Multi-Image Steganography

Shoab Khan[1], Om Waykar[2], Aditya Nagtilak[3] , Mazin Sunjufy[4] , Dr. Shraddha Khonde[5]

[1] Department of Computer Engineering, MES's Wadia College of Engineering, Pune
[2] Department of Computer Engineering, MES's Wadia College of Engineering, Pune
[3] Department of Computer Engineering, MES's Wadia College of Engineering, Pune
[4] Department of Computer Engineering, MES's Wadia College of Engineering, Pune
[5] Department of Computer Engineering, MES's Wadia College of Engineering, Pune

---***---

Abstract - Steganography is the practice of concealing information within various types of data, encompassing the embedding of confidential content like messages, images, audio, or video within a cover image. The primary objective involves hiding the secret message or image within the selected image through the utilization of the Least Significant Bit (LSB) technique. To ensure the safeguarding and security of the concealed content, the Advanced Encryption Standard (AES) Algorithm is implemented. The comparison of different image formats, each varying in text length or image size, is conducted. The algorithm's efficacy is evaluated through metrics such as Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE), with a higher PSNR value indicating a superior image quality. Steganography assumes a vital role in numerous applications, including but not limited to medical, military, One Time Password (OTP), and copyright protection.

***Key Words*:** Image steganography, LSB, Advanced Encryption Standard, PSNR Ratio, MSE

1.INTRODUCTION

Steganography is a contemporary fashion employed to conceal nonpublic information within colorful forms of digital content, similar as images, audio, videotape, or textbook, all while avoiding dubitation . This approach holds considerable significance in ultramodern communication and finds operations in fields like healthcare, military operations, One Time word(OTP) systems, brand protection, and beyond. As the volume of data changed over the internet continues to grow, icing the confidentiality and integrity of information has come consummate in guarding against unauthorized access.

Historically, individualities employed styles like unnoticeable essay, runner's discretion, or sealed wax to transmit uncommunicative dispatches. nevertheless, these ways proved to be lower than secure. In moment's digital age, steganography involves concealing nonpublic data within a train, effectively hiding it from third- party discovery.

The Least Significant Bit(LSB) fashion is a extensively honored system within the realm of steganography, used to bed nonpublic information into an image. This process entails the gradational relief of the least significant bit of the cover image with bits from the secret communication. To enhance the security of this retired data, the Advanced Encryption Standard(AES) algorithm is employed. AES is a symmetric encryption algorithm that employs block ciphers for data encryption and decryption. The paper provides an expansive companion on exercising the LSB fashion for bedding secret information into an image, and it elaborates on employing the AES algorithm to insure the security of the concealed content. likewise, it encompasses exploration papers addressing different steganography motifs, similar as image encryption and decryption, LSB steganography for multicolored images, spatial sphere-grounded arbitrary image steganography, and other affiliated subjects.

2. LITERATURE SURVEY

1. The paper investigates the application of LSB-based text and image steganography using the AES algorithm to secure concealed data within cover images. It details the methodology, encompassing the utilization of the LSB encoder, AES encryption, and decryption procedures. The experimental findings illustrate the proficient concealment and retrieval of text and image data, with PSNR and MSE measurements serving as indicators of the reconstructed images' quality. The research underscores the importance of steganography across diverse applications and underscores the efficacy of the suggested algorithm in ensuring data security.

2. The text explores the integration of LSB steganography and AES-128 encryption in a software named MPDFStego. It details how the program conceals confidential text within numerous PDF documents using the Least Significant Bit (LSB) approach and secures it with the Advanced Encryption Standard (AES). The validation of the implementation is conducted through tests, affirming the accurate execution of both methodologies. The program's proficiency in concealing data within multiple PDF files is established, and the stego PDF files generated are contrasted with those generated by another application. The outcomes indicate that MPDFStego yields smaller stego PDF files.

3. The document introduces a steganography approach employing image manipulation to conceal text within an image. This technique alters the least significant nibble of each image byte to encode every nibble of the input text, ensuring optimal data capacity and security. The implementation is executed in Java, featuring a straightforward GUI utilizing AWT and

SWING packages. To bolster the security of the scheme, the AES encryption algorithm is incorporated.

4. The article elucidates the notion of steganography, the art of concealing information within alternative data. It specifically delves into image steganography, where concealed messages are embedded within digital images. The article examines diverse steganography techniques and their practical applications, such as the least significant bit (LSB) technique. Additionally, it furnishes a systematic guide on the process of concealing and unveiling text within an image using Python.

5. The article introduces a novel method to heighten the security of image steganography through the utilization of the Data Encryption Standard (DES). The model proposed integrates S-Box mapping and a confidential key for preprocessing the secret image before its incorporation into a cover image. This preprocessing stage guarantees that extraction is unattainable without awareness of the mapping rules and the secret key. Furthermore, the suggested scheme adjusts the pixel intensity, providing an additional layer of security to the encryption process.

6. The article outlines an Android-based application of text-to-image steganography, employing a 512-bit algorithm with the least significant bit technique. The suggested algorithm employs a symmetric key block cipher for both the encryption and decryption of text and images. The least significant bit technique is applied to incorporate the confidential data into the cover image. Experimental results validate the efficacy of the proposed method in concealing secret data within non-secret files.**5.** The paper titled "Security Improvisation in Image Steganography using DES" [5]The article introduces a novel method to heighten the security of image steganography through the utilization of the Data Encryption Standard (DES). The model proposed integrates S-Box mapping and a confidential key for preprocessing the secret image before its incorporation into a cover image. This preprocessing stage guarantees that extraction is unattainable without awareness of the mapping rules and the secret key. Furthermore, the suggested scheme adjusts the pixel intensity, providing an additional layer of security to the encryption process.

7. The article explores an innovative approach to text steganography, focusing on concealing text messages within multimedia files like images. This method employs Discrete Wavelet Transform (DWT) to partition the input image into four sub-bands, with the text information concealed in the low-frequency band. Following this, the image undergoes compression using DWT, and the original image can be restored through Inverse Discrete Wavelet Transform (IDWT) coupled with a decryption technique. Through testing, the proposed method demonstrates commendable hidden invisibility, security, and resilience against diverse attacks.

8. The document presents True Edge-based 4 Least Significant Bits Steganography, a method that integrates edge detection and steganography for concealing a confidential message within the four least significant bits of edge pixels in an image. Through the utilization of edges, this technique attains superior visual image quality compared to alternative methods. Empirical findings substantiate that the suggested approach proficiently conceals a substantial volume of confidential information while preserving high-quality stego-images.

9. The article introduces an improved LSB image steganography method that integrates a status bit and AES cryptography. It employs a filtering algorithm utilizing MSB bits to enhance the concealment of substantial data within bitmap images. The primary goal of this approach is to augment security and attain a superior PSNR value in comparison to alternative methods.

10. The document discusses a research investigation into the Performance Analysis of the StegoCrypt Algorithm, utilizing the LSB-AES 128-bit approach across different image sizes. This study delves into the efficacy of integrating cryptographic and steganographic methods for ensuring secure data transmission. Furthermore, it offers insights into the influence of image size on the imperceptibility of the concealed message.

3. PROPOSED SYSTEM AND ALGORITHM

Proposed System: The system aims to enhance data security through steganography techniques, specifically utilizing the LSB (Least Significant Bit) method for embedding data into images. The system also incorporates the Advanced Encryption Standard (AES) algorithm with a key length of 128 bits to ensure secure data transmission.

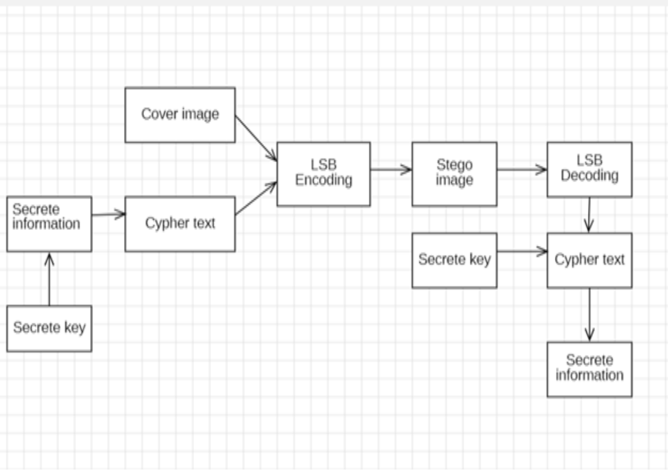

Fig -3.1: System Architecture

Algorithm Used: The system utilizes the AES (Advanced Encryption Standard) algorithm, a symmetric encryption algorithm known for its security in protecting confidential data. AES operates on plaintext of 128 bits with variable key lengths of 128, 192, and 256 bits, performing 10, 12, and 14 rounds respectively. This algorithm ensures data confidentiality and privacy by using a single key for both sender and receiver sides.

A. Least Significant Bit Least Significant Bit is one of the spatial domain techniques where each bit if the text or the image is substituted from the least significant bit of the original image. It is simple and easy to implement. The specialty of its existence in spatial domain is because the human eye cannot distinguish between the original and encrypted image . LSB can be extended up to 4-bits or 2-bits out of 8-bits, but it may cause distortion in an image due to change in the intensity of an image. LSB substitution comprises of

1. LSB Encoder 2. LSB Decoder

LSB technique has become the basis of many techniques that hide the secret data within the carrier data. First section explains about the encoding process where the secret data is hided and next section explains about the decoding process where the data gets extracted.

1. Input the secret data i.e. text or the image which needs to be hidden.
2. Input the cover (original) image of size
3. Convert the secret data i.e. asci value of each text or pixel value in case of image into binary representation.
4. Convert the pixel value of cover image into binary representation.
5. Apply LSB encoder; function is to hide each bit of text or image into the least significant bit of each 8 pixel value of cover image.
6. The resultant output is converted back to pixel values to get the stego-image.

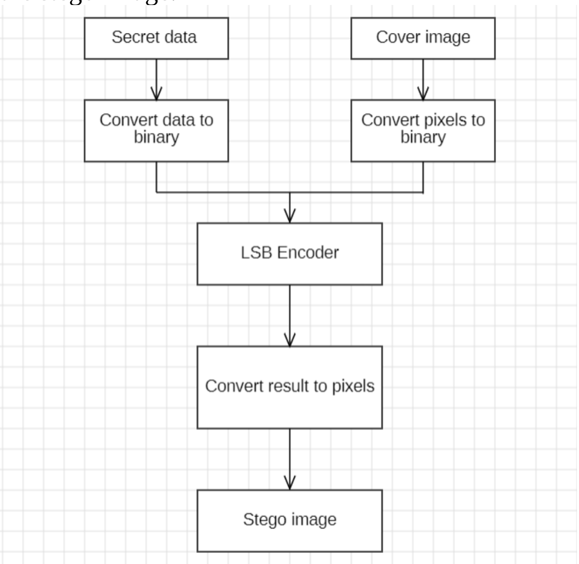

Fig -3.2: LSB Encoder

1. Input the stego image.

2. Convert the pixel value to binary representation.

3. Apply LSB decoder; function is to retrieve the secret data back from the stego-image.

4. The secret data and the cover image are separated together to get the desired output.

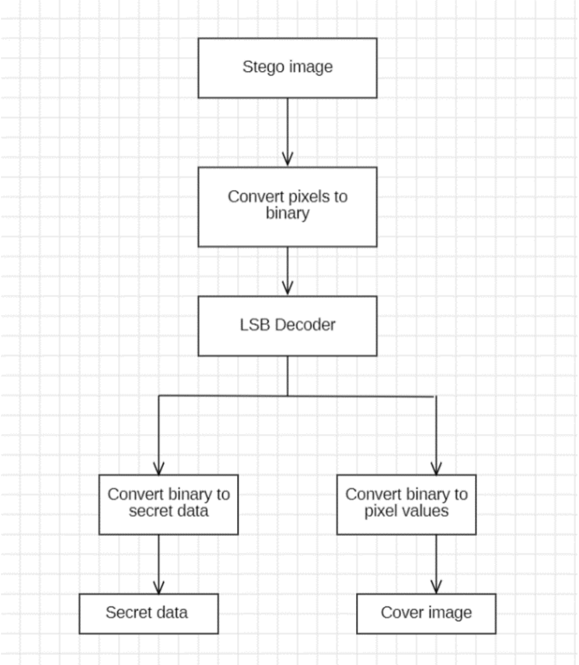

Fig -3.3: LSB Decoder

B. AES (Advanced Encryption Standard)

The AES algorithm is the symmetric algorithm that is secure enough to provide security for confidential data operating on plaintext of 128-bit with variable key length of 128, 192 and 256-bit [3]. The number of rounds performed is 10, 12 and 14 respectively. AES is one of the strongest algorithms until now and we can use only one key at the sender and receiver side, hence the privacy made by the key is secured.

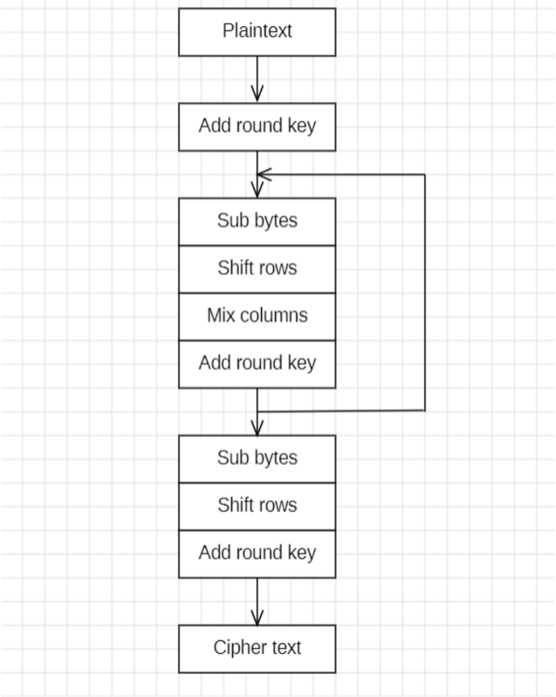

Fig -3.4: AES

4. SYSTEM FLOW DIAGRAM

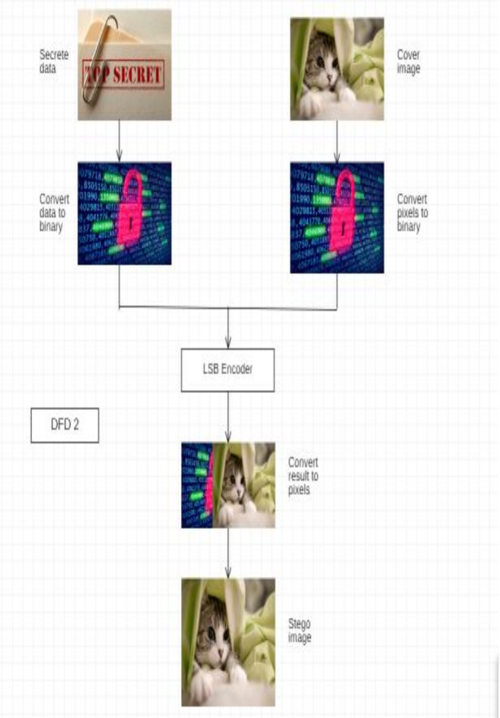

Fig -4.1: System Flow Diagram

4. IMPLEMENTATION

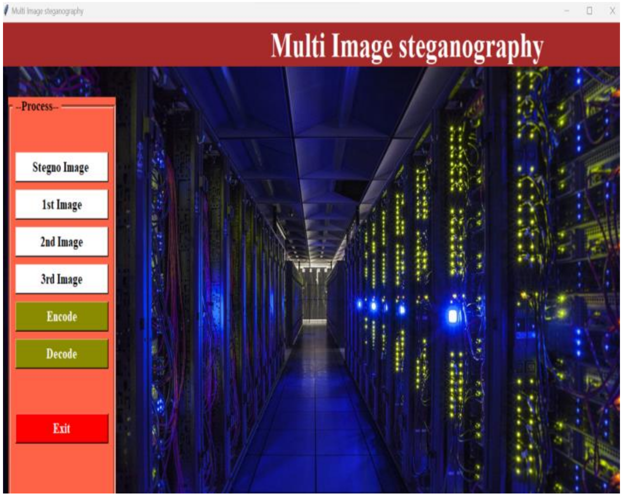

Fig -5.1: User Interface

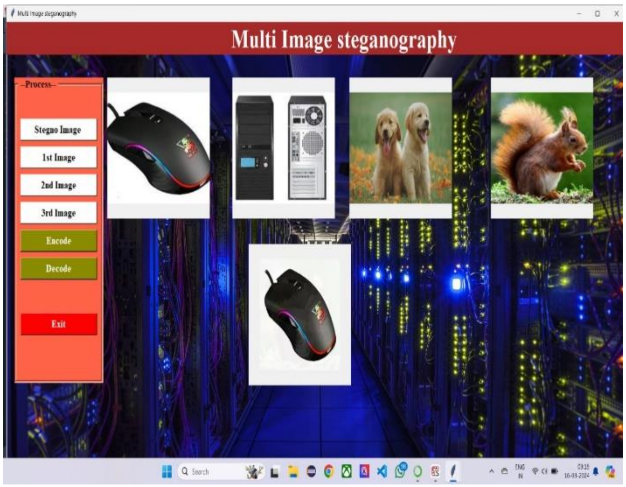

Fig -5.2: Encode

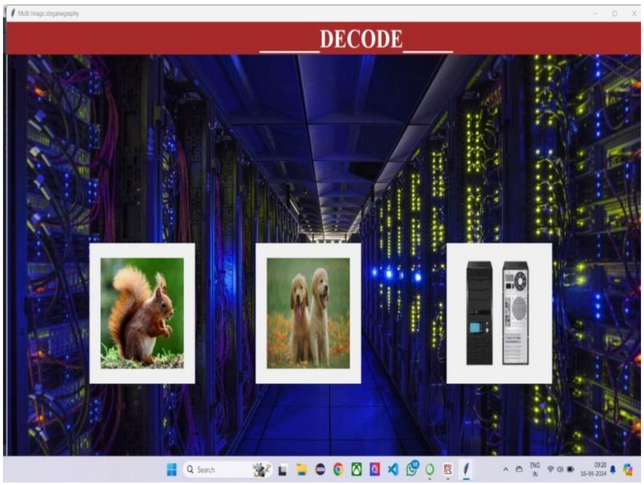

Fig -5.3: Decode

3. CONCLUSION

In this study, we employ the Least Significant Bit (LSB) technique to conceal confidential data within a cover image. The maximum number of characters embedded using this technique is 8192, while ensuring the secret image size is less than or equal to 80x80 pixels. To enhance the security of our concealed information, we implement the Advanced Encryption Standard (AES) algorithm with a key length of 128 bits. This key length is recommended by the National Institute of Standards and Technology (NIST) and offers superior security compared to other algorithms.

Our implementation in the MATLAB environment involves a comparison of Peak Signal-to-Noise Ratio (PSNR) and Mean Squared Error (MSE) for various images. The graphical representation illustrates an inverse relationship between PSNR and MSE. A lower MSE value indicates minimal error between the original and encrypted images, while a higher PSNR suggests better quality in the reconstructed image. The PSNR ratio falls within the range of 45-70 dB, and MSE ranges from 0-1.This research focuses on concealing either text or an image within another image. Subsequent investigations will explore the concealment of audio and video within an image. Additionally, there is potential to enhance security by increasing the key length used in the AES algorithm.

The prospective areas of expansion for this document involve the exploration of novel steganography techniques and algorithms, aiming to enhance the security of concealed information. There is potential for further research to be conducted, focusing on the development of more streamlined and potent approaches for data concealment and safeguarding against unauthorized access. Furthermore, the document can be enriched by incorporating the latest advancements and applications within the realm of steganography.

REFERENCES

1. Priya Paresh Bandekar and Suguna G C" LSB based text and image steganography using AES algorithm" Proceedings of the International Conference on Communication and Electronics Systems (ICCES 2018)
IEEE Xplore Part Number:CFP18AWO-ART; ISBN:978-1-5386-4765-3.0
2. Naldiyanto Sofian, Arya Wicaksana and Seng Hansun" LSB Steganography and AES Encryption for Multiple PDF Documents" 2019 5th International Conference on New Media Studies Bali, Indonesia | October 09-11, 2019
3. Utsav Sheth and Shiva Saxena" Image Steganography Using AES Encryption and Least Significant Nibble" International Conference on Communication and Signal Processing, April 6-8, 2016, India
4. Rajrishi Sengupta and C. Umarani "Steganography Using Python " IITM Journal of Management and IT Volume 12, Issue 1 • January-June 2021.
5. Manoj Kumar Ramaiya, Naveen Hemrajani and Anil Kishore Saxena "Security Improvisation in Image Steganography using DES" 2013 3rd IEEE International Advance Computing Conference (IACC) 978-1-4673-4529-3/12/$31.00_c 2012 IEEE
6. Nazmun Nahara, Md. Kawsher Ahmedb, Tareq Miahc, Shahriar Alamd, Kh. Mustafizur Rahmane, Md. Anayt Rabbi "Implementation of Android Based Text to Image Steganography Using 512-Bit Algorithm with LSB Technique" 2021 5th International Conference on Electrical Information and Communication Technology (EICT) | 978-1-6654-0906-3/21/$31.00 ©2021 IEEE | DOI:10.1109/EICT54103.2021.9733441 17-19 December 2021, Khulna, Bangladesh
7. Shashank guptai, Rachit Jain "An Innovative Method of Text Steganography" 2015 Third International Conference on Image Infonnation Processing 978-1-5090-0148-4/15/$31.00© 2015 IEEE
8. Sahib Khan#, Nasir Ahmad#, Muhmmad Ismail#, Nasru Minallah#, Tawab Khan "A Secure True Edge based 4 Least Significant Bits Steganography" 978-1-5090-0436-2/15/$31.00 ©2015 IEEE
9. Md. Rashedul Islam1, Ayasha Siddiqa2, Md. Palash Uddin3, Ashis Kumar Mandal4 and Md. Delowar Hossain "An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography" 3rd International Conference On Informatics, Electronics & Vision 2014 978-1-4799-5180-2/14/$31.00 ©2014 IEEE
10. Eko Hari Rachmawanto, Rofi' Syaiful Amin, De Rosal Ignatius Moses Setiadi and Christy Atika Sari "A Performance Analysis StegoCrypt Algorithm based on LSB-AES 128 bit in Various Image Size" 2017 International Seminar on Application for Technology of Information and Communication (iSemanic