9]. Raja, K. B., et al. "A secure image steganography using LSB, DCT and compression techniques on raw images." 2005 3rd international conference on intelligent sensing and information processing. IEEE, 2005.

[10]. Khosravi, Mohammad Javad, and Ahmad Reza Naghsh-Nilchi. "A novel joint secret image sharing and robust steganography method using wavelet." Multimedia systems 20.2 (2014): 215-226

[11]. Zhang, Hong-Juan, and Hong-Jun Tang. "A novel image steganography algorithm against statistical analysis." 2007 International Conference on Machine Learning and Cybernetics. Vol. 7. IEEE, 2007.

[12]. Singh, Amritpal, and Harpal Singh. "An improved LSB based image steganography technique for RGB images." 2015 IEEE International Conference on electrical, computer and communication technologies (ICECCT). IEEE, 2015.

[13]. Swain, Gandharba, and Saroj Kumar Lenka. "LSB array based image steganography technique by exploring the four least significant bits." *International Conference on Computing and Communication Systems*. Springer, Berlin, Heidelberg, 2011.
[14]. Subramanian, Nandhini, et al. "Image steganography: A review of the recent advances." *IEEE Access* (2021).