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 13, Issue 4, April 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

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

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304218 |

Enhanced Image Steganography using Dual Authentication and Camellia Cipher Encryption

Dr. Madhuri Kovoor [1], G. Mahalakshmi Sai Padmini [2], B. Vaishnavi [3], CH. Shreya [4]

Associate Professor, Dept. of CSE, Anurag University, Hyderabad, India

UG Student, Dept. of CSE, Anurag University, Hyderabad, India

UG Student, Dept. of CSE, Anurag University, Hyderabad, India

UG Student, Dept. of CSE, Anurag University, Hyderabad, India

ABSTRACT: In the realm of image data security and steganography applications, evaluating content similarity between different image datasets and addressing embedding distortions within images pose significant challenges. Existing methodologies often lack effectiveness, hindering the assessment of content comparability among sets of photos. To address these limitations, this project introduces a novel technique specifically tailored for PNG pictures. The proposed algorithm offers a comprehensive assessment of content similarity while accounting for embedding distortion. Beyond image comparison, the methodology extends to cover image selection, sender and receiver authentication mechanisms, and integration of Camellia Cipher encryption. Key components include algorithmic cover image selection, robust authentication mechanisms, seamless integration of Camellia Cipher encryption, and comprehensive image steganography techniques. The project aims to provide a holistic solution that enhances security and performance in image steganography applications, contributing to advancements in the field of image data security.

KEYWORDS: Image Content Similarity, Embedding Distortion, Structural Similarity Index (SSIM), Entropy, Fractal Dimension, Edge Detection, Text Compression, LZW Algorithm, Least Significant Bit (LSB) Steganography, Camellia Cipher, Base – 64 Encoding, Portable Network Graphics (PNG) images.

I. INTRODUCTION

Steganography is a technology to send secret data on public channels without drawing suspicion by slightly modifying the media content [1]. As the adversary, steganalysis aims to discover the possible covert communication by analyzing the public media [2]. The effectiveness of steganography lies in its ability to conceal the presence of hidden information within cover objects, such as images. Various techniques have been developed to enhance this concealment process, including dynamic steganography. Aside from dynamic steganography, several other methods aim to conceal the presence of steganographic activity. These may include techniques such as covert channel communication, which involves hiding information within seemingly innocuous communication channels, or adaptive steganography, where the embedding process adapts dynamically to its environment to avoid 2 detection. Additionally, methods like data fragmentation and spread spectrum techniques can also be employed to scatter hidden information across multiple data units, making it more challenging for interceptors to detect. One particularly significant method discussed in this paper is Cover Image Selection. Cover Image Selection plays a crucial role in steganography as it can deceive potential interceptors into believing that no steganographic activity has taken place, when in fact it has. This is achieved by carefully choosing cover images that blend seamlessly with the hidden information, making it difficult for covert listeners to detect any alterations. By emphasizing the importance of Cover Image Selection, this paper underscores its role in enhancing the covert nature of steganographic communication. It highlights how strategic selection of cover images can effectively mislead interceptors, ultimately safeguarding the secrecy and integrity of the hidden information. This research paper explores the integration of PNG Image Compression, Diffie-Hellman Authentication, Camellia cipher, LZB Compression, Header Text, Initialization Vector (IV), Base64 Encoding, and LSB Steganography. These elements will be applied across different phases of the project.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304218 |

II. RELATED WORK

[1] Zichi Wang, 2023 et.al: This paper, presents a pioneering methodology for cover selection in steganography, integrating considerations of image similarity and embedding distortion to bolster security measures. Diverging from conventional practices that prioritize embedding distortion alone, this approach incorporates a customized calculation of image similarity using singular value decomposition (SVD), with a focus on small singular values that align with steganographic properties. By amalgamating image similarity and embedding distortion, the proposed strategy optimizes the utilization of batch images while fortifying resilience against steganalysis. Experimental findings showcase the superior efficacy of this method compared to existing cover selection techniques, as confirmed through evaluation with contemporary steganalytic tools. **[2] X.Liao, 2022 et.al:** In light of the increasing adoption of cloud storage for storing vast collections of digital images, this paper explores the implications for steganography, which gains a new avenue for embedding secret information across multiple images. Instead of conventional single image steganography, this approach allows for the adaptive distribution of a set of secret information across multiple images shared via cloud storage. However, an unresolved challenge lies in determining how to allocate embedding payload efficiently among these images to enhance security performance. This paper formulates adaptive payload distribution in the context of multiple image steganography, leveraging image texture features, and conducts theoretical security analyses from the perspective of steganalysts. Two payload distribution strategies based on image texture complexity and distortion distribution are proposed and discussed. These strategies can be integrated with existing stateof-the-art single image steganographic algorithms. Comparative evaluations against modern universal pooled steganalysis and single image steganalyzer methods demonstrate the security performance of the proposed payload distribution strategies. Extensive experimental results underscore the effectiveness of these strategies in achieving improved security performance. **[3]T.Kalaichelvi,2020 et. al:** Abstract— Steganography is a data hiding technique, which is generally used to hide the data within a file to avoid detection. It is used in the police department, detective investigation, and medical fields as well as in many more fields. Various techniques have been proposed over the years for Image Steganography and also attackers or hackers have developed many decoding tools to break these techniques to retrieve data. In this paper, CAPTCHA codes are used to ensure that the receiver is the intended receiver and not any machine. Here a 3 randomized CAPTCHA code is created to provide additional security to communicate with the authenticated user and used Image Steganography to achieve confidentiality. For achieving secret and reliable communication, encryption and decryption mechanism is performed; hence a machine cannot decode it using any predefined algorithm. Once a secure connection has been established with the intended receiver, the original message is transmitted using the LSB algorithm, which uses the RGB color spectrum to hide the image data ensuring additional encryption**. [4] V. Sachnev, 2009 et.al:** This paper presents an efficient JPEG steganography method based on heuristic optimization and BCH syndrome coding. The proposed heuristic optimization technique significantly decreases total distortion by inserting and removing AC coefficients 1 or -1 in the most appropriate positions. The implemented data hiding technique is based on structured BCH syndrome coding. This method achieves multiple solutions for hiding data to a block of coefficients. The proposed data hiding method chooses the best solution with minimum distortion effect. As a result, the total distortion can be significantly reduced, which results in less detectability of the steganalysis. The experiments include the steganalysis of the proposed data hiding methods. The experiment results shows that the proposed heuristic optimization significantly decreases detectability of the steganalysis. The proposed methods also outperform the existing steganography methods. **[5] Sabyasachi Pramanik, 2019 et.al:** The paper delves into the integration of CAPTCHA codes within image steganography as a means of bolstering data security during internet transmissions. CAPTCHA, serving as a human verification mechanism, is embedded into cover images using ASCII encoding and encryption. This process results in stego images where the original CAPTCHA content is obscured, enhancing the confidentiality of transmitted data. By leveraging image steganography alongside CAPTCHA, the paper proposes a robust approach to safeguarding against unauthorized access and ensuring secure internet communications, thereby mitigating potential risks associated with spam and unauthorized data interception**. [6] Alaa A. Jabbar Altaay, 2012 et.al:** This paper provides an overview of image steganography, a security technique aimed at concealing messages between sender and recipient. Steganography has been employed across various file types, including digital images, audio, and video. For audio steganography, key parameters include imperceptibility, payload capacity, and robustness. Different applications may necessitate varying steganography techniques to meet specific requirements. The paper aims to explore the uses and techniques of image steganography, shedding light on its significance in ensuring covert communication in modern digital environments.

III. METHODOLOGY

In this research paper we discuss where first 8 Uncompressed PNG Images are taken and among those 1 Image is selected as Best Image based on Cover Image Selection Parameters which are Image Similarity where and the same is

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304218 |

done to the 8 Compressed PNG Images and then finally among these 2 Cover Images we select the final Cover Image that is suitable for the steganography and then we do the Text Compression using LZW Algorithm and then using we encrypt the compressed text with Camellia Cipher and then encode in the selected Cover Image using LSB Steganography.

PNG Image Compression: We aim to assess the functionality of our project by subjecting it to tests involving both compressed and uncompressed PNG images. Our testing methodology involves compressing PNG images based on parameters specified by the user, leveraging the flexibility provided by the `format_size` option. This option empowers users to finely tune the compression process according to their preferences, allowing them to specify the desired level of compression for the images.

Cover Image Selection: This research paper tackles a significant challenge in steganography, which is the absence of a universally effective method for evaluating content similarity across various image collection. Previous research often lacked adaptability to diverse content types, leading to suboptimal performance in different scenarios. Prior studies utilized KL Divergence for embedding distortion and Singular Value Decomposition for Image Similarity, which proved flawed in cases of alterations in image contrast, brightness, and flipping. Consequently, this project introduces an adaptive algorithm tailored to diverse content types, particularly PNG images, considering text and image compression while focusing on specific image parameters like fractal dimension, edge detection, SSIM calculation, and entropy. This approach comprehensively assesses content similarity, embedding distortion, and cover image selection. By minimizing image similarity within a batch, the 5 method ensures a wide range of coverings, thereby enhancing overall security. The project's primary objective is to bolster the security, resilience, and efficiency of the steganographic process. To safeguard data privacy, the project employs dual authentication processes and utilizes the Camellia algorithm for advanced encryption. This comprehensive strategy not only addresses limitations in traditional techniques but also establishes a robust foundation for secure communication.

Diffie Hellman Authentication: The Diffie-Hellman key exchange facilitates the establishment of a shared secret key between two entities, known as the sender and receiver, without directly transmitting it across an insecure communication channel. This shared key serves as a foundation for secure communication between the parties. The process begins with both parties agreeing upon common public parameters, including a large prime number 'p' and a primitive root modulo 'g'. Each entity generates a private key ('sender_private_key' for the sender and 'receiver_private_key' for the receiver) through random selection. Using their respective private keys and the agreed-upon public parameters, they compute their partial public values ('x' for the sender and 'y' for the receiver). These partial public values are then securely exchanged between the parties. Upon receiving the other party's partial public value, each entity computes the shared secret key by combining its private key with the received partial public value. If the computed shared secret keys match on both ends, authentication is successful, permitting secure communication to proceed. However, if the shared secret keys do not match, it indicates a potential security breach or unauthorized access, leading to authentication failure.

Camellia Cipher: The Camellia cipher is a symmetric key block cipher known for its robust security and efficient implementation across hardware and software platforms. It supports key lengths of 128, 192, and 256 bits, offering flexibility in encryption applications. With its origins in Japan, Camellia has gained international recognition and adoption, including being endorsed as a standard encryption algorithm by organizations such as the European Union. In this research paper we have used 256-bit key and, the Camellia cipher excels in encrypting sensitive data securely.

Initialization Vector (IV): In Camellia encryption, the Initialization Vector (IV) is a randomly generated 128-bit value, ensuring distinct ciphertexts for repeated encryption of the same plaintext with the same key. This prevents patterns and repetition in the ciphertext, enhancing the confidentiality and integrity of the encrypted data, thus bolstering overall security.

SHA-256: A cryptographic hash algorithm called SHA-256 is employed in a variety of security applications. It is intended to accept as input a message or other piece of data and output a fixed-length, 256-bit hash value. As a member of the SHA-2 family, SHA-256 is renowned for its dependability and resistance to collisions, making it ideal for secure password storing and data integrity verification.

Cipher Feedback (CFB): Cipher Feedback (CFB) mode is a block cipher mode of operation that transforms a block cipher into a stream cipher, enabling encryption and decryption of data of arbitrary length. It operates by repeatedly

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304218 |

encrypting an initialization vector (IV) or the previous ciphertext block to generate a keystream, which is then combined with the plaintext using a bitwise XOR operation to produce the ciphertext. CFB mode offers flexibility for handling plaintext of any size while maintaining security properties such as confidentiality and error propagation. However, proper IV management is crucial to prevent cryptographic vulnerabilities, as reusing IVs can lead to security weaknesses.

LZW Compression: Lempel-Ziv-Welch (LZW) compression is a widely used lossless data compression algorithm. It builds a dictionary of patterns encountered in the input data, replacing these patterns with shorter codes during compression. During decompression, the original string is reconstructed using the codes and dictionary. LZW's ability to efficiently encode repetitive patterns makes it a popular choice for file

compression utilities, achieving high compression ratios while preserving data integrity.

LSB Steganography: By carefully changing the least significant bits of the red, green, and blue color channels, LSB steganography in RGB mode is a technique for hiding data inside pictures. This technique is frequently used to cover up watermarks or hidden messages in digital photos. You can incorporate data without drastically altering the look of the image by substituting hidden information for the least important sections. Despite its drawbacks, it is nonetheless a popular and easy approach for basic picture steganography, having uses in both legal and illegal contexts, such as digital watermarking.

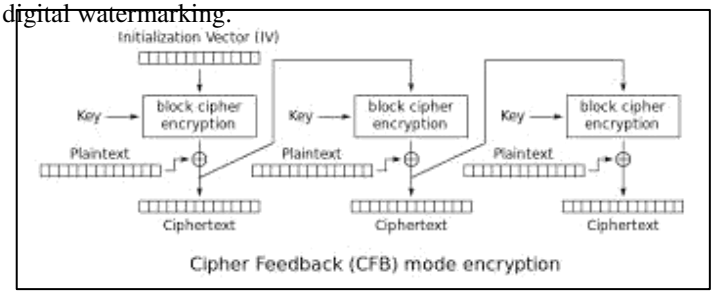


Fig 1: Cipher Feedback Mode

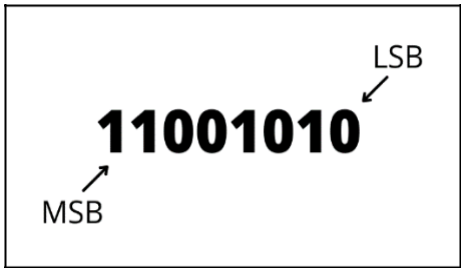


Fig 2: LSB & MSB

Developing environment is as follows:

Firstly, the Cover Image Selection is done among the 8 Uncompressed Images based on Image Similarity using SSIM Index and using the Entropy, Fractal Dimension and Edge Detection for the Embedding distortion.

Fig 3: Cover Image Selection from Batch Images

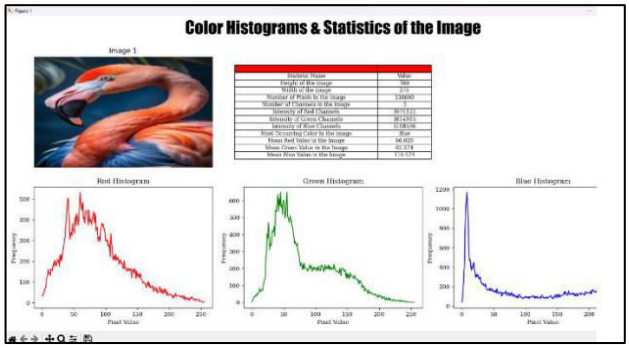


Fig 4: Color Histograms & Statistics of Image

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304218 |

Image Similarity by SSIM

Calculating Structural Similarity Index (SSIM) for all the 8 Images

Structural Similarity Index (SSIM) Values for the Images

	Image 1	Image 2	Image 3	Image 4	Image 5	Image 6	Image 7	Image 8
Image 1	1	0.0122	-0.0046	0.1509	0.0166	0.0639	0.1005	0.105
Image 2	0.0122	1	0.0374	0.0448	-0.0174	0.0882	0.0114	-0.0069
Image 3	-0.0046	0.0374	1	0.087	-0.0718	0.2204	0.2118	0.0821
Image 4	0.1509	0.0448	0.087	1	-0.0312	0.1917	0.309	0.1769
Image 5	0.0166	-0.0174	-0.0718	-0.0312	1	-0.1468	-0.0154	-0.0378
Image 6	0.0639	0.0882	0.2204	0.1917	-0.1468	1	0.2892	0.1706
Image 7	0.1005	0.0114	0.2118	0.309	-0.0154	0.2892	1	0.308
Image 8	0.105	-0.0069	0.0821	0.1769	-0.0378	0.1706	0.308	1

Calculating the Cumulative SSIM Value for Each Image

	Image 1	Image 2	Image 3	Image 4	Image 5	Image 6	Image 7	Image 8
Cumulative SSIM	0.4445	0.1697	0.5623	0.9291	-0.3038	0.8772	1.2145	0.7979

Fig 5: Image Similarity by SSIM

At this stage, we select only 4 Images based on their least Cumulative SSIM Value

Image Name	SSIM Value
Image 5	-0.3038
Image 2	0.1697
Image 1	0.4445
Image 3	0.5623

Fig 6: 4 Least Cumulative SSIM Value

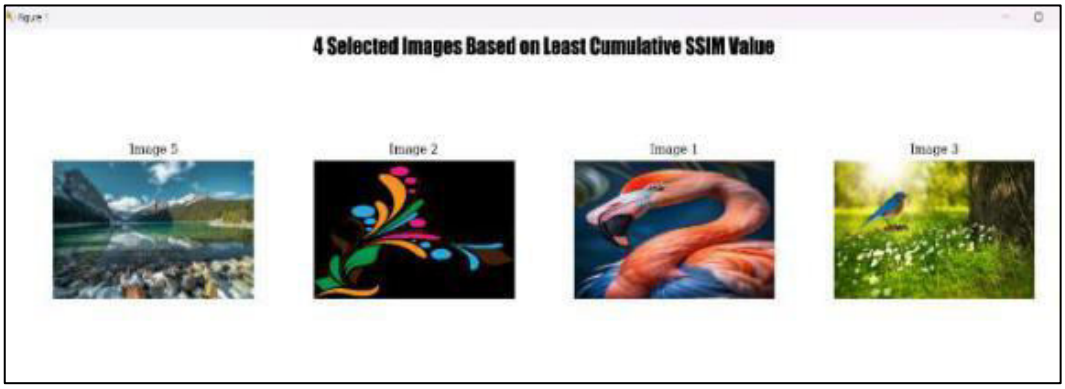


Fig 7: 4 Selected Images based on Least Cumulative SSIM Value

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304218 |

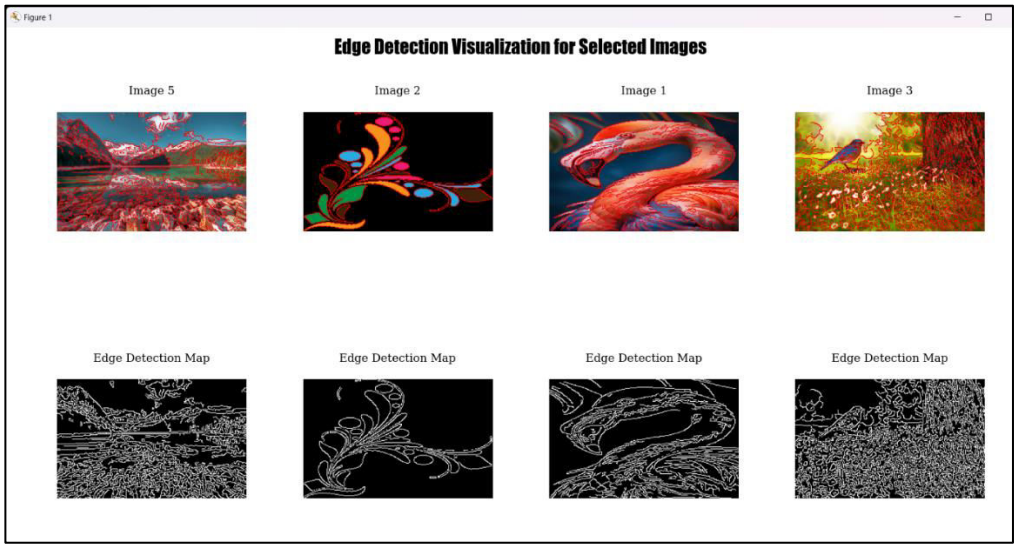


Fig 8: Edge Detection Visualization for Selected Images

EMBEDDING DISTORTION:

Calculating Embedding Distortion based on Entropy, Fractal Dimension and Edge Detection

Entropy values for the Selected Images

	Image 5	Image 2	Image 1	Image 3
Entropy	10.2037	1.3554	10.2782	10.4243

Fractal Dimension values for the Selected Images

	Image 5	Image 2	Image 1	Image 3
Fractal Dimension	0.8605	0.7623	0.884	0.9082

Edge Detection values for the Selected Images

	Image 5	Image 2	Image 1	Image 3
Edge Detection	0.2331	0.0744	0.1695	0.2843

Displaying the cumulative metrics for the embedding distortion

Cumulative Metrics for the Selected Images

	Image 5	Image 2	Image 1	Image 3
Entropy	10.2037	1.3554	10.2782	10.4243
Fractal Dimension	0.8605	0.7623	0.884	0.9082
Edge Detection	0.2331	0.0744	0.1695	0.2843
Cumulative Metrics	11.2973	2.1921	11.3317	11.6168

Selected Cover Image from 8 Compressed PNG Images is : Image 3

Fig 9: Embedding Distortion Values of the Selected Images

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304218 |

Fig 10: Final Selected Cover Image

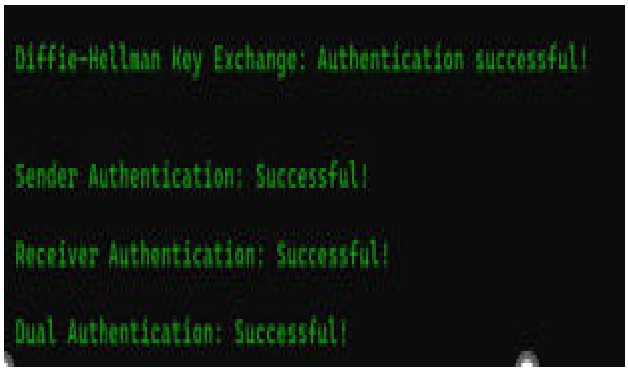


Fig 11: Diffie Hellman Authentication

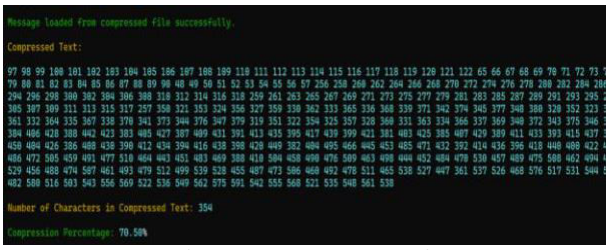


Fig 12: LZW Compression

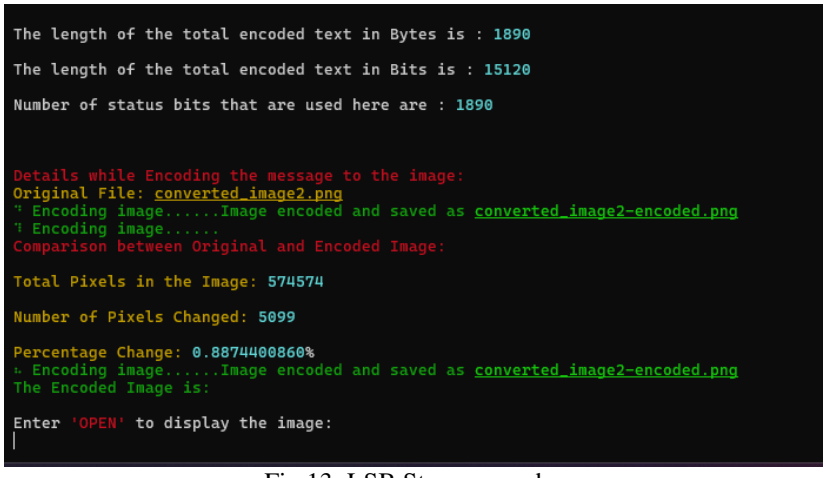


Fig 13: LSB Steganogrpahy

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304218 |

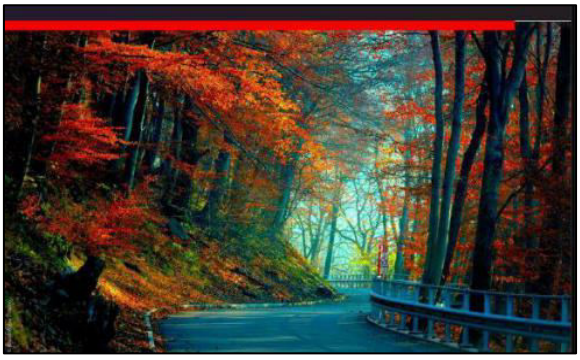


Fig 14: Stego Image illustrating the text encoded

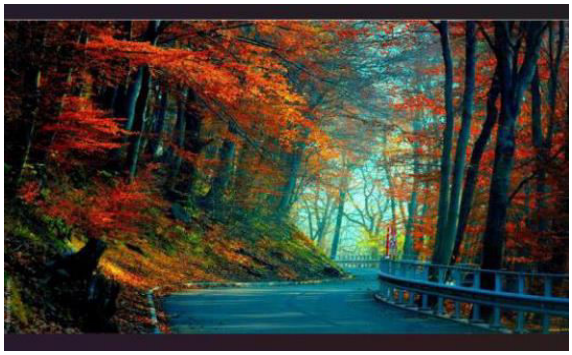
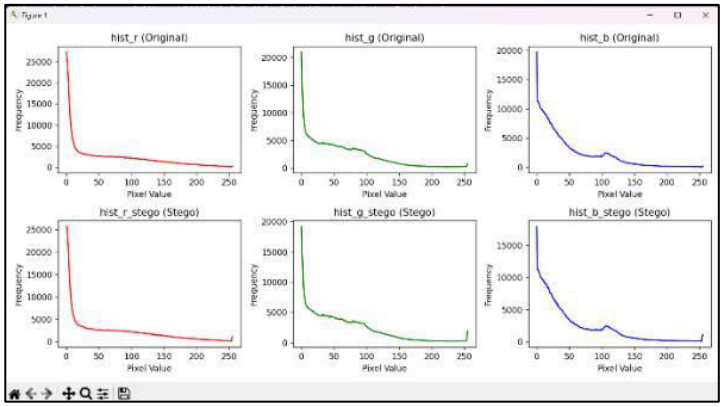


Fig 15: Final Stego Image

IV. EXPERIMENTAL RESULTS

To examine the distortion and noise in the same image of various sizes, we utilized the Mean Square Error and Peak Signal to Noise Ratio (PSNR). As can be seen, the PSNR decreases as the image size decreases and when the Encoded text size increases. But is still rather substantial, indicating that the cover image and the genuine image cannot be distinguished by the naked eye. The receiver was able to decode the image and obtain the cipher text after we successfully encrypted the message using Camellia Cipher and concealed it in the image using Steganography.



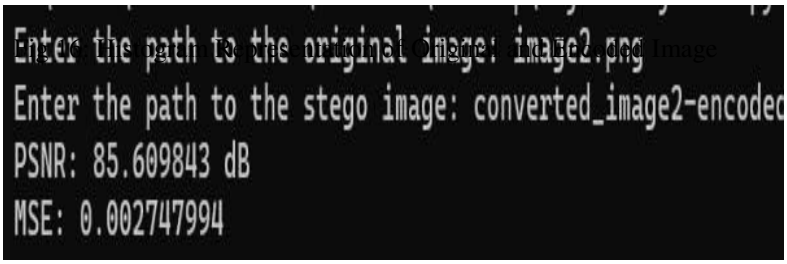


Fig 17: Calculation of PSNR & MSE Values

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304218 |

V. CONCLUSION

In conclusion, this project addresses a critical challenge in steganography by introducing an adaptive algorithm that effectively assesses content similarity across diverse image collections. Previous studies often struggled to provide universally effective methods, leading to suboptimal performance across different scenarios. By considering factors such as text and image compression, along with specific image parameters like fractal dimension, edge detection, SSIM calculation, and entropy, the proposed algorithm ensures comprehensive evaluation of content similarity, embedding distortion, and cover image selection, particularly focusing on PNG images.

One significant contribution of this project is the reduction of image similarity within a batch, leading to a diverse range of coverings and thereby enhancing overall security. The primary objective of the project is to enhance the security, robustness, and effectiveness of the steganographic process. To achieve this, the project employs dual authentication processes and leverages the Camellia algorithm for advanced encryption, ensuring data privacy and integrity.

Through this comprehensive approach, the project not only addresses limitations in traditional steganographic techniques but also lays a foundation for reliable communication security in diverse applications. By integrating adaptive algorithms, advanced encryption, and comprehensive evaluation methods, this project sets a new standard for steganography, enabling secure and effective data concealment in digital images.

REFERENCES

[1] Wang, Z., Feng, G., Shen, L., & Zhang, X. (2023). Cover Selection For Steganography Using Image Similarity. IEEE Transactions On Dependable And Secure Computing, 20(3), 305-317.
[2] Liao, X., Yin, J., Chen, M., & Qin, Z. (2022). Adaptive payload distribution in multiple images steganography based on image texture features. IEEE Transactions on Dependable Secure Computing, 19(2), 897-911.
[3] Kalaichelvi, T., et al. (2020). Image Steganography Method to Achieve Confidentiality Using CAPTCHA for Authentication. Proceedings of the Fifth International Conference on Communication and Electronics Systems (ICCES 2020), IEEE Conference Record # 48766.
[4] Sachnev, V., Kim, H. J., & Zhang, R. (2009). Less detectable JPEG steganography method based on heuristic optimization and BCH syndrome coding. In Proc. 11th ACM Workshop Multimedia Security, pp. 131–140.
[5] Pramanik, S., Singh, R.P., & Ghosh, R. (n.d.). A new encrypted method in image steganography. Indonesian Journal of Electrical Engineering and Computer Science, 14(3).
[6] Jabbar Altaay, A. A., et al. (2012). An Introduction to Image Steganography Techniques. 2012 International Conference on Advanced Computer Science Applications and Technologies.
[7] Qiao, T., Luo, X., Wu, T., Xu, M., & Qian, Z. (2021). Adaptive steganalysis based on statistical model of quantized DCT coefficients for JPEG images. IEEE Transactions on Dependable Secure Computing, 18(6), 2736–2751.
[8] Lalengmawia, C., & Bhattacharya, A. (2016). Image Steganography using Advanced Encryption Standard for implantation of Audio/Video Data. 2016 Fifth International Conference On Recent Trends In Information Technology.
[9] Cica, Z. (2016). Pipelined Implementation of Camellia Encryption Algorithm. 2016 24th Telecommunications Forum (TELFOR), IEEE.
[10] Pabbi, A., et al. (2021). Implementation of Least Significant Bit Image Steganography with Advanced Encryption Standard. 2021 International Conference on Emerging Smart Computing and Informatics (ESCI) AISSMS Institute of Information Technology, Pune, India.
[11] Sheth, U., & Saxena, S. (2016). Image Steganography Using AES Encryption and Least Significant Nibble. International Conference on Communication and Signal Processing.
[12] Krishnaveni, N., & Periyasamy, S. (2018). A Novel and Innovative Approach for Image Steganography with Chaos. Indonesian Journal of Electrical Engineering and Computer Science, 11(1), 263–267.
[13] Fridrich, J., & Kodovsky, J. (2012). Rich models for steganalysis of digital images. IEEE Transactions on Information Forensics and Security, 7(3), 868–882.
[14] Kumar, A., & Pooja, K. (2010). Steganography - A Data Hiding Technique. International Journal of Computer Applications, 9(7), 19-23.
[15] Bhargava, S., & Mukhija, M. (2019). Hide Image And Text Using Lsb, Dwt And Rsa Based On Image Steganography. ICTACT Journal on Image & Video Processing, 9(3).

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304218 |

[16] Gutub, A., Al-Qahtani, A., & Tabakh, A. (2009). Triple-A: Secure Rgb Image Steganography Based On Randomization. 2009 IEEE/ACS International Conference on Computer Systems and Applications, 400-403.
[17] Srilakshmi, P., et al. (2018). Text Embedding Using Image Steganography In Spatial Domain. International Journal of Engineering & Technology, 7(3.6), 14.
[18] Rana, M. S., Sangwan, B. S., & Jangir, J. S. (2012). Art Of Hiding: An Introduction To Steganography. International Journal Of Engineering And Computer Science, 1(1), 11-22.
[19] Mathkour, H., Al-Sadoon, B., & Touir, A. (2008). A New Image Steganography Technique. 2008 4th International Conference on Wireless Communications, Networking and Mobile Computing, 1-4.
[20] Provos, N., & Honeyman, P. (2003). Hide and seek: an introduction to steganography. IEEE Security Privacy, 1(3), 32-44.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

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