ISSN: 2455 - 9172

EIJO Journal of Engineering, Technology And Innovative Research (EIJO–JETIR)

Einstein International Journal Organization (EIJO)

Available Online at: www.eijo.in

Volume – 4, Issue – 2, March – April -2019 , Page No. : 19 - 25

Digital Image Encryption Using AES Algorithm

[1]Pradeep Jha, Assistant Professor, Department of CSE, Arya College of Engineering & Research Centre, Jaipur, Rajasthan, India

[2]Krishna Kumar Sharma, Assistant Professor, Department of CSE, Arya College of Engineering & Research Centre, Jaipur, Rajasthan, India

[3]Bhavesh Jain, Assistant Professor, Department of CSE, Arya College of Engineering & Research Centre, Jaipur, Rajasthan, India

[4]Vaishali Sharma, Assistant Professor, Department of CSE, Arya College of Engineering & Research Centre, Jaipur, Rajasthan, India

Abstract

The security of digital image transfer is important in image communications at present, due to the increasing use of images in industrial processes. It is necessary to protect confidential image data from unauthorized access. Image security has become a critical issue. Difficulties in ensuring the privacy of people are increasing. Several methods of data protection and personal privacy have been discussed and developed. Encryption is probably the most obvious. To protect valuable information from unwanted readers, image encryption is necessary. In this paper, present a digital image encryption technique which is enhancing the security of digital image using the Advanced Encryption Standard Algorithm.

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

Introduction

In recent years, advances in communication technology have seen great interest in digital image transfer. However, the growth of a computer processor that has the power and Illegal access to storage has become easier. Encryption means Apply special mathematical algorithms and keys to Convert digital data to encrypted code before it is Moving and decrypting involves an application Algorithms and mathematical keys to restore the original data of encrypted code, the scientific community has seen strength Interest in image transfer. However, the data is illegal or images. Access has become easier and more frequent in wireless technology Public telecommunication networks. Privacy of information It becomes a challenging subject. To protect valuable data or image of unwanted readers or data encryption or images / Decryption is also necessary. As such in this work, A scheme based on encryption for security has been proposed Transfer images through channels [4].

Network encryption and security is a concept for network protection and data transmission over the wireless network. Data security is the key aspect of secure data transfer over an unreliable network. Data security is a difficult topic in current data communications that affect many areas, including a secure connection channel, powerful data encryption technology, and third-party trust in maintaining the database. Traditional encryption methods can only preserve data security. Encryption is the key technology in electronic key systems. It is used to maintain data confidentiality, digitally sign documents, access control, and so on. The terms used in encryption are simple image encryption (encrypted image),

encryption, and decryption, Alice, Bob and Eve. The simple image conversion process is called encryption (encrypted image) encoding. Encryption uses encryption technology to send confidential messages over an insecure channel. Encryption occurs on the sender side. The reverse encryption process is called decryption. It is a process of converting encryption (encrypted image) into the original image. Encryption uses decryption technology on the receiver side to obtain the original message for the unreadable message [2].

The current information technology, driven by technological development, the transfer of information security of the picture is a major concern, because the transfer process, information content can be intercepted by others to attack, making it easy to send information that drain. , The privacy of people will be threatened. These are connected to a computer network that has a close relationship. Thanks to the Internet, there are some gaps in the transfer of information security which is already dangerous. Belgian algorithm algorithms Joan Daemin and Vincent Regmin have proposed the standard AES encryption algorithm. Because the AES encryption algorithm is fast and has large capacity to resist attacks, this type of algorithm is widely used in data encryption. Therefore, in this document, you design a type of image encryption based on the AES algorithm. By processing digital images for standard AES encryption data, encode the date in the package. Put all the data together, reduce the encrypted image, and achieve the desired encryption effect [1].

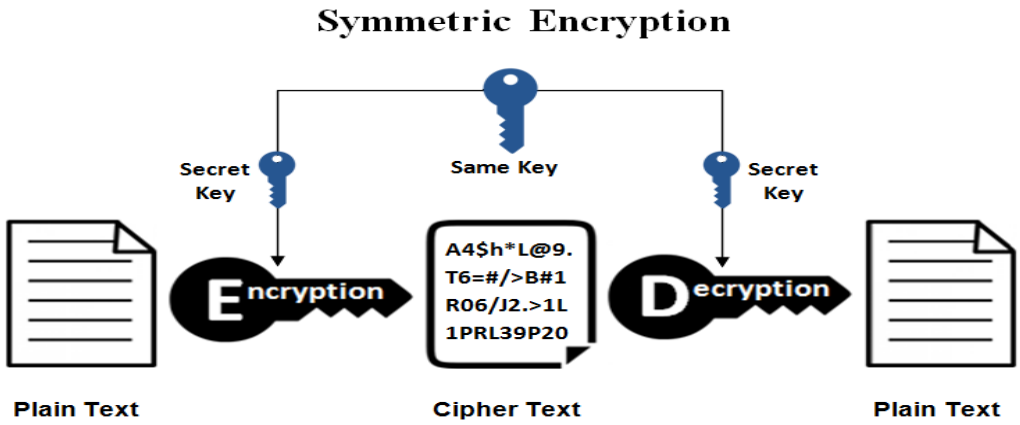

Figure 1 : Symmetric Algorithm based encryption decryption method

AES Algorithm

It is also known as Rijndael. The AES algorithm was developed by Vincent Rijman and Joan Damen. In October 2000, NIST accepted that the AES algorithm is the best algorithm for security, performance, efficiency, implementation and flexibility. The AES algorithm is a symmetric key algorithm, where both sender and receiver use the same key to encrypt data in encryption and decrypt encryption in the original data. In this algorithm, the fixed block length is 128 bits, while the size of the key size can be 128, 192, or 256 bits. AES is an iterative algorithm. It consists of 4 basic operating blocks. For full encryption, repetition is performed until "N" times. The total number of repetitions, ie, N, 10, 12 and 14, can be according to key length, ie 128, 192 and 256, respectively [3]. The AES algorithm is divided into four different stages, executed in successive rounds. These blocks work in an organized byte array as a 4 × 4 matrix called the case.

1. **Bytesub Transformation :** it is a non-linear byte substitution that uses a table of substations (sbox), which is created by a reverse transform and a multiple approximation.

2. **Converting transformation rows:** It is a simple byte switch, and the bytes are moved in the last three rows of the case. The shift to the left varies from one to three bytes.
3. **Mixcolumns Transform:** it is equivalent to multiplication matrix of case columns. Each vector is multiplied by a column with a array. Bytes are treated as multidimensional rather than numbers.
4. **Addroundkey Transformation:** It is a simple XOR between the ring key and the working condition. This shift is the opposite.

After an initial addroundkey, a round function is applied to the data block consisting of bytesub, shift rows, mix columns and addroundkey transformation, respectively. It is performed iteratively (N times) depending on the length of the key. The decryption structure has exactly the same sequence of transformations as the one in the encryption structure. The transformations Inv-Bytesub, Inv-Shiftrows, Inv-Mix columns, and Addroundkey allow the form of the key schedules to be identical for encryption and decryption [5].

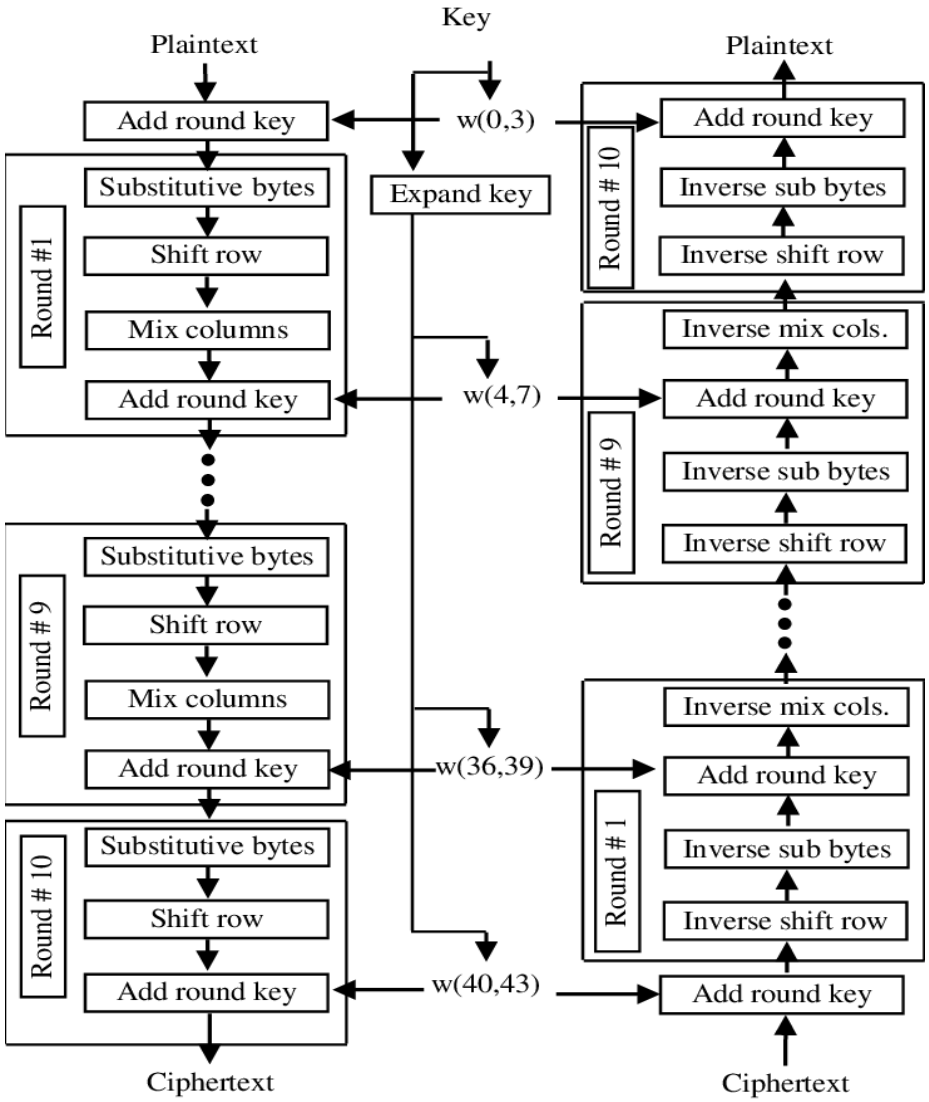

Figure 2 : Block Diagram of AES 128

AES Image Encryption

The proposed block diagram of AES 128 is shown in the figure 2. AES is the most popular and secure symmetric algorithm. The encryption and decryption key is same in AES. In the figure 3 shown the original image, Now we apply the AES algorithm on it to encrypt the image. The encrypted image is shown in the figure 4. The encrypted image is totally differing then the original image. Hence we secure the original image using the encryption. The histogram of the original image and the encrypted image is shown in the figure 5 and figure 6 respectively. If we want to get the original image from the encrypted image we apply the reverse of the AES and the decrypted image is shown in the figure 7.

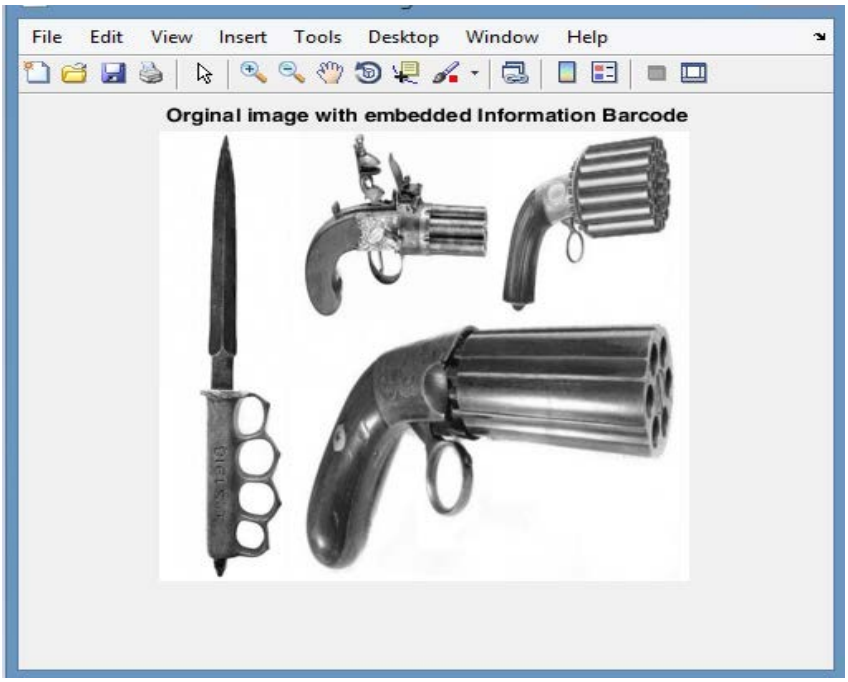

Figure 3: Original Image

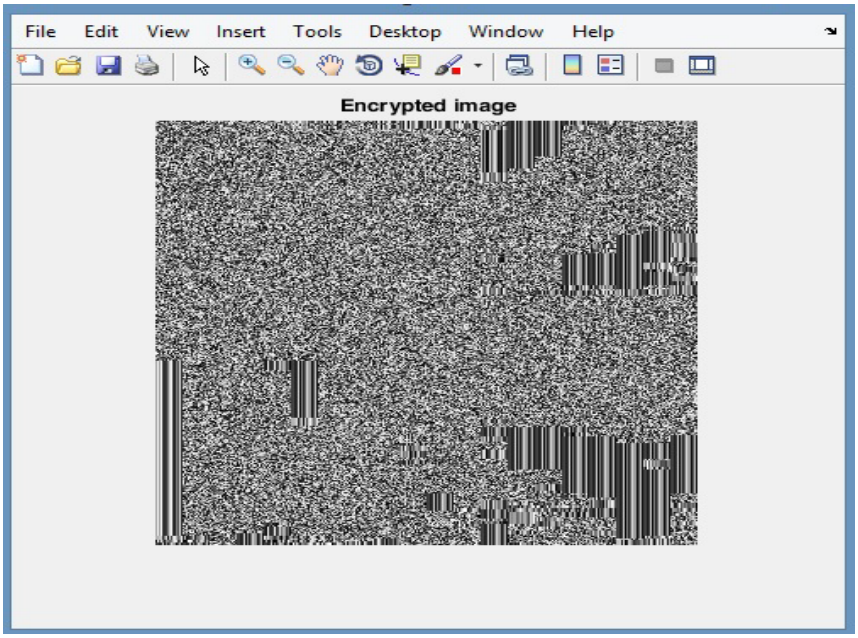

Figure 4 : Encrypted Image

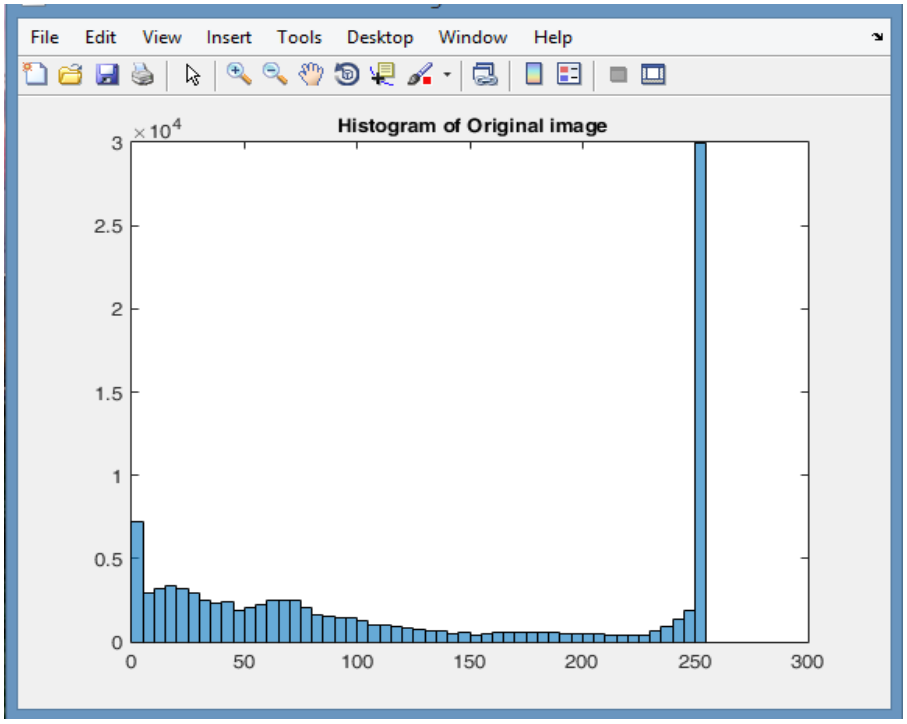

Figure 5 : Histogram of Original Image

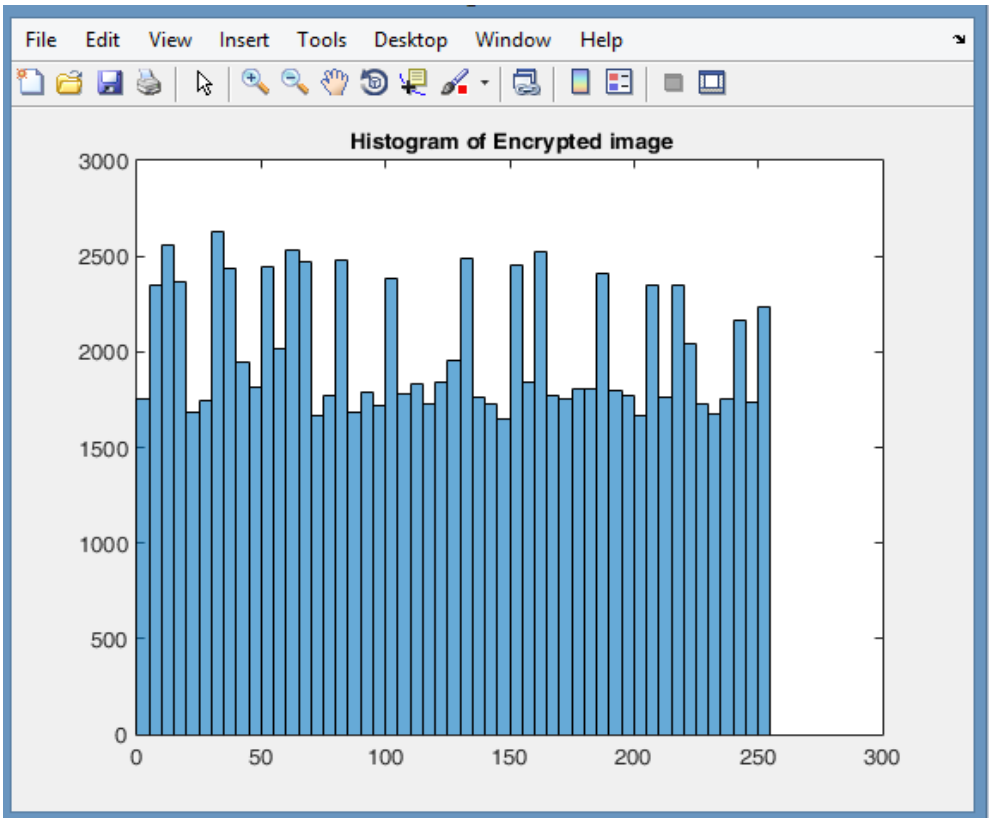

Figure 6: Histogram of Encrypted Image

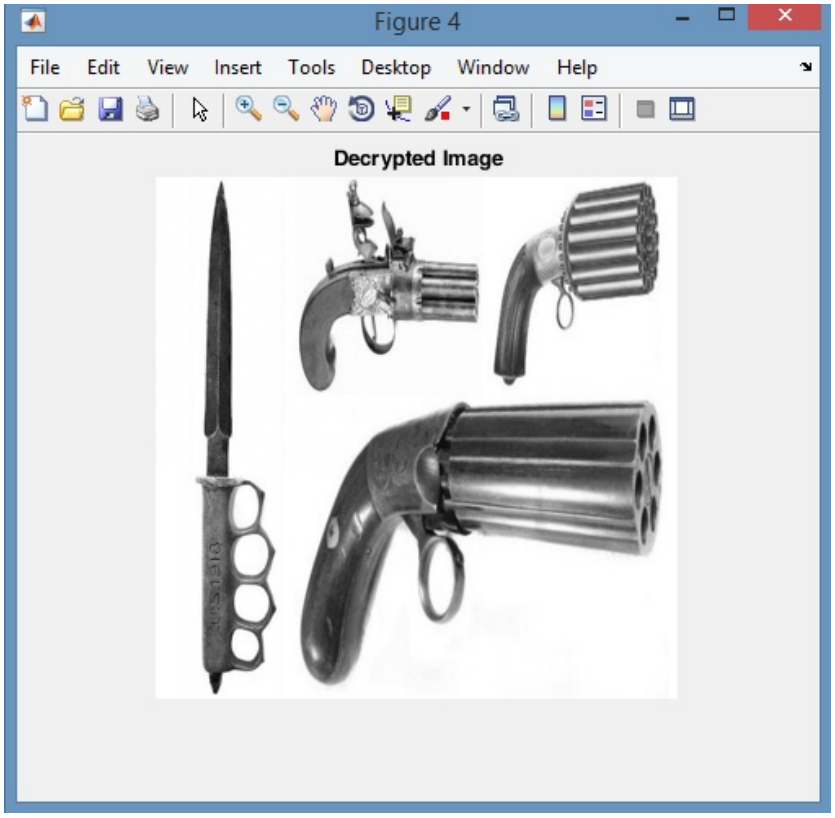

Figure 7: Decrypted Image

Conclusion

This paper puts forward the method that uses the AES algorithm with the key control to encrypt the image. This method incorporates a variety of characteristics, and with simple design. As the MATLAB has powerful numerical calculation function, especially for arrays and matrix calculations, and the infrastructure of the AES algorithm uses the matrix as the basic unit. So to implement the image encryption based on AES algorithm in the MATLAB environment is easy. From the above experimental results and analysis using this method can achieve very good effect on image encryption and the decryption essence has the same structure with the encryption, so it can easily restore the original image.

Reference

1. Qi Zhang and Qunding, “Digital Image Encryption Based On Advanced Encryption Standard(AES) Algorithm”, IEEE Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control, pp-1219-1221, 2015.
2. R. Sivakumar, B. Balakumar and V. Arivupandeeswaran, " A Review on IDEA, AES and Blowfish for Image Encryption and Decryption", International Journal of Advance Research, Ideas and Innovations in Technology, Volume 4, Issue 2, PP-2836-2838, 2018.
3. Avinash Ray, Anjali Potnis, Prashant Dwivedy, Shahbaz Soofi, Uday Bhade, " Comparative Study of AES, RSA, Genetic, Affine Transform with XOR Operation, And Watermarking for Image Encryption", IEEE Proceeding International conference on Recent Innovations is Signal Processing and Embedded Systems (RISE-2017), pp- 274-278, 27-29 October,2017.

4. P. Radhadevi and P. Kalpana, "Secure Image Encryption Using AES", IJRET: International Journal of Research in Engineering and Technology, Volume: 01 Issue: 02, PP-115-117, Oct-2012.
5. Ms. Pooja Deshmukh and Ms. Vaishali Kolhe, " Modified AES Based Algorithm for MPEG Video Encryption", IEEE ICICES2014 - S.A.Engineering College, Chennai, Tamil Nadu, India, pp-1-5, 2014.
6. Ahmad Abdulqadir Alrababah and Muasaad Alrasheedi, " Digital Image Encryption Implementations Based On Aes Algorithm", VAWKUM Transactions On Computer Sciences, Volume 13, Number 1, Pp- 1-9, May-June , 2017.
7. Akanksha Upadhyaya, Dr. Vinod Shokeen, Dr. Garima Srivastava, " Image Encryption: Using AES, Feature extraction and Random No. generation", IEEE 2015, PP-1-4, 2015.
8. Ms.Anuradha, Dr. Somesh Kumar, (Prof)Dr.Anuranjan Misra and Dr.K.Rama Krishna, " Improved Rapid AES for Secure Digital Images", IEEE International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS-2017), PP-1429-1431, 2017.