IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

VOLUME : 6 ISSUE : 1 Print / Issue Publication Date: 08-Aug-2021

ISSN : 2455-2143

DOI : 10.33564/IJEAST.2021.v06i01.030

Indexed In

Google SCHOLAR OPEN ACCESS doi Crossref

WWW.IJEAST.COM

editor@ijeast.com

International Journal of Engineering Applied Sciences and Technology, 2021
Vol. 6, Issue 1, ISSN No. 2455-2143, Pages 214-217
Published Online May 2021 in IJEAST (http://www.ijeast.com)

IMAGE ENCRYPTION FOR SECURE INTERNET TRANSFER

V Goutham Bharadwaja
Department of ISE
Dayananda Sagar College Of Engineering,
Bangalore, Karnataka, India

Yashas M S
Department of ISE
Dayananda Sagar College Of Engineering,
Bangalore, Karnataka, India

Yathendra Yadav T V
Department of ISE
Dayananda Sagar College Of Engineering,
Bangalore, Karnataka, India

Gelvesh G
Department of ISE
Dayananda Sagar College Of Engineering,
Bangalore, Karnataka, India

***Abstract*— Security is a crucial side to preserve the confidentiality of information such as pictures and text. The probability of an assailant attempting to access the image in the course of transferring process is high as assailant may get hold of important data. Therefore, encryption methods are used for securing the data. A novel image encryption algorithm that is a combination of the AES algorithm and the chaos sequence is proposed in this paper. The project will use AES for encryption and decryption of the image transfer because AES is capable of solving problem that cannot be resolved by different algorithms. The original image is transformed into cipher-image using a share secret key and this process is called encryption while the reverse of encryption process is known as decryption. This method's sensitivity to the initial values and input image, even the tiniest changes within these values will result in significant changes in the encrypted image. We show that this approach can shield the image against different attacks exploitation using histogram analysis.**

***Keywords*— AES, cipher, chaos sequence, image encryption, image decryption**

I. INTRODUCTION

Now a day's, technology has become an essential factor in our everyday life. The usage of devices like laptop, computer and mobile for communication as well as for data storage and transmission has inflated. This has led to a retardant in security. Cryptography is one of the ways of securing the data. The process of encryption is dispensed. The encrypted data is not liable to the unauthorized user.

There are numerous cryptographical techniques offered for securing crucial information like Data Encryption Standard (DES), Triple DES, RC4 and Advanced Encryption Standard (AE). The algorithm converts the text or image into cipher information and the other way around. This process is known as encryption and decryption.

There are generally two forms of cryptographical mechanisms: symmetric key cryptography within which the same key is used for both decryption and encryption. And the other type is asymmetric key cryptography, within which two different keys are used for encryption and decryption. Symmetric key algorithm is much faster and easier for implementation and needs less processing power as compared to asymmetric key algorithm.

Advanced Encryption Standard (AES) is a symmetric block cipher encryption method. This means that it operates on fixed-length chunks of data (for example, blocks), applying constant transformation to every block. The transformation can be controlled by the employment of encoding key. Block ciphers use symmetric keys, which mean that the same key used to encrypt data is also used to decrypt it.

Several standard encryption algorithms have already been proposed for the aim of text encryption. Due to redundancy of the visual data, correlation between adjacent pixels and, the high volume these algorithms have terribly low security and high encoding time. Therefore, these algorithms are not ideal for the image encryption. Numerous image encryption algorithms are introduced to overcome these issues. Generally, many evaluation criteria should be thought for image encryption, together with the data entropy, correlation between adjacent pixels. For the algorithm to resist different attacks performed by the assaulter, the values of this criteria ought to meet the required expectancy.

International Journal of Engineering Applied Sciences and Technology, 2021
Vol. 6, Issue 1, ISSN No. 2455-2143, Pages 214-217
Published Online May 2021 in IJEAST (http://www.ijeast.com)

This paper proposes an image encryption algorithm, combining the chaos system and standard encryption algorithm of AES. First, the encryption key is built using chaos system, and then, the image is encrypted by using the proposed algorithm. The subsequent sections make a case to the results in detail.

II. RELATED WORK

A technique for image encryption using digital signature [1]. The digital signature of the initial image is added to the encoded version of the initial image. The image is encoded using an appropriate error management code, such as a Bose-Chaudhuri Hochquenghem (BCH) code. At the receiver end, after the image is decrypted, the digital signature will be accustomed to verify the genuineness of the image.

A novel image encryption algorithm supported on self-adaptive wave transmission [2]. Describes a fast image encryption algorithm based on self-adaptive wave transmission that uses one half of image data to encrypt the opposite half of the image. The method to achieve the high security will be continued. During encryption, an image is equally divided into two parts, wave transmission encryption technique with four waves is employed to encrypt both the parts whose amplitudes are determined by the opposite one. Since the amplitude of the wave may be too overlarge, it is not convenient to represent it in computer due to computation complexity.

A digital image encryption algorithm based on chaotic mapping [3]. Proposes the enciphering using the chaotic technique. Distinctive data is extracted. Add-image feature procedure is applied here. The chaotic number which is selected by the sender is the key here. Chaotic number and the distinctive data chosen generates the chaotic sequence. The algorithm will be able to restore the original data with no loss of data.

A novel selective encryption method for securing text over mobile ad hoc network [4]. This paper proposes a method referred to as selective encryption for securing the text over wireless Networks. This selective encryption method encrypts only the necessary texts instead of encrypting the entire text. Usually in scenarios like wireless network devices, it is tough for a sensor to spend more computational cost on encrypting and decrypting just to use the battery. Hence by applying the selective Encryption Method over the Ad hoc networks the processing interval is reduced that additionally will increase the scalability of data transmission.

Text to image encryption technique using RGB substitution and AES [5]. This paper proposes a way of converting a text to image and then encryption is applied to that. RGB

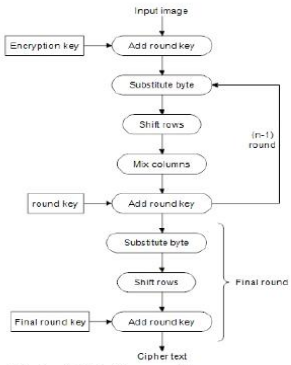

Fig1. AES Encryption

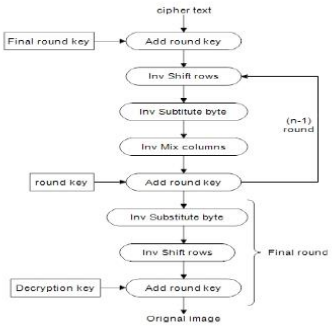

Fig2. AES Decryption

substitution method is employed to convert the text to an image where each character of the text is appointed to a pixel randomly and an image is formed through it. The image is then encrypted using AES Algorithm and therefore decryption occurs in reversed manner. This proposed technique is extremely secure because even if the assailant tries to decrypt the output would be an image.

Survey of 3D Chaotic Map Techniques for Image Encryption [6]. This paper proposes the various chaotic map techniques for image encryption. The 2D chaotic cat Map is generalized to make 3D cat map, applying the 3D cat map on the image that needs encryption helps to shuffle the image pixels and positions. Shuffling the pixels is done using two stages, these stages are namely confusion and diffusion. Due confusion occurs due to shuffling and it also makes the distinction between the plain image and cipher image. So that the resistance to attacks and security is increased that makes the image secured.

Rapid Encryption Method based on AES Algorithm for Grey Scale HD Image Encryption [7]. To handle the high computational load of the AES algorithms the number of rounds of AES are reduced to just one round, and to encrypt greyscale high-definition images a new S-box method is proposed. The reduction to only a single round showed a really vital attenuation in the encryption time of the algorithm by 1/10 and reduced the ROM used by 256 bytes.

A New Modified Version of Advanced Encryption Standard Based Algorithm [8]. An AES modification by adjusting the Shift Rows transformation was introduced by this paper. The idea of shifting of rows is from the value in the state ([0][0]) whether the value of the state is odd or even. The result shows that the proposed transformation provides better encryption time because it does not have any surplus operations.

Data security-modified AES algorithm and its applications [9]. In this paper, initially the original image is used as the input. Then, the rows and columns of the image's pixels are right-

International Journal of Engineering Applied Sciences and Technology, 2021
Vol. 6, Issue 1, ISSN No. 2455-2143, Pages 214-217
Published Online May 2021 in IJEAST (http://www.ijeast.com)

shifted to a certain value in order to eliminate the correlation between the adjacent pixels. For the consequent step, the keys are created based on the location of the mouse on the screen. Given these keys as the primary keys and using the key expansion function, 11 round keys of AES algorithm are generated. These keys are sequentially given to AES algorithm to convert the initial image to the encrypted one. This algorithm provides higher and better encryption results regarding the protection against the statistical attacks.

Image encryption based on new Beta chaotic maps [10]. A beta-based chaos map was used for generating the chaos sequence. This technique is split into three steps: permutation, diffusion and substitution. The pseudorandom sequence is generated in order to interchange the original image pixel locations to eliminate the relation between the encrypted and encrypted images. Hence, the resistance of the encrypted image will increase against the attacks.

III. PROPOSED ALGORITHM

AES and Chaos System

AES is a symmetric key encryption and block cipher algorithm. AES operates on a 4×4 matrix of bytes, National Institute of Standard and Technologies (NIST) began an endeavor to develop DES. AES also can be referred as Rijndael's algorithm because it relies on Rijndael's algorithm. AES varies slightly from Rjindael's Cipher algorithm because it needs block size to be 128-bits whereas Rjindael's cipher require any block size of multiple 32 as long as it exceeds 128.There are three completely different key lengths available in AES which are 128,192 and 256 bits. The AES algorithm uses a round function that is composed of four completely different byte-oriented transformations. For encryption purpose four rounds consist of:

- Substitute byte
- Shift row
- Mix columns
- Add round key

The length of key use for Encryption and Decryption determine the number of rounds.
For each of its Cipher and Inverse Cipher, AES algorithm uses a round function. This function is comprised of four different byte-oriented transformations.
AES has four main operational blocks:

1. Substitute byte transformation: To substitute each data block byte with another block, an S-box is used.
2. Shift transformation of rows: Every row of the state matrix is given a cyclic shift to the right side according to its location.
3. Mix Transformation of Columns: It is a matrix multiplication operation where each column of the state matrix is multiplied by that of the fixed matrix.
4. Add Round Key Transformation: An XOR operation is performed between the new state matrix and the round key one.

Chaos theory is a branch of mathematics which investigates the extremely complicated systems. In these systems, applying small changes in the input results in the significant changes in the output.
Chaos system has the subsequent features:
1. Sensitivity to the initial value: Minute changes within the initial values result in a completely different sequence that is achieved through repetitive computations with the parameters on a chaos map.
2. Sensitivity to the parameters: Minute changes within the parameters yield a very completely different sequence that is achieved through repetitive computations with the input values on a chaos map.
3. Randomness: The generated chaos sequences using the chaos maps are largely pseudorandom sequences and their structures are very complex for analysis and prediction.
If an unauthorized person does not have any idea regarding initial values and the correct control parameters, then that person cannot guess the chaos sequence. In alternative words, chaos systems can improve the protection of the image encryption systems.

IV. RESULT

In this section, the histogram of the original, encrypted and decrypted images is mentioned for analysing the encryption.

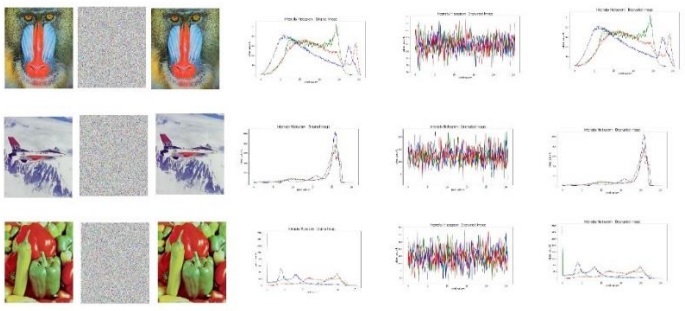

Fig**3.** Histogram of images

As it can be observed, the histogram of the encrypted image is uniform and significantly differs from that of the original one.

Therefore, no sign of the original image is existent to be used by the attacks done by the hackers or the attackers.

In this figure, column A depicts the original image, column B is the cipher image, column C is the decrypted image; column D depicts histogram of the original image; column E is the histogram of the cipher image and column E is the histogram of the decrypted image.

V. CONCLUSION

In this paper, image encryption and decryption are implemented using AES algorithm and chaos sequence. A successful implementation is done using JAVA coding for the encryption and decryption process. Histogram analysis and Adjacent pixel auto correlation is done for the images to ensure the efficiency of the encryption method implemented. Therefore, the encryption method can withstand many different attacks such as brute force attack, cipher attack and plaintext attacks.

VI. REFERENCE

[1] Aloka Sinha, Kehar Singh, A technique for image encryption using digital signature. Optics Communications, 218(4-6), 229-234

[2] X. Liao, S. Lai and Q. Zhou, A novel image encryption algorithm based on self-adaptive wave transmission. Signal Process., 90 (9) (2010), pp. 2714-2722

[3] Deng, Z., & Zhong, S. (2019). A digital image encryption algorithm based on chaotic mapping. Journal Of Algorithms and Computational Technology, 13, 1748302619853470

[4] Kushwaha, A., Sharma, H. R., & Ambhaikar, A. (2016). A novel selective encryption method for securing text over mobile ad hoc network. Procedia Computer Science, 79, 16-23

[5] Joshy, A., Baby, K. A., Padma, S., & Fasila, K. A. (2017, November). Text to image encryption technique using RGB substitution and AES. International Conference on Inventive Computing And Informatics (pp, 1133-1136).

[6] Gagnani, L. P., & Varjani, S. (2015). Survey of 3D Chaotic Map Techniques for Image Encryption. International Journal Of Science And Research (IJSR),2319,7064.

[7] S.M. Wadi and N. Zainal, "Rapid Encryption Method based on AES Algorithm for Grey Scale HD Image Encryption"

[8] S.H. Kamali, R. Shakerian, M. Hedayati, and M. Rahmani, "A New Modified Version of Advanced Encryption Standard Based Algorithm",*ICEIE*

[9] Mondal Subijit, Maitra Subhashis (2014) Data security-modifed AES algorithm and its applications. ACM SIGARCH Comput Archit News42(2):1-8

[10] Zahmoul R, Ejbali R, Zaied M (2017) Image encryption based on new Beta chaotic maps. Opt Lasers Eng 1(96):39-49

[11] Patro K, Banerjee A, Acharya B (2017) A simple, secure and time efcient multi-way rotational permutation and difusion based image encryption by using multiple 1-D chaotic maps. International Conference on Next Generation Computing Technologies. Springer, Singapore, pp 396–418

[12] Bashir A, Hasan AS, Almangush H (2012) A new image encryption approach using the integration of a shifting technique and the AES algorithm. Int J Comput Appl 975:8887

[13] Ahmed BA, Abd SB, Hamida A (2012) A novel image encryption using an integration technique of blocks rotation based on the magic cube and the AES algorithm. IJCSI 9(4):41–47

[14] Zahmoul R, Ejbali R, Zaied M (2017) Image encryption based on new Beta chaotic maps. Opt Lasers Eng 96:39–49

IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

ABOUT IJEAST

International Journal of Engineering Applied Science and Technology (IJEAST) is a peer-reviewed, open access journal that publishes high-quality research papers in the field of Engineering, Applied Science and Technology.

IJEAST aims to provide a platform for researchers, academicians, and professionals to share their innovative ideas, research findings, and practical experiences with the global scientific community.

FOCUS AREAS

- Engineering
- Applied Science
- Technology
- Innovation & Development
- Interdisciplinary Studies

PEER REVIEWED
All submissions are rigorously peer reviewed to ensure quality.

OPEN ACCESS
Free and unrestricted access to research for all.

GLOBAL REACH
Connecting researchers and professionals worldwide.

TIMELY PUBLICATION
We ensure a swift and efficient publication process.

For more information, visit our website
www.ijeast.com

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

editor@ijeast.com
www.ijeast.com
India

2455-2143