# IMAGE ENCRYPTION USING AES

## PROJECT REPORT

**18CSE383T – INFORMATION ASSURANCE AND SECURITY**

**(2018 Regulation)**

**III Year/ V Semester**

**Academic Year: 2022 -2023**

By


**SESHAPRIYAN T (RA2011030010013)**

**ANIRUDH SUNIL AMBADY (RA2011030010029)**

Under the guidance of

**Dr. K.A. VARUN KUMAR**

**Assistant Professor**

**Department of Networking and Communications**




**COLLEGE OF ENGINEERING AND TECHNOLOGY**

**SCHOOL OF COMPUTING**

**SRM INSTITUTE OF SCIENCE AND TECHNOLOGY**

**Kattankulathur, Kancheepuram**


**NOVEMBER 2022**

## BONAFIDE

This is to certify that **18CSE383T – INFORMATION ASSURANCE AND SECURITY mini project report** titled "**IMAGE ENCRYPTION USING AES"** is the bonafide work of **SESHAPRIYAN T (RA2011030010013) and ANIRUDH SUNIL AMBADY (RA2011030010029)** who undertook the task of completing the project within the allotted time.

**Signature of the Faculty**
Dr. K.A. Varun Kumar
**Assistant Professor**
Department of NWC
SRM Institute of Science and Technology

**Signature of the II Year Academic Advisor**
Dr. Annapurani Panaiyappan .K
**Professor and Head**
Department of NWC
SRM Institute of Science and Technology

# TABLE OF CONTENTS


| Chapter No. | Title | Page Number. |
|---|---|---|
| | Abstract | 4 |
| 1. | Introduction | 5 |
| 2. | Literature review | 6 |
| 3. | Proposed Model | 8 |
| 4. | Result | 11 |
| 5. | Conclusion | 12 |
| | Reference | 13 |

# ABSTRACT

The sharing of information has increased significantly in the age of digital communication. All transmitted and received data are susceptible to numerous active and passive cyberattacks. Therefore, the main problem is keeping the data secure when communicating. In order to secure network communication, cryptography plays a crucial role. It also offers a fantastic solution for providing the necessary protection against data intruders. In an effort to create robust communication security, data encryption techniques made a significant progression through time from relatively simple ways to extremely challenging mathematical calculations. Cryptographic algorithms are vulnerable to several attacks despite their complexity.

# CHAPTER 1

## INTRODUCTION

Security of images is crucial in today's systems of image communication. Confidential picture data must be shielded from unauthorised users. Finding and identifying illegal users is a difficult task. Various scholars put out various methods for protecting image transmission. Today, practically all digital services including internet communication, imaging systems for the military and healthcare, and multimedia systems demand trustworthy security for the transmission and storage of digital images. Image encryption solutions are required in order to protect photos from such attacks due to the quicker proliferation of multimedia technologies, the internet, and cellphones. To hide images in this system, we employ AES (Advanced Encryption Technique). Such encryption methods aid in the prevention of intrusion attacks.

# CHAPTER 2

# LITERATURE SURVEY

## Cryptography:

The study and application of methods for secure communication in the midst of hostile activity is known as cryptography or cryptology. Creating and evaluating methods that prohibit the public or other parties from reading private messages is more usually referred to as cryptography. Modern cryptography places a strong emphasis on data secrecy, data integrity, and authentication. The fields of mathematics, computer science, electrical engineering, communication science, and physics all connect with modern cryptography. Electronic commerce, chip-based payment cards, digital currencies, the military, and other fields all use cryptography in some capacity.

## Encryption:

Data can be scrambled using encryption so that only authorised parties can decipher it. Technically speaking, it is the process of changing plaintext that can be read by humans into ciphertext, which is incomprehensible text. In plainer terms, encryption changes readable data to make it seem random. A cryptographic key, or collection of numbers that the sender and the recipient of an encrypted message both agree upon, is needed for encryption.

Despite the fact that encrypted data appears random, encryption works in a logical, predictable manner, making it possible for someone who gets encrypted data and has the proper key to decrypt it and restore it to plaintext. A third party will be extremely unlikely to be able to decrypt or break the ciphertext via brute force, or by guessing the key, when using truly secure encryption, which employs keys that are sufficiently complicated.

Drawbacks:

The key management required to use symmetric cyphers securely is a serious drawback. A different key should preferably be shared by each unique pair of communication parties, and possibly for each ciphertext transferred as well. In order to keep them all consistent and secret, an increasingly large number of keys are needed, which quickly necessitates complex key management schemes.

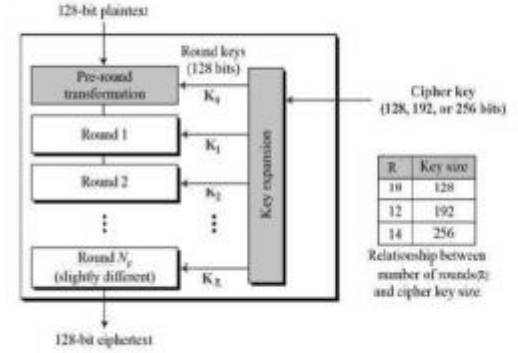
# CHAPTER 3

# PROPOSED MODEL

## 3.1 ARCHITECTURE

Its foundation is a "substitution-permutation network." It consists of a number of interconnected operations, some of which substitute certain outputs for inputs (substitutions), while others require shifting bits about (permutations). It's interesting to note that AES uses bytes rather than bits for all of its calculations. As a result, AES considers a plaintext block's 128 bits to be 16 bytes. For processing as a matri, these 16 bytes are set up in four columns and four rows. A different 128-bit round key, derived from the initial AES key, is used for each round.

The schematic of AES structure is given in the following illustration −




| R | Key size |
|---|---|
| 10 | 128 |
| 12 | 192 |
| 14 | 256 |

Relationship between number of rounds(R) and cipher key size

## 3.2 EXPLANATION OF THE PROPOSED MODEL

Encryption Process:

The encryption phase of AES can be broken into three phases:

the initial round, the main rounds, and the final round.

1. Initial Round

    - AddRoundKey

2. Main Rounds

    - SubBytes
    - ShiftRows
    - MixColumns
    - AddRoundKey

3. Final Round

    - SubBytes
    - ShiftRows
    - AddRoundKey

Decryption Process:

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order −

1. Inverse Final Round

- AddRoundKey
- ShiftRows
- SubBytes

2. Inverse Main Round

- AddRoundKey
- MixColumns -This step is similar to the MixColumns step

  in encryption, but differs in the matrix used to carry out the operation.
- ShiftRows
- SubBytes -Inverse S-box is used as a lookup table and using which the bytes are substituted during decryption.

3. Inverse Initial Round

- AddRoundKey

# CHAPTER 4

# RESULTS

The fundamentals of information security and cryptography have been thoroughly researched. I researched and studied many online resources that were available to me to learn about cryptography. We investigated encryption, including the need for data encryption and several encryption techniques. Symmetric key algorithm characteristics and principles were researched using a variety of resources. Techniques for encrypting and decrypting images using the Advanced Encryption Standard (AES) algorithm are suggested. 256-bit cypher keys are used to achieve high security since they are challenging to crack. Because of this, secure image communication may be feasible.

# CHAPTER 5

# CONCLUSION

Because image steganography is performed using AES, this technology offers protection from intrusion assaults and makes encryption and decryption more secure and quick. Therefore, this system offers security for the transmission and storage of digital photos. The cryptographic method put forth in this work will thereafter be evaluated on various input image types with varying image size and AES encryption algorithm keys.

# REFERENCES


- http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7406040&queryText=image%20aes&newsearch=true

- http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5734951&queryText=image%20aes&newsearch=true