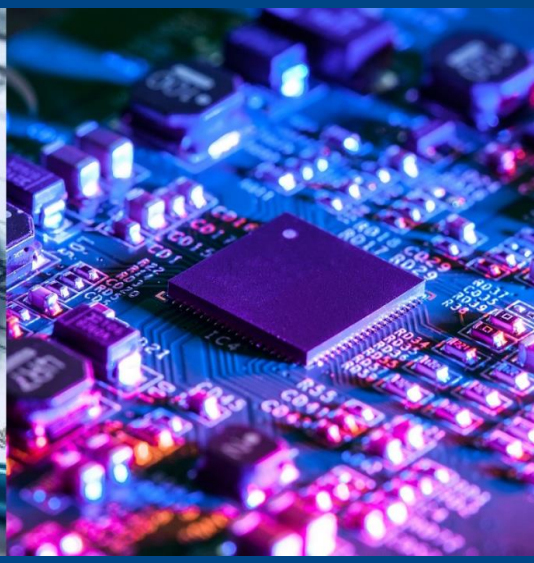
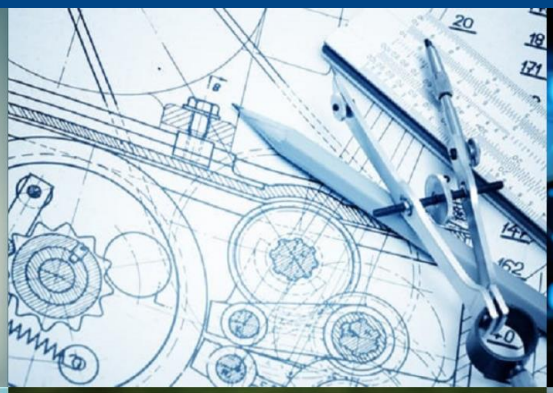
ISSN: 2582-7219

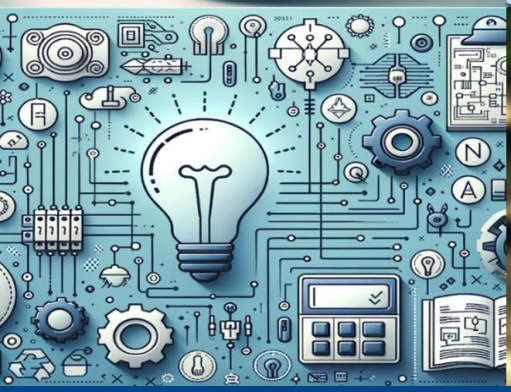




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 8, Issue 6, June 2025**

© 2025 IJMRSET | Volume 8, Issue 6, June 2025| DOI:10.15680/IJMRSET.2025.0806077

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Data Hiding in Audio using AES Algorithm

Dhanyashree

Department of Computer Applications, St Joseph Engineering (Autonomous) College, Vamanjoor, Mangalore, India

ABSTRACT: The practice of data hiding entails keeping information secret for a variety of purposes, including maintaining privacy, protecting secret information, and more. Data exchange via the internet network must be done securely. Therefore, there are numerous ways to securely transmit data to the destination, including steganography and cryptography. In this study, we propose using the AES algorithm to embed data into images, which is accomplished using C#.NET and the Microsoft.NET framework.

KEYWORDS: Data hiding, AES, encryption, decryption

I.INTRODUCTION

Personal information must be sent and received in order securely, we must be mindful of the rising Internet usage. This can be done by converting the data using a variety of approaches into different forms, which enables the final understanding of the data if the original format can be recovered. "Encryption" is the name given to this method. The fact that the data's presence is not hidden is a significant drawback of this method. The unreadable encrypted data might be converted if given enough time. restored to its initial state [1].

This problem has already solved by using the "steganography" method to covertly encode data in a cover media. The qualities of the cover material establish how well a facial recognition system works. The approach outlined below depicts the security issue with data transfer, which we can transmit messages about and is a focus of our research. over an internet network to the destination covertly? This query is addressed by steganography science.

Using Information can be concealed in carriers including photos, audio files, and text using steganography. transmissions of data, files, and movies. In this document, we offered a few strategies. Using image steganography methods, a secret message's digital text can be hidden [2].

We want to build a system for this project. To hide data, I employed the "STEGANOGRAPHY" methodology, which builds on other methods I used to develop a piece of software that employs algorithms to conceal data [3].

We discovered numerous methods of data hiding utilizing multimedia files after studying data hiding techniques, and my main concern " Where the Secret Data Is?" In order to make tiny changes to graphic or sound files without endangering their general viability for the viewer or listener, we learnt from our research that it is necessary to know the file type of the data that will be hidden and the cover file type. You can employ audio file fragments that have audio that cannot be heard by humans.

You may eliminate unnecessary color from graphic graphics and still create a picture. Steganography is the use of images that, to the human sight, appear to be unrelated and are challenging to tell apart from their source. Stego conceals information in discrete pieces. The goal of this project was to conceal data over images or encrypt 26 data. using a variety of steganographic techniques; in this system, we use the algorithm AES. to data concealment. Following the completion of our research, we developed a program that uses an algorithm to add information to images. The purpose of this research was data encryption, or employing various steganographic algorithms to cover data with a picture. The method we employ in AES is the system used to obfuscate the data [4]. Software was developed using our most recent research findings, which employ an algorithm to embed data in an image.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. LITERATURE SURVEY

Some steganographic systems combine steganography and conventional encryption; the The secret message is encrypted by the sender before the start of all communications. As a result, it becomes more challenging for a perpetrator to decipher hidden encryption words on a cover. Throughout history, It has been used by regular society kingdoms, and armies. Many of the stories revolve around steganography.

For instance, messages were masked in ancient Greece using methods like concealing. Several words are now present in the field of steganography. In the information concealing The concepts "cover," "embedded," and "stego" were defined during the session. The "cover" in this context refers to the original, unaltered data, music, video, and other communication components. the research into steganography Some steganographic systems combine steganography and conventional encryption; The secret message is encrypted by the sender before being start of all communications. As a result, it becomes more challenging for an attacker to decipher hidden encryption text in a cover. Throughout history, it has been employed by common world. Many of the stories revolve around steganography. For example, in ancient Greece, messages were masked using concealment methods. Steganography uses, a few new terms have emerged. sector. Considering the data site, the terms "cover," "embedded," and "stego" were defined. Workshop on concealment held in the countries. The original, unaltered data, sound, and video, and other message elements are referred to as the "cover" in this context. Since the inception of data, steganography has been a field of study.

[[7]] Data and information "Embedded" concealing are terms used to describe information that is concealed A general phrase is used in the cover data to refer to a number of difficulties that go beyond message embedding in content. It includes several different subfields. The term "hiding" can be used to describe both hiding information and making it invisible. information omissions this is a technique for concealment secrets that is employed redundant information like images, sounds, films, documents, etc. Recently, this method has grown in significance in a number of application sectors. In order to aid prevent unauthorized duplication, digital audio and photos, For instance, are increasingly marked with oblique indications that may be watermarks or hidden signatures. It is a performance where cover files are inserted there to conceal the existence of concealed messages. [8] Economic concerns have considerably expanded the field of information hiding study over the last 10 years. Despite the long tradition of "hidden information" concealment, the introduction of computers.

The benefit of using by adjusting the values of these sites to the values of the data to be disguised while taking into consideration the acceptable changeover limits occurs when scientific knowledge and technological methods advance, reviving this binary form of expression. These representations usually take the form of digital levels, regions, and changing values that can be detected by human senses like hearing and sight but not by other means. human awareness and sensation occur. human senses like sight and hearing.

III. METHODOLOGY

3.1 Feature extraction:

The suggested system's primary objective is to create a steganography-capable algorithm that can hide information inside of photographs. To safeguard the privacy of the data, an algorithm is created to mask all of the input data into the image. The system is then constructed using a fresh steganography method.

3.2 Sub Bytes:

The InvSubBytes step, or the inverse of SubBytes, is employed during decryption and entails taking the inverse of the affine transformation first before determining the multiplicative inverse. A straightforward transition known as SubBytes translates 8-bit data to other 8-bit data. For instance, the 8-bit value "00000000" is replaced with "01100011". What matters is that various byte data are consistently converted into various 8 bit data. If this criterion is violated, the altered data cannot be restored. Such technology is not capable of data encryption.

3.3 The shift row step:

By shifting the bytes in each row by a given offset, the ShiftRows step iterates through each the state's row. The first row is left alone for AES. The second row of bytes is shifted one position to the left. Additionally, the third and fourth rows are offset by two and three, respectively. Then, each column of the output state of the ShiftRows step is created using bytes from each column of the input state. This step is essential because AES would degrade into four different block

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

ciphers if the columns were encrypted independently. This step comes after the step of moving the bytes of each row to the left, which causes the bytes in every row to move by a specific offset value. All the rows immediately adjacent to the first row will be shifted to the left in this particular technique, but the first row's bytes won't be altered. This is accomplished because it is impossible to generate columns that are independently linear and result in four distinct block ciphers.

3.4. Mix Columns

The four bytes of each state column are mixed using an invertible linear transformation in the MixColumns step. Each input byte has an impact on all four output bytes when using the MixColumns function, which accepts fourbytes as input and outputs four bytes. Diffusion in the cipher is provided by MixColumns in conjunction with ShiftRows.

3.5 Add Round Key

In the AddRoundKey step, the subkey and state are combined. For each round, a subkey is generated from the main key using Rijndael's key schedule; each subkey is the same size as the state. The subkey is inserted by bitwise XORing the state and the relevant byte of the subkey. By using a byte-oriented method, it is possible to combine the SubBytes, ShiftRows, and MixColumns phases into a single round operation. Belgian cryptographers developed the symmetric 128- bit block data encryption technique known as the Rijndael cipher. Joan Daemen and Vincent Rijmen, acts as the Advanced Encryption Standard's (AES) foundation [23]. Technology of the United States (NIST) has accepted the symmetric block cipher known as the Advanced Encryption Standard (AES) as a standard. This was chosen through a process that lasted from 1997 to 2000 and was considerably more open and transparent than its legendary predecessor [23]. AES is based on a design method known as a substitution- permutation network, which combines both substitution and permutation, and is quick in both software and hardware. Keys with lengths of 128, 192, or 256 bits are supported by AES. Ten rounds of processing are used for encryption for 128-bit keys, twelve rounds for 192-bit keys, and fourteen rounds for 256-bit keys. All of these rounds use the same keys, with the exception of the last round, which is localized

IV. AES ALGORITHM

The AES commonly referred to as Rijndael, as a specification for the encryption of electronic data in 2001.The cryptographers created the AES form of the Rijndael block cipher and also submitted a proposal to NIST as a part of the AES hiring procedure. The Rijndael family of ciphers offers a variety of key and block sizes.

NIST chose three Rijndael family members, each having a 128-bit block size but three distinct key lengths: 128, 192 bits for use with AES. The American government has begun to support AES. Because the AES algorithm uses a symmetric key, the same key is utilized to encrypt and decrypt data. Following a five- year process for standardization in which alternative designs were submitted and assessed, the cipher was ultimately chosen as the best option. The ISO/IEC 18033-3 standard includes AES. Following approval from the Secretary of Commerce, AES became an official federal government standard in the US on May 26. As of 2002, the U.S. has approved only one publicly accessible cipher for use with top-secret material in a cryptographic module.

That cipher is AES. The United States developed the Advanced Encryption Standard (AES) in 2001 as a specification for the encryption of electronic data. Even though it is more difficult to construct than DES and triple DES, AES is nevertheless commonly used today.It produces 128 bits of output, which is encrypted cipher text, from 128 bits of input. The working of AES is based on the substitution-permutation network principle, which employs a network of interconnected processes to replace and mix incoming data.

For each block, AES employs a 16-byte grid in a column-major layout (4 bytes x 4 bytes = 128). This algorithm is very much efficient among another algorithm in this scenario. It cam be used to send secret message from one place to another place to gather the secret message and take out the secret message.

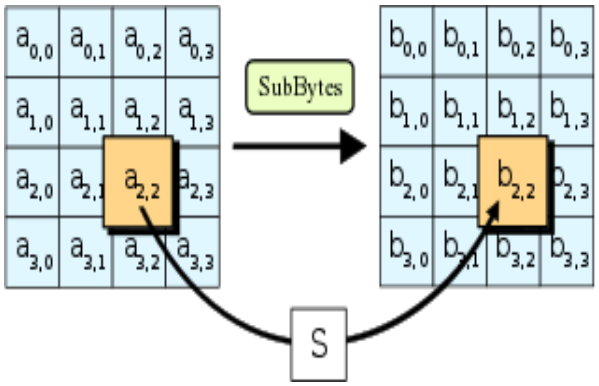
Output of 128 bits of input is encrypted cipher text. The substitution-permutation network principle, which underlies AES's functioning, involves a series of connected processes that replace and shuffle the incoming data. The Advanced Encryption Standard (AES), 4 also known as Rijndael (pronounced [rindael] in Dutch), is a specification for the encryption of electronic data that was developed in 2001 by US AES make use of a 16-byte grid in a column-major

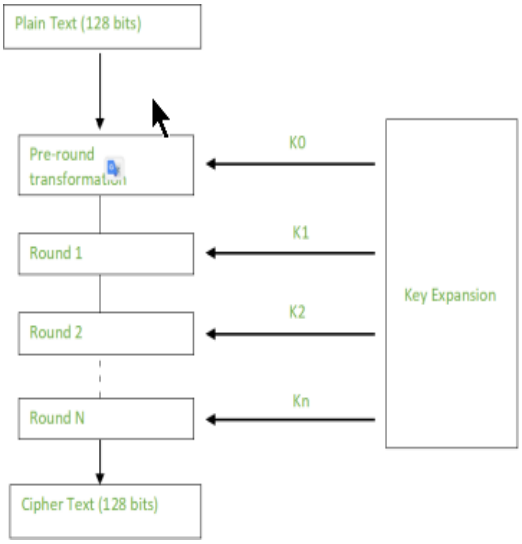
© 2025 IJMRSET | Volume 8, Issue 6, June 2025| DOI:10.15680/IJMRSET.2025.0806077

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



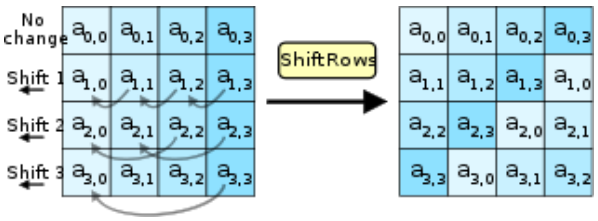


setup for each block (4 bytes x 4 bytes = 128) achieved with the aid of a lookup.Ttable is also known as S-box. The fact that a byte is never replaced by itself or by another byte throughout this replacement process is a tribute to the actual byte. This method results in the same 16-byte (4 x 4) matrix as before. Applying the permutation is done in the next two steps.

The front row does not shift. The second row is shifted left by one position. The third row is relocated twice to the left. The fourth row is relocated three times to the left. an AES The best technique for concealing audio data is an algorithm.

Mixing Columns: This procedure essentially entails a matrix multiplication. By multiplying each column by a specific matrix, the order of the in each column, bytes is changed.

The output from the prior stage is now XORed with the proper round key after round keys have been inserted. In this case, the 16 bytes are handled as a 128-bit data rather than a grid. a 128-bit encrypted data are output after each cycle. This procedure is continued until all information that needs to be encrypted has gone through it.

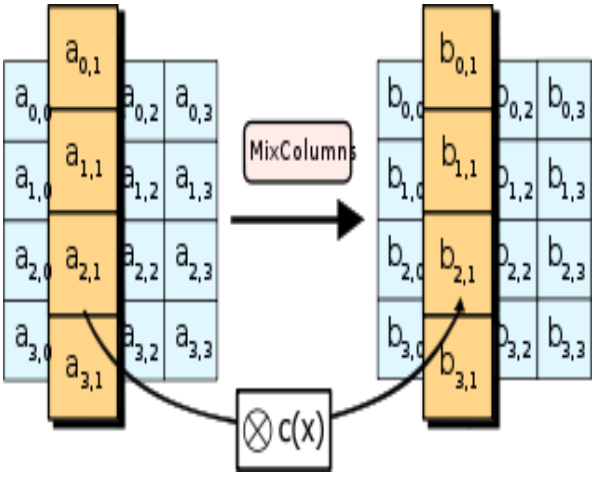


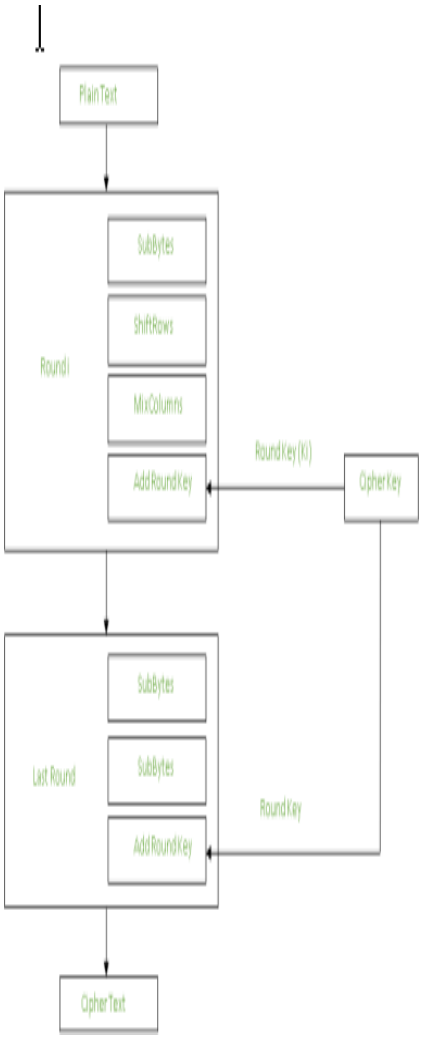
© 2025 IJMRSET | Volume 8, Issue 6, June 2025| DOI:10.15680/IJMRSET.2025.0806077

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)





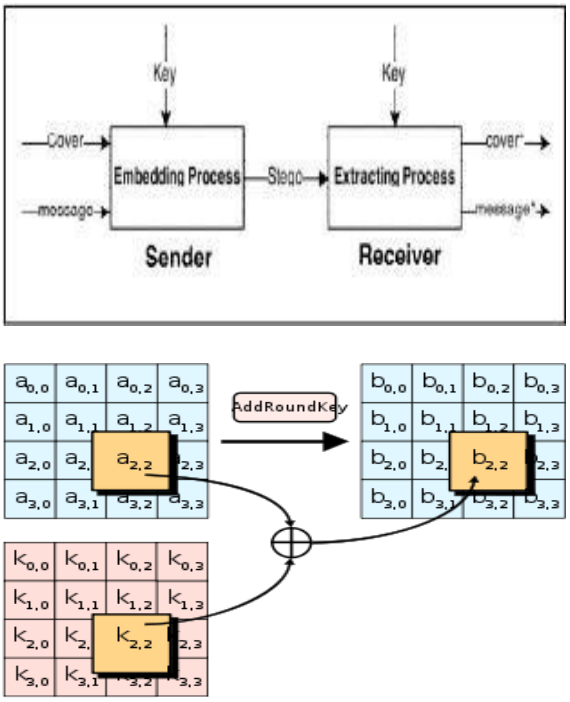
© 2025 IJMRSET | Volume 8, Issue 6, June 2025| DOI:10.15680/IJMRSET.2025.0806077

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The Inverse S-box, a lookup table, is used to alter the bytes during decryption.
ue to the CPU's integration of AES, programs that use it for encryption and decryption can now operate more quickly and securely (with throughput of several GB/s). Even with current technology, it is challenging to break the AES the algorithm, which has existed for 20 years. The algorithm's implementation is still its lone flaw.



The bytes are changed during decryption by using the Inverse S-box as a lookup table.

Apps that use AES for encryption and decryption can now function more fast and securely because AES is included into the CPU (offering throughput of many GB/s). We haven't been able to break the AES algorithm despite it being around for 20 years because it is not conceivable with the technologies we now possess. The algorithm's implementation continues to be the only problem.

V. RESULTS AND DISCUSSION

On a typical desktop computer, we used different key lengths (128, 192, and 256 bits) and block sizes (128 bits) to assess the performance of the AES algorithm. A collection of input files that were 100 KB, 1 MB, and 10 MB in size were used, and the encryption and decryption timings for each were noted.

The security of frequent cryptographic assaults against AES was the topic of the second experiment. We assessed its resistance to well- known assaults, such as brute force attacks, differential and linear cryptanalysis, and more. vectors. The validity of derived attributes is assessed using this process. The feature vector of a woman's face is represented by 0 and that of a man's by 1, respectively.

You give your interpretation of the findings in this portion of the report. Discuss the importance of your work after analyzing the implications of your findings and comparing them for the body of existing knowledge. Address any unexpected results or study restrictions.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

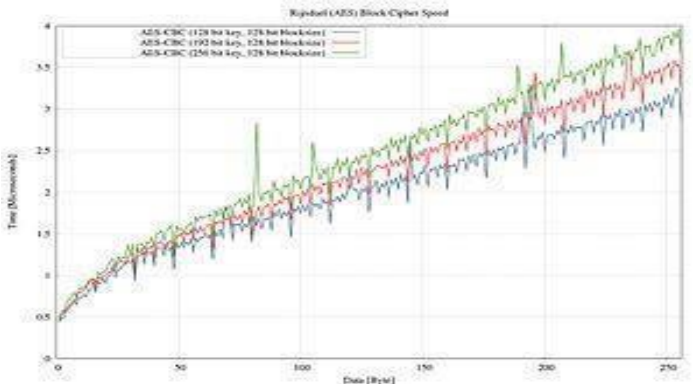
(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

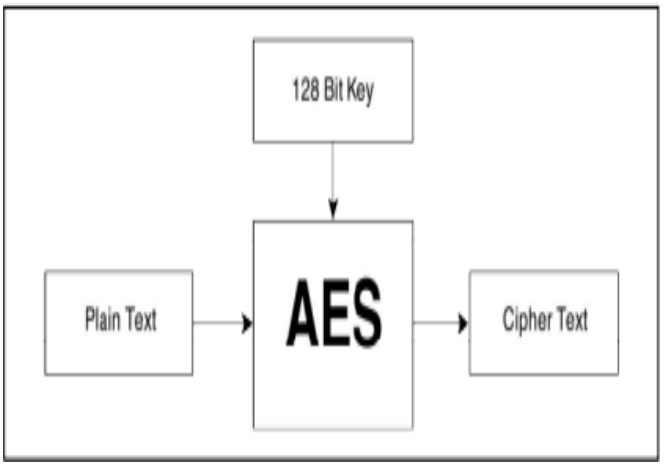
The outcomes of Experiment 1 show that the AES algorithm generally performs well for different key lengths and file sizes. The variations are insignificant for the majority of real-world applications, despite the fact that greater key lengths have a slightly higher computational overhead. This is in line with past research showing how well AES works in resource-constrained settings. AES's excellent resistance to differential, linear cryptanalysis, and brute-force assaults was shown to be demonstrated that it is resilient against a variety of cryptographic attacks. These results support AES's well-established reputation for security. It's crucial to remember that improvements in computing power may eventually affect how resistant AES is to brute force assaults.

Our investigation's focus was restricted to performance and security assessments in controlled environments. real- The actual world could introduce fresh elements that are not taken into this scenario, such as cloud service implementations or IoT device implementations. Even though we examined a variety of attack scenarios, fresh attack vectors can appear later on.

VI. CONCLUSION

Numerous methods exist for hide information in photographs, even though this document just briefly touched on a handful the majority popular image steganographic approaches. Each of the principal image file formats has an own method of concealing messages, each with varying advantages and disadvantages.





ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Where the first technique lacks payload capability, in addition option lacks robustness. For example, the patchwork technique can only successfully conceal a very little amount of data while being relatively resistant to the bulk of attacks. This is compensated for the least significant bit (AES) in both but both techniques lead to suspicious files that are more likely to be found when a warden is present. The method recommended in this study employs image steganography, a brand- new steganographic method. The cover file picture that the application generates as a stego image houses the personal data. This study designed the program using the Advanced Encryption Standard technique, which is faster, compared to earlier methods, it is more trustworthy and has a reasonable compression ratio.

Its efficiency in AES in various situations, like as IoT devices and cloud-based applications, might be explored in further research. A deeper knowledge of AES's long-term security would also result from investigating its resistance to new cryptographic assaults.

REFERENCES

[1] Rosziati Ibrahim and Teoh Suk Kuan, Steganography Imaging System (SIS): Hiding Secret Message inside an Image http://www.iaeng.org/publication/WCECS201 0/WCECS2010_pp144-148.pdf
[2] Zaidoon Kh. AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi, Overview: Main Fundamentals for Steganography http://arxiv.org/ftp/arxiv/papers/1003/1003.40 86.pd
[3] Bere Sachin Sukhadeo, User Aware Image http://www.ijcsmr.org/eetecme2013/paper19. pdf
[4] R. Ravnik and F. J. I. J. o. A. R. S. Solina, "Interactive and audienceadaptive digital signage using real-time computer vision," vol. 10, no.2, p. 107, 2013. Youssef Bassil , A Simulation Model for the Waterfall Software Development Life Cycle, 2011 http://arxiv.org/ftp/arxiv/papers/1205/1205.69 04.pdf Neamah, A. F. (2021, March). Adoption of Data Warehouse in University Management: Wasit University Case Study. In Journal of Physics: Conference Series (Vol. 1860, No. 1, p. 012027). IOP Publishing.
[6] Neamah, A. F., & Abd Ghani, M. K. (2018). Adoption of E-Health records management model in health sector of Iraq. Indian Journal of Science and Technology, 11(30), 1-20.
[7] Donald S. Le Vie, Jr., Understanding Data Flow Diagrams
http://ratandon.mysite.syr.edu/cis453/notes/D FD_over_Flowcharts.pdf
[8] B. Beizer, Software Testing Techniques. London: International Thompson Computer Press, 1990. 1030

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com