www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
Vol. 02, Issue 04, April-2022, pp : 20-24

e-ISSN : 2583-1062
Impact Factor : 2.205

IMAGE ENCRYPTION USING AES ALGORITHM

Shrinidhi Anant Patil[*1], Swarali Naik[*2], Ashana Maurya[*3], Sangeetha Selvan[*4]

[*1,2,3]Bachalor Of Engineering , Information Technology, Mahatama Education society Pillai college of Engineering ,Panvel, Maharastra, India.

[*4]Professor, Information Technology, Mahatama Education society Pillai college of Engineering , Panvel, Maharastra, India.

ABSTRACT

Every communication via the internet relies heavily on data security. Data interchange or transmission from the sender to the receiver should be done in an authenticated manner. We use the AES method to encrypt and decrypt picture data. In this work, an image or files are given as input to the AES encryption technique, which returns a decrypted output. Using secret keys, the same AES method is utilised to encrypt the decrypted data.

Keywords: AES , Security , Encrypt .

1. INTRODUCTION

The use of the internet has increased in everyday life for even the tiniest data connection transfer. DES and AES are two examples of encryption techniques that are used to make data transfer safer and more secure.

The data is encrypted at the sender's end, and the data is received in encrypted form by the receiver, who then encrypts it with the use of a secret key. Which is shared by both the sender and the receiver. Unauthorized users cannot access the encrypted data because it is in an unreadable format.

2. METHODOLOGY

The system architecture is given in Figure Each block is described in this section

Sign In : Users have to create an account , with email and password. If a user has an account she or he has to sign in with required credentials .

Figure 2.1 Proposed System Architecture

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
Vol. 02, Issue 04, April-2022, pp : 20-24

e-ISSN : 2583-1062
Impact Factor : 2.205

Image Encryption and Decryption :

Encryption

Here user can encrypt different files , either single or multiples , using anyone key size and mode ; after that user must create a secret key . And end the encryption process .

Decryption :

User have to choose the mode and key size and have to enter the secret key and then upload the encrypted file , after that user will receive the decrypted file .

5.2 Algorithm :

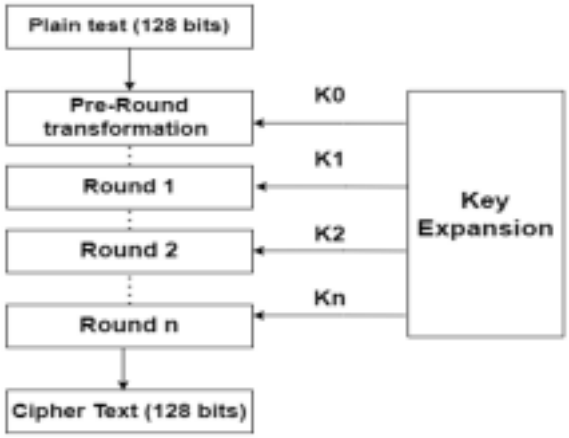

Figure 5.2.1

The Advanced Encryption Standard (AES) was created by the US National Institute of Standards and Technology (NIST) in 2001 as a specification for the encryption of electronic data. AES is the most frequently used algorithm. Because it is considerably stronger than DES as well as triple DES.

The AES cypher is a block cypher. The key can be 128 or 192 or 256 bits in length. Data is encrypted in 128-bit blocks. It accepts 128 bits as input and outputs ,128 bits of encrypted ciphertext. AES is based on the substitution-permutation network principle, which entails replacing and shuffling the input data through a series of connected processes.

Working of the cipher :

AES uses bytes rather than bits to conduct operations. The cipher handles 128 bits (or 16 bytes) of incoming data at a time since the block size is 128 bits. The number of rounds depends on the key length as follows : 128 bit key – 10 rounds 192 bit key – 12 rounds 256 bit key – 14 rounds.

Creation of Round keys :

To calculate all the round keys from the key, a Key Schedule algorithm is employed. As a result, the initial key is used to generate a number of other round keys, each of which will be used in the encryption round that follows.

Encryption : AES considers every block as a 16 byte (4 byte x 4 byte = 128) grid in a column major arrangement.

[b0 | b4 | b8 | b12 |

| b1 | b5 | b9 | b13 |

| b2 | b6 |b10| b14|

| b3 | b7 | b11| b15|]

Each round is of 4 steps :

SubBytes
ShiftRows

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
Vol. 02, Issue 04, April-2022, pp : 20-24

e-ISSN : 2583-1062
Impact Factor : 2.205

MixColumns
Add Round Key

The last round doesn't have the MixColumns round. The SubBytes does the substitution and ShiftRows and MixColumns performs the permutation in the algorithm.

SubBytes : In this step implementation of substitution happens . In this step every byte is substituted by another byte. It is performed using a lookup table which is also called the S-box. The substitution is done in such a way that a byte is never substituted by itself and is also not substituted by another byte that is complimented by the current byte. The result is the same 16 byte matrix (4 x 4). Permutation is implemented in the next two steps.

ShiftRows : Each row is shifted a particular number of times. The first row is not shifted. The second row is shifted once to the left. To the left the third row is shifted twice and the fourth row is shifted thrice to the left.

[b0 | b1 | b2 | b3] [b0 | b1 | b2 | b3]
| b4 | b5 | b6 | b7 | -> | b5 | b6 | b7 | b4 |
| b8 | b9 | b10 | b11 | | b10 | b11 | b8 | b9 |
[b12 | b13 | b14 | b15] [b15 | b12 | b13 | b14]

MixColumns : This step is if ‘ matrix multiplication’. Each column is multiplied with a specific matrix and therefore the position of each byte in the column is changed as result. In the last round ; this step is skipped.

[c0] = [2 3 1 1] [b0]

[c1] = | 1 2 3 1 | | b1 |

[c2] = | 1 1 2 3 | | b2 |

[c3] = [3 1 1 2] [b3]

Add Round Keys : Now resultant output of the previous stage is XOR-ed with a corresponding round key. Here 16 bytes isn’t considered as grid but just as dada of 128 bits .

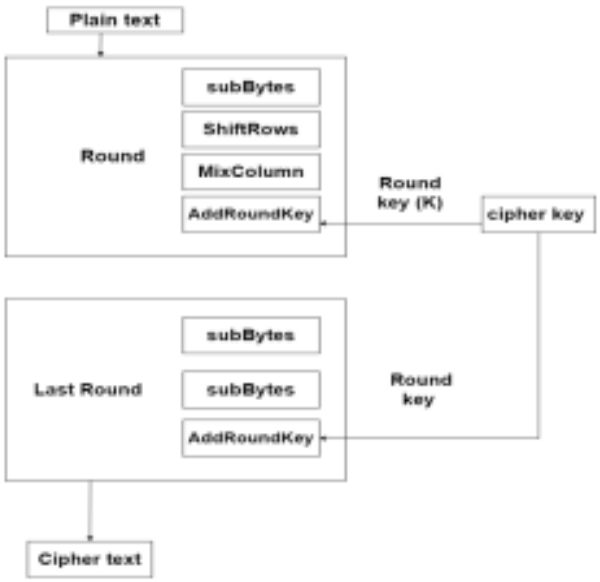

Figure 5.2.2

This process is repeated until all the data to be encrypted has undergone this process. When all these rounds have been completed, 128 bits of encrypted data is returned.

Decryption : It is easy to undo the stages in the rounds since each stage has an opposite and when the opposite is applied, it reverses the changes. This is done for each block of 128 blocks through 10,12, or 14 rounds, depending on the key size.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
Vol. 02, Issue 04, April-2022, pp : 20-24

e-ISSN : 2583-1062
Impact Factor : 2.205

The stages of each round in decryption is as follows :

- Add round key
- Inverse MixColumns
- ShiftRows
- Inverse SubByte

The 'decryption' process is the 'encryption' process which is done in reverse.

Inverse MixColumns : This step is alike to the MixColumns step in encryption, but differs in the matrix used to carry out the operation.

$$\begin{bmatrix} b0 \\ b1 \\ b2 \\ b3 \end{bmatrix} = \begin{bmatrix} 14 & 11 & 13 & 9 \\ 9 & 14 & 11 & 13 \\ 13 & 9 & 14 & 11 \\ 11 & 13 & 9 & 14 \end{bmatrix} \begin{bmatrix} c0 \\ c1 \\ c2 \\ c3 \end{bmatrix}$$

Inverse SubBytes : During decryption, the inverse S-box is used as a lookup table and to substitute the bytes.

3. RESULTS AND DISCUSSION

In this Section results and discussion of the study is written. They may also be broken into subsets with short, revealing captions. This section should be typed in character size 10pt Times New Roman.

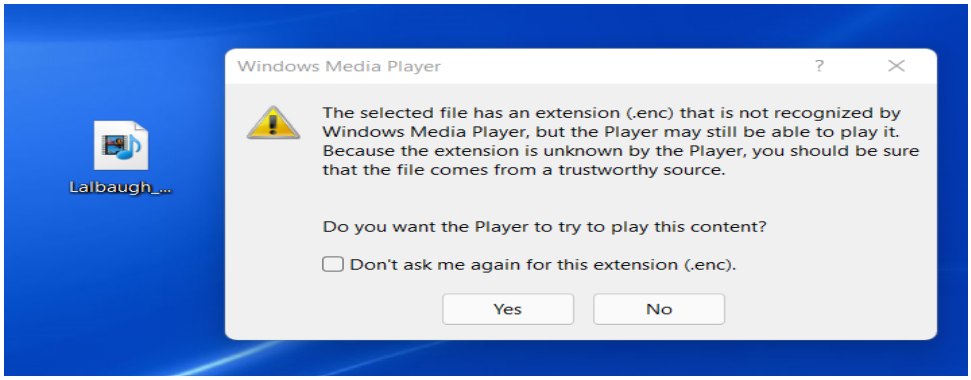

Figure 3.1After the decryption

Figure 3.2 After the encryption

4. CONCLUSION

Image encryption and decryption are the two amin processes , takes place user can choose any one of the operation to perform on images . User can set their own combination keys of passwords for decryption and have to use the same key for encryption ..

ACKNOWLEDGEMENTS

We would like to extend our deepest gratitude to our Project guide **Prof. Sangeetha Selvan** for her exemplary guidance, monitoring, and constant encouragement throughout this project which helped us improve our work.

We would also like to extend our gratitude to our Head of IT Department **Dr. Satishkumar Varma** for providing us with an opportunity and platform to carry out this project.

We are also extremely grateful to our Principal **Dr. Sandeep Joshi** who provided us with this golden opportunity as well as all the facilities needed to carry out this project .

5. REFERENCES

[1] H.Abood, "An Komal D Patel, Sonal Belani "Image Encryption using different Techniques" International Journal of Emerging Technology and Advanced Engineering Volume 1, Issue Zeghid, M., Machhout, M., Khriji, L., Baganne, A., & Tourki, R. (2007). A modified AES based algorithm for image encryption. International Journal of Computer Science and Engineering, 1,November 2011.

[2] Hoang, T. (2012, February). An efficient FPGA implementation of the Advanced Encryption Standard algorithm. In Computing and Communication Technologies, Research, Innovation, and Vision for the Future (RIVF), 2012 IEEE RIVF International Conference on (pp. 1- 4). IEEE.

[3] Patro K, Acharya B (2018) Secure multi–level permutation operation based multiple color image encryption. J Inf Secur Appl 40:111–133 .

[4] Hailan Pan, Lei Yongmei, Jian Chen (2018) Research on digital image encryption algorithm based on double logistic chaotic map. EURASIP J Image Video Process 2018(1):142

[5] William Stallings, "Advanced Encryption Standard," in Cryptography and Network Security, 4th Ed., India:PEARSON,pp. 134–165.

[6] AtulKahate, "Computer-based symmetric key cryptographic algorithm", in Cryptography and Network Security, 3rd Ed. New Delhi:McGraw-Hill, pp. 130-141 .

[7] Efficient Image Cryptography using Hash- LSB Steganography withRC4 and Pixel Shuffling Encryption Algorithms". Annual Conference on New Trends in Information Communications Technology Applications- (NTICT'2017) 7 -9 March 2017 IEEE.