Data Hiding Inside Image Using Cryptography Algorithm (RC6) And Steganography

Senthil Kumar T[*], Dinesh S[**], Harini K[**], Pavithra T[**], Sanjay kanth G[**]

*** Assistant Professor, IT, Hindusthan Institute of Technology**

**** Student, Final year, IT, Hindusthan Institute of Technology**

ABSTRACT--- Cloud-based data is safer than paper and client-server records. There are lots of security issues related to storage, which will make lots of security challenges. Cryptography is an essential tool that helps to assure our data accuracy. Cryptographic techniques can be employed to protect the data in the cloud environment. This paper presents a novel approach for data hiding inside images using both cryptography and steganography techniques. The proposed method utilizes the RC6 encryption algorithm to securely encrypt the data before embedding it into the image using steganography. The RC6 algorithm provides robust security by generating a secret key that is required to decrypt the hidden data. The steganography technique is used to embed the encrypted data into the least significant bits of the cover image to minimize distortion and make the hidden data imperceptible to the human eye. The experimental results demonstrate the effectiveness of the proposed method in terms of the high capacity of data hiding, low distortion, and strong security. This approach has various applications in the field of digital image security and can be used to transmit confidential data securely over untrusted networks.

Keywords: Cryptography, Steganography, RC6, Least Significant Bit (LSB), Data Hiding, Image Security.

Introduction:

Data hiding inside an image using a cryptography algorithm (RC6) and steganography is a technique that involves concealing information within an image file in such a way that it remains imperceptible to the naked eye. This approach combines the strengths of cryptography and steganography to ensure that data remains secure and undetectable. The RC6 algorithm is a symmetric-key block cipher that can encrypt and decrypt data using a secret key. This algorithm provides strong security, making it an ideal choice for data encryption in this technique. Steganography, on the other hand, involves embedding secret information into the least significant bits of an image's pixels. This process alters the pixel values only slightly, making it difficult for anyone to detect the presence of hidden data. By

combining RC6 encryption with steganography, this technique provides a robust approach to protecting sensitive information. The encryption ensures that even if the hidden data is discovered, it remains unreadable without the key, while steganography makes it challenging for anyone to detect the existence of secret data within the image.

Overall, data hiding inside an image using a cryptography algorithm (RC6) and steganography is an effective way to secure information while keeping it hidden from prying eyes.

Encryption process:

Encryption Algorithm is an algorithm used for the changing operation of plaintext encryption into ciphertext. The modified RC6 is done by changing the number of bits so that the constants of Pw and Qw are altered as well. For the RC6 algorithm, the value of Pw and Qw constants are 32 bits. The expansions of them have 8 digits with each digit containing 4 pixels.

RC6 Algorithm:

RC6 is a symmetric key block cipher encryption algorithm that was developed by Ron Rivest, Matt Robshaw, Ray Sidney, and Yiqun Lisa Yin. It is a modified version of the RC5 algorithm and is designed to be faster and more secure. The RC6 algorithm works by dividing the plaintext into blocks of 128 bits and then encrypting each block using a series of modular arithmetic operations. The key length can be any multiple of 32 bits, and the number of rounds can be customized based on the level of security required.

LSB Steganography:

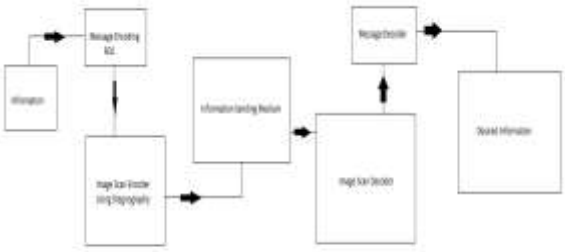
LSB (Least Significant Bit) steganography is a method of hiding secret data inside an image by modifying the least significant bits of the pixel values. The human eye is not sensitive to small changes in the least significant bits of the pixel values, so the changes are not noticeable. LSB steganography can be used to hide text, images, or other types of data inside an image. The process of LSB steganography involves dividing the secret data into small chunks and then replacing the least significant bits of the pixel values with the secret data.

Decryption process:

Decryption Algorithm is an algorithm used for the changing operation of decryption to plaintext. The conversion of encrypted data into its original form is called Decryption. It is generally a reverse process of encryption. It decodes the encrypted information so that an authorized user can only decrypt the data

because decryption requires a secret key or password.

Block Diagram:



Methodology:

The process of hiding data inside an image using a cryptography algorithm (RC6) and steganography methodology involves the following steps:

Step 1: Encryption of Data

First, the data that needs to be hidden inside the image is encrypted using the RC6 cryptography algorithm. This algorithm uses a secret key that is known only to the sender and receiver of the message. The encrypted data is then stored in a separate file.

Step 2: Selecting the Image

A suitable image is chosen for hiding the encrypted data. The image should be large enough to accommodate the data without affecting its quality.

Step 3: Encoding the Data

The encrypted data is then converted into a bit stream of 0s and 1s. This bit stream is then divided into groups of 3 bits each.

Step 4: Modifying the Image Pixels

The RGB values of the selected image pixels are modified to embed the 3-bit groups. This is done by altering the least significant bits of each pixel. The changes made to the RGB values are imperceptible to the human eye, and the image quality is not affected.

Step 5: Embedding the Encrypted Data

The modified pixels are then used to embed the encrypted data. This is done by embedding one 3-bit group in each pixel. The process continues until all the encrypted data has been embedded in the image.

Step 6: Saving the Image

The final step is to save the image with the embedded data. The image can now be transmitted to the intended recipient, who can use the same key and process to extract the hidden data.

Advantages:

1. Security
2. Authentication
3. Tamper-proofing
4. Capacity
5. Concealment
6. Ease of use

Disadvantages:

1. Limited capacity
2. Complexity
3. Detection
4. Quality loss

Conclusion:

In conclusion, data hiding inside an image using a combination of cryptography algorithm RC6 and steganography is an effective method for securely transmitting confidential information. The RC6 algorithm provides robust encryption of the data, while steganography ensures that the encrypted data is hidden within an image file. The advantage of this approach is that it allows for secure transmission of data without arousing suspicion since the image file appears to be a normal image file. Furthermore, the use of RC6 algorithm enhances the security of the hidden data by making it difficult for unauthorized parties to decrypt the data. However, it is important to note that this method of data hiding requires significant technical expertise in cryptography and steganography. Additionally, the size of the image file may increase, and it may affect the quality of the image. Therefore, careful consideration should be taken when selecting an appropriate image and encryption key to ensure that the image's quality is not significantly degraded, and the hidden data is protected. Overall, data hiding inside an image using the cryptography algorithm RC6 and steganography is a powerful technique for protecting sensitive information and ensuring secure transmission.

References:

[1]Chitra Biswas, Udayan Das Gupta, Md. Mokammel Haque, "An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography", IEEE International Conference on Electrical, Computer and Communication Engineering (ECCE), February 2012.

[2]Salim Ali Abbas, Malik Qasim Mohammed, "Enhancing Security of Cloud computing by using RC6 Encryption Algorithm", International Journal of Applied Information Systems (IJAIS), November 2017.

[3]ShengDun Hu, KinTak U, "A Novel Video Steganography based on Non-uniform Rectangular Partition", in the 14th IEEE International Conference on Computational Science and Engineering, 2011.

[4]Ako Muhamad Abdullah, "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data", published in Research Gate, 2017.

[5]Dnyanda Namdeo Hire, "Secured Wireless Data Communication", International Journal of Computer Applications, September 2012.