IJMRSET

e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 6, Issue 5, May 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.54

International Journal Of Multidisciplinary Research In Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 5, May 2023 |

Image Steganography

Prof. Shekhar Patle[1], Gunjan Gaud [2], Aditya Gaikwad[3], Tanaya Khare[4], Rushikesh Kumbhar[5], Sakshi Dubey[6]

Department of Information Technology, Zeal College of Engineering and Research, Pune,
Maharashtra, India[1,2,3,4,5,6]

ABSTRACT – The security of data in a computer is needed to protect critical data and information from other parties. There is a wide variety of algorithms used for the encryption of data, this study used a one-time pad algorithm for encrypting data. Algorithm One Time Pad uses the same key in the encryption process and decryption of the data. An encrypted data will be transformed into cipher text so that the only person who has the key can open that data. Therefore, the analysis will be done for an application that implements a one-time pad algorithm for encrypting data. The application that implements the one-time pad algorithm can help users to store data securely.

KEYWORDS: Security, Critical data, Encryption, Decryption, Cipher text.

I. INTRODUCTION

In today's image communication system, the security of images is essential. It is necessary to protect confidential image data from unauthorised users. Detecting and finding unauthorised 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, and multimedia system require reliable security in the storage and transmission of digital images. Due to faster growth in multimedia technology, the internet, and cell phones, there is a need for image encryption techniques to hide images from such attacks. In this system, we use AES (Advanced Encryption Technique) to hide images. Such an Encryption Technique helps to avoid intrusion attacks.

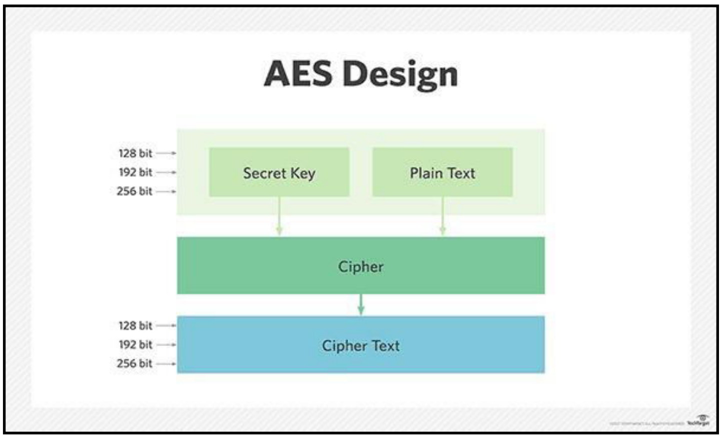


Fig 1:- AES (Advanced Encryption Standard) Design

1.1 PROBLEM STATEMENT

In this, project we will encrypt and decrypt images. Image encryption can be defined in such a way that it is the process of encoding a secret image with the help of some encryption algorithm in such a way that unauthorised users can't access it. Many encryption methods have been proposed in the 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 the transmission of images. Due to the complexity of their internal structure, they are not particularly fast in terms of execution speed and cannot be applied to images in a 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 the same time preserve the security level.

1.2 MOTIVATION

Encryption and decryption provide several security goals to ensure the privacy of data, non-alteration of data, and so on. Due to the great security advantages of cryptography, it is widely used today. The following are the various goals of cryptography –

Confidentiality has the information on the computer transmitted and must be accessed only by the authorised party and not by anyone else.

Authentication has the information received by any system has to checks the identity of the sender whether the information is arriving from an authorised person or a false identity.

Hence, it has Integrity that only permits the authorised party that allows modifying the transmitted information. No one in between the sender and the receiver is allowed to alter the given message.

And Non-Repudiation ensures that neither the sender nor the receiver of the message should be able to deny the transmission.

Therefore, only authorised parties can access the given information.

II. PROJECT OVERVIEW

Here we have implemented three parts in our project: data collection, key generation, and encryption/decryption. We take input as an image from the user, then the image is encrypted using AES, and the key generated here is also known to the sender and the receiver. Since the image is encrypted using AES, it is more secure than the DES. Hence, it makes encryption and decryption more secure.

III. LITERATURE SURVEY

A literature survey is the most important step in the software development process. Before developing the tool, it is necessary to determine the time factor, economy, and company strength. Once these things are satisfied, ten next steps are to determine which operating system and language are used for developing the tool. Once the programmers start building the tool, the programmers need a lot of external support. This support is obtained from senior programmers, books, or from websites. Before building the system, the above considerations r taken into for developing the proposed system.

This Algorithm gives a better performance of image encryption in comparison to the previous one. This algorithm is time taking and risky process. Secondly, in image encryption using block-based transformation algorithm, 2008 is based on the combination of image transformation.

In this algorithm, there is no key generator. Here we use the Blowfish algorithm which divides the image into several blocks.

Another survey is an image encryption approach using a combination of permutation techniques followed by encryption, 2008 approaches a new permutation technique based on the combination of image permutation and a well-known encryption algorithm called Raijn Dael.

In the new modified version of the advanced encryption standard-based algorithm for image encryption, 2010, the author analysis the advanced encryption standard (AES) algorithm and present a modification to the advanced encryption standard (MAES) to reflect high-level security and better image encryption. Their result so that after modification image security is high. They also compare their algorithm with the original AES encryption algorithm.

In the year 2011 one more algorithm was developed as image security by genetic algorithm, this is based on a hybrid model composed of a genetic algorithm and a chaotic function for image encryption. In their technique, the first several encrypted images are constructed using the original image with the help of the chaotic function.

A new image encryption approach using the integration of a shifting technique and the AES algorithm In March 2012, Author proposed a new encryption technique based on the integration of shift image blocks and basic AES, here the shifted algorithm is used to divide the image into blocks.

IV. RESEARCH SCOPE

Image Encryption/Decryption is a desktop-based application, built in Java using Swing and AWT. Functionality: This project is built to encrypt or decrypt the image using a key. In this, we must pass a key to encrypt the image and the image will be encrypted. The same key to be passed is necessary to decrypt that image, which will be decrypted in the same directory.

V. METHODOLOGY

AES encrypts a plaintext to a cipher text, which can be decrypted to the original plaintext by using a common private key.

It can be seen the cipher text should be different from and gives no clue to the original plaintext.

Encryption of AES operation using cipher key.

Where the plain text along with the key is given to the encryptor, which encrypts the plain text into cipher text, which is the result of the encryption process.

In reverse, the decryption takes place where the cipher text along with the key is given to the decryptor and its result into the original plain text.

With AES encryption, the secret key is known to both the sender and the receiver. The AES algorithm remains secure, the key cannot be determined by any known means, even if an eavesdropper knows the plaintext and the cipher text. The AES algorithm is designed to use one of three key sizes (Nk). AES-128, AES-196, and AES-256 use 128-bit (16 bytes, 4 words), 196-bit (24 bytes, 6 words), and 256-bit (32 bytes, 8 words) key sizes respectively. These keys, unlike DES, have no known weaknesses. All key values are equally secured thus no value will render one encryption more vulnerable than another. The keys are then expanded via a key expansion routine for use in the AES cipher algorithm.

Properties of Image:

Image encryption and decryption involve various properties that are important to consider. Here are some of the key properties:

1. Security: The most important property is the security of the encryption method. The image encryption and decryption algorithm should be strong enough to prevent unauthorised access to the image data.

2. Complexity: The complexity of the encryption and decryption algorithm is an important factor that determines the level of security. The algorithm should be complex enough to resist attacks and attempts to decrypt the image data.

3. Speed: In most cases, image encryption and decryption should be fast enough to allow real-time processing of large image files or multiple images. The encryption and decryption algorithm should not significantly slow down the processing speed or performance of the system.

4. Robustness: The encryption and decryption algorithm should be robust enough to handle common image operations such as rotation, scaling, cropping, and compression. It should also be able to handle different image formats, resolutions, and sizes.

5. Key Management: Proper management of encryption keys is essential to protect image data. The encryption key should be stored securely, and the decryption key should only be accessible to authorised users.

6. Efficiency: The encryption and decryption algorithm should be efficient in terms of memory usage and computational complexity. It should also be easily implementable in different programming languages and platforms.

In summary, image encryption and decryption should provide secure, complex, and robust protection of image data while still being fast, efficient, and manageable.

VI. EXPERIMENTAL ANALYSIS

Mathematical Understanding

Matrix Representation of Images

The smallest element of an image is a pixel (picture element). An image is represented by a matrix of pixels. A grayscale image contains various shades of the combination of black and white colors. A pixel or an element in the grayscale image matrix is 8-bit with that having 28 combinations of shades of gray. A pixel in a grayscale image or an element in the matrix is an integer value (0-255). A color image is usually a combination of three matrices, one each for the three colors RED (R), GREEN (G), and BLUE (B). Here, a pixel is 24-bit that 8 bits of Red, 8 bits of Green, and 8 bits of Blue information. It can create 224 color combinations. Each color (R/G/B) matrix has elements having values (0-255).

Requirement the Specification:

Software Requirements:

- Operating System: -Windows XP/7/8
- Programming Language: JAVA/J2EE/
- Tools: Eclipse, VSC, JDK 1.7 or Higher

Hardware Requirements:

- Processor: - Intel Pentium 4 or above
- Ram: - 2 GB or above
- Hard Disk: - 500GB

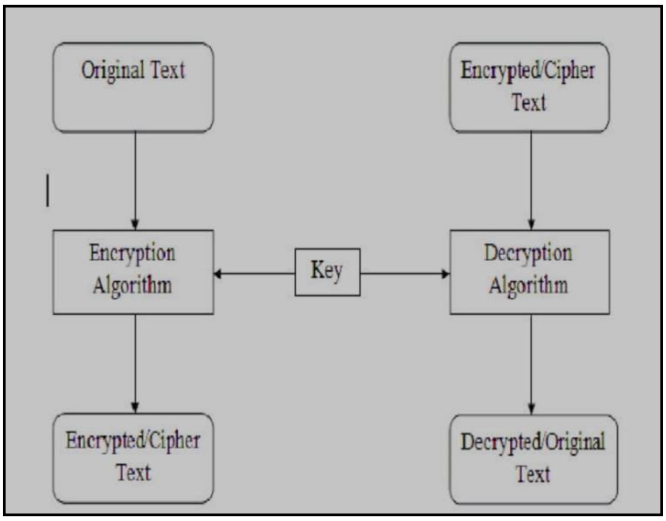


Fig 2:- Block Daigram of the process of Image Steganography

6.1 WORKING OF ALGORITHM

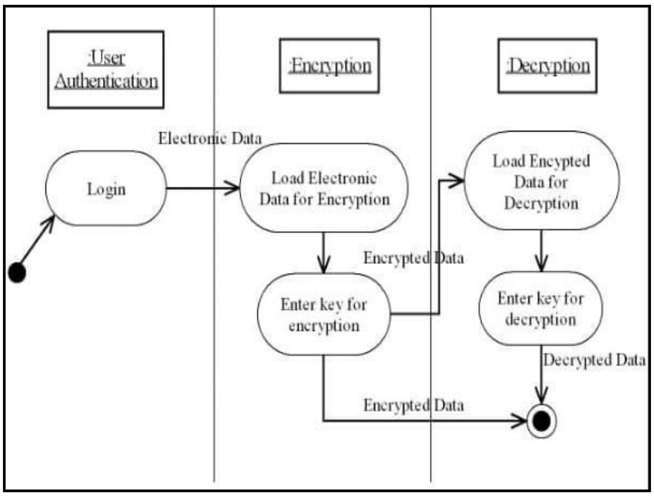


Fig 3:- Working Of Algorithm

6.2 DATAFLOW DIAGRAM

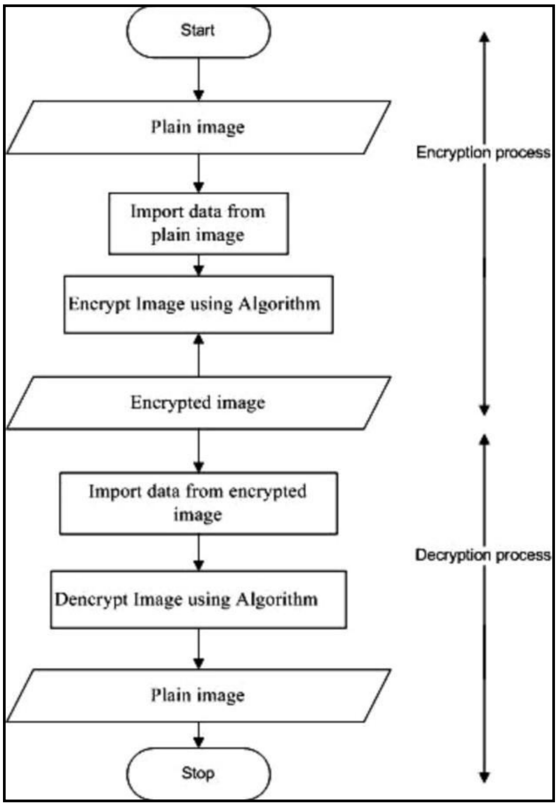

Start
Plain image
Import data from plain image
Encrypt Image using Algorithm
Encrypted image
Import data from encrypted image
Dencrypt Image using Algorithm
Plain image
Stop
Encryption process
Decryption process

Fig 4:- Data Flow Daigram

VII. RESULTS

The input image given to the AES algorithm is in JPG/PNG format. The original images given to the encryption process produced the cipher image and the decryption process is enhanced by providing the cipher image as input producing this plane image. Both encryption and decryption utilize the same key.

Fig 5:- Original Image:

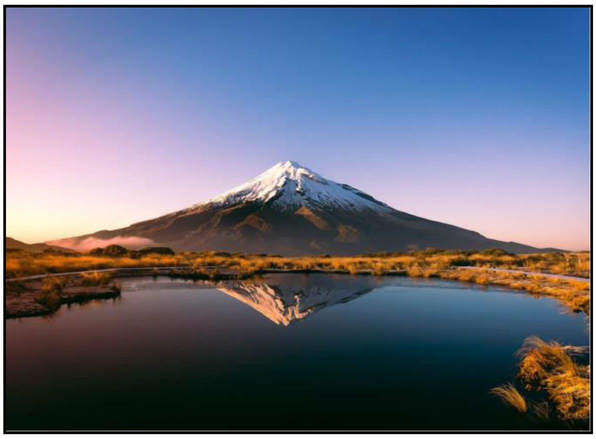
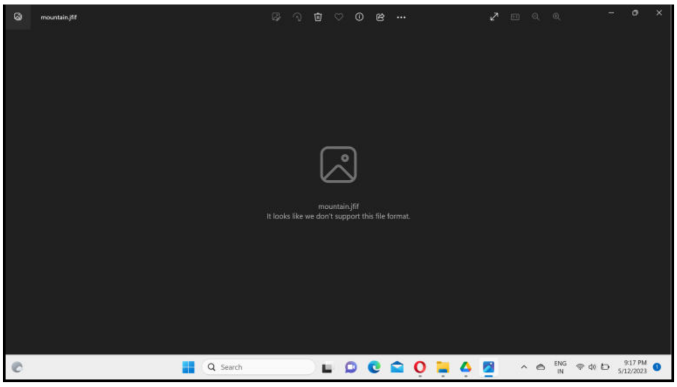
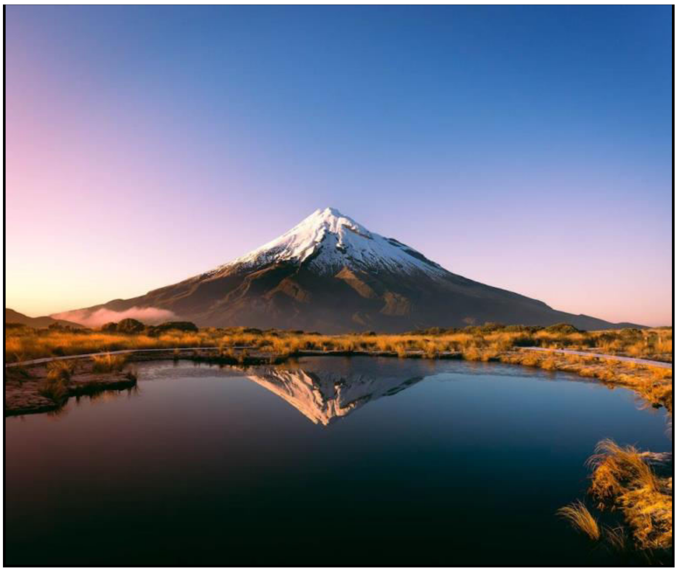


Fig 6:- Encrypted Image:



mountain.jfif
It looks like we don't support this file format.

Fig 7:- Decrypted Image:



VIII. FUTURE SCOPE

(i)Application-specific approaches: the current research in the field of image encryption is not done towards the building of application-specific image encryption approaches. So, soon, the development of application-aware image encryption approaches is a hot area of research.

(ii)Compressive sensing: development of compressive sensing-based image encryption approaches can be improved further for lightweight devices such as mobiles, spy cameras, and surveillance cameras.

(iii)Hyperparameters tuning: hyperparameters tuning of key generators such as chaotic maps can be achieved utilising the recently developed metaheuristic approaches, machine learning [155], deep learning [156], deep belief networks, or deep-transfer learning [157, 158].

IX. CONCLUSION

Using the internet and network are increasing rapidly. Every day a lot of digital data have been exchanged among users. Some data is sensitive that needs to protect from intruders. Encryption algorithms play vital roles to protect original data from unauthorized access. Various kinds of algorithms exist to encrypt data. The advanced encryption standard (AES) algorithm is one of the efficient algorithms and it is widely supported and adopted on hardware and software. This algorithm enables dealing with different key sizes such as 128, 192, and 256 bits with 128 bits block cipher.

This paper, explains many important features of the AES algorithm, various important encryption techniques have been presented and analyzed to make familiar with the other encryption algorithms used in encrypting the image which has been transferred over the network. The results of the simulation show that every algorithm has advantages and disadvantages based on the techniques which are applied to images. The results obtained from research show that AES can provide much more security compared to other algorithms like DES, 3DES, etc.

REFERENCES

1. A Deep Learning-Based Stream Cipher Generator for Medical Image Encryption and Decryption – 2022.
2. Image Encryption Based on AES and RSA Algorithms – 2020.
3. Image Encryption and Analysis using Dynamic AES – 2019.
4. An Image Encryption & Decryption And Comparison With Text - AES Algorithm.
5. Fridrich, J. (2010). Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press.
6. Johnson, N. F., & Jajodia, S. (1998). Exploring steganography: Seeing the unseen. IEEE Computer, 31(2), 26-34.
7. Westfeld, A., & Pfitzmann, A. (2000). Attacks on steganographic systems. In Information Hiding (pp. 61-76). Springer.
8. Cox, I. J., Miller, M. L., & Bloom, J. A. (2007). Digital watermarking. Morgan Kaufmann.
9. Katzenbeisser, S., & Petitcolas, F. A. P. (Eds.). (2010). Information hiding techniques for steganography and digital watermarking. Artech House.
10. Provos, N., & Honeyman, P. (2003). Hide and seek: An introduction to steganography. IEEE Security & Privacy, 1(3), 32-44.

INTERNATIONAL JOURNAL OF
MULTIDISCIPLINARY RESEARCH
IN SCIENCE, ENGINEERING AND TECHNOLOGY

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

www.ijmrset.com