www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
Vol. 02, Issue 04, April-2022, pp: 1-4

e-ISSN : 2583-1062
Impact Factor : 2.205

IMAGE ENCRYPTION USING AES ALGORITHM

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

Department of Information Technology, PCE, Navi Mumbai, India – 410206.

ABSTRACT

Data security plays an important role in every communication over the internet. Secure exchange of data or transfer from sender end to receiver should be done in authenticated ways. We are using AES algorithm for image data encryption as well as decryption , In this paper an image or files are given as input to AES encryption algorithm which gives decrypted output. The same AES algorithm is used to encrypt the decrypted data by using secret keys.

Keywords:- AES algorithm ,encrypt, decrypt .

1. INTRODUCTION

The use of the internet has increased in day to day life for the smallest communication transfer of data happened. To make this transfer of data safer and secure many encryption algorithms are used , DES and AES are examples of such algorithms .

The data is encrypted from sender end and receiver gets the data in encrypted form; which further gets encrypted by receiver end with the help of secret key . Which is kept common between receiver and sender. The encrypted data is in an unreadable form so that unauthorized users can't access the data.

2. LITERATURE SURVEY

Digital image encryption implementation based on AES algorithm:- This paper primarily is focusing on the necessary protection of these images using a specific analyses algorithm Advanced Encryption Standard (AES) with a full its description, which is known as an algorithm (Rijndael).Findings: It will be determined the address decryption, which is made up of different styles in all encryption and decryption steps in order to protect the valuable information.

An image encryption method based on chaos system and AES algorithm :- In this paper, A randomized chaos sequence is used to generate the encryption key. Then, the original image is encrypted with the modified AES algorithm and the round keys from the randomized chaos sequence.

A Review on Various Image Encryption Techniques using AES and Random RGB Substitution :- This paper simply describes the images protection when we transmit from one place to another. In this paper, the Huffman lossless image compression technique for compressing the image which is generated by the text to image encryption. In this paper, a text and convert it into image with C#.

An image encryption and decryption using AES algorithm: - In this paper, Image Encryption and Decryption using the AES algorithm is implemented to secure the image data from unauthorized access. A Successful implementation of the symmetric key AES algorithm is one of the best encryption and decryption standards available in the market.

Image Encryption with Double Spiral Scans and Chaotic Maps: - In this paper, they proposed an image encryption algorithm based on double spiral scans and chaotic maps. A key contribution is the double spiral scans, which can efficiently scramble pixels of the image block. Moreover, content-based key are generated and used to control the Lu chaotic system, so as to ensure our sensitivity to the change of input.

Table 2.1 Summary of literature survey

SN	Paper	Advantages	disadvantages
1.	**Image Encryption Technique using AES and Random RGB Substitution**	It is implemented to secure the image data from unauthorized access.	It has some drawbacks, including high computation costs, pattern appearance, and high hardware requirements.
2.	**Digital Image Encryption Implementations Based on AES Algorithm**	To increase the need for exchange in digital photos electronically, due to alarming demand for multimedia applications, and because of the increasing use of images in electronic processes.	However, there are limitations of this approach. Future research will be challenged to enhance the effectiveness of algorithms

3.	**An Image Encryption Method based on Chaos System and AES Algorithm**	In this method, the encryption key is generated by Arnold chaos sequence. Then, the original image is encrypted using the modified AES algorithm and by implementing the round keys produced by the chaos system.	The evaluation parameters of the resistance against the differential attacks. The results clarify that the small changes in the original image and key result in the significant changes in the encrypted image and the original image cannot be accessed.
4	**An Image Encryption and Decryption using AES algorithm**	Original images can also be completely reconstructed without any distortion. It has shown that the algorithms have extremely large security key space and can withstand most common attacks such as the brute force attack, cipher attacks and plaintext attacks.	Main weaknesses where AES shows are the 128 bit block size and the fact that AES 192 and 256 have far less security margin than the pure key size would suggest.
5.	**Image Encryption with Double Spiral Scans and Chaotic Maps**	A key contribution is the double spiral scans, which can efficiently scramble pixels of the image block. Moreover, content-based keys are generated and used to control the Lu chaotic system, so as to ensure our sensitivity to the change of input image.	It requires large key space. The time required during double scan is more

3. SUMMARY OF RELATED WORK

DES

For encryption and decryption, DES uses a shared secret key.

The DES algorithm as described by Davis R [9] takes a fixed length of plaintext bits and converts them through a series of operations into cipher text strings of the same length, each block being 64 bits long.

There are 16 identical stages of processing, called rounds, as well as an initial and final permutation called IP and FP.

3DES

The 3DES standard is an enhancement of the original DES and consists of 64 bit blocks and 192 bit keys. This standard uses a similar encryption algorithm to the original DES, but allows for greater encryption levels and longer safe times.

3DES is slower than other block cipher methods, since it uses two or three 56 bit keys in the sequence of Encrypt-Decrypt-Encrypt.

TDES algorithm with three keys requires 2168 combinations while TDES algorithm with two keys requires 2112 combinations; the disadvantage of this algorithm is that it is too time consuming to implement.

Blowfish

Bruce Schneier, one of the world's leading cryptologists and the president of Counterpane Systems, a firm that specializes in computer security and cryptography, developed one of the most common public domain encryption algorithms, Blowfish R[10].

Blowfish encrypts 64-bits of data with a variety of key lengths, and it has two parts. Data Encryption: This is the iteration of a simple function 16 times.

Rounds contain key dependent permutations and data dependent substitutions. Subkey Generation: It involves converting a key up to 448 bits long into 4168 bits.

RSA

A public key algorithm was invented by Rivest, Shamir, and Adleman [11]. RSA consists of a public key and a private key. The public key can be known to everyone and is used to encrypt messages.

Messages encrypted with the public key can only be decrypted with the private key. Private keys for the RSA algorithm may be generated in several ways.

4. METHODOLOGY

Modified Advanced Encryption standard . The algorithm has four operating blocks where we observe the data at either the byte or bit level, the algorithm can treat any combination of data, and the 128 bit key size allows for flexibility.

The four stages that we use are:

- Substitution bytes
- Mix columns
- Shift Row
- Add Round Key
- The four steps in each round of decryption are as follows:
- Inverse shift rows
- Inverse substitute bytes
- Add round key
- Inverse mix columns.

5. CONCLUSION

The purpose of encryption is to ensure secure communication. In this paper, it is discussed about the existing works on the encryption techniques, such as AES, 3DES, RSA, Blowfish, and DES. The key size for DES is too small when compared to other techniques, while 3DES is slower than other block cipher methods and has poor performance. Compared to the original Blowfish algorithm, AES is a better algorithm. And the adjacent pixels in an image are of close relation that cannot be removed by AES algorithm. Besides the security issue, encrypting images with these ciphers directly can take a long time and is not suitable for real-time applications. To improve this problem, a modified advanced encryption Standard is proposed. This modification may improve security as well as performance.

ACKNOWLEDGEMENT

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 .

6. REFERENCE

[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.

[8] E.Thmbiraja, G.Ramesh, Dr.R.Umarani, “A survey on various most common encryption techniques”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol 2, Issue 7, July 2012.

[9] Davis.R, "The Data Encryption Standard in Perspective", Proceeding of Communication Society magazine, IEEE, Vol 16, Nov 1978.

[10] Pratap Chandra Mandal "Superiority of Blowfish Algorithm", International Journal of Advanced Research in Computers Science and Software Engineering Vol 2 Issue 9, Sep 2012.

[11] R.L.Rivest, A.Shamir, L.Adleman, "A Method for obtaining Digital Signatures and Public- Key Cryptosystem", Communication of the ACM, Vol 21, Feb 1978.