International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 06 | June - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Efficient Data Hiding System Using Image Steganography

Vempati Sushma -sushmavempati2002@gmail.com,

Modugu Sri Lakshmi- srilakshmimdg@gmail.com,

Aliya Fatima hassanaliya1923@gmail.com,

Unnati Khanapurkar unnati.khanapurkar@gmail.com

ABSTRACT:

Image steganography is the art of concealing secret data within an image so that hackers cannot detect the information within the stego images. This is a useful method to protect sensitive information. In this paper, we focus on two techniques for hiding information in images. Firstly, we analyze the Least Significant Bit (LSB) method for storing information bits. However, this method is well-known, and attackers can easily reveal the information, making image steganography unsecured. Secondly, we propose to use R-Colour Channel encoding with the RSA algorithm to provide extra protection to information. Our approach uses a red color channel to hide information bits and the following bits for RGB pixel values of the original image. This project aims to present the performance analysis of the two most popular algorithms, LSB and RSA, along with image steganography.

KEYWORDS: Steganography, Least Significant Bit (LSB), RSA

INTRODUCTION :-

In image steganography, data is buried in images with a very high level of accuracy in such a way that only subtle changes to the image are made visible. The method is designed in a way so that the odd-looking data can never be perceived by those who don't explore further.

On the other hand, cryptography aims at the reason of secreting messages which makes them irreducible to understanding to unintended somebody, and also guarantees a decryption power to the intended recipient by the means of encryption and decryption keys.Cryptography utilizes two keys, a public one which is known to both the sender and intended recipient, and a private one known by the intended recipient only, for the process of encryption and decryption respectively The cryptography principle, using mathematics algorithms and techniques, provides a way to encode the messages, making them understandable just by the authorized recipient. The application areas of cryptography are huge, which you can see in digital document signing, data privacy protection, secure web browsing, and others that allow you to provide secure transactions like secure credit card payments. In addition to that, digital files including text, pictures, videos, and songs can be encrypted as well by using steganography for better protection of information.

Steganography is the process during which information is hidden in specific digital files without changing the overall look of the file very much. For example, LSB steganography alters the least significant bits of pixels of the image. Hence, the data can be encoded without such noticeable changes in the image that can be seen by the naked eye. This method applies to audio and video media as well, allowing the hidden data is still undetected. This steganography also includes the data weighed into file headers, network packets, and partitions on hard drives. These techniques provide for several layers of protection variation and the technical complexity in their detection, so they are valuable tools in information protection.

Steganography is of different types:
1. Text steganography
2. Image steganography
3. Audio steganography
4. Video steganography

LITERATURE REVIEW:-

[1]In this paper, the author proposed a different approach for hiding information in the image. Since the popular LSB technique is vulnerable to different attacks, he leveraged cryptography to overcome the drawbacks of LSB by combining LSB with the RSA encryption algorithm along with R-Color Channel encoding. With his method, he improved the PSNR values by 3%.

[2] Shahid Rahman in his paper discusses different approaches, that would focus on strengthening the scope of using the Least Significant Bit (LSB) substitutions for the improvement of steganography. This paper suggests a new algorithm utilizing value difference as the base to import security and reliability without getting the perceptible capacity of the device. Experiments display that the proposed method outperforms existing methods with the PSNR score and capacity of hidden data both being better than the rest, producing better image quality upon embedding the secret information. Moreover, the study has shown that PSNR 5.561 approximations have been enhanced when adding variable quantities of data into images of similar sizes and also different types of images namely (RGB, grayscale, texture, and aerial). Finally, the study is a push factoring image steganography algorithms that incorporate practicality and great effectiveness in the real world.

[3] In this paper, the author illustrates different methods that are used for hiding information in a cover image. It talks about the LSB (Least Significant Bit) method which is built on the idea of altering the values of each bit by randomly inverting them for, more specifically, improving the PSNR (Peak Signal to Noise Ratio). Another method, Pixel Value Differencing, is employed where an image is split into blocks, and the absolute difference values of the adjacent pixels are used as a hiding medium. This yields an increased number of hidden data,especially along the edges. Along with the intermittent activation of lights, the paragraph proposes using randomization based on the sensitivity of different people to the RGB colors as another technique to ensure better concealment.

[4] The paper discusses three categories of image steganography methods: namely, conventional, CNN-based, and GAN-based architectures. Algorithms used by the contemporary methods do not apply to machine learning or deep learning, while the latter technique is based on the LSB approach. Convolutional neural networks (CNN) based schemes generate steganographic messages by exploiting the power of CNN layers, while GAN-based techniques apply various GAN variants. The paper presented herein also introduces steganography and steganalysis CNN-effort or GAN-empowered architecture wherein inputs are the cipher image and the secret information. The block of steganography produces the stego image furthermore steganalysis model detects and possibly exhibits the secret information. Textual data with or without images areready to be employed as secret media for conveying more information into certain categories, which can be reached simply by addressing the nature of secret media as well as the technique. It is indeed a proven fact that text is the most prevalent type of secret data and GAN-based techniques are favored for data hiding in texts.

[5] This paper describes in detail, a new method for data encryption based on stego-image by using. An LSB least significant bit method (LSB matching) should be modified to make it more accurate. The EC capacity, in addition to image quality. Primarily to start with, each elementary pixel is then used to generate four new corresponding pixels. The embedded intelligence is shielded into each of the four output base-level pixels.Then the pixels are redone in the quality of the fake image was upgraded. There are the ones containing steganography. Produced when the four pixels are recalibrated; thus, the color will be generated. A stego-image is one unit that would hide one bit for every one bit.pixel. Those stego-images are measured with the average highest ratio of peak signal-to-noise ratios (PSNR) at 36.06.A picture of the sound sources is shown in figure, 37.88 dB, 39.60 dB, and 41.00 dB, respectively.Furthermore, the proposed

method successfully withstands against RS-steganalysis.

[6] This proposal is written to form multiple links representing the presence of data on certain channels and communication networks. The stego method is not reliant on the encryption as it progresses the level of protection.even though key management is still required on a separate key, effort for key management is lower.By this, it means that the size of the secret data which required to be the determining factor.Parameter of Search Engine Optimization indicator channel which wanted to connect with the safety.randomness. Through our analysis, it is argued that our proposed technique is more effective than the other. security measures and other parameters such as service provision compared to the other two security system providers. similar work. Shown is the pixel indicator technique as suggested, which highlights the locations where performance improvement is needed. Those experiments with hiding the message in RGB pictures became so impressive.

[7] A paper is on Generative Adversarial Networks (GANs) in steganography, the discipline of confidential information concealing innocent data. The Chapter then provides the basic things we need to know about steganography and GANs where after that it will dive into how GANs are used in steganography that is cover modification, cover selection, and cover synthesis. The cover synthesis category is also a secondary subtype based on the degree of the original picture. The steganalysis examines the features of GAN-enabled cover creation and sets up gauges for the assessment of GAN-based steganography. It outlines the paper in a systematic manner in which each section will delve into steganography traditional techniques, with special emphasis on GAN techniques for steganalysis and the generally accepted guidelines for testing the steganalysis algorithms. In general, the article is an exhaustive overview of the involvement of GANs in procedural introspection that covers both the theoretical area and the practical aspects.

[8] The paper explores various techniques used for securing data during communication: encryption, steganography, and watermarking.Cryptography: Represent embodiment of the transformation of data into an unreadable form using encryption techniques, and employing a symmetric key or public key. Of course, it is an obvious fact of life that of data, scary or not.Steganography: Conceals secret data within the non-secret data streams of plain text but preserves its structure intact. It creates a new tool for crypto dictate and implements the identity factor below cryptography. Especially this tool is very valuable in exposition.Watermarking: Enforces the digital signatures of multimedia files into data to prevent unauthorized manipulation and copyright violation while still ensuring the integrity of the content over obtrusiveness. More importantly, this technique increases the ability to track down the source of any media files that might be duplicated.

[9] The papers start by introducing steganography as a technique used to veil messages within digital formats of media such as images, video, and audio presented without any trace of indication to observers. It categorizes steganography into three main types: text steganography, image steganography, and audio/video steganography, with the latter two being relatively new developments in today's digital age. However, the most popular form of steganography is the practice of embedding messages in images. The passages are crisp on the use of the Least Significant Bit (LSB) algorithm of encoding information in the background. Besides, the passage goes further to show that by including cryptography and steganography simultaneously, the security and privacy of communication are advanced. It describes these five components of information security: confidentiality, authentication, integrity, nonrepudiation, and access control working with availability for the whole. Generally, this passage illustrates the interplay relationship between steganography and cryptography for secure communication in the overall total.

[10] This paper tells the crucial role of data security in digital communication, especially through the internet era, and introduces steganography as one of the weapons to ensure the secrecy of information. It suggests an image steganography technique in the spatial domain that uses LSB substitution and is performed with the help of a PRNG for findings of data into the cover images it also differentiates steganography from cryptography in terms of making the message unreadable versus concealing the

message. The passage explains the prevalence of digital images on the internet, making image steganography a popular area of research.Two main methods for image steganography are outlined: these two methods are spatial/domain and frequency/transform domain techniques, where the most elaborate algorithm of these techniques is lattice substitution from the spatial/domain. Within the statement, spatial domain techniques are specified and the trade-off between message size and changes in the image original is articulated. The new is suggested as robust. Therefore, a large amount of information can be hidden and compared to similar methods PRNG, or hash functions. Eventually, the passage is going to cover the literature overview, implementation steps, and the evaluation of the performance, during the following sections of the paper.

REFERENCES:-

[1] Data Hiding using Image steganography, Dr Mayank Srivastava, Pratibha Dixit, Shikha Srivastava, 2023 6th International Conference on Information Systems and Computer Networks (ISCON), DOI: 10.1109/ISCON57294.2023.10112069

[2]A novel steganography technique for digital images using the LSB substitution method,Shahid Rahman,Jammal Uddin IEEE,2022 1Department of Computer Science, Qurtuba University of Science and Information Technology, Dera Ismail Khan 29050, Pakistan DOI:10.1109/ACCESS.2022.3224745

[3]Analysis of image steganography techniques for different image formats, Lalit Kumar Gupta, Aniket Singh, Abhishek Kushwaha, and Ashish Vishwakarma 2021,Dept. of Computer Science Engineering, Institute of Engineering & Technology, Bundelkhand University, Jhansi, Uttar Pradesh,India,DOI:10.1109/ICAECT49130.2021.9392492

[4]Image steganography: A review of the recent advances, NANDHINI SUBRAMANIAN 1, OMAR ELHARROUSS1,SOMAYA AL-MAADEED 1, ANDAHMED BOURIDANE 2, (Department of Computer Science and Engineering, Qatar University, Doha, Qatar 2Department of Computer and Information Sciences, Northumbria University, Newcastle upon Tyne NE1 8ST, U.K., 2021, DOI:10.1109/ACCESS.2021.3053998

[5] A Novel Multi Stego-image based Data Hiding Method for Gray Scale Image, Aditya Kumar Sahu, Gandharba Swain, 2Department of Computer Science and Engineering, KoneruLakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India 1 Department of Computer Science and Engineering, GMRIT, Rajam, Andhra Pradesh, India, 2014, ISSN: 0128-7680/e-ISSN: 2231-8526