**PROJECT TITLE:** IMAGE ENCRYPTION AND DECRYPTION USING TRIPLE DES

**NAME** : VAIBHAV SINGH

KAMAL JANGRA

**COURSE** : INFORMATION SECURITY

DEPT.OF INFORMATION TECHNOLOGY

**INSTITUTION NAME** : MANIPAL INSTITUTE OF TECHNOLOGY BENGALURU

**DATE OF SUBMISSION** : 5/11/2024

TABLE OF CONTENTS

|  |  |
| --- | --- |
| CONTENTS | PAGE NUMBER |
| 1.INTRODUCTION | 1 |
| 2.LITERATURE REVIEW | 4 |
| 3.METHODOLOGY | 7 |
| 4.IMPLEMENTATION | 7 |
| 5.RESULTS | 15 |
| 6.CONCLUSION | 20 |
| 7.REFERENCE | 21 |

**INTRODUCTION**

1. Background

With the rapid growth of digital data sharing and storage, ensuring the security and privacy of multimedia data has become critical. Images, which are a significant part of digital communication, are often vulnerable to unauthorized access and cyber threats. Traditional encryption methods applied to text data may not be fully suitable for multimedia files, as these files demand specific handling due to their size and format characteristics. The Triple Data Encryption Standard (3DES) algorithm, an enhancement of the DES algorithm, offers increased security by applying encryption in three stages, making it a robust option for protecting image data. This project focuses on using 3DES for the secure encryption and decryption of images, aiming to demonstrate its efficacy in preventing unauthorized access and maintaining image integrity.

2. Objectives

To understand the structure and principles of the Triple DES algorithm and its application in encrypting image data.

To develop an encryption module that secures image files using the 3DES algorithm, ensuring confidentiality during storage and transmission.

To implement a decryption module that accurately restores the encrypted image to its original state without quality loss.

To analyze the security strength, computational performance, and potential limitations of 3DES for multimedia data encryption.

3. Scope

This project will focus on applying the 3DES algorithm specifically to image files (e.g., .jpg, .png formats).

The project will cover encryption and decryption processes, assessing both image quality retention and processing time.

Comparative analysis with other symmetric encryption methods will be limited to the description and general comparison, without deep implementation.

The project will include a detailed evaluation of the security effectiveness of 3DES for image data, emphasizing its practical application in secure digital image storage and transfer.

**LITERATURE REVIEW**

**1. Introduction to Image Encryption**

Image encryption has become a significant area of research due to the exponential growth in digital data and the increasing threat of unauthorized access. Multimedia files, particularly images, require specialized encryption techniques due to their large size, unique format, and high redundancy compared to text. Standard encryption techniques such as DES (Data Encryption Standard) and AES (Advanced Encryption Standard) have been extensively used in data protection, yet adapting them to images requires special consideration. The development of the Triple DES (3DES) algorithm addressed some of the limitations found in the original DES, making it a suitable candidate for secure image encryption and decryption applications.

**2. Triple DES (3DES) and its Development**

The Triple DES encryption algorithm, also known as 3DES, was developed as an improvement over the original DES to provide a higher level of security. DES, initially standardized by NIST in 1977, was found to be vulnerable to brute-force attacks due to its relatively short key length of 56 bits. To enhance security, 3DES applies the DES algorithm three times in succession with three different keys, effectively increasing the key length to 168 bits. Studies show that 3DES offers significantly improved security over single DES, making it resilient against many types of attacks and suitable for applications where data confidentiality is critical, such as in financial and military data encryption. However, despite its strength, the algorithm's computational complexity and processing time remain concerns for resource-intensive applications.

**3. Application of 3DES in Image Encryption**

Research has shown that 3DES can be effectively applied to image encryption, providing robust security while maintaining the structural integrity of the original image. Unlike textual data, image files consist of large amounts of data and require encryption methods that ensure both speed and security. Studies by Al-Hazaimeh et al. (2017) and Raval et al. (2021) indicate that 3DES offers a balanced approach by providing high security at the expense of relatively moderate computational time. Despite being slower than some modern algorithms like AES, 3DES is advantageous for environments where data sensitivity is prioritized over speed.

**4. Advantages and Limitations of 3DES for Image Encryption**

One of the primary advantages of using 3DES for image encryption is its strength in protecting against unauthorized access. Compared to single DES, 3DES provides triple the protection by performing encryption-decryption-encryption cycles with different keys. It also ensures that encrypted images cannot be easily deciphered without the correct decryption key. Research by Patel et al. (2018) highlights that, due to its relatively high key length, 3DES remains a robust option against brute-force attacks. However, the algorithm’s limitations include its relatively slower encryption speed and greater computational requirements, especially for high-resolution images. Moreover, as noted by Gupta et al. (2019), the algorithm's performance may not be optimal for real-time encryption of large multimedia files due to its higher latency.

**5. Comparison with Other Symmetric Encryption Methods**

Though 3DES is a secure option, studies often compare it with the Advanced Encryption Standard (AES), which has become the dominant symmetric encryption standard due to its efficiency and speed. AES provides a higher encryption speed and is less computationally intensive than 3DES, making it more suitable for applications requiring real-time processing. Research by Kumar and Singh (2020) demonstrates that AES typically outperforms 3DES in speed, while 3DES remains advantageous in environments requiring exceptionally high-security levels, such as sensitive image data storage. These comparisons illustrate that while AES is preferred in performance-critical applications, 3DES remains valuable for scenarios where utmost security is prioritized over encryption speed.

**6. Current Challenges and Future Directions**

Despite its established security benefits, the use of 3DES for image encryption faces certain challenges, primarily due to the growing demand for real-time encryption and the increased size of multimedia files. Recent advancements in image encryption suggest exploring hybrid encryption approaches, combining the strengths of 3DES with faster algorithms like AES or lightweight cryptographic schemes. Research by Zhang et al. (2022) suggests that integrating 3DES within hybrid frameworks could yield improved security with acceptable processing speeds for image encryption. Additionally, exploring alternative symmetric encryption techniques that balance security and efficiency could further enhance image encryption methodologies.

**METHODOLOGY**

* **Approach**: by creating a website which can help in the encryption and decryption of an image
* **Tools and Technologies**: HTML,CSS,JS.

**IMPLEMENTATION**

In this project, we created a website to facilitate the encryption and decryption of images using the Triple DES (3DES) algorithm. This web application allows users to upload images, encrypt them for secure storage or transmission, and decrypt them back to their original form. The website was developed using HTML, CSS, and JavaScript, with a focus on a clean, responsive user interface and efficient image processing.

**1. HTML (HyperText Markup Language)**

HTML is the foundation of the website, defining its structure and layout. The primary HTML components used include:

* **Basic Structure**: The HTML file starts with a <!DOCTYPE html> declaration, followed by a <html> tag that encompasses the entire content. Key sections are enclosed within <header>, <main>, and <footer> tags for semantic organization.
* **Form for Image Upload**: An <input> element of type file is used within a <form> to allow users to upload images. This element is set to accept only image files (e.g., .jpg, .png) by specifying the accept attribute as image/\*.
* **Buttons for Encryption and Decryption**: HTML <button> elements trigger JavaScript functions to handle encryption and decryption processes. Buttons like "Encrypt Image" and "Decrypt Image" are clearly labeled to guide users.
* **Display Area**: An <img> element is used to display the uploaded or encrypted image. Additionally, a <div> element is used to show the encrypted data as text for users who may want to save or share it in encrypted form.
* **Additional UI Elements**: Other HTML elements like <h1>, <p>, and <div> tags are used for headings, instructions, and layout structuring to provide a cohesive and user-friendly experience.

**2. CSS (Cascading Style Sheets)**

CSS styles are used to enhance the appearance and responsiveness of the website. Key CSS elements include:

* **Responsive Layout**: CSS Flexbox and Grid layouts are utilized to ensure the website looks good on various screen sizes, including desktops, tablets, and mobile devices.
* **Styling the Form and Buttons**: CSS is applied to style the upload form and buttons. The buttons are given consistent padding, margin, and colors, and a hover effect is added to improve interactivity. A color scheme is chosen to make the website visually appealing and align with a secure, professional theme.
* **Image Display**: The CSS rules ensure that the uploaded or encrypted image is displayed at a suitable size without distortion. A CSS class is applied to the <img> element to restrict its maximum width and height, ensuring it fits well within the designated display area.
* **Loading and Status Indicators**: CSS animations are applied to a loading spinner displayed during encryption or decryption to indicate processing status. Additionally, success and error messages are styled with different colors to help users easily understand the operation results.
* **Responsive Media Queries**: Media queries in CSS adjust the layout for different screen sizes, ensuring a responsive design that provides an optimal experience across devices.

**3. JavaScript (JS)**

JavaScript forms the core logic of the website, handling image uploads, encryption, and decryption processes with the 3DES algorithm. Key JavaScript components include:

* **Image Upload and Preview**: JavaScript FileReader API reads the uploaded image and displays it in the designated <img> element. The FileReader reads the file as a data URL, enabling an immediate preview without uploading it to a server.
* **3DES Encryption and Decryption Functions**:
  + **Encryption**: Using the crypto-js library for JavaScript, the 3DES encryption function converts the image’s binary data into an encrypted string. The library provides straightforward methods like CryptoJS.TripleDES.encrypt, which simplifies the encryption process. The encrypted data is then displayed on the website or downloaded by the user.
  + **Decryption**: A similar process is applied in reverse using CryptoJS.TripleDES.decrypt to retrieve the original image from the encrypted string, displaying it on the page.
* **Error Handling and Feedback**: JavaScript functions include error-handling code to manage issues like unsupported file types or failed encryption attempts. These functions display appropriate messages in case of any issues, guiding users on how to proceed.
* **User Interaction and Events**: JavaScript addEventListener functions respond to user actions, such as image uploads and button clicks. Event listeners trigger the encryption and decryption functions when users click the respective buttons.

**4. Project Workflow**

* **Image Upload**: Users select an image file, which is immediately previewed on the page.
* **Encryption**: Upon clicking "Encrypt Image," JavaScript reads the image data, encrypts it using 3DES, and displays the encrypted text. The encrypted data can also be downloaded as a text file if users wish to store it securely.
* **Decryption**: After loading encrypted data, users click "Decrypt Image," triggering the decryption function, which displays the decrypted image on the page.

**SCREENSHOT OF THE CODE FOR THE WORKING OF THE DASHBOARD**

A computer screen shot of a program code

Description automatically generated

**SCREENSHOT OF THE CODE FOR THE WORKING OF DECRYPTION OF AN IMAGE**

**A screen shot of a computer code

Description automatically generated**

**A computer screen with colorful text

Description automatically generated**

**A screen shot of a computer code

Description automatically generated**

**SCREENSHOT OF THE CODE FOR WORKING OF ENCRYPTION OF AN IMAGE**

**A screen shot of a computer program

Description automatically generated**

**A screen shot of a computer program

Description automatically generated**

**A screen shot of a computer code

Description automatically generated**

**RESULT**

**Analysis of Results**

The results of this project demonstrate the successful implementation of image encryption and decryption using Triple DES (3DES) in a web-based environment, aligning well with the primary objectives. Here’s an analysis of these outcomes in the context of the project’s objectives:

1. **Objective: Secure Image Encryption and Decryption**
   * **Result**: The application effectively encrypts and decrypts image files, ensuring that only authorized parties with the correct decryption key can access the original image data.
   * **Analysis**: This result meets the objective of providing robust security for sensitive images, showing that 3DES is a suitable choice for applications requiring a high level of data confidentiality. By implementing client-side processing, the application further strengthens privacy, as no data is transmitted over the network.
2. **Objective: Usable, Accessible Interface for Non-Technical Users**
   * **Result**: The web application has a straightforward layout, with an easy-to-follow process for uploading images, encrypting, and decrypting them, accompanied by real-time feedback.
   * **Analysis**: The simplicity and responsiveness of the interface support the objective of accessibility, making encryption technology available to a broader audience, including non-technical users. This outcome shows that advanced cryptographic methods can be packaged into a user-friendly form without compromising functionality.
3. **Objective: Reliable Processing of Various Image Formats and Sizes**
   * **Result**: Testing demonstrated that the application can handle common image formats (JPEG, PNG) and moderately large files, with optimizations like resizing and memory management in place.
   * **Analysis**: The ability to process different image formats efficiently ensures versatility in usage, meeting the objective of supporting a range of data types. It also highlights the balance achieved between security and performance; despite 3DES’s inherently slower processing, the application remains responsive and practical for real-world usage.
4. **Objective: Privacy by Design with No Server-Side Data Transfer**
   * **Result**: The application’s client-side processing architecture keeps all data handling on the user’s device, minimizing potential security risks associated with network transfer and server storage.
   * **Analysis**: This approach achieves the objective of maximizing user privacy, aligning with data protection standards and best practices. It reinforces the significance of client-side encryption for applications where data confidentiality and privacy are critical, contributing to a growing need for decentralized, privacy-centric applications

SCREENSHOT OF THE DASHBOARD

A screenshot of a computer

Description automatically generated

SCREENSHOT OF THE ENCRYPTION OF AN IMAGE

A screenshot of a computer

Description automatically generated

A screen shot of a computer code

Description automatically generated

SCREENSHOT OF DECRYPTION OF AN IMAGE

A screenshot of a computer screen

Description automatically generated

A squirrel holding a camera

Description automatically generated

**CONCLUSION**

The project successfully developed a web application for the encryption and decryption of images using the Triple DES (3DES) algorithm, ensuring secure handling of image data within a user-friendly interface. Key findings and contributions of the project include:

* Secure Image Encryption: The use of 3DES provided a robust security layer for images, making unauthorized access and data breaches significantly harder by employing a three-stage encryption method. By processing encryption and decryption entirely on the client side, data privacy was maximized since images were not transferred over the network.
* Usability and Accessibility: Through a clean, responsive design, users can easily upload, encrypt, and decrypt images, with clear feedback and instructions provided throughout the process. The project prioritized an intuitive interface, making it accessible for users across various devices and browsers.
* Efficient Handling of Client-Side Processing: Optimizations such as image resizing, memory management, and the use of a reputable JavaScript encryption library (crypto-js) improved processing speed and reliability, allowing the web application to handle a range of image sizes while maintaining performance.

**REFERENCES**

* General Cryptography and 3DES

<https://csrc.nist.gov/publications/detail/fips/46/3/final>

* JavaScript Libraries and Tools for Encryption

<https://developer.mozilla.org/en-US/docs/Web/API/Web_Crypto_API>

* Web Development with HTML, CSS, and JavaScript

<https://www.w3schools.com/>

* Case Studies and Research on Image Encryption

<https://ieeexplore.ieee.org/>