IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Impact Factor: 6.252

Volume 2, Issue 2, February 2022

Blur Image Enhancement with Data Encryption and Decryption using Cryptography and Steganography Algorithms

Jasvinder Kaur Deve, Neha Deo, Yukta Gajare
Guru Gobind Singh Polytechnic, Nashik, Maharashtra, India

Abstract: *This paper proposes an information hiding method behind blur image to embed data while executing image enhancement steps. In recent years, there has been an increasing interest in using the technology of multimedia. The privacy and security of data are the challenging task, during transmission time. This paper deals with hiding text in an image file using Advanced LSB algorithm in which bits are XORed with the least significant bits of cover image to derive the stego-image. In this we have also used AES (Advanced Encryption Standard) algorithm which is used to protect electronic data. Blur is a common in so many digital images. So, here Gaussian Blur technique is used for Image Blurring and De-Blurring..*

Keywords: Image Steganography, Encryption, Decryption, Advance encryption standard (AES), Information hiding, Cryptography, Image steganography, Security, Image quality

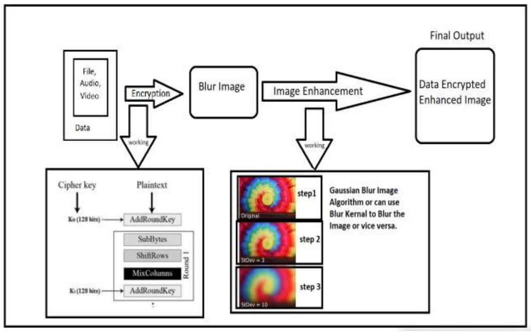
I. Introduction

In the new era of modern science and technology is developing day by day, data confidentiality is risky, all over the world and it increases rapidly [1]. In this paper, we are using Steganography and Cryptography to accomplish Information Security under Image Processing. Information hiding method is used to embed data while executing image enhancement steps [2]. Cryptography is the study of securing communications from outside observers. Steganography means secreting communication. It may be defined because the study of invisible communication that won't to hide the existence of the communicated data in such a way that it remains confidential. In this paper, a new approach is proposed based on AES (Advanced Encryption Standard), Advanced LSB and Gaussian Blur Algorithm.

The purpose of Blur Image Enhancement techniques is to avoid the loss of data and provide the double security to the confidential data. In this system we are using cryptography algorithm i.e. AES (Advance Encryption Standard) algorithm for encrypting the data. We get data from user and append it onto image and hide it by using steganography algorithm i.e. Advance LSB (Least Significant Bit) algorithm and also using Gaussian Blur Technique for Image Blurring.

One of the important technique is Video Steganography. In this technique to hide the secret information inside of video. The addition of this video is not recognized by unauthorized persons. Some of the popular techniques in Video Stenography are Advanced LSB. [3]

II. SYSTEM ARCHITECTURE



DOI: 10.48175/IJARSCT-2802A

III. METHODOLOGY

The System is divided into two parts that is Sender Side and Receiver Side. The Sender side is again divided into 5 modules that are

Input:

The data required for the encryption process is taken from user which will be in any format as provided that is textual format, or audio (mp3), or video (mp4). If user wishes to hide data in a specific Image he wants then the Image will be taken or else, random Image from Dataset will be chosen.

Conversion:

After Getting inputs, the image is converted into blur Image. In this, we are using Gaussian Blur which is widely used for Blurring the Image. The data provided by user into Encryption format by using AES Algorithm.

Gaussian Blur:

The Gaussian blur feature is obtained by blurring (smoothing) an image using a Gaussian function to reduce the noise level. It can be considered as a non-uniform low- pass filter that preserves low spatial frequency and reduces image noise and negligible details in an image. It is typically achieved by convolving an image with a Gaussian kernel.

This Gaussian kernel in 2-D form is expressed as :

G2Dxyσ=12πσ2e−x2+y22σ2

where σ is the standard deviation of the distribution and x and y are the location indices. The value of σ controls the variance as follows: around a mean value of the Gaussian distribution, which determines the extent of the blurring effect around a pixel. In the proposed image segmentation, we tested sigma values ranging from 0.1 to 16, such that, with an increase in sigma, the high- frequency information content reduces around the pixel. In our study, we use a standard deviation of 3 that generates the best segmentation results.

AES Algorithm:

The AES algorithm uses a substitution- permutation, or SP network, with multiple rounds to produce ciphertext. The number of rounds depends on the key size being used. A 128-bit key size dictates ten rounds, a 192-bit key size dictates 12 rounds, and a 256-bit key size has 14 rounds. Each of these rounds requires a round key, but since only one key is inputted into the algorithm, this key needs to be expanded to get keys for each round, including round 0. Steps in each round are : a)Substitution of the bytes, b)Shifting the rows, c)Mixing the Columns, d)Adding the Round Key.

Steganography Process:

Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. So, we are hiding the Encrypted data into Blur Image using Advance LSB of Steganalysis.

Advanced LSB :

Algorithm for embedding the message: Step 1. Input the Encrypted message using
AES Algorithm that to be hidden in the cover image.
Step 2. Select the cover image.
Step 3. Take pixels from cover image.
Step 4. Take the (LSB+1) bit from the pixel.
Step5. Divide the encrypted message in to two equal parts.
Step6. Perform XOR of first half of encrypted message with the odd position pixel values.
Step7. Perform XOR of second half of encrypted message with the even position pixel values.
Step8. Now get all the xored values of even and odd position pixel.
Step9. Now store the xored value of even in even position LSB bit of pixels. And xored value of odd in odd positioned pixel.

Image Enhancement:
The encrypted data blur image is enhanced to clear image.

Output:
At sender end the Image is received as Encrypted Enhanced Image.

Receiver Side:
Whole process took place vice versa.

IV. CONCLUSION

This Project presents that data is secured via old as well as new technologies. We are going to provide security to confidential data by encrypting data within the image and reducing the chances of data leakage. Cryptography is the study of securing communications from outside observers. Steganography means secreting communication. It may be defined because the study of invisible communication that won't to hide the existence of the communicated data in such a way that it remains onfidential. We therefore conclude that the consumer market will go in hand-in- hand with the use of Blur Image Enhancement with Cryptography and Steganography process in day-to-day life.

REFERENCES

[1] A New Approach to Hiding Data in the Images Using Steganography Techniques based on AES and RC5 Algorithm Cryptosystem
[2] INFORMATION HIDING IN IMAGE ENHANCEMENT
[3] ENCRYPTION AND DECRYPTION TECHNIQUES FOR VIDEO DATA
[4] Image And Audio Based Secure Encryption And Decryption

DOI: 10.48175/IJARSCT-2802A