

Hybrid Image ENCRYPTION using AES Algorithm and Chaos Theory

Project report submitted

In partial fulfillment of the requirement for the degree of

Bachelor of Science In Cybersecurity

By

ARIN SUKHWAL (2001830008)

Under the guidance of :

Mr. Manish Kumar

(CEO VIEH GROUP)



Department of Computer Science

School of Engineering and Technology

K. R. Mangalam University, Gurugram - 122003

8-June-2023

Registrar
K.R. Mangalam University
Sohna Road, Gurugram (Haryana)

DECLARATION

We declare that this written submission represents our ideas in our own words and where other's ideas or words have been included, we have adequately cited and referenced the original sources. We also declare that we have adhered to all the principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will be for disciplinary action by the Institute and canal so evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed. We further declare that if any violation of the intellectual property right or copyright, my supervisor and university should not be held responsible for the same.

Student Name **ARIN SUKHWAL**
DNYANAL PATIL

(Roll No.) **2001830008**
2001830002

(Signature)

Place: K.R. Mangalam University

Date: 8 June 2023

CERTIFICATE

It is certified that the work contained in the project report titled " Hybrid Image ENCRYPTION using AES Algorithm and Chaos Theory " by the following students:

VIEH GROUP

Think Secure
Think V.I.E.H

15 October 2022

Experience letter for Internship

TO WHOM IT MAY CONCERN

This is to certify that **Mr. Arin Sukhwal** has completed the Internship of 3 month at VIEH Pvt. Ltd. His Internship tenure was from **1 July 2022 to 30 September 2022**. He was the part of **CyberSecurity team** as a **CyberSecurity Intern** and was actively and diligently involved in the projects and tasks assigned to him.

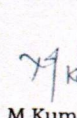

Project name: Image Encryption using AES

Teamleader: Mr. Jai Dhiyanesh J

During the span, we found him punctual and hardworking. His learning powers are good and he picks up swiftly. His feedback and evaluation proved that he learned keenly.

We wish him a bright future.

For V.I.E.H Private Limited

M Kumar
CEO - V.I.E.H Group

Ph: +91 8340254937
support@viehgroup.com
www.viehgroup.com

V.I.E.H Pvt. Ltd.
Andheri west, Mumbai
Maharashtra, India

Cert no: VIEH-INCERT202303

ABSTRACT

Modern days, image security is necessary since data volume is growing rapidly. These data can be images, videos, text, audio, etc., so methods like AES, DES, RSA, etc. have been developed to secure these images from attackers who could reduce the image quality or manipulate the images. Data security has also become a key issue with the generation.

The most significant problem confronting the world now is data security. Advanced encryption standard is applied to protect data during communication, storage, and transfer (AES). AES is a symmetric encryption algorithm that is intended to take the place of DES in business applications. It employs a key size of 128, 192, or 256 bits and a block size of 128 bits. To protect information from unauthorized users, the AES algorithm is used. Both text and image data are encrypted using the AES technique that is currently available.

Key Words: Steganography, AES, Python.

TABLE OF CONTENTS

	Page No
Declaration	i
Certificate	ii
Acknowledgement	iii
Abstract	iv
Chapter 1: INTRODUCTION	7
Chapter 2: LITERATURE REVIEW	8
Chapter 3: PROBLEM FORMULATION AND OBJECTIVES	10
Chapter 4: METHODOLOGY OF THE PROJECT	11
Chapter 5: SECURITY ANALYSIS	13
Chapter 6: IMPLEMENTATION	15
Chapter 7: RESULTS	17
Chapter 8: CONCLUSION	
REFERENCES	

Chapter 1: INTRODUCTION

Image security is very important in today's world. With the ability to share digital images across the internet, it is more important than ever to encrypt your images. AES encryption is a great option for image security. With AES encryption, your images will be safe from prying eyes.

The advanced encryption standard or AES so far all the cryptographic algorithms we have looked so far have some problems like we have seen the classical cryptosystem like shift cipher caesar cipher those are earlier cipher so those are broken. if we have modern computer speed so those are not secured. A hardware which can crack the DES in less than three days and with the cost of very less, this is an exhaustive search attack.

So we need to have an alternative for the standard so we tried with the triple DES but this is basically made from the DES itself which is basically three times more DES operations.

We have we have seen it is a problem with the block size it is a 64 bit block and so the now we need a new encryption algorithm we need a block cipher which is supposed to be secured under the all existing attack so what NIST did so instead of developing a new cipher by themselves what they did they announce a competition worldwide competition and in that competition anybody can participate so so that was in 1997 and they welcome all the cryptographer worldwide to submit their block cipher design so those who are working on the block cipher or in crypto system so they just jump into that competition and they design and so this is the first and this they they fix some requirement

In this report, I have represented a potential secure image steganography tool using Advanced Encryption Standard (AES) technique as the cryptographic tool in the spatial domain of data security.

Chapter 2: LITERATURE REVIEW

Image encryption plays a critical role in ensuring the confidentiality and integrity of digital images during transmission and storage. Advanced Encryption Standard (AES) has emerged as a popular encryption algorithm due to its robustness and efficiency. This literature review aims to explore the current state-of-the-art techniques and research trends in the field of image encryption using AES, specifically focusing on its application in final year projects. The review provides an overview of AES, discusses various image encryption schemes based on AES, highlights their strengths and limitations, and identifies potential areas for further research.

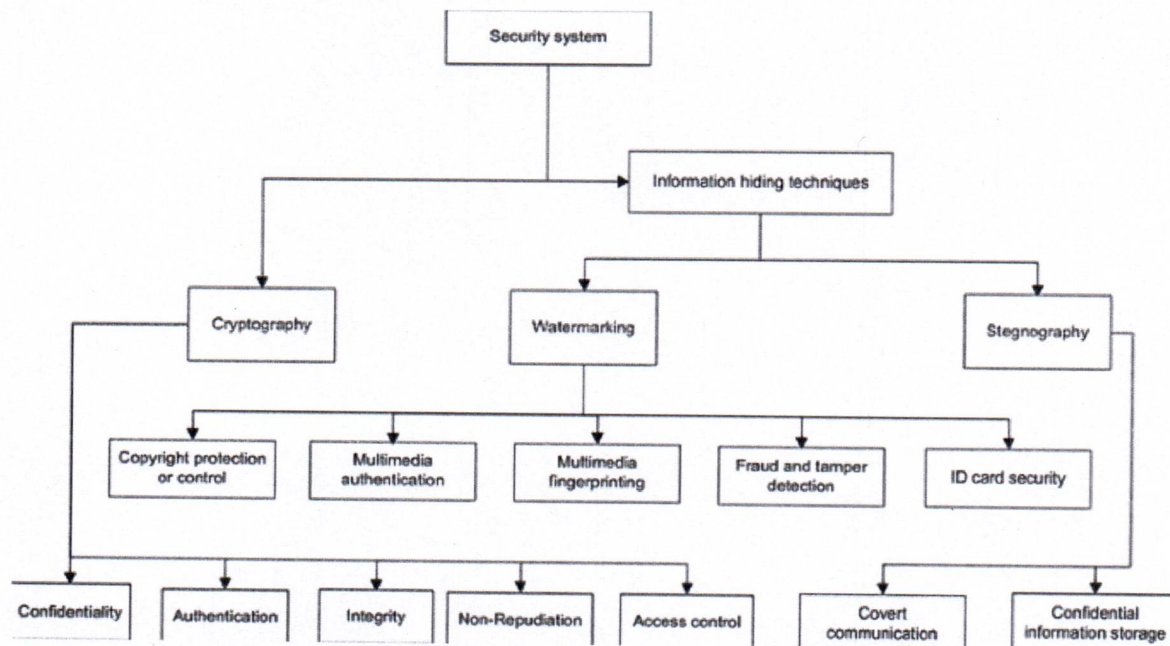
The speed and duration of encryption varies based on the encryption algorithm. Different algorithms that differ from one another are listed :

Data Encryption Standard (DES) : DES is an algorithm for encrypting data. It was developed in the 1970s and was originally used by the US government. DES is a symmetric key algorithm, which means that the same key is used for both encryption and decryption. DES is no longer considered secure, and has been replaced by newer algorithms such as AES.

Triple DES : (3DES), is a symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. Triple DES provides a relatively simple and inexpensive method of increasing the data encryption level, without the need to develop a completely new cipher algorithm. It is available in the `flake` and `libmccrypt` libraries.

RSA : The Rivest-Shamir-Adleman (RSA) algorithm is a public-key encryption method developed in 1977 by Ronald Rivest, Adi Shamir, and Leonard Adleman. It is based on the fact that it is very difficult to factorize a large number that is the product of two large prime numbers. The RSA algorithm is used in a wide variety of security protocols, including PGP, SSL, and SSH.

Information security techniques are classified, along with their uses.

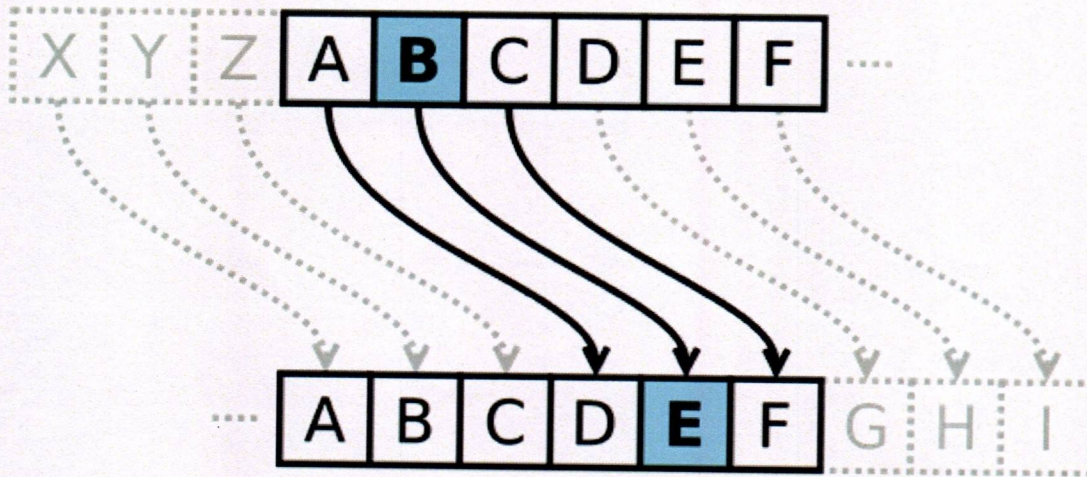


The strength of AES lies in its ability to resist various types of attacks, including brute-force attacks, differential and linear cryptanalysis, and known-plaintext attacks. It achieves this through its carefully designed cryptographic transformations, including substitution, permutation, and mixing operations.

Chapter 3: PROBLEM FORMULATION AND OBJECTIVES

In the past, encryption was critical to allowing two people to communicate secretly.

The same demand still exists today, for instance when sending your payment card information over the Internet and wanting it to be kept private from everyone but you and the vendor (like Amazon). Digital signatures, which are closely related to encryption, are another variation on this theme that allows you to sign a document while mathematically tying it to you. For practically everyone to survive and live freely, every organization and person needs privacy. A lack of privacy makes your plans, wants, and ideas known to those who have competing aims or those who want to control your conduct in a competitive world.



Chapter 4: METHODOLOGY OF THE PROJECT

Image steganography is a GUI-based project in which we are hiding a secret message within the image using encoding and decoding functions. We are creating a window in which there are two buttons: encoding and decoding.

For encoding, Type message in the message box then it will convert into base64, type the key to secure data, select any image, Then type merge this encoded string into image and the user can save the image where he/she wants.

For decoding, select the image which is encoded, the base64 string will get separated by decoding, and by Tkinter module hidden text is shown in the textbox.

Advanced Encryption Standard :

AES has an initial key addition round denoted by AddRoundKey, then $Nr-1$ number of transformation rounds and a final round at the end. The input for Nr round including AddRoundKey is State and Round key. Three stages in AES are as follows :

- 1) AddRoundKey Transformation Round
- 2) $Nr-1$ rounds each composed of 4 transformation rounds
 - a) SubBytes Transformation
 - b) Shift Rows Transformation
 - c) Mix Columns Transformation
 - d) Add Round Key Transformation
- 3) A Final Round composed of
 - a) SubBytes Transformation
 - b) Shift Rows Transformation
 - c) Add Round Key Transformation

Studied the working of AES algorithm to encrypt and then decrypt a digital image using AES algorithm using python modules. Observed and analyzed different modes of AES encryption and decryption.

1. To run the code, any python ide can be used like pycharm, jupyter notebook, google collab.
2. Following Libraries need to installed before running the python code
 - a. Dlib (The dlib library should be installed)

- b. Scipy
- c. OpenCv
- d. Numpy
- e. Imutils
- f. pygame
- g. argparse

3. Python versions above 3.6 can be used.

Chapter 5: SECURITY ANALYSIS

The project aims to develop an image encryption system that utilizes the Advanced Encryption Standard (AES) algorithm combined with Chaos Theory principles. This security analysis assesses the potential strengths and weaknesses of the proposed approach.

AES Encryption Strength:

The AES algorithm is widely recognized as a secure and robust symmetric encryption standard. It has been extensively studied and tested, with no practical vulnerabilities found when implemented correctly. By employing AES as the core encryption mechanism, the project benefits from a strong foundation for data confidentiality.

Chaotic Encryption Enhancement:

Integrating Chaos Theory principles into the image encryption process introduces additional complexity and randomness. Chaos-based encryption schemes offer the potential to enhance the security of AES by introducing more unpredictable key generation and permutation processes.

Key Generation:

The security of the encryption system heavily relies on the strength of the key generation process. AES requires a sufficiently long and truly random key to resist brute-force attacks effectively. Similarly, the chaos-based component should generate keys with high entropy and avoid patterns that could be exploited by adversaries.

Encryption Speed and Efficiency:

While security is a crucial aspect, it is also essential to consider the performance of the encryption system. AES is generally fast and efficient in hardware and software implementations, making it suitable for real-time encryption of images. However, the incorporation of Chaos Theory may introduce additional computational overhead, which needs to be evaluated to ensure acceptable processing times.

Randomness and Entropy:

Chaotic systems are known for their inherent randomness and sensitivity to initial conditions. It

is vital to evaluate the randomness and entropy properties of the chaotic sequences used in key generation and permutation processes. The level of randomness should be high enough to resist statistical attacks and ensure that the encryption system produces cipher images with properties indistinguishable from random noise.

Avalanche Effect and Diffusion:

The encryption system should possess a strong avalanche effect, meaning that a small change in the input should result in significant changes in the output. Similarly, diffusion should spread the influence of each input bit across the entire cipher image. Both properties enhance the resistance against known-plaintext attacks and guarantee that small modifications in the original image will yield a completely different cipher image.

Chapter 6: IMPLEMENTATION

While working I have gained a newer kind of experience. After collecting and analyzing data I have got some idea about the overall project management

RESOURCES AND PROJECT TIME :

I completed during this time frame and provided an estimate of how long the task took.

HARDWARE REQUIREMENTS

Processor: Intel or AMD with 2GHz or higher.

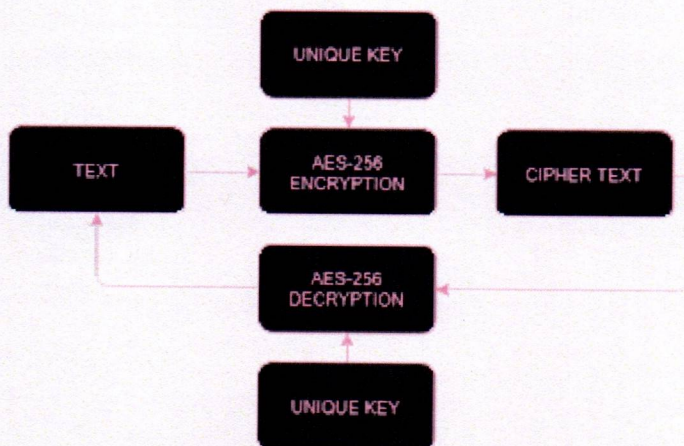
Memory: 2 GigaBytes or More.

Storage: Depending on images being used.

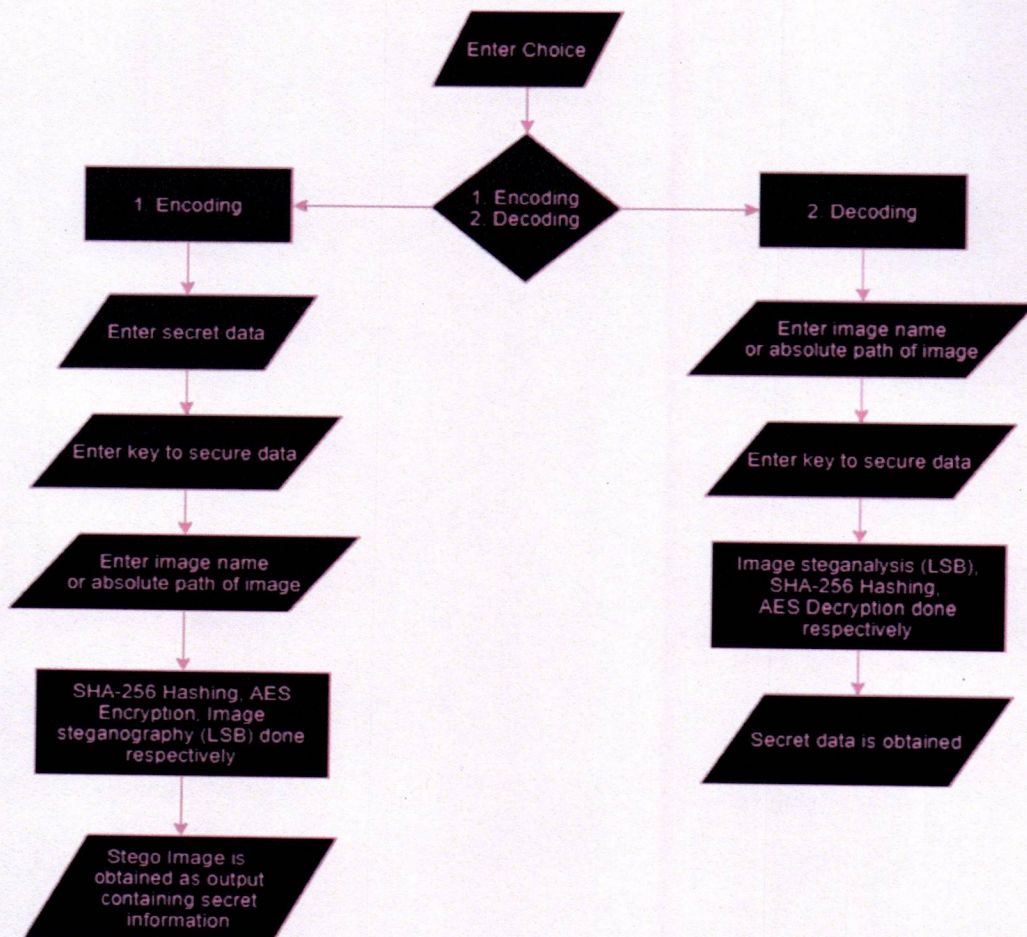
SOFTWARE REQUIREMENTS

OS: Windows 8 or Higher.

Programming Language: Python



Workflow/Mindmap of the project development :



Chapter 7: RESULTS

The project "Image Encryption Using AES" has been completed within a given time and final testing has been done , we have applied the secret key and confidential data combined on a Image.

The snap of working Encryption page code -

```
class encrypt_page():
    def __init__(self):
        self.file={}
        self.stri=""
        self.Handel_Buttons()
        self.pushButton_3.clicked.connect(self.chooseFile)
        self.pushButton_4.clicked.connect(self.onClickEncrypt)
    def Handel_Buttons(self):
        self.pushButton.clicked.connect(lambda: self.stackedWidget.setCurrentIndex(1))
    def chooseFile(self):
        self.file = QFileDialog.getOpenFileName(self, 'Open File')
        pixmap = QtGui.QPixmap(self.file[0])
        self.lbl.setPixmap(pixmap.scaledToHeight(201))
        if self.file != None:
            ba = QtCore.QByteArray()
            buff = QtCore.QBuffer(ba)
            buff.open(QtCore.QIODevice.WriteOnly)
            ok = pixmap.save(buff, "PNG")
            assert ok
            pixmap_bytes = ba.data()
            #print(type(pixmap_bytes))
            #data = self.file[0]
            self.stri = base64.b64encode(pixmap_bytes)
```

```
class decrypt_page():
    def __init__(self):
        self.cipher={}
        self.Handel_Buttons()
        self.pushButton_5.clicked.connect(self.chooseFile1)
        self.pushButton_6.clicked.connect(self.onClickDecrypt)
    def Handel_Buttons(self):
        self.pushButton.clicked.connect(lambda: self.stackedWidget.setCurrentIndex(1))
    def chooseFile1(self):
        file = QFileDialog.getOpenFileName(self, 'Open File')
        text=open(file[0]).read()
        #print(text.encode('utf-8'))
        self.cipher= text.encode('utf-8')
    def onClickDecrypt(self):
        myKey=self.lineEdit_2.text()
        x = Decrypter(self.cipher)
        image=x.decrypt_image(myKey)

        ba = QtCore.QByteArray(image)
        pixmap = QtGui.QPixmap()
        ok = pixmap.loadFromData(ba, "PNG")
        assert ok
        self.lbl_2.setPixmap(pixmap.scaledToHeight(201))
```


CONCLUSION

In order to become acquainted with the other encryption algorithms used in encoding the image that has been transmitted over link, a number of significant algorithms, image encryption techniques, different encryption schemes, type of image used, and various types of mathematical computations have been existing and examined. This project's main objective is to work in the field of data security encryption. Time and power restrictions are tested using different algorithms and techniques both separately and in combination.

REFERENCES

1. Mustafa Emad Hameed^{1,2}, Masrullizam Mat Ibrahim¹ , NurulfajarAbdManap¹,
—Review on Improvement of Advanced Encryption Standard (AES) Algorithm based on
Time Execution, Differential Cryptanalysis and Level of Security.
2. Sandeep Srivastava, Sanjay Kumar, —Image Encryption using Simplified Data
Encryption Standard