JAYPEE INSTITUTE OF INFORMATION TECHNOLOGY

CNS Project Synopsis

Topic:	Image Encryption & Decryption using AES
Group No. :	14
Batch :	B11
Faculty Name:	Ms. Kavita Pandey
Course Code:	18B11CS212
Group Members:	Utsav Dhankhar (19104014) Rajat Kumar Singh (19104016) Abhishek Pratap Singh (19104019) Suyash Nigam (19104020)

Declaration

I/We hereby declare that this submission is my/our own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where due acknowledgment has been made in the text. I/We accept the use of the material presented in this report for Education/Research/Teaching purpose by the faculty.

Signature	Signature	Signature	Signature
Utsav	Rajat Singh	Abhishek	Suyash
Utsav Dhankhar 29/10/2021 Delhi	Rajat Kumar Singh 29/10/2021 Raebareli	Abhishek Pratap SIngh 29/10/2021 Agra	Suyash Nigam 29/10/2021 Noida

Abstract

Due to increasing use of image in various field, it is very important to protect the confidential image data from unauthorized access.

An Image Encryption and Decryption Using AES (Advance Encryption Standard) Algorithm is proposed in this project.

Introduction

Today almost all digital services like internet communication, medical and military imaging systems, multimedia system requires reliable security in storage and transmission of digital images. Due to faster growth in multimedia technology, internet and cell phones, there is a need for security in digital images. Therefore there is a need for image encryption techniques in order to hide images from such attacks. In this system we use AES (Advanced Encryption Technique) in order to hide image. Such Encryption technique helps to avoid intrusion attacks.

Terminologies:

Encryption:

Encryption is the method by which information is converted into secret code that hides the information's true meaning

Decryption:

Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form.

Key:

In cryptography, a key is a variable value that is applied using an algorithm to a string or block of unencrypted text to produce encrypted text, or to decrypt encrypted text. The length of the key is a factor in considering how difficult it will be to decrypt the text in a given message.

Advanced Encryption Standard (AES):

The Advanced Encryption Standard, or AES, is an encryption algorithm created by the National Institute of Science and Technology (NIST) in 2001. The cipher utilized in AES is a block cipher from the Rjindael cipher family. When AES was created, three different Rjindael block ciphers were selected for use, to make AES even more secure. All three ciphers used were 128 bits, but the keys they each used were of different sizes: 128, 192, and 256 bits. This is considered a symmetric block cipher, as only one key is used in the encryption process.

Advantages of AES

- AES is more secure (it is less susceptible to cryptanalysis than 3DES).

- AES supports larger key sizes than 3DES's 112 or 168 bits.
- AES is faster in both hardware and software.

What we will build?

We have planned to develop a program that encrypts and decrypts the image files accurately. This will help in minimising the problem of data theft and leaks of other sensitive information. The file that we obtained after encryption is very safe and no one can steal data from this file. So, this file can be sent on a network without worrying. At the receiver side, the receiver has code for decrypting the image so that he can get the original image.

Research Papers:

- B. Subramanyan, V. M. Chhabria and T. G. S. Babu, "Image Encryption Based on AES Key Expansion," *2011 Second International Conference on Emerging Applications of Information Technology*, 2011, pp. 217-220, doi: 10.1109/EAIT.2011.60. URL:https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5734951&isnumber=5734894
- Q. Zhang and Q. Ding, "Digital Image Encryption Based on Advanced Encryption Standard (AES)," *2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC)*, 2015, pp. 1218-1221, doi: 10.1109/IMCCC.2015.261. URL:https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7406040&isnumber=7405778
- D. M. Alsaffar *et al*., "Image Encryption Based on AES and RSA Algorithms," *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS)*, 2020, pp. 1-5, doi: 10.1109/ICCAIS48893.2020.9096809. URL:https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9096809&isnumber=9096666