e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:08/August-2022 Impact Factor- 6.752 www.irjmets.com

A NOVEL IMAGE ENCRYPTION USING AES ALGORITHM

Imaad Zaffar Khan[*1], Amaan Aijaz[*2]

[*1,2]Department Of Computer Science & Engineering, SRM Institute Of Science And Technology, Kattankulathur, India.

ABSTRACT

Encryption is a defined as a procedure used to secure and safeguard the data. The encrypted information is kept private and classified. To interpret the encrypted information, we require a process called decryption. In this day and age maintaining confidentiality is a crucial obstacle. For the sake of securing our information, we use an algorithm known as Advance encryption standard (AES). This algorithm secures privileged information from uncertified users. The AES algorithm can encrypt plain text data as well as images. This paper elaborates how various operations are performed to encrypt the given image. Finally, the encrypted output obtained can be given as input to AES decryption algorithm having the same key as encryption and after certain operations our original image is retrieved. The working of the AES algorithm is simulated with the help of a GUI application.

Keywords: AES, Image Encryption, Image Decryption, Security, Application.

I. INTRODUCTION

Encryption is a strategy used to secure and safeguard our information. Encrypted information is always kept confidential where the particulars and sensitive parts of the data are revised, making it quite unalike the original information. Cryptography's use and application is deep rooted mainly in defence of a country as no one wants the enemy snooping around you

Cryptography consists of four main pillars being Authentication, Integrity, Non-repudiation and Privacy. The articles mainly focus on cryptographic algorithms like AES and DES. DES performs comparatively slower than AES. It consists of a 64-bit block size which honestly is very less compared to newer algorithms. With regard to this, AES (Advanced Encryption Standard) is determined to replace DES (Data Encryption Standard).

AES can have three types of key lengths: "128 || 192 || 256" bits. For our project we have considered 256 bits as it focuses both on performance and security. For different key-lengths, we have varying number of operations. Every round of the operations comprises of one single-byte based substitution, a row-wise permutation, a column-wise mixing, and the incorporation of the round key. The order in which these four steps are implemented are quite different for encryption and decryption.

The implementation of image encryption is primarily found in Robotics, military communication, forensics, intelligent system etc

II. LITERATURE SURVEY

A. Encryption using DES

The DES was once a top-tier symmetric-key algorithm used for encryption. Nowadays it is an outdated encryption method. It has a key-length of 56-Bits. 16 rounds of encryption are performed on each 64 bits block of data. DES nowadays can easily be cracked using brute-force search.

The key-size decides upon the encryption strength of the algorithm, and 56 bit key lengths have become too small relative to the processing power of modern computers.

B. Encryption using AES

Depending upon the key-length there are three subcategories of AES: "AES-128" || "AES-192" || "AES-256". For our project we chose AES-256 as it is the most secure amongst the three. Cryptographic libraries like pycrypto, crypto. Cipher and AES were at the core of the technological front.

The number of rounds vary in different types of AES algorithms. Like in our case the AES-192 has exactly 12 rounds of different operations. For AES-128 bit there are 10 rounds and for AES-256 there are 14 rounds.

Every single round of the operation encompasses certain actions like Byte-substitution, shifting of rows, mixing of certain columns and then finally incorporating the round-key. The sequence of these operations differs in encryption and decryption.

IRJMETS
e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:08/August-2022 Impact Factor- 6.752 www.irjmets.com

$$\begin{bmatrix} byte_0 & byte_4 & byte_8 & byte_{12} \\ byte_1 & byte_5 & byte_9 & byte_{13} \\ byte_2 & byte_6 & byte_{10} & byte_{14} \\ byte_3 & byte_7 & byte_{11} & byte_{15} \end{bmatrix}$$

To better understand and visualize the working, think of the 128-bits structure as a (4×4) array of bytes as organised above.

The main column is initially pre-occupied by the 1st four-bytes of the 128-bits structure which guarantees the 2nd column is filled by the next four-bytes, and so on.

III. PROPOSED WORK

In the modern world, data security is a crucial obstacle faced by millions of people. The usage of contemporary devices like PC's, mobile and alternative device for communication furthermore as for information storage and transmission has increased. As a result, there's an increase in the number of users, additionally, there's an increase in number of unauthorized users that are attempting to access information by unfair means. To unravel this drawback information transmitted within the encrypted format. This encrypted information is indecipherable to unauthorized users.

According to The Software Alliance in 2015 alone, cybercriminals stole 423 million identities.

We will be taking a picture of (.jpg) format as input for our model.

Our project code for AES is written in python comprising of different cryptographic libraries and modules.

The ultimate objective of this project is to develop and design an application that will enable the user to encrypt/decrypt image of the user's choice.

IV. AES METHODOLOGY

There are 3 types of AES algorithms (AES-128, AES192 and AES-256). This segregation is done on the basis of key used in the process of encryption/ decryption. Security level is determined by the no. bits used.

AES algorithm uses 4 different Byte-oriented conversions:

- Substitute Byte
- Shift row
- Mix Columns
- Add Round Key

A. Encryption

i. Substitute Byte

- First step of encryption known as Sub-Bytes which involves substitution in byte-by-byte format in the forward process.
- To locate a replacement byte in the state array, a (16x16) look-up table is used.
- The concept of Galois field is used here. The multiplicative inverses are used to fill in the entries of the table. Also scrambling of bits is carried-out to break-up the correlations made at the bit-level.
- Procedure involving bit scrambling can be expressed with the relation:

$$x_{out} = A \cdot x' + c$$

ii. Shift Row

- Second step of encryption known as shift rows which shifts certain rows in the array amidst the forward process.
- The Shift-Rows transformation involves (a) by not transposing the very "1st" row in the array (b) by transposing the "2nd" row in clock-wise direction by a single-byte to the left. (c) by transposing the "3rd" row (2 bytes to the left) (d) and by transposing the last row by 3 bytes to the left.

- The main main objective of this transposing and shifting is to mingle up all byte sequence comprising the 128-bits structure.

iii. Mix Columns

- Third step of encryption known as Mix Columns involves scrambling of the bytes in each column individually in the course of the forward process.
- Each and every byte in a column is changed by twice that byte, plus thrice the following byte, plus the impending byte, and lastly expanded with the next byte.
- The shift-rows step beside the mix-column step creates each bit of the ciphertext to rely on each bit of the plain text after processing of ten rounds.

iv. Add Round-Key

- Fourth and last step of encryption is known as Mix Columns. The bytes in each columns are scrambled amidst the ongoing process.
- The 128 bits key for every round is obtained from the 128bits encryption key using AES key-expansion. Key Expansion algorithm's logic is considered to make sure that even if a single bit of the key is altered, it ought to have an effect on the keys used in the rounds.

B. Decryption

i. Inverse Shift Row

- Amidst the decryption process, the corresponding operations scrambles the rows in precisely the opposite way as performed earlier in encryption.
- Certain steps involved: (a) "1^{st}" row is left unmodified, (b) "2^{nd}" row is transposed by a single byte to the right, (c) "3^{rd}" row {2 bytes to the right}, and the last row by 3 bytes. These transpositions are ensured to be circular in nature.

ii. Inverse Substitute Byte

- As the name suggests it is the opposite of the byte substitution transformation. This stage particularly consists of procedures where the converse of the Sbox is enforced on each byte.
- Also known as the reverse process of Substitute Byte. We acquire inverse substitution by enforcing the inverse of the affine transformation. Further-more this procedure is simultaneously accompanied with the multiplicative inverse in Galois Field.

iii. Add Round Key

- Similar to the procedure of encryption, the roundkeys are included in each and every round. The number of round-keys added depends directly upon the type of AES used.

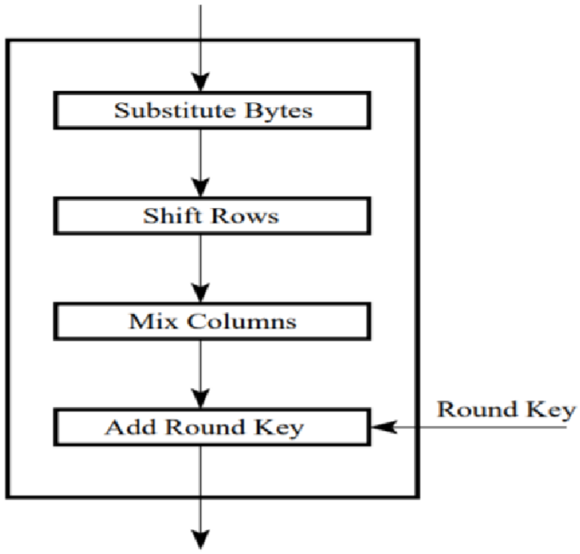
iv. Inverse Mix Columns

- Again, the exact opposite of the Mix Columns transformation done earlier in the encryption procedure. During the process on the state, managing and visualizing every column as a 4-term polynomial is necessary. Inverse Mix Columns works on the state column-by-column.
- Finally these columns are analyzed and evaluated as polynomials over the Galois Field (2^8) and are multiplied modulo (x^4+1) with a fixed polynomial (x) , given by:

$$a^{-1}(x) = \{0b\}x^3 + \{0d\}x^2 + \{09\}x + \{0e\}$$

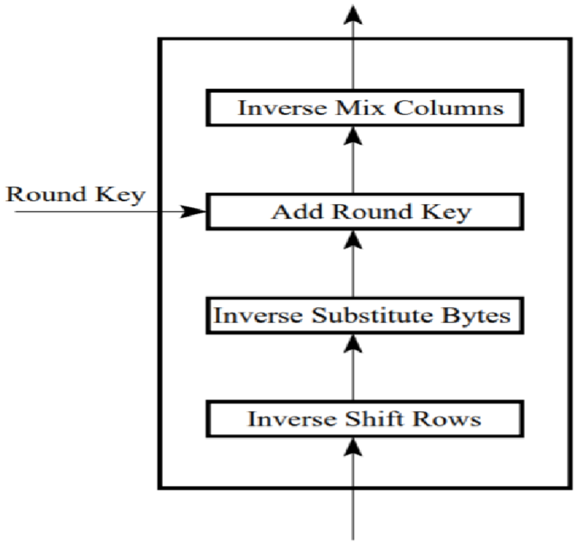
e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:08/August-2022 Impact Factor- 6.752 www.irjmets.com

V. IMPLEMENTATION



Encryption Round

Figure 1: Block Diagram for steps involved in Encryption



Decryption Round

Figure 2: Block Diagram for steps involved in Decryption

There is a massive difference in the flow of the operations. One cannot deem decryption as the exact opposite of encryption. The encryption involves substitution of bytes, row-shifting, column-mixing while as decryption also has the same operations but in inverse manner and the order is also different.

The implementation of AES encryption and decryption algorithm is done using python where modules such as pycrypto, Numpy, hashlib, cipher.AES etc were used and Tkinter is used for GUI implementations. The inputs were images of varying sizes and a detailed analysis regarding the performance is done. Figure 1 and 2 shows the flow of algorithm.

For analysing the performance of this model, we took multiple images of different sizes and dimensions.

VI. EXPERIMENTAL RESULT

The input image given to the algorithm is of jpeg format is encrypted and converted into unreadable form (jpeg.crypt format) which shows how confidentiality and privacy of an image can be maintained having a unique key. This way it is also represented how sensitive data can be transferred keeping it away from intruders and hackers making it very difficult for them to interpret the data.

For depicting the graph of performance vs size, we took 5 images of following specifications:

- Image 1: Size- 50KB and dimension - (300x300)
- Image 2: Size- 500KB and dimension - (1792x1792)
- Image 3: Size- 5MB and dimension - (5072x6761)
- Image 4: Size- 10MB and dimension - (7724x5148)
- Image 5: Size- 30MB and dimension - (13583x5417)

We encrypt these images sequentially and note the time taken for each process and then we plot a graph of time/size and after plotting the graph we observed that with increase in size of the image, the time required for the encryption increased.

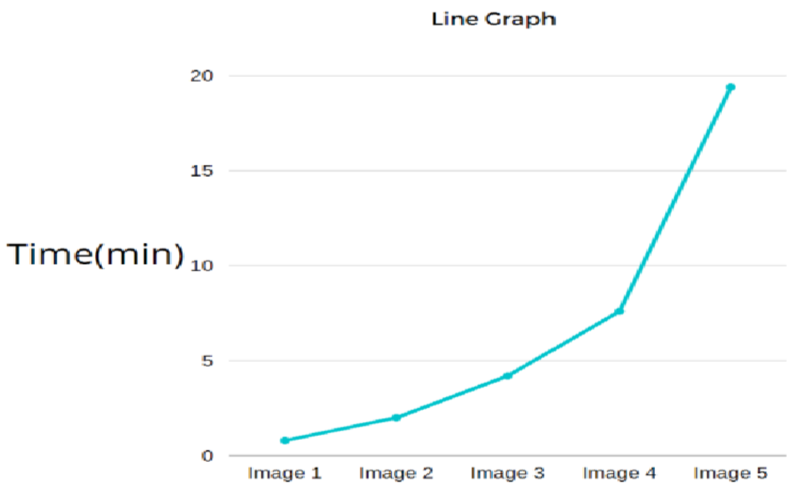


Figure 3: Bar Graph for time vs size of an image encryption

It has also been presented that if an image is of large size, it consumes more time in encrypting the image using normal PCs. (This analysis was done in PC having 8GB of RAM and Intel i7 Processor).

We obtained the following results:

Size of Image	Time(min)
50 KB	0.1
500 KB	2
5 MB	4.2
10 MB	7.6
30 MB	19.4

Hence it can be concluded that encryption/decryption requires more time for an image if it is of considerable large size.

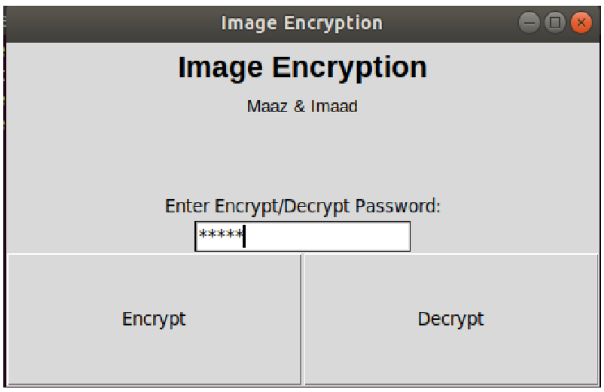


Figure 4: Application GUI designed for implementation of AES Encryption/Decryption using key

These outputs may vary according to different computing machine specifications. These values are obviously less than what DES can produce since DES is a little slower compared to AES.

Hence it is clearly evident that AES is relatively much faster than DES and why AES is intended to replace DES.

We created a simple application using tkinter module in python and the UI is quite user-friendly and easy to use.

VII. CONCLUSION

In this paper we learn how to encrypt and decrypt an image using AES algorithm where key is unique in both the process. Furthermore, we have taken different samples of images with varying sizes and analysed the performance of this particular model.

The input image given to the algorithm is of jpeg format is encrypted and converted into unreadable form which shows how confidentiality and privacy of an image can be maintained. This way it is also represented how sensitive data can be transferred keeping it away from intruders and hackers making it very difficult for them to interpret the data.

This project also shows various process involved in AES algorithm (Encryption and Decryption) and also why AES is replacing DES.

It has also been presented that if an image is of large size, it consumes more time in encrypting the image using normal PCs. (This analysis was done in PC having 8GB of RAM and Intel i7 Processor).

Hence it can be concluded encryption and decryption also requires more time for an image if it is of large size.

ACKNOWLEDGEMENT

We are grateful to Dr TK Sivakumar Associate Professor, School of Computing, SRM Institute of Science and Technology Chennai, India for his constant support and guidance.

VIII. REFERENCES

[1] William Stalings, "Advance Encryption Standard," in Cryptography and Network Security, 4th Ed., India:PEARSON.

[2] Atul Kahate, "Computer-based symmetric key cryptographic algorithm", in Cryptography and Network Security:McGraw-Hill.

[3] https://faun.pub/what-is-an-advanced-encryption-standard-aes-incryptography-1b47b1ecfadb

[4] An enhanced text to image encryption technique using substitution and AES by Sourab Singh, Anurag Jain (IJETT).

[5] New comparative study between DES,3DES, AES by Hamdan Alanazi, B.B Zaidan.

[6] International Journal of Engineering and advanced technology (IJEAT) volume-I, 2014.