International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 11 Nov 2023, pp: 229-241 www.ijaem.net ISSN: 2395-5252

Digital Image Encryption Using Various Cryptographic Algorithms *Note: Sub-titles are not captured in Xplore and should not be used

Uha Priya Sureddy, Akula Vishal Mythreya, Sola Akhil, Shivani Ch, Gajula Raghu Ram, Savaram Mythreya

Department of Computer Science and Engineering, Cyber Security and Block Chain Technology, K L Deemed To Be University, Vaddeswaram, Guntur, 522302, India
Department of Computer Science and Engineering, Cyber Security and Block Chain Technology, K L Deemed To Be University, Vaddeswaram, Guntur, 522302, India
Department of Computer Science and Engineering, Cyber Security and Block Chain Technology, K L Deemed To Be University, Vaddeswaram, Guntur, 522302, India
Department of Computer Science and Engineering, Cyber Security and Block Chain Technology, K L Deemed To Be University, Vaddeswaram, Guntur, 522302, India
Department of Computer Science and Engineering, Cyber Security and Block Chain Technology, K L Deemed To Be University, Vaddeswaram, Guntur, 522302, India
Department of Computer Science and Engineering, K L Deemed To Be University, Vaddeswaram, Guntur, 522302, India

Date of Submission: 15-11-2023 Date of Acceptance: 25-11-2023

ABSTRACT—The rapid expansion of digital data exchange for storage and transmission has made security information the main source of concern. It is crucial to safeguard private image data from hackers given the increasing expansion of the use of photos in numerous fields. The need for image protection is now essential. Private information must now be protected at all costs. The preservation of data and personal information has been studied and developed using a variety of ways. Image encryption is employed to shield sensitive data from unauthorized users. Encryption is the most widely used technology for concealing data from unauthorized parties. To improve the performance of picture encryption, the Advanced Encryption Standard (AES) is being used. AES uses a keystream generator. Blocks are 128 bits in size, and keys are either 192 or 256 bits in size, depending on the design, which uses an iterative approach. For a 256-bit key, the round numbers are 14, 10, and 12, respectively, while for a key of that size, they are 14. The complexity and security of cryptography algorithms both rise with the use of secret keys. This paper presents a method for encrypting images with AES, then decrypting them with AES to recover the original images. The study in the paper demonstrates how a system could be utilized for reliable image data encryption and keygeneration of differenttypesof platforms such that integrity of sensitive data and secret data should be maintained.

Keywords— Cryptography, Encryption Advanced Encryption Standard (AES), Security, Digital Image, Image Encryption, Crypt Tool.

I. INTRODUCTION

A. Need of the study

Image security is critical in today's image communication systems. Now-a-days it has become very hard to user for protecting the sensitive data. .Since it has become very difficult to identify unauthorized users . Many academics have proposed approaches for securing picture transmission. Present days digital communications consisting internet communication, military imaging systems and healthcare, and multimedia systems, require high integrity for securing the digital picture. Image encryption algorithms are important to defend photographs from such attacks, given the fast spread of multimedia technology such as the internet and smart phones. This image-hiding approach makes use of the Advanced Encryption Standard (AES). Such encryption solutions can help against intrusion threats.

B. Problem Definition

In literature, a variety of encryption strategies have been put forth, but the most popular option for securing huge multimedia files is to use traditional encryption algorithms. The transmission of images is not a good fit for private key mass encryption methods like Triple DES. Because of the complexity of their underlying structure, they are slow to execute and cannot be used in real time.

Because of picture characteristics such as huge storage capacity, huge redundancy and strong correspondencepixel to pixel, DES cannot be performed to protect images. If they strive for efficiency while maintaining the security level, picture encryption algorithms can become a crucial component in the delivery of images.

C. Scope of the study

An original picture will be converted into a digital image via the process of "image processing," which will then utilize the digital image to analyze and extract useable information. The input for this process is a picture and output is same images as original image but with different attributes. Because of recent developments in communication technology, digital picture transmission has sparked massive interest. Illegal storage access is also growing easier as computer processors become more powerful.

The scientific community has taken a keen interest in image transmission because encryption involves converting picture into a cipher text and in order to retrieve the information we decrypt the encrypted picture such that it gives the encrypted message. People's privacy is becoming increasingly harder to defend. Furthermore, data or image encryption or decryption is critical for preventing unwanted readers from acquiring sensitive information. This paper presents an encrypted approach for safe picture transmission via network channel.

D. Aim

Many organizations appear to be engaged in criminal activity. It appears that the culprits carried out their acts using PCs and unauthorized wireless networks, accessing unprotected files and documents without encryption. As a result, the focus of this study will be on developing picture encoding and decoding software. Security has emerged as a critical issue. It is recognized that photos may be safely conveyed via encryption. Any picture encryption method's purpose is to generate high-quality concealed images to secure data.

II. LITERATURE SURVEY

A. Cryptography

The use and study of secured communication technologies ofthe face of adverse action is known as cryptography. Cryptography, in its broadest sense, is the development and application of processes that make it impossible for members of the public or unauthorized individuals to read secret messages. Modern encryption prioritizes data integrity, privacy, and authentication.
Electrical engineering, computer science, communication science, and physics all intersected in the creation of contemporary cryptography.
Cryptography is utilized in a wide range of applications, including e-commerce, smart payment cards, virtual currencies, and military applications.

1) Plain Text:

Plain text is the format used for all communications that take place in the language that we frequently use—that is, human communication. Everyone who has access to it from a UN agency, including the sender, recipient, and related parties, understands the message.

2) Cipher Text:

A security key is a secret code or communication. If the comprehensible text is constructed using a proper model, the final message is referred to as "ciphertext."

3) Key:

The key is an essential component in pretending to write in secret and use cryptography. The secret code employed in cryptography and secret writing is what makes the process secure.

B. Encryption

The data may be encrypted so that it is incomprehensible to anybody other than those authorized to receive it. It is the technical term for the process of transforming ordinary human-readable text into encrypted or unrecognizable text. To put it simply, encryption transforms readable data into erratic information. Encryption requires a cryptographic key, which is a group of numbers agreed on both the sender as well as the receiver of the protected communication.

Even thoughthe encrypted data appears to be arbitrary, the encryption process is scientific and consistent, allowing one person to receive the encrypted data and have the appropriate keys to decode that data as well as restore the original plain text. It helps to secure connections between client and server applications while also safeguarding personal information.

C. Decryption

Decryption is a method of transforming encrypted data back to its original state. We also convert the encrypted image back to its initial form in the process of image decryption.

D. Purpose of Cryptography

There are various purposes, some of them are:

1) Privacy:

Apart from the designated receiver or the legitimate data owner, messages and information at rest cannot be read. By doing this, sensitive data is protected from cybercriminals, the web service companies,advertising networks, and occasionally governments.

2) Authentication:

The owner of a website's ownership of the individual key specified in the TLS certificate of website can be verified and other information, using public key encryption. Due to this, website visitors can be certain they are connecting to the legitimate website.

3) Integrity:

Aside from preventing unlawful actions like on-path attacks, encryption also helps. Encryption, together with other integrity safeguards, ensures that data sent over the Internet hasn't been changed in transit and that what the recipient receives is accurate.

4) Security:

Encryption aids in the prevention of data misuse, whether the data is in transit or at rest. If the hard disc is correctly encrypted, the information on it will stay safe even if the device is lost or stolen. Similarly, encrypted communications allow interlocutors to transmit confidential information without disclosing it.

5) Regulations:

All these issues necessitate that organizations that handle user data retain that data encrypted to comply with various industry and government laws. HIPAA, PCI-DSS, and GDPR are a few instances of legal and compliance mandates that necessitate encryption.

E. Types of Cryptography

Secret Key Cryptography and Asymmetric Key Cryptography are the two main forms of cryptography.

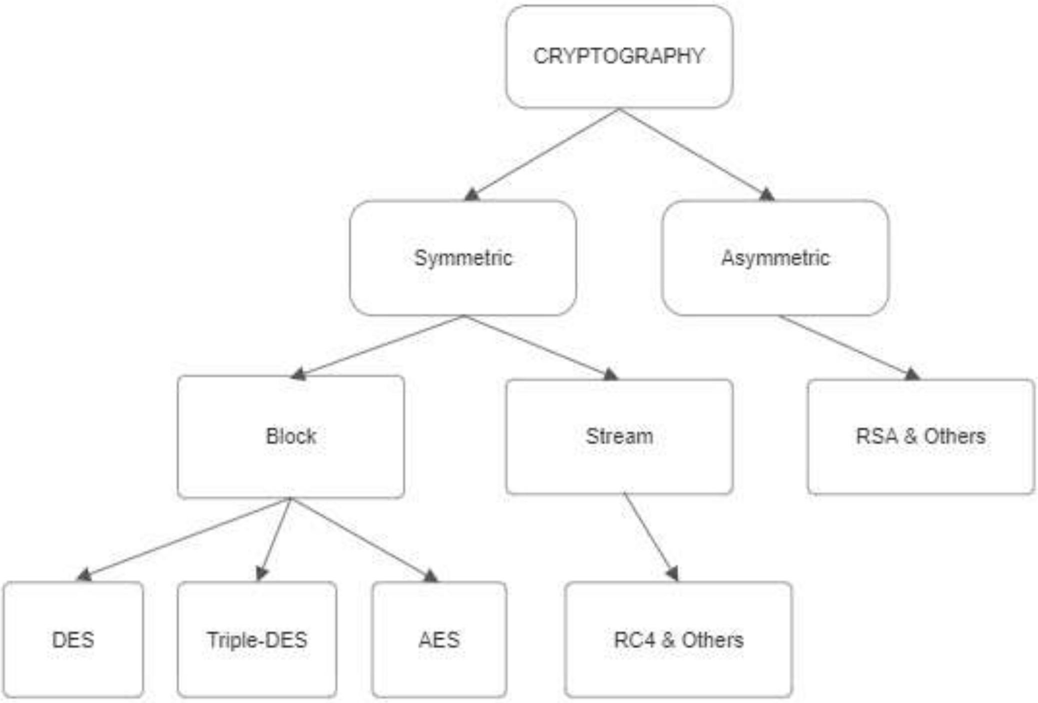


Fig: -1 Classification of Cryptography

1) Symmetric Key Cryptography:

Symmetric encryption is a type of encryption in which a single key (secret key) is employed in both encryption and decryption. of data on computers. The parties utilizing symmetric encryption must exchange keys to use the key in the decryption procedure. Besides, asymmetric encryption, which employs a pair of keys (a public key and a private key) to encrypt and decode a message, this encryption approach just needs one key.

The data is encrypted using symmetric encryption methods and translated into a cryptic format that can only be read by someone with the secret key. When theintendedrecipient, who also holds the key, receives the message, the algorithm will reverse its operation, restoring the message back to its initial, intelligible state. Symmetric encryption methods are useful.

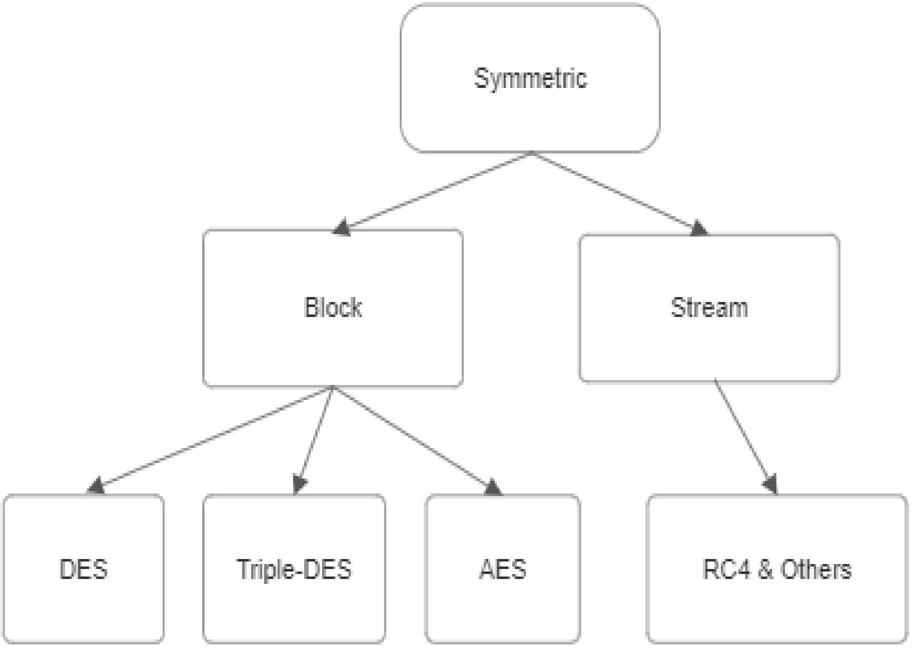


Fig: -2 Types of Symmetric Cryptography

1.1) Block Ciphers:

The system holds data in memory while waiting for the entire block to be encrypted.1.1.1) Data encryption standard (DES) was vulnerable to extremely powerful attacks, DES's position in the cryptographic community was said to have decreased slightly. Because DES is a block cipher, it encrypts input into block of 64-bits. The resulting 64 bits of plain text are used as input to DES, which then produces 64 bits of cipher text. For encryption and decryption, the same key and algorithm are applied with some minor changes. It has a key of 56 bits. DES uses a 56-bit key as mentioned before. There are 64 bits in the initial key. However, the key is reduced to 56 bits by dropping one of the eight bits before the DES procedure begins. That is, bits in place of 8, 16, 24, 32, 40, 48, 56 and 64 are not used. Therefore, from the unique 64-bit key, a 56-bit key is created by discarding every eighth bit. Substitution and transposition are the two main components of encryption that DES relies on. Cycle is the term used to describe each of the 16 stages that make up DES. Substitutions and transpositions are performed each round. Now let's talk about the DES process in general.

1. First, a First Permutation function is given for plain text of 64-bit for control.
2. It uses plain text for the initial permutation.
3. Following that, the First permutation results in the creation of Left Plain Text and Right Plain Text, two halves of the permuted block.
4. Sixteen rounds of encryption are now performed for each LPT and RPT.
5. Last Permutation is then carried out on the combined block once LPT and RPT are reunited.

6. This procedure generates ciphertext with a 64-bit size.

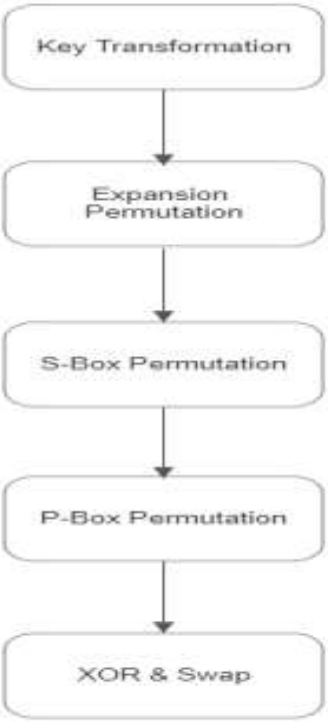


Fig: -3 Details of One Round in DES

1.1.1) Triple-Data Encryption Standard(3-DES)

After 1990, DES users became dissatisfied with the speed with which lengthy keys could be found. Customers, however, are hesitant to convert to DES because upgrading widely used encryption algorithms that are part of a sophisticated security architecture is costly and time-consuming.

Don't completely give up on DES, but rather changing how it is used, was the realistic approach. As a result, Triple DES also referred to as 3DES, had its schemes updated. Also known as 3-key Triple DES (3TDES) and 2-key Triple DES (2TDES), these two Triple DES variations exist.

A 3TDES key L, which consists of three separate DES keys L1, L2, and L3, must first be generated and distributed before employing 3TDES. In other words, the true 3TDES key is 3*56 = 168 bits long.

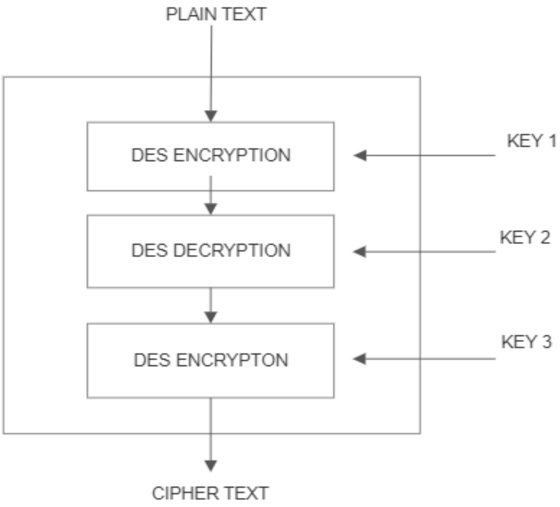


Fig: -4 3DES Algorithm

Following is a description of the encryption-decryption process:

1. Utilizing key L1 and a single DES algorithm for encrypting plain text.
2. Use single DES and key L2 for decrypting cipher text of step 1.
3. In the end, use key L3 and single DES to encrypt the output of step 2's second step.
4. The ciphertext is what step 3 produces.
5. The reverse process of decrypting a ciphertext.
6. Using L3, L2, and L1 in that order, the user first decrypts before using L3.

L1, L2, and L3 must not be the different value in order to utilize the 3TDES execution for a DES. Because Triple DES is built as an encryption-decryption-encryption method, this is conceivable. As a result, DES is always compatible.

L1 is utilized instead of L3 in 2TDES, as it is in 3TDES. The blocks of plaintext encrypted using L1, decode them with key L2, and then encrypt them again with key L1. The obtained key length for 2TDES is 112 bits.

Despite being significantly slower than single DES, triple DES systems are generally moreprotected than single DES.

1.1.2) Advanced Encryption Standard(AES)

Joan Daemen and Vincent Rijmen, two Belgian cryptographers, devised the Rijndael block cypher, which is nearly equivalent to the AES cypher. In the AES algorithm, a fixed secret may be used for encryption and decryption of data, indicating that it is a secret key algorithm. The length of the key can influence the number of internal rotations of the digit. Ten rounds are necessary for a 128-bit secret. Unlike its predecessor, DES, AES does not employ the Feistel network. The Feistel network does not encrypt full blocks every round. In DES, 32 bits are encrypted in a particular round. AES is used to encrypt all 128 bits in a single repetition.

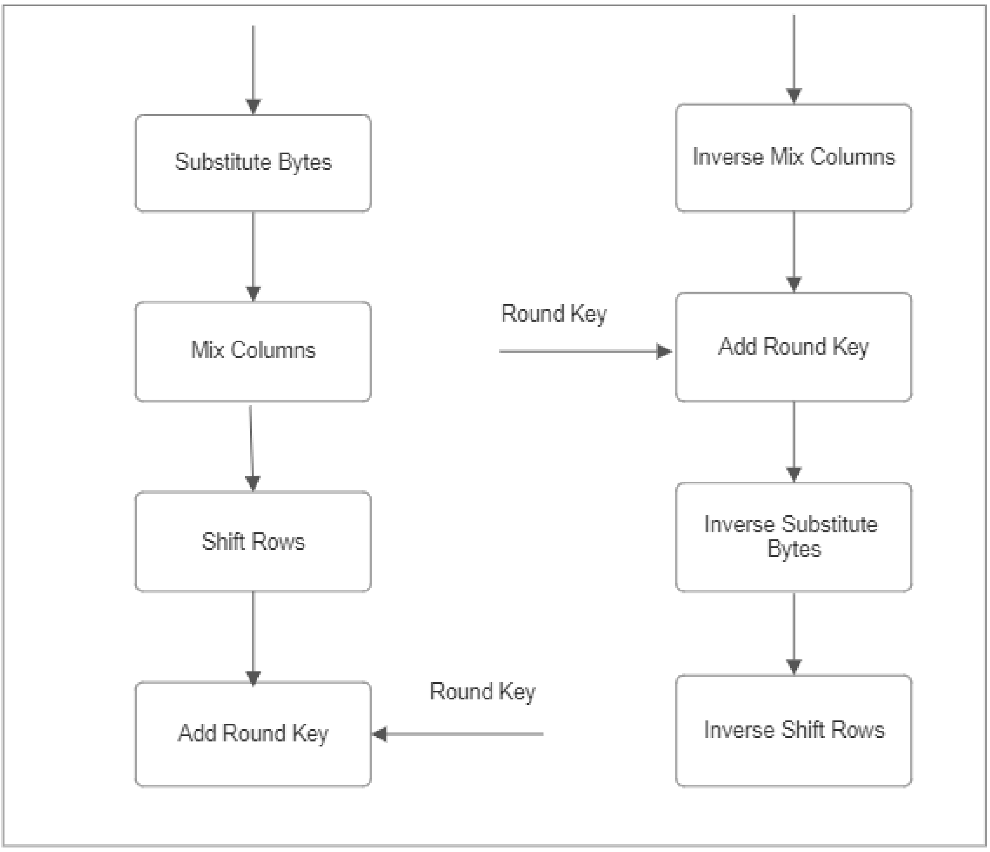


Fig: -5 One Round Encryption and Decryption in AES

1. Decryption:Inverse functions like InvSubBytes, InvShiftRows, and InvMixColumns are used to reverse all the steps made during secret writing during decryption. Decryption Round after the Encryption Round It takes four stages to process each round.
2. Substitute Computer Storage Unit: a non-linear replacement phase where each computer memory

unit is swapped out with a different computer storage unit utilizing a hunt table.

3. Shift Rows: A step that transpose the state's rows are each cycled through a certain type of steps throughout this step.
4. Mix Column: Four bytes from each column are combined in the state's columns during mixture operations.
5. Add Spherical Key: A round key employing bitwise XOR is used for each computer storage unit in the state.

1.1) Stream Ciphers:

Data is encrypted when transferred rather than retained in system memory.

1.2.1) Rivest Cipher (RC4)

Ron Rivest developed Rivest Cypher 4, or RC4, for RSA Security in 1987. Stream cyphers are exactly what they sound like. A stream cypher is used to process data byte by byte. There are two major sizes available: 64-bit and 128-bit.

This method employs a variable-length key (K) that the user selects from 1 to 256 bytes (8 to 2048 bits), commonly 5 to 16 bytes. The 256-byte key is generated using the master key.

Working of RC4 as follows-
Encryption:

1. A secret key is entered, along with a plain text file.
2. The key stream using the KSA and PRGA algorithms.
3. The encrypted text is created by performing a byte-by-byte XOR operation on this keystream and the plain text.
4. Once the intended recipient has decrypted the text, they will receive the original plain text. The encrypted text is then sent to the intended recipient.

Decryption:
The identical byte-wise X-OR technique on the Ciphertext is used for decryption.

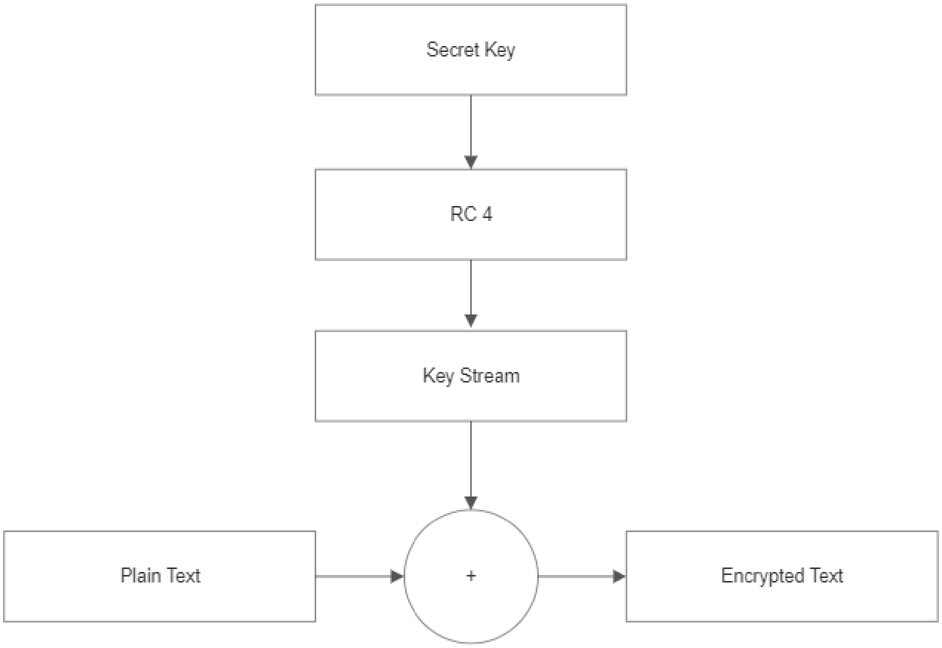


Fig: -6 RC4 Block Diagram

2) Asymmetric Key Cryptography:

Asymmetric key cryptography, often known as public key cryptography, employs two separate but mathematically linked keys: a open key and a secret key. Asymmetric key cryptography, as opposed to symmetric key cryptography,it encrypts and decrypts using the same key, uses a public key for encryption and a private key for decryption.

III. COMPARISON

Algorithm	Key Size (Bits)	Block Size(Bits)	Average Encryption Time
DES	56	64	663.1
3DES	112 OR168	128	742.31
AES	256	64	542.38

IV. PROPOSED ALGORITHM

Hence in this paper, by applying the cryptography method AES, we attempt to provide a higher level of security for data that is transported between different locations. Encryption and decryption are two different processes that change plain text into cipher text and cipher text back into plain text. When encrypting or decrypting text or image data in this application, we try to use the AES algorithm.

The suggested system has the following benefits, in that order:
1. In this proposed approach, the data is secure.
2. The information is encrypted, preventing all users from having direct access to it.
3. Using the decryption key, only authorized users can unlock the data.
To secure sensitive data, the US government has chosen symmetric block encryption known as Advanced Encryption Standard (AES).

AES is employed in both hardware and software.

Globally, sensitive data is encrypted. It is critical for government information security, cyber security, and the safeguarding of electronic data. AES is the most extensively used symmetric key encryption method today.

1. Features of AES
1.1. According to NIST standards, this algorithm is effective for processing 128-bit blocks and up to the sizeof 256-bit keys. When selecting the next AES algorithm, the following factors are also taken into account:
1.2. Security: Competing algorithms must be resistant to assaults in order to be comparable to other metrics presented. Everyone agrees that security strength will be the most essential element of the competition.
1.3. Cost: Potential algorithms will be examined for compiling time and memory allocation before being provided globally.
2. Implementation:

This algorithm can be implemented on every software.

3. Attacks on AES- Encryption

Studies into AES encryption threats have been ongoing. On reduced-round versions of AES, several researchers have published attacks.

AES encryption may be vulnerable to the following attacks, which researchers have discovered: They found what might be a related-key assault in 2009.

By analyzing a cipher's operation while employing several keys, this cryptanalysis sought to break it. Only AES systems that are configured improperly undergone attacks.

In 2009, a known key attack against AES-128 occurred. A known key is used to establish the encryption structure.

Additionally, utilizing randomization techniques can aid in removing any connections between data protected by the cypher and any leaked data that could be gathered through a side-channel attack.

4. Working of AES Algorithm

Three-block ciphers come with AES:

AES-128 and AES-192 both use key lengths of 128 bits and 192 bits to encrypt and decrypt blocks of messages, respectively.

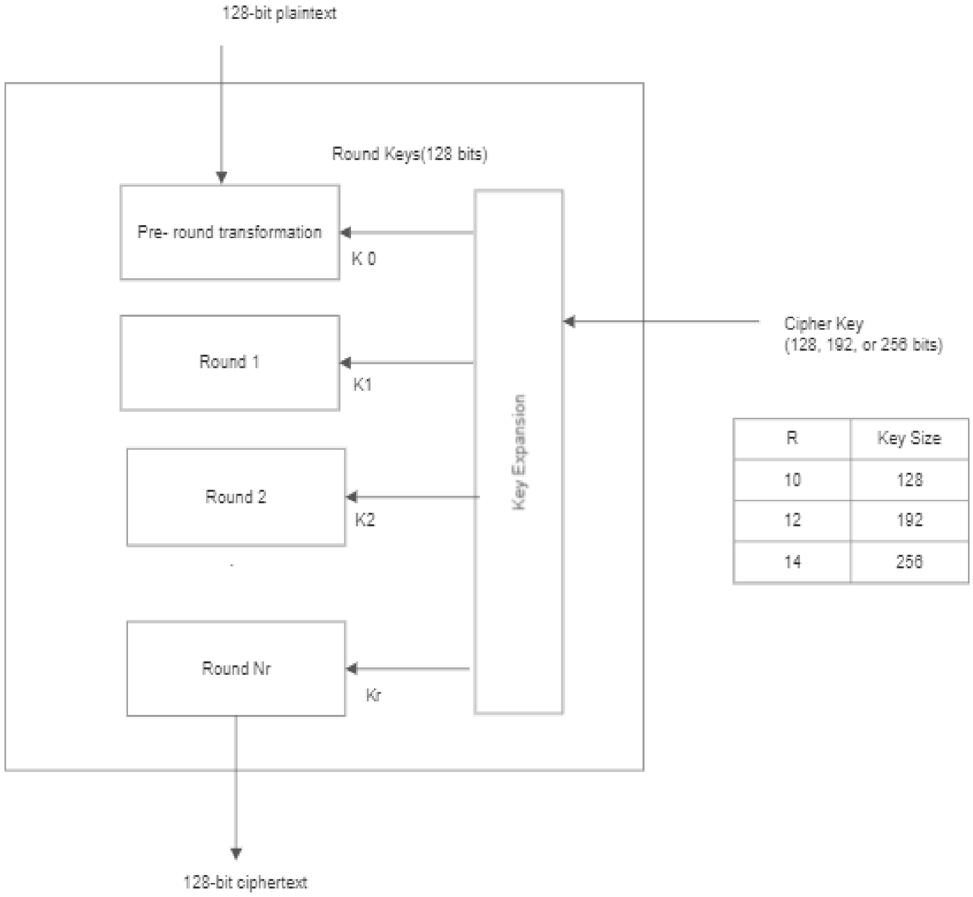
Each cipher encrypts and decrypts 128-bit blocks of data using cryptographic keys of 128, 192, and 256 bits, respectively.

The secret key must be known and utilized by both the sender and the receiver. There are 10, 12, and 14 rounds for a 128-bit key, and 12 cycles for a 192-bit key. The input plaintext is processed through numerous stages in one pass to create the final ciphertext output, including substitution, displacement, and disturbance.

5. Detailed working of AES Algorithm

A "substitution permutation network" is used to construct it. It is made up of several interrelated processes, some of which require the exchange of specific inputs for specific outputs (substitution), while others entail the movement of bits (permutation). What's notable is that AES does all calculations in bytes rather than bits. As a result, AES considers 128 bits to be 16 bytes. 16 bytes. These 16 bytes are organized in the matrix. Each round, the 128-bit round keys created all AES key are unique.

In the figure that follows, the AES structure schematic is provided.



R	Key Size
10	128
12	192
14	256

Fig: -7 Working of AES

6. Encryption Process

The first round, the middle rounds, and the final round can be considered the three stages of the AES encryption phase.

1. The first round is AddRoundKey.
2. The Main Rounds are SubBytes, Shifted Rows, Mixed Columns, and AddRoundKey
3. The last Round are SubBytes, ShiftRows, and AddRoundKey

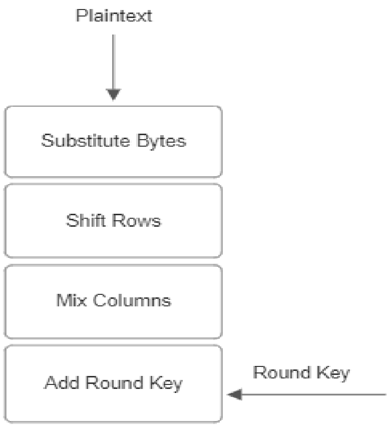


Fig: -8 Round 1 in AES

Round keys' creation:

Calculating all the round keys from the key requires the Key Schedule algorithm. As a result, the initial key is used to build several round keys that are going to be applied in the relevant round of encryption.

The Substitution of Bytes:

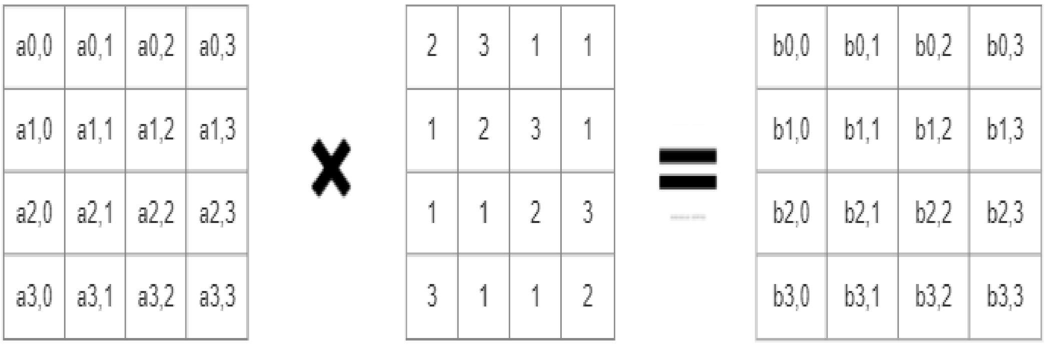
16 bytes input is replaced by table S box. Four rows and four columns make up the resulting matrix. The substitution is put into effect in this stage. Each byte is changed with a different byte in this stage. This substitution is done such that no byte can change independently and with another byte that complements the present byte. This phase produces the same 16-byte (4 x 4) matrix as before. The permutation is carried out in the next two steps.

Shift rows:

Each of the matrix's four rows has a left shift. Any items that "drop" will be again inserted on the row's side of right.
The top row has not been shifted.

Columns of Mix:

Now, a specific mathematical function is performed to transform every four-byte column. This function outputs four entirely new bytes, which replace the old column, and accepts as input the four bytes of one column. A second new matrix with 16 more bytes is the outcome. This stage is not carried out in the final round, it should be noted.



$$\begin{bmatrix} a0,0 & a0,1 & a0,2 & a0,3 \\ a1,0 & a1,1 & a1,2 & a1,3 \\ a2,0 & a2,1 & a2,2 & a2,3 \\ a3,0 & a3,1 & a3,2 & a3,3 \end{bmatrix} \times \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} = \begin{bmatrix} b0,0 & b0,1 & b0,2 & b0,3 \\ b1,0 & b1,1 & b1,2 & b1,3 \\ b2,0 & b2,1 & b2,2 & b2,3 \\ b3,0 & b3,1 & b3,2 & b3,3 \end{bmatrix}$$

Fig: -9 Mix Columns

Add round key:

The round key's 128 bits are performed XOR with the matrix's 16 bytes, which are now regarded as 128 bits. The code text will be produced when it is the last round. If not, the 128 bits that are produced are converted into 16 bytes, and we start a new round in the same way.

V. RESULTS AND DISCUSSION

It has been well explored how cryptography works. Through reading various online resources, we became knowledgeable about cryptography. The topic of encryption was studied, along with the need for data encryption and different encryption techniques. Symmetric key algorithm characteristics and fundamental concepts were researched using a variety of resources. High security is achieved by using 256-bit cipher keys because they are challenging to crack. Consequently, it may be possible to transmit images securely.

The study of the Advanced Encryption Standard algorithm(AES) usedfor secure and effective image encryption is the aim of this paper. AES algorithm techniques have been used to encrypt images, which is important. Since the encryption algorithm used in hardware is also used in critical communication devices, research into the AES algorithm is also expected to play an important role in mission-critical applications. There are excellent reasons for us to think that using this technology to encrypt images will be very successful in the future.

Visible scene and histogram: Distribution of the histogram for the test one.bmp image

Noting that the histogram has a uniform distribution, the suggested technique is effective in preventing this. The following equation can be used to compute entropy.

$$H(x) = \sum_{i=1}^{K} P(x_i)\, log_2 \frac{1}{P(x_i)} = -\sum_{i=1}^{K} P(x_i)\, log_2\, P(x_i)$$

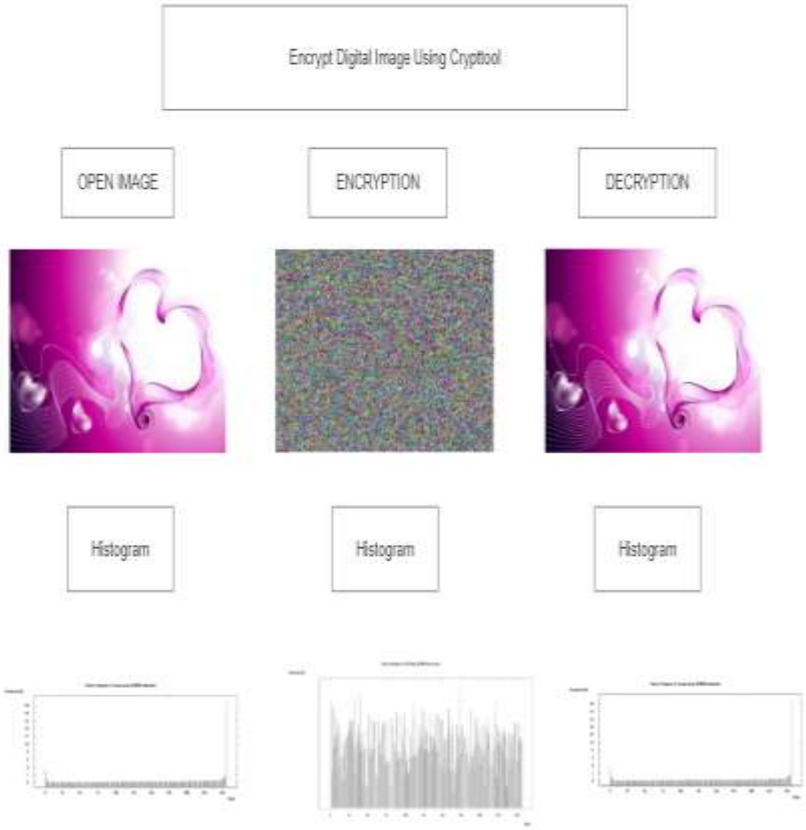


Fig: -10 Digital Image Encryption Using CryptTool

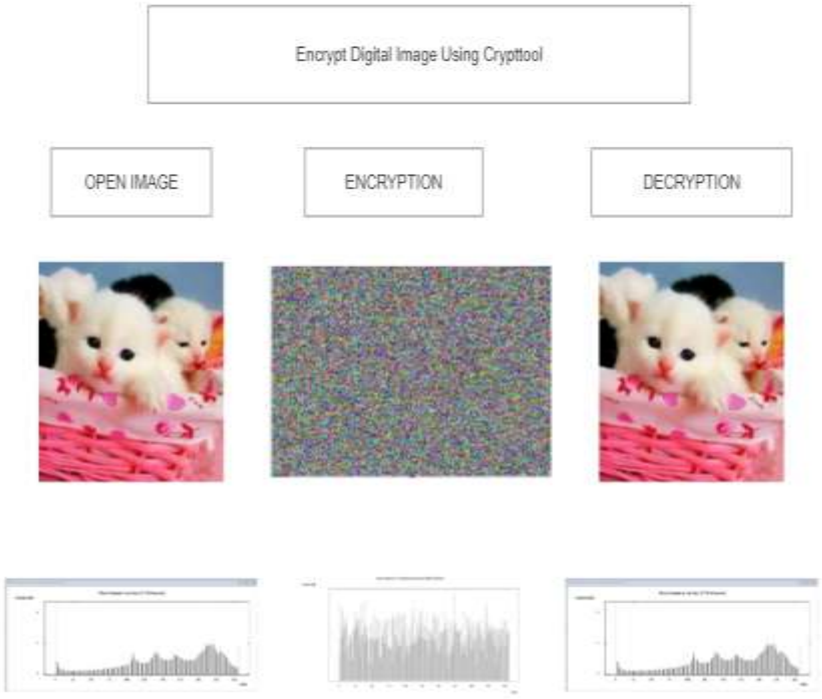


Fig: -11Simulation for Digital Image Encryption

VI. CONCLUSION AND FUTTURE SCOPE

Due to the use of AES for image steganography, this solution offers protection from intrusion attempts and enables faster and more secure encryption and decryption. The storage and transmission of digital photographs using this method are thus secure. The encryption technique outlined in this research will also be evaluated using various input image types with varying image size and AES encryption algorithm keys.

The research presented in the paper demonstrates how a system can be used where important and confidential data must be secured in images.

The installation of the system, followed by an evaluation of its efficacy, accuracy, and dependability, will be the next step in this direction.

In order to achieve the highest encryption speed in a constrained implementation area, we will continue this research in upcoming work in order to generate more secure keys.

We will put into practice a revolutionary approach that utilizesthe AES algorithm to securely encrypt and decryptimages thatare being used for future image communication systems. Future uses include military communication, forensics, intelligent systems, and more.

REFERENCES

[1]. https://www.ijraset.com/research-paper/image-encryption-and-decryption-technique

[2]. Munir, R. (2006). Cryptography. Bandung: Informatika Bandung.

[3]. https://www.researchgate.net/publication/357232938_AES_Image_Encryption

[4]. https://www.iosrjournals.org/

[5]. https://ijcrt.org/papers/IJCRT1813263.pdf

[6]. Sun, . "Cryptography and Conditional Access for Video Transport Systems" , Digital Video Transcoding for Transmission and Storage, 2004.

[7]. Kundankumar Rameshwar Saraf, Vishal Prakash Jagtap, Amit Kumar Mishra, “Text and Image Encryption Decryption Using Advanced Encryption Standard”, 2014

[8]. B.Subramanyan, Vivek.M.Chhabria, T.G.Sankar babu , “Image Encryption Based On AES Key Expansion”, 2011

[9]. P.Karthigaikumar, Soumiya Rasheed “Simulation of Image Encryption using AES Algorithm”, 2011.

[10]. Jose´ J. Amador, Robert W. Green, “Symmetric-Key Block Cipher for Image and Text Cryptography”, 2005

[11]. Jui-Cheng Yen and Jim-In Guo, “A New Chaotic Key-Based Design for Image Encryption and Decryption”,2000.

[12]. P. Radhadevi, P. Kalpana , “Secure Image Encryption Using Aes”,2012

[13]. https://nevonprojects.com/image-encryption-using-aes-algorithm/

[14]. R.Gopinath, M.Sowjanya, (2012, October).”Image Encryption for Color Images Using Bit Plane and Edge Map Cryptography Algorithm”, International Journal of Engineering Research and Technology (IJERT) volume-1, issue-8, pp.1-4.

[15]. VedkiranSaini, ParvinderBangar, Harjeet Singh Chauhan, (2014, April).”Study and Literature Survey of Advanced Encryption Algorithm for Wireless Application”, International Journal of Emerging Science and Engineering (IJESE) volume-2, issue-6, pp.33-37.

[16]. Logunleko, Abolore Muhamin. "Enhancement of a Symmetric Based Cryptosystem Using Deoxyribonucleic Acid Sequence and Residue Number System" , Kwara State University (Nigeria), 2023

[17]. https://www.ijraset.com/

[18]. https://www.ijser.org/researchpaper/An-image-encryption-and-decryption-using-AES-algorithm.pdf

[19]. Yoga Palilianto. Design of Encryption Applications And Digital Image Descriptions Using Java-based Rijndael Algorithms SE .2014.

[20]. William Stallings, “Advance Encryption Standard,” in Cryptography and Network Security, 4th Ed., India:PEARSON,pp. 134–165.

[21]. https://iaeme.com/MasterAdmin/Journal_uploads/IJECET/VOLUME_6_ISSUE_1/40120150601004.pdf

[22]. P.Karthigaikumar, Soumiya Rasheed,Simulation of Image Encryption using AES Algorithm,IJCA Special Issue on Computational Science-New Dimensions & Perspectives NCCSE, 2011, 166-172.

[23]. KundankumarRameshwarSaraf, Vishal PrakashJagtap, Amit Kumar Mishra, (2014, May-June).”Text and Image Encryption Decryption Using Advance Encryption Standard”, International Journal of Emerging Trends and Technology in computer science(IJETTCS) volume-3, issue-3, pp.118-126.

[24]. Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani, (2010, March), “New Comparative Study Between DES, 3DES and AES within Nine Factors”, Journal of computing,volume2-,issue-3,pp.152-157

[25]. Journal of cardiovascular Disease Researchs (jcdronline.org)

[26]. https://www.simplilearn.com/data-encryption-methods-article

[27]. https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard

[28]. https://www.scitepress.org/Papers/2018/89055/89055.pdf