IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Special Issue 2, March 2023

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

| International Conference on Recent Innovations in Engineering and Technology (ICRIET'23)|

| Sharadchandra Pawar College of Engineering, Pune, India |

|| Volume 11, Special Issue 2, March 2023 ||

Review Paper on Steganography

Humbe Rupesh, Khond Pranesh, Ukirde Rohan, Prof. K.D. Dere

UG Student, Dept. of C.S., JCOE, SPPU University, Pune, India

Assistant Professor, Dept. of C.S., JCOE, SPPU University, Pune, India

ABSTRACT: This research paper aims to deliver the knowledge about the Steganography technique which uses ciphering through images. Encryption is the most satisfying approach for the Data Protection but nowadays technology has been evolved ina way that Data leakage can be Disastrous due to high-end computers to have enough power to Decipher the Data that has been hidden. A huge number of messages are circulated over the internet and carry private data which requires the security and protection. The Project involves the use of Discrete Cosine Transforms (DCT) technique and Advanced Encryption Standards (AES) in Steganography which will keep attackers away from the Data. The hidden text can only revealed or retrieved through deciphering the image. The methodology is for securing the private information or confidential Data in harmless Environment with under controlled situations.

KEYWORDS: DCT, AES, Steganography, Encryption

I. INTRODUCTION

Steganography is performed to protect data from theft, which can be done in many ways. the text hidden under the images is the method we are looking to develop in a application. the project is based on discrete transform (dct) technique which will be used for hiding text under the image. the retrieval of the image needs decoding from the platform. the project aims to secure data or private information by encryption and decryption of the image. the proper communication between platforms will help secure the data without the third party interference which will cause damage to the data, and the information will loose its confidentiality. a large

Volume of data travels through internet which interact with platforms to communicate with one another, which requires the proper intervention of a application or a platform that will ensure the safety of the data. The confidentiality, integrity, authenticity are the three most important factors that conveys that the data is safe. Cryptography ensures data protection through encryption and decryption in current scenario, but the many issue is that the attackers probably now are smart enough to decipher the encrypted data to leak or tamper it. The projects proposes is a solution to ensure the security for the confidential data that is transferred through today's available platforms for communication. The mobile devices are drastically used nowadays, hence an android/ios based application will be efficient to the current scenario of data security as well as for the future with more improvised system and technology. The project ensures the secure data transferring while communication within various platforms such as android/ios.

MOTIVATION

To limit unauthorized access and provide a better security while communication or message transmission. To hide the data from any kind of Censorship or discovery of that information. Steganography is equal to copy protection that means if you cant see the data, you cant copy that data or message. If a message is hidden behind the image or the media it is hard for any attacker to suspect the hidden information under that image so the chances of data theft are less and the data will be transmitted without any interference from the external or the attacker.

II. RELATED WORK

DESCRETE COSINE TRANSFORM (DCT): In the paper, DCT transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into high and low frequency components. Embedding in DCT domain is simply did by altering the DCT coefficients. DCT transformation and compression using quantization and run-length coding on raw images can be used to obtain secure steganography images.

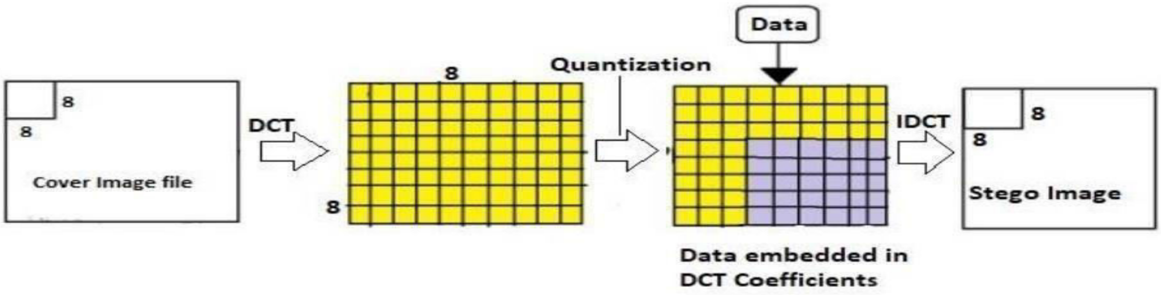


Fig. Working of Discrete Cosine Transform

ADVANCED ENCRYPTION STANDARD (AES): In the paper, The Advanced Encryption Standard (AES) is a fast and secure form of encryption that keeps eyes of attacker away from our data. The earliest types of encryptions were simple, using techniques like changing each letter in a sentence to the one that comes after it in the alphabet. As people got better at cracking codes, the encryption had to become more sophisticated so that the messages could be kept secret.

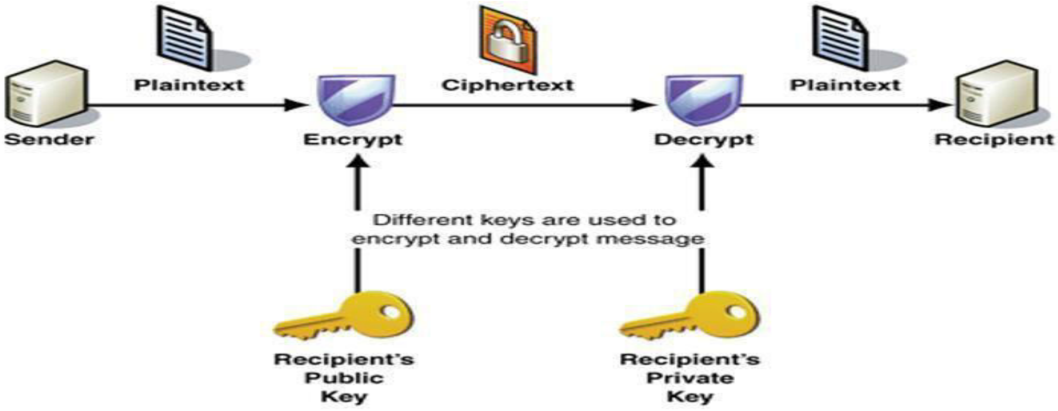
Stego App: Android based Image Steganography Application using LSB

In this paper, I got to know that Steganography is used with Least Significant Bit (LSB)Technique. First, the cover image and the secret data to be hidden is loaded into the application after that user can add password if wanted then LSB algorithm is used to replace the last bit of every byte of cover image with secret image. After embedding data (text or image) into the cover image successfully the stego image is obtained.

III. EXISTING SYSTEM

Cryptography

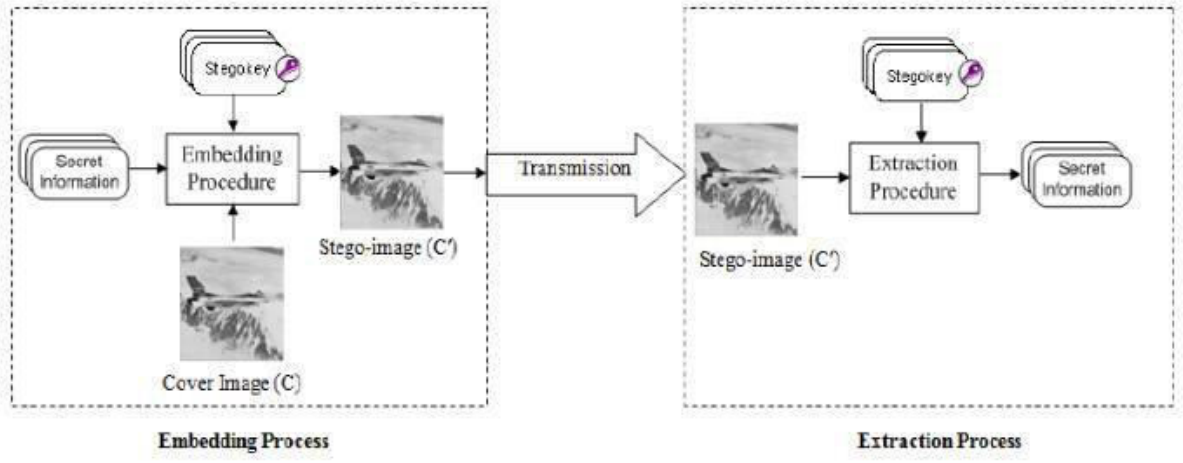
The security of network is vital component in data transfer and communication form one public network to another. The techniques that are used for the network security are Stegnography and Cryptography.. Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it. Cryptography converts the data into unreadable format for the unsanctioned user. and decodes the data into the readable form and allow it be transmitted only for the authorized users. The Public key encryption and Private key encryption is used in the existing technique. Public Key Encryption : public key encryption is associated with the creator or sender for encrypting information. Private key Encryption : private key is also named as secrete key. Secret keys are only shared with the key's generator or authorized party to decrypt the data.



Steganography

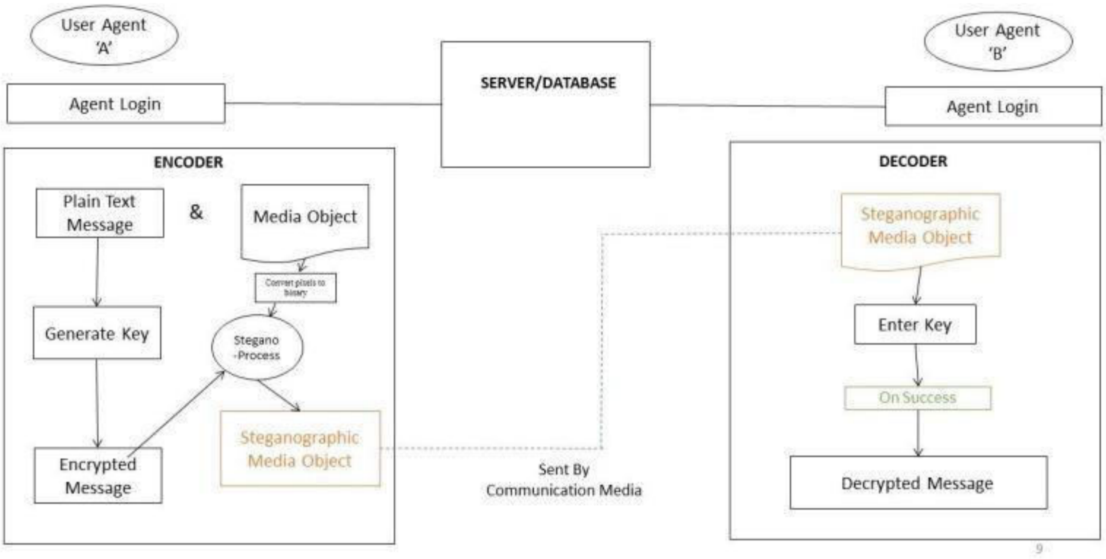
Steganography is said to be hiding the secrete data into within the ordinary data. That means it is the practice of representing information within another message or physical object, in such a manner that the presence of the information is not evident to human inspection. The steganography basically works on the hidden data and the cover data. The data that we want to keep it secrete is known as the hidden data and the data under which secrete data is stored is known as the cover data.

In existing system the image encryption and decryption algorithms is used by using AES-128 bit core. hence the image information is converted into the hexadecimal data using the MATLAB code. Then hexadecimal information is transmitted via UART (Universal Asynchronous Receiver/Transmitter.).for the decryption same process is used.



IV. SYSTEM ARCHITECTURE

Below figure shows the proposed system architecture where the encryption side functioning is handle by the Agent 'A' and the decryption side functioning is handle by the Agent 'B'. for both user 'A' and user 'B' side must have to go through for the login and then the agent have access to use the encryption and the decryption process. Image media object, plain text message and key is required at the encryption side then the Steganographic Media Object is given as a output by the stegano process. that steganographic media object is send to the user Agent 'B'. User Agent 'B' takes a steganographic media object (the output of encryption side) as an input. The user authentication process will takes place by entering the key which is used in the encryption side processing. After completing the successful authentication the user will be able to perform the decryption process to see the decrypted information into the plain text.



V. CONCLUSION

In this paper, a steganography technique is used to hide a message within image . after the change in bit values a part of data may be lost, the embedded message is added to the image after the change in bit stage. Image Steganography refers to the process of hiding data within an image file. such a way that no one can doubt for the existence of the secrete message apart from the sender and considered recipient. each pixel considered a less significant bits for the embedding. The pixel bits are increased or decreased. A strong encryption algorithm is used to encode the message and then embedded into a carrier by using steganography. With this technique we have proposed our plan to build a system to hide the secret data into the cover image using steganography and AES method of encryption that are combined to achieve much stronger encryption routines. The results implicate that our method is able to keep secret data while the quality of the stego image is almost similar to the original.

REFERENCES

[1] Darbani, A., AlyanNezhadi, M. M., & Forghani, M. (2019, February). A new steganography method for embedding message in JPEG images. In 2019 5th conference on knowledge-based engineering and innovation (KBEI) (pp. 617-621). IEEE.

[2] Bandekar, P. P., & Suguna, G. C. (2018, October). LSB Based Text and Image Steganography Using AES Algorithm. In 2018 3rd International Conference on Communication and Electronics Systems (ICCES) (pp. 782-788). IEEE.

[3] Dahiya, M., & Kumar, R. (2018, December). A Literature Survey on various Image Encryption & Steganography Techniques. In 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC) (pp. 310-314). IEEE.

[4] Astuti, Y. P., Rachmawanto, E. H., & Sari, C. A. (2018, March). Simple and secure image steganography using LSB and triple XOR operation on MSB. In 2018 International Conference on Information and Communications Technology (ICOIACT) (pp. 191-195). IEEE.

[5] Watni, D., & Chawla, S. (2019, October). A comparative evaluation of jpeg steganography. In 2019 5th International Conference on Signal Processing, Computing and Control (ISPCC) (pp. 36-40). IEEE.

[6] Elharrouss, O., Almaadeed, N., & Al-Maadeed, S. (2020, February). An image steganography approach based on k-least significant bits (k-LSB). In 2020 IEEE. International Conference on Informatics, IoT, and Enabling Technologies (ICIoT) (pp. 131-135). IEEE

[7] Zhang, Q., & Ding, Q. (2015, September). Digital image encryption based on advanced encryption standard (aes). In 2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC) (pp. 1218-1221). IEEE.

[8] Kaur, H., & Kakkar, A. (2017, September). Comparison of different image formats using LSB Steganography. In 2017 4th International Conference on Signal Processing. Computing and Control (ISPCC) (pp. 97-101). IEEE.

[9] Saleh, M. A. (2018). Image steganography techniques-a review paper. Ijarcce, 7(9), 52-58.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING