IMAGE ENCRYPTION AND DECRYPTION USING AES ALGORITHM

Sandip S. Patil, Associated Professor SSBTCOET Jalgaon MS
Rohit R. Pingale, SSBTCOET Jalgaon MS India
Ajinkya S. Chikhlodkar, SSBTCOET Jalgaon MS India
Vaibhav C. Toradmal, SSBTCOET Jalgaon MS India
Aniket R. Surwade, SSBTCOET Jalgaon MS India

DEPARTMENT OF COMPUTER ENGINEERING
SSBT's COLLEGE OF ENGINEERING AND TECHNOLOGY, BAMBHORI, JALGAON - 425 001 (MS)

Abstract- Security concerns have taken front stage in the rapidly expanding digital exchange of data storage and transmission. Since the use of images is expanding quickly across a wide range of industries, it is crucial to safeguard sensitive image data from hackers. The need for image protection has become critical. It is now essential to secure someone's privacy. The preservation of data and personal information has been studied and developed using a variety of ways. Image encryption is used to shield sensitive data from unauthorised users. One of the most popular methods for keeping data concealed from unauthorised access is encryption. For picture encryption, the Advanced Encryption Standard (AES) is utilised, which leverages the key stream generator to improve image encryption performance.

Keywords-
- AES:- Advanced Encryption Standard
- DES:- Data Encryption Standard

I. INTRODUCTION

The most pressing issue in recent years has been the security and integrity of the data. Nowadays, practically all data is exchanged across computer networks, which has led to an upsurge in network attacks. Data must be encrypted and stored before being transmitted in order to prevent attacks from different types of attackers. Data is concealed by the process of encryption, which changes the original text into cypher text. Several algorithms are used in encryption to encrypt data into various forms. A set of keys with various characters is used by cryptographic algorithms for both encryption and decryption. The plaintext is encrypted using a key, and it is decrypted by transforming the plaintext back to the original form from the encrypted text. Data is transmitted and stored using cryptography so that only authorised users can access it. Data can be protected by encoding it in an unreadable format using the science of cryptography. Using a mathematical form technique for both encryption and decryption is a practical method of securing sensitive information. The key value affects both the encryption and decryption processes. The algorithm's strength is how challenging it is to figure out the key value and obtain the original text. According to the keys, the method is primarily separated into two types: symmetric and asymmetric. A symmetric algorithm is one in which the same keys are used for both encrypting and decrypting data. Stream and block cyphers are further subdivided under symmetric algorithms. A block cypher is performed on a block of data, as opposed to a stream cypher, which is performed on a single byte. One key is used for encryption and the other for decryption in asymmetric algorithms. In order to prevent message decryption, the key must be kept a secret. The goals of cryptography are to give authentication (indicating one's identity), non-repudiation (letting the recipient know the sender isn't lying), integrity (ensuring that the data is accurate, trustworthy, and reliable), and privacy/confidentiality (message is read by only the intended receiver).

The primary goal of this is to establish file security using the most advanced and robust algorithm, which was created by Vincent Rijmen and Joan Daemon and was originally published in 1997. There are two parts to the project. Encryption is the subject of the first module, and decryption is the subject of the second.

AES ALGORITHM: NIST started working on developing AES in January 1997. AES is a symmetric key encryption method that outperforms the DES algorithm. The number of algorithms has been decreased from the original 15 types to just 4. Rijndael algorithm is another name for the AES algorithm. when neither the encryption nor decryption of the text block is fixed.

The difference between DES and AES

Factors	DES	AES
Key Length	56 bits	128, 192, 256 bits
Block Size	64 bits	128, 192, 256 bits
Cipher Text	Symmetric block cipher	Symmetric block cipher
Developed	1977	2000
Security	Proven inadequate	Considered secure
Possible Keys	2^{56}	2^{128}, 2^{192}, 2^{256}

II. Literature Survey

To study and analyze more about Machine Learning, the following literature survey has been done.

In [1] the authors present a new Chaotic Key-Based Design for Image Encryption and Decryption. It is suggested to use a VLSI architecture for image encryption and decryption. Predetermined keys for the chaotic binary sequence of each pixel's grey level are created using bit-by-bit XORing or XNORing. Little computing complexity, no distortion, and excellent security are some of the characteristics. The advantages of VLSI architecture include inexpensive hardware costs, quick processing, and effective hardware use. The architecture and MPEG2 scheme are both incorporated, and simulation results are also available.

In [2] the authors present a Modified AES Based Algorithm for Image Encryption. Encryption is the most often used method for protecting images. Images and videos have a wide range of uses, including in internet communication, multimedia systems, telemedicine, medical imaging, and military communication. There are various methods of protecting images, like vector quantization. There are various vector quantization techniques that involve breaking the image down into individual vectors and encoding and decoding them one at a time. Or by creating a large number of shadows that guarantee the image will be undetectable to unauthorised users.

In [3] the authors present secure image encryption using AES. In today's world, security is the most important and pressing concern. A big challenge is protecting secrecy from unauthorised access as image transmission for communication has risen. Security for an individual is challenging to give. There are many ways to keep data safe from unauthorised users. When an image needs to be encrypted or decrypted, AES is employed. With the key, the image is first transformed into a format that cannot be recognised, and then, when the recipient is authorised, it is transformed back into the original image.

In [4] the authors present an image encryption and decryption using AES algorithm. By applying the AES algorithm for encryption and decryption, efficient security for image transmission is designed. Data Encryption Standard (DES) has been replaced with AES since it offers greater security. AES key expansion encrypts data using a 128-bit key using bitwise exclusives or operations on image-set pixels.

In [5] the authors present an Image Encryption Based n AES Key Expansion. Images have certain properties such a high rate of transmission with a constrained bandwidth, redundancy, bulk capacity, and pixel correlation. Before encrypting the image, certain features must be taken into consideration. In order to apply bit wise exclusive encryption or operate on image pixels set along with a 128 bit key, the AES technique is used with key expansion. The AES Key Expansion is used to produce the key on both the sender and receiver sides.

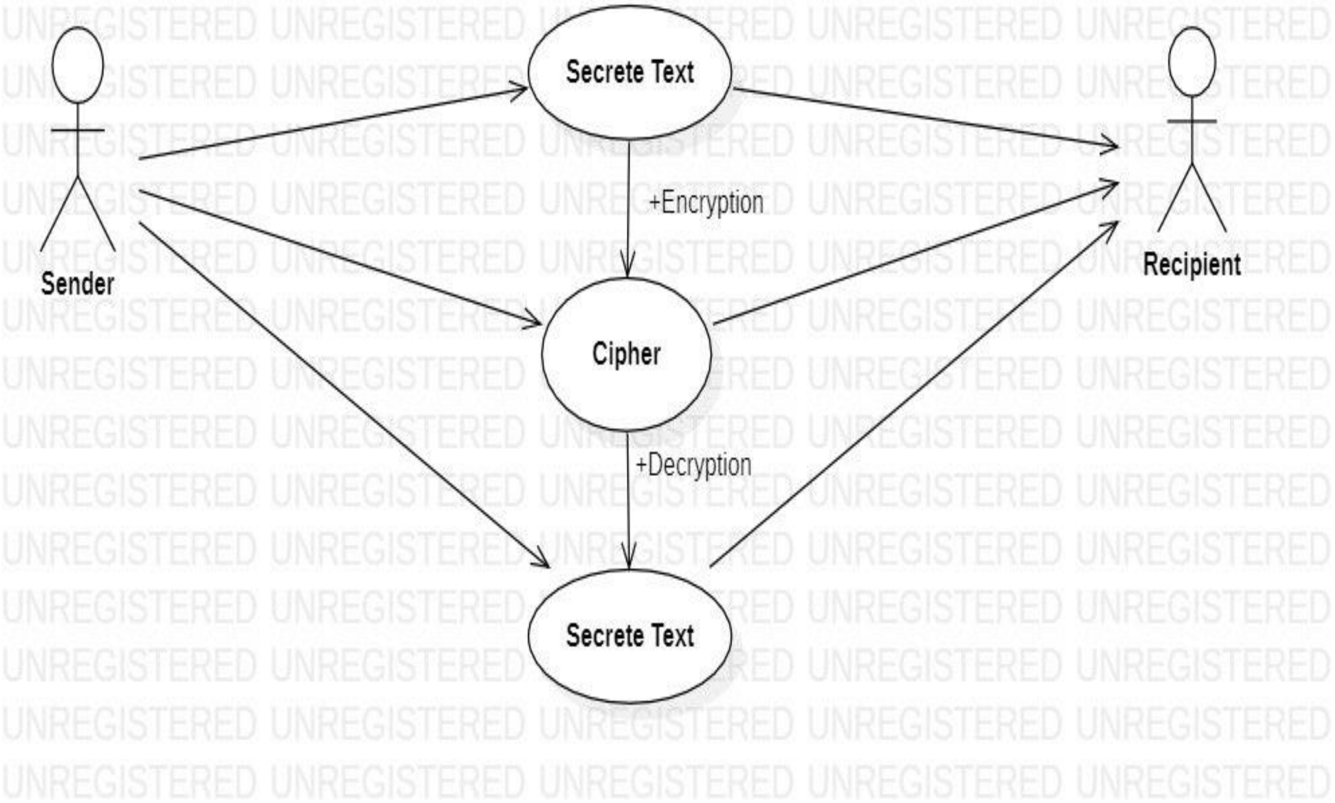
III. Proposed Work

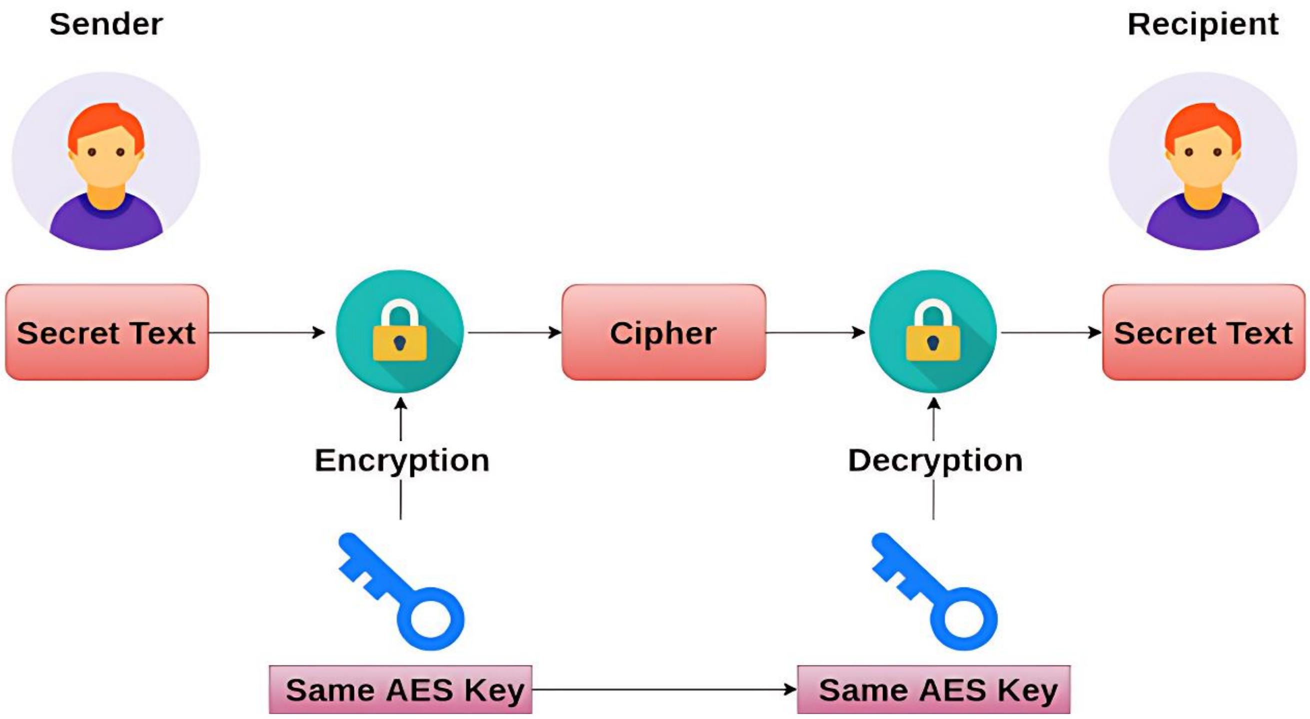
Everywhere it has been used, such as in multimedia systems, medical imaging systems, and military imaging systems, there should be a dependable means of storage and transmission for digital images. The most pressing issue is image security because of the societal use of internet, mobile, and multimedia technology. This project uses the AES algorithm to suggest a safe image encryption and decryption form. Several everyday items, like smart cards, mobile phones, automated teller machines, and web servers, use the AES algorithm. AES converts plaintext into cypher text, which may then be unlocked using a shared private key to reveal the original plaintext. To ensure that it has no memory of the original plain text, the encrypted text is created in a radically different format. Using a key that shouldn't be aware of the image's original shape, the AES encrypts and decrypts images in different ways. It should be restored to its original state after being decrypted. To prevent hackers from learning the image's encryption key, it must be strong.

Strengths of AES:

- AES is extremely fast compared to other block ciphers.
- As the round transformation is parallel for the design, which makes the important for the hardware to allow it for fast execution.
- AES was designed to be agreeable to pipelining.
- There is no arithmetic operations for the cipher, so there is no bias towards the big or little endian architectures.
- AES is fully self-supporting.
- AES is not based on obscure or not well understood processes.

Use Case Diagrams





.

IV. Architecture

Figure 1a is an example of how AES encrypts plaintext to create a cypher text that can be decrypted to reveal the original plaintext using a common private key. As can be seen, the cypher text should be distinct from and provide no hint as to the original plaintext. Figure 1a illustrates the use of a cypher key to encrypt an AES operation. When the plain text and key are provided to the encryptor, it encrypts the data and produces cypher text as the end result of the encryption process. Reverse decryption occurs when the cypher text and key are delivered to the decryptor, which produces the original plain text.

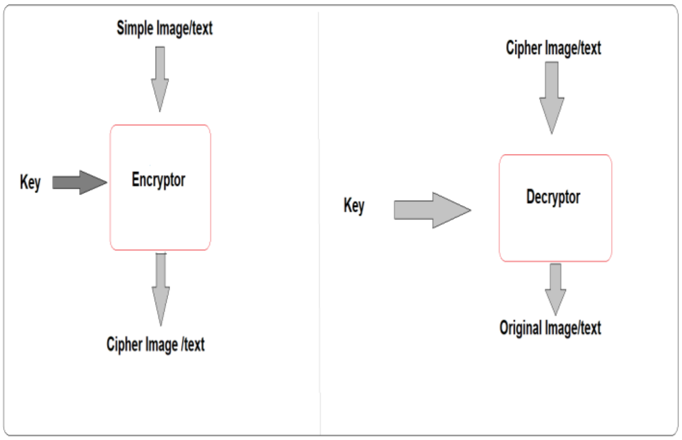


Fig 1a: Encryption and decryption of AES operation.

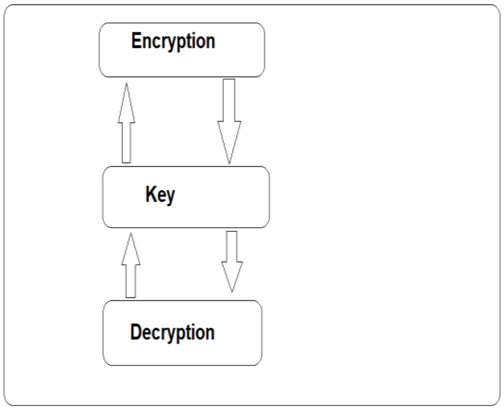


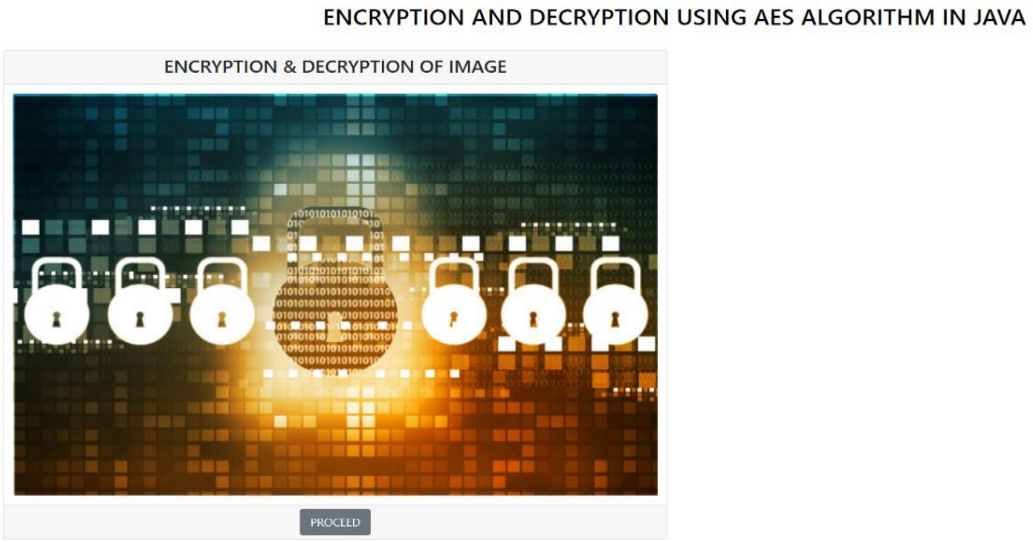
Fig 1b: Example for AES Encryption and Decryption

For the applications of AES image encryption and decryption, the encrypted image should be different from and give no clue to the original one, an example figure1b is shows the encrypted image and that encrypted image to original image.

With AES encryption, the secret key is known to both the sender and the receiver. The AES algorithm remains secure, the key cannot be determined by any known means, even if an eavesdropper knows the plaintext and the cipher text. The AES algorithm is designed to use one of three key sizes (Nk). AES-128, AES-196 and AES-256 use 128 bit (16 bytes, 4 words), 196 bit (24 bytes, 6 words) and 256 bit (32 bytes, 8 words) key sizes respectively. These keys, unlike DES, have no known weaknesses. All key values are equally secured thus no value will render one encryption more vulnerable than another. The keys are then expanded via a key expansion routine for use in the AES cipher algorithm.

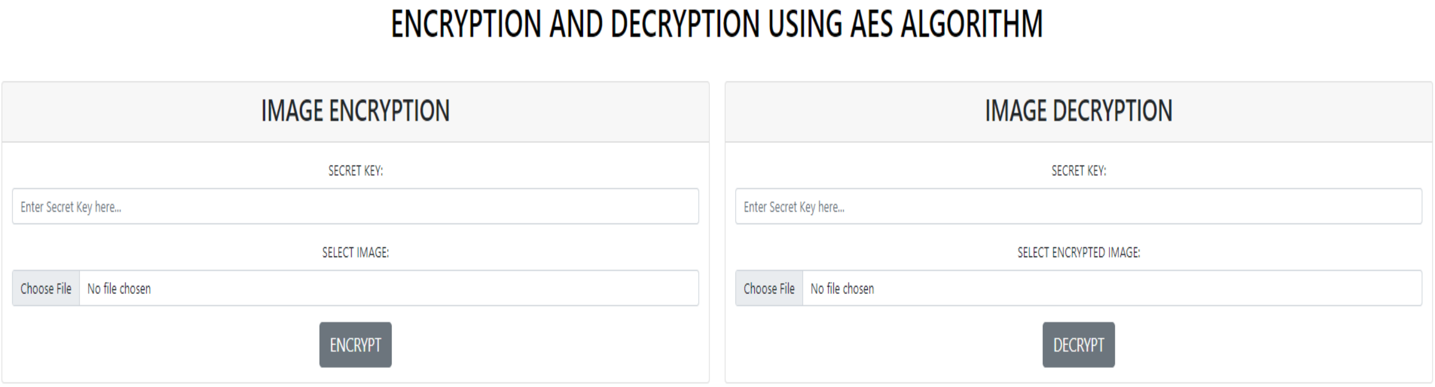
V. Results and Discussion

The image which has to be encrypted is chosen from the folder and the encrypt button is clicked. The original input image taken in the form of .GIF file as shown in fig 3. Once the image is encrypted successfully then the message is displayed fig 4. And when the image is viewed it show that the image is encrypted fig 5. For decryption of the image which has been encrypted then the encrypted image has to be select and then decrypted button is clicked, then the successful decryption messaged is shown fig 6. When the image is viewed then it shows the original image shown in fig 7.



ENCRYPTION AND DECRYPTION USING AES ALGORITHM IN JAVA

ENCRYPTION & DECRYPTION OF IMAGE



ENCRYPTION AND DECRYPTION USING AES ALGORITHM

IMAGE ENCRYPTION

SECRET KEY:

Enter Secret Key here...

SELECT IMAGE:

Choose File No file chosen

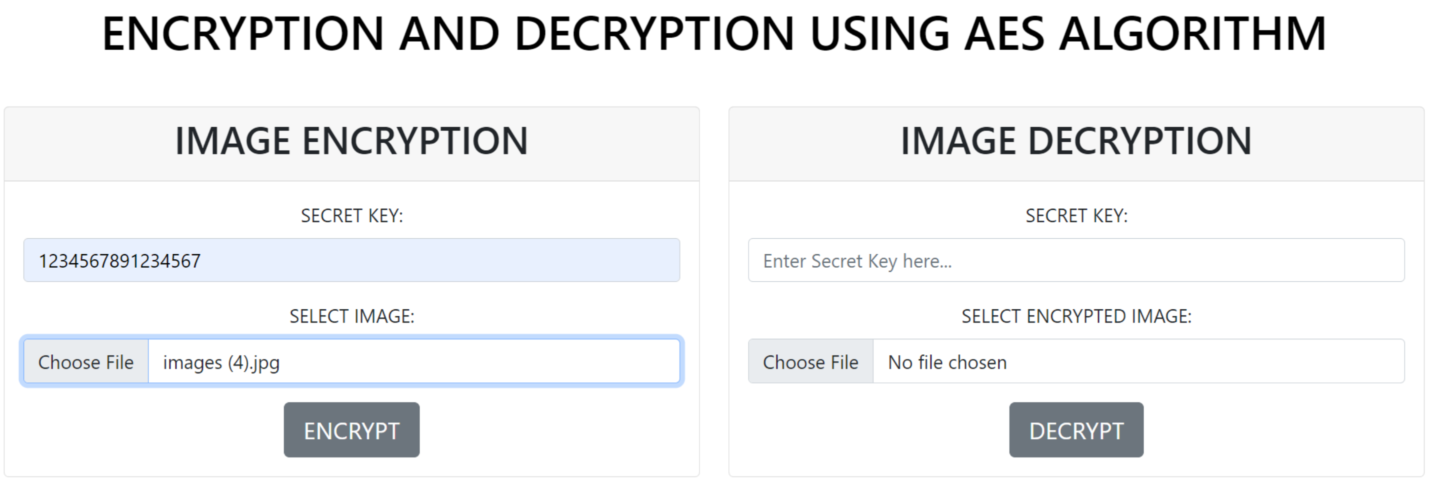
IMAGE DECRYPTION

SECRET KEY:

Enter Secret Key here...

SELECT ENCRYPTED IMAGE:

Choose File No file chosen



ENCRYPTION AND DECRYPTION USING AES ALGORITHM

IMAGE ENCRYPTION

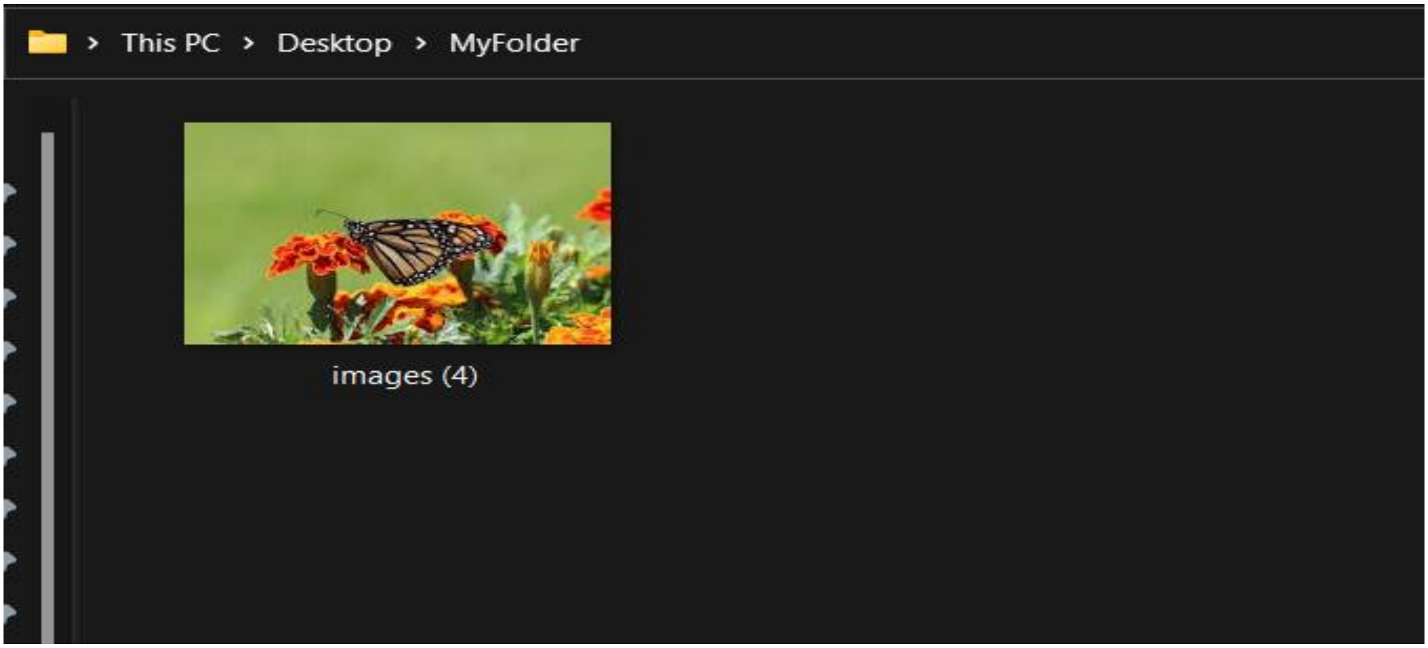
SECRET KEY: 1234567891234567

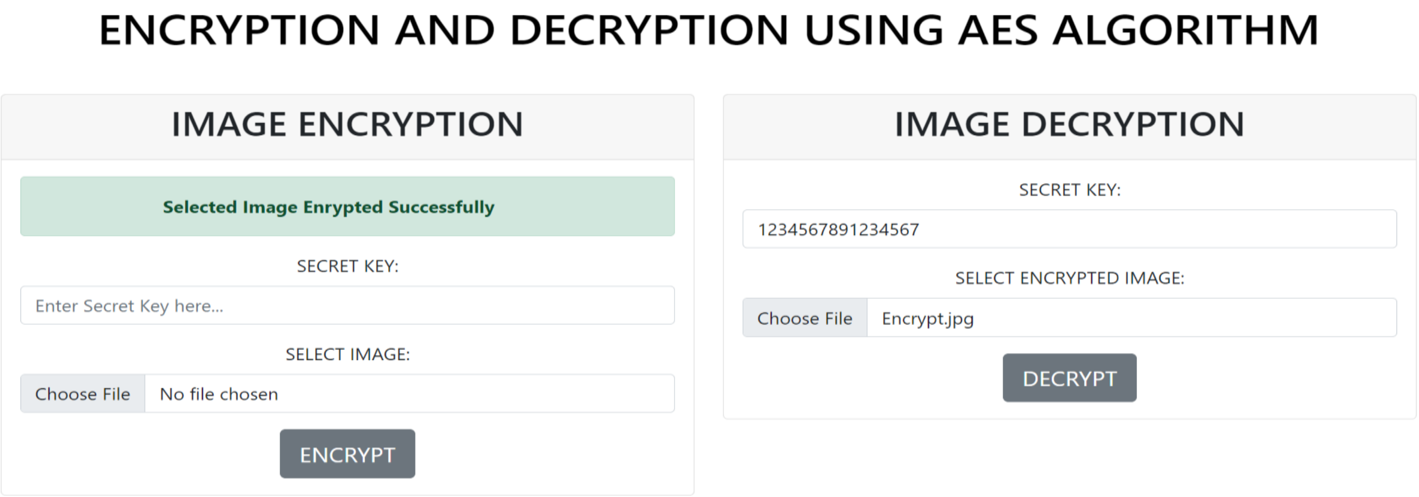
SELECT IMAGE: Choose File images (4).jpg

IMAGE DECRYPTION

SECRET KEY: Enter Secret Key here...

SELECT ENCRYPTED IMAGE: Choose File No file chosen





ENCRYPTION AND DECRYPTION USING AES ALGORITHM

IMAGE ENCRYPTION

Selected Image Enrypted Successfully

SECRET KEY:

Enter Secret Key here...

SELECT IMAGE:

Choose File No file chosen

ENCRYPT

IMAGE DECRYPTION

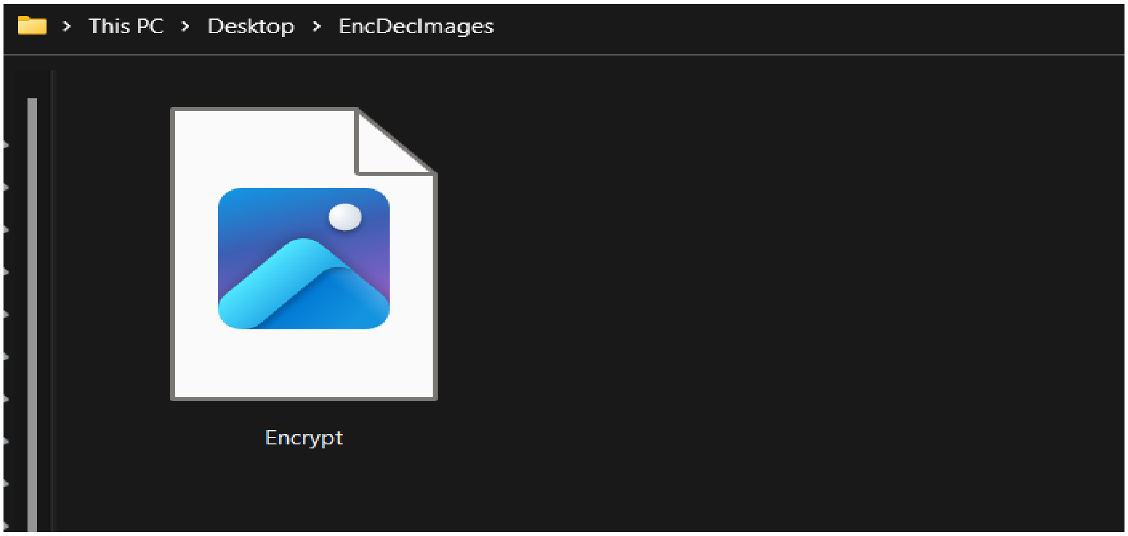
SECRET KEY:

1234567891234567

SELECT ENCRYPTED IMAGE:

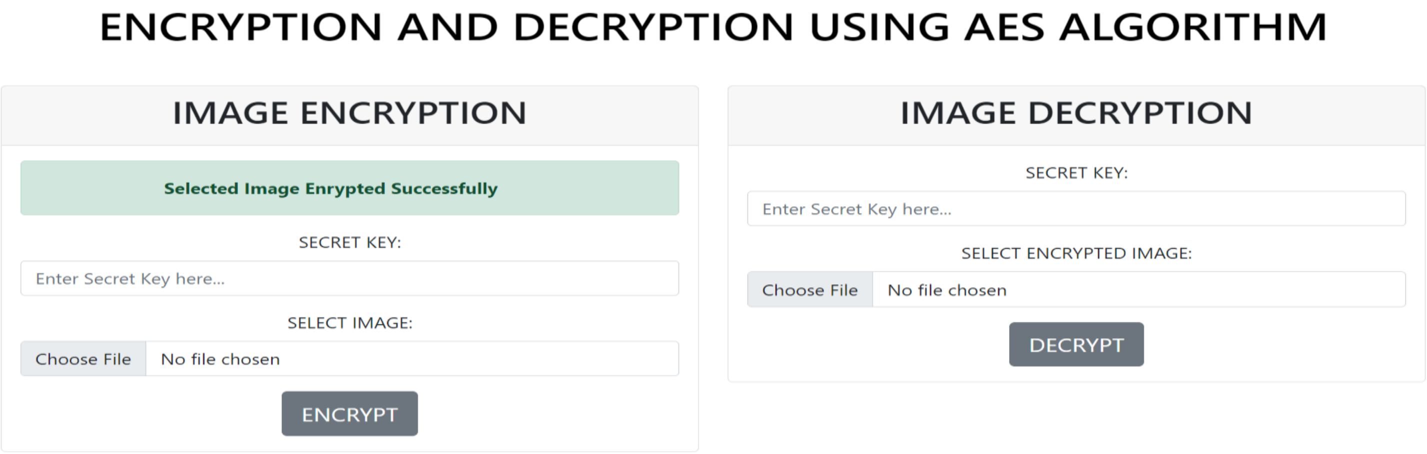
Choose File Encrypt.jpg

DECRYPT



This PC › Desktop › EncDecImages

Encrypt



ENCRYPTION AND DECRYPTION USING AES ALGORITHM

IMAGE ENCRYPTION

Selected Image Enrypted Successfully

SECRET KEY:

Enter Secret Key here...

SELECT IMAGE:

Choose File No file chosen

ENCRYPT

IMAGE DECRYPTION

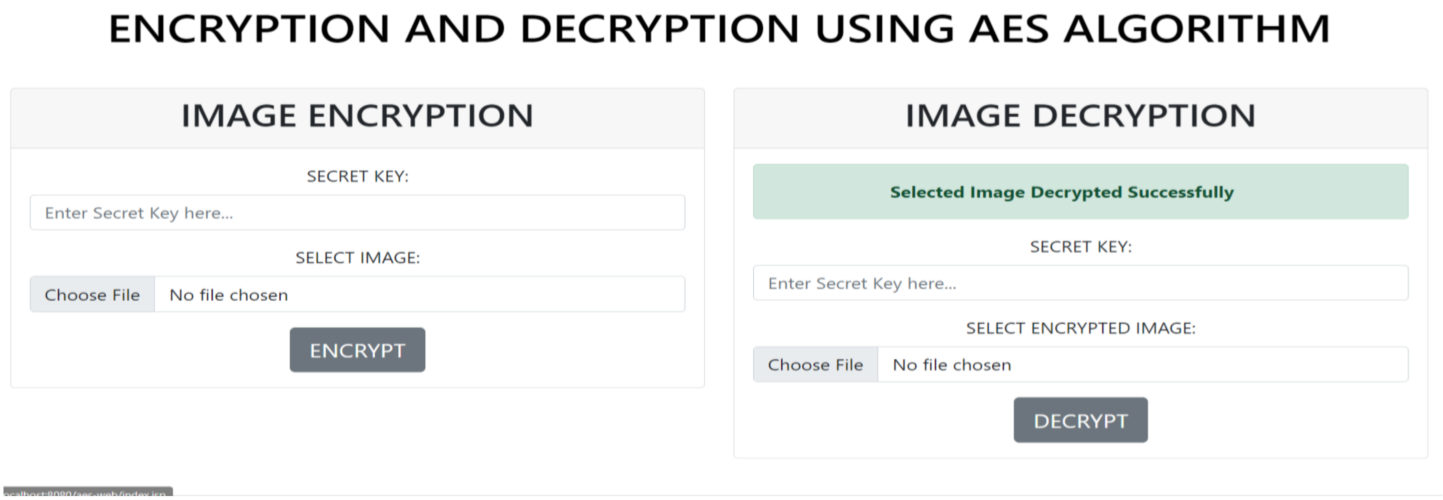
SECRET KEY:

Enter Secret Key here...

SELECT ENCRYPTED IMAGE:

Choose File No file chosen

DECRYPT



ENCRYPTION AND DECRYPTION USING AES ALGORITHM

IMAGE ENCRYPTION

SECRET KEY: Enter Secret Key here...

SELECT IMAGE: Choose File No file chosen

ENCRYPT

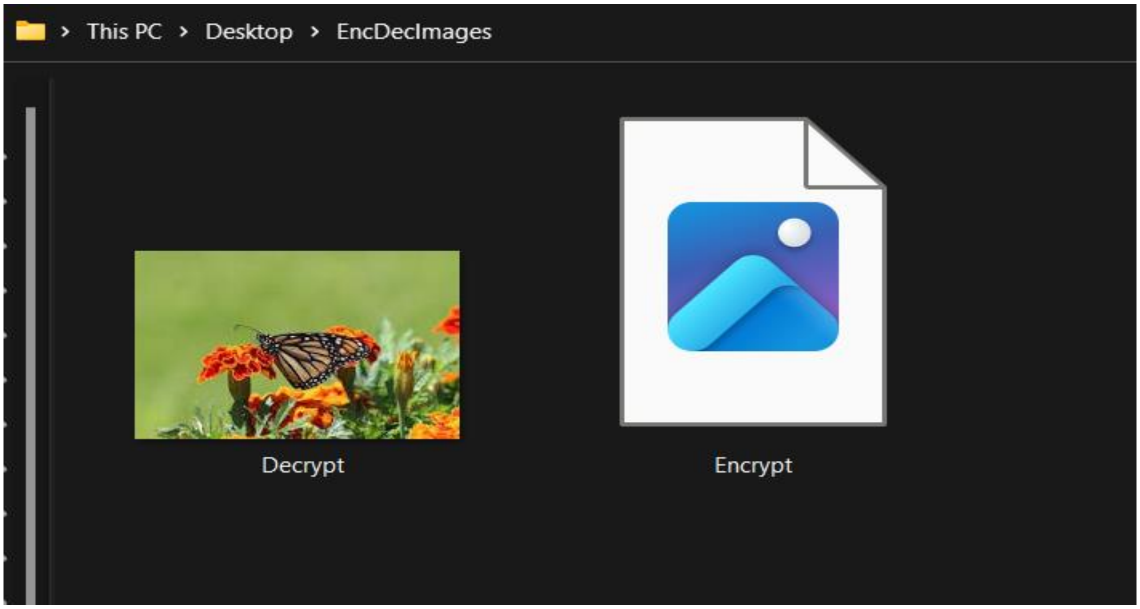
IMAGE DECRYPTION

Selected Image Decrypted Successfully

SECRET KEY: Enter Secret Key here...

SELECT ENCRYPTED IMAGE: Choose File No file chosen

DECRYPT



The image is encrypted and decrypted using AES algorithm with 128 bit of key. The original image with key is given where it is converted into a blank form and send to the receiver where receiver will convert back into original image using key. It provides the security form inducer and widely used.

VI. Conclusion and Futurework

The numerous future possibilities that our project presents excite us greatly. Getting the decrypted image back in colour is one improvement that might be made. Also, we are eager to encrypt videos by simultaneously extracting and encrypting each frame. We are aware that every video has sound. Hence, we want to concurrently encrypt frames and sound. Lastly, once we have accomplished everything above, we hope to design an app that will accomplish everything. If there are two users of the app, one will switch between being the sender and the receiver at any given time depending on which user's needs to be met. We are considering the future of our project and looking forward to effectively putting all of the aforementioned into practice.

VII. Biblography

[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