WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

IMAGE ENCRYPTION AND DECRYPTION

Mathesh.K

Bachelor of computer science,Sri Krishna Adithya College of Arts and Science.

ABSTRACT :

Security information has become the major concern for the fast growth of the digital exchange of data storage and transmission. As there is rapid growth of using images in many fields, so it is important to protect the private image data from the intruders. Image protection has become an imperative issue. To protect an individual privacy has become a crucial task. Different methods have been explore and developed to preserve data and personal information. To protect the important information from unauthorized users, image encryption is used. Encryption is the one of the most used technique to hidden the data from unauthorized users. The Advanced Encryption Standard (AES) is used for image encryption which uses the key stream generator to increase the performance of image encryption.

Keywords: Image Encryption,Data Security,Privacy Protection,Advanced Encryption Standard(AES)

1. Introduction :

In the last few years the security and integrity of the data is the most important concern. Now a day's almost all the data is transferred over the computer networks and it has increased the attacks over the network. Before transmitted data it has to be encrypted and store so that it cannot be attacked by various attackers. Encryption is a process of hiding the data, where it converts the original text into cipher text. Encryption uses different algorithm to encrypt the data into different form. Cryptographic Algorithm uses a set of keys with the different characters for both encryption and decryption. By using key the plain text is converted to the cipher text and decryption is done by converting back the plaintext from the cipher text. Cryptography is a process of transmitting and storing data in a form that it is read only by authorised users. Cryptography is a science of protection of data by encoding it into unreadable form. It is useful way of protecting the important sensitive information by using mathematical form algorithm for both encryption and decryption process. The encryption and decryption process depend on the key value. The strength of the algorithm is how difficult it is to determine the key value and get the original text. The algorithm is majorly divided into two types symmetric and asymmetric depending on the keys. If same keys are used for both encrypting and decrypting then it is called symmetric algorithm. Symmetric algorithm is further divided into stream and block ciphers. A stream cipher is done on the single byte of data, where as the block a cipher is done on the block of data. Asymmetric algorithm uses two different keys one for encryption and both for decryption. The key should be kept secret so that the message should be not be decrypted. The purpose of cryptography is to provide Authentication (proving the one's identity), Non-repudiation (the receiver should know the sender should not be faking), Integrity (data should be correct, accuracy, and trustworthiness), and Privacy/confidentiality (message is read by only the intended receiver).

1.1 AES ALGORITHM: : The development of AES was begun on January 1997 by NIST; a symmetric key encryption algorithm is made successful over the DES algorithm. The algorithms where initially divided into 15 types, later it has reduced to 4 algorithms. The AES algorithm is also called as Rijndael algorithm. Where the block of the text both for encryption and decryption is not fixed.

The difference between DES and AES

Factors	**DES**	**AES**
Key Length	56 bits	128,192,256 bits
Block Size	64 bits	128,192,256 bits
Cipher Text	Symmetric block cipher	Symmetric block cipher
Developed	1977	2000
Security	Proven inadequate	Considered secure
Possible Keys	2^56	2^128,2^192,2^256

2. Problem Definition :

2.1 Existing System The variation in the characteristics of the multimedia data such as correlation among the pixels and high redundancy of the image. Therefore there were some limits where same techniques cannot be used for protection all type of multimedia data. The traditional encryption algorithms may not use to encryption the image directly because of these reasons:

- As the size of image will be not same as the text it may varies. Hence the traditional encryption algorithm may take longer time to encrypt and decrypt the image compare to text.

There is condition which says that the text encryption both decrypted and original text must be equal but it can be never true for the image. For decryption of image the small distortion is also accepted by the human perceptive.

- Computational time is high in exiting system.
- High computing power is required.
- For networking Systems it is not efficient.
- Security is also a major issue.

3. Proposed System :

There should be a reliable storage and transmission of digital image where it has been served such as multimedia systems, medical and military imaging systems. The security of image is the most critical problem, due to increase in the growth of internet, cell phones and multimedia technology in the society. This project is to propose a secure image encryption and decryption form by using AES algorithm. The AES algorithm is widely used in the applications of daily life, such as smart cards, cell phones, automated teller machines and WWW servers. AES encrypts a plaintext to a cipher text, which can be decrypted to the original plaintext by using common private key. The cipher text is made very different form so that it should not have any idea of the original plain text. For image encryption and decryption, the AES encrypt the image in different form using the key which should have no idea of original form. After decrypting it, it should be in the original form. The encryption of image should be strong so that it should not be known by the intruders.

Strengths of AES:

- AES is extremely fast compared to other block ciphers.
- As the round transformation is parallel for the design, which makes the important for the hardware to allow it for fast execution.
- AES was designed to be agreeable to pipelining
- There is no arithmetic operations for the cipher, so there is no bias towards the big or little endian architectures.
- AES is fully self-supporting.
- AES is not based on obscure or not well understood processes.

III. LITERATURE SURVEY :

To study and analyze more about Machine Learning, the following literature survey has be done.

In [1] the authors present a new Chaotic Key-Based Design for Image Encryption and Decryption. The VLSI architecture for image encryption and decryption algorithm is proposed. The XORed or XNORed bit-by-bit is used to predetermine keys for the chaotic binary sequence of the gray level of each pixel. There are the following features such as low computational complexity, no distortion, and high security. VLSI architecture has advantages such as low hardware cost, high computing speed, and hardware utilization efficiency. The architecture is also integrated with MPEG2 scheme and simulation results are also known.

In [2] the authors present a Modified AES Based Algorithm for Image Encryption. Most common technique to provide the security for image is encryption. There are wide applications of image and video such as internet communication, multimedia systems, medical imaging, tele medicine and military communication. There are different image protection techniques such as vector quantization. There are different methods for vector quantization where the image is decomposed into vectors where encoding and decoding is done by vector by vector. Or by dividing the image into desired form into large number of shadows that guarantee the undetectable to illegal users.

In [3] the authors present secure image encryption using AES. Security is the main and major issue in today's world. The transmission of image for communication has been increased and providing confidentiality from unauthorized access is the major task. It is difficult to provide an individual the security. There are various methods to protect the data from unauthorised user. AES is used for encryption and decryption of the image where the image using the key is converted into a form which cannot be recognised and later by authorised receiver it is converted back to original image.

In [4] the authors present an image encryption and decryption using AES algorithm. The design of effectively security for the communication of the image is done by using AES algorithm for encryption and decryption. AES has replaced Data Encryption Standard (DES) by providing more security. AES key expansion uses the 128 bit key for encryption process by using bit wise exclusive or operation of image set pixels.

In [5] the authors present an Image Encryption Based n AES Key Expansion. There are specific characteristics of image such has high rate of transmission with limited bandwidth, redundancy, bulk capacity and correlation among the pixels. These are characteristics has to be notice will encrypting the image.

So, AES algorithm is used with the key expansion where encryption process is done by using bit wise exclusive or operation of image pixels set along with 128 bit key. The key is generated at the sender and receiver side based on the AES Key Expansion

4. Aims And Objectives

The model for encryption and decryption of an image is designed with the some objectives:

- For transmission of the image based on data as well as storage it should have confidentiality and security by using suitable key. • To study the architecture of the image file.
- To encrypt the image file by developing the application.
- Eventually, the image is focused on most famous file type of image format i.e. JPG.
- The image is focused to JPG file type which is the most famous type of image format.
- The application must be simple, easy to use and powerful.
- Many factors have to be considered in order to develop the application such as processing speed of image, the strength of encryption result and ease of use to end users.

5.Methodology :

AES encrypts a plaintext to a cipher text, which can be decrypted to the original plaintext by using common private key, an example is shown in Figure 1a, It can be seen the cipher text should be in different from and gives no clue to the original plaintext. Figure 1a shows the Encryption of AES operation using cipher key. Where the plain text along with key is given to encryptor, which encrypt the plain text into cipher text, which is the result of encryption process. In reverse the decryption take place where the cipher text along with key is given to decryptor and it result into the original plain text

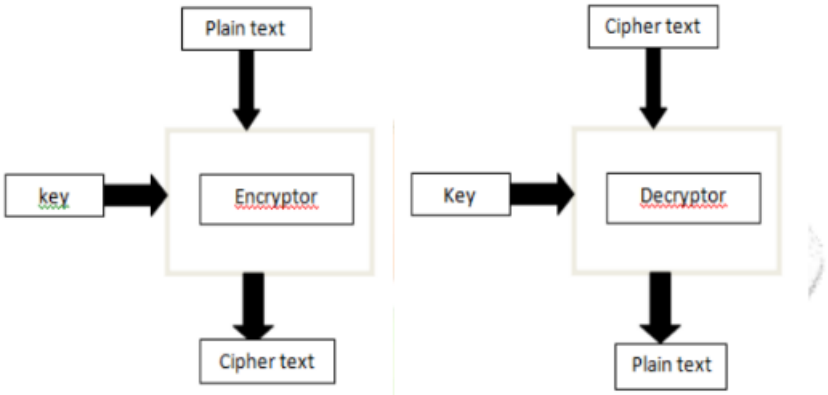

Fig 1a: Encryption and decryption of AES operation.

For the applications of AES image encryption and decryption, the encrypted image should be different from and give no clue to the original one, an example figure1b is shows the encrypted image and that encrypted image to original image.

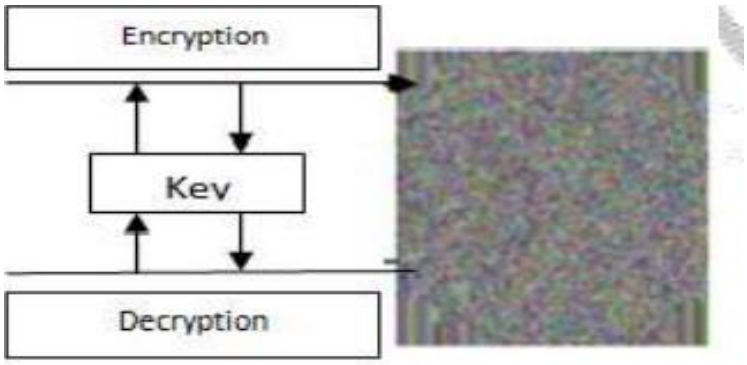

Fig 1b: Example for AES Encryption and Decryption

With AES encryption, the secret key is known to both the sender and the receiver. The AES algorithm remains secure, the key cannot be determined by any known means, even if an eavesdropper knows the plaintext and the cipher text. The AES algorithm is designed to use one of three key sizes (Nk). AES-128, AES-196 and AES-256 use 128 bit (16 bytes, 4 words), 196 bit (24 bytes, 6 words) and 256 bit (32 bytes, 8 words) key sizes respectively. These keys, unlike DES, have no known weaknesses. All key values are equally secured thus no value will render one encryption more vulnerable than another. The keys are then expanded via a key expansion routine for use in the AES cipher algorithm.

REFERENCES :

[1] Jui-Cheng Yen and Jim-In Guo, "A New Chaotic Key-Based Design for Image Encryption and Decryption",2000.
[2] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki , "A Modified AES Based Algorithm for Image Encryption" ,2007 .
[3] P. Radhadevi, P. Kalpana , "Secure Image Encryption Using Aes",2012 .
[4] Roshni Padate, Aamna Patel, "Image Encryption And Decryption Using Aes Algorithm" ,2014.
[5] Jose´ J. Amador, Robert W. Green, "Symmetric-Key Block Cipher for Image and Text Cryptography", 2005.
[6] Philip P. Dang and Paul M. Chau, "Image Encryption For Secure Internet Multimedia Applications", 2000.
[7] Sanjay Kumar, Sandeep Srivastava, "Image Encryption using Simplified Data Encryption Standard (S-DES) ", 2014.
[8] Kundankumar Rameshwar Saraf, Vishal Prakash Jagtap, Amit Kumar Mishra, "Text and Image Encryption Decryption Using Advanced Encryption Standard", 2014
[9] P.Karthigaikumar, Soumiya Rasheed "Simulation of Image Encryption using AES Algorithm", 2011.
[10] B.Subramanyan, Vivek.M.Chhabria, T.G.Sankar babu , "Image Encryption Based On AES Key Expansion", 2011