Image Encryption and Decryption Using Triple DES

Authors: Vineeth Amsham, Suresh Babu Changanaboyina, Puja Lahari Sajja and Nikhil Adigoppula.

Introduction:

Ensuring security has become a top priority with the exponential growth of digital data storage and transmission. In various fields, the use of images has seen significant expansion, emphasizing the need to protect sensitive image data from unauthorized access. Preserving personal privacy has become a crucial undertaking, leading to the investigation and development of various techniques to maintain data integrity and safeguard personal information.

To achieve this goal, our plan is to develop an Image Encryption and Decryption System utilizing Triple DES. The primary objective of the system is to offer a strong encryption and decryption process that guarantees the confidentiality and integrity of the images. Through the utilization of the Triple DES algorithm, which involves cascading the DES algorithm three times, the system will enhance encryption strength and minimize the potential for unauthorized access.

The utilization of the Triple DES algorithm in the system converts the images into ciphertext, making them incomprehensible to unauthorized individuals. This guarantees the protection of sensitive or private images, even if they are intercepted or accessed without authorization. As a result, the system will maintain the confidentiality, integrity, and accessibility of the encrypted images, fulfilling the requirements of various applications and meeting the diverse needs of users.

Model Proposal:

In light of the rapid growth of digital data storage and transmission, ensuring security has become a top priority. The increasing use of images in various domains highlights the significance of safeguarding confidential image data from unauthorized intrusion. Preserving personal privacy has become essential, leading to the exploration and development of various techniques to uphold data integrity and protect personal information.

To address this issue, we propose the development of an Image Encryption and Decryption System using Triple DES. This system aims to provide a robust encryption and decryption mechanism, guaranteeing the confidentiality and integrity of images. By employing the Triple DES algorithm, which involves cascading the DES algorithm three times, the system strengthens encryption and minimizes the risk of unauthorized access.

Through the application of the Triple DES algorithm, the system converts images into ciphertext, making them incomprehensible to unauthorized individuals. This ensures the protection of sensitive or private images, even if they are intercepted or accessed without authorization. Consequently, the system will ensure the confidentiality, integrity, and accessibility of encrypted images, meeting the requirements of various applications and users with diverse needs.

The refined description of the scope and objective of an Image Encryption and Decryption System using Triple DES (Data Encryption Standard) revolves around the protection of digital images by implementing secure encryption techniques. The primary goal is to ensure the confidentiality and integrity of sensitive visual information during storage or transmission, thereby preventing unauthorized access. By leveraging the symmetric encryption method of Triple DES, the system establishes robust security measures.

The system encompasses multiple aspects, including encryption, decryption, key management, and image processing. Encryption involves transforming the original image into an unintelligible format using a secret key, making it incomprehensible to unauthorized individuals. Decryption, on the other hand, reverses the encryption process and restores the original image using the same key. Key management pertains to securely generating, storing, and exchanging encryption keys to ensure the confidentiality of the images.

Moreover, this system integrates image processing techniques to augment the security and robustness of the encrypted images. Approaches such as manipulating bits at the lowest level, shuffling pixels, and introducing randomization can be utilized to bolster the resistance of the encrypted images against potential attacks and guarantee enhanced security.

The objective of an Image Encryption and Decryption System using Triple DES is to provide a high level of confidentiality and integrity for digital images. It aims to protect sensitive visual data from unauthorized access, tampering, or interception.

Image Encryption and Decryption Using Triple DES

By employing the Triple DES algorithm, which employs multiple rounds of encryption and provides a stronger security level than the original DES, the system ensures robust encryption and decryption processes.

In general, the scope and objective of an Image Encryption and Decryption System utilizing Triple DES are centered on fortifying the security of digital images through the utilization of encryption, decryption, key management, and image processing techniques.

By proficiently implementing these measures, the system strives to protect the confidentiality and integrity of visual information, allowing only authorized individuals to access and interpret the images. Moreover, the system ensures data privacy and safeguards against potential threats, thereby ensuring comprehensive data protection.

Existing System:
The current scenario in encryption methods for securing digital communications poses certain problems. Despite the availability of encryption techniques, there is always a potential risk of vulnerabilities. In the event that a flaw or weakness is found in an encryption algorithm or its implementation, it compromises the confidentiality of the encrypted message.

Drawbacks of the existing system:
The current image encryption and decryption systems have certain limitations that make them vulnerable to security breaches. Attackers can exploit these vulnerabilities to gain unauthorized access to encrypted images. Weak encryption algorithms, inadequate key management practices, and implementation flaws are some of the factors that contribute to the risk of unauthorized access to encrypted images.

Proposed System:
In order to address the issues associated with the current scenario, we propose the development of a new system. The proposed system aims to overcome the vulnerabilities and risks that exist in encryption methods for securing digital communications. By implementing robust encryption algorithms and ensuring their secure implementation, the proposed system will enhance the confidentiality and integrity of secret messages.

Purpose:
The main purpose of the proposed model is to provide confidentiality, integrity, and availability of digital images through secure encryption techniques. Its primary goal is to prevent unauthorized access and safeguard sensitive visual information during storage or transmission. By implementing the Triple DES algorithm, a symmetric encryption method, the system guarantees robust security measures.

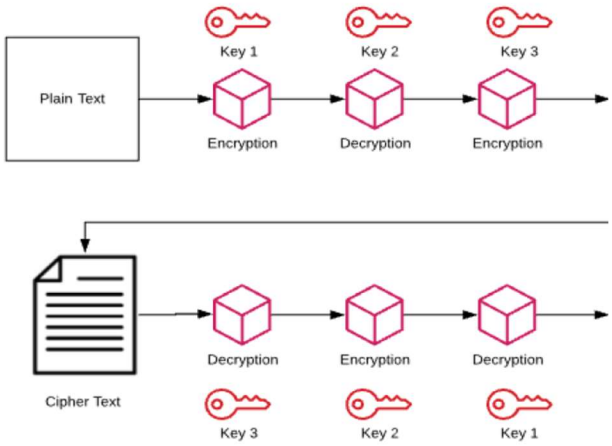
This system covers a wide range of aspects, including encryption, decryption, key management, and image processing. Encryption entails transforming the original image into an unreadable format using a secret key, making it unintelligible to unauthorized individuals. Conversely, decryption reverses the encryption process and retrieves the original image using the same key. Key management is responsible for securely generating, storing, and exchanging encryption keys to uphold the confidentiality of the images.

Triple DES Algorithm:
When the original DES cipher was created, a key size of 56 bits was considered adequate. However, as computing power has advanced, it has become possible to launch brute-force attacks on DES. To counter this, Triple DES offers a straightforward solution by increasing the key size without requiring the development of an entirely new block cipher algorithm.

This system has been developed using the Triple DES algorithm to ensure optimal performance. The Triple DES (3DES), also referred to as TDEA (Triple Data Encryption Algorithm), is a symmetric encryption algorithm widely employed in image encryption and decryption systems. It serves as an improved iteration of the Data Encryption Standard (DES) algorithm.

Triple DES employs a specific keying pattern wherein the DES algorithm is applied three times, leading to an elevated level of security. This process encompasses three key operations: encryption, decryption, and encryption once more. Each operation employs a distinct key, resulting in a sequence of "key1-key2-key3."

Image Encryption and Decryption Using Triple DES



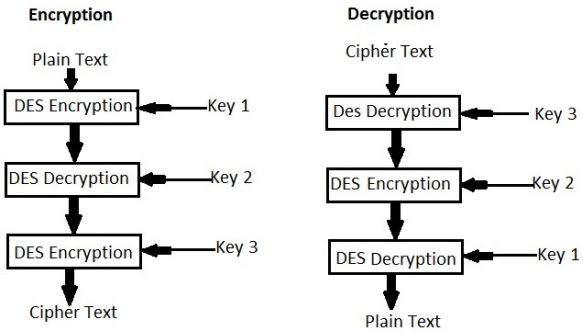
Triple DES employs three DES keys, namely K1, K2, and K3, each consisting of 56 bits, excluding the parity bits.

The encryption algorithm follows this pattern:
CipherText = EK3(DK2(EK1(plaintext))).

In other words, the plaintext undergoes DES encryption with K1, followed by DES decryption with K2, and finally, DES encryption with K3.

The decryption process is the reverse:
PlainText = DK1(EK2(DK3(CipherText)))

In this case, the CipherText is decrypted with K3, then encrypted with K2, and ultimately decrypted with K1.



Security Analysis:
Triple DES employs a key length of 168 bits, which is achieved by combining three 56-bit keys. This key length is considered highly secure against brute-force attacks, as it results in 2^{168} possible combinations. According to NIST's recommendation, the Triple DES scheme, utilizing three distinct keys, provides a security level of 100 bits, which is deemed sufficient until the year 2030.

We have gathered a specific quantity of images and uploaded them for encryption and decryption purposes. The main objective is to evaluate the accuracy of the decryption process. Our experiments involved multiple users and images. So far, the system is functioning correctly, and, from a computational standpoint, it is secure due to the successful implementation of the Triple DES algorithm.

User Registration marks the initial step of the login process, where users are obligated to furnish fundamental registration information. The registration page comprises multiple fields that necessitate completion. Notably, the login ID field follows specific validation criteria and does not permit the use of certain characters.

For the Login process, users are required to input both a login ID and a password, both of which are mandatory fields. In the event that the provided login ID or password does not correspond to the stored credentials, an error message will be displayed.

Steps in designing proposed model:
The user's interaction with the system involves multiple steps. Firstly, registration is necessary to obtain access to the system. After completing the registration process, the user will receive credentials that will be used for logging into the system.

After successfully logging in, the user is provided with the option to send a file. This process entails uploading an image file and providing the corresponding encryption key. Furthermore, the user is required to specify the intended recipient of the image file. This step ensures the secure transmission of the image file to the designated recipient.

Moreover, the system includes a functionality that allows users to view their sent or received data conveniently. Users can easily access the data they have sent or received through the system. In the case of receiving an encrypted image file, the user can decode it by entering the corresponding key. This ensures that the recipient can decrypt and access the received image file successfully. In summary, the system offers a comprehensive image encryption and decryption experience by incorporating functionalities such as registration, login, file sending, file viewing, and decoding.

In this project, HTML, CSS, and JavaScript will be utilized on the front end, while Python will be employed on the back end. The Django framework and MySQL Database will be implemented for the development process.

Image Encryption and Decryption Using Triple DES

Module Description:
In the field of cryptography, image encryption involves manipulating the output of the initial bits based on a cryptographic key using a standard stream cipher. This technique is employed to securely encrypt data and prevent unauthorized individuals from accessing or compromising the information.

The image is transformed into a series of bits, which provides an additional layer of security, making it difficult for others to visualize the original image. To retrieve the original image, the encoded data must be decrypted back into its original form by decoding the bit code using the appropriate cryptographic techniques.

The system consists of one major module with several sub-modules, each serving a specific function. The "User" module plays a central role in the system, and it offers various features to registered users. To access the system, users are required to complete a registration process. Once registered, they can log in using their credentials.

One of the primary functionalities of the system is the "Send File" option, which enables users to upload image files along with encryption keys. When sending files, users must select the recipient to whom they wish to share the image file securely.

Moreover, the "View File" sub-module allows users to access and view both sent and received data. For decryption of received data, users need to enter the appropriate key. This comprehensive system empowers users with the ability to securely exchange image files and manage their data effectively.

Data embedding:
This process begins with image preparation and key generation. Firstly, the selected image is prepared in a suitable format. Then, three unique keys are generated specifically for Triple DES encryption. These keys are essential for ensuring the security and integrity of the encrypted image.

Next, the encryption phase begins by converting the image into a binary representation, typically in the form of a series of bits. The binary representation is then divided into blocks of equal size. Each block undergoes the Triple DES encryption algorithm, using the generated keys. This process encrypts the blocks individually, guaranteeing the confidentiality and integrity of the data within.

Once the encryption is complete, the data embedding step comes into play. In this step, specific pixels within the image are chosen for data embedding. These pixels should be inconspicuous to avoid noticeable alterations in the image's visual quality. The encrypted blocks are converted into bit sequences, and the least significant bits (LSBs) of the selected pixels are modified to embed the bit sequences. This careful embedding process ensures that the embedded data remains hidden within the image.

To decrypt the image and retrieve the embedded data, the decryption phase is initiated. The image containing the embedded data is obtained, and the pixels containing the embedded information are identified. The LSBs of these pixels are then extracted to obtain the bit sequences. By applying the Triple DES decryption algorithm using the same set of keys used during encryption, the bit sequences are decrypted back into the original data blocks. These decrypted blocks are reconstructed to obtain the original image, with the embedded data now recovered.

Throughout the entire process, it is crucial to manage the encryption keys securely. The generated keys must be safeguarded to ensure the security of the encrypted image. If necessary, the decryption keys can be securely distributed to authorized parties for the purpose of image decryption.

By following this data embedding process, images can be securely encrypted using the Triple DES algorithm. The embedded data can be extracted during decryption, allowing authorized parties to recover the original information while maintaining the confidentiality and integrity of the data.

The Triple DES algorithm takes a plaintext message and a secret encryption key as input and produces a ciphertext. The same key is used for encryption and decryption, making it a symmetric encryption algorithm. The algorithm involves three stages: key generation, encryption, and decryption.

Key Generation:
To generate the encryption and decryption keys for Triple DES, we start with a single 64-bit key. The key is divided into two 56-bit keys: K1 and K2. These two keys are derived by applying a process called key permutation (parity drop) and shifting operations. Finally, the original key is duplicated to create the third 56-bit key, K3.

Encryption Process:
The encryption process in Triple DES consists of three stages: encryption with K1, decryption with K2, and encryption with K3.

Image Encryption and Decryption Using Triple DES

Stage 1: Encryption with K1 The plaintext image is divided into blocks, typically 64 bits in size. Each block undergoes an initial permutation (IP) operation. The resulting block is then encrypted using the first key, K1, through the DES algorithm. The output is a ciphertext block.
Stage 2: Decryption with K2 The ciphertext block obtained in Stage 1 is decrypted using the second key, K2, through the DES algorithm. This step effectively reverses the encryption performed in the previous stage.
Stage 3: Encryption with K3 The block resulting from Stage 2 is encrypted again, but this time using the third key, K3, through the DES algorithm. This final encryption stage adds an extra layer of security to the encrypted image.

Decryption Process:
The decryption process in Triple DES follows the same stages as the encryption process but in reverse order.

Stage 1: Decryption with K3 The encrypted image is divided into blocks, typically 64 bits in size. Each block undergoes an initial permutation (IP) operation. The resulting block is then decrypted using the third key, K3, through the DES algorithm. The output is an intermediate block.
Stage 2: Encryption with K2 The intermediate block obtained in Stage 1 is encrypted using the second key, K2, through the DES algorithm. This step reverses the decryption performed in the previous stage.
Stage 3: Decryption with K1 The block resulting from Stage 2 is decrypted one final time using the first key, K1, through the DES algorithm. This stage reverses the initial encryption performed in Stage 1 and recovers the original plaintext image.

Example: Let's consider a simple example using a grayscale image represented by a 4x4 pixel matrix, where each pixel value ranges from 0 to 255. For simplicity, we'll use a single 64-bit key: 0110101101100101.

Encryption:
Generate Keys:
Key Generation splits the 64-bit key into three 56-bit keys: K1, K2, and K3.
Encrypt with K1:
Perform initial permutation (IP) on the 4x4 pixel matrix.
Encrypt the resulting matrix using the first key, K1, through the DES algorithm.
Decrypt with K2:
Decrypt the ciphertext obtained in Step 2 using the second key, K2, through the DES algorithm.
Encrypt with K3:
Encrypt the intermediate matrix obtained in Step 3 using the third key, K3, through the DES algorithm.
The resulting ciphertext matrix represents the encrypted image.

Decryption:
Decrypt with K3:
Decrypt the encrypted image using the third key, K3, through the DES algorithm.
Encrypt with K2:
Encrypt the intermediate matrix obtained in Step 1 using the second key, K2, through the DES algorithm.
Decrypt with K1:
Decrypt the ciphertext obtained in Step 2 using the first key, K1, through the DES algorithm.

The resulting matrix represents the decrypted grayscale image, which matches the original input.

Note: In practice, Triple DES typically uses a key length of 168 bits, generated from three 56-bit keys. This provides enhanced security compared to the example using a single 64-bit key.

In summary, Triple DES applies the DES encryption algorithm three times using different keys to encrypt and decrypt images. This multiple encryption process adds an additional layer of security to the data being encrypted.

PROJECT IMPLEMENTATION:
The project was conceived and built using the Django Framework. For coding purposes, we employed the Django Framework, and all databases were created and managed through MySQL Server. Within MySQL Server, tables were generated, and queries were written to store project data and records.

Hardware Requirements:

- Laptop or PC
- Operating System: Windows 7 or higher
- Processor: Intel Core i3 or higher
- RAM: 4 GB or higher
- Storage: 100 GB ROM or higher

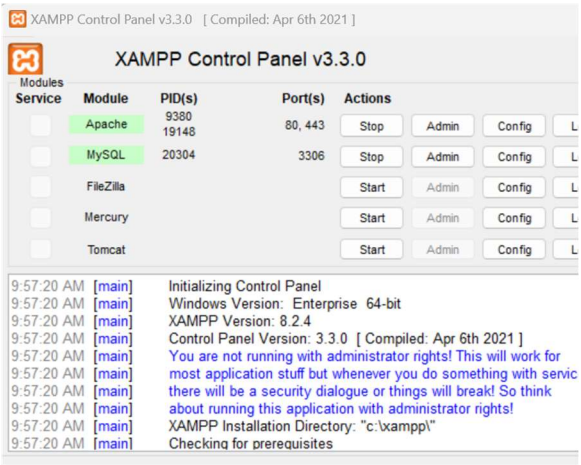
Software Requirements:

- Python
- XAMPP Server
- Visual Studio

Image Encryption and Decryption Using Triple DES

XAMPP Server:
In our project, we have utilized XAMPP, an all-in-one software package that combines the Apache web server, MySQL database (MariaDB), Php, and Perl within a single distribution.

This versatile package is designed to work seamlessly on Windows, MAC, and Linux operating systems. One of its advantageous features is the effortless integration of Php with MySQL, which does not necessitate any additional configuration.



Project Execution:
To initiate our code execution, we begin by activating the scripts in the project folder through the command "venv\scripts\activate".

Subsequently, we launch the XAMPP server and start the Apache web server and MySQL database services.

To run the server, we utilize the command "python manage.py runserver".

Upon running the server, we access the website by copying and pasting the provided URL from the command prompt, which is usually "http://localhost:8000/".

Once the website is accessible, we can create a user login, enabling us to send and view files securely using a secret key.

Activity diagram for user:

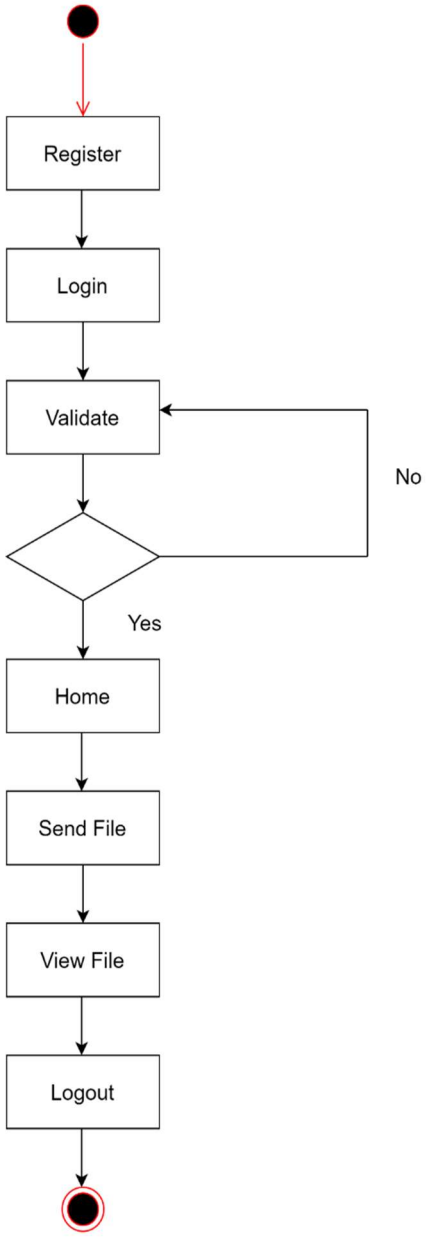
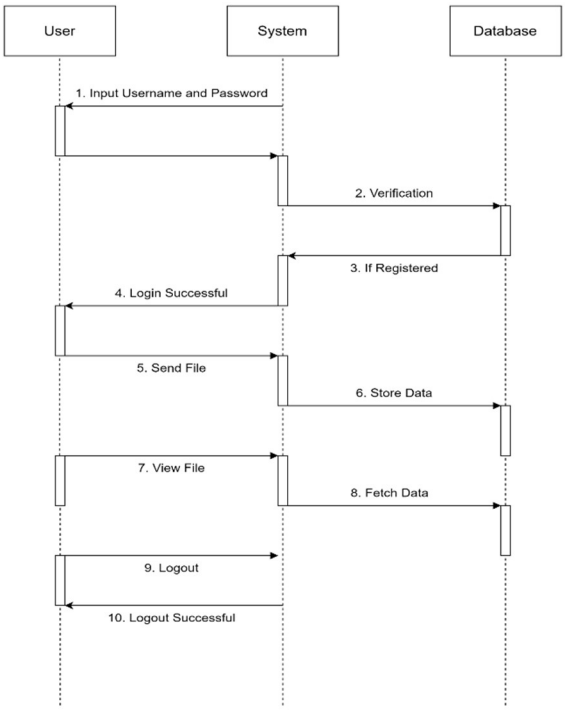


Image Encryption and Decryption Using Triple DES

Sequence Diagram of User:



Technical Feasibility:

In this phase, we conduct an evaluation of the technical feasibility of the proposed systems. The primary objective is to determine the availability of necessary technologies for the successful development of the system.

Technical Feasibility involves assessing whether the organization possesses the required technology and expertise to carry out the project or if they need to acquire them. The viability of the system can be justified based on the following factors:

- Availability of all essential technologies required for system development.
- The system demonstrates a high level of adaptability and can be easily expanded in the future.
- The system ensures accuracy, user-friendliness, reliability, and data security.
- The system provides timely and efficient responses to user inquiries.
- In our project, we have established that it is technically feasible since all the technology needed for implementation is readily accessible.

Advantages:

- Triple DES utilizes an exceptionally secure encryption algorithm.
- The system significantly enhances the difficulty of unauthorized decryption of encrypted images.
- The encryption process involves applying the DES algorithm thrice to each data block, thereby greatly bolstering the overall encryption strength.
- It enables secure sharing and decryption of encrypted images.
- Encryption keys can be securely stored and distributed to authorized users, safeguarding the confidentiality of the image data.

Limitations:

- The necessity for repeated encryption and decryption operations in Triple DES can adversely affect the overall speed of encrypting and decrypting large image files.

System Architecture:

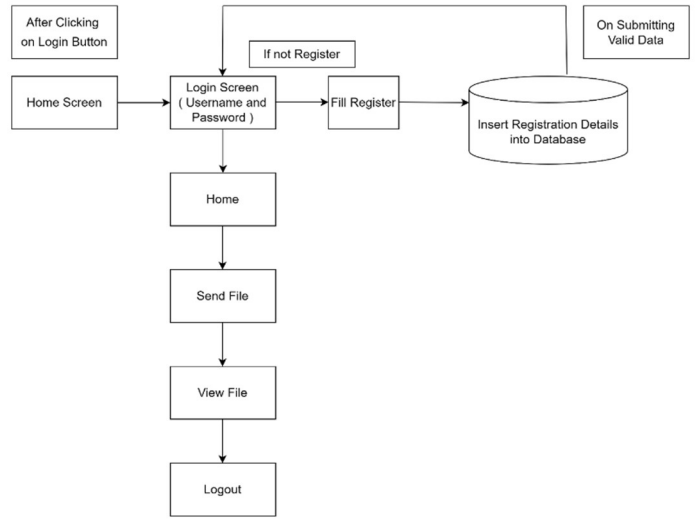
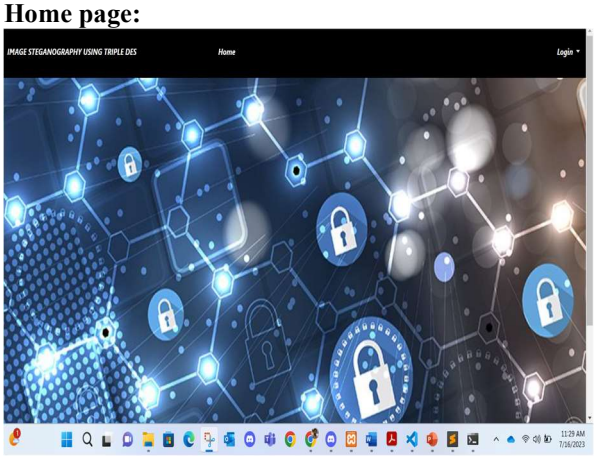


Image Encryption and Decryption Using Triple DES

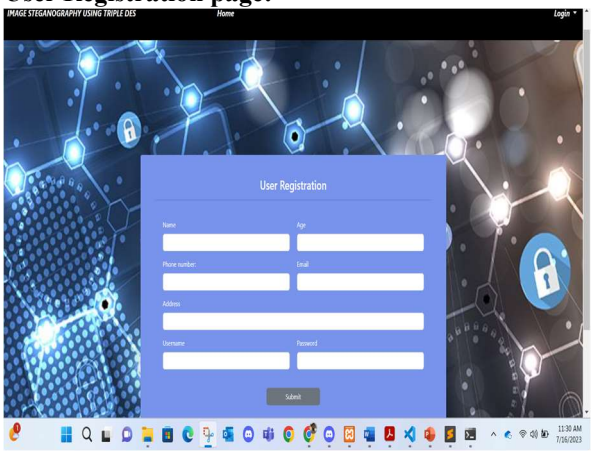
The below screenshots are user interface for different options that we implemented in the project:

Home page:

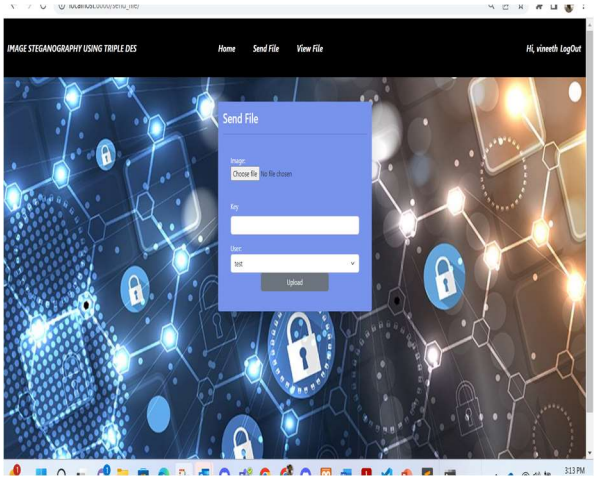


After user logged in user can able to send and view the file as shown in below image:

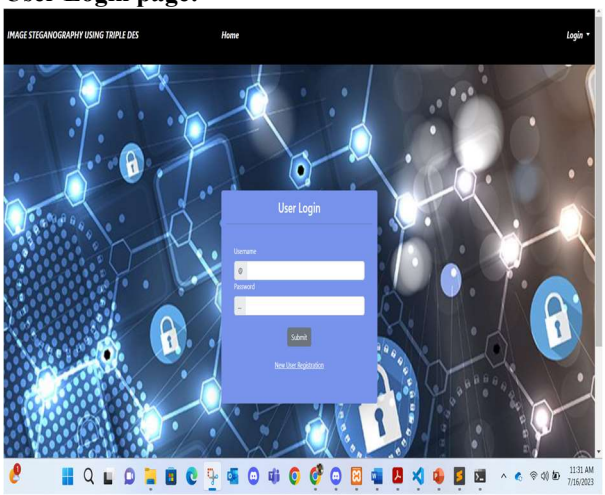
User Registration page:



Send file:



User Login page:



View File:

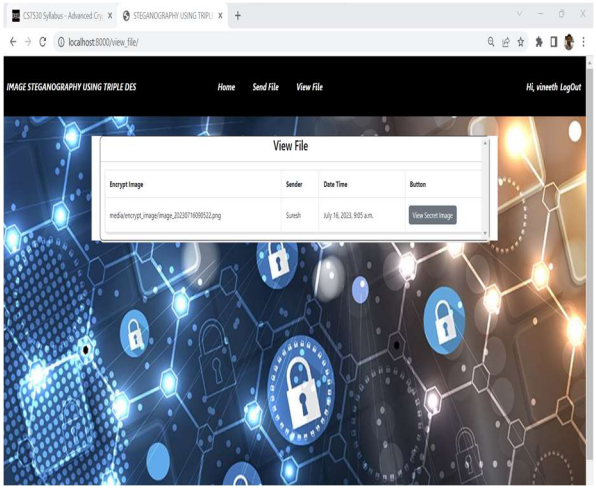


Image Encryption and Decryption Using Triple DES

Applications:

Secure Image Transmission: This Project can be applied in scenarios where there is a need to securely transmit images over networks, such as in confidential communication channels or sensitive data transfers. By encrypting the images using 3DES, the projects ensure that only authorized recipients can decrypt and access the images, protecting them from interception or unauthorized viewing.

Image Storage and Archiving: The project can be utilized in applications that require secure storage and archival of digital images, such as in databases, cloud storage, or digital repositories. By encrypting the images before storage, they provide an additional layer of protection against unauthorized access or data breaches.

Sensitive Image Sharing: In contexts where sensitive images need to be shared with specific individuals or entities, This Project can be employed to encrypt the images and ensure that only authorized recipients can decrypt and view them. This can be useful in scenarios like medical imaging, military intelligence, or confidential document sharing.

Privacy Preservation: This project can be applied in applications where privacy preservation is essential, such as in multimedia systems, social media platforms, or personal image collections. By encrypting the images, they prevent unauthorized individuals from viewing or analyzing the content, maintaining the privacy and confidentiality of the images**.**

Features:

Load Balancing: Efficient workload management is achieved through load balancing, ensuring that only the administrator has access to the system. This approach maintains manageable server load levels during the administrator's active session.

Convenient Accessibility: Users benefit from easy retrieval and storage of records and other relevant information within the system.

User-Friendliness: The website/application is thoughtfully designed to offer a highly user-friendly experience, ensuring intuitive use and smooth navigation for all users.

Efficiency and Reliability: The system's robustness stems from secure database storage on the server and tailored user access, resulting in high efficiency and reliability. By eliminating the need for physical records or customer data in spreadsheets, maintenance costs are reduced.

Simplified Maintenance: The Image Encryption and Decryption System, employing Triple DES, is intentionally crafted for straightforward maintenance, ensuring the system remains easy to manage and operate.

Github Code link:

- **https://github.com/Vineethamsham/Advanced_Crypto_Project**

Conclusion:

Our team successfully accomplished a System Design project centered around "Image Encryption and Decryption System using Triple DES," leveraging the Django framework in the Python programming language. The development of this system demanded considerable effort, and we take pride in the final outcome. Nevertheless, we recognize that perfection is a constant pursuit in the development realm, and there may be opportunities for further enhancements in this application. Throughout the project, we acquired valuable knowledge and valuable insights, enriching our expertise in the development field.

References:

[1]. K. N. Sreehari, " Efficient key management methods for symmetric cryptographic algorithm", in 2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2018.

[2]. National Institute of Standards and Technology,Title:Information Technology Laboratory COMPUTER SECURITY RESOURCE CENTER: Data Encryption Standard (DES)- FIPS 46-3

[3]. Aman Kumar, Sudesh Jakhar, Sunil Maakar, "Distinction between Secret key and Public key Cryptography with existing Glitches", Volume: 1, 2012.

[4]. Performance Evaluation of Symmetric Encryption Algorithms. Authors: Diaa Salama, H. M. A. Kader, Mohie M. Hadhoud Published 2008

[5]. N. Lalit hamani and Dr. Soman K. P ., " T owards Generating Irrevocable Key for Cryptography from Cancelable Fingerprints", in Proceedings 2009-2nd IEEE International Conference on Computer Science and Informat ion Technology(ICCSIT 2009)

[6]. Elaine Barker, "Recommendation for Key Management" NIST Special Publication 800-57 Part 1 Revision 4

[7]. A. V. Sreedhanya and Dr. Soman K. P., "Secrecy of cryptography with compressed sensing", Proceedings - 2012 International Conference on Advances in Computing and Communications, ICACC 2012.

[8]. Abdul kader, Diaasalama and Mohiv Hadhoud, "Studying the Effect of Most Common Encryption Algorithms," International Arab Journal of e-technology, Vol.2. No.1.

[9]. Grabbe J., Data Encryption Standard: The DES algorithm illustrated, Laissez faire City time, vol. 2, no 28, 2003.

[10]. Barker W, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, NIST Special Publication, 2008, 800-67

[11]. Jian L and ligan, Study on Chaotic Cryptosystem for Digital Image Encryption, 2011 Third International Conference Measuring Technology and Mechatronics Automation, IEEE, 2011

[12]. Guru, J & Srivatsava, Mohish & Sheeja, R.. (2020). Implementation of Triple DES ALGORITHM in Data Hiding and Image Encryption Techniques. International Journal of Advanced Science and Technology. 29. 10549-10559.

[13]. Aamer Nadeem, "A Performance Comparison of Data Encryption Algorithm," IEEE 2005.

[14].] Triple Data Encryption Algorithm Modes of Operation, ANSI X9.52 - 1998.

[15]. Jian L and Ligan S, Study on Chaotic Cryptosystem for Digital Image Triple Data Encryption Algorithm Modes of Operation, ANSI X9.52 - 1998.