iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** XII **Month of publication:** December 2021

DOI: https://doi.org/10.22214/ijraset.2021.39542

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 9 Issue XII Dec 2021- Available at www.ijraset.com

AES Image Encryption (Advanced Encryption Standard)

Paavni Gaur[1], Mr. Ajay Kaushik[2]
[1]*B-Tech: Information Technology*
[2]*Guided by: Assistant Professor- Department of IT Maharaja Agrasen Institute of Technology, Guru Gobind Singh Indraprastha University*

Abstract: An Image Encryption and Decryption Using AES (Advance Encryption Standard) Algorithm is proposed in the project. Due to increasing use of image in various field, it is very important to protect the confidential image data from unauthorized access. The design uses the iterative approach with block size of 128 bit and key size of 128, 192 or 256 bit. The numbers of round for key size of 256 bits is 14 , for 128 bits is 10 and for 192 bits is 12. As secret key increases the security as well as complexity of the cryptography algorithms. In this paper , an algorithm in which the image is an input to AES Encryption to get the encrypted image and then input it to AES Decryption to get the original image is proposed and explained which will further be implemented by me. The paper shows the study in which a system 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.

I. INTRODUCTION

A. Need of the Study

In today's image communication system security of images is essential. It is necessary to protect confidential image data from unauthorized users. To detect and find unauthorized users is a challenging task. Different researchers proposed different techniques for securing image transmission. Today almost all digital services like internet communication, medical and military imaging systems, multimedia system requires reliable security in storage and transmission of digital images. Due to faster growth in multimedia technology, internet and cellphones, there is a need for image encryption techniques in order to hide images from such attacks. In this system we use AES (Advanced Encryption Technique) in order to hide image. Such Encryption Technique helps to avoid intrusion attacks.

B. Problem Definition

Many encryption methods have been proposed in literature, and the most common way to protect large multimedia files is by using conventional encryption techniques, Private key bulk encryption algorithms, such as Triple DES, are not so suitable for transmission of images. Due to complexity of their internal structure, they are not particularly fast in terms of execution speed and cannot be applied for images in the real time scenario Also traditional cryptographic techniques such as DES cannot be applied to images due to intrinsic properties of images such as bulk data capacity, redundancy and high correlation among pixels. Image encryption algorithms can become an integral part of the image delivery process if they aim towards efficiency and at same time preserve the security level.

C. Scope of the Study

Image processing is a mechanism in which an original image will be converted into digital image and after converting in digital form process it to get useful information. It is a type of signal processing in which input is an image and output may be image or characteristics/features associated with that image. .In recent years, the advances in communication technology have seen strong interest in digital image transmission. However, growth of computer processor possessing power and storage illegal access has become easier. Encryption involves applying special mathematical algorithms and keys to transform digital data into cipher code before they are transmitted and decryption involves the application of mathematical algorithms and keys to get back the original data from cipher code, scientific community have seen strong interest in image transmission. Information privacy becomes a challenging issue. In order to protect valuable data or image from undesirable readers, data or image encryption / decryption is essential, furthermore. As such in this paper, a scheme based on encryption has been proposed for secure image transmission over channels.

©IJRASET: All Rights are Reserved

D. Objective of the Study

There appears to be illegal activity taking place at different organization. The suspects are apparently the use of computers and an illegal wireless network by intruders to conduct their activities by access an unsecure file and document without an encrypted password. Therefore this project will deal with the development of encrypting and decryption software for images.

Security is one of the core areas of study in recent days. Encryption of the image is widely known as an effective method for its secure transmission. The objective of any image encryption method is to obtain a top quality hidden image in order to keep information secret.

In this project I will do a thorough research on basics of cryptography, AES algorithm, how AES is implemented, how AES algorithm is modified to be used on images and will at the end of gaining knowledge of cryptography and AES , will implement it to showcase my learnings.

II. LITERATURE REVIEW

A. Cryptography

Cryptography, or cryptology is the practice and study of techniques for secure communication in the presence of adversarial behavior. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages; various aspects in information security such as data confidentiality, data integrity, authentication are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, communication science, and physics.

Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, military etc.

B. Encryption

Encryption is a way of scrambling data so that only authorized parties can understand the information. In technical terms, it is the process of converting human-readable plaintext to incomprehensible text, also known as ciphertext. In simpler terms, encryption takes readable data and alters it so that it appears random. Encryption requires the use of a cryptographic key: a set of mathematical values that both the sender and the recipient of an encrypted message agree on. Although encrypted data appears random, encryption proceeds in a logical, predictable way, allowing a party that receives the encrypted data and possesses the right key to decrypt the data, turning it back into plaintext. Truly secure encryption will use keys complex enough that a third party is highly unlikely to decrypt or break the ciphertext by brute force — in other words, by guessing the key.

C. Types of Encryption

The two main kinds of encryption are symmetric encryption and asymmetric encryption.

In symmetric encryption, there is only one key, and all communicating parties use the same (secret) key for both encryption and decryption. In asymmetric, or public key, encryption, there are two keys: one key is used for encryption, and a different key is used for decryption. The decryption key is kept private (hence the "private key" name), while the encryption key is shared publicly, for anyone to use (hence the "public key" name).

D. Data Encryption Reasons

1) *Privacy:* Encryption ensures that no one can read communications or data at rest except the intended recipient or the rightful data owner. This prevents attackers, ad networks, Internet service providers, and in some cases governments from intercepting and reading sensitive data.
2) *Security:* Encryption helps prevent data breaches, whether the data is in transit or at rest. If a device is lost or stolen and its hard drive is properly encrypted, the data on that device will still be secure. Similarly, encrypted communications enable the communicating parties to exchange sensitive data without leaking the data.
3) *Data integrity:* Encryption also helps prevent malicious behavior such as on-path attacks. When data is transmitted across the Internet, encryption (along with other integrity protections) ensures that what the recipient receives has not been tampered with on the way.
4) *Authentication:* Public key encryption, among other things, can be used to establish that a website's owner owns the private key listed in the website's TLS certificate. This allows users of the website to be sure that they are connected to the real website
5) *Regulations:* For all these reasons, many industry and government regulations require companies that handle user data to keep that data encrypted. Examples of regulatory and compliance standards that require encryption include HIPAA, PCI-DSS, and the GDPR.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

E. Symmetric Encryption

Symmetric encryption is a type of encryption where only one key (a secret key) is used to both encrypt and decrypt electronic information. The entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process. This encryption method differs from asymmetric encryption where a pair of keys, one public and one private, is used to encrypt and decrypt messages.

By using symmetric encryption algorithms, data is converted to a form that cannot be understood by anyone who does not possess the secret key to decrypt it. Once the intended recipient who possesses the key has the message, the algorithm reverses its action so that the message is returned to its original and understandable form.

F. Types of Symmetric Encryption

There are two types of symmetric encryption algorithms:

1) *Block Algorithms:* Set lengths of bits are encrypted in blocks of electronic data with the use of a specific secret key. As the data is being encrypted, the system holds the data in its memory as it waits for complete blocks.
2) *Stream Algorithms:* Data is encrypted as it streams instead of being retained in the system's memory.

G. Drawbacks

A significant disadvantage of symmetric ciphers is the key management necessary to use them securely. Each distinct pair of communicating parties must, ideally, share a different key, and perhaps for each ciphertext exchanged as well. The number of keys required increases as the square of the number of network members, which very quickly requires complex key management schemes to keep them all consistent and secret.

1) *Key Exhaustion:* Symmetric Encryption suffers from behavior where every use of a key 'leaks' some information that can potentially be used by an attacker to reconstruct the key. The defenses against this behavior include using a key hierarchy to ensure that master or key-encryption keys are not overused and the appropriate rotation of keys that do encrypt volumes of data. To be tractable, both these solutions require competent key-management strategies.
2) *Attribution Data:* Unlike asymmetric (public-key) Certificates, symmetric keys do not have embedded metadata to record information such as expiry date or an Access Control List to indicate the use the key may be put to - to Encrypt but not Decrypt for example. The latter issue is somewhat addressed by standards(eg ANSI X9-31) where a key can be bound to information prescribing its usage. But for full control over what a key can be used for and when it can be used, a key-management system is required.
3) *Key Management at Large Scale:* Where only a few keys are involved in a scheme (tens to low hundreds), the management overhead is modest and can be handled through manual, human activity. However, with a large estate, tracking the expiration and arranging rotation of keys quickly becomes impractical.

III. ADVANCED ENCRYPTION STANDARD (AES)

The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the U.S. government to protect classified information. AES is implemented in software and hardware throughout the world to encrypt sensitive data. It is essential for government computer security, cybersecurity and electronic data protection. AES has become the most popular algorithm used in symmetric key cryptography. The transparent selection process established by NIST helped create a high level of confidence in AES among security and cryptography experts.

A. Features of AES

NIST specified the new AES algorithm must be a block cipher capable of handling 128-bit blocks, using keys sized at 128, 192 and 256 bits. Other criteria for being chosen as the next AES algorithm included the following:

Security: Competing algorithms were to be judged on their ability to resist attack as compared to other submitted ciphers. Security strength was to be considered the most important factor in the competition.

Cost: Intended to be released on a global, nonexclusive and royalty-free basis, the candidate algorithms were to be evaluated on computational and memory efficiency.

Implementation: Factors to be considered included the algorithm's flexibility, suitability for hardware or software implementation, and overall simplicity.

B. Attacks on AES Encryption

Research into attacks on AES encryption has continued since the standard was finalized in 2000. Various researchers have published attacks against reduced-round versions of AES.

Researchers have found a few potential ways to attack AES encryption:

In 2009, they discovered a possible related-key attack. This cryptanalysis attempted to crack a cipher by studying how it operates using different keys. The related-key attack proved to be a threat only to AES systems that are incorrectly configured.

In 2009, there was a known-key attack against AES-128. A known key was used to discern the structure of the encryption. However, the hack only targeted an eight-round version of AES-128, rather than the standard 10-round version, making the threat relatively minor.

A major risk to AES encryption comes from side-channel attacks. Rather than attempting a brute-force assault, side-channel attacks are aimed at picking up leaked information from the system. Side-channel attacks, however, may reduce the number of possible combinations required to attack AES with brute force. Side-channel attacks involve collecting information about what a computing device does when it is performing cryptographic operations and using that information to reverse-engineer the device's cryptography system. In one case, a side-channel attack was used successfully to deduce AES-128 encryption keys by carefully monitoring the cipher's shared use of the processors' cache tables.

Side-channel attacks can be mitigated by preventing possible ways data can leak. Additionally, using randomization techniques can help eliminate any relationship between data protected by the cipher and any leaked data that could be collected using a side-channel attack.

C. Working of AES Algorithm

AES includes three block ciphers:

1) AES-128 uses a 128-bit key length to encrypt and decrypt a block of messages.
2) AES-192 uses a 192-bit key length to encrypt and decrypt a block of messages.
3) AES-256 uses a 256-bit key length to encrypt and decrypt a block of messages.

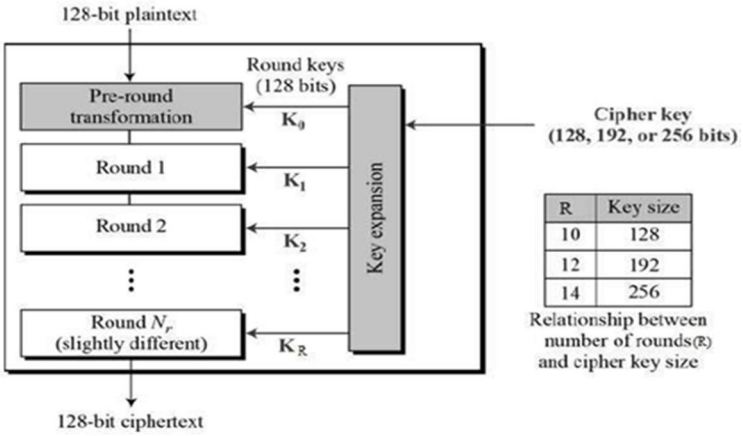
Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192 and 256 bits, respectively.

The sender and the receiver must both know -- and use -- the same secret key. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. A round consists of several processing steps that include substitution, transposition and mixing of the input plaintext to transform it into the final output of ciphertext.

D. Detailed Working of AES Algorithm

It is based on ‘substitution–permutation network’. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matri. Each of the rounds uses a different 128-bit round key, which is calculated from the original AES key.

The schematic of AES structure is given in the following illustration −



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

E. Encryption Process

The encryption phase of AES can be broken into three phases: the initial round, the main rounds, and the final round.

1) *Initial Round*

2) AddRoundKey

3) Main Rounds

a) SubBytes

b) ShiftRows

c) MixColumns

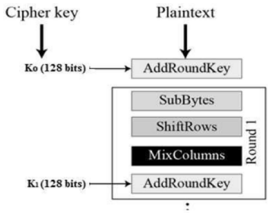
d) AddRoundKey

4) Final Round

a) SubBytes

b) ShiftRows

c) AddRoundKey



5) *Creation of Round Keys:* A Key Schedule algorithm is used to calculate all the round keys from the key. So the initial key is used to create many different round keys which will be used in the corresponding round of the encryption.

6) *Byte Substitution (SubBytes):* The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns. This step implements the substitution. In this step each byte is substituted by another byte.(Its performed using a lookup table also called the S-box. This substitution is done in a way that a byte is never substituted by itself and also not substituted by another byte which is a compliment of the current byte. The result of this step is a 16 byte (4 x 4) matrix like before. The next two steps implement the permutation.

7) *Shiftrows*

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row.

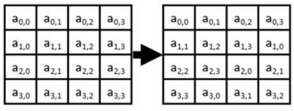
a) First row is not shifted.

b) Second row is shifted one (byte) position to the left.

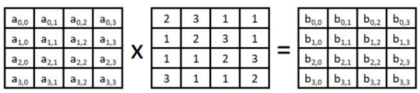
c) Third row is shifted two positions to the left.

d) Fourth row is shifted three positions to the left.

The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.



8) *MixColumns:* Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. *It should be noted that this step is not performed in the last round.* (This multiplication has the property of operating independently over each of the columns of the initial matrix, i.e. the first column when multiplied by the matrix, produces the first column of the resultant matrix.)



9) Addroundkey : The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

F. Decryption Process

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order −

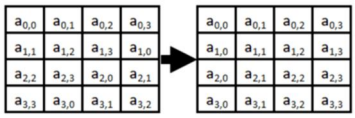
1) Inverse Final Round
a) AddRoundKey
b) ShiftRows
c) SubBytes
2) Inverse Main Round
a) AddRoundKey
b) MixColumns -This step is similar to the MixColumns step in encryption, but differs in the matrix used to carry out the operation.
c) ShiftRows
d) SubBytes -Inverse S-box is used as a lookup table and using which the bytes are substituted during decryption.
3) Inverse Initial Round
a) AddRoundKey

Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms needs to be separately implemented, although they are very closely related.

Of the four operations in AES encryption, only the AddRoundKey operation is its own inverse (since it is an exclusive-or).

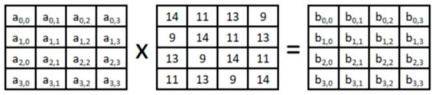
To undo AddRoundKey, it is only necessary to expand the entire AES key schedule (identically to encryption) and then use the appropriate key in the exclusive-or. The other three operations require an inverse operation to be defined and used.

The first operation to be undone is ShiftRows. The Inverse ShiftRows operation is identical to the ShiftRows operation except that rotations are made to the right instead of to the left.



The next operation to be undone is the SubBytes operation. The Inverse S-Box is used which is read identically to the S-Box matrix.

The last inverse operation to define is MixColumns. Like MixColumns, Inverse MixColumns can be defined as the matrix multiplication .



IV. RESULTS AND DISCUSSION

Cryptography and its principles have been studied carefully. I read and learned about Cryptography from various materials available on the internet.Encryption including why data encryption is necessary and types of encryption algorithms were studied. Features and principles of Symmetric key algorithm were studied from various materials available. Image encryption and decryption techniques using Advanced Encryption Standard (AES) algorithm is proposed .The usage of 256 bit cipher key to achieve the high security, because 256 bit cipher key is difficult to break. As a result of this secure transmission of image can be possible.

The goal of this research is to study the application of Advanced Encryption Standard algorithm (AES) for secure and efficient image encryption. The importance of image encryption by AES algorithm processes have been studied. It is also expected that AES algorithm study will have an effective role in strategic applications, because the encryption algorithm applied on hardware is also take a place in strategic communications equipment, it is safe and possible to develop this algorithm in terms of height and speed of time that have approved mainly on logistical aspects not on the technical aspects. It is possible to encrypt and decrypt by AES encryption used in many highly sensitive applications like Image encryption. We have reason to believe that use this method to encrypt the image will have a very good prospect in the future.

V. CONCLUSION AND FUTURE SCOPE

Since image steganography is done using AES, this system provides security from intrusion attacks and the usage of AES technique allows the encryption and decryption process to be more secure and faster. Thus this system provides security in storage and transmission of digital images. The cryptographic methodology proposed in this paper will further be tested on different types of input images with change in size of the image and keys of AES encryption algorithm.

The report shows the study in which a system 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.

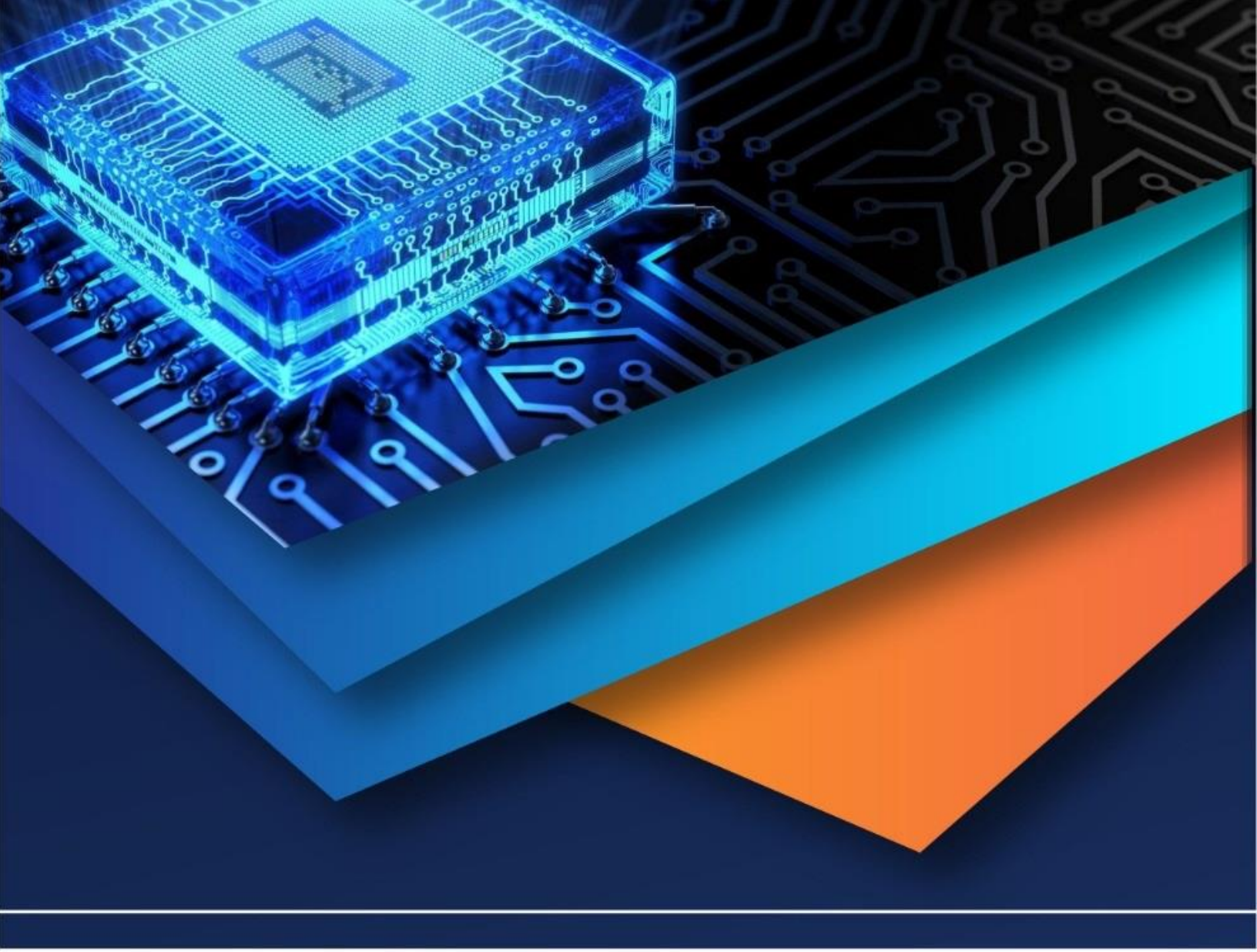
The next step in this direction will be system implementation, and then analyzing it for its efficiency, accuracy and reliability.

As a future work, I am going to continue this research in order generating more secure key to get the maximum encryption speed in limited implementation area.

I will implement a novel mechanism in which AES algorithm will be apply to encrypt and decrypt images securely for further applications in image communication system. Future scope is, it can be used in various applications like Military communication, Forensics, Intelligent systems etc.

REFERENCES

[1] https://www.iosrjournals.org/
[2] https://www.researchgate.net/
[3] https://citeseerx.ist.psu.edu/
[4] https://www.ijser.org/
[5] https://www.educative.io/edpresso/what-is-the-aes-algorithm
[6] https://www.researchgate.net



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)