Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Cyber Sentinel: A Combined Steganographic and Encryption Framework for Enhanced Data Privacy

Praneeta Sudam Ahire[1], Dr. Puja Padiya[2], Dr. Amarsinh Vidhate[3]

[1]Research Student, Department of Computer Engineering Ramrao Adik Institute of Technology, D. Y. Patil Deemed to be University,Nerul,Navi Mumbai 400706.
[2]Assistant Professor, Department of Computer Engineering Ramrao Adik Institute of Technology, D. Y. Patil Deemed to be University,Nerul,Navi Mumbai 400706.
[3]Professor, Department of Computer Engineering Ramrao Adik Institute of Technology, D. Y. Patil Deemed to be University,Nerul,Navi Mumbai 400706.
Email: ahirepraneeta19@gmail.com

In contemporary times, the transmission of information through insecure channels poses a significant risk due to the omnipresence of potential online intruders. To mitigate this concern, the conventional solution involves the implementation of encryption for safeguarding data. This study proposes an innovative strategy by integrating both steganography and cryptography to achieve dual-layered data encryption. The presented model leverages sophisticated artificial intelligence to categorize images into sensible, nonsensical, and suspicious classifications. By employing image saturation and segmentation techniques, concealed data can be unveiled. The model modifies the least significant bit of each pixel, incorporating covert data to generate a securely encrypted image. Adhering to the least significant bit (LSB) model and employing symmetric-key encryption, the resultant image maintains an indistinguishable appearance to an unencrypted steganographic photograph, both to the human observer and a computer lacking a stego-image for comparison. Importantly, the encrypted data remains impervious to decryption, even when subjected to image saturation or data extraction methods. This methodology augments cybersecurity, particularly in the realm of the Internet of Things (IoT), by furnishing a secure and inconspicuous means of data transmission.

Keywords: Cyber security, IoT security, steganography, cryptography, encryption, LSB, AES.

1. Introduction

In recent times, the increasing frequency of online attacks and data breaches has heightened the importance of cyber security. To address this ongoing challenge, researchers have developed various methodologies to protect data in the digital realm, with steganography and encryption emerging as key components. The security of digital data has been a critical concern since the inception of the Internet, constituting an essential aspect of communication and information technology. Cryptography primarily focuses on maintaining the confidentiality of communications, employing diverse techniques for data encryption and decryption. However, there are situations where ensuring the concealment of a message becomes crucial, a requirement fulfilled by steganography. Steganography involves the covert embedding of information within other data to obscure the occurrence of communication. In this context, digital photographs,

given their widespread use on the Internet, are commonly chosen as carrier files, establishing image steganography as a significant tool for enhancing information security.

Image steganography proves invaluable for secure information transfer, preserving data integrity over time, and ensuring compatibility across diverse platforms and devices. Beyond practical applications, it serves as a valuable resource for researchers in cryptography and information security, contributing insights into the capabilities and limitations of digital security systems.

Despite the advantages of steganography, it is not infallible. Consequently, the combination of steganography and cryptography emerges as a potent strategy to enhance overall effectiveness. This paper explores the utilization of images for steganography, distinguishing between overt and covert stenographic data, and addressing the challenges associated with suspicious images.

The proposed model integrates steganography and encryption, aiming to fortify data security in cyberspace. The approach involves implementing a technique for encryption for safeguarding crucial information and data and subsequently All information within that is encrypted an image using steganography. This combined technique provides a multifaceted solution, providing an additional layer of security, efficiency in storage and transmission, and versatility across various data types. Moreover, the proposed model is user-friendly and easily implementable, making it accessible even to inexperienced users. In summary, the improved model for information security in the internet, incorporating combined steganography and encryption techniques, gives an effective way to safeguard sensitive data transmitted via the internet online. By leveraging the Benefits of both methods, it offers heightened security, productivity, adaptability, and convenience a crucial asset in the evolving landscape of digital data security. The ensuing sections of this paper delve into a comprehensive an examination of the methods now in use to conceal secret communications, highlighting their pros and cons, and proposing a novel solution to address their limitations. The proposed approach integrates the Least Significant Bit method for putting data into images and then encrypting them using a symmetric key technique. The paper concludes with an evaluation of the proposed solution, presenting results and suggesting avenues for future research to extend and enhance the proposed approach.

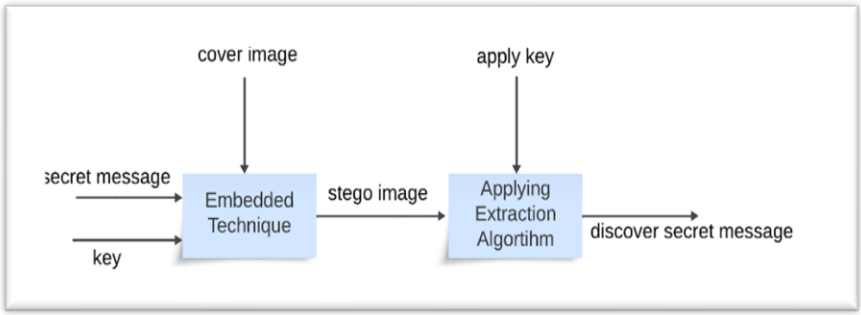

Fig. 1. Steganography technique

The field of image steganography represents a dynamic intersection between art and science, dedicated to concealing confidential information within digital images. As the prevalence of digital images continues to rise, both in communication and storage applications, the significance of image steganography as a pivotal tool for information security becomes increasingly pronounced. The imperative for employing image steganography arises from various considerations. Foremost among these is its ability to facilitate secure data transfer, especially for personal or confidential business data or sensitive information details. By seamlessly embedding this information within images, the technique adds an extra layer of safety, reducing the likelihood of detection by unauthorized individuals. This paper delves into the intricacies of image steganography and explores the integration of complementary encryption techniques, aiming to further fortify the security of information in the realm of digital communication and storage.

2. Related Work

Steganography involves concealing information within a cover picture or media to make it imperceptible to third parties. This paper reviews various stenographic techniques, counting Edge identification, RSA, LSB, DES, hashing, and chomped discovery, highlighting their strengths and weaknesses. The study proposes the use of the Least Significant Bit (LSB) steganography model containing an additional symmetric encryption layer as an effective and secure alternative Commonly used techniques, such as Bit detection, hashing, RSA, LSB, DES, and edge recognition exhibit drawbacks like complexity, low security, noise effects, slow computation, and conspicuous appearance. The symmetric encryption second layer of security in the LSB model addresses these issues, offering simplicity, efficiency, and heightened security. This approach can be implemented with various encryption algorithms, providing flexibility for different applications The paper emphasizes the LSB method's significance in picture steganography because of its straightforwardness, security, low effect on picture quality, and flexibility .The LSB method involves hiding information in the least significant bits of image pixels, making it difficult to detect or extract the message without the steganography technique and the original picture. Additionally, This procedure has minimal influence on the appearance of the image and can be used for many image types and sizes[1].

To enhance security further, the paper introduces a symmetric encryption model, ensuring that only a exceptional confidential key at the client end can decipher the information. The suggested model alters the last bit of each character in pixel values, creating an encrypted image that appears no suspect and trustworthy. The shift in pixel values is imperceptible to the natural eye, and a PC cannot remember it as a stenographic picture without a stego-picture for examination. The model maintains computational efficiency and avoids drawing attention to the stenographic and encrypted form of the image. An analysis of existing steganographic models reveals their limitations and vulnerabilities. The need for a double encryption model to address these issues becomes apparent[2].

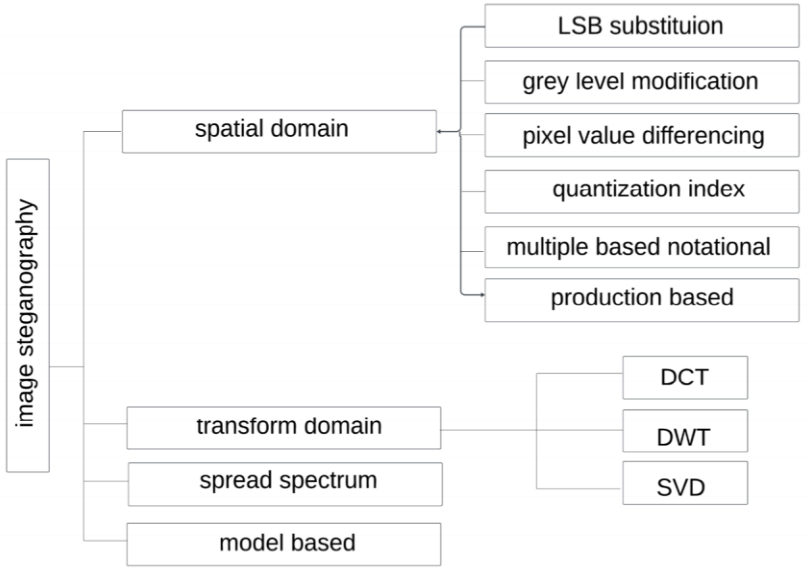

Fig. 2. Classification of Steganographic Techniques

2.1) Existing Overview:

This paper directs a deliberate survey of picture steganography draws near, obtaining articles from trustworthy data sets like IEEE Investigate, Web of Science (WOS), ACM, and Willey. The review covers the fundamental concepts, performance metrics, and these approaches' types. An broad comparison is made Of the current techniques to assess their individual benefits and drawbacks. Furthermore, the paper explores the potential of blockchain-based steganography techniques in improving the stego-medium. Recognizing the limitations of current image steganography methods, the paper also outlines several future research directions. The systematic review aims to provide guidance for researchers shaping the future trajectory of investigations in the realm of image steganography. This paper looks at how deep learning can be used in image steganography, categorizing techniques into traditional methods, CNN-based approaches, and GAN-based methods. It details methodologies, datasets, and experimental setups, providing a comprehensive table for reference. Despite showcasing the potential of deep learning, the paper acknowledges challenges like robustness and computational complexity. It aims to aid researchers by consolidating trends,

addressing challenges, and suggesting future directions, contributing to the understanding and innovation in secure data transmission through image steganography [3].

J. Qin et al. (2019): Surveys coverless image steganography, discussing techniques and challenges in this specific area. The first paper underscores the increasing significance of information security in the digital age, particularly concerning multimedia data. It introduces coverless image steganography, a departure from traditional methods, eliminating the need for a predefined cover image. Instead, it utilizes inherent image properties like pixel attributes, variety, surface, and significant level semantics to directly convey secret information. The primary aim is to thwart detection by steganalysis tools, significantly enhancing image security. The paper provides a comprehensive survey covering essential frameworks, feature extraction, and pre-processing, hash sequence creation and relationship mapping in coverless image steganography. It evaluates existing methods and outlines prospects for future research [4].

J. Kadhim et al. (2019): Presents a thorough investigation of image steganography, covering methods, assessments, and future research trends. The second paper delves into the critical aspect of securely storing and transmitting confidential information using digital image steganography. Recognizing the prevalence and popularity of digital images, the paper addresses the challenge of striking a between increased bit embedding, imperceptibility, security, and robustness rates in steganographic systems. It offers an extensive review of various image steganography types, highlighting recent contributions across multiple modalities. The paper covers general operations, requirements, aspects, types, and performance evaluations of image steganography. Additionally, it discusses performance analysis measures and strategies for selecting cover media based on different applications, providing insights into state-of-the-art steganalysis systems[5].

D. Hu et al. (2018): presents a cutting-edge technique for picture steganography that makes use of deep convolutional generative adversarial networks. (DCGANs). : The paper presents a steganography without embedding (SWE) approach, leveraging deep convolutional generative adversarial networks (DCGANs) to enhance image steganography security. This technique utilizes a noise vector to encode secret information, generating a carrier image without modifying its original content. The method demonstrates effective information extraction and robust resistance against advanced steganalysis algorithms. However, there are potential drawbacks, including the computational intensity during training and image generation, reliance on the performance of neural networks, and the need for additional validation across diverse scenarios. The analysis could benefit from a more explicit discussion of quantitative metrics and considerations regarding real-world scalability [6].

Khaldi (2020): Classifies steganographic techniques based on image format, providing a structured approach to understanding different methods .This study provides an all-encompassing categorization of steganographic methods tailored for digital images, coupled with a classification based on the particular image type in use. The observation emphasizes the absence of a one-size-fits-all method for all image formats, recognizing the unique features of each image type and the necessity for steganographic methods to conform to specific colorimetric representations [7]

The classification systematically delineates the diverse techniques applied in the domain of

digital image steganography. The paper has notable limitations, such as a lack of detailed discussion on the evaluation of steganographic methods, creating a gap in understanding their effectiveness. Additionally, there is insufficient exploration of the challenges associated with adapting techniques to diverse image types. The consideration for adaptability to emerging image technologies is also limited, overlooking potential advancements in the field. Furthermore, the discussion on practical implications and challenges in real-world implementation lacks depth. On a positive note, the paper presents valuable specifications, including a comprehensive classification system for steganographic methods. The recognition of colorimetric precision provides insight into aligning methods with specific representations. The systematic outline of various steganographic techniques in digital image steganography enhances clarity, offering a structured overview. Moreover, the acknowledgment of distinctive image characteristics contributes to a nuanced understanding, adding depth to the analysis [8].

S. Kang and H. Park (2021): Proposes a scenery categorization of steganographic algorithms using hierarchical CNN, emphasizing the role of convolutional neural networks: This paper proposes a novel hierarchical CNN structure for senary classification in image steganalysis, aiming to identify specific steganographic algorithms used in stego images. While current CNN-based methods excel in detecting stego images, they struggle with algorithm identification. The hierarchical CNN structure offers a stepwise approach, significantly improving classification accuracy in experiments compared to conventional methods [9].

Mishra and P. Bhanodiya (2015): Securing digital data transmission is vital in the current landscape, given concerns about potential intruders on unsecured channels. To address this, Cryptography and Steganography are employed, with Cryptography encrypting messages but facing the challenge of potential exposure. Steganography, on the other hand, conceals the very existence of communication. The paper advocates for a combined approach, leveraging the strengths of both techniques to enhance message security. Cryptography's limitation is the visibility of encrypted messages, a challenge addressed by Steganography's covert communication, allowing messages to be hidden within various media types. The paper underscores the versatility of Steganography and highlights the complementary roles of Cryptography and Steganography in preserving message confidentiality.Advanced Image Steganography Techniques [10].

Ahmad et al. (2021): Introduces an enhanced halftone-based secure visual cryptog-raphy scheme for color/binary images, combining security and improved visual quality The paper introduces an innovative Visual Cryptography (VC) scheme employing enhanced half toning for pictures in both binary and color. The process involves three stages: identification, encrypting, and unlocking, incorporating Cryptography with visuals (2, 2) and introducing fake shares to enhance security. However, certain limitations exist, including uncertainty about its resilience against advanced attacks, unexplored challenges in practical implementation, and insufficient details regarding usability, algorithm complexity, and comprehensive testing. Additional research is required to validate the scheme's effectiveness and its practical suitability in real-world applications [11].

W. S. Farhani and A. Dwiharzandis (2022): Talk about steganography on MPEG spatial audio object coding utilizing the least significant bit (LSB) approach. Although it proposes

an intriguing concept, the paper on steganography in MPEG spatial audio object coding utilizing the least significant bit (LSB) method has some noticeable drawbacks. The simplicity of the LSB method may make it susceptible to advanced steganalysis techniques, potentially compromising the covert nature of embedded information. Concerns are raised regarding the impact on perceptual audio quality due to manipulation of least significant bits, though this issue is not thoroughly addressed. The paper lacks a comprehensive examination of the technique's robustness against diverse attacks or vulnerabilities within the MPEG spatial audio object coding framework. Practical aspects, such as embedding and extraction speed, as well as computational overhead, are not extensively explored. A more detailed comparative analysis with alternative steganography methods specific to MPEG spatial audio object coding would enhance understanding of the proposed approach's efficacy. Despite these limitations, the paper provides valuable insights into LSB steganography in this unique context, laying the groundwork for future research to address and overcome these challenges [12]. In their 2012 work a steganography method originated with V. K. Sharma and V. Shrivastava that is specifically designed for hiding pictures inside other images. The method refines the traditional Least Significant Bit (LSB) replacement strategy, giving priority to reducing detection risks. Using this technology, information may be embedded into the front cover image by changing the least significant bits of pixel values. . The algorithm distinguishes itself by incorporating improvements in LSB substitution, aiming to enhance the efficacy of image hiding while minimizing However, it is crucial to acknowledge the inherent limitations of the algorithm. These constraints may encompass potential implications for image quality, constraints in data capacity for information concealment, and susceptibilities to specific types of attacks. Recognizing these limitations is essential for a comprehensive evaluation of the algorithm's practicality and its suitability for diverse applications [13].

A. M. Al-Shatnawi (2012): In 2012, A. M. Al-Shatnawi introduced an innovative image steganography technique with a primary focus on enhancing image quality. The paper likely includes a comprehensive review of various steganography methods. The objective of this method is to advance steganography by addressing the specific challenge of improving image quality while concealing information within images. This demonstrates a deliberate effort to minimize the visual impact of steganographic. Although the paper provides valuable insights into novel approaches to image steganography, it is crucial to consider potential limitations. These limitations may encompass factors such as computational complexity, constraints in data capacity, and vulnerabilities to specific types of attacks. Recognizing these limitations is essential for a thorough evaluation of the practical feasibility and potential challenges associated with implementing the introduced steganography method [14].

Jour and Verma, D. (2014): By applying a Discrete Cosine Transform (DCT) to the pixels, your suggested solution replaces the Least Significant Bit (LSB) in the transformed domain of the same picture with the Advanced Encryption Standard (AES) in the spatial domain of the carrier/cover image. Applying the XOR technique with the carrier image's pixel values to the AES-encrypted message adds another layer of security. This multi-layered strategy integrates steganography and cryptography to offer a more secure communication route. The method's strengths include the stealthy characteristics of steganography, the robust

encryption provided by AES, and the transformation of the image pixels for added security. The use of DCT and LSB replacement further contributes to the complexity of the algorithm However, it's important to acknowledge some limitations. One potential drawback is the computational overhead introduced by the combination of these techniques, which may impact real-time applications. Additionally, the method's security may still be vulnerable to advanced attacks or sophisticated steganalysis techniques. Regular updates and improvements may be necessary to address emerging threats and ensure long-term effectiveness [15].

3. Limitation of Existing System

Existing steganographic models often lack robustness against advanced AI systems and image saturation techniques. The proposed model aims to bridge this research gap. The model faces challenges such as vulnerability to adversarial attacks, efficient handling of large payloads, adaptation to evolving steganalysis methods, the need for comprehensive testing, effective management of computational resources, ensuring consistent performance across platforms, and addressing legal and ethical considerations. Continuous research and testing are crucial to enhance the model's robustness and practical effectiveness.

4. Proposed Work

The proposed work introduces a two-phase algorithm aimed at securing data in the digital space. In the first phase, the algorithm uses any image to hide secret information through steganography. The second phase involves applying encryption for added security. The user-friendly application presents two tabs, "encrypt" and "decrypt," allowing users to easily navigate through the process.

Users can choose an information file, an image file, and whether to save the image file while encryption is in effect when the program launches. Users can choose an image file and decide where to save the secret file if they select the "decrypt" option. The project mainly uses encryption and decryption techniques, which allow secret information to be extracted during decryption and sensitive data to be hidden within any picture file during encryption.

A. Encoding:

- Steganographic techniques are used during encoding to encode data in a picture, especially for BMP image files. The suggested encryption procedure entails: Extracting the ASCII value of each character and transforming it into an 8-bit binary.
- After binary transformation, one character is stored in the first eight RGB values while reading three pixels at a time. Contrasting binary data and RGB values, adjusting RGB values based on binary digits.
- The ninth value establishes if more pixels should be scanned. continuing until all data is encoded.

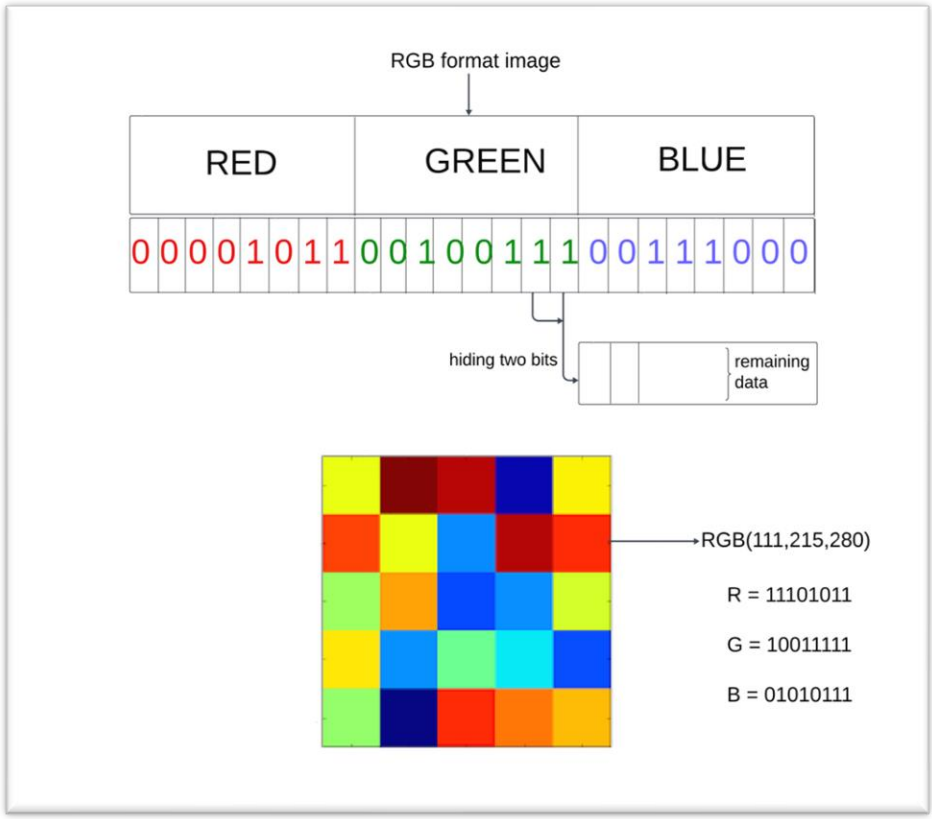

Fig. 3. Binary Distribution of RGB Data

B. Decoding:

The decoding process reverses the encoding steps:

- Three pixels at a time are read, and the first eight RGB values provide hidden information, while the ninth value indicates whether to move forward or not.
- Creating a binary string using the first eight numbers; the bit is set to 1 for odd values and 0 otherwise.
- Breaking the steganographic image into three pixels at a time if the ninth value is even, extracting hidden data.

LSB steganography is used in conjunction with encryption techniques to increase security. The secrecy of the concealed message can be assured using symmetric-key encryption, which uses the same key for both encryption and decryption. In order to achieve this, a safe random key needs to be created, the concealed message must be encrypted using a symmetric encryption algorithm like AES, and the encrypted message must be stored inside the image. The message can be decoded by the receiver utilizing the same key. Furthermore, parties can securely exchange symmetric keys by using public-key encryption. The symmetric key is scrambled by the public key and decoded by the private key. Through doing this, and

safeguard private data included in a photograph. Ensuring the security and secrecy of the concealed message requires careful control of keys and the selection of the appropriate encryption method.

5. Conclusion

In conclusion, we studied hiding information in image files through techniques like encryption and steganography. Our review of current steganographic software revealed that using basic encryption or steganography alone isn't foolproof for confidentiality. However, combining these methods enhances encryption. Unlike encrypted messages that can be detected if intercepted, steganography can hide a secret message without the interceptor knowing. We proposed a method using advanced AI algorithms to analyze steganographic data, making double encryption necessary for improved security. This approach ensures that hidden data remains unreadable to both humans and computers, even with saturation or segmentation techniques. In picture steganography, the Least Significant Bit (LSB) technique has emerged as a safe and convenient solution when combined with symmetric encryption. It offers excellent safety, little effect on image quality, works with different formats and sizes, and is simple to use. A lot of individuals use LSB since it is less complicated and more efficient than other methods. In the future, symmetric encryption optimization of the LSB approach may improve safety as well as effectiveness. Investigating its use in other fields, such video steganography, offers a fascinating avenue for investigation.

References

1. S. Kaur, S. Singh, M. Kaur, and H.-N. Lee, “A systematic review of computational image steganography approaches,” Archives of Computa- tional Methods in Engineering, pp. 1–23, 2022.
2. N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, “Image steganography: A review of the recent advances,” IEEE access, vol. 9, pp. 23409– 23423, 2021.
3. J. Qin, Y. Luo, X. Xiang, Y. Tan, and H. Huang, “Coverless image steganography: a survey,” IEEE Access, vol. 7, pp. 171372– 171394, 2019.
4. I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, “Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research,” Neurocomputing, vol. 335, pp. 299–326, 2019.
5. D. Hu, L. Wang, W. Jiang, S. Zheng, and B. Li, “A novel image steganography method via deep convolutional generative adversarial networks,” IEEE Access, vol. 6, pp. 38303–38314, 2018. [6] A. Khaldi, “Steganographic techniques classification according to image format,” International Annals of Science, vol. 8, no. 1, pp. 143– 149, 2020.
6. S. Kang and H. Park, “Hierarchical cnn-based senary classification of steganographic algorithms,” Journal of Korea Multimedia Society, vol. 24, no. 4, pp. 550–557, 2021. [8] R. Mishra and P. Bhanodiya, “A review on steganography and cryp- tography,” in 2015 International Conference on Advances in Computer Engineering and Applications, pp. 119–122, IEEE, 2015.
7. S. Ahmad, M. F. Hayat, M. A. Qureshi, S. Asef, and Y. Saleem, “Enhanced halftonebased secure and improved visual cryptography scheme for colour/binary images,” Multimedia Tools and Applications, vol. 80, no. 21-23, pp. 32071–32090, 2021.
8. W. S. Farhani and A. Dwiharzandis,

9. "Steganografi metode least sig- nificant bit (lsb) pada mpeg spatial audio object coding," Rang Teknik Journal, vol. 5, no. 2, pp. 364–368, 2022. [11] K. Lakhwani and K. Kumari, "Kvl algorithm: Improved security & psnr for hiding image in image using steganography," International Journal of Computational Engineering Research, vol. 3, no. 10, pp. 1–6, 2014.
10. V. K. Sharma and V. Shrivastava, "A steganography algorithm for hiding image in image by improved lsb substitution by minimize detection," Journal of Theoretical and Applied Information Technology, vol. 36, no. 1, pp. 1– 8, 2012.
11. A. M. Al-Shatnawi, "A new method in image steganography with improved image quality," Applied Mathematical Sciences, vol. 6, no. 79, pp. 3907–3915, 2012.
12. J. Kour and D. Verma, "Steganography techniques–a review paper," In- ternational Journal of Emerging Research in Management &Technology ISSN, pp. 2278–9359, 2014.
13. A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Enhancing steganography in digital images," in 2008 Canadian Conference on Computer and Robot Vision, pp. 326–332, IEEE, 2008.
14. L. Riley, J. Mandal, and D. Das, "Colour image steganography based on pixel value differencing in spatial domain," International Journal of Information Sciences and Techniques (IJIST) Vol, vol. 2, 2012.
15. R. Halder, S. Sengupta, S. Ghosh, and D. Kundu, "A secure image steganography based on rsa algorithm and hash-lsb technique," IOSR Journal of Computer Engineering (IOSR-JCE), vol. 18, no. 1, pp. 39– 43, 2016.
16. S. P. Bansod, V. M. Mane, and R. Ragha, "Modified bpcs steganography using hybrid cryptography for improving data embedding capacity," in 2012 International Conference on Communication, Information & Computing Technology (ICCICT), pp. 1–6, IEEE, 2012.
17. A. Priyadharshini, R. Umamaheswari, N. Jayapandian, and S. Priyananci, "Securing medical images using encryption and lsb steganography," in 2021 international conference on advances in electrical, computing, communication and sustainable technologies (ICAECT), pp. 1–5, IEEE, 2021.