Steganographic Key Embedding in AI-Generated Images

Agniva Bagchi[1, a)], Swapnaneel Banerjee[1, b)], Aniruddha Das [1, c)],

Sampurna Ghosal [1, d)] and Adrika Mondal [5, e)]

[1]*University of Engineering and Management, Kolkata , India*

Author Emails
[a)]agniva10270@gmail.com,
[b)]swapnaneel.banerjee23@gmail.com,
[c)]aniruddha.das@uem.edu.in,
[a)]sampurnaghosal2002@gmail.com,
[e)]adrikamondal.in@gmail.com

Abstract. Ensuring secure digital communication remains a paramount challenge in today's interconnected world. This research project delves into the realm of steganography, an ancient practice of concealing sensitive information within innocuous carriers. Specifically, it explores innovative techniques for embedding cryptographic keys within AI-generated images, capitalizing on their visual complexity to evade detection. By leveraging advanced encryption algorithms, and tailored embedding methodologies, the proposed solution aims to significantly enhance the embedding capacity while maintaining imperceptibility. This approach not only safeguards the very existence of covert communications but also fortifies their resilience against modern steganalysis techniques.

The fusion of steganography and artificial intelligence presents a multifaceted endeavour, encompassing data hiding, information security, image processing, and computational efficiency. The project commences with generating high-quality AI images using generative models. Subsequently, an intricate embedding algorithm is developed to seamlessly integrate cryptographic keys into the visual content, optimized for maximizing payload capacity while preserving image integrity.

Furthermore, the research incorporates advanced encryption techniques to ensure the confidentiality of embedded information, enhancing the efficiency of the covert communication channel. The proposed methodology is subjected to rigorous evaluation, assessing its performance across various metrics, including imperceptibility, embedding capacity, robustness against attacks, and computational complexity. The successful realization of this project holds profound implications for secure digital communications across critical domains, offering a potent tool to safeguard sensitive data exchanges. By pioneering novel steganographic techniques tailored for AI-generated multimedia, this research endeavours to push the boundaries of information security, fostering a more resilient and privacy-preserving digital ecosystem.

Keywords: steganography, cryptographic keys, AI-generated images, data hiding, information security, covert communication, embedding algorithm

I. INTRODUCTION

In the era of ubiquitous digital communication, ensuring the confidentiality and security of sensitive information has become a critical imperative. Conventional encryption techniques, while effective, may still leave digital transmissions vulnerable to detection and interception by malicious actors. This vulnerability has prompted the exploration of innovative approaches that not only encrypt data but also conceal its very existence within innocuous carriers, a practice known as steganography.

Steganography, derived from the Greek words "steganos" meaning covered and "graphein" meaning writing, is the ancient art and science of concealing messages within other media. Its origins can be traced back to ancient civilizations, where techniques such as invisible inks, microdots, and coded messages were employed to safeguard sensitive communications. In the modern digital landscape, steganography has evolved to leverage the complexities of multimedia data, such as images, audio, and video files, as carriers for hidden information.

This research project ventures into the realm of steganography, specifically focusing on the integration of cryptographic keys within AI-generated images. By leveraging the intricate visual characteristics of AI-generated imagery, we explore the potential to embed keys seamlessly into the visual content, capitalizing on the complexity of these images to evade detection by traditional steganalysis techniques.

The fusion of steganography and artificial intelligence presents a multifaceted challenge, encompassing aspects of data hiding, information security, and image processing. Our approach aims to develop innovative embedding algorithms tailored for AI-generated images, ensuring imperceptibility and payload capacity while maintaining the integrity of the cover medium.

Additionally, we investigate advanced encryption and compression techniques to enhance the security and efficiency of the embedded information, further fortifying the clandestine nature of the communication channel.

The following sections of this paper delve into the theoretical underpinnings, methodologies, and experimental results of our research, elucidating the potential applications and implications of this cutting-edge approach to secure digital communication

II. BACKGROUND

A. Medieval Intricacies:

Embarking on a journey through the annals of history, this literature survey navigates the captivating evolution of steganography, an age-old practice of concealing messages within the fabric of everyday life. From ancient civilizations to the digital age, the art of hidden communication has woven its intricate threads through the tapestry of human ingenuity and secrecy.

Our expedition commences amidst the whispers of antiquity, where civilizations such as ancient Egypt and Greece employed rudimentary steganographic techniques to safeguard sensitive information. From tattooed messages on shaved heads to invisible ink inscriptions, these early manifestations of steganography laid the groundwork for clandestine communication.

Venturing further into the medieval era, we encounter the enigmatic Codex Seraphinianus and the Voynich manuscript, cryptic tomes veiled in mystery and speculation. These medieval marvels exemplify the artful fusion of steganography and cryptology, tantalizing scholars with their inscrutable contents and cryptic symbols.

B. Digital Renaissance:

With the advent of the digital age, steganography transcended the physical confines of parchment and paper, venturing into the ethereal realms of binary code and digital imagery. From LSB-based hiding techniques to advanced algorithms leveraging the complexities of multimedia data, modern steganography has evolved into a sophisticated art form, challenging adversaries and encryption algorithms alike.

C. Conclusion:

As our journey through the annals of steganography draws to a close, we emerge enlightened by the rich tapestry of human ingenuity and secrecy that has defined this ancient art. From ancient civilizations to the digital frontier, the practice of hidden communication continues to captivate the imagination and intrigue of scholars and enthusiasts alike, reminding us that the quest for secrecy is as timeless as the human spirit itself.

III. PROPOSED SOLUTION

A. Methodology:

The project will involve the following steps:

1. *AI Image Generation:*

Use generative models (such as GANs) to create high-quality images.

2. Key Embedding:

Develop an algorithm to embed keys into the AI-generated images. Algorithm for embedding the key:

Key Conversion: Convert the stegano key(payload) into its ASCII representation.

Binary Conversion: Convert each ASCII character into its binary representation.

Pixel Modification:

- Divide the 8 bits of each binary digit into groups of 3.
- Iterate through the pixels of the image.
- For each pixel, check the corresponding group of 3 bits from the binary representation of the key.
- If the group is '000' and the value of the pixel's RGB component is odd, add one to make it even. Otherwise, leave it unchanged.
- If the group is '001' and the value of the pixel's RGB component is even, add one to make it odd. Otherwise, leave it unchanged.

Repeat this process for each group of 3 bits and each RGB component of the pixel.

Flag Embedding: Once all bits of the key have been processed, set the last RGB value of the image to 1 to indicate the end of the data embedding process. This serves as a flag to indicate where the data embedding ends.

Output Image: The modified image now contains the hidden data encoded within its RGB components, with the last RGB value serving as a flag to denote the end of the embedded data.

It's important to note that the decoding process will need to reverse this algorithm to retrieve the hidden information from the image. Additionally, thorough testing and validation should be conducted to ensure the effectiveness and robustness of the algorithm in concealing and retrieving data while maintaining image quality.

The keys will be hidden in such a way that they are undetectable to the human eye and traditional steganalysis methods.

3. Key Extraction:

Design a mechanism to extract the embedded keys from the images without causing noticeable alterations.

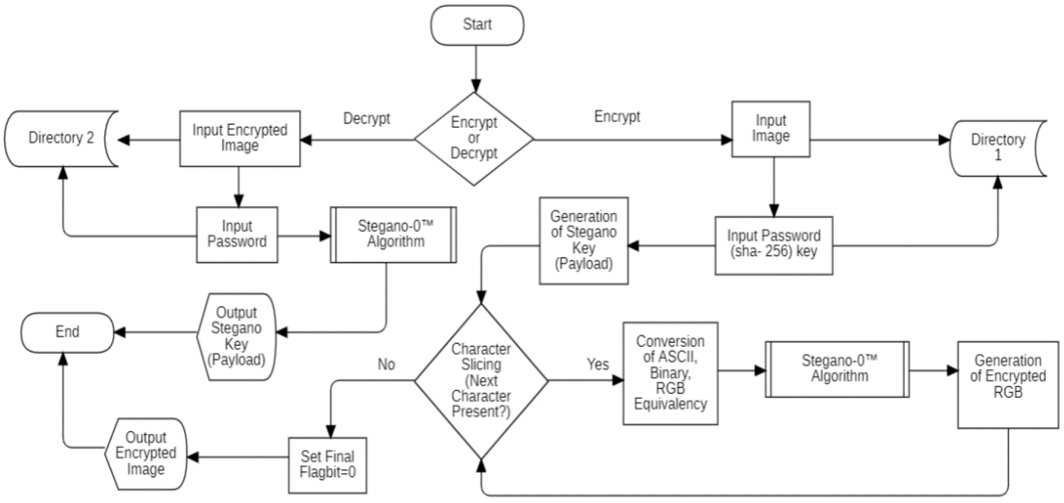
Start
Decrypt
Encrypt or Decrypt
Encrypt
Input Image
Directory 1
Input Encrypted Image
Directory 2
Input Password
Stegano-0™ Algorithm
Generation of Stegano Key (Payload)
Input Password (sha- 256) key
Output Stegano Key (Payload)
End
No
Character Slicing (Next Character Present?)
Yes
Conversion of ASCII, Binary, RGB Equivalency
Stegano-0™ Algorithm
Generation of Encrypted RGB
Set Final Flagbit=0
Output Encrypted Image

Fig1. Encryption and Decryption Flowchart

IV. EXPERIMENTAL SETUP AND ANALYSIS

Experimental Setup:

A. Accepting the Image:

Ensure the image includes images with different color distributions, complexities, and sizes to evaluate the algorithm's performance across different scenarios.

B. Implementation:

Develop an implementation of the steganographic algorithm described earlier. Use a programming language like Python and relevant libraries such as pycryptodomex.

C. Test Images and Keys:

Select the given image and the stegano key to be embedded. Ensure the keys cover a range of complexities and are representative of real-world scenarios.

D. Embedding Process:

Apply the steganographic algorithm to embed the secret keys into the selected images. Record the time taken for embedding and any errors encountered during the process.

E. Fidelity Measures:

Fidelity measures imply the measure type that utilized to compute the variation range between images after applying these measures and hiding the confidential message.

Mean Square Error (MSE)

The mean square error demonstrates the cumulative squared error (i.e., pixel variations) in two images, The MSE is computed as follows:

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}[c(i,j) - s(i,j)]^2$$

Where: m and n are the image dimensions and C(i,j) and S(i,j) are the cover image and pixels of stego image.

Peak Signal to Noise Ratio (PSNR)

The peak error can be measured by PSNR. A better image quality means higher PSNR

$$PSNR = 10\log_{10}\frac{R^2}{MSE}$$

R is the highest potential value of the pixel's densities

V. RESULT ANALYSIS

No. of Chars	PSNR (Image)					MSE (Image)				
	Amusement	Apple	Flower	House	Man	Amusement	Apple	Flower	House	Man
20	100.378003	97.729824	104.491205	100.207669	97.197369	0.000006	0.000011	0.000002	0.000006	0.000012
40	97.455442	95.665085	102.998225	98.794378	94.672573	0.000012	0.000018	0.000003	0.000009	0.000022
100	94.104344	93.750424	100.717022	95.844819	92.713874	0.000025	0.000027	0.000006	0.000017	0.000035
1000	84.922457	84.972205	90.801903	84.166240	83.244778	0.000209	0.000207	0.000054	0.000249	0.000308
5000	78.537906	78.414582	84.241300	77.715686	76.830006	0.000911	0.000937	0.000245	0.001100	0.001349
10000	77.140121	77.352962	83.106154	76.945099	75.802211	0.001256	0.001196	0.000318	0.001314	0.001709

Table 1. PSNR and MSE Values for Different Characters

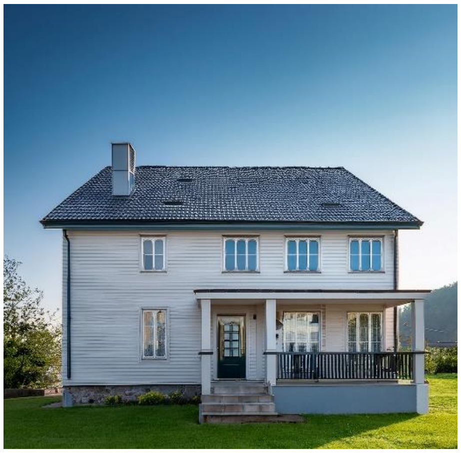

Fig 2. Original Image

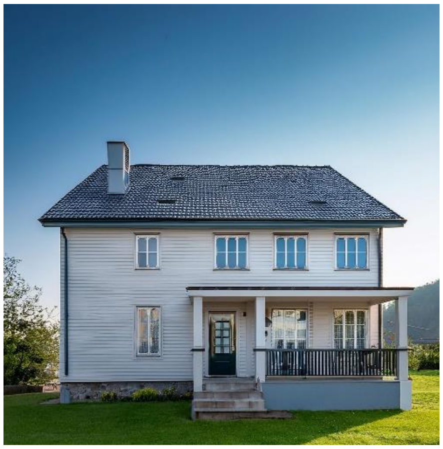

Fig 3. Embedded Image

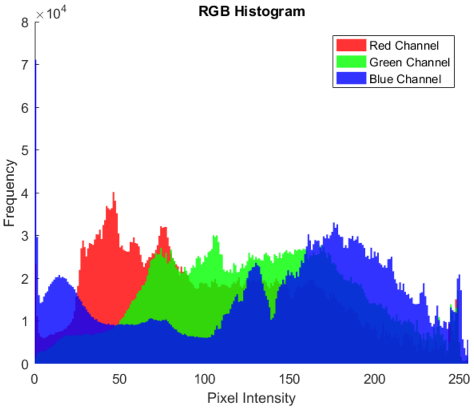

Fig 4. RGB Histogram of Original Image

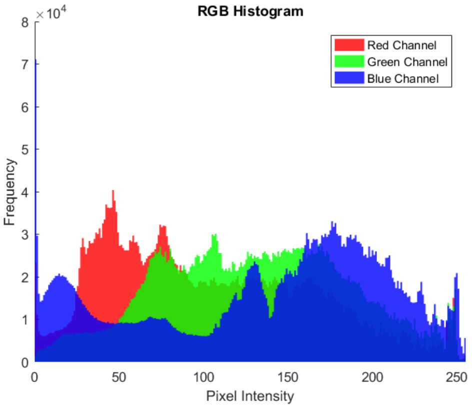

Fig 5. RGB Histogram of Embedded Image

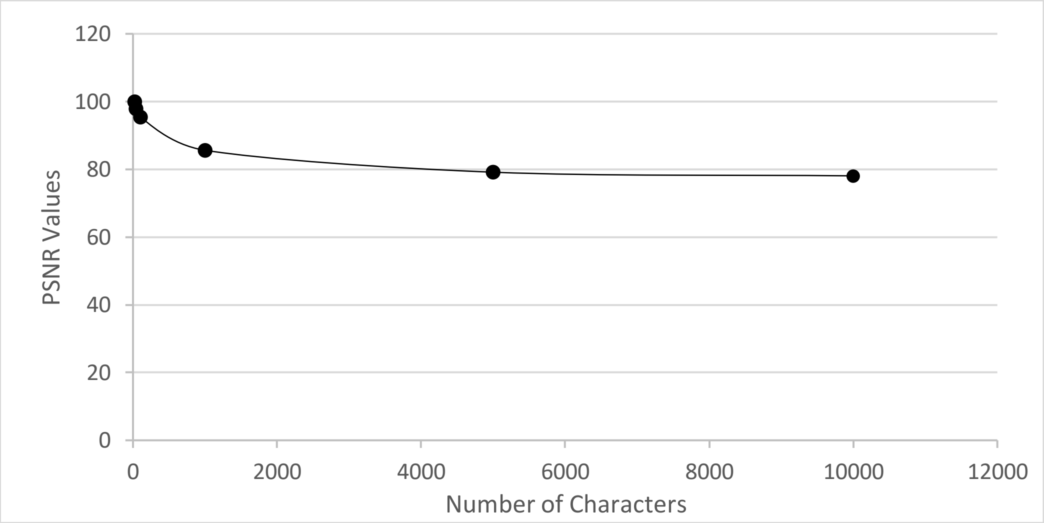

Fig 6. PSNR Value Versus Number of Characters Graph

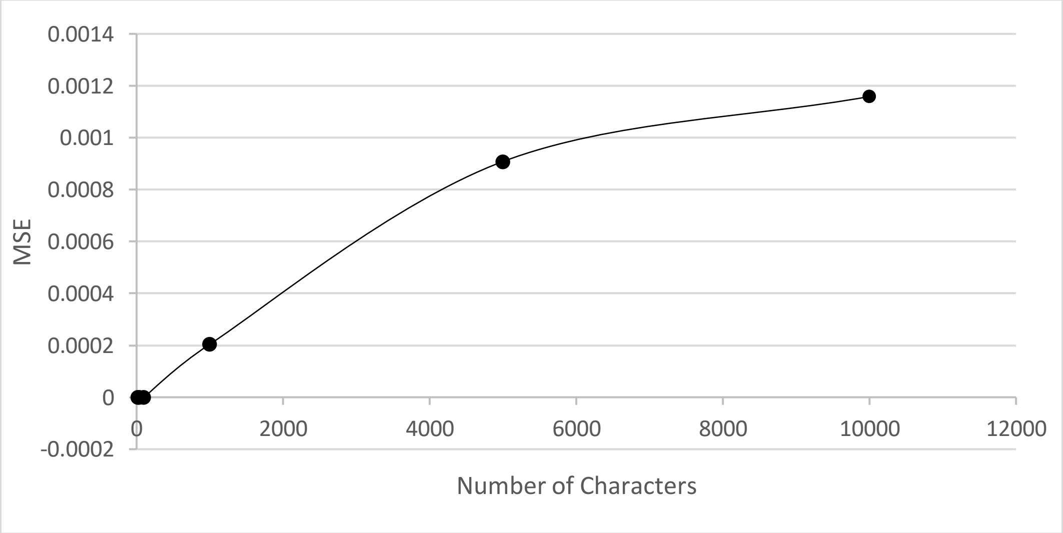

Fig 7. MSE Value Versus Number of Characters Graph

VI. CONCLUSION

Conclusion:

In conclusion, the culmination of this project yields a robust steganographic method tailored to securely embed keys within AI-generated images. This achievement holds profound implications for the landscape of secure digital communication, extending its reach into critical domains such as cybersecurity, digital rights management, and secure social networking.

The development of this steganographic method represents a significant stride forward in the realm of information security, offering a potent tool to safeguard sensitive data in the face of escalating cyber threats. By seamlessly integrating cryptographic keys into visually complex AI-generated content, our method ensures covert communication channels that are resilient against detection and interception.

Furthermore, the versatility of our approach opens avenues for its application across diverse domains, from ensuring the integrity of digital assets in content distribution networks to fortifying the privacy of communication in social media platforms. As we navigate the increasingly complex digital landscape, the adoption of our steganographic method promises to bolster the foundations of secure communication, empowering individuals and organizations to safeguard their digital assets and uphold their privacy rights.

In essence, the successful completion of this project marks a pivotal milestone in advancing the frontiers of steganography and its transformative potential in shaping the future of secure digital communication. As we continue to refine and extend our method, we remain committed to fostering a safer and more resilient digital ecosystem for generations to come.

Future Scope:

- Cross-Domain Applications: Explore the applicability of the proposed steganographic method in diverse domains beyond traditional digital communication, such as healthcare, finance, and Internet of Things (IoT). Investigate how the method can be adapted to securely conceal sensitive information in various contexts, addressing domain-specific challenges and requirements.
- Integration with Security Technologies: Investigate the integration of the proposed steganographic method with other security technologies to create comprehensive and layered defense mechanisms. Explore synergies with encryption algorithms, digital watermarking techniques, and authentication protocols to enhance data security and integrity in digital ecosystems.
- Robustness Against Advanced Attacks: Conduct further research to assess the method's resilience against more sophisticated attacks and steganalysis techniques. Explore adversarial training approaches, anomaly detection methods, and machine learning-based defenses to strengthen the algorithm's robustness and resilience in the face of evolving threats.
- User-Centric Design and Usability: Consider the usability and user experience aspects of deploying the steganographic method in practical settings. Conduct user studies and usability evaluations to understand user preferences, requirements, and challenges. Design intuitive interfaces and tools that facilitate seamless integration and adoption of the method in everyday communication workflows.
- Standardization and Interoperability: Work towards standardization and interoperability of steganographic methods to promote adoption and compatibility across different platforms and systems. Collaborate with standardization bodies and industry stakeholders to establish guidelines, protocols, and best practices for secure data hiding and communication.
- By pursuing these avenues of future research and development, we can further advance the capabilities, applicability, and resilience of the proposed steganographic method, paving the way for enhanced security and privacy in digital communication and beyond.

VII. ACKNOWLEDGEMENT

We are immensely grateful to our esteemed teacher and guide, Dr. Aniruddha Das, whose invaluable mentorship and unwavering support were instrumental in the successful completion of this independent research endeavor. His profound insights, constructive feedback, and steadfast encouragement played a pivotal role in shaping the direction and quality of our work.

REFERENCES

1. Guofang Kessler, "An Overview of Steganography for the Computer Forensics Examiner," Garykessler.net, 2021. [Online]. Available: https://www.garykessler.net/library/steganography.html.
2. Abhishek Raut and R. Babu, "An Approach to Watermarking Using Polymorphic Algorithms For Increased Data Security," Research Gate, Apr. 2022. [Online]. Available: https://www.researchgate.net/publication/380891108_An_Approach_to_Watermarking_Using_Polymorphic_Algorithms_For_Increased_Data_Security.
3. "OpenStego - Open Source Steganography Solution," Openstego.com, 2023. [Online]. Available: https://www.openstego.com/.
4. Richard E. Ziemer and William H. Tranter, "Digital Communication Techniques: Signal Design and Detection," Dspguide.com, 1976. [Online]. Available: https://www.dspguide.com/ch27/2.htm.
5. William Barker and W. Timothy Polk, "Recommendation for Key Management – Part 3: Application-Specific Key Management Guidance," NIST Special Publication 800-86, Dec. 2005. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf.
6. Shujun Li, Chunhua Chen and Yun-Qing Lo, "Steganography for Multimedia Data Based on High Efficiency Video Coding (HEVC)," in IEEE Access, vol. 7, pp. 179087-179095, 2019.
7. Sabyasachi Changder, Debasish Ghosh and Nirmal Chandra Debnath, "Wavelet-based blind signal processing technique for image steganography," Multimedia Tools and Applications, vol. 76, no. 15, pp. 16723–16745, Aug. 2017.
8. Zonghua Cao, Lihua Chen and Xiaoping Yang, "Hash against Packet Augmented for Improving Receiver-End Multimedia Data Security," Computers, Materials & Continua, vol. 55, no. 3, pp. 440-454, 2018.
9. Yucui Wang, Hao Zhang, Dexing Wu, Xueye Yang, and Shu-Ming Kwok, "A Steganographic Method for Digital Images with Four-Pixel Differencing and LSMR Technique," Multimedia Tools and Applications, vol. 80, no. 16, pp. 24489–24519, Nov. 2021.
10. Youssoufa Mohamadou, Sylvain Loua Batog and Malam Halidou, "Robust Steganography based on Matching Pixel Locations," Research Gate, Nov. 2016. [Online]. Available: https://www.researchgate.net/publication/317609880_Robust_Steganography_based_on_Matching_Pixel_Locations.
11. Nas I. Haidar and Anas Dabbagh, "New Image Steganography Method by Matching Pixels and Rows," unpublished. [Online]. Available: https://d1wqtxts1xzle7.cloudfront.net/31134027/1.New_image.full-libre.pdf.
12. Pabak Indu and B. Sathish Babu, "Hiding Data in Text using ASCII Mapping Technology (AMT)," Research Gate,Sep.2013.[Online].Available: https://www.researchgate.net/publication/258815654_Hiding_Data_in_Text_using_ASCII_Mapping_Technology_AMT.
13. Haibo Zhang and Huating Yu, "A Content-Adaptive Multi-Embedding Scheme for Enhancing Payload of Video Steganography," Signal Processing, vol. 147, pp. 77-85, 2018.
14. M. T. Pilihal and V. Ananda Mohan, "A Novel Approach for Video Steganography," in IEEE International Conference on Signal Processing, Communications and Networking, 2007, pp. 286-289.
15. Ravi Chandramouli and Nasir Memon, "On Steganalytic Attacks for Spatial Domain Image Steganography," in Digital Forensic Research Workshop, 2001.
16. Akhil Kumar and V. Priyadarshini, "Image Steganography Based on Chaos, DCT and LSB Technique," Journal of Theoretical and Applied Information Technology, vol. 95, no. 5, 2017.
17. Mitrakshara Ray et al., "Data Hiding Technique for Image using Compression and Encrypted LSB Data," in International Conference on Cyber Security and Computer Science, pp. 85-100, 2018.
18. A.M. Rafi, R. Alesii, G.N. Ali and Y.V. Cheplygina, "A Survey on Digital Image Steganography and Steganalysis," OpenBook, Feb. 2007. [Online]. Available: https://books.google.co.in/books?id=wcAZ-QEthqkC.
19. Gopikrishna Unnikrishnan and Kavita Singh, "Double Random Fractional Fourier Domain for Spread Spectrum Image Watermarking," in IET Image Processing, vol. 3, no. 1, pp. 19-35, Feb. 2009.
20. Balvinder Singh, Meenakshi Singh and Akshay Agarwal, "A Secure Image Steganography Model Using Image Shaping and XOR Encoding," in Procedia Computer Science, vol. 84, pp. 143-149, 2016.

21. Akhilesh Kumar, Gopinath Parimala Gupta, Rajeev Singh Yadav and Sanjay Kumar Singh, "A Novel Digital Image Watermarking Technique for Effective and Robust Image Recovery," Wireless Personal Communications, vol. 106, no. 2, pp. 601–621, 2019.
22. Niels Provos and Peter Honeyman, "Hide and Seek: An Introduction to Steganography," IEEE Security and Privacy Magazine, vol. 1, no. 3, pp. 32-44, 2003.
23. Vijaya Balasubramanian and William H. Stark, "A Data Hiding Technique Using Binary Encoded Audio Files," in International Conference on Security and Management, 2022, in press.
24. Christian Cachin, "An Information-Theoretic Model for Steganography," Information and Computation, vol. 192, no. 1, pp. 41-56, 2004.
25. Andreas Westfeld and Gunter Wolf, "Steganography in a Video Conferencing System," in Information Hiding, vol. 1768, pp. 32-47, Oct. 2000.