International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 12 | Dec 2023 www.irjet.net p-ISSN: 2395-0072

AES-BASED IMAGE ENCRYPTION AND DECRYPTION FOR ROBUST DATA SECURITY AND DEFENSE AGAINST INTRUSION ATTACKS.

V. Priya Darsini [1], P. Priyanka [2], P. Padmaja [3]

[1] Assistant Professor, Department of IT, Panimalar Engineering college, Chennai, India.
[2,3] UG Student, Department of IT, Panimalar Engineering college, Chennai, India.

Abstract - *With the advancement of information technology, image data has become the mainstream of information transmitted over networks. The development of image information stealing technology is being carried out in parallel with the development of image encryption technology. We need to explore stronger image encryption techniques to keep up with the increasing number of information theft techniques. The development of communication technology has enabled the fast and reliable transmission of information, increasing its use in various fields such as business, military, civilian and scientific. The process of converting plain text or other kind of data from a readable form into an encrypted version that can only be decrypted if another entity has access to the decryption key is called cryptography in computer science. It improves security and helps protect sensitive data and personal information. Data is protected by encryption and decryption to prevent theft, tampering or compromise. Many technologies have been developed such as DES, TRIPLE DES, RSA, BLOW FISH, Genetic Algorithms, Chaotic Maps. Data security has also become an important issue for generations. In response to these problems, this system proposed image encryption/decryption using AES (Advanced Encryption Standard) technology, which ensures confidentiality, integrity, and authentication. Such techniques help evade intrusion attacks.*

Key Words: **Images, encryption, decryption, AES, Data security.**

1.INTRODUCTION

Today, more and more people use gadgets such as computers, smartphones and many other devices to communicate as well as store and transfer data. Communication is critical in everyday exchanges of huge amounts of data in industries such as banking, medicine, and finance. precisely a consequence of that, both the number of users and the number of illegal users attempting to get data has gone up. The question of data security then arises. Typically, encryption processes are used to secure this data so that it cannot be viewed by unauthorized third parties. The security of data and communications in the presence of the enemy is the main goal of cryptography. The science of information security known as cryptography protects data during transmission and storage.

The key and method for data encryption and decryption are two components of any encryption operation. The reliability of the cryptographic procedure depends on the use of keys. Two types of cryptographic mechanisms exist: Symmetric key cryptography refers to the application of equivalent key for encryption and decryption. Asymmetric key cryptography uses two distinct keys to encrypt and decode data. Compared with the asymmetric key algorithm, the symmetric key method is efficient, fast and simple to apply. The National Institute of Standards and Technology (NIST) released the Advanced Encryption Standard (AES) in 2001. Two Belgian cryptographers, Vincent Rijmen and Joan Daemen, developed the Rijndael block cipher, of which AES is a subset [1]. As the symmetric block cipher that has become the industry standard, AES has largely replaced the DES algorithm in applications [2]. AES symmetric encryption has been found to be more difficult than other symmetric or public key encodings. The AES standard, which is recognized by FIPS, defines encryption algorithms that may be used to safeguard computerized information [3].

Due to the shortcomings of 3DES, including a slow software algorithm and the use of 64-bit blocks, which are not sufficient for higher levels of security, larger blocks must be used. That's why AES is supposed to play the role of 3DES [4]. The advantages of AES over 3DES include increased computational power, a larger block size of 128 bits, and a high level of security against cryptographic analysis techniques such as linear attacks, differential-squares attacks, interpolation, and truncation. The main areas of use of image processing are robotics, intelligent systems, forensics, and military communications. In this study, we will use AES algorithm to encrypt and decrypt images to ensure data security and maximize computing performance.

There are two parts to the paper. Encryption is the subject of the first module, followed by the second module on decryption.

1.1 Encryption

The process of encryption involves the transformation of data from visible (also referred to as "normal" or "plain" data) into encrypted (also known as "ciphertext" data) that is not easily deciphered by external sources. The conversion is controlled by an algorithm and a key. The process must be reversible so that the intended recipient can convert the data back to its

original, readable form, but the process cannot be reversed without the required encrypted data. Therefore, the specifics of the key must also be kept secret. Most people agree that using encryption to protect against unintentional or intentional security breaches is the safest option. The work factor, or the amount of force required to "break" the encryption, is a common way to gauge the strength of an encryption technique. Strong systems take longer to break, but using more force can speed up the process (the longer the time spent in the attack, the faster the code can be broken).

1.2 Decryption

Data that has been encrypted and rendered unreadable will be converted back to the unencrypted state by decryption. The system extracts the scrambled and transformed data and converts it into text and images that are easy to grasp for the reader and the system. Decryption, in simple words, is the opposite of encryption, which encrypts data to make it incomprehensible but helps to make it readable by matching the decryption keys. Decoding will be required more often due to the use of the most complex decoding techniques, which inevitably also leads to high computational requirements.

2. LITERATURE SURVEY

SH Kamali proposed a modified AES (MAES) algorithm in this article; There is a strong amount of security and is often used as a reliable method of image encryption [5]. Rows and columns have mostly been changed in the updated design. If the primary row's bit position is within the even and first columns, the primary and fourth rows remain intact, and every byte within the second and third rows is moved to the proper. If both the initial and second lines of the report remain intact, the second and fourth lines are shifted to the left. Even at the highest entropy, security remains constant. Compared to the previous design, this design has a higher level of coding.

A composite association structure based on 128-bit AES DES key length has been proposed by Jignesh [6]. Here, the input image is transformed to 128-bit text first for encryption before being divided into two separate 64-bit plain text sets. The DES receives this plain text as its input. These two 64-bit encrypted messages combine to make a 128-bit message that's further scrambled using the AES encryption. this type of blending screen provides traditional AES with good non-linearity as a comparison. This approach enhanced the diffusion by convergent with the DES calculation.

Ju-Young proposed the idea of a selective encryption algorithm that fulfills five main requirements, including plaintext compression, cipher block size, configurable rings, optimized software implementation, and ability is only used in certain situations [7]. The compressed input image file is extremely secure, and the average duration of operation of the original AES file has been decreased by as much as thirty-five percent.

All systems currently in use cannot securely encrypt and decrypt data. Lack of security in simple approaches because in most cases data sent from sender to receiver will be sent in plain text.

Various systems are available, such as DES, Triple-DES and IDEA image encryption algorithms but,

1. In this case, a single system will be used to perform both encryption and decryption in existing systems.

2. Users cannot change their initial settings and will not be subject to repeated treatment.

3. Possesses desirable characteristics for diffusion ciphers and very low confusion.

Problems with the existing system:

a. In CBC mode, they only give an elevated degree of security.

b. They necessitate a vast amount of data.

c. The current architecture requires a significant amount of processing time.

d. They require a lot of processing power.

e. Not effective for networked systems.

3. PROPOSED SYSTEM

Therefore, using the AES approach, we are trying to add a new level of security to the data being transported from site to site in this project. The processes of encryption and decryption include converting plaintext into ciphertext and ciphertext back into plaintext, respectively. In this application we try to encrypt or decrypt text or image data using AES algorithm.
Our idea of providing a new level of security involves creating a new file for encrypted image with a ".crypt" extension but not a executable one. Unlike traditional files, images encrypted using our project are stored with the ".crypt" extension. This extension serves as a visual indicator to users that the file contains encrypted content and requires a decryption process to access the original image.

This innovation addresses a significant security concern present in many projects that use AES encryption without clear file extension differentiation. In such cases, users might inadvertently attempt to open encrypted files without following the proper decryption process, potentially leading to unauthorized exposure of sensitive content. By utilizing the ".crypt" extension, our project provides an intuitive solution that prevents accidental exposure and encourages users to follow the secure decryption protocol.
Security is paramount in our idea, and we have incorporated robust authentication mechanisms and access controls to ensure that only authorized users can initiate the decryption process and access the original image.

This approach stands in contrast to projects that might prioritize security to the detriment of user-friendliness. By striking a balance between security and usability, we offer an improved solution that enhances security while maintaining a positive user experience.

The advantages of the proposed system include:
1. Offers a high level of protection.
2. Information is encrypted, making it impossible for any user to access it directly.
3.Only authorized users can decrypt data employing a decryption key.
4. Simple maintenance.
5. This project handles erratic, difficult and difficult data reliably and efficiently while using less processing time and energy.
6. It works best with multimedia documents, especially images.

3.1 ADVANCED ENCRYPTION STANDARD(AES)

A. AES PROCESS

The AES algorithm possesses the following attributes:

- Referred to as a symmetric block cipher, it employs a shared (symmetric) public key.
- The key size can range from 128 to 192 or 256 bits, with 128 bits being the standard for data of varying sizes.
- In each round, AES employs a single S-Box, in contrast to DES, which utilizes eight S-Boxes.
- It boasts high resilience and offers sixfold greater speed compared to 3-DES, making it notably faster and more potent than RSA.

Compared to Fiestel encryption, the AES process is iterative in nature. The substitution and permutation operations are the basis of AES.Each cycle consists of a series of connected operations. This technique is repeated in each round 1) The input is exchanged with the output of the substitution process. 2) A cyclic shift is applied to the bits. 3) Transformed columns to combine them. 4) The AES algorithm combines the key and input data through an XOR operation. 128 bits of ordinary text are translated into a 4x4 matrix block by AES, which operates at the byte level [8]. The AES cycle count is influenced by key length, 12 cycles for AES-128, 10 cycles for AES-192, and 14 cycles for AES-256, each employing a different 128-bit round key at every round.

The AES algorithm's design criteria encompass three essential aspects:

(1) It should demonstrate resilience against all known attack methods.

(2) It should efficiently compress the code for fast execution.

(3) It should maintain a straightforward and uncomplicated structure.

B. AES SPECIFICATION

AES-128, AES-192, and AES-256 are the three different iterations of the AES algorithm. These designations are determined by the bit size of keys employed in the process. The numerical values in these designations indicate the key's bit size. The security level of AES is directly linked to the key size, with higher key sizes providing increased security. The rounding function used by the AES algorithm is made up of four distinct byte-direction modifiers [9]. Four rounds are used for encryption and they include:

1.substitute Byte

2. Shift Row

3. Mix columns

4.addroundkey

The encryption process is reversed during decryption, which includes the following steps:

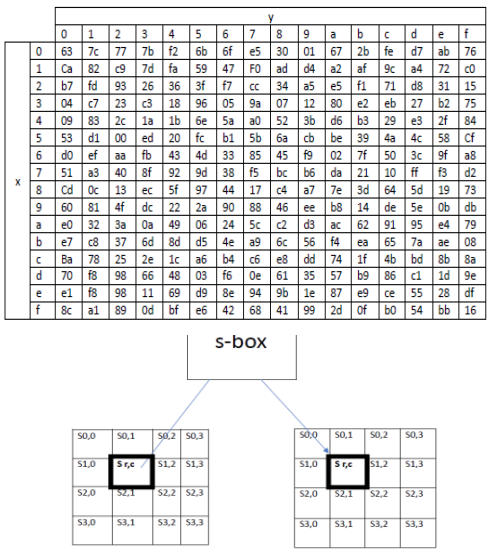
- inverse shift row
- inverse byte substitution
- Add round key
- Inverse mix column

The algorithm contains a number of rounds for both the key and the block. How long a key is utilized for encryption and decryption affects the number of rounds.

3.2 AES ENCRYPTION PROCESS

3.2.1 Substitute Byte

Utilizing an S-box-driven substitution table, For each individual byte in the State, the Substitute Bytes transformation performs an unpredictable byte replacement [10].



x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	e5	30	01	67	2b	fe	d7	ab	76
1	Ca	82	c9	7d	fa	59	47	F0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	Cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	Cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	Ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	f8	98	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Fig -1: Substitute byte function

3.2.2 Shift Rows Transmission

The bytes in the final trio of rows are periodically moved throughout all available bytes during the Shift Rows transformation.

- The first row remains in its original position.
- There is a one-space shift to the left of the second row.
- A two-position leftward shift occurs in the third row.
- There will be a three-position leftward movement for the fourth row.

The 16 bytes in the resulting matrix are the same, but they are shifted together.

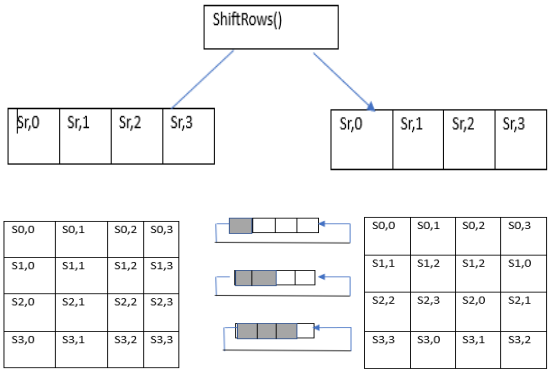


Fig -2: Operation of shift byte transformation

3.2.3 Mix Columns

Each four-byte column is transformed individually using the Mix Columns transformation. It converts the original column's four bytes into a completely different set of four bytes for output. The resulting array's dimensions match those of the plaintext content. In the Final Round, column permutation is not performed. The data columns are multiplied by a preset equation a(x) specified as:

$$a(x) = \{03\}x3+ \{01\}x2 + \{01\}x + \{02\}$$

This computation treats the columns as polynomials operating within the Galois Field GF (28).

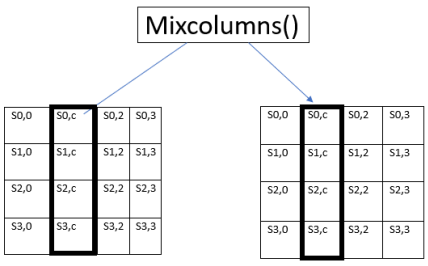


Fig -3: Operation of mix columns

3.2.4 Add Round Key

An basic bitwise XOR operation is used in the AddRoundKey transformation to connect a round key to the current situation. The 128-bit round key is XORed with the 16 bytes produced by the Mixing Column, resulting in a total of 128 bits. The relevant ciphertext is generated by repeating the above process until the last round. Using key planning technique, an encrypted key has been utilized to create a round key. The round key and the condition are both the same size, and every component is subject to XOR operations to create the following state: b (i, j) = a (i, j) ⊕ k (i, j)

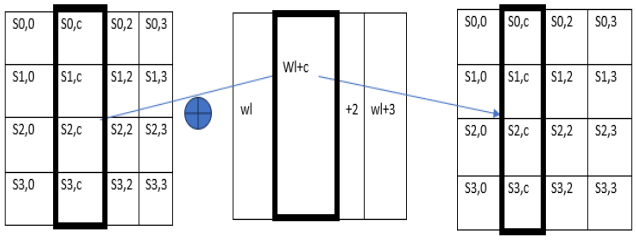


Fig -4: Add round key operation

3.3 AES–DECRYPTION PROCESS

3.3.1 Inverse Substitute Bytes

The transformation of substitution bytes is called inverse substitution bytes. This is accomplished using an inverse S-box [11]. To get this conclusion, the multiplicative counterpart of the Galois Field GF (28) is used, as well as the inverse of substitution bytes.

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	E	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	De	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	Fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	6b	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	C9	9c	Ef
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Fig -5: Inverse S-box

3.3.2 Inverse Shift Rows Transformation

The counterpart to the Shift Rows transformation is referred to as Inverse Shift Rows. In this process, the final three rows are circularly shifted in the opposite direction, while one byte in the second row has been switched to the other side in a circular manner. This process is repeated until the (n-3)rd row.

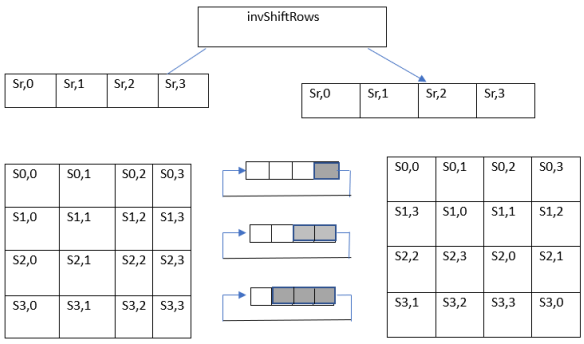


Fig -6: Inverse Shift row transformation operation.

3.3.3 Inverse Mix Columns

The Inverse Mix Columns Transformation serves as the counterpart to the Mix Columns Transformation. It conducts matrix operations column by column, resulting in columns represented as polynomial forms. Columns in the Galois Field GF (28) are mod multiplied by a known equation $a^{-1}(x)$ and are conceptualized as polynomials, where:

$a^{-1}(x) = \{0b\}x3 + \{0d\}x2 + \{09\}x + \{0e\}$

This operation takes place within the context of $(x^4 + 1)$.

3.4 IMPLEMENTATION

3.4.1 AES-Encryption Algorithm

Python is used to perform AES encryption. A simple image is used as input to the encoding process. There are a total of 10 rounds for this method because the image is divided into a 4*4 matrix. A total of four transformations (substitute byte, row shift, mix column, and add round key) were used in the nine rounds. In addition, three transformations that ignore the Mix columns form the 10th round [12]. Initially, the image will be encrypted.

3.4.2 AES-Decryption Algorithm

The process of decrypting in AES is the reverse of the encryption process. The decoding procedure is shown in the figure below. The decryption procedure takes the encoded picture as its input and performs the four operations of "Inverse substitute bytes, Inverse Shift rows, Inverse Mix columns, and Add round key." for up to nine rounds before execution. three transformations while ignoring Inverse Mix columns in rounded tenths. The receiver will receive the original image due to the decoding process.

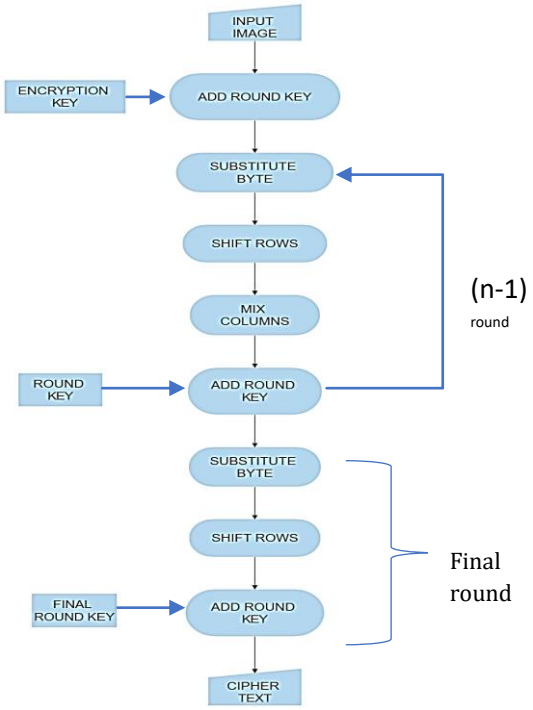


Fig -7: AES-Encryption algorithm flowchart.

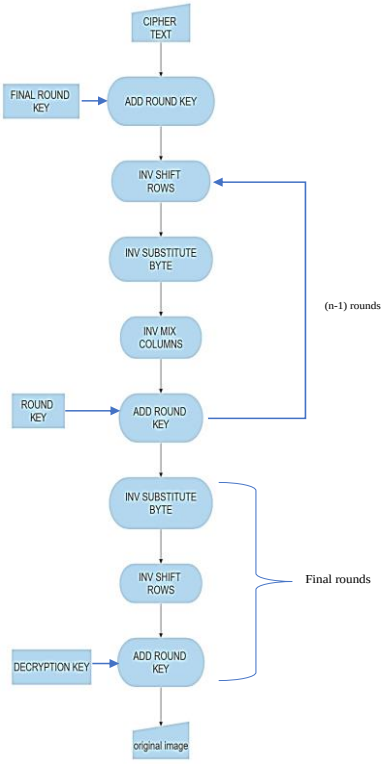
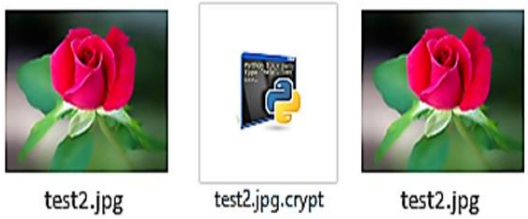


Fig -8: AES-Decryption algorithm flowchart.

4. RESULT

The algorithm's initial input image is a JPG file. By using the decryption process, the original JPG format image can be recovered from the unreadable encrypted image. The encrypting process uses the original image as input to generate the encrypted image, which is stored as .crypt file and the decrypting process is reinforced by using the encrypted image (.crypt file) as input to generate a original image. Throughout this article, an identical key is utilized for encryption and decryption.



5. CONCLUSIONS

In summary, this paper outlines an approach to image encryption and decryption utilizing the AES algorithm distinguishes itself through a combination of innovative security features and user-centric design. The use of the ".crypt" file extension, robust authentication and access controls contribute to a more secure solution compared to other projects using the AES algorithm.

Hence, the idea in this paper not only harnesses the strength of AES encryption but also leverages additional security layers to enhance the overall security posture. By addressing potential vulnerabilities and implementing comprehensive security measures, our idea provides a more secure environment for image encryption and decryption, offering users the confidence that their sensitive content remains protected against unauthorized access and attacks.

In future iterations of this project, enhancements could focus on implementing AES algorithm used in the idea of tailoring encryption techniques for specialized application domains, such as medical imaging, remote sensing, and augmented reality, etc., would depend on the specific requirements and characteristics of each domain. This could be exploring novel methods to enhance the adaptability and versatility of image encryption and decryption systems for specific application domains. An additional avenue for future work could involve studying the energy efficiency of the AES- based image encryption and decryption process. This could include researching methods to reduce the power consumption during encryption and decryption operations, making the algorithm more suitable for energy-constrained devices or environments where power efficiency is a critical factor.

REFERENCES

[1] J. Daemen and V. Rijmen, The Design of Rijndael: AES The Advanced Encryption Standard J. Springer-Verlag. 2002:55-56

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

[3] 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

[4] Agrawal, M., & Mishra, P. (2012). A comparative survey on symmetric key encryption techniques. International Journal on Computer Science & Engineering, 4(5), 877.

[5] S.H Kamali, R.Shakerian, M.Hedayati,”A new modified version of Advanced Encryption Standard based algorithm for image encryption”, International Conference on Electronics and information Engineering, ICEIE-2010.

[6] JignaeshR.Patel, Rajesh S.Bansode, VikasKaul,”Hybrid security algorithm for data transmission using AES-DES”,.IJAIS-2012.

[7] Ju-Young Oh, Dong-II Yang PhD and ki-Hwan Cho,”A selective Encryption Algorithm based on AES for medical Information”,Healthcare informatics research-2010.

[8] 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.

[9] 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.

[10] Siti Zarina Md Naziri, Norina Idris, “The Memory Siti Zarina Md Naziri, Norina Idris,“The Memory -less Method of Generating Multiplicative Inverse Values for SMethod of box in AES Algorithm”, In the Proceedings of 2008 IEEE International Conference on Electronic Design, Penang, Malaysia, pp.978978978-982, 2008.98

[11] 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.

[12] B.Subramanyan, Vivek.M.Chhabria, T.G.Sankar babu, In the "Image Encryption Based On AES Key Expansion" In Proceedings of the 2011 Second International Conference on Emerging Applications of Information Technology, Kolkata, India, pp.217-220, , 2011.