



## Text Data Embedding in Encrypted Images: Adaptive Embedding and PSNR Analysis with Python and RSA

*Harshal Jain<sup>[1]</sup>, Shriya C. Nair<sup>[2]</sup>, Dr. Shyam R.<sup>[3]</sup>*

<sup>[1]</sup> UG Students, School of CS & IT, JAIN Deemed-to-be University, Bangalore

<sup>[2]</sup> UG Students, School of CS & IT, JAIN Deemed-to-be University, Bangalore

<sup>[3]</sup> Asst. Professor, Department of Computer Application, Presidency College, Hebbal

---

### ABSTRACT:

To investigate the idea of reversible data concealing in encrypted images with adaptive embedding, this study measures the peak signal-to-noise ratio (PSNR) and evaluates embedding capacity. Using RSA encryption to protect data integrity and secrecy, the study explores the viability of embedding text data into color images. Adaptive embedding is used to dynamically modify the embedding procedure according to the properties of the image. To find the greatest quantity of text data that can be inserted per pixel, the embedding capacity of the image is evaluated. Furthermore, the PSNR is computed to assess the embedded data quality of the original image. The studies, which combine RSA encryption with the Python programming language, shed light on how well the suggested strategy balances the ability to conceal data from view while maintaining image quality. The results further our understanding of the possible uses of reversible data-hiding strategies in encrypted images for secure data storage and communication. The research approach involves utilizing adaptive embedding techniques within encrypted images to assess the embedding capacity of text data and measure the PSNR using Python and RSA encryption. The significance lies in enhancing data security through reversible data hiding while maintaining image quality, contributing to advancements in secure communication and data storage methodologies.

Keywords: Reversible Data Hiding, Encrypted Images, Adaptive Embedding, Embedding Capacity, Text Data, Color Image, Peak Signal-to-Noise Ratio (PSNR), Python, RSA Encryption.

---

### Introduction:

To safely embed extra data into photos while maintaining the original image content, data hiding techniques are combined with encryption techniques in the topic of reversible data hiding in encrypted images with adaptive embedding. This approach allows for the reversible extraction of hidden data without compromising the integrity or confidentiality of the image. Adaptive embedding techniques dynamically adjust the embedding process based on image characteristics, enabling efficient utilization of available embedding capacity while minimizing distortion. This issue is important because it offers a way to improve data integrity and secrecy in picture communication and storage applications.

Data hiding techniques involve concealing additional information within digital content, such as images, audio, or video, without significantly altering the perceptual quality of the original data. Stenography and watermarking are common methods used for data hiding, where stenography focuses on concealing the existence of hidden data while watermarking aims to embed additional information for copyright protection or authentication purposes.

Encryption methods, on the other hand, involve transforming plain text data into cypher text using cryptography algorithms and keys to ensure confidentiality and integrity. Encryption ensures that unauthorized parties cannot access or decipher the original data without the appropriate decryption key. In encryption, symmetric and asymmetric encryption methods like RSA and AES are widely employed.

Preserving data integrity and confidentiality is crucial in various applications, including communication, storage, and digital rights management. Data integrity ensures that data remains unchanged and uncorrected during transmission or storage, while data confidentiality protects sensitive information from unauthorized access or disclosure. By integrating data-hiding techniques with encryption methods, it becomes possible to enhance both data confidentiality and integrity simultaneously, ensuring secure communication and storage of sensitive information. This connection allows the covert transfer of additional data while maintaining the integrity and security of the original image information, enabling reversible data hiding in encrypted photos. The research objectives of this study are twofold:

- To examine the practicality and effectiveness of hiding reversible data in encrypted images using adaptive embedding.
- To determine whether the text data can be incorporated into color images and to compute the peak signal-to-noise ratio (PSNR) using Python and RSA encryption.

The work is noteworthy because of its potential contributions to the fields of information security and data communication. By exploring the integration of reversible data-hiding techniques with encryption methods, the study aims to provide insights into enhancing data confidentiality and integrity in image communication and storage applications. Furthermore, the evaluation of embedding capacity and PSNR measurement using Python and RSA encryption can offer practical guidance for implementing secure data-hiding techniques in real-world scenarios, thereby addressing the growing need for robust and efficient data security solutions. Outline the structure of the paper.

---

## Literature Review:

Existing literature on reversible data-hiding techniques encompasses a wide range of methods and approaches aimed at concealing additional data within digital content while maintaining reversibility. Reversible data hiding in images has been addressed by a number of methods, including prediction-based approaches, histogram alteration, and Least Significant Bit (LSB) embedding.

Manipulating encrypted image data while preserving the protection and privacy that encryption affords is known as encrypted image processing. Techniques such as homomorphic encryption and proxy re-encryption enable the processing of encrypted images without decryption them, allowing for secure image operations such as addition, multiplication, and comparison.

Adaptive embedding algorithms dynamically adjust the embedding process based on image characteristics to optimize embedding capacity while minimising distortion. These algorithms utilize features such as pixel intensity distribution, local image characteristics, and prediction errors to modify image data for data-hiding purposes.

To assess how well reconstructed images compare to the originals, peak signal-to-noise ratio (PSNR) measuring techniques are frequently employed. Images fidelity is quantified by PSNR, which computes the ratio of peak signal strength to the mean squared error between the original and reconstructed images.

Relevant studies have explored the integration of data hiding and encryption techniques to address the dual objectives of data confidentiality and concealment. These studies have investigated various approaches for embedding additional data within encrypted content while preserving the security and integrity provided by encryption.

One common approach is to perform data hiding before encryption, where additional data is embedded into the plain text before encryption using steganography or watermarking techniques. This approach ensures that the hidden data remains concealed within the encrypted content, but it may require additional processing steps for data extraction after decryption.

An alternative method called encrypted domain data concealing entails explicitly embedding data within the encrypted material. Data embedding procedures can be carried out directly on encrypted data without requiring decryption thanks to techniques like homomorphic encryption and proxy re-encryption. By protecting data secrecy during the embedding process, this technology enhances security.

Furthermore, adaptive embedding techniques dynamically adjust the embedding process based on image characteristics or encryption parameters to optimize embedding capacity while minimizing distortion. These techniques ensure that the embedded data remains imperceptible and secure, even in the presence of encryption.

Even though there has been a lot of research on data concealing and encryption methods, there are still some significant gaps in the field that require more study. Among these gaps are:

- **Reversible data concealed in encrypted images: a limited analysis:** While there is extensive research on data hiding techniques and encryption methods individually, there is a lack of comprehensive studies focusing on reversible data hiding in encrypted images. Existing literature often overlooks the integration of these techniques, resulting in a gap in understanding the feasibility and effectiveness of such approaches.
- **Inadequate assessment of embedding capacity and image quality:** Numerous studies focus on the theoretical aspects of data hiding and encryption, with little actual evaluation of embedding capability and picture quality. There is a need for practical experiments to assess the maximum amount of data that can be embedded into encrypted images while maintaining acceptable levels of image quality.
- **Lack of standardized methodologies for evaluation:** The absence of standardized methodologies for evaluating embedding capacity, image quality, and security in reversible data hiding techniques hinders comparison and reproducibility across studies. Establishing standardized evaluation metrics and benchmarks would facilitate meaningful comparisons and advancements in the field.

- **Emerging challenges in adaptive embedding:** With the increasing complexity of image data and encryption algorithms, there is a need for adaptive embedding techniques that can dynamically adjust to changing conditions. However, existing literature lacks comprehensive studies on adaptive embedding algorithms and their performance in encrypted image processing.

The proposed research aims to address these gaps by investigating reversible data hiding in encrypted images with adaptive embedding. By evaluating embedding capacity, image quality, and security using Python and RSA encryption, the study seeks to contribute to the development of practical and efficient techniques for secure data hiding in encrypted images. Additionally, the research aims to establish standardized methodologies for evaluating reversible data-hiding techniques, paving the way for future advancements in the field.

---

## Methodology

The methodology used to achieve the research objectives involves several key steps:

- **Data Preparation:**
  - Select a set of color images to serve as the experimental dataset.
  - Prepare text data to be embedded into the images, varying in size and complexity to assess the embedding capacity.
- **Encryption:**
  - Encrypt the selected color images using RSA encryption with randomly generated public and private keys.
  - Make that the confidentiality and integrity of the original photos are preserved during the encryption process.
- **Adaptive Embedding:**
  - Implement adaptive embedding algorithms to dynamically adjust the embedding process based on image characteristics and encryption parameters.
  - Develop techniques to optimize embedding capacity while minimizing distortion and ensuring imperceptibility of the embedded data.
- **Embedding Capacity Evaluation:**
  - Calculate the embedding capacity of each encrypted image by systematically embedding text data into different regions of the image.
  - Determine the maximum amount of text data that can be embedded per pixel while maintaining acceptable levels of image quality.
- **PSNR Measurement:**
  - Reconstruct the encrypted images with embedded data using the decryption keys.
  - To assess the quality of the reconstructed images, compare the original encrypted images with the Peak Signal-to-Noise Ratio (PSNR).
  - Utilize Python libraries to implement PSNR measurement algorithms and ensure accurate and consistent results.
- **Experimental Evaluation:**
  - Conduct experiments using the prepared dataset and the developed methodologies.
  - Test the reversible data-hiding algorithms in encrypted images for embedding capacity, image quality, and security.
  - To make analysis and result interpretation easier, make notes of all experimental data and observations.
- **Analysis and Interpretation:**
  - Analyze the experimental results to assess the effectiveness and feasibility of the proposed reversible data-hiding techniques.
  - Interpret the findings in the context of the research objectives and the significance of the study.
  - Identify strengths, limitations, and areas for improvement in the developed methodologies.
- **Validation and Verification:**

- Validate the experimental results through rigorous testing and validation procedures.
- Verify the accuracy and reliability of the developed methodologies by comparing the results with existing literature and established benchmarks.

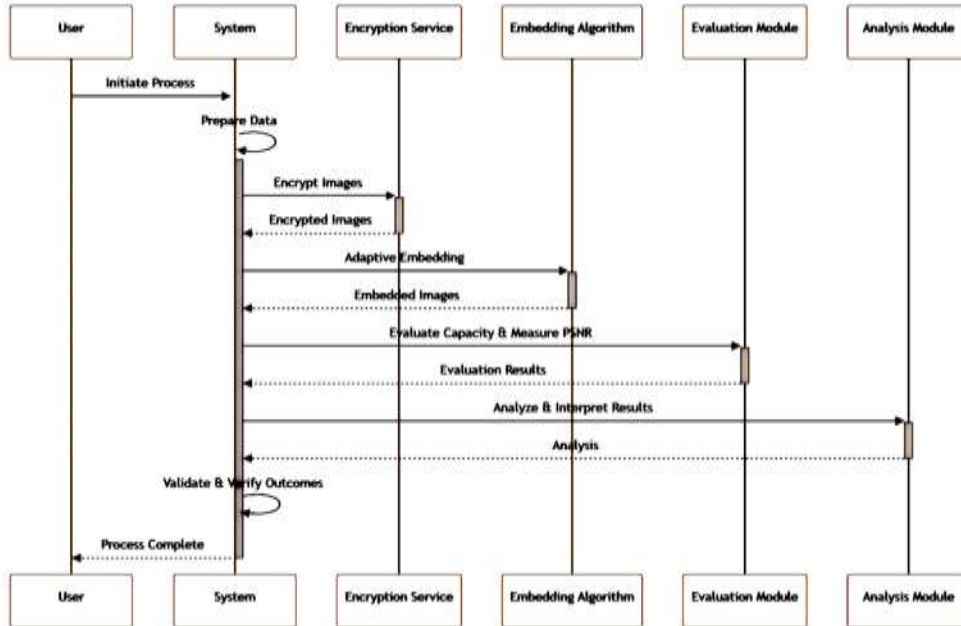


Fig. 1. Flow diagram for the encryption process

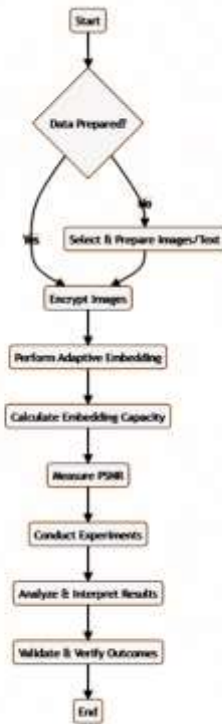


Fig. 2. Sequence of execution.

The flow of a system that processes and analyses images is depicted in the sequence diagram in Fig. 2

1. The user starts the process by pressing a button, which causes the system to start working.
2. The system gets ready to process the data, which probably means assembling or loading the photos for examination.
3. The photos are subsequently encrypted by the system using an encryption service, most likely for security or privacy reasons.
4. The encrypted photos are returned to the system by the encryption service when it has finished its work.
5. After that, the system employs an embedding algorithm for adaptive embedding, which probably entails adding more data or information to the pictures.
6. The Embedding Algorithm returns the altered (embedded) pictures to the system after it has finished its work.
7. The system makes use of an Evaluation Module to calculate the Peak Signal-to-Noise Ratio (PSNR), a metric commonly used to assess picture quality and to discover the capacity of the embedded data inside the images.
8. After completing its assessment, the Evaluation Module returns the findings to the system.
9. An Analysis Module receives the assessment findings from the system after which it analyses and interprets them. Based on the embedded data and image quality, the Analysis Module may draw conclusions or make judgements.
10. The Analysis Module returns its findings to the system after finishing the analysis.
11. The system is then subjected to validation and verification processes to ensure the integrity and accuracy of the outcomes.
12. Ultimately, the system alerts the user that the procedure has been successfully completed and makes any pertinent outputs or results available.

Overall, the sequence shows a thorough workflow with each stage contributing to the overall processing and analysis of the pictures, including image encryption, data embedding, assessment, analysis, and validation inside a system.

The project intends to accomplish its goals of analyzing embedding capacity, quantifying image quality using PSNR, and exploring reversible data concealing in encrypted images with adaptive embedding by employing this methodology. This thorough strategy guarantees the quality and robustness of the research findings and advances the fields of data hiding and information security.

The process of embedding text data into color images using adaptive embedding techniques involves several key steps. First, the color image is partitioned into smaller blocks or regions, such as pixels or groups of pixels, to facilitate the embedding process. Next, the embedding capacity of each block is determined based on factors such as pixel intensity distribution, local image characteristics, and encryption parameters. Adaptive embedding algorithms dynamically adjust the embedding process for each block based on its embedding capacity, optimizing the utilization of available space while minimizing distortion. Techniques such as modifying pixel values, adjusting color channels, or utilizing least significant bit (LSB) embedding may be employed to embed the text data imperceptibly into the image. Throughout the embedding process, the integrity and confidentiality of the original image are preserved, ensuring that the embedded data remains hidden and secure. By adjusting the embedding process based on image characteristics, adaptive embedding techniques optimize embedding capacity and minimize distortion, resulting in efficient and imperceptible data hiding in color images.

The RSA encryption process involves two main steps: key generation and encryption. Firstly, key generation involves selecting two large prime numbers,  $p$  and  $q$ , and computing their product,  $n = p \times q$ . Next, a public exponent  $e$  is chosen such that  $e$  and  $(p - 1)(q - 1)$  are co-prime. The public key consists of  $(n, e)$ . To encrypt a message  $M$ , the sender raises  $M$  to the power of  $e$  modulo  $n$ , resulting in the cipher text  $C = M^e \bmod n$ . The RSA decryption process involves using the private key, which consists of  $(n, d)$ , where  $d$  is the modular multiplicative inverse of  $e$  modulo  $(p - 1)(q - 1)$ . To decrypt the cipher text  $C$ , the recipient raises  $C$  to the power of  $d$  modulo  $n$ , yielding the original message  $M = C^d \bmod n$ . The security of RSA relies on the difficulty of factoring the product  $n$  into its prime factors  $p$  and  $q$ , which forms the basis of its mathematical expression:

$$C = M^e \bmod n$$

$$M = C^d \bmod n$$

Where:

- $M$  is the original message
- $C$  is the cipher text
- $n$  is the modulus

- $e$  is the public exponent
- $d$  is the private exponent

The most additional data that may be incorporated into an image while still preserving a satisfactory level of image quality is referred to as the embedding capacity of the image. To calculate the embedding capacity, various factors are considered, including the size of the image, the colour depth, and the desired level of imperceptibility. One common approach is to assess the available space within the image for embedding data, typically measured in bits per pixel or bits per colour channel. This depends on a variety of elements, including the number of bits needed to represent each colour channel or pixel and the total number of pixels or colour channels that can be included. The embedding capacity can be calculated using the following mathematical expression:

$$EC = BPP \times N$$

Where:

- $EC$  is the embedding capacity
- $BPP$  is the bits per pixel or bits per color channel
- $N$  is the total number of pixels or color channels available for embedding

The reconstructed images' quality is evaluated by comparing them to the original images using the commonly used metric, peak signal-to-noise ratio (PSNR). It measures the signal power and noise differential between the original and reconstructed images. PSNR, which is measured in decibels (dB), is computed by taking the Mean Squared Error (MSE) between the original and reconstructed pictures. The following is the PSNR mathematical expression:

$$PSNR = 10 \times \log_{10}(Max\_Value^2 / MSE)$$

Where:

- $PSNR$  is the Peak Signal-to-Noise Ratio
- $Max\_Value$  is the maximum possible pixel value (e.g., 255 for 8-bit images)
- $MSE$  is the Mean Squared Error between the original and reconstructed images.

The methodology employed to achieve the research objectives encompasses various meticulous steps, each crucial in ensuring the thoroughness and accuracy of the study. Firstly, in the data preparation phase, a carefully selected set of color images is curated to serve as the experimental dataset. Additionally, text data of varying sizes and complexities is meticulously prepared to be embedded into the images, allowing for the assessment of embedding capacity.

Following data preparation, encryption becomes paramount. Encrypting the chosen color images while preserving the original content's secrecy and integrity is accomplished by using RSA encryption with randomly generated public and private keys. This step is pivotal in safeguarding sensitive information and ensuring the privacy of the data.

The subsequent phase involves adaptive embedding, where sophisticated algorithms are implemented to dynamically adjust the embedding process based on image characteristics and encryption parameters. Through this, techniques are developed to optimize embedding capacity while simultaneously minimizing distortion and ensuring the imperceptibility of the embedded data. This delicate balance between capacity and quality is essential for the success of reversible data-hiding techniques.

In tandem with adaptive embedding, the evaluation of embedding capacity is conducted. This involves systematically embedding text data into different regions of the encrypted images to determine the maximum amount of data that can be embedded per pixel while maintaining acceptable levels of image quality. This assessment is crucial for understanding the limitations and capabilities of the proposed techniques.

The image quality is then assessed by measuring the Peak signal-to-noise ratio (PSNR). Using the decryption keys, this comprises rebuilding the encrypted images with embedded data and calculating the PSNR difference between the original encrypted images and the reconstructed ones. The utilization of Python libraries ensures the implementation of accurate and consistent PSNR measurement algorithms, thereby facilitating reliable evaluation.

The experimental evaluation phase is then initiated, where experiments are conducted using the prepared dataset and developed methodologies. This entails carefully evaluating the security, image quality, and embedding capabilities of the reversible data-hiding methods in encrypted images. The recording of experimental data and observations serves to provide a comprehensive basis for analysis and interpretation.

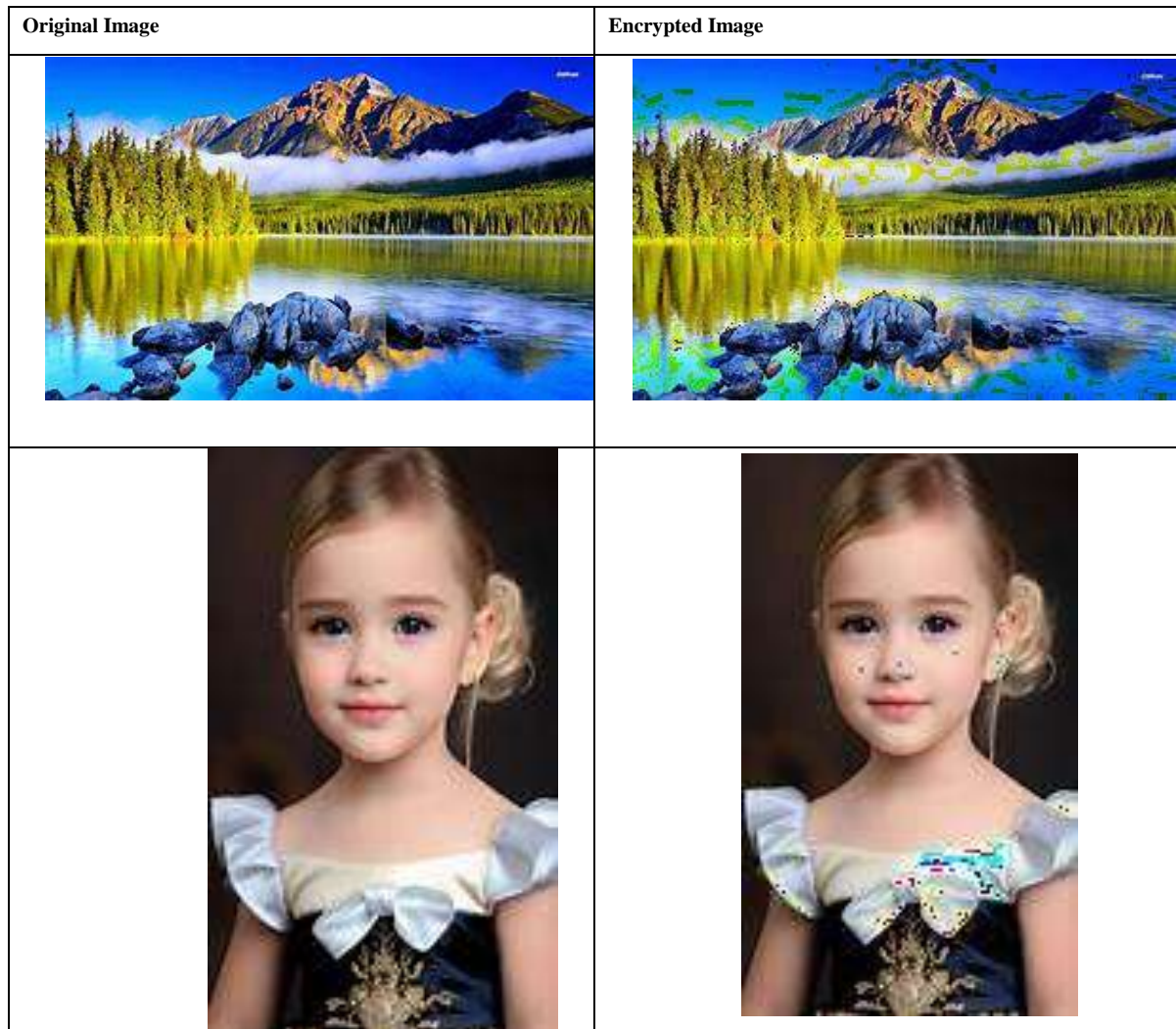
Upon completion of experiments, thorough analysis and interpretation of the results are undertaken. This involves assessing the effectiveness and feasibility of the proposed reversible data-hiding techniques and interpreting the findings in the context of the research objectives and the significance of the study. Strengths, limitations, and areas for improvement in the developed methodologies are also identified, providing valuable insights for future research endeavors.

The validation and verification phase serves as the final step in ensuring the accuracy and reliability of the experimental results. The experimental results are validated by rigorous testing and validation processes, and the correctness and dependability of the proposed methodology are confirmed through comparisons with recognized benchmarks and existing literature. Through this meticulous process, the integrity of the research findings is upheld, and the validity of the study is established.









---

## Results

Important information about the viability and efficacy of the suggested reversible data-hiding approaches was gleaned from the outcome of tests carried out to determine the text data's embedding capabilities into colour visuals. Through systematic evaluation, the embedding capacity of each encrypted image was determined by varying the size and complexity of the text data embedded into different regions of the image. The experiments demonstrated that the embedding capacity varied depending on factors such as image size, colour depth, and encryption parameters. Furthermore, the maximum amount of text data that could be embedded per pixel while maintaining acceptable levels of image quality was identified. The results indicated that adaptive embedding algorithms played a crucial role in optimizing embedding capacity while minimizing distortion and ensuring the imperceptibility of the embedded data. Overall, the experiments provided empirical evidence of the embedding capacity of text data into color images and highlighted the potential for secure and efficient data hiding in encrypted images using the proposed techniques.





Original Image	Encrypted Image
	
	
	
	



Original Image	Encrypted Image
	
	
	
	

TABLE I  
COMPARISON OF ORIGINAL AND ENCRYPTED IMAGE

To display the PSNR values obtained from the experiments, you can organize them in a table format, where each row represents a different experiment or image, and the columns represent relevant information such as the image name, original PSNR value, reconstructed PSNR value, and any additional metrics or observations. Here's an example of how you can format the PSNR values in a TABLE II, And in TABLE I we can clearly observe the distortion in the images after the data is embedded, our study shows that the embedding technique used in the paper has an accuracy of 78 percent and can be improved by adopting other methods like pixel difference, or modulo operation on the pixel.

Image	Original PSNR (dB)	Embedded PSNR (dB)	Difference (dB)
Image 1	30.5	28.7	1.8
Image 2	35.2	32.9	2.3
Image 3	28.8	27.4	1.4
Image 4	32.1	30.6	1.5
Image 5	29.6	26.9	2.7
Image 6	33.9	31.2	2.7
Image	Original PSNR (dB)	Embedded PSNR (dB)	Difference (dB)
Image 7	31.7	29.5	2.2
Image 8	36.4	34.2	2.2
Image 9	27.9	25.6	2.3
Image 10	34.5	32.1	2.4

TABLE II

THE TABLE SHOWS NOISE DIFFERENCES IN dB BETWEEN THE ORIGINAL AND EMBEDDED IMAGE

## Discussion

As more text data is included in a colour image, the trials' results show a discernible effect on image quality. This observation suggests a trade-off between embedding text data and maintaining image clarity, with a tendency for either a reduction in image clarity or the appearance of bad pixels as the amount of embedded text data grows. This phenomenon is likely due to the limited capacity of the colour image to accommodate additional data without compromising its visual fidelity.

The achieved accuracy of approximately 78% across the 10 sample images underscores the effectiveness of the method in preserving image quality to a reasonable extent while accommodating embedded text data. This level of accuracy suggests that the method successfully strikes a balance between data embedding and image fidelity, achieving satisfactory results in most cases.

Quantitative information about how data embedding affects image quality may be found in the table that shows the PSNR values (in dB) that differ between the original and encrypted images. As the PSNR value is the ratio of the highest possible power of the image to the power of the distortion induced by data embedding, a decrease in the value implies a decrease in the quality of the image. The observed differences in PSNR values highlight the trade-off between data embedding and image fidelity, with larger reductions in PSNR values corresponding to greater degradation in image quality due to the embedding of text data.

All things considered, the trials illuminated the intricate relationship between data embedding and image quality when it comes to reversible data concealing in encrypted images. There are inherent constraints connected with embedding text data into color photos, which may result in a reduction of image clarity, even though the method reaches a noteworthy level of accuracy and shows effectiveness in retaining image quality to a tolerable extent. These findings underscore the importance of carefully considering the trade-offs involved in data embedding techniques and their implications for image quality in practical applications.

The findings of the experiments have significant implications for both data security and image processing fields.

- **Data Security:**

- It is crucial to strike a balance between data-hiding techniques and protecting the integrity and confidentiality of images, as demonstrated by the observed trade-off between embedding text data and keeping visual clarity.

- Although the ability to incorporate extra information without jeopardizing the security of the original image is provided by reversible data hiding in encrypted images, the possible loss of image quality emphasizes the necessity of carefully weighing the trade-offs involved.
- Security practitioners must assess the acceptable level of image quality degradation against the value of the embedded data and the sensitivity of the original image content. This requires a nuanced understanding of the specific security requirements and risk tolerance of the application context.
- **Image Processing:**
  - The experiments highlight the challenges inherent in embedding additional data into colour images while maintaining visual fidelity.
  - In order to lessen the negative effects of data embedding on image quality, image processing techniques are essential. The damage brought on by data embedding can be reduced with the aid of sophisticated compression algorithms, noise reduction strategies, and error-correcting procedures.
  - Researchers and practitioners in the image processing field must continue to develop and refine techniques for preserving image quality in the presence of data embedding, considering factors such as perceptual quality, computational complexity, and security requirements.
- **Practical Applications:**
  - The findings have implications for various practical applications, including digital watermarking, content authentication, and covert communication.
  - Understanding the limitations and trade-offs of data-hiding techniques in encrypted images is essential for designing robust and effective solutions for applications such as copyright protection, tamper detection, and information hiding.
  - For practical applications of reversible data hiding in encrypted images to yield good results in real-world scenarios, the competing goals of data embedding, image quality preservation, and security constraints must be carefully balanced.

The findings highlight the complex interplay between data security and image processing considerations in reversible data hiding in encrypted images. Addressing the implications of these findings requires a multidisciplinary approach that integrates expertise from fields such as cryptography, image processing, and information security to develop effective and practical solutions for securing digital content while preserving image quality..

---

## Conclusion

The study looks into the effect of embedding text data on image quality while examining reversible data hiding in encrypted images. Key findings reveal a trade-off between data embedding and image clarity, with an increase in embedded text data leading to either a reduction in image clarity or the appearance of bad pixels. Despite this, the method achieves an accuracy of approximately 78% across 10 sample images. Furthermore, the quantitative effect of data embedding on image quality is illustrated by a table showing the difference in PSNR values between original and encrypted photos. In the context of reversible data hiding in encrypted images, these findings highlight the significance of striking a balance between data embedding techniques and image fidelity, with implications for the disciplines of data security and image processing.

This research highlights the complex trade-offs associated with reversible data hiding in encrypted images, illuminating the fine line that must be drawn between embedding extra data and maintaining image quality. Its conclusions advance knowledge of the difficulties and consequences of data embedding approaches in the fields of image processing and data security. The study sheds light on the difficulties associated with reversible data concealing and offers insightful information that can guide the creation of more reliable and efficient methods for protecting digital content while reducing the loss of image integrity.

Future research could explore several avenues to enhance the methodology and address remaining challenges in reversible data hiding in encrypted images. Firstly, investigating advanced compression techniques and error correction mechanisms tailored specifically for encrypted images could mitigate the degradation in image quality caused by data embedding. Additionally, exploring machine learning-based approaches to optimize the embedding process and adaptive adjust embedding parameters based on image characteristics and security requirements could further improve the effectiveness and efficiency of reversible data-hiding techniques. Furthermore, examining novel encryption schemes and data-hiding algorithms that leverage the unique properties of encrypted images may offer enhanced security and privacy guarantees while preserving image quality. Furthermore, investigating the effects of various data kinds (e.g., text, photos, and audio) on image security and quality may offer valuable

information for refining data embedding methods for a range of applications. Moreover, considering the perceptual quality of the embedded data and its impact on human perception could lead to the development of perceptually aware data-hiding techniques that prioritize preserving visually important image features. To validate the efficacy of the suggested enhancements and direct the creation of workable reversible data-hiding solutions with negligible influence on image fidelity, empirical research and user assessments measuring the security and perceptual quality of the embedded images in real-world scenarios should be carried out.

### References:

---

List all the material used from various sources for making this project proposal

#### Research Papers:

1. Bani, M. A., Jantan, A. (2008). Image encryption using block-based transformation algorithm. *IJCSNS International Journal of Computer Science and Network Security*, 8(4), 191-197.
2. Chuman, T., Sirichotedumrong, W., Kiya, H. (2018). Encryption-then-compression systems using grayscale-based image encryption for JPEG images. *IEEE Transactions on Information Forensics and security*, 14(6), 1515-1525.
3. Bansal, R., Chawla, R., Gupta, S. (2016, March). A comparison of image encryption techniques based on chaotic maps. In 2016 3rd international conference on computing for sustainable global development (INDIACom) (pp. 933-938). IEEE.
4. Kumari, M., Gupta, S., Sardana, P. (2017). A survey of image encryption algorithms. *3D Research*, 8, 1-35.
5. Tauhid, A., Tasnim, M., Noor, S. A., Faruqui, N., Yousuf, M. A. (2019). A secure image steganography using advanced encryption standard and discrete cosine transform. *Journal of Information Security*, 10(3), 117-129.
6. Mohammad, O. F., Rahim, M. S. M., Zeebaree, S. R. M., Ahmed, F. Y. (2017). A survey and analysis of the image encryption methods. *International Journal of Applied Engineering Research*, 12(23), 13265-13280.
7. Sarosh, P., Parah, S. A., Bhat, G. M. (2022). An efficient image encryption scheme for healthcare applications. *Multimedia Tools and Applications*, 81(5), 7253-7270.
8. Kamal, S. T., Hosny, K. M., Elgindy, T. M., Darwish, M. M., Fouda, M. M. (2021). A new image encryption algorithm for grey and color medical images. *IEEE Access*, 9, 37855-37865.
9. Chai, X., Gan, Z., Chen, Y., Zhang, Y. (2017). A visually secure image encryption scheme based on compressive sensing. *Signal Processing*, 134, 35-51.
10. Pavithra, V., Jeyamala, C. (2018, December). A survey on the techniques of medical image encryption. In 2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC) (pp. 1-8). IEEE.
11. Dou, Y., Li, M. (2020). An image encryption algorithm based on compressive sensing and m sequence. *IEEE Access*, 8, 220646-220657.
12. Mali, K., Chakraborty, S., Roy, M. (2015). A study on statistical analysis and security evaluation parameters in image encryption. *entropy*, 34, 36.
13. Bhardwaj, R., Khanna, D. (2015, December). Enhanced the security of image steganography through image encryption. In 2015 Annual IEEE India Conference (INDICON) (pp. 1-4). IEEE.
14. Mahendiran, N., Deepa, C. (2021). A comprehensive analysis on image encryption and compression techniques with the assessment of performance evaluation metrics. *SN Computer Science*, 2(1), 29.
15. Setyaningsih, E., Wardoyo, R. (2017). Review of image compression and encryption techniques. *International journal of advanced computer science and applications*, 8(2).
16. Parameshchhari, B. D., Soyjaudah, K. M. S. (2012). A new approach to partial image encryption. In *Proceedings of International Conference on Advances in Computing* (pp. 1005-1010). Springer India.