IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 6, June 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206100 |

Image Encryption Using Steganography:Survey

D D Shrivastava, Chandra Prakash Bhargava, Dr Deepak Gupta

Assistant Professor, Department of Information Technology, Institute of Technology and Management, Gwalior, India

Assistant Professor, Department of Computer Science and Engineering, Institute of Technology and Management, Gwalior, India

Associate Professor, Department of Computer Science and Engineering, Institute of Technology and Management, Gwalior, India

ABSTRACT: This research paper examines various techniques in the field of Steganography for encrypting information. Steganography refers to a method of concealing data within an image. The focus of this paper is to delve into the fundamentals of Steganography, including its definition and associated terms. Additionally, the paper explores different types of Steganography methods, namely image, audio, video, and text Steganography, which are employed to hide information within digital carriers. In image-based Steganography systems, two crucial factors are considered: the quality of the resulting hidden image (stego image) and the capacity of the original image (cover image). By evaluating existing Steganalysis techniques, this paper enables researchers to enhance Steganography techniques, thereby increasing metrics such as Mean Square Error (MSE), Bit Error Rate (BER), and Peak Signal-to-Noise Ratio (PSNR).

KEYWORDS*:* Steganography, encrypting information, conceal, data, image, mage-audio-video-text Steganography, MSE, BER and PSNR

I. INTRODUCTION

Introduction to Network Security:

Network security encompasses a range of tools aimed at safeguarding data and thwarting unauthorized access by hackers. In the present landscape, the term "Network Security" can be misleading, as nearly all businesses, government entities, and educational institutions possess interconnected networks. This interconnected network of networks is commonly referred to as the Internet, leading to the term "Internet Security" being used interchangeably.

Introduction to Steganography and Cryptography:

With the rise of the internet, ensuring the security of information has become a vital aspect of Information Technology and Communication. In order to protect sensitive data, two fundamental techniques have emerged: cryptography and steganography. Cryptography involves encoding information to ensure its confidentiality, while steganography focuses on hiding information within other entities to maintain its secrecy. These techniques play significant roles in safeguarding data in diverse digital contexts.

Steganography:

Steganography is a technique that goes beyond traditional encryption methods by concealing messages within other objects, allowing them to evade detection. It does not directly encrypt the message but rather hides it within another medium. The term "steganography" derives from the Greek words "Steganos," meaning "covered," and "Graphy," meaning "writing." In this process, innocent files, such as text, images, or audio, serve as cover mediums. Once the secret message is embedded, it becomes part of the stego medium, remaining concealed within it.

Cryptography:

Cryptography is a method of encoding information in such a way that it remains unreadable to anyone except the individual possessing the corresponding key. The term "cryptography" is derived from the Greek words "Crypto," meaning "secret," and "Graphy," meaning "writing."

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206100 |

Need for Steganography and Cryptography:

Both steganography and cryptography serve essential roles in ensuring secure communication. Encryption through cryptography enables the transmission of information in a secure manner, requiring a key for decryption. While encryption protects data from being removed, it is susceptible to alterations that render it unreadable for the intended recipient.In contrast, steganography enables concealed communication by embedding information within data, making it more difficult to detect. The embedded data remains private until an attacker finds a way to identify it, as it requires significant alterations to the host data. Thus, the combined use of steganography and cryptography enhances the privacy and security of communication.

II. REVIEW OF LITERATURE

Different techniques are available to ensure secure communication in today's digital age. With the widespread use of Internet-based applications, there is a growing need to maintain the confidentiality of communication. Cryptography and steganography are employed to address this requirement. This research paper explores various digital steganographic techniques that can embed secret information within images without being discernible to the human eye. The effectiveness of these techniques is evaluated through a comparative analysis, utilizing metrics such as Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). Over the past decade, numerous steganographic techniques have been developed for images, both in the spatial and frequency domains.

LSB Substitution Method:
The LSB substitution method is utilized when concealing information within images. It involves
replacing the 8th bit of each byte in the carrier file with a bit of the secret information. This technique is straightforward and easy to implement.

Optimum Pixel Adjustment Procedure:
To minimize the distortions caused by the LSB substitution method, the Optimum Pixel Adjustment Procedure (OPAP) is employed. After embedding the secret data, pixel values are adjusted using the OPAP technique. This adjustment enhances the quality of the resulting stego image without affecting the concealed information.

Inverted Pattern Approach (IP):
The Inverted Pattern Approach (IP) employs a preprocessing step for the secret message prior to embedding. This approach determines whether each section of the secret images should be inverted or left unchanged. Additionally, bits are used to record the transformation, which can serve as a secret key or additional data to be re-embedded at a later stage.

Relative Entropy-based IP Method:
The IP method utilizing relative entropy employs relative entropy calculations instead of mean square error computations. This alternative approach quantifies the difference between the inverted pattern technique and the original data.

Hiding Streams of 1s and 0s (Proposed Method):
This novel steganographic technique diverges from the conventional approach by utilizing streams of alternating 1s and 0s for hiding data. The hidden information is converted into binary form, and the occurrences of 1s and 0s are calculated and distributed across the pixels of the cover image. The placement follows a pattern where odd columns hold the occurrences of 1s, and even columns hold the occurrences of 0s. This method offers several advantages, including simplicity of implementation, large embedding capacity, and a smaller key size.

Pixels Value Differencing (PVD):
In the Pixels Value Differencing (PVD) method, the focus is on maintaining a high-quality stego image rather than maximizing the capacity for concealed information. This technique considers the differences between adjacent pixels, with greater differences in edge areas and smaller differences in smooth areas.

Mod-based Hiding Method (Proposed Method):
The proposed mod-based method involves hiding data by subtracting the remainder obtained from dividing the pixel's gray value by 10. This approach provides a high embedding capacity while retaining image quality. The data is hidden based on the differences between adjacent pixels, and extraction requires the presence of a key.

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206100 |

MOD10-based Hiding Method (Proposed Method):
In this technique, the data is hidden within the remainder obtained by dividing the pixel's gray value by 10. A key is utilized to determine whether the hidden data corresponds to the remainder or 10 minus the remainder. The inclusion of the key enhances the quality of the resulting stego image.

Discrete Cosine Transform (DCT):
In order to conceal information within images, various techniques are employed, including transform domain methods. One such technique is the Discrete Cosine Transform (DCT), which is utilized to hide messages in significant regions of the cover image. In this approach, the pixels of the image are divided into 8x8 blocks, and each block undergoes a DCT transformation. Each transformed block is then used to encode a single secret message bit.

Benefits:
This method exhibits robustness against various attacks, including compression and cropping, ensuring the integrity of the hidden information.
The resulting image maintains a high quality, although the embedding capacity is relatively low.
In the Image Encryption method, the Least Significant Bit (LSB) technique is employed to hide information within an image. This approach involves encrypting the information first and then embedding the encrypted data in the LSB position of the image. The process involves measuring the entropy and correlation values of both the stego image and the original image. If these values remain unchanged, the method is considered secure.

To implement this technique, vertical and horizontal blocks are created at the sender's end and mixed with the encrypted image before transmission to the receiver. Upon receiving the image, the receiver extracts the secret information and reconstructs the secret transformation table. Only the secret information is transferred, rather than the entire transformation table. The LSB technique is then overwritten by the randomly positioned binary representation of the hidden data within the encrypted image. Before and after the insertion process, the correlation and entropy values are expected to remain the same. This approach effectively reduces the risk of the encrypted image being detected, thereby enhancing the security level of the encrypted image.[2]
[2] A novel steganography method employs the Least Significant Bits (LSB) technique to conceal data within encrypted image data. The LSB positions of the encrypted image are overwritten with binary representation of the hidden data in a random manner. Experimental results demonstrate that the correlation and entropy values remain unchanged before and after the data incorporation. This method effectively suppresses the hidden data within the encrypted image, minimizing the risk of detection. The receiver can reconstruct the secret transformation table and reproduce the original image by extracting the secret information from the encrypted image.

[3] This topic covers security, capacity, and imperceptibility aspects. A hybrid data hiding scheme combining LSB techniques with the key-permutation method is employed. An optimal key permutation method is developed using a genetic algorithm for selecting the best key. The system is based on LSB substitutions, where a random key is generated and shared between the communicating parties. The secret data is embedded in the k least significant bits (LSBs) of the host image, where k is limited to a value below 3 to avoid excessive key permutations. Evaluating the Peak Signal-to-Noise Ratio (PSNR) for each substitution and selecting the substitution with the highest PSNR value yields optimal results. However, this approach is time-consuming and impractical. To address this, a genetic algorithm is employed, offering randomized search capabilities, superior image quality, increased message capacity, and enhanced system security.

[4] In this study, the Discrete Wavelengths Transform (DWT) is utilized to conceal a secret message in the frequency domain through steganography. Specifically, the Haar-DWT is applied, involving horizontal and vertical operations. The technique scans pixels from left to right in the horizontal direction, performing addition and subtraction operations on neighboring pixels and accumulating the results. This approach effectively reduces extraneous data in the stego-image and optimizes the size of the key matrix.

[5] The paper introduces the spread spectrum image steganography (SSIS) technology as a part of modern digital steganography. It combines image renovation, error-control coding, and spread spectrum communication within the SSIS framework, with the system behavior being illustrated. The primary concept involves embedding hidden information within noise, along with a digital cover image. The SSIS technique can be extended to audio signals and color imagery. It enables the communication of hidden messages of significant length while preserving the original image size and

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206100 |

dynamic range, and the hidden messages can be enhanced using appropriate keys without requiring knowledge of the original image.

[5] Spread-Spectrum Image Steganography (SSIS) is a concealed communication method that hides and retrieves messages of considerable length within digital images while preserving their original size and dynamic range. This approach allows for the enhancement of hidden messages using appropriate keys, without requiring knowledge of the original image. The messages can be in various formats, including text, imagery, or other digital signals.

[6] A novel steganography algorithm is proposed, utilizing bitmap images to hide data. The algorithm consists of two stages: the development of a steganography algorithm for data hiding, and the creation of a decryption algorithm for retrieving the hidden data from the stego-image. This method ensures privacy and accuracy of the concealed data, maintaining the integrity of the original image.

[7] An efficient steganography technique is presented based on Hamming codes. The embedding and retrieval algorithms have similar computational rates, and the method employs a product code of two Hamming codes to improve the embedding rate.

[8] The paper investigates two different approaches: blind watermarking and steganography with perfect security, which aims to minimize the relative entropy between stego data and cover data. The performance of the schemes is compared in terms of embedding distortion, rate, and security. The design of the information embedding process ensures that the embedded information remains intact during subsequent processing, making it suitable for steganography.

[9] Steganography is the art of concealing messages within multimedia data. A study focuses on reducing visual and numerical differences between the cover data and stego-image while increasing the payload capacity. The algorithm involves converting a grayscale image into binary codes and using a chaotic sequence generated by the Henon map. The secret message is XORed with the LSB of selected pixels in the cover image. This algorithm provides security and confidentiality for the hidden message.

[10] The authors discuss steganography and its relationship with cryptography and traffic security. They propose an information-theoretic approach for achieving ideal confidentiality. Various approaches, including encrypted copyright characters and consecutive numbers in digital audio or video, are examined. The paper also addresses attacks on information hiding formats and the challenges in establishing a common theory for information hiding systems.

[11] Mohammed A.F. Al Husain introduces a unique steganography method that maps English letters and special characters to image pixels.

[12] Ran-Zan Wang and Yeh-shun Chen explore the use of two-way block matching for image steganography.

[13] The paper describes a dual-layered embedding process for plus-minus steganography using binary covering codes and wet paper codes. The messages are hidden in the LSB plane and the second LSB plane, respectively.

[14] It is discovered that embedding unusual information modifies the statistical properties of natural images. However, by avoiding the modification of certain image features, the problem can be addressed.

[15] A steganographic approach based on Hamming codes is proposed in this study.

[16] The authors present a method for secure communication using both cryptography and steganography techniques. They use steganography with images as the carrier and encrypt the confidential information using their own substitution cipher. The resulting image is then transmitted to the receiver, who performs the reverse operation to retrieve the secret information.

[18] The paper proposes the combination of steganography and cryptography techniques for secure communication. The undisclosed message is encrypted using the twelve square substitution cipher algorithm and embedded in the carrier image at specific bit locations. The receiver recovers the cipher text and decrypts it using the same algorithm to obtain the secret message. The approach ensures security as the embedding locations vary in all pixels of the carrier image.

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206100 |

III. RESEARCH SCOPE

Although the Least Significant Bit (LSB) technique is straightforward, it has a drawback of causing noticeable distortion when more than three bits are embedded per pixel. In order to mitigate this distortion, various adaptive steganography methods have been proposed [1]. Human perception is less sensitive to subtle changes in edge areas of a pixel but more sensitive to alterations in the size of smooth areas [1].

The use of image encryption approaches results in a lower payload capacity [2]. When the key size is large, it requires significant computational time [3]. To increase the payload capacity, key compression can be employed [4]. This method has the potential to be extended to color imagery and audio signals [5]. Specifically, it utilizes only bitmap (BMP) images for data hiding [6]. The system's security can be enhanced by incorporating the extension of HPDM (Histogram Preserving Data Mapping) [7]. Chaos systems are highly sensitive [8] and can be expanded to include the hiding of secret images in cover images, as well as in audio and video carrier files [9].

However, a disadvantage of this approach is that Table 1 and Table 2 are divided into alphabets where the letter 'q' is missing, and digits are not included. In the future, it is possible to extend this approach to hiding secret images within cover images, as well as in audio and video carrier files [16]. Another method described in reference [17] utilizes six square substitution ciphers, which include only lowercase alphabets.
A steganography method utilizing twelve square substitution ciphers has been proposed. This method includes both alphabets and digits, although it lacks the alphabet 'q' and the special character 'space' [18].

IV. CONCLUSION

Over the past few years, steganography has emerged as an intriguing and relevant topic, particularly when it comes to hiding information within image cover media. This paper aims to offer a comprehensive understanding of steganography by providing an extensive overview of its concepts and principles. It also introduces several techniques that can be employed to effectively embed data within images.

These techniques serve multiple purposes. First and foremost, they enable the detection of stego images, which are images that have concealed data within them. By employing these techniques, it becomes possible to identify and analyze the presence of hidden information, contributing to the field of image security.

Furthermore, these techniques are particularly advantageous for embedding data in complex areas of an image. Complex areas refer to regions with intricate patterns, diverse colors, or detailed textures. Embedding data in such areas poses challenges due to the need to maintain the visual quality and integrity of the image while concealing the information. The techniques discussed in the paper offer solutions to effectively handle these complexities, ensuring that the hidden data remains secure and inconspicuous.

To evaluate the effectiveness of the employed techniques, the paper suggests utilizing quantitative steganalytic techniques. These methods involve analyzing various statistical and mathematical properties of the image to determine the embedding rate—the amount of data that can be successfully concealed within the image. By employing quantitative steganalytic techniques, researchers and practitioners can assess the efficiency and reliability of the chosen steganographic methods.

In summary, this paper serves as a comprehensive guide to steganography, covering fundamental concepts and introducing practical techniques for data embedding. It highlights the importance of detecting stego images, addresses the challenges associated with embedding data in complex image areas, and emphasizes the significance of quantitative steganalytic techniques in assessing embedding rates.

REFERENCES

1. R. Amirtharajan, R. Akila and P. Deepika Chowdavarapu: A Comparative Analysis of Image Steganography, IJCA, Vol 2, (2010), 975-8887
2. Aman Jantan and Mohammad Ali Bani Younes: A New Steganography Approach for Image Encryption Exchange by using the LSB insertion, International Journal of Computer Science and Network Security, Vol 8 (2008), 247-254.
3. M. Mhamed, M. Bamatraf and Fadwa Al-afari: Data Hiding by LSB Substitution Using Genetic Optimal Key-Permutation, International Arab Journal of e-Technology, Vol. 2 No. 1, 2011.

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206100 |

4. Po Yuch Chen and Hung Ju Lin: A DWT Based Approach for Image Steganography, International journal of AppliedScience and Engineering, Vol.4, (2006), 275-290
5. Charles G. Boncelet and Lisa M. Marvel: Spread Spectrum Image Steganography, IEEE Transactions on Image Processing, Vol. 8, (1999),1075-1083.
6. Rosziati Ibrahim and Teoh Suk Kuan: Steganography Algorithm to Hide Secret Message inside an Image, ComputerTechnology and Application Vol. 2, 102-108.
7. H. Rifa-Pous and J. Rifa: Product Perfect Codes and Steganography, Digital Signal Processing, Vol.19, (2009), 764-769.
8. Joachim J. Eggers, R.Bauml and Bernd Girod: A Communications Approach to image steganography, Proc. of SPIE Volume 4675, San Jose, Ca, 2002,1-12.
9. Bhavana. S and K. L. Sudha: Text Steganography using LSB Insertion Method along with Chaos Theory,
10. ISRO,E.33011/74/2011-V
11. Ross J. Anderson and Fabian A.P. Petitcolas: On The Limits of steganography, IEEE Journal of selected Areas in communication, Vol.16, No.4, 1998, pp. 474-481.
12. Mohammed A.F Al-Husainy: Image Steganography by mapping Pixels to letters, Journal of Computer science, Vol.5, No.1, 2009, pp. 33-38.
13. Ran-Zan Wang and Yeh-Shun Chen, ―High Payload Image Steganography Using Two-Way Block Matching‖, IEEE
14. Signal Processing letters, Vol. 13, No.3, 2006, pp.161-164
15. Weiming Zhang, Xinpeng Zhang and Shuozhong Wang, ―A Double layered Plus-Minus One data Embedding Scheme‖, IEEE Signal Processing Letters, Vol. 14, No.11, 2007. pp. 848-851.
16. Alvaro Martin, Guillermo Sapiro and Gadiel Seroussi, ―Is Steganography Natural‖, IEEE Transactions on Image
17. processing, Vol. 14, No. 12, 2005. pp. 2040-2050.
18. H. Rifa-Pous and J. Rifa, ―Product Perfect Codes and Steganography‖, Digital Signal Processing, Vol.19, 2009, pp.764-769.
19. Gandharba Swain, Saroj Kumar Lenka: A Technique for Secure Communication using Message Dependent Steganography, Special issue of IJCCT, Vol. 2, No. 12,2010.
20. Gandharba Swain, Saroj Kumar Lenka: Better Steganography using the Six Square Cipher Algorithm, (ICAET-2010), Chennai, India, 2010, 334-338.
21. Gandharba Swain, Saroj Kumar Lenka: Steganography using the Twelve Square Substitution Cipher and Index Variable , IEEE transactions on Image Processing, 2011, 84-88.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details