International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Reversible Data Encrypted Images with Hiding Based on Progressive Recovery

Dr. E. Ranjith[1], Mr. P. Madhan[2]

[1]MCA., M. Phil., Ph. D. Assistant. Prof. Department of MCA & Krishnasamy College of Engineering & Technology
[2](MCA) Department of MCA & Krishnasamy College of Engineering & Technology

ABSTRACT

In this project, we expand the LSB matching revisited image steganography and propose an edge adaptive scheme which can select the embedding regions according to the size of secret message and the difference between two consecutive pixels in the cover image. For lower embedding rates, only sharper edge regions are used while keeping the other smoother regions as they are. When the embedding rate increases, more edge regions can be released adaptively for data hiding by adjusting just a few parameters.

1.INTRODUCTION

Steganography is indeed a technique used for secret communication, where the focus is on hiding the existence of the communication rather than making the message unintelligible to unauthorized individuals, as cryptography does. Instead of encrypting the message itself, steganography involves concealing the message within a cover medium such as digital images, videos, sound files, or other computer files.

The cover medium, also known as a carrier, contains perceptually irrelevant or redundant information that can be used to hide the secret message. By embedding the secret message into the cover medium, a stego image or stego file is created. The goal is to ensure that the stego image or file appears indistinguishable from a regular cover medium, without any detectable artifacts that could reveal the presence of a hidden message.

The process of embedding a secret message into the cover medium involves manipulating the cover medium in a way that the changes are subtle and do not draw attention. Various techniques are employed in steganography to achieve this, such as modifying the least significant bits of pixel values in an image or altering the amplitude of certain frequency components in an audio signal.

2.LITERATURE SURVEY

1) Digital steganography: Hiding data within data

AUTHORS: D. Artz

Digital steganography is a technique used to hide data within other data in an inconspicuous manner. The objective is to ensure that unintended recipients do not suspect the presence of hidden data. This article emphasizes the importance of being aware of digital steganography technology and its implications, as it is expected to play a growing role in society alongside the development of privacy concerns in digital communication. It also highlights the ethical considerations surrounding the use of steganography and steganalysis, emphasizing that steganography complements encryption rather than replacing it. The focus is on keeping the existence of a message hidden rather than the content itself.

2) Advanced high dynamic range imaging: theory and practice

AUTHORS: F. Banterle, A. Artusi, K. Debattista, and A. Chalmers

Traditionally, photography and computer graphics approached the issue of high dynamic range (HDR) differently. However, recent advancements and collaborative efforts have bridged the gap between these disciplines, leading to the development of powerful tools for creating intricate, captivating, and lifelike images. This book serves as a practical introduction to the emerging field of HDR imaging, which combines the principles of photography and computer graphics.

The book equips readers with detailed equations and code, providing them with the necessary tools to explore and experiment with new techniques for generating visually compelling images. It offers insights into the unified approaches that have emerged in the past decade, enabling professionals and enthusiasts to achieve better results in capturing and representing the dynamic range of light in their visual creations.

3)High Dynamic Range Imaging: Acquisition, Display, and Image-Based Lighting

Authored :E. Reinhard, G. Ward, S. Pattanaik, P. Debevec, W. Heidrich, and K. Myazkowski.

It serves as a comprehensive resource that covers various aspects of HDRI (High Dynamic Range Imaging) technology, making it the first of its kind to provide a complete description of the subject. The book delves into a wide range of topics, including the different capture devices used in HDRI, tone reproduction techniques, and image-based lighting methods.

The techniques outlined in the book empower readers to produce images that possess a dynamic range much closer to what is observed in the real world. This enhanced dynamic range results in an unparalleled visual experience, offering a more realistic and immersive representation of the captured scene. Whether working in computer graphics, film, video, photography, or lighting design, this book serves as both an introductory guide and an authoritative technical reference for anyone involved in working with images

4) The RADIANCE lighting simulation and rendering system

AUTHORS: G. J. Ward

that focuses on a physically-based rendering system designed specifically for lighting design and architecture. The system employs a light-backwards ray-tracing technique and extends it to efficiently solve the rendering equation under various conditions. It encompasses specular, diffuse, and directional-diffuse reflection, as well as transmission in any combination, at different levels and in complex environments with curved geometries.

The simulation presented in the paper integrates deterministic and stochastic ray-tracing techniques to strike a balance between speed and accuracy in both local and global illumination methods. The paper provides an overview of some intriguing techniques and refers to more detailed descriptions elsewhere for further exploration. Additionally, successful applications of this freely available software by other individuals or organizations are showcased, demonstrating its practicality and value in real-world scenarios.

5) LogLuv encoding for full-gamut, high-dynamic range images

AUTHORS: G. W. Larson

In this paper, the authors highlight the significant difference between the dynamic range and color gamut capabilities of the human eye compared to typical computer monitors. While the human eye can perceive luminance over a range of approximately 10,000:1 and distinguish about 10,000 colors at a given brightness, computer monitors fall short with a luminance range of less than 100:1 and only covering around half of the visible color gamut. Despite this discrepancy, most digital image formats are designed to align with the capabilities of conventional displays rather than considering the characteristics of human vision.

To address this limitation, the authors propose a compact encoding method specifically designed for high dynamic range (HDR) color images. This encoding format serves as an alternative to conventional RGB images and employs a different representation scheme. Instead of directly encoding RGB values, color pixels are encoded using logarithmic luminance values and CIE (u',v') chromaticity coordinates. This approach allows for the preservation and efficient storage of the extensive dynamic range and color information present in HDR images.

System Modules :

MODULES:

1 Encryption module

2 Decryption module

ENCRYPTION MODULE

The Encryption module of the system incorporates a Key file component, allowing the user to specify a key file along with a password for enhanced security. This key file serves as a crucial element in the encryption process.

In addition to manually typing the data, the user has the option to upload the data from a file. By clicking the browse button, an open file dialog box appears, enabling the user to select the desired secret message file from their system.

To proceed with the encryption process, the user is required to select an image file. Clicking the image button opens another open file dialog box, specifically for choosing a BMP file. This image file will serve as the cover or carrier for hiding the secret message.

Once the secret message file and the cover image file are selected, the user can initiate the hiding process by clicking the Hide button. This triggers the application of the LSB (Least Significant Bit) matching revisited technique, which conceals the secret data or message within the picture while ensuring the visual appearance of the image is preserved.

By leveraging the LSB matching revisited technique, the system embeds the secret data or message in a manner that is inconspicuous and not easily detectable. This technique ensures the security and confidentiality of the hidden information within the image.

DECRYPTION MODULE

The Decryption module is designed as the counterpart to the Encryption module, providing the means to retrieve the hidden message from an encrypted image.

Similar to the Encryption process, the user is required to specify the Key file used during the encryption phase.

Once the Key file is provided, the user can select the encrypted image file that contains the hidden message. This file is typically generated using the Encryption is to the module of the system.

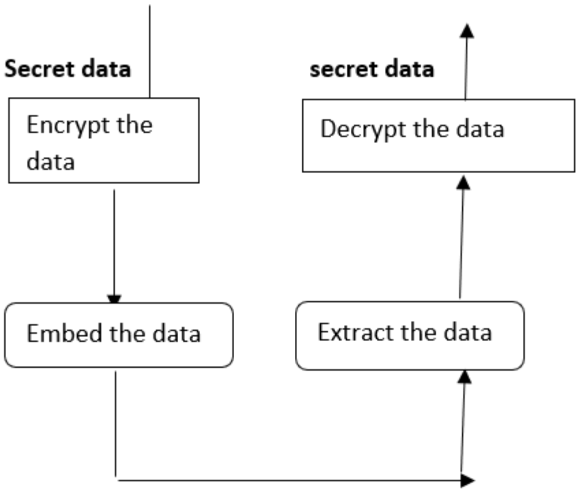
After selecting the encrypted image file.

The extracted message can be displayed in the designated text area within the application, allowing the user to view the concealed information directly

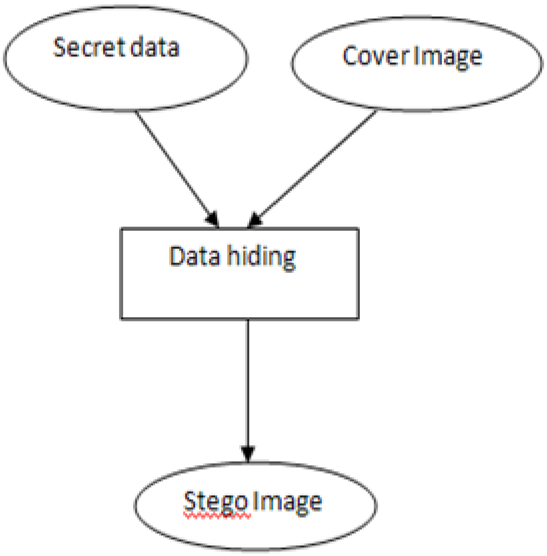
By following these steps, the Decryption module enables users to retrieve and access the hidden message from an encrypted image using the specified Key file, providing a secure and controlled decryption process.

Regenerate response

4. ARCHITECTURE DIAGRAM



5. WORK FLOW DIAGRAM



6. ACTIVITY DIAGRAM

Activity diagrams provide a visual representation of stepwise workflows, activities, and actions, incorporating features such as choice, iteration, and concurrency. Within the Unified Modeling Language (UML), activity diagrams serve as a means to describe the sequential operational workflows of system components, both in terms of business and operational processes. By illustrating the flow of control, activity diagrams offer a comprehensive overview of how activities progress throughout a system or process. They are a valuable tool for modeling and understanding complex systems, aiding in the analysis, design, and documentation of workflows.

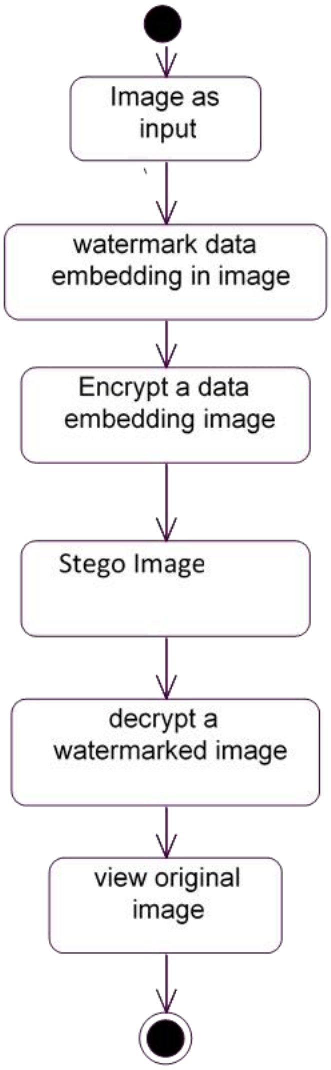


Image as input
watermark data embedding in image
Encrypt a data embedding image
Stego Image
decrypt a watermarked image
view original image

7. CONCLUSION

Among various steganographic techniques, the Adaptive LSB (Least Significant Bit) substitution method has emerged as an efficient and secure approach for hiding data within an image.

In this project, a diverse range of images has been employed as cover images for steganography purposes. The Adaptive LSB technique has been leveraged to effectively embed different types of data, including video, audio, and other file formats, with a high level of accuracy.

Compared to traditional LSB techniques, the Adaptive LSB technique excels in both security and accuracy aspects. By intelligently adapting the LSB substitution based on the characteristics of the cover image, this method ensures efficient data hiding while minimizing the visual impact on the image. This approach enhances the security of the hidden data by making it harder to detect or recover without proper knowledge of the embedding algorithm

REFERENCES.

1. Weiqi Luo, Fangjun Huang, Jiwu Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited," IEEE Transactions on Information Forensics and Security, Vol. 5, No. 2, June 2010.

2. C.C. Chang, H.-W. Tseng, "A Steganographic method for digital images using side match," Pattern Recognition Letters, 25, 1431-1437, 2004.

3. C.K. Chan, L.M. Cheng, "Hiding data in images by simple LSB Substitution," Pattern Recognition, 37, 469-474, 2004.

4. C.C. Chang, M.H. Lin, Y.-C. Hu, "A fast and secure image hiding scheme based on LSB substitution," International Journal of Pattern Recognition and Artificial Intelligence, 16(4), 399-416, 2004.

5. R.Z. Wang, C.F. Lin, J.C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm," Pattern Recognition, 34, 671-683, 2001.

6. Suk-Ling Li, Kai-Chi Leung, L.M. Cheng, Chi-kwong Chan, "Performance Evaluation of a Steganographic Method for Digital Images Using Side Match," ICICIC 2006, IS16-004, Aug 2006.

7. J. Mielikainen, "LSB matching revisited," IEEE Signal Processing Letters, vol. 13, no. 5, pp. 285-287, May 2006.

8. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," in Proc. 3rd Int. Workshop on Information Hiding, 1999, vol. 1768, pp. 61-76.

9. J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color and grayscale images," IEEE Multimedia, vol. 8, no. 4, pp. 22-28, Oct. 2001.

10. S. Dumitrescu, X. Wu, and Z. Wang, "Detection of LSB steganography via sample pair analysis," IEEE Transactions on Signal Processing, vol. 51, no. 7, pp. 1995-2007, Jul. 2003.

11. D. Ker, "A general framework for structural steganalysis of LSB replacement," in Proc. 7th Int. Workshop on Information Hiding, 2005, vol. 3427, pp. 296-311.

12. D. Ker, "A fusion of maximum likelihood and structural steganalysis," in Proc. 9th Int. Workshop on Information Hiding, 2007, vol. 4567, pp. 204-219.

13. J. Harmsen and W. Pearlman, "Steganalysis of additive-noise modelable information hiding," Proc. SPIE Electronic Imaging, vol. 5020, pp. 131-142, 2003.

14. D. Ker, "Steganalysis of LSB matching in grayscale images," IEEE Signal Processing Letters, vol. 12, no. 6, pp. 441-444, Jun. 2005.

15. F. Huang, B. Li, and J. Huang, "Attack LSB matching steganography by counting alteration rate of the number of neighborhood gray levels," in Proc. IEEE Int. Conf. Image Processing, Oct.