IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Secure Information Transmission Using Steganography And Cryptography

[1]Pradyumna Alhad,[2] Abhinav Tonde,[3]Atharva Bhokare ,[4]Pratiksha Dabade, [5] Ms. Prachi Nilekar

[1,2,3,4] Students and [5] Asst. Prof. of Department of Computer Engineering,

Alard college of engineering and management, Pune.

Savitribai Phule Pune University, Pune, India.

Abstract: **Information and data security is most essential factor during transmitting secret information. We have used cryptography for data encryption and sending hidden data message in the form of text. Technology is changing day by day, so there are many techniques used for hiding information. The most important technique is steganography. In steganography , two different images are used for hiding information and the information is in the form of text, image, audio etc, can be used as a secret message. With the help of LSB Steganography. we can implement good level of information security without any damage to cover image. In this project we are going to use hybrid approach i.e. cryptography and Steganography. So, the system has higher security level than existing systems.**

Keywords- Cryptography, Steganography, AES algorithm, face recognition, CNN (Convolutional Neural Network)

1. 1. INTRODUCTION

Information security is important aspect at the time of transmitting secret information. In ancient Greece there was attempt to hide a message and deliver it across the enemy territory. Basically, we make use of cryptography for message hiding and sending message in the form of text. Today in the world of digital communication, there are various techniques used for hiding data in any medium. One of that is steganography. in which images are used to hide the information and the information in the form text, image, audio and video file may be used as secret message. The word steganography is obtained from two Greek words: steganos and graphos. steganos means covered and graphos means writing and often refers to data hiding. In this project we use the below methods to provide security and data hiding

1. Cryptography:
2. Steganography

LSB Steganography, AES algorithm Technique can implement secured level information and security methods without any destruction to cover image. In Least Significant Bit (LSB) is a technique the last bit of each pixel is modified and replaced with the secret messages data bit. AES have in built and good flexibility of key length, that allows a degree of "future proofing" against progress in order to perform exhaustive key searches. For example, It is 128 bits long, that means, AES would be able operate on 128 bits of plaintext to produce 128 bits ciphertext.

1.2. MOTIVATION

- Information security plays an important role in every information transfer security and can be obtained by hiding the information that mainly focuses on covering the existence of secret messages.
- Steganography is message hiding technique which focuses on to hide the existence of the communication and make other parties unaware of the contribution of Stenographic exchange.

1.3. PROBLEMSTATEMENT

In today world, Information security is a tough challenge for any communication systems. Cryptography and steganography is the way of hiding sensitive information in another transmission medium and By enhancing more security to it by the use of machine learning.

1.4. OBJECTIVES

- The main objectives of this project are:
- Huge importance of the steganography system is that, Hidden message that are carried by stego-media shouldn't be accessible to human beings.
- The technique of message hiding technique has recently become an benefical in a number of application area.
- To Secure the data transfer system with high tech security login techniques.

1.5. SCOPE OF THE PROJECT

- The project scope is developed for hiding information in many image files and access this system with high security Login method with the help of Face Recognition as well the User ID and Password will provide High security of exchange the data between different organisation parties and provides good security during message transmission.
- The scope of the project is implemented using steganography tools for hiding information includes any types of the information file and image file and the path where the user wants to save images and extruded file.
- We will be using LSB technique which is used for steganography algorithm for embedding the data in an image files for military application.

1.6. EXISTING SYSTEM

- Cryptography can be used to provide message confidentiality and integrity and sender verification. The basic function of the Cryptography encryption, decryption and Cryptography is hashing. Hashing is a technique that generates a fixed length of string from the message of arbitrary length.
- If the Sender provides a cryptographic hash with the message, the recipient can verify its integrity. Modern cryptographic methods are based on complex mathematical relationships and processes.

2.1. MATHEMATICAL MODEL

Discrete Wavelet Transform, based on the concept of Multi-Resolution Analysis, can be applied to each signal examined. The studied input (ECG, PPG, Holter) signal can be represented by a wavelet function φi, j and scaling function ψi,n.

$$\varphi_{i,j}(t)=2^{-i/2}\varphi_0(2^{-i}t-j),\ j\in Z;$$
$$\psi_{i,j}(t)=2^{-i/2}\psi_0(2^{-i}t-j),\ j\in Z.$$

In the implementation of the wavelet transform, the digital signal x(t)∈ L2(R) is represented as the sum of orthogonal scaling functions and wavelets collection of details and a low-resolution approximation:

$$x(t) = approx_N(t) + \sum_{i=1}^{N} detail_i(t) =$$
$$\sum_j a_x\,(N,j)\,\varphi_{N,j}\,(t) + \sum_{i=1}^{N}\sum_j d_x\,(N,j)\,\varphi_{N.i}\,(t)$$

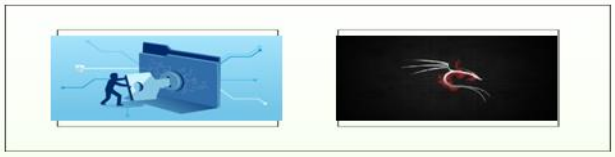
At each subsequent level *i* of the wave decomposition of the data, the corresponding signal energy is calculated, using the current values of the detailed coefficients *D* (*i*, *j*), total *K* for the respective level:

$$E_{Di} = \sum_{j=1}^{K}(D\,(i,j))^2$$

A Discrete Wavelet Transform (DWT) is a transform that decomposes a given signal into a number of sets, where each set is a time series of coefficients describing the time evolution of the signal in the corresponding frequency band.

2.2. ALGORITHM

Step 1 : Start
Step 2 :Login Authentication:-
  i.UserID
  ii.Password
  iii.User face Image
Step 3 :AES algorithm is used for encryption.
  i. Use of 64 bit key.
Step 4 : Step of DES is used.
Step 5 : Conversion ofalgorithm ciphered text into 2 different parts.
  i.CipheredPart1
  ii.CipheredPart2
Step 6 :Use of Steganography technique.



Step 7 :Uploads this SteganoImages to server.
Step 8 :Steganalysis
Step 8.1:Extraction of Ciphered Text
Step 8.2: Merging of extracted Text
Step 8.3: Decryption of cypher text to plain text
Step 9 :End

3.1. SYSTEM ARCHITECTURE

Fig. 3.1 shows the System Architecture, In above system , Sender imputs secret data in the system. After inputing secret data, system does encryption on secret data and divide the cipher text into two parts. The two parts of cipher text is then hidden within the cover images which is taken from user inputed images and the LSB technique method is applied on the cipher text, then the hidden message within the images is send to the receiver. At the receiver end, user will use steganalysis on the stego images. after unstegoing images, it will use AES decryption algorithm to decrypt the cipher text and merge plain text and then secret data is retrieved and the secret message is displayed.

- LSB Steganography hides the given information stored at a particular position of the LSB in the image.
- Put the binary representation of the hidden message, overwrite the LSB of each and every byte within the cover image.
- Formula: cover image + secret key + hidden message = stego image
- Good LSB method is used for hiding secret messages written in text file of color image.
- Each character of the secret image is converted into its equivalent ASCII value and then each code is converted into 8 bit binary, and each bit is inserted into the last LSB of each pixel of the cover image.

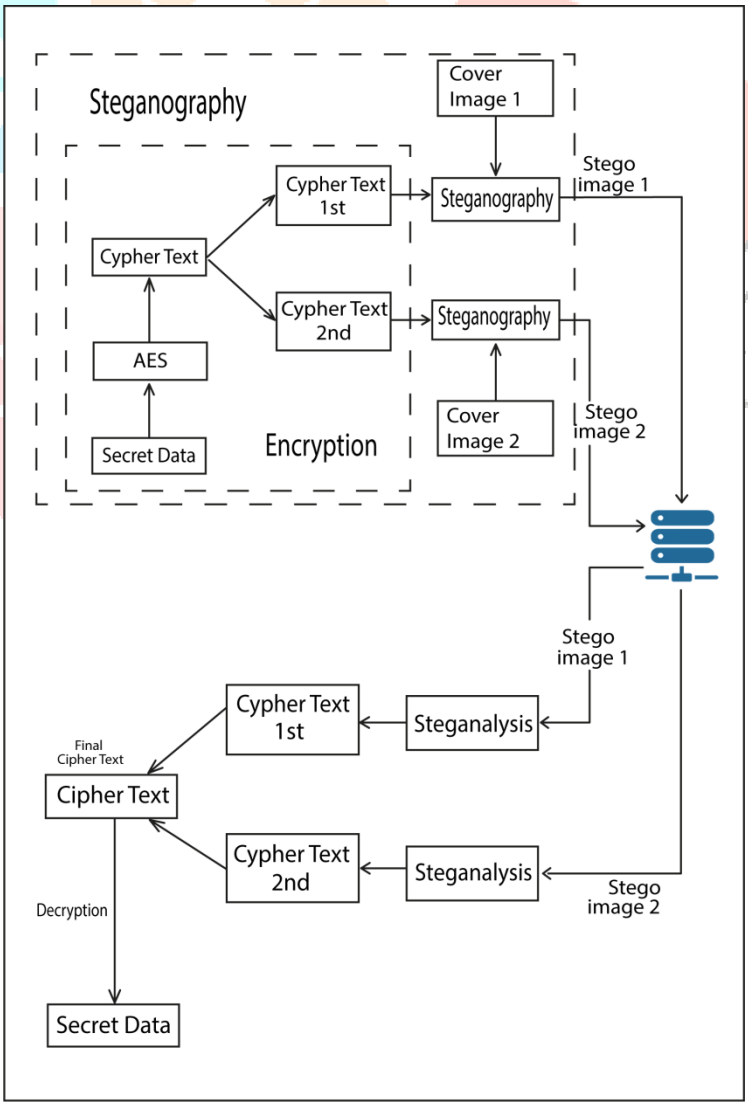


Fig.3.1. System Architecture

3.2. RESULT

The important packages of Python programming language has been installed and the code is being implemented using PyCharm Integrated development environment (IDE) and the python code we have developed runs in both Python 2.7 and Python 3.x.

3.3. OUR APPROACH

- We have executed hybrid approach (cryptography + steganography)
- So, our system has better security level than existing systems.
- Our approach provides two way security mechanism using cryptography and steganography.

3.4. ADVANTAGES

- Using LSB Technique we can implement high level of information security without any damage to cover image.
- LSB Steganography has very less MSE value (Mean square error) as compared to DWT & Other techniques
- LSB steganography has more PSNR value as compared with DCT & DWT steganography
- As LSB has good performance in terms of MSE & PSNR, it becomes very daunting task for hackers to hack the information.

4.1CONCLUSION

- In this project, we have made use of high level of data security without any damage to cover image using LSB technique. ˆ
- It will be almost impossible for any hackers to attack the stego Image because cover image and stego image looks vert similar. ˆ
- In this project, with steganography we have also used cryptography i.e. we have first encrypted our text message and divide the cipher text and then embedded it into the two image file i.e two stego image. This approach helps us to achieve more security, in case anyone intercepts our transmission. Moreover two image file is used as a cover medium because we can embed more data into it as compared to other cover mediums.

4.2. REFERENCES

1. Prateek Kumar Singh, Pratikshit Tripathi, Rohit Kumar, Deepak Kumar, IRJET, Secure Data Transmission, Volume: 04 Issue: 04 — Apr2017.
2. Dalia Nashat* and Loay Mamdouh,An efficient steganographic technique for hiding data.
3. Mustafa Sabah Taha, Mohd Shafry Mohd Rahim, Sameer abdulsattar lafta, Mohammed Mahdi Hashim, Hassanain Mahdi Alzuabidi, Combination of Steganography and Cryptography: A short Survey, ICSET 2019
4. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica ridrich, Ton Kalker," Digital Watermarking and Steganography"
5. Hussein L. Hussein, Ahmed A. Abbass, Sinan A. Naji, Salam Al-augby and Jasim H. Lafta, Hiding text in gray image using mapping technique, IOP Publishing 2018
6. Deepesh Rawat and Vijaya Bhandari, Steganography technique for hiding text information in color image using improved LSB method, IJCA 2013
7. Mehdi Hussain, A survey of image steganography techniques, IJAST 2013
8. Hamad A. Al-Korbi, Ali Al-Ataby, Majid A. Al-Taee and Waleed AlNuaimy, Highly efficient image steganography using Haar DWT for hiding miscellaneous data, JJCIT 2016