D.Y. PATIL COLLEGE OF ENGINEERING & TECHNOLOGY, KOLHAPUR

(An Autonomous Institute)

DEPARTMENT OF CSE (DATA SCIENCE)

A

Project Report

on

Cipher Image

Submitted by

Name	Roll No.
Divya Patil	48
Tanishka Powar	50

Under the guidance of

Mrs.Tejashri Deokar

Second Year B. Tech. CSE (Data Science)

Academic Year 2023-24

D. Y. PATIL COLLEGE OF ENGINEERING & TECHNOLOGY, KOLHAPUR

(An Autonomous Institute)

DEPARTMENT OF CSE (DATA SCIENCE)

CERTIFICATE

This is to certify that,

Roll No.	Unique ID	Student Name	Exam Seat No.
48	EN22205857	Divya Patil	17505
50	EN22186100	Tanishka Powar	17612

have successfully completed the project work entitled,

Cipher Image

In partial fulfilment for the curriculum of **S. Y. B. Tech. CSE (Data Science)**. This is the record of their work carried out during academic year 2023-2024.

Date: **Place:** Kolhapur

Guide Name	**Prof. DR. G. V. Patil**	**Prof. DR. S. D. Chede**
Project Guide	HoD	Principal

External Examiner

DECLARATION

We the undersigned students of **S. Y. B. Tech. CSE (Data Science)** declare that the project work report entitled "**Project Title"** written and submitted by us, under the guidance of **Guide Name** is our original work. The empirical findings in this report are based on the data collected by us. The matter assimilated in this report is not the reproduction of any readymade report. We have not violated any of the provisions under the Copyright and Piracy / Cyber / IPR Act amended from time to time.

Date:

Place: Kolhapur

Roll No.	Unique ID	Student's Name	Signature
48	EN22205857	Divya Patil	
50	EN22186100	Tanishka Powar	

ACKNOWLEDGMENT

We extend our heartfelt gratitude to Prof. DR. A. K. Gupta Sir, Executive Director DYPCET, whose visionary leadership and unwavering support provided the foundation for this endeavor. We also express our sincere gratitude to Prof. DR. S. D. Chede Sir, Principal DYPCET, for their guidance and encouragement throughout this journey. Special thanks to DR. G. V. Patil Sir, Head of Department Data Science, for their invaluable insights and mentorship, shaping our understanding and approach within the field of data science.

We are immensely grateful to our project guide ---Guide Name--- whose expertise and dedication empowered us to navigate challenges and achieve milestones with confidence.

To our esteemed colleagues in the project group, your collaboration and dedication have been instrumental in realizing the goals of this project. Together, we have embraced innovation and teamwork, driving the project towards success. This project report stands as a testament to the collective efforts and support extended by each individual mentioned above. We acknowledge and appreciate your contributions, which have enriched our learning experience and propelled us towards excellence.

Date:

Place: Kolhapur

INDEX

INTRODUCTION

Encryption is a widely recognized method for enhancing information security in communication. Within encryption, image encryption plays a crucial role. The primary aim of image encryption is to transform the original image in a manner that makes it challenging to decipher, ensuring that only authorized individuals can access the information.

The encryption and decryption procedures hinge on a specific key value. The effectiveness of the encryption algorithm is measured by its capacity to safeguard the key value, thereby preserving the integrity of the original content. Encryption algorithms are broadly categorized into two types: symmetric and asymmetric, depending on the nature of the keys employed. Symmetric algorithms employ identical keys for both encryption and decryption processes.

Maintaining the secrecy of the key is paramount to prevent unauthorized decryption. Cryptography serves multiple purposes, including ensuring authentication, non-repudiation, integrity, and confidentiality.

Image encryption and decryption is a technique used to secure images from unauthorized access and modification. The security of images is a critical issue due to the growth of the internet, cell phones, and multimedia technology in society.

The motivation behind working on image encryption and decryption is to explore various issues associated with the existing image encryption techniques and to design a techniques that can increase security. Images, a ubiquitous medium for information sharing, have become crucial components of our personal lives and professional endeavors. Ensuring the confidentiality and integrity of these images, whether stored in cloud servers, transmitted over networks, or shared in personal communications, is a pressing concern.

PROBLEM STATEMENT

Develop an efficient encryption and decryption system for digital images, ensuring confidentiality, integrity, and authenticity of sensitive visual data.

Image encryption ensures that sensitive or private visual information remains confidential. By encrypting images, unauthorized individuals cannot view or understand the content, protecting the privacy of individuals or organizations.
When images are transmitted over networks or stored in the cloud, they are vulnerable to interception. Encrypting images before transmission or storage helps ensure that only authorized parties can access and interpret the data.

OBJECTIVE –

The primary objective of working on image encryption and decryption is to ensure the confidentiality and security of digital images. Image encryption techniques are used to protect images from various security threats such as eavesdropping, illegal modification, duplication, etc.

The model for encryption and decryption of an image is designed with the following objectives :
1. To ensure confidentiality and security while transmitting the image over a network.
2. To study the architecture of the image file.
3. To encrypt the image file by developing the application.

System Design

Designing a system for image encryption and decryption using XOR operations involves defining the architecture, components, and their interactions

System Architecture:

User Interface (UI):

- The system should have a user-friendly graphical interface to allow users to interact with the encryption and decryption processes.
- Users can select image files, provide encryption keys, and initiate the encryption/decryption process.

Encryption Module:

- Responsible for encrypting image data using XOR operations.
- Accepts the original image and a secret key as input.
- XORs the image pixels or blocks with the key to produce the encrypted image.

Decryption Module:

- Responsible for decrypting the encrypted image. Accepts the encrypted image and the same secret key used for encryption.
- XORs the encrypted data with the key to produce the original image.

Cross-Platform Compatibility:

- Ensure compatibility with various operating systems and devices.

Quality Assurance:

- Implement quality control mechanisms to ensure the encrypted and decrypted images maintain acceptable quality.
- Include error checking and handling to address issues that may arise during the encryption and decryption processes.

Deployment:

- Deploy the image encryption and decryption system on a suitable platform. It can be a desktop application, a web-based application, or even a mobile app, depending on your project's requirements.

Security Considerations:

- Ensure that the system follows best practices for secure key management, data protection, and user authentication to maintain the confidentiality and integrity of encrypted images.
- This comprehensive system design will provide a foundation for the development of your image encryption and decryption project using the XOR operation.

Key Components and Interactions:

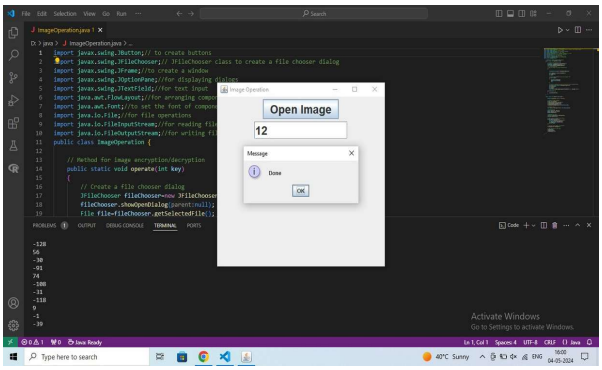
- Users interact with the UI to select images, specify encryption keys, and start the encryption or decryption process.
- The UI communicates with the Encryption and Decryption Modules.
- The Encryption Module XORs the image data with the encryption key and produces an encrypted image.
- The Decryption Module XORs the encrypted image with the decryption key to recover the original image.
- File I/O handles the reading and writing of image files, allowing users to input original images and save the encrypted or decrypted images.

Hardware and Software Requirements

1. Operating System: Windows 8 or above
2. Ram : 4GB Minimum
3. Java Development Kit : 7 or above
4. Software: Visual Studio Code
5. Packages for VS code: Extension Pack for Java

RESULT ANALYSIS

Picture to be decrypted



Locking the image by a passkey

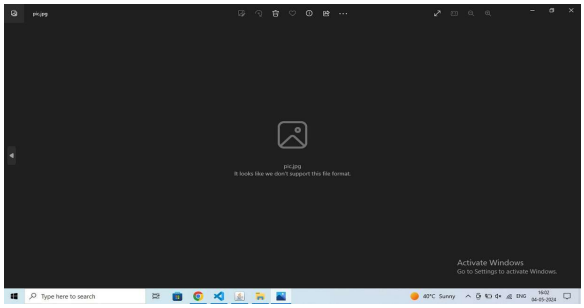
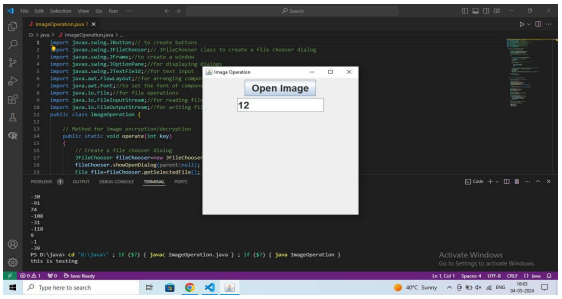


Image has been decrypted



To encrypt execute the code and enter passkey

Picture has been encrypted !!

CONCLUSION

We found that the XOR cipher is a useful tool for encrypting images. When we use the XOR cipher to encrypt an image, the randomness of the pixels in the original image increases. If the randomness is high, we can say that the image is safer. From the analysis of histograms, horizontal and vertical relationships, and data entropy, it can be concluded that the difference between encrypted images increases after different images are differentiated, which means that encrypted images are more secure and cannot be decrypted. The security key used to encrypt and decrypt the original image is the same. During this process, perform an XOR operation between the original image and the security key to access the image. Then perform an XOR operation on the encrypted image and security key to decrypt the image again. Therefore, decryption using the security key depends on the encryption result. Therefore, we can conclude that this process increases the stability of the image.

Image encryption and decryption algorithms are designed and used to provide privacy and security when transmitting and storing grayscale image data. The solutions in this article have an easy-to-use module. The proposed encryption algorithm can guarantee various parameters such as loss, maximum corruption, maximum efficiency, and maximum efficiency. The encryption method proposed in this study was tested on different grayscale images and was found to be effective.

FUTURE SCOPE

Future work will focus on developing an algorithm to encrypt and decrypt larger files or applications.

While the project has successfully implemented XOR-based image encryption and decryption, there are several avenues for future work and improvement:

- Enhanced Security: Explore more advanced encryption techniques and combine them with XOR encryption to increase the level of security. Consider using asymmetric key cryptography for secure key exchange.
- Steganography Integration: Combine XOR encryption with steganography to hide encrypted messages or information within images, adding an additional layer of security.
- Performance Optimization: Improve the system's performance, particularly for handling large images, by optimizing image processing and encryption algorithms.
- Multi-Image Support: Extend the system to support batch processing for multiple images, making it more convenient for users.

References

[1] Jui-Cheng Yen and Jim-In Guo, “A New Chaotic Key-Based Design for Image Encryption and Decryption”,2000.

[2] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki , “A Modified AES Based Algorithm for Image Encryption”,2007 .

[3] P. Radhadevi, P. Kalpana , “Secure Image Encryption Using Aes”,2012 .

[4] Roshni Padate, Aamna Patel, “Image Encryption And Decryption Using Aes Algorithm” ,2014.

[5] Jose´ J. Amador, Robert W. Green, “Symmetric-Key Block Cipher for Image and Text Cryptography”, 2005.

[6] Philip P. Dang and Paul M. Chau, “Image Encryption For Secure Internet Multimedia Applications”, 2000.

[7] Sanjay Kumar, Sandeep Srivastava, “Image Encryption using Simplified Data Encryption Standard (S-DES) “, 2014.

[8] Kundankumar Rameshwar Saraf, Vishal Prakash Jagtap, Amit Kumar Mishra, “Text and Image Encryption Decryption Using Advanced Encryption Standard”, 2014

[9] P.Karthigaikumar, Soumiya Rasheed “Simulation of Image Encryption using AES Algorithm”, 2011.

[10] B.Subramanyan, Vivek.M.Chhabria, T.G.Sankar babu , “Image Encryption Based On AES Key Expansion”, 2011

[11] Xu, Lu, et al. "A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion." Optics and Lasers in Engineering 91 (2017):.