IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

IMAGE STEGANOGRAPHY USING AES ENCRYPTION

[1]Jai Dhiyanesh J, [2]Anish Khan, [3]Anish Kumar

[1]B. Tech (ISDF) Student, [2]B. Tech (ISDF) Student, [3]B. Tech (ISDF) Student,
[1]Department of Computer Science Engineering,
[1] Dr.M.G.R Educational and Research Institute, Chennai, Tamilnadu, India

Abstract: Today, nearly all digital services, such as internet communication, medical and military imaging systems, and multimedia systems, require dependable security in digital picture storage and transmission. Because of the rapid advancement of multimedia technologies, the internet, and cell phones, there is an increased demand for digital picture security. As a result, picture encryption solutions are required to protect images from such attacks. To disguise the image in this system, we employ AES (Advanced Encryption Technique). This type of encryption technology aids in the prevention of intrusion assaults.

Keywords **- Steganography, Cryptography, AES encryption standard, Cipher Text.**

CHAPTER 1
INTRODUCTION

The Advanced Encryption Standard (AES), often known by its original name Rijndael, is a specification for electronic data encryption developed by the United States National Institute of Standards and Technology (NIST) in 2001. AES is a Rijndael block cypher variant devised by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, who submitted a proposal to NIST during the AES selection process. Rijndael is a cypher family with varying key and block sizes. NIST chose three members of the Rijndael family for AES, each with a block size of 128 bits but three different key lengths: 128, 192, and 256 bits. The US government has adopted AES. It succeeds the Data Encryption Standard (DES), which was published in 1977.

The AES algorithm is a symmetric-key algorithm, which means that the same key is used to encrypt and decrypt data. On November 26, 2001, the NIST announced AES as U.S. FIPS PUB 197 (FIPS 197) in the United States. Following a five-year standardization process in which fifteen competing designs were submitted and reviewed, the Rijndael encryption was chosen as the best fit. The ISO/IEC 18033-3 standard includes AES. AES became a federal government standard in the United States on May 26, 2002, following approval by the Secretary of Commerce. When employed in an NSA-approved cryptographic module, AES is the first (and only) publicly accessible cypher allowed by the United States National Security Agency (NSA) for top secret information.

CHAPTER 2
LITERATURE SURVEY

2.1 Modified AES Based Algorithm for Image Encryption, 2007:

M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki investigate the Advanced Encryption Standard (AES) and incorporate a key stream generator (A5/1, W7) into AES in their picture encryption technique to improve encryption performance.

2.2 Image Encryption using Self-Invertible Key Matrix of Hill Cipher Algorithm, 2008

Image encryption using the Hill cypher is presented by Saroj Kumar Panigrahy, Bibhudendra Acharya, and Debasish Jena. They're making a self-invertible matrix for the Hill Cipher method. They encrypted both grayscale and colour photos with this key matrix. Except for photographs with backgrounds of the same grey level or colour, their technique works effectively for all types of grey scale and colour images.

2.3 An Image Encryption Approach using a Combination of Permutation Technique Followed by Encryption, 2008

Mohammad Ali Bani Younes and Aman Jantan provide a new permutation strategy based on the combination of picture permutation and the well-known RijnDael encryption algorithm. The original image was divided into 4 pixels by 4 pixels blocks, which were then reassembled into a permuted image via a 3-permutation process, and the resultant image was encrypted via the RijnDael algorithm. Their findings revealed that employing the combination strategy reduced the correlation between image parts greatly while increasing entropy.

2.4 Image Encryption using Advanced Hill Cipher Algorithm, 2009

Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda have suggested an advanced Hill (AdvHill) cypher algorithm that encrypts with an Involutory key matrix. They encrypted various photos using the classic Hill cypher algorithm and their proposed AdvHill cypher technique. And it is evident that the original Hill Cipher cannot correctly encrypt images that have a big area covered with the same colour or grey level. However, their proposed approach is applicable to both grayscale and colour images.

2.5 Digital Image Encryption Algorithm Based on Chaos and Improved Des, 2009

Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan, and Dai Wei-di conduct research on chaotic encryption, DES encryption, and picture encryption algorithm combinations. In their method First, the new encryption approach employs a logistic chaos sequencer to generate a pseudo-random sequence, which is then chaotically applied to the RGB of an image, followed by double time encryptions with improved DES. Their results demonstrate a high initial value sensitivity, as well as high security and encryption speed.

2.6 New Modified Version of Advance Encryption Standard Based Algorithm for Image Encryption, 2010

Kamali S.H., Shakerian R., Hedayati M., and Rahmani M. analyse the AES algorithm and suggest a modification to the Advanced Encryption Standard (MAES) to reflect more security and improved picture encryption. Their result is that image security is high after modification. In addition, they compare their approach to the original AES encryption technique.

2.7 Permutation Based Image Encryption Technique, 2011

With the goal of preserving image quality, Sesha Pallavi Indrakanti and P.S.Avadhani suggest a new image encryption algorithm based on random pixel permutation. The encryption procedure is divided into three stages by the technology. The first step is picture encryption. The crucial generation phase is the second phase. The identifying process is the third phase. This provides colour 5 image confidentiality while requiring fewer computations. The permutation process is much faster and more efficient. The key generation method is distinct and distinct**.**

2.8 Image Security via Genetic Algorithm, 2011

Rasul Enayatifar and Abdul Hanan Abdullah suggested a new approach for image encryption based on a hybrid model made of a genetic algorithm and a chaotic function. With the use of the chaotic function, they first generate a number of encrypted images from the original image. In the following stage, these encrypted photos are used as the initial population for the genetic algorithm to begin operation. The genetic method is then utilised to optimise the encrypted images to the greatest extent possible. Finally, the best cipher-image is selected as the final encryption image.

2.9 Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on It, 2011

Four chaotic maps are compared by Kuldeep Singh and Komalpreet Kaur. On the image, there are cross chaotic, logistic, Ikeda and Henon map, and noise effects. To begin, they employ an image encryption method to convert the original image to an encrypted image. They then apply noise to the encrypted image and decrypt the cypher image with noise to return to the original image. They discovered that the cross chaotic map outperformed the other three chaotic maps.

2.10 Image Encryption Based on The General Approach for Multiple Chaotic Systems, 2011

Qais H. Alsafasfeh and Aouda A. Arfoa suggested a new image encryption technique based on two chaotic systems: the Lorenz chaotic system and the Rössler chaotic system. According to the experimental results, the picture encryption technique has the benefits of a huge key space, high-level security, a high obscure level, and high speed.

2.11 Image Encryption Using Differential Evolution Approach in Frequency Domain, 2011

Ibrahim S I Abuhaiba and Maaly A S Hassan describe a new effective image encryption method that employs magnitude and phase modification via the Differential Evolution (DE) approach. To show the security of the novel picture 6 encryption technique, they performed key space analysis, statistical analysis, and key sensitivity analysis.

CHAPTER 3
ADVANCED ENCRYPTION STANDARD

The AES Encryption algorithm (also known as the Rijndael algorithm) is a 128-bit symmetric block cypher algorithm. It translates these individual blocks using 128-, 192-, and 256-bit keys. It encrypts these blocks and then connects them to generate the ciphertext. It is built on a substitution-permutation network, or SP network. It is made up of a sequence of connected processes, such as substituting inputs for particular outputs (substitutions) and others involving bit shuffling (permutations).

In fact, as of 2021, AES is the world's most popular data protection method. **Wi-Fi networks, Google Cloud, Facebook Messenger, Java programming, and many password managers** use AES encryption to protect sensitive data.

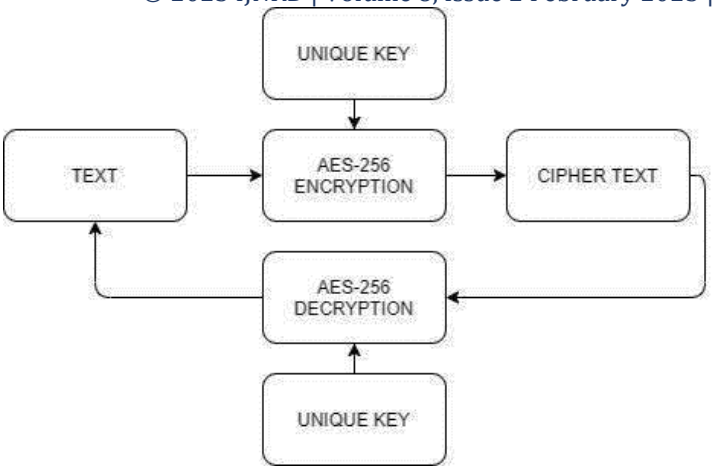

Fig. 2: The Diagrammatic representation of AES-256

CHAPTER 4
EXISTING SYSTEM

The current technique encloses the data with the image's histogram. This procedure also improves the image's contrast. Histogram equalisation is used to create the image. The histogram's highest crests are selected. The bins between the crests have remained constant, while the outside bins have shifted outwards, allowing each of the two crests to be divided into two adjoining bins. To increase contained capacity, the top two bins in the modified histogram might be further divided, and so on until a suitable composition improvement effect is obtained. The position map is wrapped in the host image, in sync with the carrier message bits and other side data, for the restoration of the original image. Image histogram generation is a difficult and time-consuming operation. However, the image's divergence is increasing. The information is only hidden in the image where the security level is at its lowest. Because the information is buried, and if the procedure of restoring is known to the intruder, he will be able to retrieve the image quickly and easily.

CHAPTER 5
PROPOSED SYSTEM

Image steganography is a GUI -based project in which we are hiding the image using encoding and decoding functions. We are creating a window in which there are two buttons: Encryption and Decryption.

•For Encryption, Enter the key in the message box to secure data, select any image, then type merge this encoded string into image and the user can save the text file where he/she wants.
•For Decryption, select the cipher text which is encoded, type the key to decrypt the data, and by Tkinter module cipher text is converted to image and shown in the GUI.

CHAPTER 6
MODULES INVOLED

6.1 Securing the image

Securing the image using a key to encrypt and encrypting the image using Cryptography and AES Algorithm.

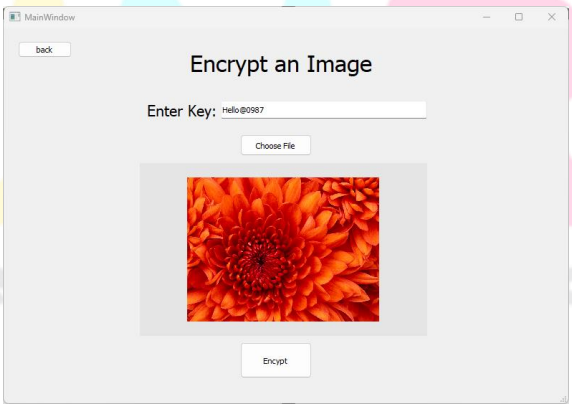

Fig. 1: Securing the image with a key

6.2 Image encryption

In this module the image is encrypted and converted into cipher text. The cipher text has to be saved in the local disk with an extension .txt (Text File).

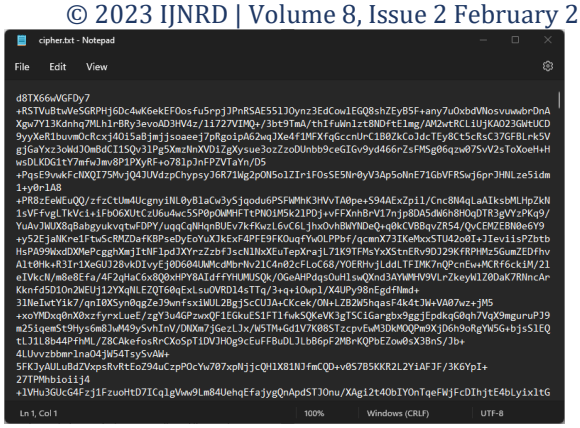

Fig. 2: Encrypt image and convert

6.3 Decrypting cipher text

In this module the cipher text is decrypted and converted into image with enter the correct key. The decrypted image has to be saved in the local disk with an extension .png (Portable Network Graphics).

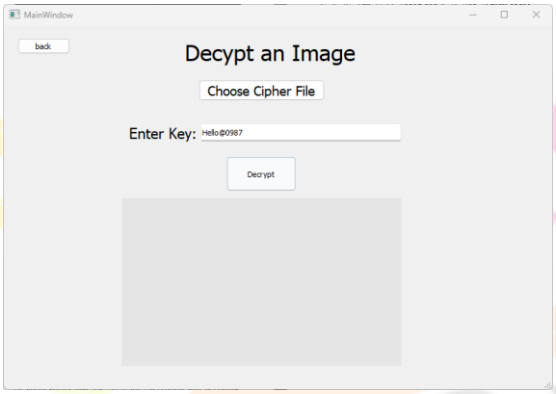

Fig. 3: Decrypt data and retrieve the original data

6.4 Retrieving image/data

The image is encrypted by using AES algorithm. The receiver which has both keys information hiding and encipher key only able to open same image. The decrypted image will be displayed in GUI

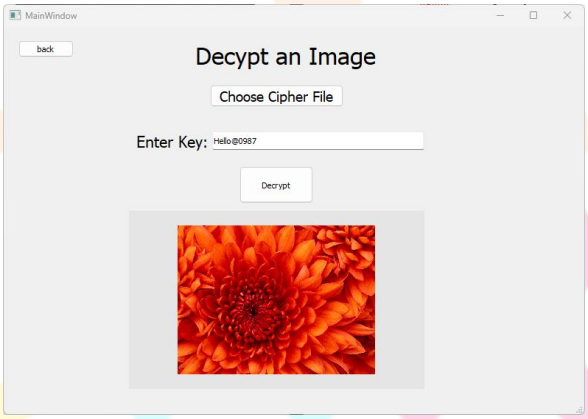

Fig. 4: Retrieve the original data

CHAPTER 7
CONCULSION

Image steganography is a GUI-based project in which we use encoding and decoding methods to hide a hidden message within an image. We're going to make a window with two buttons: encoding and decoding. In order to encode, enter a message in the message box, and it will be converted to base64. Enter a key to secure data, choose a picture, and then enter merge this encoded text into image. The user may then store the image wherever he or she wishes. Select the encoded image, type the key to decode the data, and concealed text is displayed in the textbox using the Tkinter module. The AES instruction set is now integrated into the CPU (it provides throughput of several GB/s, which improves the performance and security of applications that use AES for encryption and decoding. Despite the fact that it has been 20 years since its release, we have yet to break the AES algorithm since it is infeasible even with current technology. The only remaining vulnerability is in the algorithm's implementation. Because image steganography is performed using AES, this system protects against intrusion assaults, and the use of AES allows the encryption and decryption processes to be more secure and faster. As a result, this system ensures the security of digital image storage and transfer.

ACKNOWLEDGMENT

We are really very thankful and we will also like to display our sincere recognition for our Head of the Department Dr S Geetha and our project guide Srilakshmi for the guidance and support in making this Research possible. Their Valuable guidance from initial to final level helps us to achieve to complete this research paper. Our sincere thanks to all the faculties who helped us to complete this and gave their valuable advice and made it easy to complete this.

REFERENCES

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

[2] M. Zhang, G. Shao and K. Yi, "T-matrix and Its Applications in Image Processing J.n Electronics Letters", vol. 40, no. 25, pp. 1583-1584, 2004.

[3] L. Y. Fan, J. J. Luo and H. L. Liu, "Data Security Concurrent with Homogeneous by AES Algorithm in SSD Controller J. Ieice Electronics Express", vol. 11, no. 13, pp. 115-118, 2014.

[4] Y. J. Li and W. L. Wu, "Improved Integral Attacks on Rijndael C", Journal of Information Science and Engineering, vol. 27, no. 6, pp. 2031-2045, 2011.

[5] Y. W. Zhu, H. Q. Zhang and Y. B. Bao, "Study of the AES Realization Method on the Reconfigurable Hardware C", 2013 International Conference on Computer Sciences and Applications, pp. 72-76, 2013.

[6] K. Stevens and O. A. Mohamed, "Single-Chip FPGA Implementation of a Pipelined Memory-Based AES Rijndael Encryption Design C", 2005 Canadian Conference on Electrical and Computer Engineering, pp. 1296-1299, 2005.

[7] J. Tpldinas, V. Stuikys and R. Damasevicius, "Energy Efficiency Comparion with Cipher Strength of AES and Rijndael Cryptographic Algorithms in Moble Devices J", Elektonika IR Elektrotechnika, vol. 2, pp. 11-14, 2011.

[8] J. T. Zhou, A. C. Oscar and G. T. Zhai, "Scalable Compression of Stream Cipher Encrypted Images Through Context-Adaptive Sampling J", IEEE Transactions on Information Forensics and Security, vol. 9, no. 11, pp. 1857-1868, 2014.

[9] D. Das, M. Mukherjee, N. Choudhary, A. Nath and J. Nath, "An Integrated Symmetric Key Cryptography Algorithm Using Generalised Modified Vernam Cipher Method and DJSA Method: DJMNA Symmetric Key Algorithm C", 2011

[10] World Congress on Information and Communication Technologies, pp. 11991204, 2011.