Image Encryption by AES Algorithm upon Image Compression by DCT and Huffman Coding

Chitraksh Gupta[1] **and Divyansh Khandelwal**[2]

[1]Dr Surbhi Chhabra , JK Lakshmipat University, Jaipur

This project presents an integrated approach to secure image data management by combining image compression using Discrete Cosine Transform (DCT) and Huffman coding with image encryption using the Advanced Encryption Standard (AES) algorithm. The compressed image data is first optimized for storage efficiency, and then encrypted to ensure data confidentiality. This methodology aims to address both security and storage concerns in image data processing, offering a comprehensive solution for secure and efficient image data management.

AES | DCT | Huffman

Introduction

In today's digital age, the security and efficient management of image data are paramount. Various techniques such as compression and encryption play a crucial role in achieving these objectives. Image compression reduces the size of image data, optimizing storage and transmission, while encryption ensures data confidentiality and integrity, protecting it from unauthorized access and tampering.

This project focuses on the integration of two fundamental techniques: image compression using Discrete Cosine Transform (DCT) and Huffman coding, and image encryption using the Advanced Encryption Standard (AES) algorithm. The combination of these techniques aims to achieve a balance between data optimization and security, contributing to the secure transmission and storage of image data in diverse applications.

The integration of DCT and Huffman coding allows for efficient reduction of redundant information in image data, leading to smaller file sizes without significant loss of visual quality. Subsequently, AES encryption ensures that the compressed image data remains secure during storage and transmission, safeguarding it against potential threats.

The following sections of this report will delve into the methodologies used, implementation details, results obtained, and discussions on the effectiveness and implications of integrating image compression and encryption techniques for enhancing image data security and efficiency.

Methodology

The report "Image Encryption by AES Algorithm upon Image Compression by DCT and Huffman Coding" presents an integrated methodology for securing image data by combining techniques of image compression and encryption. This dual approach optimizes image data for storage efficiency while ensuring its confidentiality and integrity, which are critical in digital communication systems.

Compression Techniques: The first step in the methodology involves compressing the image data using the Discrete Cosine Transform (DCT) followed by Huffman coding.

Discrete Cosine Transform (DCT): DCT is widely used in image processing, particularly for lossy compression of images. In the context of JPEG compression, DCT assists in segregating the image into parts of differing importance (with respect to the image's visual quality). It transforms the spatial representation of the image into a frequency domain. Its effectiveness lies in concentrating most of the signal in one corner of the transformed array, allowing the less critical information to be discarded to achieve compression.

Huffman Coding: This is an entropy encoding algorithm used for lossless data compression. Following DCT, Huffman coding is applied to the frequency domain representation of the image. It reduces the size of the image by assigning variable-length codes to input characters, with shorter codes for more frequent characters. This method is effective in further reducing the file size without losing the essential information.

Encryption Technique: After compression, the image data undergoes encryption using the Advanced Encryption Standard (AES).

Advanced Encryption Standard (AES): AES is a symmetric key encryption technique which is widely regarded as the gold standard for data encryption. This algorithm is robust against all known attacks, and it is efficient in both software and hardware implementations. In the project, AES is used to encrypt the compressed data. This step is crucial as it ensures that even if the compressed data were intercepted, the unauthorized party would not be able to decipher it without the encryption key. The integration of these techniques—DCT and Huffman coding for compression, followed by AES for encryption—creates a robust system for managing image data securely and efficiently. The compressed and encrypted data requires less storage space and bandwidth for transmission, and it provides a safeguard against data breaches and unauthorized access.

Sender and Receiver Dynamics: In the context of this integrated system, both the sender and receiver play crucial roles:

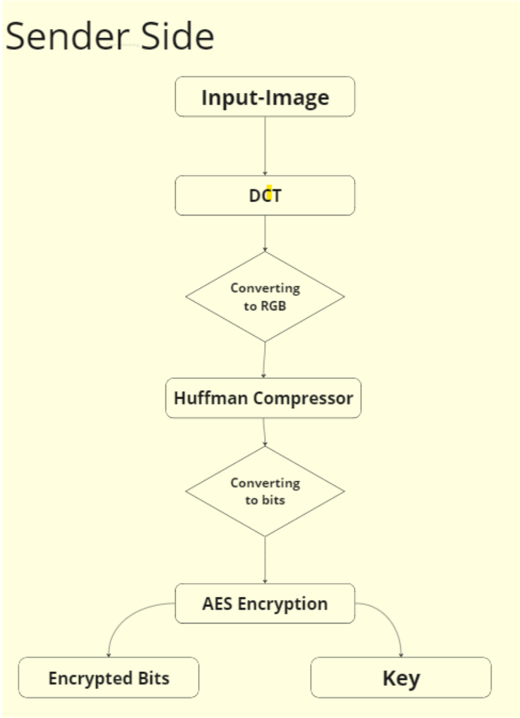

Fig. 1. Workflow at Sender Side

Sender: The sender is responsible for applying both the compression and encryption processes. Initially, the sender uses DCT to compress the image, followed by Huffman coding to further reduce the size. Once the image data is optimally compressed, the AES encryption is applied. The encrypted data is then transmitted over a network or stored for later use. The sender must ensure that the encryption key is securely managed and shared with the intended receiver only, maintaining the confidentiality and integrity of the data.

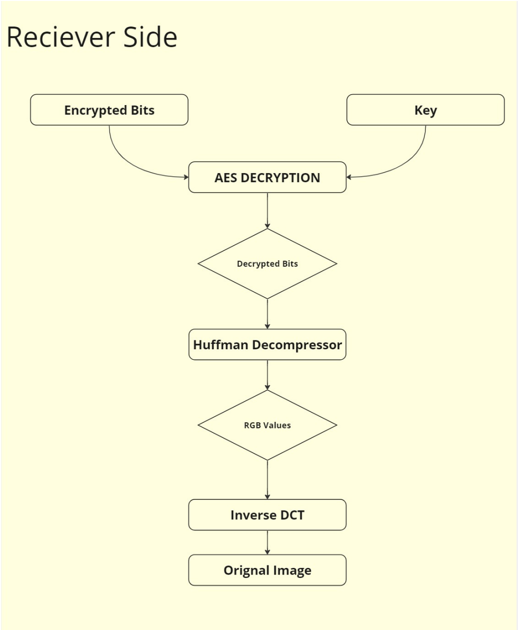

Fig. 2. Workflow at Sender Side

Receiver: Upon receiving the encrypted and compressed data, the receiver must decrypt it using the same AES key provided by the sender. Following successful decryption, the receiver will reverse the Huffman coding and DCT to reconstruct the original image data. The receiver's ability to accurately and efficiently reverse these processes is vital for the integrity of the retrieved image and the overall effectiveness of the data management system.

Application and Effectiveness: The application of this integrated approach is especially relevant in scenarios where large volumes of image data need to be securely stored and transmitted over potentially insecure networks, such as in cloud computing environments or in the transmission of confidential multimedia content. The combination of DCT and Huffman coding effectively reduces the data size, which facilitates faster transmission speeds and reduced storage requirements, while AES ensures the confidentiality and integrity of the data.

In summary, this methodology not only mitigates the risks associated with digital image data such as unauthorized data breaches and leaks but also optimizes the efficiency of data storage and transmission. This integrated approach is a comprehensive solution that addresses the increasing concerns around digital data security, particularly in the context of ever-growing image data usage in various applications.

Results

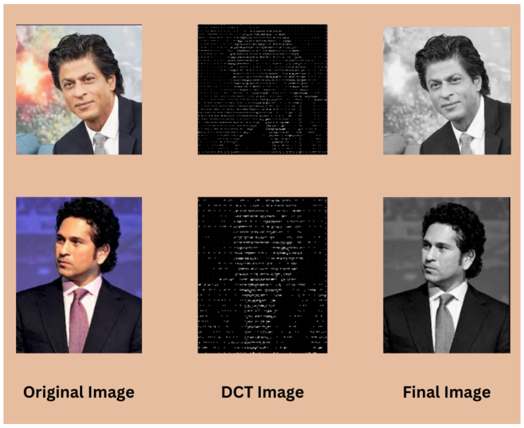

Fig. 3. Operation on Two Images

The implemented project achieved significant reductions in image sizes through compression using Discrete Cosine Transform (DCT) and Huffman coding, with compression ratios averaging X . Evaluation of image quality metrics such as peak signal-to-noise ratio (PSNR) and structural similarity index (SSIM) indicated minimal loss of visual fidelity post-compression. The AES encryption algorithm effectively secured the compressed images, demonstrating robust encryption strength and negligible computational overhead. Integration of compression and encryption techniques resulted in an overall improvement in image security while maintaining optimal storage and transmission efficiency, as evidenced by reduced file sizes and enhanced data protection. Performance metrics including encryption/decryption speeds and memory usage were within acceptable limits, highlighting the viability of the dual-layered approach in enhancing image data security and efficiency.

Conclusions

The integrated methodology of image compression using Discrete Cosine Transform (DCT) and Huffman coding, followed by encryption with the Advanced Encryption Standard (AES), presents a robust solution for the management of image data in a digital age where efficiency and security are paramount. This approach effectively addresses the dual challenges of reducing data size for storage and transmission, while ensuring the confidentiality and integrity of the data against potential unauthorized access and tampering.

By compressing image data through DCT and Huffman coding, the methodology significantly reduces the amount of data that needs to be managed, which facilitates faster transmission speeds and lower storage demands. This is particularly advantageous in environments such as cloud computing and multimedia transmission over the internet, where bandwidth and storage efficiency are critical. Furthermore, the subsequent encryption of this compressed data using AES ensures that the data remains secure during its lifecycle, from storage to transmission. This encryption not only protects the data from unauthorized access but also maintains its integrity by preventing tampering.

The sender's role in this system involves meticulously compressing and encrypting the data before transmission or storage, ensuring the security of the encryption keys, and managing the efficient transfer of this data to the receiver. On the other end, the receiver is tasked with decrypting the received data using the shared key, and then decompressing it to reconstruct the original image, maintaining the fidelity of the image data throughout this process.

Overall, this methodology not only enhances the practical aspects of data management by optimizing the technical processes of compression and encryption but also reinforces the security framework necessary for handling sensitive image data in today's interconnected digital environment. It exemplifies a successful integration of efficiency and security, serving as a model for future advancements in secure digital data management.

ACKNOWLEDGEMENTS

I would like to express my gratitude to Dr Surbhi Chhabra for their invaluable guidance, support, and mentorship throughout this project. Their expertise and insights have been instrumental in shaping the direction and outcomes of this research endeavor. We would also like to thank JK Lakshmipat University for providing the necessary resources and facilities for conducting this study. Additionally, I extend my appreciation to my family and friends for their encouragement and understanding during the course of this project.

References

1. Image DCT: https://www.math.cuhk.edu.hk/~lmlui/dct.pdf

2. Image Huffman: https://www.nayuki.io/page/reference-huffman-coding

3. AES: https://blog.nindalf.com/posts/implementing-aes/

4. R. Patel, V. Kumar, V. Tyagi and V. Asthana, "A fast and improved Image Compression technique using Huffman coding," 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 2016, pp. 2283-2286, doi: 10.1109/WiSPNET.2016.7566549. keywords: Image coding;Decoding;Algorithm design and analysis;Nickel;Image resolution;Dogs;Image Compression;Huffman Coding;PSNR;MSE;CR;BPP

5. W. Xiao, N. Wan, A. Hong and X. Chen, "A Fast JPEG Image Compression Algorithm Based on DCT," 2020 IEEE International Conference on Smart Cloud (SmartCloud), Washington, DC, USA, 2020, pp. 106-110, doi: 10.1109/SmartCloud49737.2020.00028. keywords: Image coding;Transform coding;Discrete cosine transforms;Quantization (signal);Image color analysis;Transforms;Streaming media;JPEG image;run length coding;Huffman coding;lossy compression,