iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.53365

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 11 Issue V May 2023- Available at www.ijraset.com

Description of Image encryption Using AES-256 bits

Sahil Wade[1], Santosh Madiwal[2], Srivaramangai R[3]
Department of Information Technology, University of Mumbai, Mumbai, India

Abstract: ***Image Encryption using AES Algorithm is a technique to secure the confidentiality of images. One of the most popular and secure encryption algorithms is the AES (Advanced Encryption Standard) algorithm. It is a symmetric encryption algorithm that encrypts data using a 128-bit block cipher. In this process, the image is first converted into a binary format. Then, a random 128-bit key is generated, which is used to create a sequence of subkeys that will be used for each round of encryption. The binary image is then divided into 128-bit blocks, and the encryption algorithm is applied to each block using the subkeys generated earlier. This process ensures that the image is encrypted securely and is only accessible to those who have the key to decrypt it. One of the advantages of using AES is that it provides a high level of security, making it difficult for hackers to decrypt the encrypted data. Additionally, AES is a fast algorithm and can be implemented easily in hardware or software. The use of AES for image encryption ensures that the image is protected against unauthorized access and provides a secure way of transmitting sensitive images over the internet. Thus we can say that Image Encryption using AES Algorithm is a secure and efficient way to protect the confidentiality of images. It uses AES, a widely used encryption algorithm, to encrypt images securely, making it difficult for hackers to decrypt them without the key.***

Keywords: Image encryption, Image decryption, AES, Security, Confidentiality.

I. INTRODUCTION

The method of encrypting images is called transcoding photos to be secure a format that is only readable by legitimate users. The use of image encryption has become increasingly important as more and more sensitive information is being shared through digital images. The AES (Advanced Encryption Standard) algorithm is one of the most popular choices for image encryption due to its high level of security and efficiency. The importance of image encryption lies in the fact that it provides a secure way of sharing sensitive information through digital images. This is particularly important in fields such as medicine, defence, and finance where confidential images need to be protected from unauthorized access. Encryption ensures that only those with the appropriate decryption key can access the information contained within the image. Due to its high level of security and effectiveness, AES is a well-liked option for encryption. It is a symmetric encryption algorithm that encrypts data using a 128-bit block cypher. As a result, it is simple for authorised users to access the encrypted image because the same key is used for both encryption and decryption. AES is also very efficient and can encrypt and decrypt images quickly, making it a practical choice for image encryption. This paper aims to provide an overview of image encryption using the AES using 256 bits algorithm. We will discuss the importance of image encryption and why AES is a popular choice for encryption. We will also provide a detailed description of the AES algorithm and how it is used to encrypt images. Finally, we will discuss the advantages and limitations of the AES algorithm and provide some recommendations for future research in this area.

II. BACKGROUND

AES (Advanced Encryption Standard) is a symmetric encryption algorithm that uses a block cipher to encrypt data. It was first published in 1998 and has since become one of the most widely used encryption algorithms. AES has three key sizes: 128-bit, 192-bit, and 256-bit. The block size is fixed at 128 bits. The larger the key size, the more secure the encryption is, but also the more processing power required to encrypt and decrypt the data. One of the main properties of AES is its ability to resist attacks, such as brute force attacks, which try all possible key combinations until the correct one is found. AES uses a complex algorithm that makes it very difficult to crack the encryption without the correct key. Key management is very important in AES. The data is encrypted and decrypted using a key, and if the key is compromised, the encryption can be simply broken. Therefore, it is important to keep the key secure and to change it regularly. Additionally, the key should be generated using a secure random number generator to ensure that it is not predictable. Overall, AES is a very secure encryption algorithm that is widely used to protect sensitive data. Its strength lies in its ability to resist attacks and its dependence on the key for encryption and decryption.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

III. TYPES OF ENCRYPTION TECHNIQUES

Encryption is the process of transforming ordinary text or data into cypher text, which is an unintelligible format for those without the necessary decryption keys. The confidentiality of the data being sent or stored is protected in this way. Data is altered using encryption methods such that it can no longer be read, using a set of criteria. On the other side, decryption is the process of transforming encrypted text into plain text or data so that it may be read. A decryption method and key that is only known to the designated recipient are used to accomplish this. The decryption algorithm reverses the encryption process to recover the original data. Encryption and decryption are often used in conjunction with each other to secure sensitive information. For example, when you transmit your credit card information over the internet, it is encrypted to prevent unauthorized access. The recipient of the information then uses a decryption key to recover the original information.

A. Block-Based Encryption Techniques

Block-based encryption techniques divide the image into fixed-size blocks and encrypt each block independently. Some of the popular block-based encryption techniques that use AES algorithm include:

1) *Electronic Codebook (ECB):* This technique encrypts each block of the image independently using the same key. It is simple and efficient, but it has several drawbacks. For instance, it is susceptible to pattern attacks, and identical blocks in the original image will result in identical blocks in the encrypted image.
2) *Cipher Block Chaining (CBC):*This technique uses a chaining mechanism that ensures the encryption of each block depends on the previous block. The disadvantage of CBC is that it requires an initialization vector (IV), which must be kept secret to prevent attacks.
3) *Cipher FeedBack(CFB):*This technique converts the block cipher into a stream cipher by encrypting the previous ciphertext block and XORing it with the next plaintext block. The advantage of CFB is that it can handle arbitrary-length plaintext without padding.
4) *Output FeedBack(OFB):*This technique is similar to CFB, but instead of using the previous ciphertext block, it uses the output of the block cipher. The advantage of OFB is that it can be used to encrypt multiple plaintext blocks in parallel.

B. Stream Based encryption Techniques

Stream-based encryption techniques encrypt the image as a stream of bits. These techniques do not divide the image into fixed-size blocks. Some of the popular stream-based encryption techniques that use AES algorithm include:

1) *Counter(CTR):* Counter (CTR): This technique converts the block cipher into a stream cipher by encrypting a counter value and XORing it with the plaintext. The advantage of CTR is that it can handle arbitrary-length plaintext without padding and can be parallelized.
2) *Salsa 2.0:* This technique is a stream cipher that uses a 256-bit key and a 64-bit nonce to encrypt data. It is designed to be fast and secure, and it is widely used in applications that require high-speed encryption.

C. Advantages and Disadvantages

Each of these techniques has its own advantages and disadvantages. Block-based encryption techniques are simple and efficient but have some limitations, including the need for padding and susceptibility to pattern attacks. Stream-based encryption techniques, on the other hand, are more flexible and can handle arbitrary-length plaintext without padding, but they require additional precautions to ensure the nonce is not repeated, and they are not suitable for parallel implementation. Overall, the choice of technique will depend on the specific requirements of the application.

IV. WORKING OF AES ALGORITHM

AES is a symmetric is an encryption technique that encrypts data using a block cypher. It employs a 128-bit key for encryption and works with 128-bit data blocks. Each time there encryption round, a set of subkeys is created using the key. The AES encryption algorithm consists of four main steps as shown in figure 1. To totally scramble the data, the procedures include of breaking it up into blocks, swapping out various bytes, shifting rows, and combining columns. By the time it's done, the characters are utterly random and unintelligible to anyone who doesn't have the decryption key. The strongest and longest level of encryption that it offers is AES-256. In order to crack the encryption, a hacker would have to try out 2256 unique combinations, each of which had a total of 78 digits.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

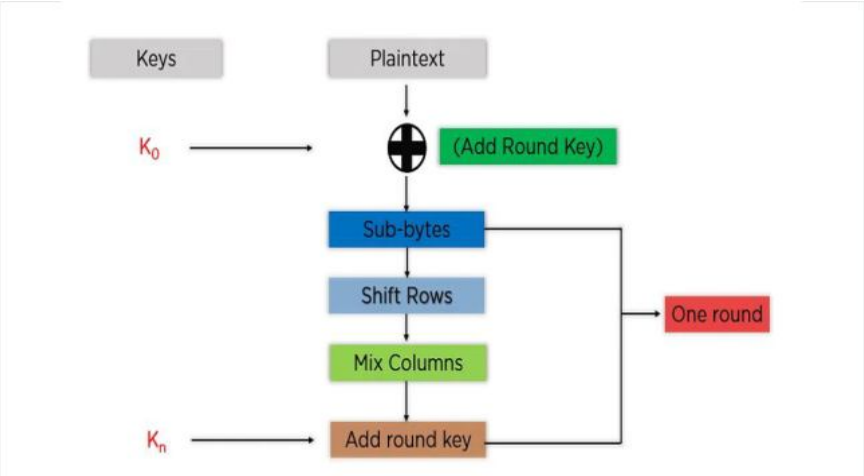


Fig. 1 Working of AES Algorithm

1) *Divide Information Into Blocks:* Blocking the data is the first step in the AES 256 encryption process. AES divides the data into 4x4 columns of 16 bytes because its block size is 128 bits.
2) *Key Expansion:* The AES algorithm uses Rijndael's key schedule to generate numerous round keys from the initial key in the subsequent stage of AES 256 encryption.
3) *Adding the Round Key:* The AES algorithm adds the initial round key to the data after it has been partitioned into 4x4 blocks in round key addition.
4) *Byte Substitution:* Each byte of data is replaced with another byte in this phase.
5) *Shifting Rows:* The 4x4 arrays' rows are subsequently shifted by the AES method. The second row's bytes are moved one space to the left, the third row's bytes are moved twice, and so on.
6) *Mixing Columns:* The 4x4 columns of the data array are mixed by the AES algorithm using a pre-made matrix.
7) *Another Round Key Addition:* The AES algorithm then repeats the second phase, adding the around key once more, before repeating the entire procedure.

V. EXISTING WORK

Image Encryption had been in lace for a long period and has improved a lot in the functioning with more security algorithms and image processing algorithms. Given below is some of the existing work that has been done by various researchers in the similar area of research. In order to safeguard the private image data from unauthorized access, Image Encryption and Decryption using AES is designed and implemented in their study by Manoj and Manjula[1]. According to them, one of the best encryption and decryption standards now on the market is a successful implementation of the AES algorithm. They achieved a maximum frequency of 165.462MHz from the design and the throughput reached the value of 252.132Mbit/sec for Image Encryption and Decryption. Saraf and et.al[2] in their research have proposed to use simple and simplified steps of the AES algorithm for image encryption. The proposed algorithm provides high randomness in image data for providing high security in minimum number of operations. Java has been used for the implementation. Saini and et.al[3], present a literature review, studied the AES algorithm for high-speed wireless communication applications, and also looked at the sub-byte process in addition of a round key and key expansion, row transformation with a shift, mixed column transformation, and transformation. In order to improve the effectiveness of the encryption techniques and to guarantee the security of the processes, the current AES algorithm was extensively investigated and analysed in their work. AES subblock design has been incorporated a circular key, a mix column, and an S-box. In their paper, Joshy and et.al[4] suggest an Android application that uses an RGB replacement to convert text into an image, which is then encrypted using the AES encryption technique. This method cleverly sends the secret key and the cypher text together in a single transfer so that the key exchange issue that typically arises in encryption models can be resolved using this way. For text to picture transformation, the encryption and decryption procedure uses a combined database on the transmitter and receiver sides. The value of the combinational number that was used to convert the text into the image is stored in an additional pixel that has been added to the encrypted image. The key that was utilized using the AES technique is converted into the RGB resultant value that corresponds to it. Finally, the destination host receives the created resultant value and picture. Decryption is carried out at the receiver side using reverse procedures.

According to them if the proposed technique is used, it will result in a highly secure text communication. Two lossless encryption techniques are used by Gopinath and Sowjanya[5], in their work where to create the key image, they have uses the EdgemapCrypt algorithm or a bit plane with the BitplaneCrypt algorithm. For all types of formats, including JPEG, BMP, and others, these two techniques generated lossless encryption. Both algorithms operate at the binary levels, making hardware implementation simple. They are also appropriate for real-time, multimedia applications like wireless networks and mobile phone services. Kundankumar and et.al[6], have described the encryption methods utilised for the internet of things (IoT). Many requirements of an embedded system should be followed by the security algorithm utilised for IoT. The primary topics covered in their work include the necessity for security in IoT, the idea of lightweight cryptography, and several cryptographic algorithms and their drawbacks in the context of IoT. Their work also presents a comparison of their performance based on the algorithm size (i.e., the necessary number of gate equivalents, block size, key size, throughput, and algorithm execution speed). The chapter examines how these algorithms work in the IoT system as well as their benefits and drawbacks. Alanazi and et.al[7] have used nine key factors such as Key length, cipher type, block size, developed, cryptanalysis resistance, security, possibility key, possible ACSII printable character keys, time required to check all possible keys at 50 billion seconds—these nine factors—were presented in their paper as a new comparative study between DES, 3DES, and AES. These factors demonstrated that AES is superior to DES and 3DES. The four widely used secret key encryption algorithms—DES, 3DES, AES (Rijndael), and Blowfish—have all been implemented in their study by Nadeem, Aamer and Javed[8], and the effectiveness of each is evaluated by encrypting input files with variable contents and sizes on various hardware platforms. To provide an accurate comparison of execution speeds, the algorithms have been developed using a unified language and using their standard specifications. A conclusion has been offered after a summary of the performance findings. The trials have shown that among the methods chosen for implementation, the Blowfish algorithm performs the best. Performance assessments of specific symmetric encryption algorithms are provided in their study by Abd and et.al[9]. The chosen algorithms are RC6, Blowfish, DES, RC6, AES, and RC2. The Experimental data lead to several conclusions. First off, there is no discernible difference between the values displayed in base 64 encoding and hexadecimal base encoding. Second, it was determined that Blowfish performs better than other widely used encryption algorithms in the event of increasing packet size, followed by RC6. Thirdly, they discovered that 3DES still performs poorly when compared to the DES algorithm. Fourthly, they found that RC2 is slower than all other algorithms in terms of time usage. Fifthly the AES outperforms RC2, DES, and 3DES in terms of performance. They further discovered that the outcome was the same for audio and video files as it was for text and documents. Finally, it can be shown that increasing the key size results in a noticeable shift in the battery and time usage. Jain and et.al[10] in their project have documented a new iteration of the advanced encryption standard algorithm that makes efficient use of CPU and memory resources. The input block and key are both 512 bits for the new AES 512 algorithm. This feature makes it more resistant to linear and differential encrypt analysis, increasing security and throughput while using less processing and memory. The results demonstrate a remarkable 230% throughput gain over the AES 128 bit method. The first "fully-documented" experimental Piret's DFA demonstration using actual hardware is described in the work done by Selmane and et.al[11]. In their work, they have tried to establish the viability of Piret's DFA on smart cards. Furthermore, they have noticed that errors do not consistently influence AES rounds and sboxes. Berent Adam[12] has given an introduction of the AES algorithm, and then have gone in detail about a few key aspects of it, and demonstrated some earlier research on it by contrasting it with other algorithms like DES, 3DES, Blowfish, etc. Benvenuto and Juan[13] in their research paper introduced the fundamentals of the Galois Field as well as how it is used to store data. Their study demonstrates and aids in the visualization of how data storage in Galois Fields enables manageable and efficient data manipulation, with a primary emphasis on applications in computer cryptography. There will also be information about the Advanced Encryption Standard (AES) algorithm, which is an illustration of computer encryption that makes use of the Galois Field. In order to measure the effectiveness of the AES encryption method by the size of the plaintext and the cost of operation per hop in accordance with the network scale, Lee and et.al[14] recommended the use of a dependable sensor network. This is because they found that a network approach used to construct a ubiquitous computing environment is the sensor network. It is a wireless network environment made up of numerous low-power, lightweight sensors. Even though sensor networks are capable of many things, they cannot provide secure node-to-node authentication. Over time, it results in a loss of network reliability as a whole and numerous security issues. As a result, the appropriate sensor network needs an encryption mechanism to construct reliable sensor network environments. Padate and et.al[15] have outlined a design for efficient encryption and decryption using the AES algorithm for data communication security. According to them, the Federal Information Processing Standard (FIPS) for the Advanced Encryption Standard (AES) has been developed by the National Institute of Standards and Technology (NIST), and it specifies an Advanced Encryption Algorithm to replace the Data Encryption Standard (DES), which expired in 1998. The Advanced Encryption Standard can be developed using pure hardware or software.

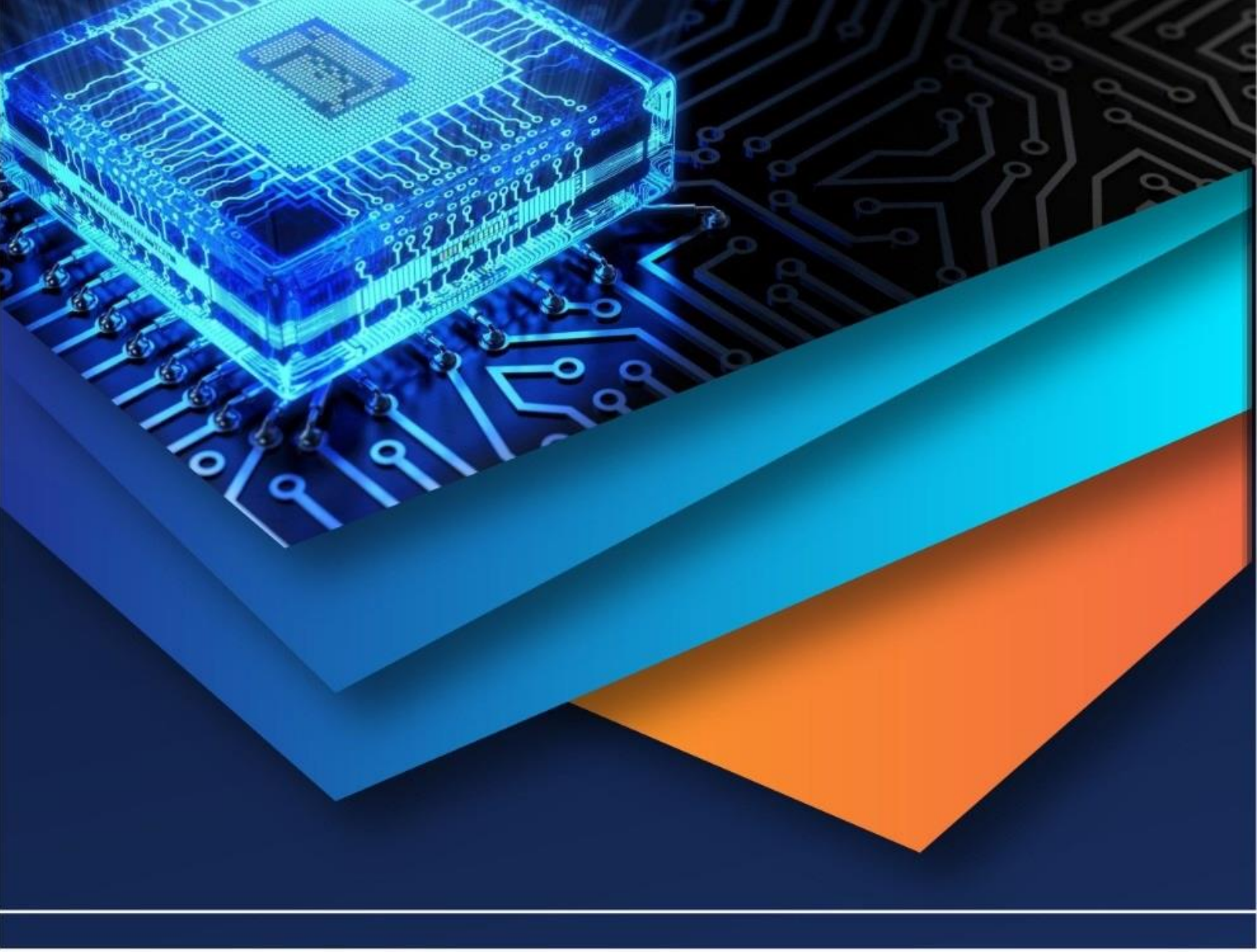
Reddy and et.al [16] have researched Micro Blaze and assessed it with some simple programmes. They used the Microblaze processor to implement the AES algorithm in all three modules, including the software platform, hardware platform, and combination of software and hardware platforms. The best option compared to software and hardware implementation is to implement the AES algorithm using the EDK (embedded development kit). When compared to hardware implementation, FPGA implementation has a faster execution rate, uses less power, and requires less space.

VI. CONCLUSION

Image Encryption using AES Algorithm is a powerful and secure way to encrypt images. It uses a 128-bit block cipher that makes it difficult for unauthorized users to decrypt the image. The algorithm is symmetric, meaning that the same key is used for encryption and decryption, making it a fast and efficient way to encrypt images. Overall, AES is widely used and is considered one of the most secure encryption algorithms available. The literature survey also emphasizes on Public key encryption algorithm which is a fundamental and widely using technology around the world.

REFERENCES

[1] Manoj, B., and Manjula N. Harihar. "Image encryption and decryption using AES." International Journal of Engineering and Advanced Technology (IJEAT) 1, no. 5 (2012): 290-294.
[2] Saraf, Kundankumar Rameshwar, Vishal Prakash Jagtap, and Amit Kumar Mishra. "Text and image encryption decryption using advanced encryption standard." International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) 3, no. 3 (2014): 118-126.
[3] Saini, Vedkiran, Parvinder Bangar, and Harjeet Singh Chauhan. "Study and Literature Survey of Advanced Encryption Algorithm for Wireless Application." International, Journal of Emerging Science and Engineering (IJESE) ISSN (2014): 2319-6378.
[4] Joshy, Amal, KX Amitha Baby, S. Padma, and K. A. Fasila. "Text to image encryption technique using RGB substitution and AES." In 2017 International Conference on Inventive Computing and Informatics (ICICI), pp. 1133-1136. IEEE, 2017.
[5] Gopinath, R., and M. Sowjanya. "Image encryption for color images using bit plane and edge map cryptography algorithm." International Journal of Engineering Research & Technology (IJERT) 1, no. 8 (2012): 4.
[6] Saraf, Kundankumar R., and Sunita P. Ugale. "IMPLEMENTATION OF TEXT ENCRYPTION AND DECRYPTION IN ADVANCED ENCRYPTION STANDARD." ASM'S International E-journal of ongoing Research in Management and IT.
[7] Alanazi, Hamdan, B. Bahaa Zaidan, A. Alaa Zaidan, Hamid A. Jalab, Mohamed Shabbir, and Yahya Al-Nabhani. "New comparative study between DES, 3DES and AES within nine factors." arXiv preprint arXiv:1003.4085 (2010).
[8] Nadeem, Aamer, and M. Younus Javed. "A performance comparison of data encryption algorithms." In 2005 international Conference on information and communication technologies, pp. 84-89. IEEE, 2005.
[9] Abd Elminaam, Diaa Salama, Hatem Mohamed Abdual-Kader, and Mohiy Mohamed Hadhoud. "Evaluating The Performance of Symmetric Encryption Algorithms." Int. J. Netw. Secur. 10, no. 3 (2010): 216-222.
[10] Jain, Rishabh, Rahul Jejurkar, Shrikrishna Chopade, Someshwar Vaidya, and Mahesh Sanap. "AES algorithm using 512 bit key implementation for secure communication." Int. J. Innov. Res. Comput. Commun. Eng 2, no. 3 (2014): 3516-3522.
[11] Selmane, Nidhal, Sylvain Guilley, and Jean-Luc Danger. "Practical setup time violation attacks on AES." In 2008 Seventh European Dependable Computing Conference, pp. 91-96. IEEE, 2008.
[12] Berent, Adam. "Advanced Encryption Standard by Example." Document available at URL http://www. networkdls. com/Articles/AESbyExample. pdf (April 1 2007) Accessed: June (2013).
[13] Benvenuto, Christoforus Juan. "Galois field in cryptography." University of Washington 1, no. 1 (2012): 1-11.
[14] Lee, Hyubgun, Kyounghwa Lee, and Yongtae Shin. "Aes implementation and performance evaluation on 8-bit microcontrollers." arXiv preprint arXiv:0911.0482 (2009).
[15] Padate, Roshni, and Aamna Patel. "Encryption and decryption of text using AES algorithm." International Journal of Emerging Technology and Advanced Engineering 4, no. 5 (2014): 54-9.
[16] Reddy, M. Sambasiva, and Y. Amar Babu. "Evaluation of Microblaze and implementation of AES algorithm using Spartan-3e." International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering 2, no. 7 (2013): 3341-3347.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY