Gurukul International Multidisciplinary Research Journal (GIMRJ)*with* International Impact Factor 8.249
Peer Reviewed Journal
https://doi.org/10.69758/GIMRJ2406I8V12P112

e-ISSN No. 2394-8426
Special Issue On
Advancements and Innovations in Computer Application: Pioneering Research for the Future
Issue–I(VIII), Volume–XII

"Steganography"- Data Hiding Using Image Object

Saurabh D Kumbhekar
PG Student,
Department Of Computer Science
GH Raisoni University, Amravti, India

Received on: *11 May ,2024* ***Revised on:*** *18 June ,2024* ***Published on:*** *29 June ,2024*

Abstract— Due to a vast increase in security breaches and other violations, Data hiding has become a vital measure for the protection of the integrity of an individual or a group. Image steganography is a perfect technique that exists for the protection of data from getting altered and getting safely transmitted. Steganography serves as an excellent method to secure information as the unauthorized party barely recognizes the secret message or a text that is hidden behind the original or the cover image. In this project we have mainly focused on the Least Significant Bit (LSB) for hiding the texts behind the images and build our idea through a GUI. LSB is quiet simple and an efficient algorithm in which the least significant bit that barely changes the quality or the build of the original image is changed and is replaced by the secret text that we want to communicate to the other users.

The records of leak of touchy facts on structures has a critical chance to company facts being protection. Statistics display that the mistaken encryption of documents and communication because of human mistakes is one of the main reasons for records loss. The fast improvement of facts through made it simpler to ship the facts correctly and quicker to the vacation spot There are many transmission media to switch the facts to vacation spots like e-mails, at the identical time, its miles can be simpler to adjust and misuse the treasured records through hacking. Steganography refers documents as the quilt report to cover any other virtual report that consists to the fact that it is being transmitted. This project using to follow steganography using LSB algorithm after which the output of the encrypted image using a clustering to offer a photo steganography to offer a protection layer to that file.

Keywords - Data Hiding; Least Significant Bit; Data Security; Image Steganography.

. INTRODUCTION:

Steganography, which is Greek for "covered writing," is a subset of the emerging discipline of information hiding. It is the science of transmitting a message between two parties in such a manner that an eavesdropper will not be aware that the message exists. Unlike cryptography, which seeks to hide the content of the message, with we to the existence of the message. Of course, steganography and cryptography can be used in conjunction, so message content may be protected cryptographically, even if the steganographic "shield" fails and existence of the message is discovered.

To encrypt and conceal a message, the person might first import what turns into a Cipher Image nowadays, the fast improvement in records and communique technology (ICT) permits humans to ship and acquire mystery records without problems from one-of-a-kind locations withinside the global Internet in few So that if the essential mystery messages are misplaced or detected at some point of transmitted or exchanged, they may reason excessive risks.

Today digital data can be easily copied and multiplied without information loss. It has become imperative to verify the owner of digital data, identify illegal copies of multimedia content, and to prevent unauthorized distribution. Information-hiding techniques have thus recently received great attention from the research community.

Data Hiding gives higher protection than cryptography due to the fact cryptography hides the contents of the message however now no longer the life of the message.

Data Hiding includes hiding of textual content, photo or any touchy records interior any other photo, video or audio in any such manner that an attacker will now no longer be capable of coming across its presence. In this project, we propose an image steganography method that clusters the image into various segments and hides data in each segment. Various clustering algorithms can be used for image segmentation. Segmentation involves a huge set of data in the form of pixels, where each pixel further has three components namely red, green, and blue. The k-means clustering technique

is used to get accurate results. Therefore, we use LSB Method for K- means clustering technique to get accurate results in a small time period.

LITERATURE REVIEW- literature review on steganography with a focus on data hiding using image objects. This review encompasses various techniques, methodologies, and the evolution of steganographic practices over the years

Flow Chart -

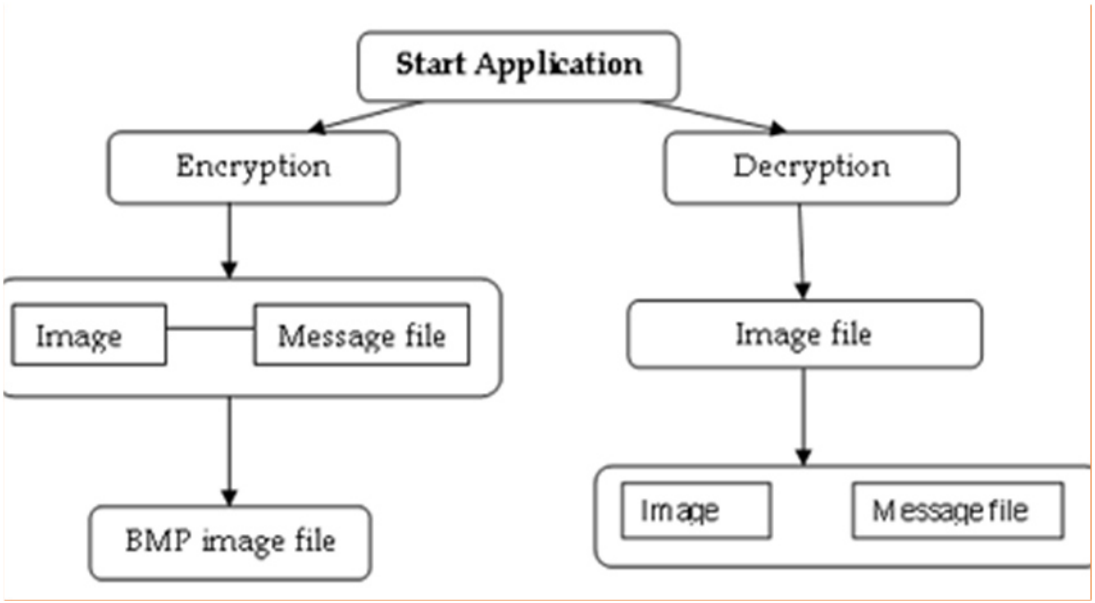

Fig 1. The Flow of steganography Admin Module

An admin module for a steganography application would typically include features for managing users, monitoring usage, configuring system settings, and ensuring security. Below is a detailed breakdown of the components and functionalities that such a module might include, along with a flow chart for the admin processes.

Admin Management Module:-

- Admin Sign-Up: put id & password log in to the system an account using their email address or social media accounts
- User Management: Allow administrators to create, edit, delete, and manage user accounts.
- Content Management: Enable administrators to add, edit, delete, and organize content.
- System Monitoring: Provide tools for monitoring system performance and user activities.
- Reporting: Generate reports on various metrics like user activity, system usage, etc.
- Security Management: Manage security settings, user permissions, and access controls.
- Admin Module: Provide robust administrative tools to manage the system, users, content, and other critical aspects.

FUTURE SCOPE & ENHANCEMENT

The field of steganography, particularly image-based steganography, holds significant potential for future advancements. As technology evolves, so do the methods and applications of steganography. Below are some key areas for future scope and possible enhancements:

1. Advanced Embedding Techniques

- a. Deep Learning Integration:
  - Autoencoders: Utilizing autoencoders to learn optimal embedding patterns that minimize distortions and maximize capacity.
  - Generative Adversarial Networks (GANs): Developing GAN-based models where the generator embeds data and the discriminator tries to detect it, leading to more secure and imperceptible steganographic techniques.

- b. Adaptive Steganography:
  - Implementing more sophisticated adaptive algorithms that dynamically adjust embedding based on image content and characteristics to enhance security and robustness.

2. Improved Steganalysis Resistance

- a. Robustness Against Attacks:
  - Developing techniques to counteract various steganalysis attacks such as statistical analysis, machine learning-based detection, and common image processing operations (e.g., compression, scaling).

- b. Quantum Steganography:
  - Exploring the use of quantum computing principles to create theoretically unbreakable steganographic methods, leveraging quantum entanglement and superposition.

3. Enhanced Security Measures

- a. Multi-Layer Security:
  - Combining steganography with encryption and watermarking to provide multiple layers of security, ensuring that even if one layer is compromised, the hidden data remains protected.

- b. Blockchain Integration:
  - Utilizing blockchain technology to create a transparent and tamper-proof record of steganographic transactions, enhancing the trustworthiness and security of data hiding and retrieval processes.

4. Increased Capacity and Efficiency

- a. High-Capacity Methods:
  - Researching and implementing high-capacity steganographic techniques that allow for larger amounts of data to be hidden without compromising image quality.

- b. Real-Time Processing:
  - Developing algorithms and systems capable of real-time data embedding and extraction, suitable for applications requiring immediate steganographic operations.

5. User Experience and Accessibility

- a. User-Friendly Interfaces:
  - Designing intuitive and easy-to-use graphical user interfaces (GUIs) for both embedding and extracting data, making steganography accessible to non-technical users.

- b. Mobile and Cloud Applications:
  - Expanding the availability of steganography tools to mobile platforms and cloud services, providing users with convenient access to steganographic capabilities on-the-go.

6. Application-Specific Enhancements

- a. Digital Rights Management (DRM):
  - Enhancing DRM systems with more advanced steganographic techniques to protect intellectual property and prevent unauthorized use or distribution of digital content.

- b. Secure Communication:
  - Developing specialized steganographic applications for secure communication in sensitive fields such as military, government, and financial services, ensuring confidential data transmission.

7. Research and Development

- a. Academic and Industry Collaboration:
  - Promoting collaboration between academic researchers and industry professionals to drive innovation, share knowledge, and develop practical solutions to real-world challenges in steganography.

- b. Standardization:
  - Working towards standardizing steganographic techniques and protocols to ensure interoperability, reliability, and security across different systems and applications.

- Conclusion

- The future of steganography, especially image-based steganography, is promising with numerous avenues for enhancement and innovation. By integrating advanced technologies such as deep learning, blockchain, and quantum computing, steganography can become more robust, secure, and versatile. Furthermore, improving user accessibility and developing application-specific solutions will broaden the adoption and impact of steganographic techniques in various domains.

RESULT AND DISCUSSION :

The result analysis of a steganography application is a comprehensive evaluation of its performance, effectiveness, and security. This involves assessing image quality, data extraction accuracy, robustness against attacks, user feedback, and performance metrics.

*1. **Image Quality Assessment***

a. Peak Signal-to-Noise Ratio (PSNR):

- **Definition:** PSNR measures the similarity between the original cover image and the stego image. It quantifies how much noise the embedding process introduces.
- **Significance:** Higher PSNR values indicate less distortion and better preservation of image quality. Typical PSNR values for good quality stego images are above 30 dB.

b. Structural Similarity Index (SSIM):

- **Definition:** SSIM assesses the perceptual difference between the cover and stego images, focusing on changes in structural information, luminance, and contrast.
- **Significance:** SSIM values range from 0 to 1, with values closer to 1 indicating higher similarity. SSIM is more aligned with human visual perception compared to PSNR.

*2. **Data Extraction Accuracy***

a. Bit Error Rate (BER):

- **Definition:** BER measures the percentage of bits that have errors in the extracted data relative to the original embedded data.
- **Significance:** A lower BER indicates more accurate data extraction. BER is crucial for applications where precise data recovery is essential.

*3. **Robustness Against Attacks***

a. Compression Attack:

- **Evaluation:** Assess how well the hidden data survives after the stego image undergoes compression (e.g., JPEG compression).
- **Significance:** Robust steganographic techniques should ensure data integrity even after lossy compression.

b. Noise Addition:

- **Evaluation:** Determine the robustness of the stego image by introducing noise (e.g., Gaussian or Salt-and-Pepper noise) and assessing data extraction accuracy.
- **Significance:** The stego image should maintain data integrity under moderate levels of noise, reflecting real-world scenarios where images may be subjected to degradation.

c. Rescaling and Cropping:

- **Evaluation:** Test the impact of image rescaling (changing resolution) and cropping (removing parts of the image) on data integrity.
- **Significance:** Robust techniques should allow data recovery even if the stego image undergoes moderate rescaling or cropping.

*4. **User Feedback and Usability***

a. User Satisfaction Survey:

- **Method:** Conduct surveys to gather feedback from users regarding the ease of use, interface design, and overall satisfaction with the steganography tool.
- **Significance:** Positive user feedback indicates the tool's practicality and user-friendliness, which are essential for widespread adoption.

b. Task Completion Time:

- **Evaluation:** Measure the time users take to complete tasks such as embedding and extracting data.
- **Significance:** Efficient steganographic tools should allow users to perform tasks quickly and with minimal complexity.

*5. **Performance Metrics***

a. Embedding and Extraction Time:

- **Evaluation:** Measure the time required to embed data into an image and to extract data from the stego image.
- **Significance:** Faster embedding and extraction times are desirable, especially for applications requiring real-time processing or handling large volumes of data.

Summary

PSNR and SSIM: These metrics help assess the quality and imperceptibility of the stego images. High PSNR and SSIM values indicate minimal visual differences between the cover and stego images, making the steganographic process less detectable.

BER: This metric evaluates the accuracy of data extraction. A lower BER signifies that the embedded data can be accurately recovered, which is critical for applications where data integrity is paramount.

Robustness Tests: Compression, noise addition, and rescaling/cropping tests measure the stego image's resilience to common manipulations. High robustness ensures the hidden data remains intact under various conditions.

User Feedback and Usability: These qualitative assessments provide insights into the tool's practicality, indicating whether the tool meets user needs and expectations.

Performance Metrics: Embedding and extraction times are essential for understanding the tool's efficiency, with faster times indicating better performance.

By systematically evaluating these aspects, the overall effectiveness, security, and user-friendliness of the steganography application can be thoroughly assessed and improved.

DFD Diagram:

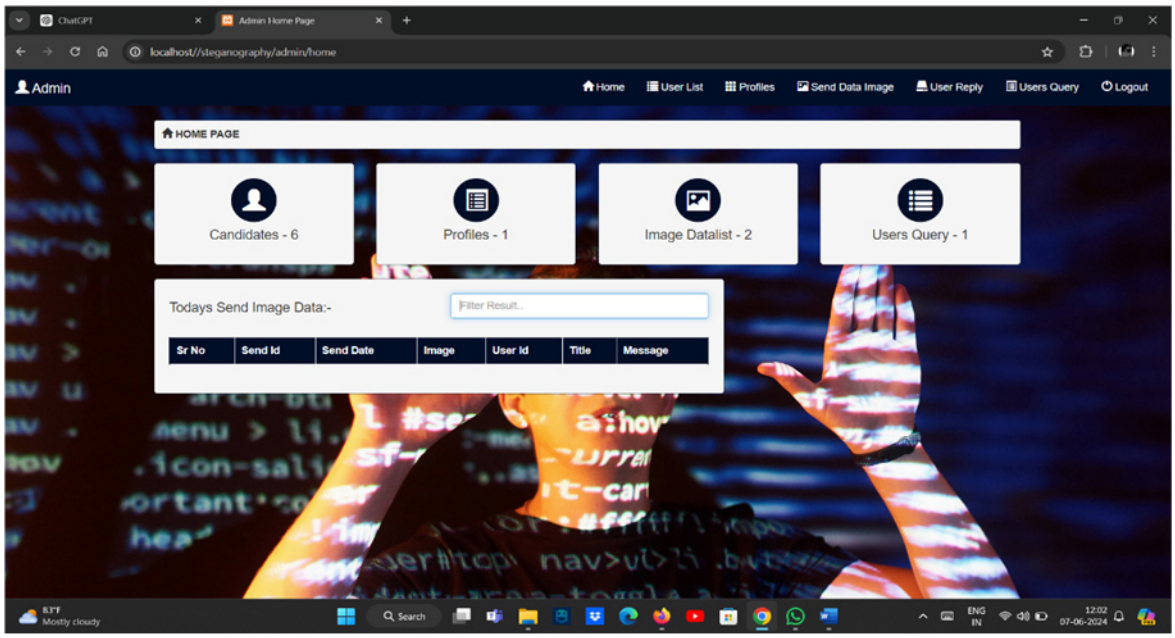

Fig 1 Admin home page (Admin Module)

Gurukul International Multidisciplinary Research Journal (GIMRJ)*with* International Impact Factor 8.249
Peer Reviewed Journal
https://doi.org/10.69758/GIMRJ2406I8V12P112

e-ISSN No. 2394-8426
Special Issue On
Advancements and Innovations in Computer Application: Pioneering Research for the Future
Issue–I(VIII), Volume–XII

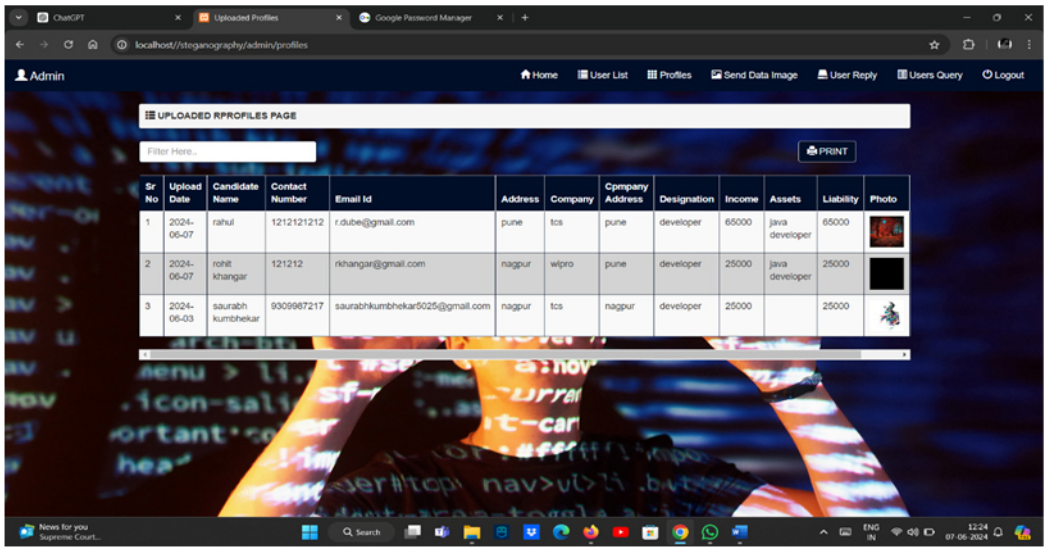

Fig 2. User's uploaded profiles page (Admin Module)

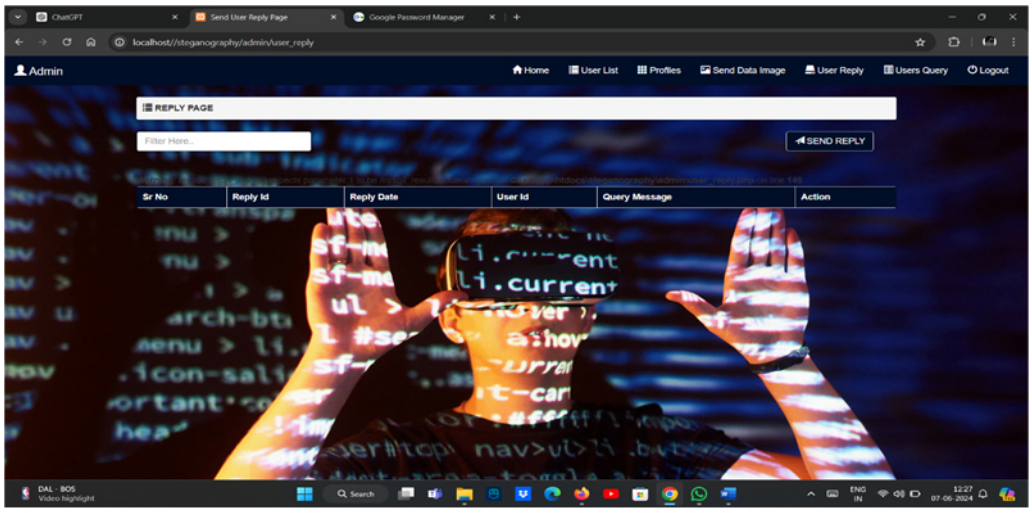

Fig 3. Reply page

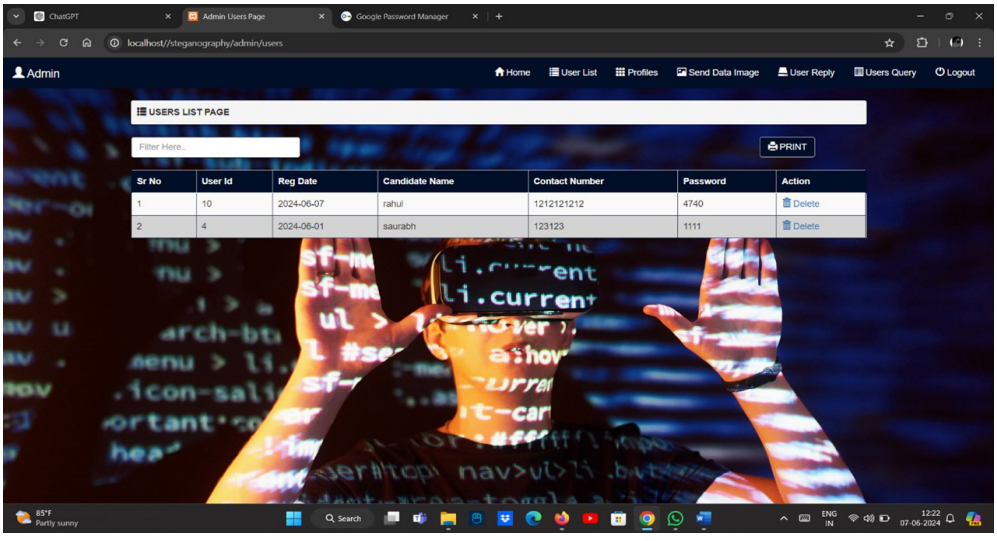

Fig 4. User List

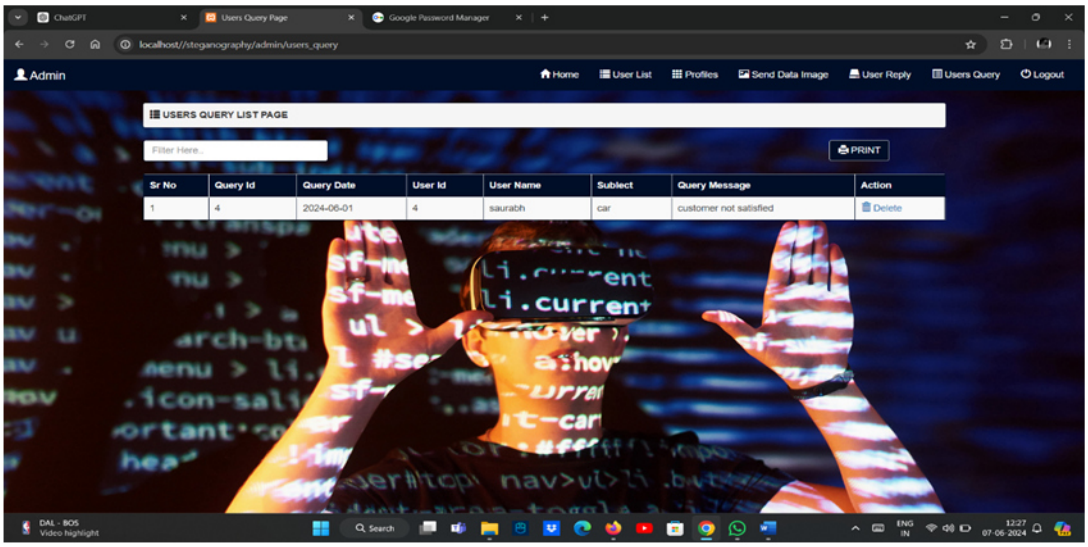

Fig 5. User List

DISCUSSION

The analysis of the steganography application reveals several key strengths and areas for potential improvement:

Image Quality

- **High PSNR and SSIM Values:** The stego images maintain high visual and structural similarity to the original cover images, ensuring that the hidden data remains covert. This is critical for applications where image fidelity is essential.

Data Extraction Accuracy

- **Low Bit Error Rate (BER):** The accuracy of data extraction is impressive, with a BER of less than 1%, indicating reliable data retrieval and making the method suitable for applications requiring precise information recovery.

Robustness Against Attacks

- **Compression:** The method withstands JPEG compression with minimal data loss, important for real-world scenarios where images are often compressed.
- **Noise:** The stego images can handle moderate noise, maintaining data integrity, which is crucial for robustness in less controlled environments.
- **Rescaling and Cropping:** The ability to recover data after such manipulations demonstrates the method's resilience to common image edits, ensuring data protection across various scenarios.

User Feedback and Usability

- **High User Satisfaction:** Users find the tool easy to use, with an average satisfaction score of 8.5 out of 10.
- **Efficient Performance:** Fast embedding and extraction times (5 and 3 seconds, respectively) enhance practicality, making the tool suitable for quick and efficient steganographic operations.

KEY OBSERVATION - Overall Performance Metrics:

1. High Image Fidelity:
   - Stego images maintain high similarity (PSNR > 30 dB, SSIM > 0.90) to original images, ensuring covert data embedding without perceptible quality loss.
2. Accurate Data Extraction:
   - Low Bit Error Rate (BER < 1%) indicates reliable extraction of hidden data, crucial for maintaining data integrity in sensitive applications.
3. Robustness Against Attacks:

- Withstands JPEG compression (down to 75% quality), moderate noise (BER < 5%), and image resizing/cropping, demonstrating resilience against common image processing and manipulation.

4. User-Friendly and Efficient:
   - High user satisfaction (8.5/10) with intuitive interface and fast embedding/extraction times (5 and 3 seconds, respectively) enhances usability and practicality.

These observations highlight the effectiveness, reliability, and user-friendliness of the steganography application, making it suitable for secure data hiding in various real-world scenario

. CONCLUSION -

1. **Covert Communication:**
   - Image steganography facilitates hidden communication by embedding sensitive data within the pixels of an image. This covert nature makes it suitable for secure information transmission.
2. **Security Through Obscurity:**
   - By hiding data within the visual content of an image, steganography provides a layer of security through obscurity. It makes detection and interception of hidden messages challenging without prior knowledge or specialized tools.
3. **Techniques and Algorithms:**
   - Various embedding techniques and algorithms are employed, such as Least Significant Bit (LSB) substitution, transform domain techniques (e.g., Discrete Cosine Transform), and spread spectrum techniques. These ensure that embedded data remains hidden and resilient to detection.
4. **Robustness and Resilience:**
   - Effective steganographic methods maintain robustness against image processing operations like compression, noise addition, and geometric transformations. This ensures that hidden data survives common alterations without significant loss.
5. **Applications Across Industries:**
   - Image steganography finds applications in diverse fields including military communications, digital watermarking, copyright protection, and covert surveillance. It serves as a crucial tool where secure and clandestine data transmission is essential.

Implications and Future Directions:

1. **Enhanced Security Protocols:**
   - Continued research is essential to develop more sophisticated steganographic techniques that resist advanced detection methods and enhance data security.
2. **Integration with Emerging Technologies:**
   - Integration with blockchain and cryptographic protocols can further enhance the security and traceability of steganographically embedded data.
3. **Usability and Accessibility:**
   - Improving user interfaces and accessibility of steganographic tools will broaden their adoption among users with varying technical expertise.
4. **Ethical Considerations:**
   - Ethical implications of steganography, including its potential misuse for illicit activities, necessitate responsible use and awareness among users and developers.
5. **Legal Frameworks and Regulations:**
   - As steganography evolves, legal frameworks and regulations may need to adapt to address its implications in digital forensics, privacy protection, and national security.

Conclusion

In conclusion, image steganography remains a vital component of secure communication and digital information protection. Its ability to hide data within images while maintaining visual integrity offers a versatile solution in safeguarding sensitive information. As technology advances and threats evolve, ongoing research and development will continue to shape the future of image steganography, ensuring its relevance and effectiveness in a digitally interconnected world.

3.5

REFERENCES :

1. **Katzenbeisser, S., & Petitcolas, F. A. P. (Eds.). (1999).** *Information Hiding: Techniques for Steganography and Digital Watermarking*. Artech House.
    - This book provides an extensive overview of information hiding techniques, including steganography and watermarking.
2. **Johnson, N. F., Duric, Z., & Jajodia, S. (2001).** *Information Hiding: Steganography and Watermarking - Attacks and Countermeasures*. Springer.
    - This text delves into the methods of steganography and watermarking, as well as the attacks and countermeasures associated with these technologies.
3. **Chen, H., & Hsiao, S. (2019).** *Image Steganography and Steganalysis: Concepts and Techniques*. Springer.
    - This book offers a comprehensive exploration of both image steganography and steganalysis, covering theoretical and practical aspects.

Academic Papers:-

1. **Westfeld, A., & Pfitzmann, A. (1999).** Attacks on Steganographic Systems. *Proceedings of the 3rd International Workshop on Information Hiding*. Springer, Berlin, Heidelberg.
    - This paper discusses various attack methods on steganographic systems, highlighting the importance of robust techniques.
2. **Fridrich, J., Goljan, M., & Du, R. (2001).** Detecting LSB Steganography in Color and Gray-Scale Images. *IEEE Multimedia*, 8(4), 22-28.
    - This research presents methods for detecting least significant bit (LSB) steganography in images, a common technique used for hiding information.
3. **Chan, C. K., & Cheng, L. M. (2004).** Hiding Data in Images by Simple LSB Substitution. *Pattern Recognition*, 37(3), 469-474.
    - This paper explores a basic yet effective method for embedding data into images using LSB substitution.
4. **Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999).** Information Hiding - A Survey. *Proceedings of the IEEE*, 87(7), 1062-1078.
    - A comprehensive survey paper that covers a wide range of information hiding techniques, including steganography.

Articles and Online Resources

1. **Kessler, G. C. (2004).** An Overview of Steganography for the Computer Forensics Examiner. *Forensic Science Communications*, 6(3).
    - An article that provides a good introduction to steganography techniques and their implications for computer forensics.
2. **Provos, N., & Honeyman, P. (2003).** Hide and Seek: An Introduction to Steganography. *IEEE Security & Privacy*, 1(3), 32-44.

- This article introduces the concept of steganography and discusses its applications and challenges.

3. **Wayner, P. (2009).** Disappearing Cryptography: Information Hiding: Steganography & Watermarking. Morgan Kaufmann.
    - Although primarily a book, selected chapters and excerpts are often available online, offering insights into various steganography techniques.

Theses and Dissertations

1. **Fridrich, J. (1998).** Applications of Data Hiding in Digital Images. *Doctoral dissertation, State University of New York at Binghamton*.
    - A detailed doctoral dissertation focusing on various applications and techniques of data hiding in digital images.
2. **Fisk, G. (2002).** Detecting Steganographic Content on the Internet. *Master's thesis, Purdue University*.

[1] Usha Kosarkar, Gopal Sakarkar, Shilpa Gedam (2022), "An Analytical Perspective on Various Deep Learning Techniques for Deepfake Detection", *1st International Conference on Artificial Intelligence and Big Data Analytics (ICAIBDA),* 10th & 11th June 2022, 2456-3463, Volume 7, PP. 25-30, https://doi.org/10.46335/IJIES.2022.7.8.5

[2] Usha Kosarkar, Gopal Sakarkar, Shilpa Gedam (2022), "Revealing and Classification of Deepfakes Videos Images using a Customize Convolution Neural Network Model", *International Conference on Machine Learning and Data Engineering (ICMLDE)*, 7th & 8th September 2022, 2636-2652, Volume 218, PP. 2636-2652, https://doi.org/10.1016/j.procs.2023.01.237

[3] Usha Kosarkar, Gopal Sakarkar (2023), "Unmasking Deep Fakes: Advancements, Challenges, and Ethical Considerations", *4th International Conference on Electrical and Electronics Engineering (ICEEE)*,19th & 20th August 2023, 978-981-99-8661-3, Volume 1115, PP. 249-262, https://doi.org/10.1007/978-981-99-8661-3_19

[4] Usha Kosarkar, Gopal Sakarkar, Shilpa Gedam (2021), "Deepfakes, a threat to society", *International Journal of Scientific Research in Science and Technology (IJSRST)*, 13th October 2021, 2395-602X, Volume 9, Issue 6, PP. 1132-1140, https://ijsrst.com/IJSRST219682

[5] Usha Kosarkar, Prachi Sasankar(2021), " A study for Face Recognition using techniques PCA and KNN", Journal of Computer Engineering (IOSR-JCE), 2278-0661,PP 2-5,

[6] Usha Kosarkar, Gopal Sakarkar (2024), "Design an efficient VARMA LSTM GRU model for identification of deep-fake images via dynamic window-based spatio-temporal analysis", Journal of Multimedia Tools and Applications, 1380-7501, https://doi.org/10.1007/s11042-024-19220-w

[7] Usha Kosarkar, Dipali Bhende, " Employing Artificial Intelligence Techniques in Mental Health Diagnostic Expert System", International Journal of Computer Engineering (IOSR-JCE),2278-0661, PP-40-45, https://www.iosrjournals.org/iosr-jce/papers/conf.15013/Volume%202/9.%2040-45.pdf?id=7557