## PROJECT REPORT

## ON

## IMAGE ENCRYPTION USING TRIPLE DES

## By

## V.Sharath

## B.Tech(Information Technology)

## Institute: Gokaraju Rangaraju Institute of Engineering and

## Technology,Hyderabad

## Email: sharathmithun@gmail.com

***Under the Esteemed guidance of***

**Exposys Data Labs, Bangalore**

**ABSTRACT**

Encryption is the process of encoding information or data in order to prevent unauthorized access. These days we need to secure the information that is stored in our computer or is transmitted via internet against attacks.

In this project we will encrypt and decrypt the image using triple des algorithm.At the time encryption of image we use a key to encrypt the image and also we use the same key at the time of decryption of image. This project works in such a manner that the sender will encrypt the image using a key and sends the encrypted image to the reciver , now the reciver should use the same key to decrypt image. So we can understand that we protect our data from intruders while transfering any classified information from sender to reciver. So many military organizations, intelligence agencies and many more companies use these kind of technequiue to transfer data . and with the help of 3DES we can protect our data from meet in the middle attack from the hackers which Double DES and DES algorithms cant’t do .

**TABLE OF CONTENTS**

s.no Name pg.no

1 **Certificate** 1

2 **Abstract** 2

3 **Table of contents** 3

4 **Introduction** 4-5

5 **Existing Method** 6-7

6 **Proposed Systems** 7

7 **Proposed Method with Architecture** 8-11

8 **Methodology** 12

9 **Implementation** 13

9.1Sample code 13

10 **Conclusion** 14

**INTRODUCTION**

Cybersecurity is a set of strategies for securing networks, programmes, and data against attack, harm, and unwanted access. Information security, which is designed to maintain the confidentiality, integrity, and availability of data, is a subset of cybersecurity. The use of cyber security can help prevent cyber attacks, data breaches, and identity theft and can aid in risk management. On an information system, the data that is stored, transported, or utilised. After all, data is what a criminal seeks. The network, servers, and computers are merely conduits for data. Cybersecurity that is effective decreases the danger of cyber-attacks and protects organisations and individuals against illegal use of systems, networks, and technology. People, processes, and technology are the three pillars of a strong cybersecurity deployment. This three-pronged strategy protects businesses from both highly orchestrated attacks and frequent internal dangers like unintentional breaches and human error.

**Why is cybersecurity important?**

Listed below are the reasons why cybersecurity is so important in what’s become a predominant digital world:

* With each passing year, the sheer volume of threats is increasing rapidly. *According to the report by McAfee, cybercrime now stands at over $400 billion, while it was $250 billion two years ago.*
* Cyber attacks can be extremely expensive for businesses to endure. In addition to financial damage suffered by the business, a data breach can also inflict untold reputational damage.
* Cyber-attacks these days are becoming progressively destructive. Cybercriminals are using more sophisticated ways to initiate cyber attacks.
* Regulations such as GDPR are forcing organizations into taking better care of the personal data they hold.

Because of the above mentioned reasons, cybersecurity has become a significant aspect of the business, and the focus today is on building suitable reaction strategies that minimise the impact of a cyber assault. However, an organisation or individual can only design a proper response strategy if he or she understands the foundations of cybersecurity.

## ****The CIA Triad****

***Confidentiality, integrity, and availability***, also known as the CIA triad, is a model designed to guide companies and organizations to form their security policies. Technically, cybersecurity means protecting information from unauthorized access, unauthorized modification, and unauthorized deletion in order to provide confidentiality, integrity, and availability.



**EXISTING METHOD**

There are many methods to encrypt and decrypt images now-a-days.well there are mainly two types of methods .

## 1.Symmetric Encryption

The symmetric encryption method, as the name implies, uses a single cryptographic key to encrypt and decrypt data. The use of a single key for both operations makes it a straightforward process, and hence it’s called “symmetric.”

There are hundreds of symmetric key algorithms in existence, which you may or may not be aware of! AES, RC4, DES, 3DES, RC5, RC6, and other encryption algorithms are some of the most popular. The DES and AES algorithms are the most well-known of these algorithms.

#### **DES Symmetric Encryption Algorithm**

#### **3DES Symmetric Encryption Algorithm**

#### **AES Symmetric Encryption Algorithm**

These three algorithms are most commonly used for encryption these days.

**2.Asymmetric Encryption**

Asymmetric encryption, in contrast to the symmetric encryption method, involves multiple keys for encryption and decryption of the data. Asymmetric encryption encompasses two distinct encryption keys that are mathematically related to each other. One of these keys is known as the “public key” and the other one as the “private key.” Hence, why the asymmetric encryption method is also known as “public key cryptography.”

#### **. RSA Asymmetric Encryption Algorithm**

#### **ECC Asymmetric Encryption Algorithm**

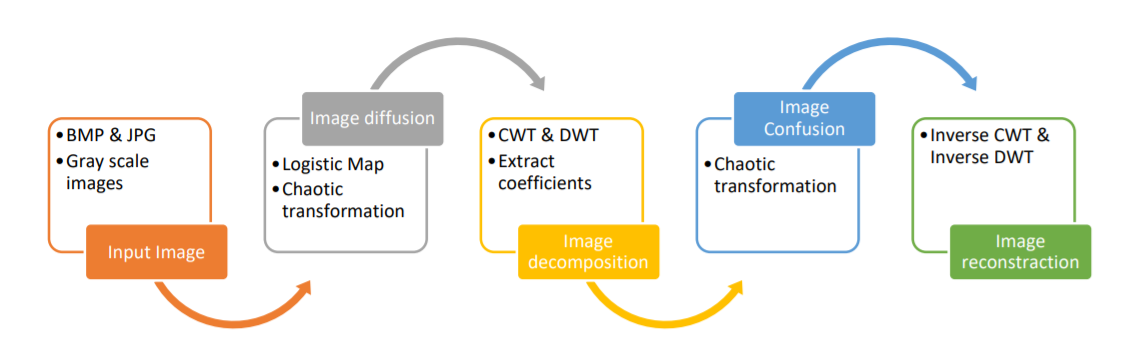
These are the most common asymmetric algorithms for encryption .

**PROPOSED SYSTEMS**

* **Digital Image Encryption Based on Chaos Theory**

Image encryption has attracted a large number of researchers and experts in recent decades as one of the most important information security topics. However, multiple studies using various methodologies have been conducted, and unique and valuable algorithms have been proposed to improve secure image processing.

Nowadays, chaotic methods have been found in diverse fields, such as the design of cryptosystems and image encryption. Chaotic methods-based digital image encryptions are a novel image encryption method. This technique uses random chaos sequences for encrypting images, and it is a highly-secured and fast method for image encryption. Limited accuracy is one of the disadvantages of this technique. This paper researches the chaos sequence and wavelet transform value to find gaps. Thus, a novel technique was proposed for digital image encryption and improved previous algorithms. The technique is run in MATLAB, and a comparison is made in terms of various performance metrics such as the Number of Pixels Change Rate (NPCR), Peak Signal to Noise Ratio (PSNR), Correlation coefficient, and Unified Average Changing Intensity (UACI). The simulation and theoretical analysis indicate the proposed scheme’s effectiveness and show that this technique is a suitable choice for actual image encryption.



The proposed algorithm for image encryption

**PROPOSED METHOD WITH ARCHITECTURE**

* **ENCRYPTION**

NORMAL IMAGE

TRIPLE DES ALGORITHM PERFORMED

ON PLAIN IMAGE

ENCRYPTED IMAGE

* **DECRYPTION**

ENCRYPTED IMAGE

TRIPLE DES ALGORITHM IS PERFORMED

ON ENCRYPTED IMAGE

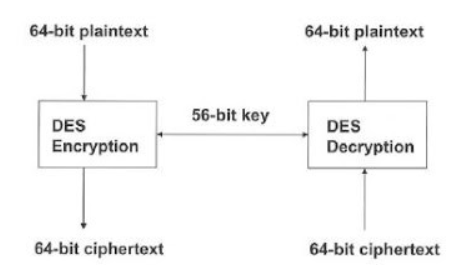
NORMAL IMAGE

**DES ALGORITHM**

DES is a block cypher that encrypts data in 64-bit blocks. This implies that 64 bits of plain text are fed into DES, which generates 64 bits of encrypted text. Encryption and decryption employ the same algorithm and key, with slight variations. The key is 56 bits long.

We have mention that DES uses a 56 bit key. Actually, the initial key consists of 64 bits. However, before the DES process even starts, every 8th bit of the key is discarded to produce a 56 bit key. That is bit position 8, 16, 24, 32, 40, 48, 56 and 64 are discarded.

Thus, the discarding of every 8th bit of the key produces a 56-bit key from the original 64-bit key.

****

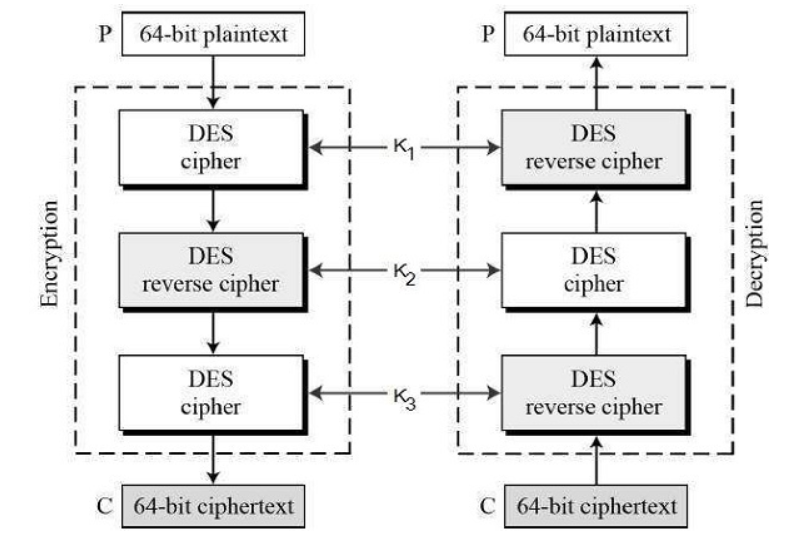
DES is built on two cryptographic fundamentals: substitution (also known as confusion) and transposition (also called as diffusion). DES has 16 steps, each of which is referred to as a round. Substitution and transposition are performed in each round.

In DES encryption and decryption process is done according to feistel process.

**TRIPLE DES ALGORITHM**

Triple DES algorithm is more secure than DES and Double DES algorithms.In

Triple DES the DES is performed thrice on plain text/image for encryption and as well as decryption . In triple DES it uses three security keys for encryption and decryption



The encryption-decryption process is as follows −

* Encrypt the plaintext blocks using single DES with key K1.
* Now decrypt the output of step 1 using single DES with key K2.
* Finally, encrypt the output of step 2 using single DES with key K3.
* The output of step 3 is the ciphertext.
* Decryption of a ciphertext is a reverse process. User first decrypt using K3, then encrypt with K2, and finally decrypt with K1.

Because Triple DES is vulnerable to a meet-in-the-middle attack, it uses a total security level of 2^112 instead of a 168-bit key. Because of the small block size and the usage of the same key to encrypt huge amounts of text, a block collision attack is also possible. It's also prone to a sweet32 attack.

**METHODOLOGY**

The methodology of this project is very simple.we have to select the image we want to encrypt and the image will be encrypted using triple DES algorithm ,finally we will get output as encrypted image.Simillarly the image will be decrypted using triple DES algorithm.

Let’s see the process by using our code

* Firstly we should run our code ,then the code will run and it will ask us to select options 1.Encryption and 2.Decryption
* We should as option 1 and after this it asks for image file path
* We should give the path of the image ,then after this it will asks for key(password) . we should give the password give our password.
* After this all steps the image file will be encrypted.
* We should repeat same process for Decryption as well.

**IMPLEMENTATION**

* **SAMPLE CODE**

from Crypto.Cipher import DES3  
from hashlib import md5  
  
  
while True:  
 print('Choose operation to be done:\n\t1- Encryption\n\t2- Decryption')  
 operation = input('Your Choice: ')  
 if operation not in ['1', '2']:  
 break  
  
   
 file\_path = input('Image File path: ')  
  
 key = input('Enter your Triple DES key: ')  
  
 key\_hash = md5(key.encode('ascii')).digest()  
  
   
 tdes\_key = DES3.adjust\_key\_parity(key\_hash)  
  
 cipher = DES3.new(tdes\_key, DES3.MODE\_EAX, nonce=b'0')  
  
   
 with open(file\_path, 'rb') as input\_file:  
 file\_bytes = input\_file.read()  
  
 if operation == '1':  
 new\_file\_bytes = cipher.encrypt(file\_bytes)  
 else:  
 new\_file\_bytes = cipher.decrypt(file\_bytes)  
  
   
 with open(file\_path, 'wb') as output\_file:  
 output\_file.write(new\_file\_bytes)  
 print('Operation Done!)  
 break

**pycryptodome library is used for this code**

**CONCLUSION**

This is low cost and flexible project . In this project TRIPLE DES algorithm is used . with the help of this project we can encrypt any plain text/images and decrypt them . with the help of this project we can transform any classified information from one person to other without any interruption from intruders.And also we protect our data from several attacks like Meet-in-the-middle attack,block collision attack and sweet32 attacks.