IMAGE ENCRYPTION USING AES FEATURE EXTRACTION AND RANDOM NO. GENERATION

Dr.M.Rajaiah,Dean Academics & HOD, Dept of CSE, Audisankara College of Engineering and Technology, Gudur.

Mr. Syed Akthar Basha, Associate Professor ,Dept of CSE, Audisankara College of Engineering and Technology, Gudur.

Mr.D.Hidayathulla, UG Scholar, Dept of CSE, Audisankara College of Engineering and Technology, Gudur.

Mr.V.Anirudh Reddy, UG Scholar, Dept of CSE, Audisankara College of Engineering and Technology, Gudur.

Ms.S.Kusuma, UG Scholar, Dept of CSE, Audisankara College of Engineering and Technology, Gudur.

Mr.S.Ansar Ahammad, UG Scholar, Dept of CSE, Audisankara College of Engineering and Technology, Gudur.

ABSTRACT:

During data transmission, data can be transmitted in the form of text, image, audio and video, hence securing all kinds of data is most essential in today's era. With the advent of internet technology, the number of unauthorized users to access the data increases.so, the transmission of information through imagesbecomes more. And it also becomes a more reliable form to transmit data. There are a number of algorithms available to solve this problem. One of the efficient methods is to use the AES (Advanced Encryption Standard) algorithm, the most notable and extensively used cryptographic algorithm because itis six times faster than 3- DES and much faster than the RSA algorithm. In this paper we proposed an image encryption and decryption algorithm using AES in which encryption contains a random image and decryption contains the original image. The efficiency of AES is compared using image and text and it is analyzed. The result thus shows that the sharing of information through image is much more reliable and efficient than sharing information as text. Index Terms: AES, Cryptography, Decryption, Encryption, Image.

Keywords: AES, Cryptography, Decryption, Encryption, Image.

1.INTRODUCTION:

EVERY cryptographic process has two aspects: the algorithm and the key used for the encryption and decryption [1]. The use of the keys makes the cryptographic process reliable. There are two types of cryptographic mechanisms: Symmetric key cryptography - uses the same key for encryption and decryption process. Asymmetric key cryptography - uses two different keys for encryption and decryption process. Symmetric key algorithm is efficient, fast and easy to implement as compared to asymmetric key algorithm. The Advanced Encryption Standard (AES) was published. AES is a subset of the Rijndael block cipher developed by two Belgian cryptographers, . AES isa symmetric block cipher and it is believed to be the standardprocess, So, it replaces the DES algorithm in most applications[1]. When compared to other symmetric and public key ciphers, the AES symmetric cipher is found to be complex. Images are sent over an insecure transmission channel from different sources, some image data contains secret data, some images itself are highly confidential hence, securing them from any attack is essentially required. One way to provide image data security is by using Visual Cryptography. Visual cryptography is a technique in which visual information is enciphered in such a way that no one able to identify the image during transmission.

2.PROPOSED SYSTEM:

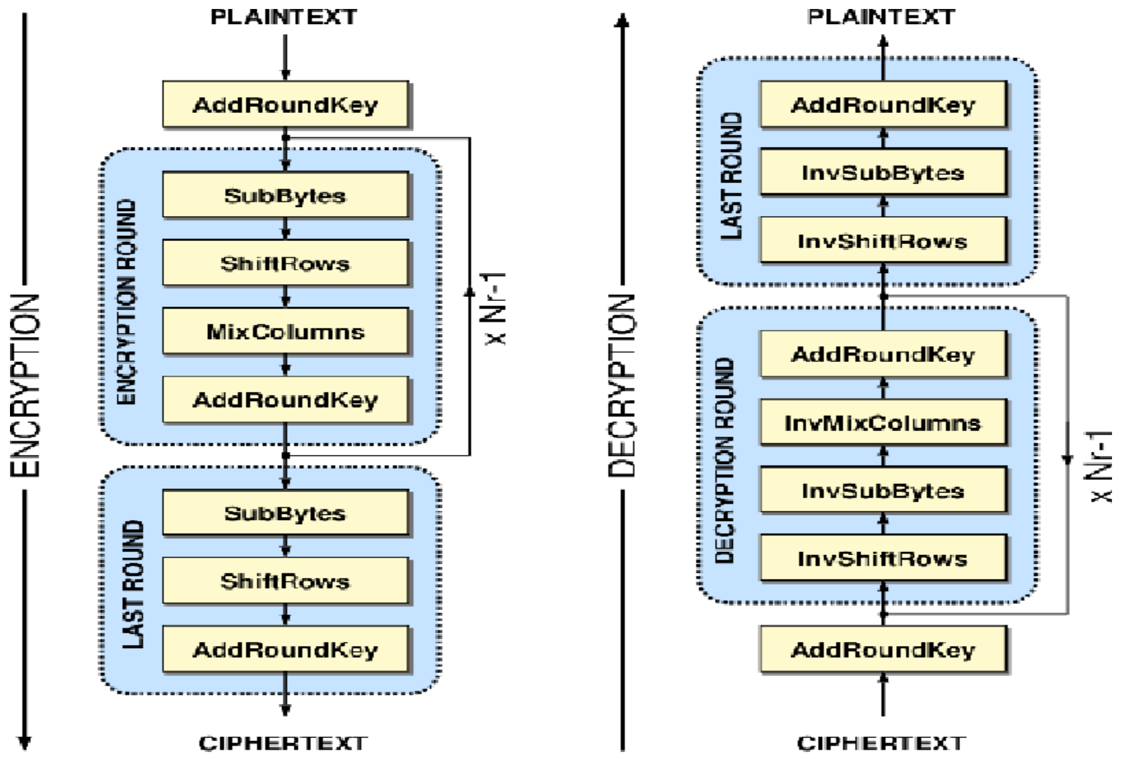
AES is a symmetric key encryption technique the secret key is known to both the sender and the receiver it is an iterative rather than Feistel cipher. It is base on substitution–permutation network. The design of AES algorithm supports the use one of any three key sizes (Nr). AES-128, AES-196 and AES-256 use 128 bit (16 bytes, 4 words), 196 bit (24 bytes, 6 words) and 256 bit (32 bytes, 8 words) key sizes respectively. It comprises of a sequence of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations) in dedicated hardware AES allows even faster execution as the round transformation is parallel by design.

3.LITERARTURE SURVEY:

The Paper is organized into seven sections. Section I gives the introduction of Image data security, visual cryptography and threats related to Image data. In Section II related work done on Image security and visual cryptography is discussed. Next section introduces and explains the proposed system. We have shown process flow, to explain our algorithm in more detailed and expressive manner. At last, we concluded our paper followed by its future scope.

3.1 BLOCK DIAGRAM

The below Figure shows the Block diagram of the proposed system which has been



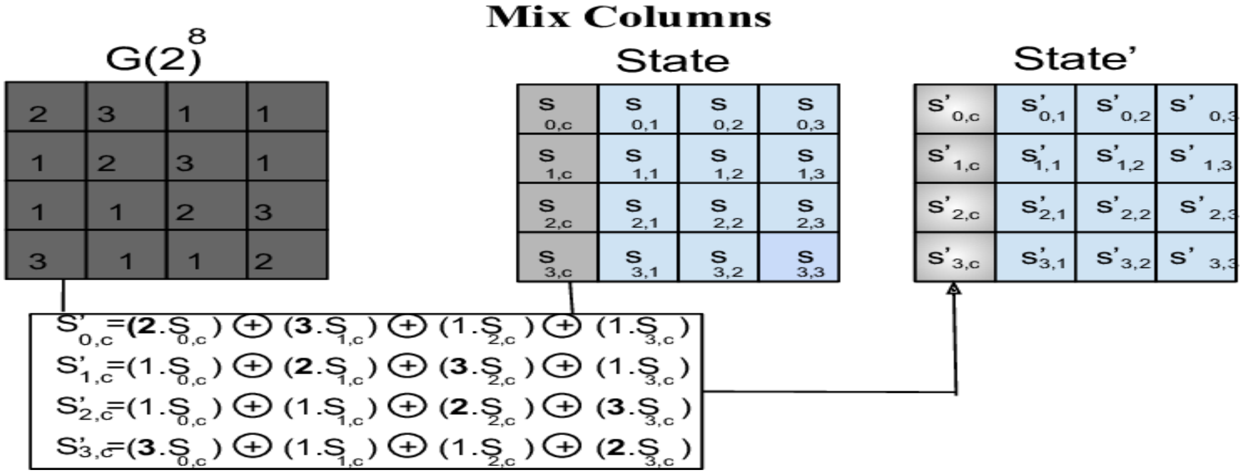
Hardware requirements:

- Synchronous clock system
- Asynchronous clock subsystem
- Image encryption subsystem
- AES Algorithm 128-bit

3.2 AES - Encryption and Decryption Specification:

AES is called AES-128, AES-192 and AES-256. This classification depends on the different key sizes used for cryptographic processes. Those different key sizes are used to increase the security level. As the key size increases the security level increases. Hence, key size is directly proportional to the security level. The input for the AES process is a single block of 128 bits. The processing is carried out in several rounds where it depends on the key length: 16 byte key consists of 10 rounds, 24byte key2 rounds, and 32 byte key consists of 14 rounds. Thefirst round of encryption process consists of four distinct transformation functions: Substitution Bytes ShiftRows MixColumns AddRoundKey The final round consists of only three transformations ignoring MixColumns. The encryption and decryption consists of four transformations . Inverse Substitution Bytes Inverse ShiftRows Inverse MixColumns AddRound.

Mix Columns



$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

$$\begin{bmatrix} s_{0,c} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,c} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,c} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,c} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} \qquad \begin{bmatrix} s'_{0,c} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,c} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,c} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,c} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix}$$

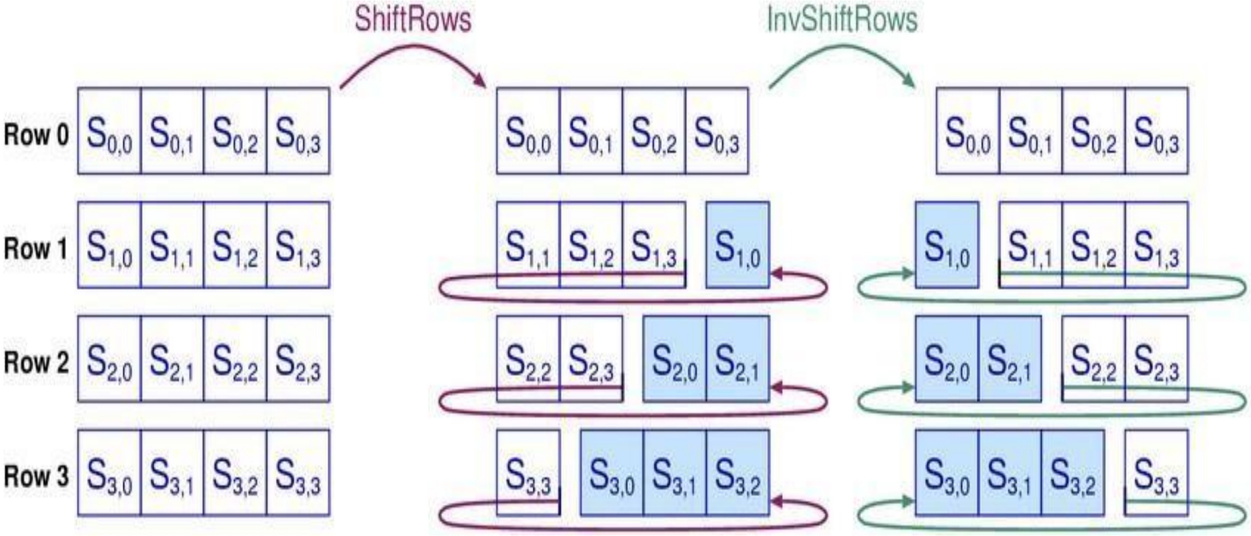
$$S'_{0,c}=(\mathbf{2}.S_{0,c}) \oplus (\mathbf{3}.S_{1,c}) \oplus (1.S_{2,c}) \oplus (1.S_{3,c})$$
$$S'_{1,c}=(1.S_{0,c}) \oplus (\mathbf{2}.S_{1,c}) \oplus (\mathbf{3}.S_{2,c}) \oplus (1.S_{3,c})$$
$$S'_{2,c}=(1.S_{0,c}) \oplus (1.S_{1,c}) \oplus (\mathbf{2}.S_{2,c}) \oplus (\mathbf{3}.S_{3,c})$$
$$S'_{3,c}=(\mathbf{3}.S_{0,c}) \oplus (1.S_{1,c}) \oplus (1.S_{2,c}) \oplus (\mathbf{2}.S_{3,c})$$

Shift Rows:

In shift rows transformation, the bytes in the last 3 rows will be shifted cyclically over the number of bytes present.

- The first row will remain the same.
- The second row will get shifted to the left by one position.
- The third row will get shifted to the left by two positions.
- The fourth row will be shifted to the left by three positions.

The resulting matrix consists of the same 16 bytes but shifts with one another.



AES – DECRYPTION PROCESS

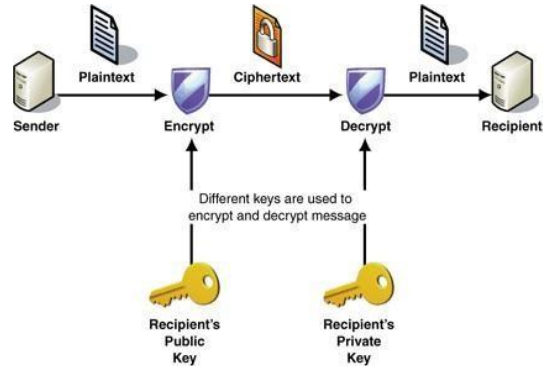
Inverse Substitution Bytes:

Inverse Substitution Bytes is the inverse of the substitution byte transformation. This is performed through an inverse S-box [6,7]. This is obtained by applying inverse of substitution bytes and by computing the multiplicative inverse of Galois Field.

Inverse ShiftRows:

Inverse ShiftRows is the inverse of ShiftRows transformation. It carries out circular shifts in reverse direction for each last 3 rows and for the 2nd row, it performs a one-byte circular shift to the right and it continues the process till (n-3)rd row.

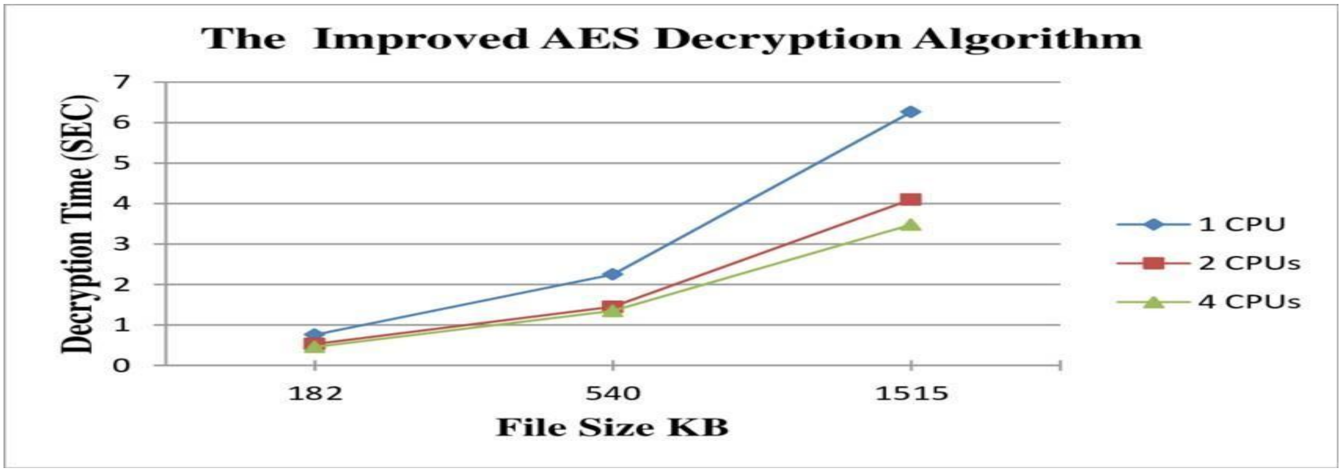
Encryption and Decryption System process:



ANALYSIS:

Text-Time Complexity**:**

The time complexity of encryption and decryption for text has been calculated using AES algorithm and the following results are obtained.



It shows the time complexity of text for encryption and decryption. The result conveys that —as the size increases the encryption time increases and the decryption time also increases.

4.CONCLUSION:

The proposed work makes use of the AES algorithm to encrypt and decrypt the image and text. It makes use of a 128 bit key for encryption which makes AES secure and faster than DES.As the key size is larger, it helps to overcome several attacks such as brute force attack and man in the middle attack. In our proposed system, the encryption image doesn't remain the same. The encryption image is chosen at random.So, it is difficult for intruders to differentiate the encrypted image and the original image. So, the AES algorithm is most suited for image encryption in real time applications. As a future work, we are planning for a different encryption key in each round to perform encryption. The paper proposes a secure mechanism for image data security. The mechanism provides simple and strong method using two level AES, LSB as feature extraction, random number and key generation and encryption. Hence, security blend of these methods applied, increases security and confidentiality of the proposed system and hence it can be used in applications where sensitive image data needs to be transmitted or shared.

Future Work:

The research paper proposes a system that could be used for effective image data encryption and key generation in diversified application areas, where sensitive and confidential data needs to be transmitted along with the image. The next step in this direction will be system implementation, calculating time and space complexity for the same using some experimental data and then comparing it with existing algorithms and schemes for its efficiency, accuracy, and reliability.

References:

[1]. William Stallings, —Cryptography and network Security:principles and practice‖; Pearson Publication, london, pp. 148-183, 2011.

[2]. Mohammad Amjad, —Security Enhancement of IPV6 Using Advance Encryption Standard and Diffie Hellman‖, InternationalJournal of Scientific Research in Network Security andCommunication, Vol.5, Issue.3, pp.182-187, 2017 .

[3]. Roshni Padate, Aamna Patel, ―Image Encryption and Decryption Using AES Algorithm‖, International Journal of Electronics and Communication Engineering & Technology (IJECET), Vol.6, Issue.3, pp.23-29, 2015.

[4]. Priya Deshmukh, ―An Image Encryption and Decryption Using AES Algorithm‖, International Journal of Scientific & Engineering Research(IJSER), Vol.7, Issue.2, pp.210-213, 2016.

[5]. M. D. Randeri1, S. D. Degadwala, A. Mahajan, ―A Study on Image Encryption Using Key Matrix Generation from Biometric Mixed Fingerprint Image for Two Level Security‖, International Journal of Scientific Research in Computer Science, Engineering and Information Technology(IJSRCSEIT), Vol.2, Issue.6, pp.486-490, 2017.

[6]. Guang-liang Guo, Quan Qian, Rui Zhang, ―Different Implementations of AES Cryptographic Algorithm‖, In the Proceedings of the 2015 IEEE International Conference on High Performance Computing and Communications (HPCC 2015), New York, USA, pp.1848-1853, 2015.

Author Profiles

Dr.M.Rajaiah, Currently working as an Dean Academics & HOD in the department of CSE at ASCET (Autonomous), Gudur, Tirupathi(DT).He has published more than 35 papers in Web of Science,Scopus,UGC Journals.

Mr.Syed Akthar Basha, Currently working as an Associate professer in the department of CSE at ASCET Autonomous),Gudur, Tirupati(DT).

Mr.D.Hidayathulla, B.Tech student in the department of CSE at Audisankara College of Engineering and Technology, Gudur. He has pursuing in computer science and engineering.

Mr.V.Anirudh Reddy,B.Tech student in the department of CSE at Audisankara College of Engineering and Technology, Gudur. He has pursuing in computer science and engineering.

Ms.S.Kusuma,B.Tech student in the department of CSE at Audisankara College of Engineering and Technology, Gudur. She has pursuing in computer science and engineering.

Mr.S.Ansar Ahammad,B.Tech student in the department of CSE at Audisankara College of Engineering and Technology, Gudur. He has pursuing in computer science and engineering.