International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-9 Issue-2, July 2020

Information Security using Cryptography and Image Steganography

G. Mallikharjuna Rao

Abstract*: Typically, hackers are ready to hack the confidential documents for their vested interests. The main challenge is to construct a secure relation between the secret message and image quality. To avoid dangerous illegal attacks by the third person, a scheme is proposed to have a combination of cryptography and image steganography techniques. This scheme will enable the security, secret message and image cannot be extracted. The International Data Encryption Algorithm (IDEA) cryptographic algorithms and Discrete Cosine Transform (DCT) based steganography algorithm is chosen for the functionality. Cryptography is used to encrypt and decrypt the document. Steganography to hide document inside an image with increasing payload for the secure transmission of confidential data across the internet. In this paper we present a single application to hide the information by the sender, which is so important document and confidential in the form of files, it will be invisible to unauthorized person. The results of a suggested scheme with respect to PSNR of 90.06 dB with a payload of 52,400 bytes of information in an image.

Keywords: **Data Hiding, cryptography, steganography, Image processing, DCT, IDEA.**

I. INTRODUCTION

In a computerized world, there is a rapid increase in digital data transmissions over the network. The sender and the beneficiary are the two important persons, where they are trying to communicate with each other. People are trying to communicate over the network. Therefore, millions of people are relying on digital world, in such a case, security is the foremost factor.

To overcome this overwhelming situation, data hiding techniques are used for the protection of the secret data [1]. In the means of communication, data hiding plays a key role to preserve the details of the host and the beneficiary. At the same time, while streaming the image on the network, it should not be hacked by the third person.

In the existing framework the extension is restricted to content of documents just without encryption. The current framework is to show a single application, having both cryptography and image steganography.

Manuscript received on May 25, 2020.
Revised Manuscript received on June 29, 2020.
Manuscript published on July 30, 2020.
***** Correspondence Author
G. Mallikharjuna Rao*, ECE department, Affiliated to Osmania University, Hyderabad, India. Email: mallikharjunag@gmail.com

A. Information Security Techniques

Data Hiding techniques plays a key role to protect the data from the third person. In order to fix the security, authentication, authorization, data integrity is achieved by data Hiding techniques [2]. There are ways, where these techniques are classified into cryptography, steganography, and watermarking. In this paper work, we have proposed to use both Cryptography and steganography. Cryptography is to change the original data; Steganography is to hide original data in an image. We have different approaches to hide the information as shown in fig 1.

1) Cryptography

The cryptography technique is a mathematical model to change the plain text into cipher text using an encryption method. The applied methods are known by the intended persons only.

In cryptography, there are two methods of classification, one is symmetric key cryptography and another one is public-key cryptography methods. Symmetric key cryptography is an encryption standard, where both the parties use the same key for encryption and decryption of messages.

a) Block cipher

Block ciphers are widely used in cryptography algorithms for encrypting huge data into chunks. The plain text is divided into the fixed size of chunks, while the encryption process is generated with a fixed key size. The key length decides the algorithm strength, where IDEA is a symmetric key block cipher.

Stream cipher

There are methods like stream cipher, and block cipher to streamline the data. In case of stream cipher, the data bit is combined with a pseudo-random key to generator a ciphertext. In order to process the data, they are grouped into blocks.

The blocks are encrypted using a key, the normal key size may vary, typical block size is 64 bits. The execution of the block ciphers is much faster than the stream ciphers.

B. Steganography

Steganography is a split word, where stego is secret, graph is writing, it's nothing but secret writing of data into a cover file [3].

Usually, the key generation will depend upon the algorithm and based on the problem of effective security. Depending upon the cover file the steganography methods are classified as

1) Text steganography

The secret data is embedded into a text file. After embedding the binary format of the secret data with the public key, it generates an embedded file without disturbing its quality of a text file.

2) Audio steganography

The audio cover file is embedded with secret data. Here the binary form of the secret data is stored in a selected bit version and generates the stego audio file using audio steganography techniques.

3) Image steganography

The image file is used to hide the secret binary data. The Secret data is embedded into the selected pixel location by using a transform domain method or spatial domain method [4,5]. To apply image steganography, the secret data is embedded into the selected images as shown in Fig. 2.

4) Video steganography

Video file is a combination of audio and number of frames or images. Therefore, the secret binary data can be stored in images or audio format. It has a large capacity to store The Secret data and provides high security when compared to other techniques. In this paperwork, we have chosen the image steganography method.

II. RELATED WORK

The biggest challenge in the data hiding schemes is to invade a huge amount of data into an image without losing the quality assurance with security. The major strength of the techniques is attacks against hackers. There are several schemes suggested by the authors, to hide a huge amount of data into an image. [6,7] the author identified the modern techniques in hiding data to attain good results. The researcher has given scope to understand the methods like LSB and EMD [8].

Least significant method is a very popular method, which can be used for dealing with the data within images. In this method, the least significant bit of an image pixel is replaced with secret information. This particular method will not impact human visual impairment. Therefore, it is one of the useful methods among Data Hiding techniques. [9,10].

The author explains the Exploiting Modification Direction (EMD) technique [11]. The basic operation of the technique is to partition the image into several groups of pixels. Where the group of pixels is loaded with the secret message array encoding system. While insertion process the pixel, rate grouped inside may increase or reduce the pixels by 1. But the major problem in this method is the image quality assurance, it is due to the group has two pixels.

The researcher developed a traditional EMD method using each pixel in an image to embed secret message [12]. This advanced technique doubles the information storage into an image. Even the quality of the image is retained.

The researcher opted for a technique called opt EMD, where the relation between the number of pixels in a group embedded in an image has reduced the distortions [13]. The method helps in achieving high image quality. However, the method is affected by the amount of payload.

The author has introduced a method of Huffman coding, affine cipher, and knight tour methods. The method emphasizes to encode the secret message into a compressed affine cipher and Huffman coding. The Secret message is embedded into an image using LSB and knight tour algorithm. [14]

The researcher explains the method of improved EMD and Huffman coding Method [15]. The Secret message is segmented into two subgroups among the group of pixels. The Segmented groups may contain two and three pixels are in sequential order to increase the payload without losing image quality.

The author has introduced the Data Hiding scheme to increase the quantity of information embedded in an image using EMD method [16].

The author has suggested a method where LSB is to increase the numerous amounts of payload and increase the intensity of secret message.

He has suggested using the knight tour method and EMD scheme for embedding the secret message into a cover image [17]. The author has introduced an EMD method, the image is divided into n number of pixels that are embedded into 2K-n ary in a row [18-20].

III. SUGGESTED SCHEME

In this paper, it is suggested to combine the cryptography and the steganography methods. The main aim of this work is to establish a secret messages and images between end-to-end sender and receiver communication. To achieve this, a combination of cryptography and steganography methods are used as shown in Fig. 2. To attain the approach, encrypt the information and hide them in an image. Insert information with increasing payload without reducing the quality of image.

The steps proposed in the suggested scheme:

1. Encryption process: The secret message is encrypted using International Data Encryption Algorithm (IDEA) method.
2. Embedding process: The secret message is appended into an image and apply discrete cosine transform.
3. Extraction process: By applying inverse discrete cosine transform obtain the original image and extract the secret message.
4. Decryption Process: The secret message is Decrypted using Inverse International Data Encryption Algorithm (IDEA) method.

A. *Encryption process algorithm*

The International Data Encryption Algorithm standard is represented with similar key and block cipher [21]. Proposed Encryption Standard (PES) is replica of IDEA, later Improved Proposed Encryption Standard (IPES) name is replaced with IDEA. It is a 64- bit plain text encrypted into 64-bit cipher with 128-bit key. The IDEA is processed with 8 similar rounds and one-half round.

It consists of three major operations.

total rounds = 8, plain text block size = 64 -bit, 16 * 4 (Sub blocks)

Therefore, sub-blocks: X_1, X_2, X_3, X_4 (Concatenated Sub blocks)

Each round = 6 (subkeys)
Where key =128-bit = 8 * 16-bit blocks (which is nothing but 8 subkeys)
Out of eight subkeys, six subkeys are allocated in round one. Two subkeys are allocated round two.
All rounds access the algebraic operations

1. Bitwise XOR (16- bit blocks)
2. Addition modulo 2^{16}
3. Multiplication modulo $2^{16}+1$ (zero is not an element)

The steps involved in encryption process of IDEA structure is

Step 1: $X_1 = X_1 \odot Z_1$ (Where Z_1, Z_2, Z_3, Z_4, Z_5, Z_6, Z_7, Z_8 are subkeys)
Step 2: $X_2 = X_2 \boxplus Z_2$
Step 3: $X_3 = X_3 \boxplus Z_3$
Step 4: $X_4 = X_4 \odot Z_4$
Step 5: Results of step 1 $\oplus$ step 3.
Step 6: Results of step 2 $\oplus$ step 4.
Step 7: Result of step 5 $\odot$ Z_5.
Step 8: Results of step 6 $\boxplus$ step 7.
Step 9: Result of step 8 $\odot$ Z_6.
Step 10: Results of step 7 $\boxplus$ 9.
Step 11: Results of step 1 $\oplus$ 9.
Step 12: Results of step 3 $\oplus$ 9.
Step 13: Results of step 2 $\oplus$ 10.
Step 14: Results of step 4 $\oplus$ 10.

Round 1 result = $X_1 \| X_2 \| X_3 \| X_4$ = Results of (step 11 || step 13 || step 12 || step 14).

Similarly, round 2, round 3, round 4, round 5, round 6, round 7 and round 8.

After completion of 8th round, a round 9 (half round) is final change, is executed as :

Step 15: $X_1 = X_1 \odot Z_1$
Step 16: $X_2 = X_2 \boxplus Z_2$
Step 17: $X_3 = X_3 \boxplus Z_3$
Step 18: $X_4 = X_4 \odot Z_4$

Round 9 result = $X_1 \| X_2 \| X_3 \| X_4$ = Results of (step 15 || step 16 || step 17 || step 18). The blocks output is concatenated.

1) *KEY SCHEDULING*

Round1… Round 8 = 6 subkeys (Where Z_1, Z_2, Z_3, Z_4, Z_5, Z_6, Z_7, Z_8 are subkeys) as shown in Table 1:
Round 9 (Half round) = 4 subkeys
Total keys required = (48 + 4) = 52 subkeys

Key size = 128-bit, 1 subkey = 16-bits. Then 25-bits left shift, where 128-bit = 16-bit blocks * 8 becomes subkeys.

The splitting of bits and 25-bit shifting operation is continued till 52 subkeys are obtained. Where no two keys are similar to eachother is given in Table -I.

From the final 4 subkeys are used in the ninth "half round" final transformation.

B. *Embedded process algorithm*

The steps involved in basic process of Discrete Cosine Transforms as follows:

Step 1: The input image is of size N by M pixels, where N-number of rows, M – number of Columns.

Step 2: Consider the intensity of pixel f (i, j), where i[th] -row nd j[th]-column;

Step 3: The DCT coefficients F (u, v)

$$F(u,v) = \left(\frac{2}{N}\right)^{\frac{1}{2}}\left(\frac{2}{M}\right)^{\frac{1}{2}}\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}\Lambda(i)\,.\,\Lambda(j)\,.\,cos\left[\frac{\pi.u}{2.N}\right](2i+1)\,.\,cos\left[\frac{\pi.v}{2.M}\right](2j+1\,.\,f(i,j) \quad (1)$$

Where

$$u = 0,1,2,\ldots\ldots N-1, v = 0,1,2,3\ldots.M-1$$

Table-I: Encryption key subblocks

Round 1	$z_1^{(1)}$ $z_2^{(1)}$ $z_3^{(1)}$ $z_4^{(1)}$ $z_5^{(1)}$ $z_6^{(1)}$
Round 2	$z_1^{(2)}$ $z_2^{(2)}$ $z_3^{(2)}$ $z_4^{(2)}$ $z_5^{(2)}$ $z_6^{(2)}$
Round 3	$z_1^{(3)}$ $z_2^{(3)}$ $z_3^{(3)}$ $z_4^{(3)}$ $z_5^{(3)}$ $z_6^{(3)}$
Round 4	$z_1^{(4)}$ $z_2^{(4)}$ $z_3^{(4)}$ $z_4^{(4)}$ $z_5^{(4)}$ $z_6^{(4)}$
Round 5	$z_1^{(5)}$ $z_2^{(5)}$ $z_3^{(5)}$ $z_4^{(5)}$ $z_5^{(5)}$ $z_6^{(5)}$
Round 6	$z_1^{(6)}$ $z_2^{(6)}$ $z_3^{(6)}$ $z_4^{(6)}$ $z_5^{(6)}$ $z_6^{(6)}$
Round 7	$z_1^{(7)}$ $z_2^{(7)}$ $z_3^{(7)}$ $z_4^{(7)}$ $z_5^{(7)}$ $z_6^{(7)}$
Round 8	$z_1^{(8)}$ $z_2^{(8)}$ $z_3^{(8)}$ $z_4^{(8)}$ $z_5^{(8)}$ $z_6^{(8)}$
Round 9	$z_1^{(9)}$ $z_2^{(9)}$ $z_3^{(9)}$ $z_4^{(9)}$

In an image maximum energy of the signal is under lower frequencies. These frequencies exist in the upper left corner of Discrete Cosine Transform. Where image compression is obtained by supressing higher frequencies appearing at lower right corner values.

Step 4: The DCT input is an 8 * 8 integer array.
Each pixel = 8-bit gray scale. Gray scale level value ranges from 0 to 255.

Step 5: The output array of data coefficients are integer values; it ranges from -1024 to 1023 for F[0,0].

The basis function of 2D array of image data can be generated to multiply the 1D array horizontal data array with vertical data array with a set of basis functions.

C. *Decryption process algorithm*

IDEA decryption method is same as encryption with different key generation.

Where k_i^j denotes round i, jth decryption key.
z_i^j denotes round i, jth encryption key.

Therefore, decryption key for round 1: $k_1^1 = \left(z_1^{(9)}\right)^{-1}$ (multiplicative inverse of encryption key of round 9)

$k_1^1 = -z_2^{(9)}$ (additive inverse of encryption key of round 9)

$k_1^3 = z_5^{(3)}$, $k_1^4 = \left(z_4^{(5)}\right)^{-1}$, $k_1^6 = z_4^{(6)}$.

Similarly, the dectyption keys are same as generated in the decryption round 1, …… round 9. In case of round 9, $k_1^9 = \left(z_1^{(1)}\right)^{-1}$ $k_9^2 = -z_2^{(1)}$ $k_9^3 = -z_3^{(1)}$ $k_9^4 = \left(z_4^{(1)}\right)^{-1}$.

The decryption keys are shown in Table 2.
All rounds access the algebraic operations

1. Bitwise XOR (16- bit blocks)
2. Addition modulo 2^{16}
3. Multiplication modulo $2^{16}+1$ (zero is not an element)

The steps involved in decryption process of IDEA structure is

Step 1: $X_1 = X_1 \odot K_1$ (Where K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_8 are subkeys)
Step 2: $X_2 = X_2 \boxplus K_2$
Step 3: $X_3 = X_3 \boxplus K_3$
Step 4: $X_4 = X_4 \odot K_4$

Step 5: Results of step 1 ⊕ step 3.
Step 6: Results of step 2 ⊕ step 4.
Step 7: Result of step 5 ⊙ K5.
Step 8: Results of step 6 ⊞ step 7.
Step 9: Result of step 8 ⊙ K6.
Step 10: Results of step 7 ⊞ 9.
Step 11: Results of step 1 ⊕ 9.
Step 12: Results of step 3 ⊕ 9.
Step 13: Results of step 2 ⊕ 10.
Step 14: Results of step 4 ⊕ 10.
Step 15: $X_1 = X_1 \odot K_1$
Step 16: $X_2 = X_2 \boxplus K_2$
Step 17: $X_3 = X_3 \boxplus K_3$
Step 14: $X_4 = X_4 \odot K_4$

Round 1 result = $X_1 \| X_2 \| X_3 \| X_4$ = Results of (step 11 ‖ step 13 ‖ step 12 ‖ step 14).

Similarly, round 2, round 3, round 4, round 5, round 6, round 7 and round 8.

After completion of 8th round, a round 9 (half round) is final change, is executed as:

Step 15: $X_1 = X_1 \odot K_1$
Step 16: $X_2 = X_2 \boxplus K_2$
Step 17: $X_3 = X_3 \boxplus K_3$
Step 18: $X_4 = X_4 \odot K_4$

Round 9 result = $X_1 \| X_2 \| X_3 \| X_4$ = Results of (step 15 ‖ step 16 ‖ step 17 ‖ step 18). The blocks output is concatenated.

D. *Extraction process algorithm*

The steps involved in basic process of Inverse Discrete Cosine Transforms as follows:
Step 1: The input image is of size N by M pixels, where N-number of rows, M – number of Columns.
Step 2: Consider the intensity of pixel f (i, j), where i[th] -row and j[th]-column;

$$f(i,j) = \left(\frac{2}{N}\right)^{\frac{1}{2}}\left(\frac{2}{M}\right)^{\frac{1}{2}} \sum_{n=0}^{N-1}\sum_{m=0}^{M-1} \Lambda(i)\,.\,\Lambda(j)\,.\,cos\left[\frac{\pi.m}{2.N}\right](2i+1).cos\left[\frac{\pi.n}{2.M}\right](2j+1\,.\,F(u,v) \quad (2)$$

Where *i= 0, 1 ,2, ……. N-1 and j= 0,1, 2……. M-1.*

To retrive the original image using above equation (2). is applied on an image

Table- II: Decryption key subblocks

Round 1	$(z_1^{(9)})^{-1} - z_2^{(9)} - z_3^{(9)} (z_4^{(9)})^{-1}\ z_5^{(8)}\ z_6^{(8)}$
Round 2	$(z_1^{(8)})^{-1} - z_2^{(8)} - z_3^{(8)} (z_4^{(8)})^{-1}\ z_5^{(7)}\ z_6^{(7)}$
Round 3	$(z_1^{(7)})^{-1} - z_2^{(7)} - z_3^{(7)} (z_4^{(7)})^{-1}\ z_5^{(6)}\ z_6^{(6)}$
Round 4	$(z_1^{(6)})^{-1} - z_2^{(6)} - z_3^{(6)} (z_4^{(6)})^{-1}\ z_5^{(5)}\ z_6^{(5)}$
Round 5	$(z_1^{(5)})^{-1} - z_2^{(5)} - z_3^{(5)} (z_4^{(5)})^{-1}\ z_5^{(4)}\ z_6^{(4)}$
Round 6	$(z_1^{(4)})^{-1} - z_2^{(4)} - z_3^{(4)} (z_4^{(4)})^{-1}\ z_5^{(3)}\ z_6^{(3)}$
Round 7	$(z_1^{(3)})^{-1} - z_2^{(3)} - z_3^{(3)} (z_4^{(3)})^{-1}\ z_5^{(2)}\ z_6^{(2)}$
Round 8	$(z_1^{(2)})^{-1} - z_2^{(2)} - z_3^{(2)} (z_4^{(2)})^{-1}\ z_5^{(1)}\ z_6^{(1)}$
Round 9	$(z_1^{(1)})^{-1} - z_2^{(1)} - z_3^{(1)} (z_4^{(1)})^{-1}$

IV. RESULTS

The significant objective behind this investigation is to hide a huge amount of data with a high security and safeguard the image quality simultaneously. Six different test images of size 512 * 512 pixels TIFF images were collected from USC-SIPI Data Base (USC-SIPI) [22] and used to assess the recommended method. The images shown in Fig. 5, are most widely used by the researchers for quality assurance in the field of information security. These figures are used for the case study and experimenting with it. Image steganography application development tool for encryption embedding extraction and decryption is as shown in Fig. 6.

Using this application, the first step is to collect the original text file in English alphabets used as a payload as shown in Fig. 7. There text file is encrypted using IDEA algorithm as shown in Fig. 8. The long length keying is used for better approximation of keys applied on the algorithm; we can evidence that the encrypted text is an unreadable form as shown in Fig 9. and Fig 10.

The airplane F16 is a case study it's a combination of encrypted text file Undercover image as shown in Fig. 11, applying the DCT algorithm converting it into density questions where the actual picture is invisible as shown in Fig. 12. Again, at the receiver side inverse discrete Fourier transform is applied to extract the stego image as shown in Fig. 13. Extraction process is applied on the image so that it separates the encrypted file from the image. Here using a decryption tool and password we can obtain the original text as shown in Fig. 14, Fig. 15, and Fig. 16.

The results evident that the encryption and decryption of the text file with high accuracy. Similarly, the embedding and extraction of the stego image and this Fig. 17 image outcomes are high quality.

Here we have applied three measuring metrics to analyze the image quality. One is mean square error which is used to quantify the average mistakes among the pixels of the image

The stego image whose values are calculated by the formula given below in the equation (3):

$$MSE = \frac{1}{m*n}\sum_0^{m-1}\sum_0^{n-1} \|CI(i,j) - SI(i,j)\|^2 \quad (3)$$

CI represents the matrix data of our original image
SI represents the matrix data of our degraded image in question
m represents the numbers of rows of pixels of the images and i represents the index of that row
n represents the number of columns of pixels of the image and j represents the index of that column

Another matrix is peak to signal noise ratio to calculate the quality of thing test images by comparing the original image and the stego image to state the value of human visual system, which is greater than 30 db, implies that the picture quality is good for the viewers.

Therefore, PSNR value is calculated on different images using the equation (4):

$$PSNR = 20 * log_{10}\left(\frac{max_f}{\sqrt{MSE}}\right) \quad (4)$$

max_f is the maximum signal value

Another major matrix which speaks about the similarity are likeliness amount the images. Here we're trying to compare the cover image and the stego image to state about the structural similarity index metrics. The range of SSIM. The similarity matrix is calculated by using the equation given below in the equation (5):

$$SSIM(x,y) = \frac{(2*\mu_x\,\mu_y + c_1)(2*\sigma_{xy} + c_2)}{(\mu_x{}^2 + \mu_y{}^2 + c_1)(\sigma_x{}^2 + \sigma_y{}^2 + c_2)} \quad (5)$$

μ_x $-$ *mean values of cover image* (x) *and*
μ_y $-$ *mean values of stego image* (y)
σ_x $-$ *Standard deviation of cover image* (x)
σ_y $-$ *Standard deviation of stego image* (y)
c_1 , c_2 $-$ *constant value to fix the division*

Table- III shows the data set of images in terms of PSNR, MSE, SSIM for different payloads and different test images trusted by the researchers. The test images which are used for the case study is providing accurate results once after conducting an experiment by using different algorithms.

In this paperwork as per the suggested scheme the different payloads are considered with respect to the other researchers those have contributed on the same experimenting. We can evident the results of lena, Baboon, aeroplane, Tiffany, peppers and a Man. Each image is of size 512 X 512 the to TIFF format is considered as a standard test image.

At the same time fixed payload size is considered to calculate the PSNR MSE and SSIM of six different images. These metrics will be sure about the quality, quantity and similarity. In order to check the suggested scheme with respect to the old schemes with the same payload on different images. Therefore, four (Lena, Baboon, Airplane F16, Tiffany) images are considered for the test the old schemes. Table- IV comprises the understanding between the suggested scheme and old schemes. The psnr value is 89.3059 dB of a suggested scheme when compared toena, Baboon, Airplane F16, Tiffany) to the old scheme is 55.71 dB for 52400-bytes payload. The EMD method [19], Opt EMD [23] and LSB data [9] limits beyond 49,152-bytes are overflow. It is observed the experiment results are more efficient then the older schemes to increase the payload within an image without loosing image quality.

In Table- V four different images Lena, Baboon, airplane, Tiffany, are considered for the comparisons by applying different methods as they were compared with respect to the suggested scheme with an older scheme [13]. According to the results observed in the tablular column, the suggested scheme is more efficient it maintains good quality after retreiveing the image. Even the text message is also not lost when compared to old methods discussed by other researchers.

V. CONCLUSION

The major goal of this scheme was to examine the association between cryptography and steganography. Steganography methods are used to store huge amount of information inside an image without destroying the image quality. A keen observation of the methods, it is observed that the suggested scheme of merging cryptography and steganography protects the secret message and image quality. Firstly, the Secret messages encrypted using the IDEA algorithm in order to protect the data and to increase the security of the suggested scheme. Then the encrypted message is compacted to minimize the message size and to increase the payload in an image. Subsequently, the compressed encoded message is inserted within an image using DCT method. The scheme is evaluated by considering certain measures of image quality using PSNR, MSE, and SSIM with different payloads. It is evident that the quality of the image and the payload suggested scheme is better than the earlier schemes. Further, it is observed that the suggested scheme is reliable in protesting the cyber-attacks. There is a lot of scope to work with a combination of steganography and cryptography to have a protest against image and text data.

REFERNCES

1. Zeyad SafaaYounus, Mohammed KhaireHussain, " Image steganography using exploiting modification direction for compressed encrypted data", Journal of King Saud University - Computer and Information Sciences, pp. 1-13, 2019..
2. Aiswarya, S. Gomathi, R., "Review on Cryptography and Steganography Techniques in Video" 2018 IEEE International Conference on Computational Intelligence and Computing Research, ICCIC 2018, pp. 119-122, 2018.
3. Morkel, T., Eloff, J., Olivier, M., 2005. An overview of image steganography. Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005). Sandston, South Africa. 2005.
4. Kumar, V., Kumar, D., Performance evaluation of modified color image steganography using discrete wavelet transform. J. Intell. Syst., 2017.
5. Wang, H., Wang, S., “Cyber warfare: steganography vs. steganalysis. Commun.” ACM 47, 10. 2004.
6. Kalra, M., Singh, P., “EMD techniques of image steganography a comparative study”. Int. J. Technol. Explor. Learn. 3 (2). 2014.
7. Hashim, M., Rahim, M., “Image steganography based on odd/even pixels distribution scheme and two parameters random function” J. Theor. Appl. Inf. Technol. 95 (22), pp. 5977–5986, 2017.
8. Chang, C., Tai, W., Chen, K., Improvements of EMD embedding for large payloads. In: Third International Conference on International Information Hiding and Multimedia Signal Processing (IIH-MSP 2007). ACM, pp. 473–476, 2007,
9. Chan, C., Cheng, L., Hiding data in images by simple LSB substitution. Pattern Recogn. 37, pp. 469–474, 2004,
10. Shjul, A., Kulkarni, U., “A secure skin tone-based steganography using wavelet transform. Int. J. Comput. Theory Eng. 3 (1), 16–22.
11. Lee, C., Wang, Y., Chang, C., “A steganography method with high capacity by improving exploiting modification direction. In: IEEE Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP), pp. 497– 500, 2007,
12. Jung, K., Yoo, K., “Improved exploiting modification direction method by modulus operation”, Int. J. Signal Process. Image Process. Pattern. 2 (1), pp. 79–87, 2009.
13. Lin, K., Hong, W., Chen, J., Chen, T., Chiang, W., n et al. “Data hiding by exploiting modification direction technique using optimal pixel grouping. In: IEEE 2010 2nd international Conference on Education Technology and Computer (ICETC). 2010.
14. Mohsin, A.T., A New Steganography Technique Using Knight’s Tour Algorithm, Affine Cipher and Huffman Coding (Master Thesis). Faculty of Computer Science and Information Systems, Universiti Teknologi Malaysia. 2013.
15. Ahmad, A., Sulong, G., Rehman, A., Alkawaz, M., Saba, T., Data hiding based on improved exploiting modification direction method and huffman coding. J. Intell. Syst. 23 (4), pp.451–459, 2014.
16. Alsaffawi, Z.S.Y., Image steganography by using exploiting modification direction and knight tour algorithm. J. Al- Qadissiya Comput. Sci. Math. 8 (1), pp.1– 11, 2016.
17. Lee, C., Chang, C., Pai, P., Liu, C., Adjustment hiding method based on exploiting modification direction. Int. J. Netw. Security 17 (5), pp. 607–618, 2015.
18. Saha, S., Ghosal, S., Chakraborty, A., Dhargupta, S., Sarkar, R., Mandal, J., Improved exploiting modification direction-based steganography using dynamic weightage array. Electron. Lett. 54 (8), pp. 498–500, 2018.
19. Zhang, X., Wang, S., Efficient stenographic embedding by exploiting modification direction. IEEE Commun. Lett. 10 (11), pp.781–783, 2006.
20. Mawengkang, H., Sitepu, I., Efendi, S., Security analysis in file with combinations One Time Pad Algorithm and Vigenere Algorithm. In: IOP Conf. Series: Materials Science and Engineering (2018) 2nd Nommensen nternational Conference on Technology and Engineering, pp. 21–29, 2018.
21. Mediacrypt AG, The IDEA Block Cipher, submission to the NESSIE Project, http://cryptonessie.org
22. USC-SIPI Image Database. Available from: https://sipi.usc.edu/database/.

23. Lin, K., Hong, W., Chen, J., Chen, T., Chiang, W., n et al., Data hiding by exploiting modification direction technique using optimal pixel grouping. In: IEEE 2010 2nd international Conference on Education Technology and Computer (ICETC). 2010.
24. Naidu, Deeraj Ananda Kumar, K. S. Jadav, Shwetha L. Sinchana, M. N. " Multilayer Security in Protecting and Hiding Multimedia Data using Cryptography and Steganography Techniques", 2019 4th IEEE International Conference on Recent trends on Electronics, Information, Communication and Technology, RTEICT 2019 – Proceedings, pp. 1360-136, 2019.

AUTHORS PROFILE

G.Mallikharjuna Rao is working as Assistant Professor in the ECE department and associated to coordinate with student clubs and industry research. He has gudied several projects under his supervision. He did his B. Tech degree from Madras University. He completed his M. Tech degree from KLU University and pursuing Ph. D from Osmania University. He is working as an Assistant Professor in the Department of Electronics and Communication Engineering at Chaitanya Bharathi Institute of Techcnology, Hyderabad. He contributed International journals and conferences. His area of speciliazation is inforamtion security.

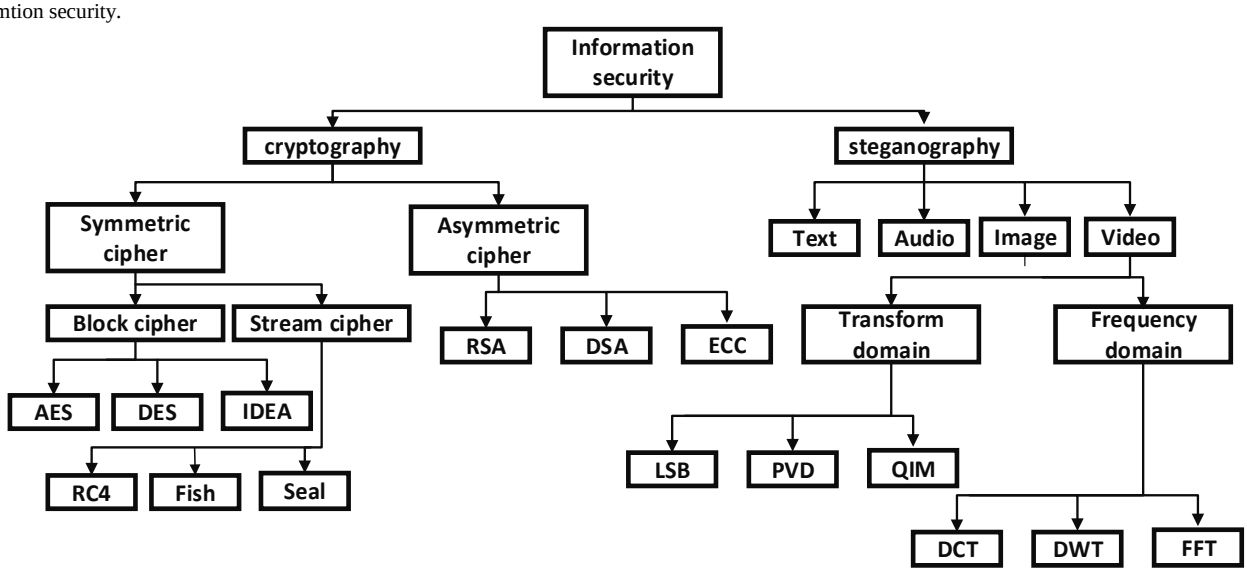


Fig 1: Cryptography, and image steganography methods tree diagram

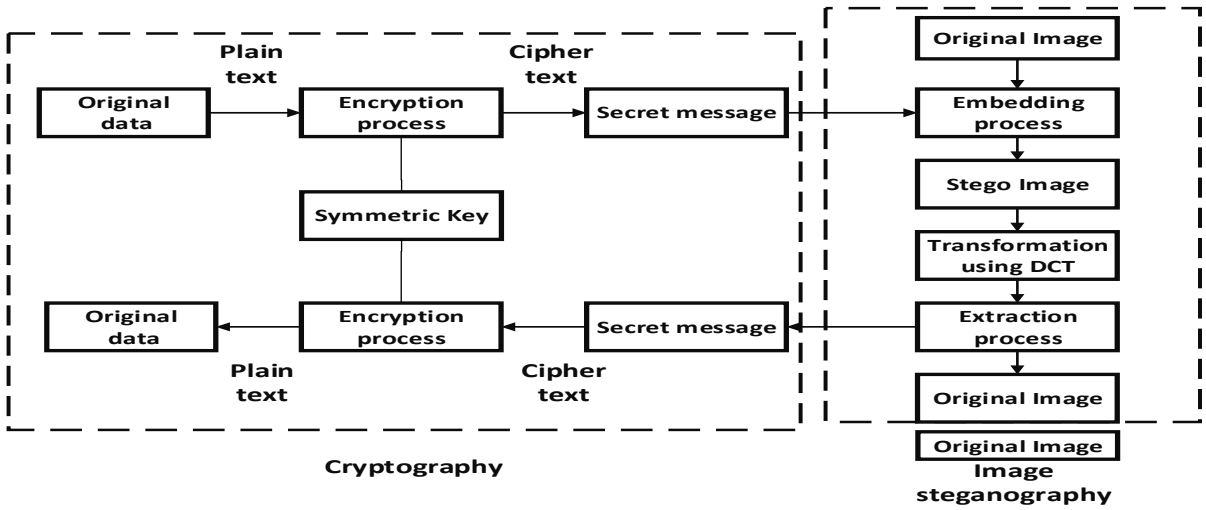


Fig. 2. Combination of Cryptography and Image steganography

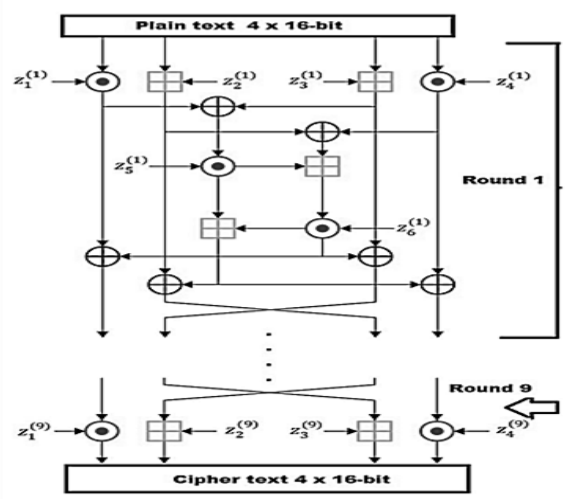


Fig. 3. Encryption process using IDEA

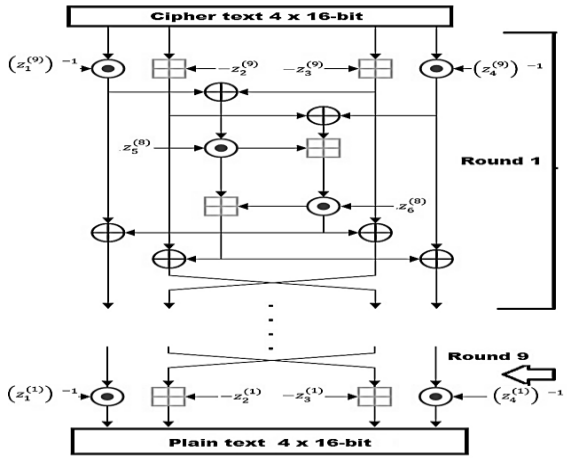
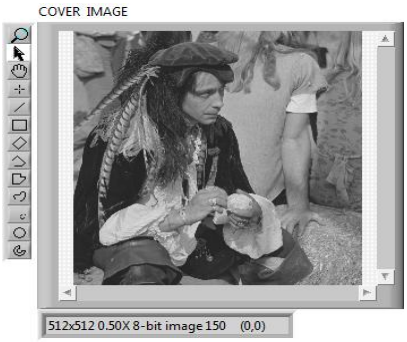


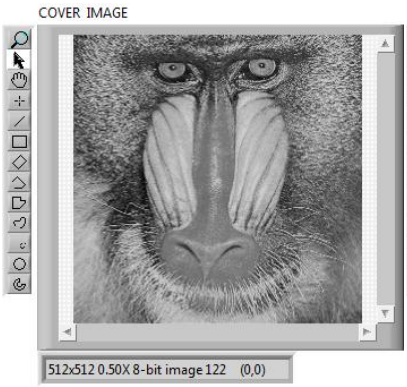
Fig. 4. Decryption process using IDEA

(a) Airplane F16



(b) Man

(c) Lena



(d) Baboon

(e) Pepper

(f) Tiffany

Fig. 5. The test cover images a, b, c, d, e, and f to experiment with different payloads by a suggested scheme

Fig. 6. Application tool development for encryption, embedding, extracting and Decryption

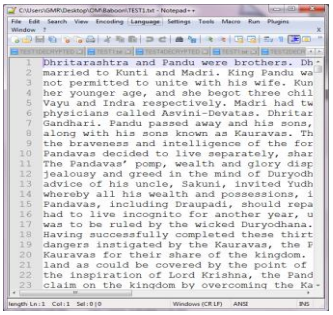


Fig. 7. Original Text file in english alphabets used as a payload

Fig. 8. Encryption form of text file using IDEA algorithm

Fig. 9. Password protected process of hiding information

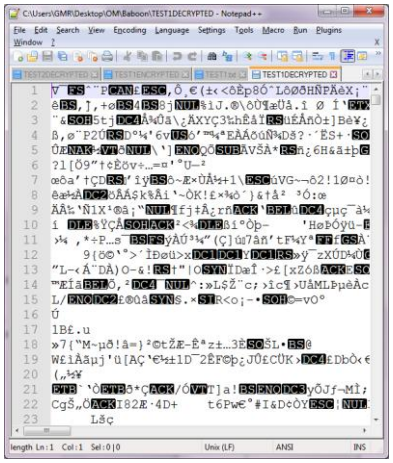


Fig. 10. Unreadable form of encrypted text

Fig. 11. Airplane F16 test image with text file after embedding process

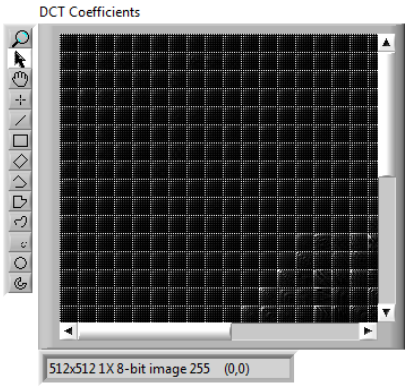


Fig. 12. Unreadable form of DCT coefficients of Airplane F16 test image with text file

Fig. 13. Airplane F16 test image with text file after extraction process

Fig. 14. Decrypting the original text file in english alphabets

Fig. 15. Applying password to retrive the text file

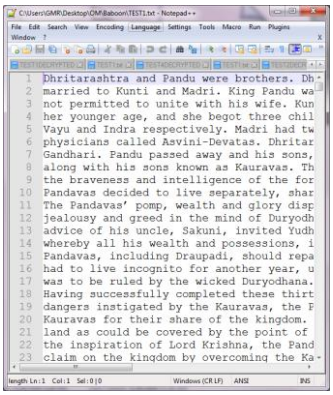


Fig. 16. Recovered original Text file in english alphabets without loosing information

Table- III: PSNR, MSE and SSIM values of suggested scheme

Payload	Standard test images						
	Metrics	Airplane F16	Baboon	lena	Man	Peppers	Tiffany
52,400 bytes	PSNR	89.3059	89.3059	89.7635	89.3059	91.9023	91.9023
	MSE	7.62E-5	7.62E-5	6.86E-5	7.62E-5	4.19E-5	4.19E-5
	SSIM	1	1	1	1	1	1
49,152 bytes	PSNR	89.3059	89.3059	89.7635	89.3059	91.9023	91.9023
	MSE	7.62E-5	7.62E-5	6.86E-5	7.62E-5	4.19E-5	4.19E-5
	SSIM	1	1	1	1	1	1

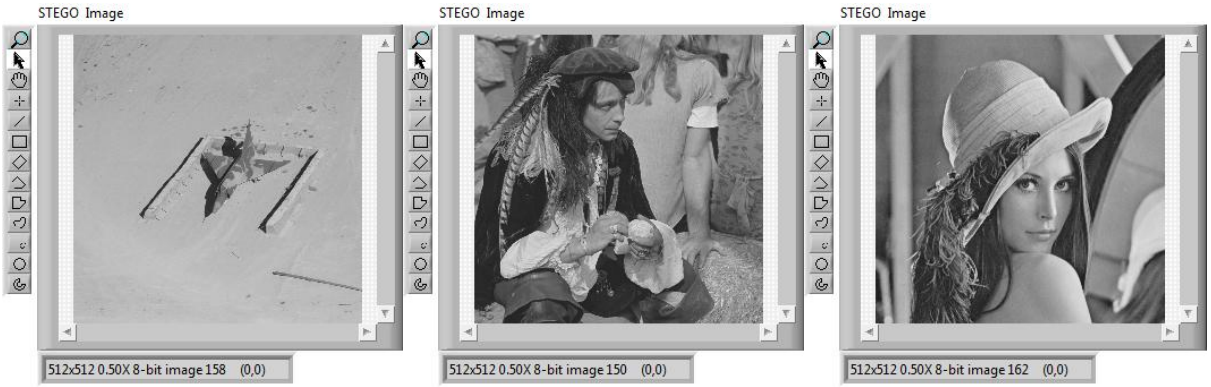
32,768 bytes	PSNR	89.3059	89.3059	89.7635	89.3059	91.9023	91.9023
	MSE	7.62E-5	7.62E-5	6.86E-5	7.62E-5	4.19E-5	4.19E-5
	SSIM	1	1	1	1	1	1
16,384 bytes	PSNR	89.3059	89.3059	89.7635	89.3059	91.9023	91.9023
	MSE	7.62E-5	7.62E-5	6.86E-5	7.62E-5	4.19E-5	4.19E-5
	SSIM	1	1	1	1	1	1

Table- IV: A comparison between suggested scheme and old methods

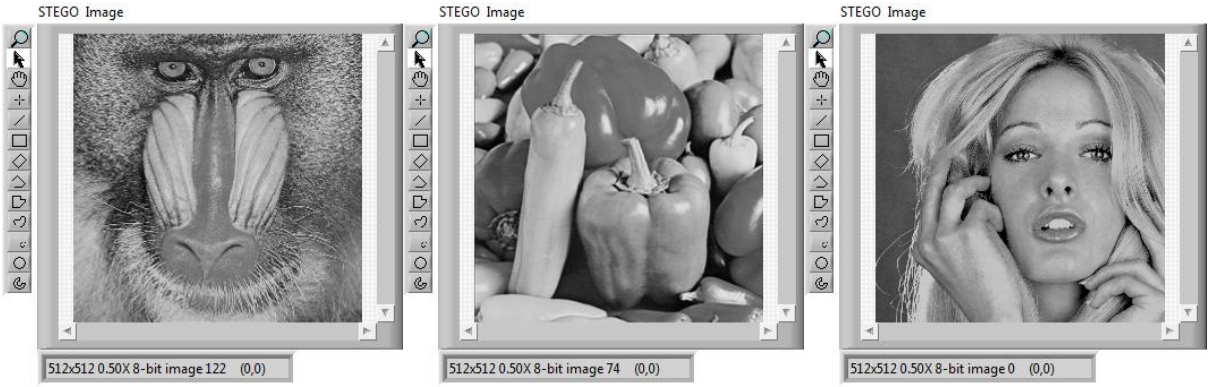
Methods	Payload	PSNR value				Average of PSNR value
		lena	Baboon	Airplane F16	Tiffany	
Suggested scheme	52,400 bytes	89.7635	89.3059	89.3059	91.9023	90.06
Opt EMD [23]		overflow				
EMD [19]		overflow				
LSB [9]		overflow				
Suggested scheme	49,152 bytes	89.7635	89.3059	89.3059	91.9019	90.06
Opt EMD [23]		52.11	52.11	52.10	52.11	52.11
EMD [19]		52.11	52.11	52.10	52.11	52.11
LSB [9]		45.91	45.92	45.63	45.94	45.85
Suggested scheme	32,768 bytes	89.7635	89.3059	89.3059	91.9019	90.06
Opt EMD [23]		54.67	54.66	54.67	54.66	54.66
EMD [19]		53.86	53.87	53.87	53.86	53.87
LSB [9]		51.14	51.14	51.16	51.14	51.14
Suggested scheme	16,384 bytes	89.7635	89.3059	89.3059	91.9019	90.06
Opt EMD [23]		58.37	58.38	58.36	58.36	58.37
EMD [19]		56.88	56.89	56.89	56.88	58.89
LSB [9]		54.16	54.15	54.16	54.15	54.16

Table- V: A comparison between the suggested scheme and other scheme

Methods	Payload	PSNR value				Average of PSNR value
		lena	Baboon	Airplane F16	Tiffany	
Suggested scheme	32,768 bytes	89.7635	89.3059	89.3059	91.9023	90.06
Knight tour algo [13]		43.871	43.893	44.098	44.018	43.97
Suggested scheme	20,480 bytes	89.7635	89.3059	89.3059	91.9023	90.06
Knight tour algo [13]		45.928	45.936	46.261	46.076	46.05
Suggested scheme	10,240 bytes	89.7635	89.3059	89.3059	91.9023	90.06
Knight tour algo [13]		49.038	48.943	49.196	49.042	49.05
Suggested scheme	5,120 bytes	89.7635	89.3059	89.3059	91.9023	90.06
Knight tour algo [13]		52.079	51.936	52.168	52.138	52.08
Suggested scheme	5,120 bytes	89.7635	89.3059	89.3059	91.9023	90.06
Knight tour algo [13]		58.834	58.973	58.874	59.091	58.94



(a) Airplane F16 **(b) Man** **(c) Lena**



(d) Baboon **(e) Pepper** **(f) Tiffany**

Fig. 17. Reconstructed Images a, b, c, d, e and f after complete process