www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int. Peer-Reviewed Journal)
Vol. 04, Issue 08, August 2024, pp: 84-88

e-ISSN : 2583-1062
Impact Factor : 5.725

ENCRYPTION AND DECRYPTION IMAGES USING AES ALGORITHM

Wael Saad ahmed [1], Saad Ahmed Mohammed [2], Rasha Rokan ismall [3]

[1] Tikrit medicine college, Tikrit university , Tikrit, Saladin, Iraq

[2]human anatomy department , Tikrit medicine college , Tikrit university, Tikrit , Saladin, Iraq

[3] Diyala university , Diyala, Diyala, Iraq.

DOI: https://www.doi.org/10.58257/IJPREMS35641

ABSTRACT

In today's world, data security is a major issue to be addressed. To secure, store and transmit data during communication use Advanced Encryption Standards (AES). AES is a symmetric block cipher that aims to replace DES for commercial applications. It uses a block size of 128 bits and a key size of 128, 192 or 256 bits. AES algorithm is used to secure data from unauthorized users. AES algorithm is available for text data as well as image data. In this paper, an image is given as input to AES encryption algorithm which gives encrypted output. This encrypted output is given as input to AES decryption algorithm and the original image is restored as output .

Keywords: Encryption ,Decryption, AES, Image

1. INTRODUCTION

Now days, the use of devices such as computers, mobile phones and many other devices for communication, storage and transmission of data is increasing. As a result, there is an increase in the number of users and the number of unauthorized users who try to access the data through illegal means. This causes a problem for data security. To solve this problem, data is stored or transmitted in an encrypted format and the encrypted data is unreadable by the unauthorized user. Encryption secures data during its transmission and storage. Every encryption and decryption process has two aspects: the algorithm and the use of the key for encryption and decryption. The key used for encryption and decryption is what makes the encryption process secure. There are two types of encryption mechanisms: Symmetric key encryption where the same key is used for encryption and decryption. In the case of asymmetric key encryption, two different keys are used for encryption and decryption. The symmetric key algorithm is faster, easier to implement and requires less processing power compared to the asymmetric key algorithm. The Advanced Encryption Standard (AES) defines an encryption algorithm approved by the Federal Information Processing Standards (FIPS) publication that can be used to protect electronic data. AES has high computational efficiency, 128-bit block size, and strong cryptanalysis resistance against differential, linear, interpolation, and square attacks [1] [2] [3] . The application of image processing is mainly found in military communications, forensics, robotics, intelligent systems, etc. In this paper, we implement AES algorithm on images with the help of MATLAB software

2. RELATED WORK

There are many works that related with our work, which presents the security of data as follow :-

A wide variety of cryptographic algorithms for images have been proposed in the literature.

Kuo [4] proposed an image encryption method known as image distortion which obtains the encrypted image by adding the phase spectra of the plain image with those of the key image. This method is safe but no image compression is considered.

N.G. Bourbakis [5] have presented a new methodology which performs both lossless compression and encryption of binary and gray-scale images. The compression and encryption schemes are based on SCAN patterns generated by the SCAN methodology. The SCAN is a formal language-based two-dimensional spatial- accessing methodology which can efficiently specify and generate a wide range of scanning paths or space filling curves.

Chin –Chen Chang [6] have used the popular image compression technique, vector quantization to design an efficient cryptosystem. The images are first decomposed into vectors and the sequentially encoded vector by vector.

Fridrich [7] demonstrated the construction of a symmetric block encryption technique based on two dimensional standard chaotic map.

Scharinger [8] designed a Kolmogorov flow based image encryption technique in which the whole image is taken as a block and permuted through a key controlled chaotic system. A shift register pseudo random generator is also used to provide confusion in data.

3. ADVANCED ENCRYPTION STANDARD ALGORITHM (AES)

The Advanced Encryption Standard (AES) is the United State Government standard for symmetric encryption. AES is a block cipher that encrypts a 128-bit block (plaintext) to a 128-bit block (cipher text), or decrypts a 128-bit block (cipher

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int. Peer-Reviewed Journal)
Vol. 04, Issue 08, August 2024, pp: 84-88

e-ISSN : 2583-1062
Impact Factor : 5.725

text) to a 128-bit block (plaintext).AES uses a cipher key of length either 128or 192, or 256 bits. Hereafter encryption/decryption with a key of 128, 192, or 256 bits in cipher is denoted AES128, AES192, AES256.The notation AES128, AES192, AES256 process the data block in 10,12,14 iterations respectively of a pre-defined sequence of transformations, which are also called ―rounds‖ (AES rounds) for short. The rounds are identical except the last one, which slightly differs from the others (by skipping one of the transformations). The rounds operate on two 128-bit inputs: State and Round key. Each round from 1 to either 10or12or14 uses a different round keys. Eithe10or12or14 round keys are redeemed from the cipher key by the algorithm called ―Key Expansion‖ .AES algorithm is not dependent of processed data, and can be easily carried out without depending on any encryption or decryption phase AES is a symmetric encryption algorithm that operate in block of data (4x4 square matrix of bytes (128 bits)) called state with key length of 128, 192, or 256 bits. The encryption and decryption operation consist of N round, where the number of rounds depends of key length (10, 12, or 14). Figure (1) show the AES algorithm architecture.

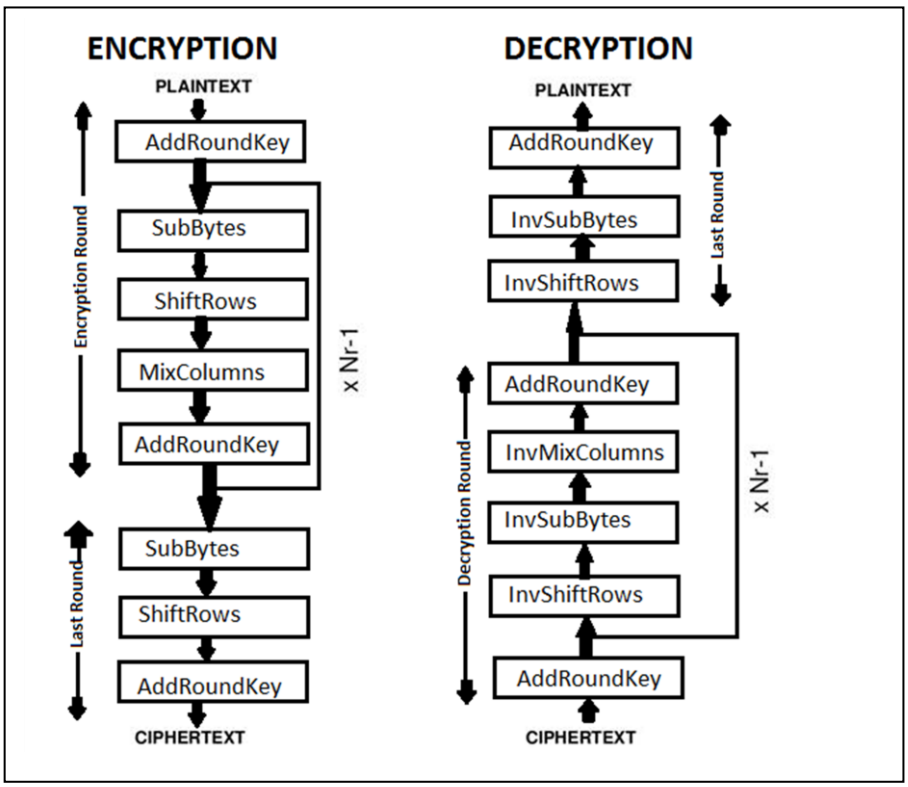

Figure (1): Encryption and Decryption Process in AES

As illustrated in figure (1) AES architecture contain the following processes:

1- Key Expansion: In this operation the key expansion algorithm will used to derive key to each round from the cipher key.

2- Initial Round: In this step the cipher key will combine with the state matrix using XOR operation.

3- Sub-Byte/ Inverse Sub-Byte: In substitution byte operation will be working the state which resulting from the initial round. Each byte in state matrix will replaced with S-box table. While in Inverse Sub-Byte operation the bytes in state will replaced with InvS-box table.

4- Shift Rows/ Inverse Shift Rows: Shift row operation will apply on state which resulting from sub-byte step, in this step the 1st row remain without shifting, the 2nd row shifted one byte to the left, the 3rd row shifted two bytes to the left, the 4th row shifted three bytes to the left. In inverse shift rows only the direction of rotation will be reflects.

5- Mix Columns/ Inverse Mix Columns: In this step the state that resulting from shift row step will multiply with special matrix. The inverse mixed column will done by multiply with another special matrix as follow:

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \quad \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix}$$

Mix Column Matrix Inverse Mix Column Matrix

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int. Peer-Reviewed Journal)
Vol. 04, Issue 08, August 2024, pp: 84-88

e-ISSN : 2583-1062
Impact Factor : 5.725

6- AddRound Key: In this step the round key will added to the matrix which resulting from Mix Cloumn using XOR operation.[9][10]

4. PROPOSED METHOD ARCHITECTURE

In this paper we want to implement a safe method to secure the images and files that we want to save them in cloud computing. The user can encrypted the images and files by using modified AES algorithm based on password and then uploaded them to cloud, also he can download any uploaded file previously. The following figure show the diagram of the proposed system.

A. Uploading Data

The following processes will explain upload data step-

1- The user login by enter the user name and password

2- The user choose image to be uploaded

3- The password of user saved to used it for generate encryption key.

4- Apply encryption AES algorithm.

5- Press upload key to upload image to server.

6- The user logout from system.

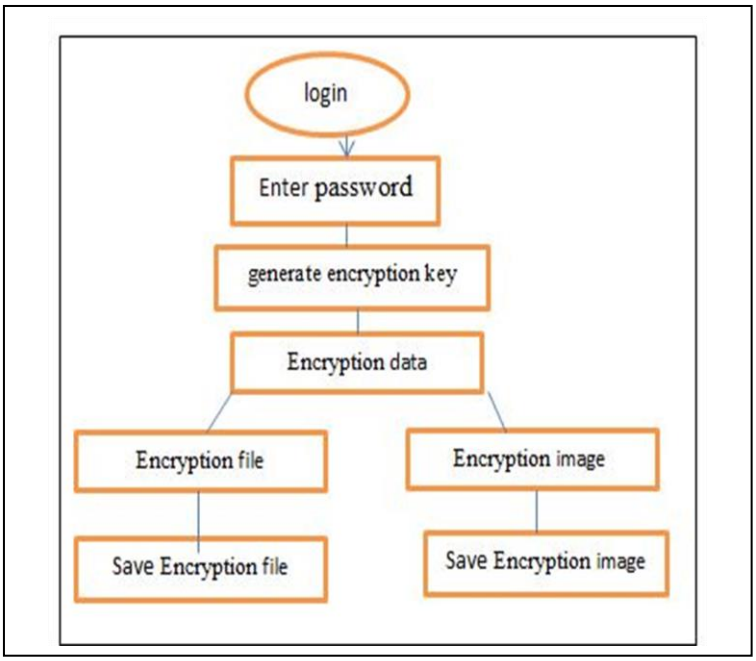

Figure (2): Uploaded Data Processes

B. Downloading Data

The following processes will explain downloading data step.

1- The user login by enter the user name and password

2- The user choose the data to download it.

3- The user enter the same password that used in encryption operation to generate the same encryption key because AES is symmetric key algorithm.

4- Apply decryption algorithm.

5- The user will get the same original data

6- The user logout from system.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int. Peer-Reviewed Journal)
Vol. 04, Issue 08, August 2024, pp: 84-88

e-ISSN : 2583-1062
Impact Factor : 5.725

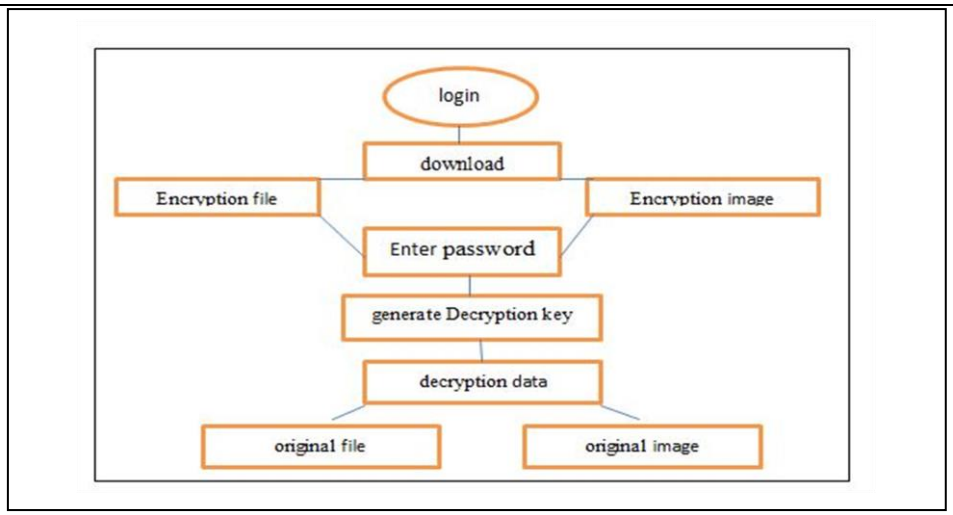

Figure (4): Download Data Processes

5. RESULT

The original input image given to the algorithm is of JPG And of 8.32 Kb size. The unreadable image is the encrypted image and by applying the decryption algorithm the original image is obtained in JPG format. In this paper, For Encryption

.

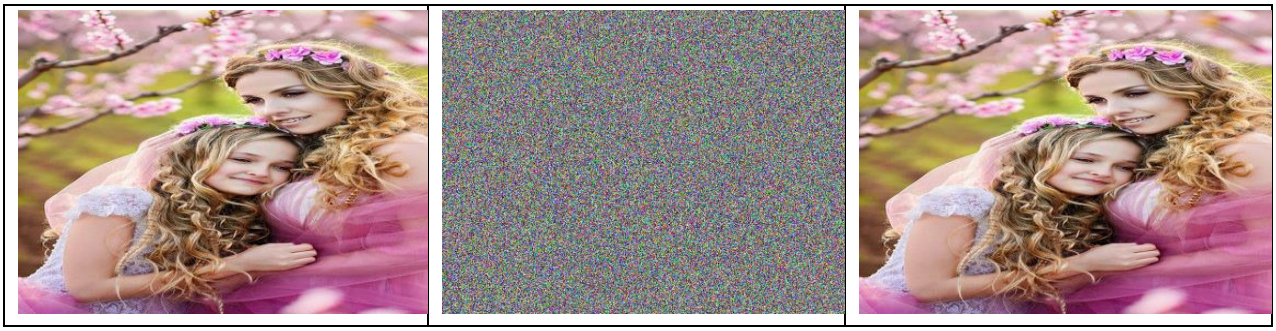

Figure (5) show a- Original image b- the encryption image c- decryption image in AES algorithm

6. HISTOGRAM ANALYSIS

The Histogram Analysis of the three bands (red, green, blue) for original image and encrypted image are shown in Figure (6).

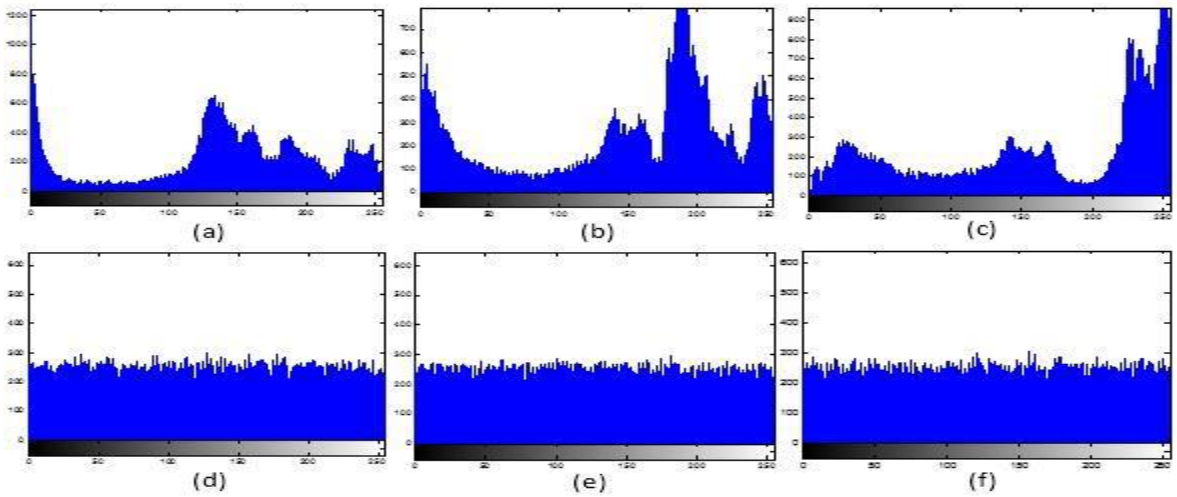

Figure (6): The Histogram Analysis: (a), (b) and (c) are The Histogram of (Red, Green and Blue) of the Original Image, (d),(e) and (f) are The Histogram of (Red, Green and Blue) Encrypted Image by using MAES algorithm

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int. Peer-Reviewed Journal)
Vol. 04, Issue 08, August 2024, pp: 84-88

e-ISSN : 2583-1062
Impact Factor : 5.725

7. TIME ANALYSIS

In Table 1, we have recorded the time taken by our algorithm to perform the encryption of images .From Figure 9 we can see that the relationship between size and time to encrypt is almost linear and as the file size increases there is no abrupt change in the time taken for encryption and it increases proportionally .

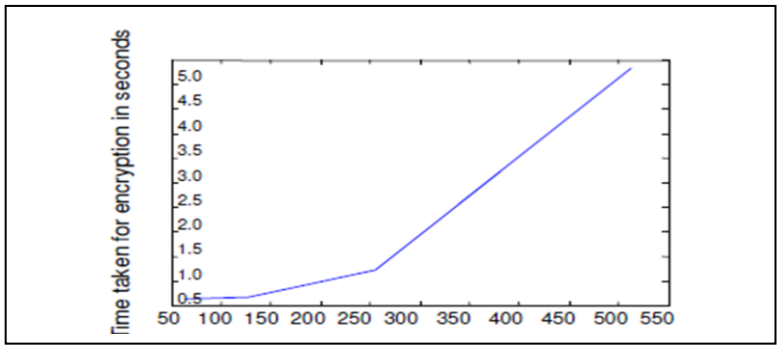

Figure 7. Plot of image size versus time taken forencryption

Table 4. Time analysis for various image sizes.

Size of image (Kb)	No. of pixels	Time taken (s)
2.01	64x64	.1400
4.76	128x128	.1710
12.8	256x256	.7170
612	512x512	4.8350

8. CONCLUSION

In this paper, Image Encryption and Decryption using AES algorithm is implemented to secure the image data from unauthorized access. Successful implementation of the symmetric key AES algorithm is one of the best encryption and decryption standards available in the market. Implementation of an AES algorithm is for Image Encryption and Decryption original reconstructed without any distortion. It has shown that the algorithms have extremely large security key space and can withstand most common attacks such as brute force attacks, cipher attacks, and plaintext attacks

9. REFERENCES

[1] [William Stallings, “Advance Encryption Standard,” in Cryptography and Network Security, 4th Ed., India:PEARSON,pp. 134–165.

[2] AtulKahate, “Computer-based symmetric key cryptographic algo-rithm”, in Cryptography and Network Security, 3th Ed. New Del-hi:McGraw-Hill, pp. 130-141.

[3] Manoj .B,Manjula N Harihar (2012, June). “Image Encryption and Decryption using AES”, International Journal of Engineering and Advance Technology (IJEAT) volume-1, issue-5, pp.290-294.

[4] C.J.Kuo, Novel image Encryption Technique and its application in progressive transmission. Journal of Electron imaging 24 1993 pp345-351.

[5] N.J.Bourbakis , C.Alexopoulos, Picture data encryption using SCAN patterns. Pattern Recognition 256 1992 pp567 -581.

[6] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, “A newencryption algorithm for image cryptosystems”, The Journal of stemsand Software 58 (2001), 83-91.

[7] Fridrich Jiri, Symmetric ciphers based on two dimensional chaotic maps, Int. J. Bifurcat Chaos 8 (1998) (6), pp. 1259– 1284.

[8] J. Scharinger, Fast encryption of image data using chaotic Kolmogrov flow, J. Electronic Eng 7 (1998) (2), pp. 318–325.

[9] VedkiranSaini, ParvinderBangar, Harjeet Singh Chauhan, (2014, April).”Study and Literature Survey of Advanced Encryption Algo-rithm for Wireless Application”, International Journal of Emerging Science and Engineering (IJESE) volume-2, issue-6, pp.33-37.

[10] Sourabh Singh, Anurag Jain, (2013, May). “An Enhanced Text to Image Encryption Technique using RGB Substitution and AES”, In-ternational Journal of Engineering Trends and Technology (IJETT) volume-4,issue-5,pp.2108-2112.