ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 3, March 2019

Data Hiding Using Steganography Combined Cryptography

S.Loga Priya, M.Saraiyu, R.Premalatha

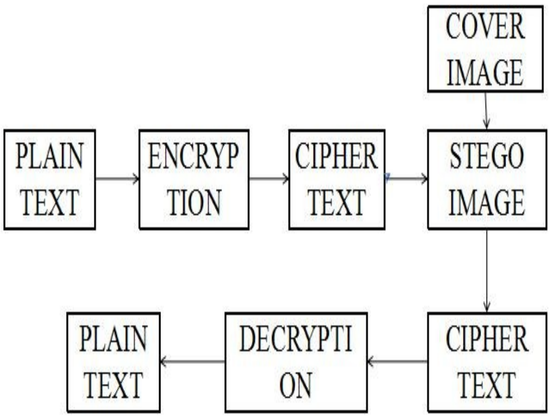
Department of ECE, Builders Engineering College Tirupur, Tamilnadu, India

ABSTRACT: Information security is the major issue in this technological world. Securing the confidential information from the access of unauthorized user is very difficult. There are lot of techniques to secure the informtion. One of them is steganography which is used to hide an secret message within an ordinary data. The other technique is an cryotography which scrambles the information into cipher and encrypt the secret messages. Both the techniques provides better security. The proposed method combines both the techniques and thus security level can be increased.

KEYWORDS: Steganography, Cryptography, LSB, DWT and 3DES.

I. INTRODUCTION

Cryptography is an encryption method which converts information into cipher text so that only intended user can read and perform it. Cipher text is also known as encrypted or encoded information because it contains a oreiginal plain text that is unreadable by human or coumpter without proper decrypting algoriyhm. Steganographyis the art of hiding secret messages in the way recepient only know about the hidden messages. Both the techniques plays vital role in computing. The cipher text are vulnerable to cryptanalysis and the steganography techniques can be easily detected. To provide better security both the techniques can be combined. If any of the system fails, the Secret message remains safe because of encoding technique.The steganography and cryptography are the two sides of a coin where the steganography hides the traces of communication while cryptography uses encryption to make the message incomprehensible. By combining these two techniques, messages can be hidden in various multimedia files such as text, audios, images and videos with dual layers of security.



DOI: 10.15680/IJIRCCE.2019. 0703025

This model provides a dual layer of security by combining both cryptography and steganography. It consists of four stages namely encryption, embedding, extracting and decryption. The plain text is converted to a cipher text using a cryptographic algorithm , after which the cipher text is embedded into a cover image using steganographic algorithm.

II. OVERVIEW OF CRYPTOGRAPHY AND STEGANOGRAPHY TECHNIQUES

This section gives different kinds of cryptography and steganography techniques.

I.CRYPTOGRAPHY

Symmetric key algorithms: This uses the same cryptographic keys for both encryption of plain text and decryption of cipher text.

RC4

RC4 is a stream cipher developed by Ron Rivest. It is well known for its simplicity and speed.Its key length is between 40 and 2048 bits.

AES

It also known by its original name Rijndael algorithm. It uses three different key lengths 128, 192 and 256 bits respectively.

3DES

Tripple data encryption algorithm, is a symmetric key block cipher, which applies algorithm three times to each data block. It is easy to implement in both hardware and software. Key sizes are 168,112 or 56 bits.

Asymmetric key algorithm: This algorithm uses two different keys private key and public key to encrypt and decrypt the datas.

RSA

It is developed by Ron Riverst , Adi Shamir and Leonard Adleman. Key sizes are between 1,024 to 4096 bits.

2.STEGANOGRAPHY

Image steganography

It refers to hiding information such as text , audio, images within an image based on pixel intensities.

Audio steganography

This technique is used to transmit hidden information by modyfiying an audio signal. Here cover object is audio file.

Text steganography

It hides the text behind some other text file. It is a difficult form of steganography as the redundant amount of text to hide the secret message is scarce in text files.

Video steganography

This technique is used to hide any kind of files into a cover video file. This is more secure than other multimedia files, because of its size and complexity.

DOI: 10.15680/IJIRCCE.2019. 0703025

III.METHODOLOGY

The proposed work implements combined cryptography and steganographic algorithms. The confedential text will be encrypted with the 3DES encryption and the key,which will be used for decryption. Then the cipher text will be embedded into the cover object using steganographic LSB and DWT algorithms. In the encryption module , both the secret key and secret data gets encrypted. It performs the following operations on secret key and secret data. Select the secret data and a suitable secret key for encryption. Convert the secret key into one-dimensional (1-D) array of bits. Apply the bit xor operation on these bits with logical 1.Shuffle these encrypted bits such that the bits with even and odd indices . If secret key bit =1,Then perform bit xor operation of secret message bit with logical 1. Else, Do not perform bit xor operation. After this mapping module is responsible for mapping the secret encrypted data into the carrier image pixels. Before mapping, the carrier image channels are transformed and then a 1-1 mapping between secret data bits and image pixels is maintained. In the embedding module, the inputs are cover colour image ,secret key, secret data and the output is an stego image which contains the secret images. These all operations are performed on the transmitter side .

Least Significant Bit (LSB) embedding is a simple strategy to implement steganography. Like all steganographic methods, it embeds the data into the cover so that it cannot be detected by a casual observer. The technique works by replacing some of the information in a given pixel with information from the data in the image. While it is possible to embed data into an image on any bit-plane, LSB embedding is performed on the least significant bit(s). This minimizes the variation in colors that the embedding creates. The least significant bit technique works well for media files, where slightly changing byte values creates only slight imperceptible changes, but not so well for things like ASCII text, where a single bit out of place will completely change the character.

In the receiver side, to read the secret information extracting technique is performed which is the reverse process of embedding. Then to read the cipher text , using decryption technique which is the reverse process of encryption the cipher text is converted into a plain text. Considering the security aspects, proposed algorithm is more secure than existing as it uses dual level security which uses symmetric key sharing. Image quality is degraded for gray images as compared with the colour images. Figure 2a is the original image to which the secret data is to be hidden. Then figure 2b is the stego image which contains the secret information.

Figure2a: Original image

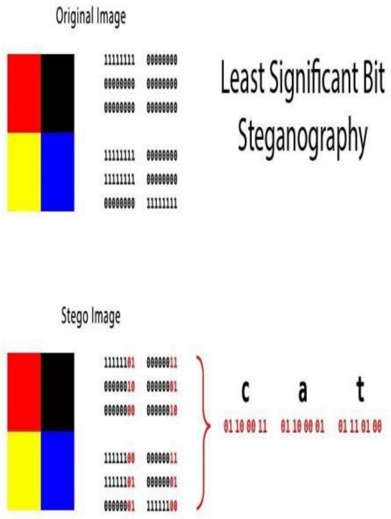
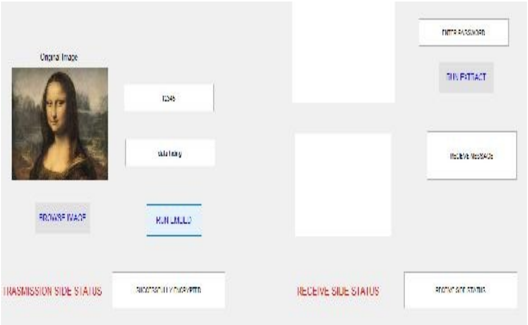


Figure 2b: Stego image

Figure3: embedding process



IV.RESULTS AND DISCUSSION

The main intention of this work is to provide multi layer security. To examine the performance of the proposed technique performance parameters like PSNR, MSE have been evaluated.

PSNR(PEAK SIGNAL-TO-NOISE RATIO)
Peak signal-to-noise ratio, often abbreviated PSNR, is an term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale.

PSNR is most easily defined via the mean squared error (MSE). Given a noise-free m×n monochrome image I and its noisy approximation K, MSE is defined as:

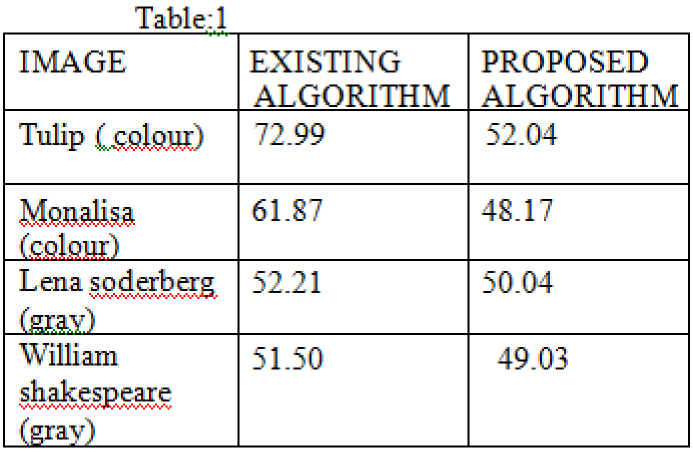


Table:1

IMAGE	EXISTING ALGORITHM	PROPOSED ALGORITHM
Tulip (.colour)	72.99	52.04
Monalisa (colour)	61.87	48.17
Lena soderberg (gray)	52.21	50.04
William shakespeare (gray)	51.50	49.03

This method gives better quality for the colour images , compared with gray images which is slightly degraded.

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

The PSNR (in dB) is defined as:

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

V. CONCLUSION AND FUTURE WORK

Ensuring data security is a big challenge faced by the users. To make the datasecure from the various attacks, both steganography and cryptography are combined together. It uses effecient steganographic algorithm LSB for data embedding and 3DES algorithm for data encryption to increase the levels of security. The performance of this algorithm is verified by the parameters like PSNR and MSE . The proposed algorithm provides better results for colour images with dual layer security.By accurately observing the visual quality, the process of DWT and LSB can be better improved to achieve the more satisfactory results.

VI. ACKNOWLEDGEMENT

This work is supported by Mr.M.Prakash (AP/ECE), Builders Engineering college, Tirupur , Tamilnadu.

REFERENCES

1. P.Joseph and S,Vishnukumar,"A study on steganographic techniques,"2015 Global IEEE conference on Communication (GCCT),Thuckalay, 2015,pp.206-210.doi:.1109/GCCT.2 015.7342653
2. S.Chandra,S.Alam and G.Saynal,"A comparative survey of Symmetric and Asymmetric Key Cryptography,"2014 IEEE International Conference on Electronics,Communication and computational Engineering (ICECCE),Hosur,2014,pp.83-93.doi: 10.1109/ICECCE.2014.7086640
3. A Novel Approach of Watermarking for Multiple Images with DWT-DCT by P.Srilakshmi, Ch.Himabindu and suvarna on 2017 IEEE.
4. "A Single, Triple Chaotic Cryptography Using Chaos in Digital Filter and Its Own Comparison to DES and Triple DES"by Reatrey Pich,Sorawat Chivapreecha,Jaruwit Prabnasak on 2018 IEEE.
5. N.Kumar and S.Agrawal,"An efficient and effective lossless symmetric key cryptography algorithm for an image,"2014 IEEE International Conference on Advances in Engineering & Technology Research (ICAETR -2014),Unnao,2014,pp.1-5.doi:10.1109/ICAETR.2014.7012788